# Algebraic certificates for graph problems

Rémi Pellerin



THÈSE
en vue de l'obtention du grade de Docteur, délivré par
l'ÉCOLE NORMALE SUPERIEURE DE LYON

**École Doctorale** N°512
École Doctorale en Informatique et Mathématiques de Lyon

**Discipline :** Informatique

Soutenue publiquement le 11/12/2023, par :

**Rémi Pellerin**

# Certificats algébriques pour des problèmes de graphes

Devant le jury composé de :

| | | | |
|---|---|---|---|
| OSSONA DE MENDEZ, Patrice | Chargé de Recherche | Rapporteur | CAMS |
| HAVET, Frédéric | Directeur de Recherche | Rapporteur | Université Côte d'Azur |
| KOIRAN, Pascal | Professeur des Universités | Examinateur | ENS de Lyon |
| NEWMAN, Alantha | Chargée de Recherche | Examinatrice | Université Grenoble Alpes |
| THOMASSÉ, Stéphan | Professeur des Universités | Directeur de thèse | ENS de Lyon |

*À Charles, qui a encore tant à apprendre!*

# Résumé

Les problèmes étudiés dans le domaine de la combinatoire sont souvent de la forme "Est-il vrai qu'un objet $X$ satisfait la propriété $Y$ ?". Si c'est vrai, l'informaticien aime avoir un "certificat". Par exemple, si la question est de savoir si un graphe admet une 3-coloration, alors, une telle coloration fournit un certificat dans le cas d'une réponse positive. Qu'en est-il si la réponse est négative ? Quel serait un certificat du fait qu'un graphe n'est pas 3-coloriable ? Quelle serait une raison "évidente" pour laquelle un graphe n'admet pas de couplage parfait, ou qu'un autre n'admet pas de stable de taille $n/3$ ? Dans le cas d'une réponse négative, l'idée de certificat semble plus complexe. Au cours de cette thèse, nous avons travaillé sur le problème de la coloration. Nous avons proposé un type de certificat canonique de non $k$-coloriabilité dans le cas général qui, si $G$ est un graphe tel que $\chi(G) > k$, fait intervenir un nouvel objet combinatoire construit à partir de $G$ : le graphe ${\mathbb{Z}_k}^G$. Cet objet est lié aux certificats algébriques liés au théorème des zéros de Hilbert (Nullstellensatz) déjà mis en évidence par Bayer ([5]), Alon et Tarsi ([2]) et étudiés par De Loera et al ([13]) et Li, Lowenstein et Omar ([6]). Notre construction donne une interprétation combinatoire à ces certificats qui n'étaient jusque là que de purs objets algébriques. De plus, les graphes ainsi définis, appelés *graphes exponentiels* sont en eux-mêmes des objets intéressants dont nous avons exploré les propriétés. Nous avons défini, plus généralement, ${\Gamma_k}^G$ où $\Gamma_k$ désigne soit l'anneau $\mathbb{Z}_k$, soit, si défini, le corps à $k$ éléments $\mathbb{F}_k$. Lorsque $k$ est un nombre premier, les deux structures sont identiques et on les note alors $k^G$. À l'inverse, si $k$ est une puissance non triviale d'un nombre premier, ces deux structures sont différentes. Pourtant, nous montrons que aussi bien ${\mathbb{Z}_k}^G$ que ${\mathbb{F}_k}^G$ comportent un certificat de non $k$-coloriabilité pour $G$ dès lors que $\chi(G) > k$ sans pour autant que ces deux graphes soient isomorphes. Ce certificat, appelé *edge-clique certificat* est lié aux certificats algébriques issus du Nullstellensatz dans le cas de ${\mathbb{Z}_k}^G$ mais pas dans celui de ${\mathbb{F}_k}^G$ où nous ne connaissons pas de correspondance simple en algèbre. L'étude de ces graphes exponentiels s'est révélée riche. Nous avons notamment montré que si ${\Gamma_k}^G$ et ${\Gamma_k}^{G'}$ sont isomorphes, alors $G$ et $G'$ sont isomorphes. Autrement dit, il est possible de définir un logarithme sur les graphes exponentiels. Nous avons également étudié les colorations des graphes exponentiels. Un de nos résultats qui justifie l'intérêt porté à la structure est le suivant : Pour toute puissance de nombre premier $q$, un graphe $G$ vérifie $\chi(G) = q$ si, et seulement si, $\chi\left({\mathbb{F}_q}^G\right) = q$. La preuve que nous proposons est non constructive en ce sens qu'elle ne permet pas de trouver une $q$-coloration de $G$ à partir d'une $q$-coloration de ${\mathbb{F}_q}^G$. De plus, s'il est possible de construire une $q$-coloration de ${\mathbb{F}_q}^G$ à partir

d'une coloration de $G$, nous ne savons pas, en général, ce que sont les $q$-colorations de ${\mathbb{F}_q}^G$. Cependant, dans le cas particulier où $q = 3$, nous avons établi que toutes les 3-colorations du graphe $3^G$ sont des extensions affines d'une coloration de $G$.

L'étude de ces graphes exponentiels a révélé un lien étroit avec ce que nous appelons l'*analyse de Fourier sur les graphes*. En particulier, nous introduisons la notion de *precoloring* qui est une fonction sommant à zéro sur toutes les *edge-cliques* (qui sont un type spécial de cliques dans le contexte des graphes exponentiels) d'un graphe exponentiel. L'existence d'un precoloring non nul conduit à l'existence d'une coloration de $G$. L'ensemble de ces fonctions est un espace vectoriel et les transformées de Fourier des colorations de $G$ en forment une base. Ceci nous a conduit à donner une preuve simple du théorème des zéros dans le cas particulier qui nous intéresse dans cette thèse.

À partir de ces notions, nous avons développé une théorie visant cette fois à montrer l'existence d'une $k$-coloration. Bien que, selon nous, fort prometteuse, cette théorie est difficile à appliquer, même dans des cas simples. Nous avons cependant pu l'utiliser pour donner une nouvelle preuve, assez courte et élégante, de la conjecture d'Erdös sur la 3-colorabilité des graphes formés d'un cycle hamiltonien et d'une union disjointe de triangles ([16]).

Enfin, nous donnons un noyau en $O(k^2 \log k)$ pour le *cograph editing problem*, améliorant un résultat de Havet et al ([17]).

# Abstract

Problems in combinatorics are often questions of the form "Is it true that object X satisfies property Y?". If true, the computer scientist often wants some "certificate". For instance, if the question is whether some graph admits a 3-coloring, we would like an example of such coloring as a certificate. However, in case the answer is negative, the notion of certificate is unclear. How could you certify that some graph is not 3-colorable? Is there an obvious reason for which some graph has no perfect matching, or that another graph has no stable set of size $n/3$? In this PhD thesis, we have studied the coloring problem. We have introduced a canonical way to certify the non $k$-colorability of graphs. If $\chi(G) > k$, this certificate is related to a new graph defined from $G$ that we denote by ${\mathbb{Z}_k}^G$ and that we call *power graph*. This combinatorial object is connected the algebraic certificates related to Hilbert's Nullstellensatz theorem introduced by Bayer ([5]), Alon and Tarsi ([2]), and studied by De Loera et al ([13]) and Li, Lowenstein and Omar ([6]). Our construction allows a combinatorial interpretation of those Nullstellensatz certificates. Moreover, those power graphs are interesting objects of which we explored the properties. We have defined, more generally, ${\Gamma_k}^G$ where $\Gamma_k$ is either the ring $\mathbb{Z}_k$, or, when defined, the field with $k$ elements $\mathbb{F}_k$. When $k$ is a prime number, those structures are identical so we use the notation $k^G$. On the contrary, if $k$ is a non trivial power of a prime number, those structures are different. Yet, we prove that ${\mathbb{Z}_k}^G$, as well as ${\mathbb{F}_k}^G$, contains a certificate of non $k$-colorability whenever $\chi(G) > k$ although those two graphs are not isomorphic. This certificate, called *edge-clique certificate*, is connected to the Nullstellensatz certificates in the case of ${\mathbb{Z}_k}^G$ but not in the case of ${\mathbb{F}_k}^G$ where we do not know any correspondence in algebra. The study of those power graphs revealed itself interesting. For instance, we prove that if ${\Gamma_k}^G$ and ${\Gamma_k}^{G'}$ are isomorphic then $G$ and $G'$ are isomorphic. In other words, it is possible to define a logarithm on the power graphs. We did also study the colorings of those power graphs. One of our results that justify the interest for the structure is the following: For every power of a prime number $q$, a graph $G$ satisfies $\chi(G) = q$ if, and only if, $\chi\left({\mathbb{F}_q}^G\right) = q$. Our proof of this result is non constructive in the sens that it does not explain how to build such $q$-coloring of $G$ from a $q$-coloring of ${\mathbb{F}_q}^G$. Moreover, although we can build a $q$-coloring of ${\mathbb{F}_q}^G$ from a $q$-coloring of $G$, we do not know the shape of the $q$-colorings of ${\mathbb{F}_q}^G$ in general. However, in the specific case where $q = 3$, we prove that the $q$-colorings of ${\mathbb{F}_q}^G$ are affine extensions of the $q$-colorings of $G$.

The study of those power graphs has shown a narrow connection with what we call the *Fourier analysis on graphs*. In particular, we introduce the notion of *precoloring* that is a function that sums to zero on every edge-cliques (which are special cliques in the context of power graphs) of a power graph. The existence of a non zero precoloring leads to the existence of a coloring for $G$. The set of those functions is a linear space and the Fourier transform of the colorings of $G$ form a basis of that space. This allowed us to propose a simple proof of the Nullstellensatz theorem in the specific case of interest for this thesis.

With those notions, we developed a theory aiming at proving colorability results. Although, according to us, this theory is promising, it is hard to use, even on simple examples. Still, we have been able to use it in order to make a new simple and quite elegant proof of Erdös conjecture on the 3-colorability of graphs formed by a Hamiltonian cycle and a disjoint union of triangles.

Finally, we prove a kernel in $O(k^2 \log k)$ for the *cograph editing problem*, improving a result of Havet et al ([17]).

# Acknowledgements

I want to thank my advisor Stephan Thomassé for his help all along these 4 last years. Working with him was pleasant and very beneficial to the young mathematician I was in 2019.

I am also grateful toward Natasha Morrison and Pierre Charbit for fruitful collaboration, especially at the earliest stage of my PhD. I have really enjoyed those moments when each of us were at the blackboard proposing new ideas. Pierre and Natasha played an important role in the discovery of the Fourier method.

To my collegues and friends from the LIP Julien Duron, Paul Fermé, Carl Fegahli for the time spent nearby the coffee machine talking about graphs, mathematics in general but also of non scientific topics, which contributed to an important equilibrium during those years working on my thesis.

To Nicolas Trotignon, head of laboratory, the other researchers of the LIP and to the members of the jury: Patrice Ossona de Mendez, Frédéric Havet, Alantha Newman and Pascal Koiran.

Last but not least, I want to sincerely thank my wife Marie for daily support, my parents Sylvain and Frédérique and my stepparents Pierre-Marc and Bénédicte.

# Notations

| | |
|---|---|
| **Common** | |
| $\mathbb{N}$ | The set of all non negative integers |
| $\mathbb{Z}$ | The set of all integers |
| $\mathbb{R}$ | The set of all real numbers |
| $\mathbb{C}$ | The set of all complex numbers |
| $[\![ k\ ;\ \ell ]\!]$ | The set of integers $\{i \in \mathbb{Z} \colon k \leq i \leq \ell\}$ with $k, \ell \in \mathbb{Z}$ |
| $F^E$ | The set of the total functions from set $E$ to set $F$ |
| $\mathcal{P}(X)$ or $2^X$ | The power set of the set $X$ |
| $\binom{X}{k}$ | The subsets of the set $X$ of cardinality $k$ |
| $E \uplus F$ | The union of $E$ and $F$ when $E \cap F = \varnothing$ |
| $\lvert X \rvert$ | The cardinality of set $X$ |
| $\mathbb{1}_x$ | For a set $E$ and $x \in E$, the indicator function of $x$ in $E$ |
| j | The primitive cubic root of unity $\mathrm{e}^{\frac{2\mathrm{i}\pi}{3}}$ |
| **Graph theory** | |
| $G[X]$ | The subgraph induced by $X$ on $G$ |
| $H \subseteq G$ | $H$ is an induced subgraph of $G$ |
| $uv$ | The (unoriented) edge between the vertices $u$ and $v$ |
| $G \oplus H$ | The fulljoin of graph $G$ and graph $H$ |
| $G + H$ | The disjoint union of graphs $G$ and $H$ |
| **General algebra** | |
| $k \wedge n$ | The GCD of integers $k$ and $n$ |
| $\mathbb{F}_q$ | The field of cardinality $q$ (when defined) |
| $\mathbb{Z}_n$ | The ring of integers modulo $n$ |
| $\mathbb{U}_n$ | The group of $n^{\text{th}}$ roots of unity in $\mathbb{C}$ |
| $\mathcal{A}[X_1, \ldots, X_n]$ | Polynomials in $X_1, \ldots, X_n$ with coefficients in the ring $\mathcal{A}$ |
| **Linear algebra** | |
| $\mathrm{Im}_{\mathbb{K}}\, M$ | The image of the matrix $M$ in the field $\mathbb{K}$ |
| $\mathrm{Ker}_{\mathbb{K}}$ | The kernel of the matrix $M$ in the field $\mathbb{K}$ |
| $\mathscr{M}_{n,k}(\mathcal{A})$ | The set of $n \times k$ matrices with coefficients in the ring $\mathcal{A}$ |
| $M \otimes N$ | The kronecker (or tensor) product of matrix $M$ by matrix $N$ |
| ${}^{\mathrm{t}}M$ | The transpose of matrix $M$ |
| $X^{\perp}$ | The set of vectors orthogonal to every element of the set $X$ |

# Contents

# Introduction (in french)

This chapter is an introduction for french readers. A translation of this introduction can be found in the next chapter.

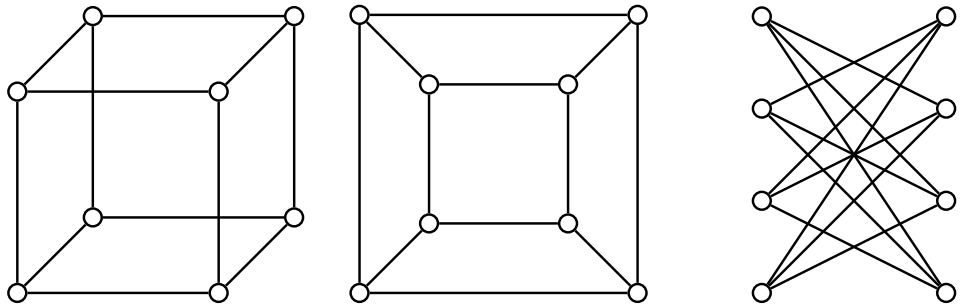
Cette thèse traite de *théorie des graphes*, un sous-domaine des *mathématiques discrètes* aussi appelées *informatique fondamentale*. Son objectif est la mise en place d'outils théoriques algébriques utiles pour la résolution de problèmes combinatoires portant sur les graphes.

Les graphes constituent un concept mathématique simple et pourtant très utile pour beaucoup de situations concrètes. C'est en 1735 que Leonhard Euler utilise cette notion pour résoudre une énigme devenue célèbre : le problème des sept ponts de Königsberg. Cette ville de Prusse-Orientale[1] compte sept ponts permettant de rallier une île et une presqu'île. Est-il possible de se promener dans la ville en empruntant une et une seule fois chacun des ponts et en revenant à son point de départ ? Cela semblait bien impossible... Cependant, comment en être certain ? Euler chercha une preuve mathématique de cette impossibilité. Sans nous comparer à cet immense mathématicien, c'est également ce que nous avons cherché à faire au cours de cette thèse : donner des certificats d'impossibilité pour des problèmes de graphes. Et, le problème des sept ponts de Königsberg en est un !

Formellement, un graphe est un ensemble de points appelés *sommets* reliés entre eux par des traits appelés *arêtes*. On dit de deux sommet reliés par une arête qu'ils sont *adjacents*. Par exemple, un cube, ou plus généralement n'importe quel polyèdre, est un graphe. On peut parfois dessiner un graphe. Par exemple, la Figure 1 donne trois représentations différentes d'un même graphe : le cube. Cela peut sembler surprenant de prime abord mais il s'agit bien du même objet dessiné de trois façons différentes. Les relations d'adjacence, seule information contenue dans un graphe, sont en effet les mêmes dans les trois cas.

Dans un graphe, un ensemble de sommets $S$ tel qu'aucune arête ne relie deux de ces sommets est appelé un *stable* ou encore un *ensemble indépendant*. Inversement, un graphe dont toutes les paires de sommets sont reliées par des arêtes est appelée une *clique*. Pour illustrer ces notions, considérons une communauté de personnes, par exemple, les paroissiens d'une église dans une grande ville comme Lyon. Supposons vouloir organiser un dîner en rassemblant des paroissiens qui ne se connaissent pas. On peut modéliser ce problème à l'aide d'un graphe : chaque sommet représente un paroissien et on relie deux paroissiens par une arête si, et seulement si, ils se connaissent déjà. Un stable du graphe fournit un

[1] qui est désormais russe et rebaptisée Kaliningrad



(a) Représentation usuelle (b) Représentation planaire (c) Représentation bipartie

Figure 1: Trois représentations graphiques du cube

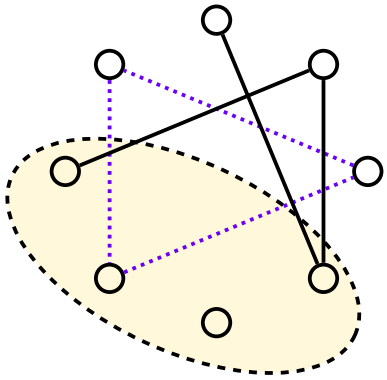


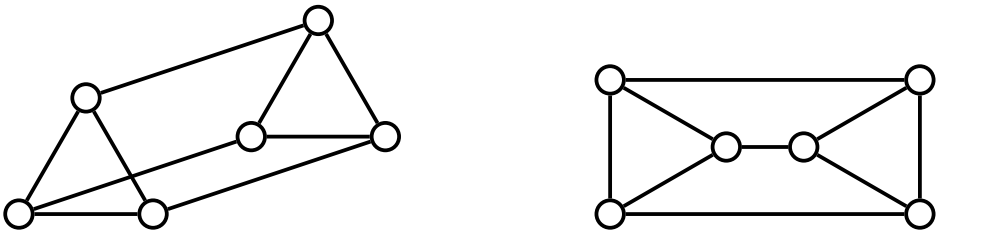
Figure 2: Une clique de taille maximale en pointillés violets et un stable de taille maximale en dans l'ellipse en pointillé

ensemble de paroissiens qui ne se sont encore jamais rencontrés (sur la Figure 2, on peut par exemple considérer les sommets dans l'ellipse). Si à l'inverse on souhaite réunir uniquement des gens se connaissant déjà, on chercherait alors une *clique*, c'est-à-dire un ensemble de sommets comportant un maximum d'arête (par exemple, le triangle en pointillés violets sur la Figure 2). Le degré d'un sommet est le nombre de ses voisins. Ainsi, un sommet de degré maximum représente ici un paroissien parmi les plus populaires. Le problème de déterminer un stable de taille maximale (ou *stable maximum*) est en général difficile[2]. Il en va de même pour le problème de trouver une clique de taille maximale dans un graphe, ces deux problèmes étant substantiellement identiques puisqu'une clique dans $G$ est un stable dans le *complémentaire* de $G$, c'est-à-dire le graphe obtenu à partir de $G$ en inversant la relation d'adjacence.

[2]C'est un problème NP-complet.

## Une brève histoire de la théorie des graphes

En 1852, les frères mathématiciens Francis et Frédérick Guthrie font une conjecture surprenante : toute carte peut être coloriée avec seulement quatre couleurs. Plus précisément, si l'on veut colorier chaque zone d'une carte (les pays du monde, les départements français ou encore ceux d'un pays imaginaire) de sorte que deux zones frontalières n'aient pas la même couleur[3], alors, il existe toujours une solution n'utilisant pas plus que quatre couleurs. Ne parvenant pas à prouver la conjecture, Frédérick demandera à son professeur : Auguste De Morgan. Ce brillant mathématicien fût également mis en échec. C'est Alfred Kempe qui en publiera la première démonstration, ou plutôt, tentative de démonstration car celle-ci s'avèrera fausse ! Kempe parvient tout de même à une preuve correcte d'un résultat plus faible : le théorème des cinq couleurs qui énonce que, sous les mêmes hypothèses, cinq couleurs suffisent. Ce problème de coloration de cartes se formalise naturellement avec les graphes en représentant chaque zone par un sommet et en définissant la relation d'adjacence par le fait de partager une frontière. Les graphes ainsi obtenus sont dits *planaires* car ils peuvent être représentés dans le plan sans qu'aucune de leurs arêtes ne se croise. Une telle classe de graphes est difficile à appréhender car la propriété qui la caractérise est plus complexe que l'on pourrait le croire. En effet, il est difficile de formaliser le fait qu'il existe une représentation dans laquelle les arêtes ne se croisent pas. C'est un concept difficile à manipuler formellement. Par exemple, la Figure 3 représente deux fois le même graphe : de façon planaire en 3b et non planaire en 3a. En outre, montrer qu'un graphe est non planaire n'est, en général, pas chose aisée. Par exemple, le graphe de Petersen (voir Figure 4) ne peut pas être représenté de façon planaire.



(a) prisme (b) prisme représenté de façon planaire

Figure 3: Deux représentations du prime

Ainsi, colorier les régions de la carte revient à choisir une couleur pour chaque sommet du graphe planaire sous-jacent sans que deux sommets adjacents n'aient la même couleur. Plus généralement, une *coloration* d'un graphe est un choix de couleurs pour chacun de ses sommets tel que deux sommets adjacents n'aient pas la même couleur. En particulier, les sommets d'une même couleur forment un stable. Malgré l'aspect moins esthétique, on utilisera des nombres en lieu et place des couleurs. Par exemple, le cube dont on a

[3]Il faudra considérer uniquement les frontières de longueur non nulle et donc exclure notamment les points triples comme il en existe sur Terre. De plus, on parle de couleur pour une zone, pas pour un pays. Ainsi, une exclave est considérée comme une zone distincte du pays auquel elle appartient.

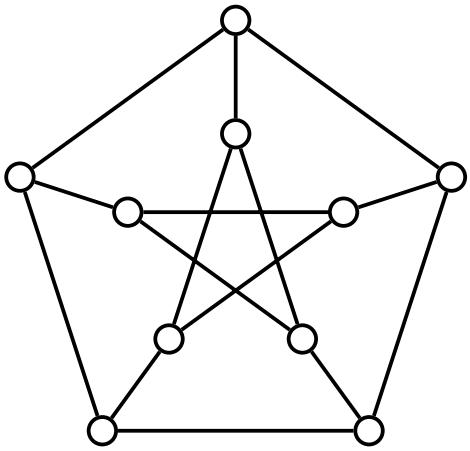
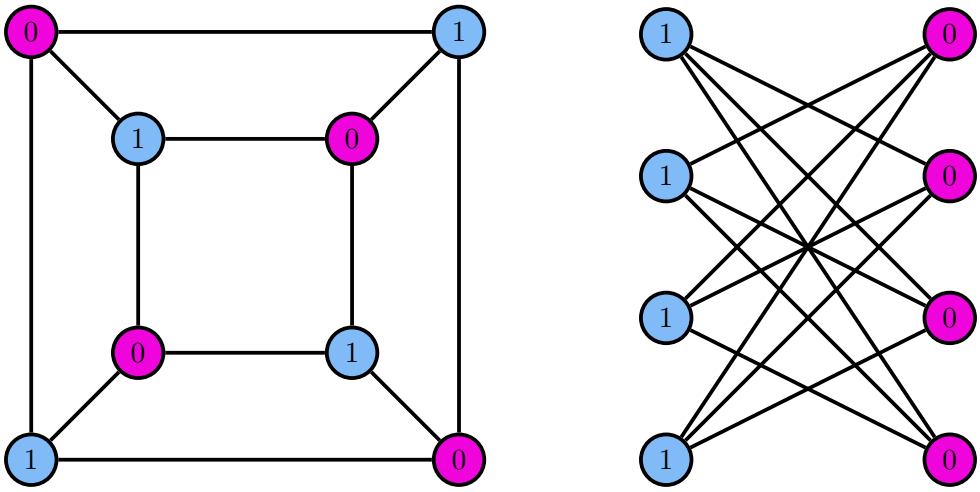


Figure 4: Graphe de Petersen

déjà donné trois représentations à la Figure 1 peut être colorié avec deux couleurs (voir Figure 5a). C'est particulièrement évident lorsque l'on adopte la représentation du cube comme un graphe biparti (voir Figure 5b) et, bien sûr, cette notion ne dépend pas de la manière dont on pourrait dessiner le graphe. Nous parlerons de *bonne coloration* (en anglais, *proper coloring*) ou simplement de *coloration* pour faire référence à un *étiquetage* des sommets (en anglais, *labelling*) qui respecte la condition énoncée ci-dessus. À l'inverse, lorsque cette condition n'est pas supposée vérifiée, on parlera simplement d'étiquetage.




(a) Une 2-coloration du cube (b) Une 2-coloration du cube

Figure 5: Coloration du cube avec deux couleurs

Dans le cas du cube, il est impossible d'utiliser moins de deux couleurs. On dit alors que le nombre chromatique du cube vaut 2. Plus généralement, le nombre chromatique d'un

graphe $G$, noté $\chi(G)$, est le nombre minimal de couleurs nécessaire pour colorier ce graphe. La Figure 6 montre une 3-coloration du graphe de Petersen. Il est impossible de colorier ce graphe avec moins de trois couleurs et donc son nombre chromatique vaut 3. Déterminer le nombre chromatique d'un graphe est, en général, un problème difficile.

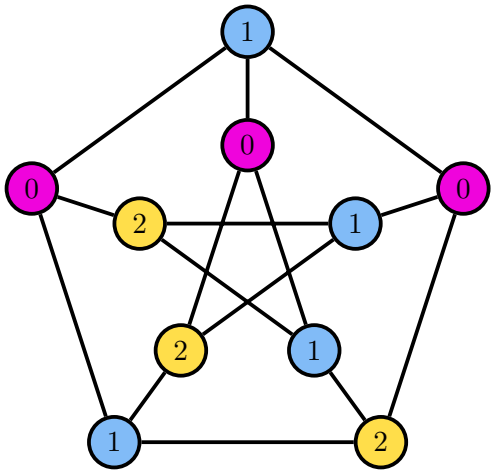



Figure 6: Une 3-coloration du graphe de Petersen

Le théorème des quatre couleurs énonce donc que le nombre chromatique d'un graphe planaire vaut au plus 4. Il faudra attendre 1976, soit plus d'un siècle après la conjecture des frères Guthrie, et les mathématiciens Kenneth Appel et Wolfgang Haken ([3]) pour avoir preuve correcte. Pour la première fois, la démonstration est assistée par ordinateur ce qui posera le problème suivant : comment être certain que la preuve est correcte en dépit d'une disjonction sur pas moins de 1478 cas et d'une longueur astronomique de 600 pages une fois imprimée[4] ? Plus tard, Robertson, Sanders, Seymour et Thomas simplifieront la preuve en ramenant le nombre de cas à 633. Aujourd'hui encore, le résultat reste mystérieux et la preuve peut laisser le mathématicien sur sa faim car peu éclairante sur les raisons de la validité du théorème. Selon Paul Erdös, le théorème des quatre couleurs est "un problème subtil et non pas un problème complexe", et une démonstration simple[5] devrait exister car la classe des graphes planaire est, selon lui, un sous-ensemble de la classe des graphes à considérer. Une preuve simple de ce célèbre résultat constituerait sans doute une grande nouvelle pour la communauté des mathématiciens.

La coloration de graphe intervient dans de nombreux problèmes d'optimisation. C'est sans doute la raison pour laquelle ce problème continue d'intéresser les chercheurs. Nous en donnons ici quelques exemples. Supposons devoir organiser des examens dans une université comportant de nombreuses classes et de nombreux cours. Bien sûr, deux épreuves auxquelles doit participer un même étudiant ne peuvent avoir lieu en même temps. Comment organiser les examens en parallélisant le plus possible les épreuves ? Définissons $G$ comme le graphe

[4]Une erreur sera d'ailleurs trouvée dans la preuve initiale !
[5]Une "proof from the Book" !

dont les sommets sont les épreuves et la relation d'adjacence entre deux sommets est définie par le fait que les deux épreuves concernent un même étudiant. Dans toute coloration, les sommets d'une même couleur sont des épreuves pouvant avoir lieu au même moment. Ainsi, une coloration atteignant $\chi(G)$ parallélise les examens de façon optimale.

Un autre exemple, en réalité tout à fait similaire, est celui du plan de table. Supposons devoir placer des invités à un mariage autour de tables de sorte que toute paire d'invités qui ne s'apprécient pas (ce qui, hélas, semble arriver dans toutes les familles) ne soient pas à la même table. Là encore, on peut modéliser le problème avec un graphe dont les sommets sont les invités et la relation d'adjacence définie par le fait que les invités ne s'apprécient pas. Une table doit donc être un stable du graphe. Ainsi, une coloration du graphe dont le nombre de couleurs est minimal donne un plan de table respectant les contraintes en minimisant le nombre de tables.

Enfin, supposons vouloir déployer un réseau d'antennes téléphoniques. On a besoin d'associer une bande de fréquences à chaque antenne. Idéalement, on aimerait réutiliser au maximum les bandes de fréquences car cela représente un coût. Cependant, deux antennes proches risquent d'interférer si elles communiquent sur les mêmes fréquences. On peut alors représenter chaque antenne par un sommet et relier les paires d'antennes trop proches par des arêtes. Le nombre chromatique du graphe ainsi obtenu correspond au nombre de bandes de fréquences minimal requis pour le dispositif.

D'une façon générale, on cherche des majorants et des minorants des nombres chromatiques des graphes d'une certaine classe. On dispose notamment de l'encadrement simple suivant :

**Théorème.** Soit $G$ un graphe, $\omega(G)$ la taille de sa plus grande clique et $\Delta(G)$ son degré maximum. On a

$$\omega(G) \leq \chi(G) \leq \Delta(G) + 1$$

Malheureusement, $\chi(G)$ peut être arbitrairement éloigné de ces bornes. En effet, il existe des graphes sans triangle de nombre chromatique arbitrairement grand (voir [25]) et, par ailleurs, un graphe constitué d'un sommet de degré $n$ et de $n$ sommets de degré 1 a un nombre chromatique de 2 mais un degré maximum de $n$.

Le problème de la coloration optimale d'un graphe est difficile car, bien que les contraintes soient locales, l'optimalité du nombre de couleurs se comprend globalement, dans le graphe entier. Ainsi, raisonner à partir de sous-graphes ne peut être une méthode fonctionnelle en général[6]. À l'inverse, la notion de *mineur*[7] d'un graphe semble prometteuse. Citons à ce titre la célèbre conjecture de Hadwiger ([18]), ouverte depuis 1943. Notons $\mathcal{H}(G)$ le nombre de Hadwiger de $G$, c'est-à-dire le plus petit entier $k$ tel que $G$ ait le graphe complet à $k$ sommets pour mineur.

**Conjecture** (Hadwiger)**.** Pour tout graphe $G$, $\chi(G) \leq \mathcal{H}(G)$.

[6]Si c'était le cas, le problème de la détermination du nombre chromatique serait dans $P$ et donc, on aurait P = NP...

[7]Un mineur d'un graphe $G$ est un graphe obtenu à partir de $G$ suite à l'application des opérations suivantes : suppression d'un sommet isolé, suppression d'une arête, contraction d'une arête.

## Les idées développées au cours de cette thèse

Prouver que l'on peut colorier un graphe donné $G$ avec $k$ couleurs est une chose. Montrer que ce nombre est minimal en est une autre. Un moyen de faire est de montrer qu'il est impossible de colorier $G$ avec $k-1$ couleurs. Ceci permet alors de déterminer le nombre chromatique de $G$ en l'approchant "par dessous". C'est le point de départ de cette thèse. Plus généralement, on aimerait, lorsque $\chi(G) > k$, un certificat de non $k$-coloriabilité pour $G$. Un tel certificat pourrait, *a priori*, prendre plusieurs formes. Par exemple, si $G$ contient une clique de taille $k+1$, alors cette clique constitue bien une preuve, un certificat que $\chi(G) > k$. La Figure 7 représente un graphe qui n'est pas 3-coloriable car il contient une clique de taille 4 représentée dans l'ellipse en pointillé.

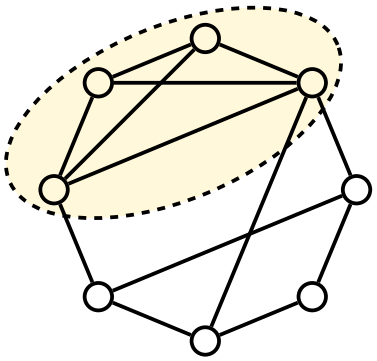
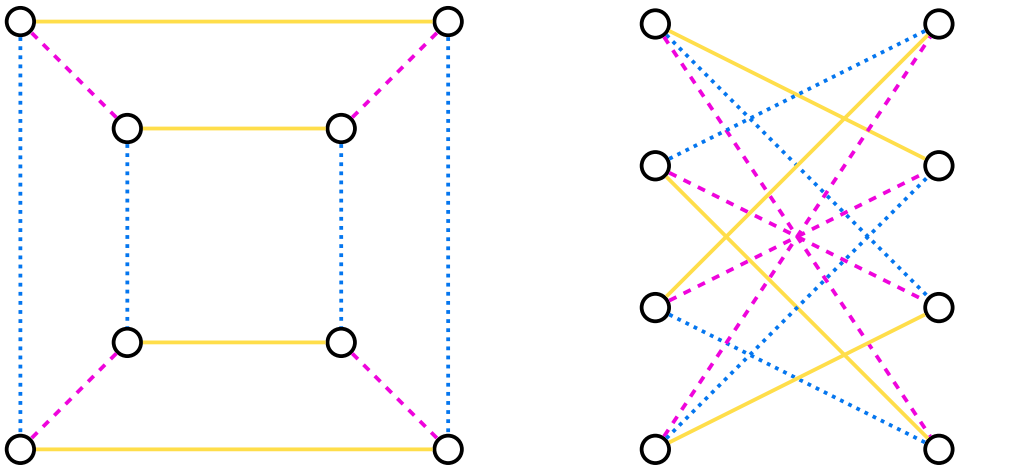


Figure 7: Un graphe contenant une clique de taille 4

Malheureusement, il n'est pas toujours possible de trouver un sous-graphe pouvant servir de certificat. Au cours de cette thèse, nous présenterons une méthode générique permettant de certifier qu'un graphe est non $k$-coloriable. Nos travaux s'inscrivent dans la lignée de ceux de Bayer ([5]), De Loera ([12], [13]) et Li, Lowenstein et Omar ([6]). Ceux-ci s'intéressent à l'utilisation des polynômes multivariés pour encoder le problème de la 3-colorabilité d'un graphe. En effet, le théorème Nullstellensatz d'Hilbert (1.5.1) fournit un certificat dans le cas où le graphe n'est pas $k$-coloriable. Ce certificat prend cependant la forme d'une famille de polynômes et n'a, *a priori*, aucun lien avec le graphe de départ $G$. Nous montrerons pourtant qu'il est possible de créer une extension "naturelle" du graphe $G$ dans laquelle un tel certificat algébrique a une interprétation combinatoire. Par exemple, si l'on s'intéresse à la 3-coloriabilité d'un graphe $G$, on peut définir un graphe noté $3^G$ qui vérifie $\chi(G) \leq 3 \Leftrightarrow \chi\left(3^G\right) \leq 3$ (voir la Section 1.3). Nous verrons qu'il y a, dans un cadre plus général, plusieurs extensions de graphes possibles lorsque $k$ n'est pas un nombre premier. Nous discuterons des différences entre ces différentes extensions à la Section 1.4.

Après avoir étudié ces extensions de graphes, que nous appelons *graphes exponentiels* ou *power graphs*, nous avons découvert un lien avec ce que l'on pourrait nommer *l'analyse de Fourier sur les graphes*. Afin d'illustrer ce concept, nous introduisons ici une nouvelle notion concernant la coloration de graphes : on souhaite maintenant colorier les arêtes d'un graphe.

La condition à respecter est désormais que deux arêtes adjacentes, c'est-à-dire reliées à un même sommet, doivent avoir des couleurs différentes. On parle alors de *edge-coloration* par opposition à la *vertex-coloration* que nous avons vue juste avant. Bien sûr, il ne s'agit pas là d'un problème fondamentalement différent puisque colorier les arêtes d'un graphe revient à colorier les sommets de son line graph[8]. La Figure 8a représente une 3-edge-coloration du cube. Il est bien sûr également possible de visualiser la même chose sur une représentation du cube comme graphe biparti (voir Figure 8b).



(a) 3-coloration des arêtes du cube (b) 3-coloration des arêtes du cube

Figure 8: Deux représentations d'une edge-coloration du cube avec trois couleurs

Notre idée est d'utiliser la seconde représentation et de faire la remarque suivante : une coloration des arêtes d'un graphe biparti est correcte si, et seulement si, elle est correcte pour les sommets de droite ainsi que pour les sommets de gauche. Dit autrement, une coloration des arêtes d'un graphe biparti est bonne si, et seulement si, deux arêtes incidentes à droite (resp. à gauche) sont de couleurs différentes. Ceci peut être exprimé simplement à l'aide d'un produit scalaire : considérons le vecteur $f_L$ de taille $3^{m/2}$ ($m$ étant le nombre d'arêtes du graphe) indexé par tous les 3-étiquetages possibles des arêtes qui a un 1 en face des 3-colorations des arêtes bonnes du point de vue des sommets de gauche, et un 0 sinon. De même, on définit de façon analogue $f_R$ le vecteur caractéristique des 3-colorations des arêtes bonnes à droite. Par construction, $\langle f_L, f_R \rangle$ est le nombre de bonnes 3-colorations des arêtes de $G$. Ainsi, montrer que ce produit scalaire est non nul revient à prouver que $G$ est 3-edge-coloriable. Une introduction plus formelle de cela est faite à la Section 2.1.

Plutôt que de calculer directement ce produit scalaire, nous calculons $\left\langle \widehat{f_L}, \widehat{f_R} \right\rangle$ où $\widehat{\cdot}$ désigne la multiplication par une matrice de Fourier appropriée (voir Section 2.2). Ces matrices ont la propriété de conserver le produit scalaire de sorte que $\langle f_L, f_R \rangle = \left\langle \widehat{f_L}, \widehat{f_R} \right\rangle$. Dans

[8]Le line graph d'un graphe $G$, noté $\mathscr{L}(G)$, a pour ensemble de sommets les arêtes de $G$. De plus, deux sommets de $\mathscr{L}(G)$ sont reliés si et seulement si les arêtes correspondantes sont adjacentes dans $G$.

certains cas, nous avons un argument simple permettant d'affirmer que ce dernier produit scalaire est non nul. Notons que notre méthode fonctionne également avec des graphes non bipartis moyennant quelques changements (voir par exemple la Proposition 2.1.2) ainsi qu'avec la coloration de sommets. Nous proposons à ce titre une nouvelle preuve du théorème de Fleischner et Stiebitz ([16]) à la Section 2.3.1.

L'analyse de Fourier sur les graphes développée dans cette thèse a un lien avec les graphes exponentiels. Les transformées de Fourier des bonnes colorations forment en effet une base de l'espace des *precolorings* qui sont des fonctions qui admettent une caractérisation simple sur les graphes exponentiels. Ceci est détaillé à la Section 2.2.5.

Enfin, de nombreuses questions naturelles peuvent être traitées au sujet des graphes exponentiels. En particulier, quelles sont les propriétés de $G$ qu'on retrouve nécessairement dans ses différentes exponentielles ? Comment une modification sur $G$ se répercute-t-elle ? Ces questions sont délicates et beaucoup restent ouvertes. Au cours de nos recherches, nous avons étudié le problème d'édition vers un cographe : Étant donné un graphe $G$, comment éditer (changer les relations d'adjacence), de façon optimale (à la fois en nombre d'arêtes modifiées et en temps d'éxécution) pour le transformer en un graphe sans chemin de taille 4 induit ? Une introduction plus complète à ces problèmes d'édition est faite à la Section 3.1. Nous avons amélioré un résultat de Havet et al ([17]) en passant d'un noyau cubique à un noyau "quasi-quadratique"[9]. L'article a été accepté dans *Discrete Applied Maths* et sera publié prochainement.

## Introduction aux preuves algébriques sur les graphes

Dans le but de mettre en perspective les travaux réalisés au cours de cette thèse, nous illustrons ici quelques résultats sur les polynômes qui ont été utilisés pour montrer des théorèmes sur les graphes. Ceux-ci sont essentiellement basés sur le résultat suivant, dit Nullstellensatz combinatoire. Ce théorème a permis de montrer de nombreux résultats et, en particulier, des résultats de coloration. Nous donnons ici certains de ces résultats et en esquissons certaines preuves. L'idée générale consiste à introduire un polynôme dont les racines sont les solutions du problème (typiquement, une bonne coloration d'un graphe donné). Le Nullstellensatz combinatoire donne des conditions sur les racines d'un tel polynôme et permet alors de conclure, en utilisant une preuve par l'absurde, à l'existence d'une solution.

**Théorème** (Nullstellensatz combinatoire)**.** Soient $\mathbb{K}$ un corps commutatif, $n \in \mathbb{N}^*$ et $P \in \mathbb{K}[X_1, \ldots, X_n]$. Soient $S_1, \ldots, S_n$ des parties finies de $\mathbb{K}$. Si $P$ s'annule en tout point de $S_1 \times \cdots \times S_n$, alors

$$P \in \left\langle \prod_{s \in S_i} (X_i - s) \right\rangle_{i \in [\![ 1 \ ; \ n ]\!]}$$

De plus, $P$ peut s'écrire $$P = \sum_{i=1}^{n} \left( \prod_{s \in S_i} (X_i - s) \right) H_i$$

[9] Le noyau est en $O\left(k^2 \log k\right)$.

avec $$\forall i \in [\![ 1 \ ; \ n ]\!] \qquad \deg(H_i) \leq \deg P - |S_i|$$

*Remarque.* Dans le cas où un des $S_i$ est vide, le produit cartésien $S_1 \times \cdots \times S_n$ est vide et l'idéal engendré par les $\prod_{s \in S_i} (X_i - s)$ contient alors 1 et est donc égal à $\mathbb{K}[X_1, \ldots, X_n]$.

Ce théorème vient généraliser le résultat bien connu sur les polynômes à une seule indéterminée :

**Théorème.** Soient $\mathbb{K}$ un corps commutatif et $P \in \mathbb{K}[X]$. Si $\alpha \in \mathbb{K}$ est tel que $P(\alpha) = 0$, alors

$$(X - \alpha) \mid P$$

On peut prouver le théorème du Nullstellensatz combinatoire par récurrence en utilisant le fait qu'un polynôme de $\mathbb{K}[X_1, \ldots, X_{n+1}]$ est un polynôme en $X_{n+1}$ dont les coefficients sont des éléments de $\mathbb{K}[X_1, \ldots, X_n]$. Autrement dit,

$$\mathbb{K}[X_1, \ldots, X_{n+1}] = \mathbb{K}[X_1, \ldots, X_n][X_{n+1}]$$

La grande idée consiste à utiliser le fait bien connu que seul le polynôme nul a strictement plus de racines que son degré dans le contexte des polynômes à une indéterminée mais dont les coefficients sont des polynômes en d'autres indéterminées[10]. Une preuve du Nullstellensatz combinatoire peut être trouvée dans [1] où Alon en donne plusieurs applications à la théorie des graphes. Il prouve notamment le théorème suivant, qui généralise un résultat conjecturé par Berge et Sauer et démontré pour la première fois par Taśkinov dans [33] : tout graphe 4-régulier contient un sous-graphe 3-régulier.

**Théorème.** Soit $p$ un nombre premier. Tout graphe dont le degré moyen est strictement supérieur à $2p - 2$ et dont le degré maximum est inférieur à $2p - 1$ contient un sous-graphe $p$-régulier.

*Preuve.* Soient $p$ un nombre premier et $G = (V, E)$ un graphe dont le degré moyen est strictement supérieur à $2p - 2$ et le degré maximum inférieur à $2p - 1$. On note $m = |E|$ et on considère l'anneau de polynômes $\mathbb{Z}_p[X_1, \ldots, X_m]$. Posons

$$P = \prod_{v \in V} \left( 1 - \left( \sum_{e \ni v} X_e \right)^{p-1} \right) - \prod_{e \in E} (1 - X_e)$$

On fait ici l'abus de notation $e = i$ où $i$ est le numéro de l'arête $e$. Comme nous le verrons, la plupart des notions abordées dans cette thèse, à l'instar du rang d'une matrice d'adjacence, sont indépendantes du choix de la numérotation faite sur les sommets (ou les arêtes) du graphe. Posons

$$Q = \prod_{v \in V} \left( 1 - \left( \sum_{e \ni v} X_e \right)^{p-1} \right) \qquad \text{et} \qquad R = \prod_{e \in E} (1 - X_e)$$

*Remarque.* Les calculs qui suivent sont faits dans $\mathbb{Z}_p$. Il faut donc considérer toutes les sommes et tous les produits modulo $p$.

[10] Un élément de $\mathbb{K}[X_1, \ldots, X_n]$ est, en particulier, un élément de $\mathbb{K}(X_1, \ldots, X_n)$, le corps des fractions rationnelles en $X_1, \ldots, X_n$.

Remarquons à présent que, $(x_1, \ldots, x_m) \in \{0,1\}^m$ vérifie $\prod_{v \in V} \left(1 - \left(\sum_{e \ni v} x_e\right)^{p-1}\right) = 0$ si, et seulement si,

$$\exists v \in V \qquad \sum_{e \ni v} x_e \neq 0$$

En effet, $\mathbb{Z}_p$ est un anneau intègre donc le produit $\prod_{v \in V} \left(1 - \left(\sum_{e \ni v} x_e\right)^{p-1}\right)$ est nul si, et seulement si, un de ces termes, au moins, est nul. Cela équivaut donc à l'existence d'un $v \in V$ tel que

$$\left(\sum_{e \ni v} x_e\right)^{p-1} = 1$$

Or, comme $p$ est premier, $(\mathbb{Z}_p{}^*, \times)$ est un groupe fini d'ordre $p-1$ et que les $x_e$ sont dans $\{0,1\}$, le théorème de Lagrange[11] permet donc d'affirmer que cela équivaut à $\sum_{e \ni v} x_e \neq 0$. Cependant, une telle somme est non nulle dans $\mathbb{Z}_p$ si, et seulement si, son nombre de termes non nuls n'est pas un multiple de $p$. Supposons l'existence de $(x_1, \ldots, x_m) \in \{0,1\}^m$ tel que $Q(x_1, \ldots, x_m) \neq 0$. Dès lors, d'après ce que nous venons de faire, dans le sous-graphe constitué des arêtes $e \in E$ pour lesquelles $x_e = 1$, tout sommet a pour degré un multiple de $p$. Le degré maximal de $G$ étant $2p-1$, un tel multiple vaut soit 0, soit $p$. Un tel sous-graphe donne donc le résultat escompté.

Montrons donc l'existence de $(x_1, \ldots, x_m) \in \{0,1\}^m$ tel que $Q(x_1, \ldots, x_m) \neq 0$. Supposons par l'absurde que $P$ s'annule en tout point de $\{0,1\}^m$. Dès lors, d'après le Nullstellensatz combinatoire, $P$ peut s'écrire

$$P = \sum_{i=1}^{m} X_i(X_i - 1)H_i$$

avec $H_i \in \mathbb{Z}_p[X_1, \cdots, X_m]$ tels que

$$\forall i \in [\![\, 1 \,;\, m \,]\!] \qquad \deg(X_i(X_i-1)H_i) \leq \deg(P)$$

Remarquons que $\deg(Q) \leq (p-1)\,|V|$. Or, $(p-1)\,|V| < m$. En effet la condition sur le degré moyen de $G$ se traduit par

$$\frac{1}{|V|} \sum_{v \in V} \deg(v) > 2p - 2$$

d'où, d'après la formule d'Euler, $\qquad m > (p-1)\,|V|$

En revanche, $\deg(R) = m$. De ce fait, le coefficient du monôme $\prod_{i=1}^{m} X_i$ dans $P$ vaut $(-1)^{m+1}$. Notons, comme nous le ferons à la Section 2.2.4, $\left(X^{(x_1,\ldots,x_m)}\right)^*(P)$ le coefficient de $\prod_{i=1}^{m} {X_i}^{x_i}$ dans $P$. On a donc

$$\left(X^{(1,\ldots,1)}\right)^*(P) = (-1)^{m+1}$$

De ce fait $\qquad \sum_{i=1}^{m} \left(X^{(1,\ldots,1)}\right)^*(X_i(X_i-1)H_i) = (-1)^{m+1}$

[11] Ou encore, plus directement, le petit théorème de Fermat.

On note alors $m_i = (1, \dots, 1, 0, 1, \dots, 1)$ le $m$-uplet de $\{0,1\}^m$ qui a un zéro uniquement en position $i$. Il existe donc $i \in [\![ 1 \ ; \ m ]\!]$ tel que

$$(X^{m_i})^* (H_i) \neq 0$$

puis

$$\deg(H_i) \geq m - 1$$

d'où

$$\deg(X_i(X_i - 1)H_i) \geq m + 1$$

ce qui est absurde. Ainsi, il existe donc $(x_1, \dots, x_m) \in \{0,1\}^m$ tel que $P(x_1, \dots, x_m) \neq 0$. De plus, comme $P(0, \dots, 0) = 0$ (et $1 \neq 0$ dans $\mathbb{Z}_p$), on a donc $(x_1, \dots, x_m) \in \{0,1\}^m \setminus \{(0, \dots, 0)\}$. Ainsi, $R(x_1, \dots, x_m) = 0$. Il s'ensuit que $Q(x_1, \dots, x_m) \neq 0$ ce qui conclut. □

*Remarque.*

- Il faut comprendre ici que le polynôme $R$ ne joue qu'un rôle technique dans cette démonstration. Il sert essentiellement à augmenter artificiellement le degré de $P$ afin d'utiliser le Nullstellensatz combinatoire. De fait, il y a bien d'autres polynômes possibles pour mener à bien cette preuve. Le choix d'un polynôme adapté, afin de rendre la preuve la plus simple possible est donc crucial. Cette question sera abordée dans cette thèse et constitue un axe de recherche intéressant.

- La preuve n'est pas constructive en ce sens qu'elle ne donne pas de moyen d'exhiber un tel sous-graphe. Il s'agit en effet d'une preuve d'existence par l'absurde. Cela sera, nous le verrons, récurrent dans les preuves menées au cours de cette thèse.

Nous donnons à présent les grandes lignes de la preuve du théorème de Fleischner et Stiebitz (voir [16]). Une nouvelle preuve, utilisant les outils développés au cours de cette thèse sera faite à la Section 2.3.1. Comme la première preuve, celle-ci utilisera un argument de comptage dû à Petrov qui, lui-même, reprouve aussi le théorème de Fleischner et Stiebitz (voir [30]).

**Théorème** (Fleischner et Stiebitz)**.** Tout graphe qui est l'union arête disjointe d'un cycle hamiltonien et d'une union sommet disjointe de triangles est 3-choisissable.

La notion de "choisissabilité" (en anglais "choosability") se définit de la manière suivante. Étant donné un graphe $G$ et une application $f \in \mathbb{N}^{V(G)}$, on dit que $G$ est $f$-choisissable si, et seulement si, pour toute famille d'ensembles $(S_v)_{v \in V(G)}$ telle que

$$\forall v \in V(G) \qquad |S_v| = f(v)$$

il existe une coloration de $c$ de $G$ vérifiant

$$\forall v \in V(G) \qquad c(v) \in S_v$$

Autrement dit, étant donné $f(v)$ possibilités de couleurs pour chaque sommet $v \in V(G)$, il est possible de choisir une de ces possibilités pour chaque sommet de manière à avoir une coloration de $G$. Un graphe est dit $k$-choisissable (avec $k \in \mathbb{N}$) si, et seulement si, il est $f$-choisissable où $f$ est la fonction constante égale à $k$. Un graphe $k$-choisissable est en particulier $k$-coloriable (il suffit de prendre $S_v = [\![ 0 \ ; \ k - 1 ]\!]$ pour tout $v \in V(G)$) mais la réciproque est fausse en général : le graphe biparti complet $K_{3,3}$ est 2-coloriable mais pas 2-choisissable. Le théorème de Fleischner et Stiebitz est donc plus fort que la conjecture

initiale d'Erdös en 1990 où il était simplement question de 3-colorabilité. Il convient de noter qu'une autre preuve, "élémentaire", de la conjecture d'Erdös a été faite par Sachs en 1994 (voir [31]).

On note $D = (V, E)$ le graphe obtenu à partir de $G$ en orientant le cycle hamiltonien et chaque triangle de manière cyclique. L'idée de la preuve de Fleischner et Stiebitz consiste alors à considérer une telle orientation $D$ de $G$ et d'introduire le polynôme suivant :

$$P_D = \prod_{(u,v)\in E} (X_u - X_v)$$

Notons $EE(D)$ (resp. $EO(D)$) le nombre de sous-graphes eulériens qui ont un nombre pair (resp. impair) d'arêtes. Fleischner et Stiebitz montrent dans [16], grâce des arguments de comptages, que

$$\left|\left(X^{(1,\dots,1)}\right)^* (P_D)\right| = |EE(D) - EO(D)|$$

et que de plus, $EE(D) - EO(D) = 2\,[4]$ ce qui permet de conclure que le coefficient de $X^{(1,\dots,1)}$ dans $P_D$ est non nul. Comme précédemment, on montre, grâce au Nullstellensatz combinatoire, qu'il n'est pas possible que $P_D$ s'annule en tout point de $\{0,1,2\}^n$.

En effet, supposons par l'absurde que $P_D$ s'annule en tout point de $\{0,1,2\}^n$. Dès lors, d'après le Nullstellensatz combinatoire, $P_D$ peut s'écrire

$$P_D = \sum_{i=1}^{n} X_i(X_i - 1)(X_i - 2)H_i$$

avec $$\forall i \in [\![ 1\ ;\ n ]\!] \qquad \deg(H_i) \leq \deg(P_D) - 3$$

Notons comme précédemment $n_i = (1, \dots, 1, 0, 1, \dots, 1)$ le $n$-uplet de $\{0,1\}^n$ qui a un zéro uniquement en position $i$. Comme $\left(X^{(1,\dots,1)}\right)^* (P_D) \neq 0$, il existe $i \in [\![ 1\ ;\ n ]\!]$ tel que $(X^{n_i})^* (H_i) \neq 0$ ce qui, là encore, contredit l'hypothèse sur le degré de $H_i$.

*Remarque.* La définition de coloration pour un graphe orienté ne change pas par rapport à celle relative au graphe non orienté sous-jacent. En réalité, si $G$ est un graphe et $D$ une orientation de $G$, alors en posant

$$P_G = \prod_{(u,v)\in E(G)} (X_u - X_v) \qquad \text{et} \qquad P_D = \prod_{(u,v)\in E(D)} (X_u - X_v)$$

on a $$P_G = (-1)^{|E(D)|} {P_D}^2$$

De ce fait, les polynômes $P_G$ et $P_D$ ont les mêmes racines. Le fait de travailler avec une version orientée du graphe permet simplement de simplifier l'argument de comptage.

En fait, une importante partie de la preuve de Fleischner et Stiebitz repose sur le résultat suivant de Alon et Tarsi (voir [2]) :

**Théorème.** Soit $D = (V, E)$ un graphe orienté vérifiant $EE(D) \neq EO(D)$. Dès lors, $D$ est $f$-choisissable avec

$$f : \left\{ \begin{array}{ccc} V & \to & \mathbb{N} \\ v & \mapsto & d_v + 1 \end{array} \right.$$

où $d_v$ est le degré sortant de $v \in V$.

*Preuve.* Posons $P_D = \prod_{(u,v)\in E} (X_u - X_v)$. Sans perdre en généralité, on suppose que les sommets de $D$ sont les éléments de $[\![ 1 \ ; \ n ]\!]$. De même que dans la preuve précédente, on a

$$\left|\left(X^{(d_1,\dots,d_n)}\right)^* (P_D)\right| = |EE(D) - EO(D)|$$

ce qui prouve que le coefficient de $X^{(d_1,\dots,d_n)}$ dans $P_D$ est non nul. On considère alors, pour tout $i \in [\![ 1 \ ; \ n ]\!]$, un ensemble $S_i$ de cardinal $d_i + 1$. Supposons par l'absurde que $P_D$ s'annule en tout point de $S_1 \times \cdots \times S_n$. Dès lors, d'après le Nullstellensatz combinatoire, $P_D$ peut s'écrire

$$P_D = \sum_{i=1}^{n} \left( \prod_{s\in S_i} (X_i - s) \right) H_i$$

avec $\forall i \in [\![ 1 \ ; \ n ]\!] \qquad \deg(H_i) \leq \deg P_D - |S_i|$

Comme $\left(X^{(d_1,\dots,d_n)}\right)^* (P_D) \neq 0$, il existe $i \in [\![ 1 \ ; \ n ]\!]$ tel que

$$\left(X^{(d_1,\dots,d_n)}\right)^* \left( \left( \prod_{s\in S_i} (X_i - s) \right) H_i \right) \neq 0$$

ce qui amène à une contradiction quant au degré de $H_i$. □

Un corollaire simple de ce résultat est qu'un graphe $G$ de degré maximum $\Delta$ est $\Delta + 1$-choisissable et donc, en particulier $\Delta + 1$-coloriable. On retrouve alors une partie du théorème de Brooks. La preuve complète du théorème de Brooks a d'ailleurs été refaite par Hladkýa, Král et Schauz dans [22] grâce au Nullstellensatz combinatoire.

Les idées d'Alon et Tarsi ont véritable été prolifiques, et pas seulement dans le cadre de la coloration de graphe classique. Par exemple, Norine, Wong et Zhu les ont réinvesti dans [28] pour démontrer des résultats de $(p, q)$-list coloring. Si $(p, q) \in \mathbb{N}^2$ vérifient $p > q$, on appelle $(p, q)$-coloration d'un graphe $G$ une coloration à au plus $p$ couleurs vérifiant une contrainte supplémentaire de distance entre les couleurs : deux couleurs sur des sommets adjacents doivent être à distance au moins $q$. Cependant, une telle définition conduirait à des effets de bord qui casseraient la symétrie entre les couleurs. On utilise donc $\mathbb{Z}_p$ comme ensemble de couleurs et on définit la distance suivante :

$$d : \begin{cases} [\![ 0 \ ; \ p-1 ]\!]^2 & \to & \mathbb{R} \\ (i,j) & \mapsto & \min\left(|i-j|, p-|i-j|\right) \end{cases}$$

Intuitivement, il s'agit de la longueur du plus court chemin entre $i$ et $j$ si l'on représente les éléments de $\mathbb{Z}_p$ comme des points équidistants sur un cercle. Ainsi, une $(p, q)$-coloration d'un graphe $G$ est une coloration de $G$ grâce aux éléments de $\mathbb{Z}_p$ qui vérifie que deux sommets adjacents ont des couleurs à distance au moins $q$ au sens de la distance $d$. Pour $q = 1$, on retrouve la définition d'une $p$-coloration.

Il est aussi possible de définir la $f$-$(p, q)$-choisissabilité de manière analogue à la $f$-choisissabilité lorsque $f$ est majorée par $p$. Norine, Wong et Zhu proposent alors dans [28] une extension du résultat précédent dont la preuve utilise, la encore, le Nullstellensatz combinatoire.

Les travaux présentés dans cette thèse reprennent l'esprit général des démonstrations précédentes. Ils sont cependant réellement novateurs et proposent un point de vue différent sur ces preuves algébriques. Une des valeurs ajoutées est l'introduction d'un objet dual aux

polynômes qui encodent les problèmes de coloration (et plus généralement, les problèmes de graphes pouvant s'exprimer à l'aide de polynômes) : les precolorings (voir Section 1.10). Une des difficultés des preuves précédentes est le choix d'un bon polynôme pour encoder le problème. La même difficulté se retrouvera dans le choix de bons precolorings. Cependant, nous donnons des pistes pour les choisir judicieusement, ce qui ouvre peut-être une voie nouvelle et passionnante à explorer.

Après ces années de thèse, et à l'heure où il faut se résoudre à mettre un point final à ce travail, je réalise que cette exploration n'en est peut-être qu'à son commencement. Il y a encore tant à faire !

Nous espérons que, malgré la lourdeur du formalisme, hélas tout à fait indispensable à la rigueur que requièrent les concepts développés dans cette thèse, la lecture de cette dernière sera agréable et qu'elle pourra inspirer d'autres mathématiciens pour la poursuite des travaux humblement commencés ici.

Enfin, ces années de thèse constituent le point final de longues études et le présent manuscrit, le dernier examen. Nous remercions le jury de se livrer à sa critique malgré l'appréhension bien naturelle que cela provoque fatalement chez tout étudiant.

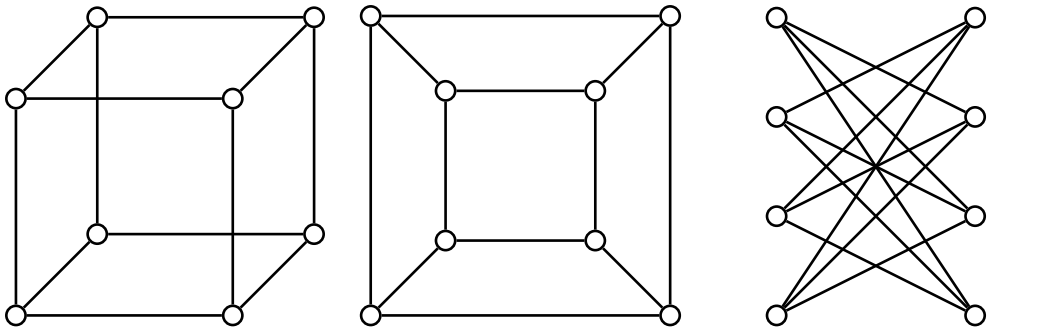
> "L'épreuve de l'examen est utile et juste, et en dépit de faciles déclamations, celui qui ne l'a point surmontée n'en surmontera aucune autre."
>
> Paul Valéry

# Introduction (in english)

This thesis deals with *graph theory*, which is a part of the *discrete mathematics*, or, more specifically, of *computer science*. It aims at developing new theoretical tools in order to solve problems on graphs.

A graph is a simple object, yet very useful. In 1735, Leonhard Euler used the notion of graphs to solve a famous problem: the seven bridges of Königsberg. Königsberg is a city located in Prussia[12] has seven bridges in order to connect two islands. Is it possible to do a closed walk in the city, taking each bridges exactly once? It seems impossible but can we prove it? Euler did seek a formal proof of this negative result. Although we are certainly not as bright as Euler was, this thesis is also about finding proofs, certificates of infeasibility for graphs related problems. Indeed, the problem of the seven bridges of Königsberg is a graph problem!

A graph is a set of points called *vertices* connected with each other by lines called *edges*. Two vertices connected by en edge are said to be *adjacent*. For instance, a cube, or more generally any polyhedron, is a graph. Sometimes, we can make a drawing of a graph. For instance, Figure 9 shows three drawings of the same graph: the cube. This can be surprising but this is really the same object. Indeed, the adjacency relations are the same, and this is all that matters when we are dealing with graphs.



(a) Usual representation (b) Planar representation (c) Bipartite representation

Figure 9: Three drawings of the cube

[12]Nowaday the city is russian and named Kaliningrad.

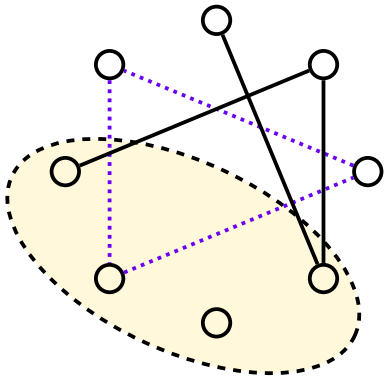


Figure 10: A clique of maximum size with edges in dotted purple and a maximum size stable set inside the dotted ellipse

A set of vertices $S$ of a graph such that there is no edge between any pair of elements of $S$ is called a *stable set* or an *independent set*. Conversely, a graph such that every pair of vertices are connected by an edge is called a *clique*. Let us make an example. Suppose one wants to organize a diner with every parishioners of a church that never met. We can model this with a graph: each parishioner is represented by a vertex and, two vertices are connected by an edge if, and only if, the corresponding parishioners have already met. A stable set of this graph provides a set of parishioners that we can invite to the diner (on Figure 10, we can take all the vertices inside the ellipse). If, on the contrary, we want to invite only people that already know each other, we can take a clique of the graph, which is a set of vertices with a maximum number of edges (for instance, this is the case for the purple dashed triangle on Figure 10). We called *degree* of a vertex its number of neighbours. Then, a vertex of maximum degree represents a very popular parishioner! Finding a stable set of maximum size is difficult in general[13]. The same goes for finding a clique of maximum size within a graph: those problems are substantially identical since a clique in $G$ is a stable set in the complementary of $G$, which is the graph obtained from $G$ when we invert the adjacency relation.

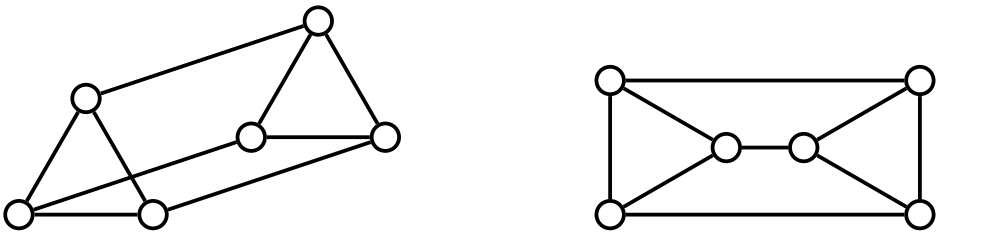
## A short history of graph theory

In 1852, two brothers, Francis and Frederick Guthrie, who were mathematicians, discovered a surprising fact: every map can be colored with only 4 colors. More precisely, if one wants to color every area of a map (for instance, the world map, the departments of France or even those of a random country we may invent) so that two areas that share a border do not have the same color[14] then, there always exists a solution using at most four colors.

[13]This problem is NP-complete.

[14]We must forbid the borders that are not real lines. For instance, some borders are points between two states of USA. Moreover, we choose a color for each area, not for each country.

Frederick did not succeed in proving the conjecture so he asked his professor: Augustus De Morgan. This brilliant mathematician did not succeed either. Alfred Kempe will make the first proof of the result, or, we should say, attempt of proof as there was a mistake! Kempe still managed to prove a weaker result: the five colors theorem which states that, under the same hypothesis, five colors are enough. This map coloring problem can be formalized with graphs by representing each area by a vertex and by connecting every pair of edges if, and only if, they share a border. The graphs one can obtain from a map are said to be *planar* because they can be drawn in the plane with no pair of edges crossing. Such a class of graphs is actually more complex that one may think. Indeed, the fact that there exists a drawing in which no pair of edges ever cross is hard to formalize mathematically and to hard manipulate. For instance, Figure 11 represents twice the same graph: in a planar way in 11b an in a non planar way in 11a. Beside, proving that a graph is not planar can be difficult. For instance, the Petersen's graph (see Figure 12) cannot be represented in a planar way.



(a) prism (b) prism represented in a planar war

Figure 11: Two representations of the prism

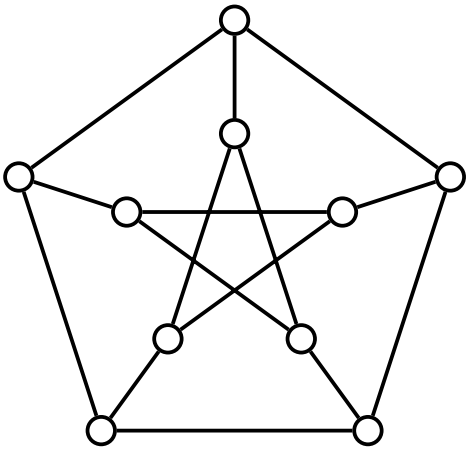
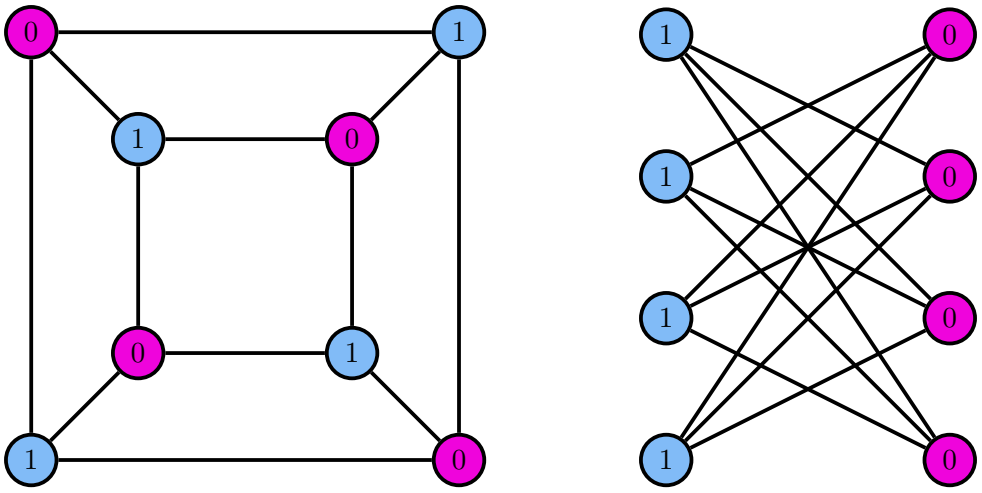


Figure 12: Petersen's graph

Then, coloring the area of the map is the same as choosing one color for every vertices of the underlying planar graph so that no two adjacent vertices share the same color. More generally, a coloring for a graph is a choice of colors for each of the vertices so that no adjacent vertices share the same color. In particular, the vertices with the same color is a stable set. For convenience, we will use numbers instead of colors. For instance, the cube can be colored with two colors (see Figure 13a). This is really obvious if we think of the bipartite representation (see Figure 13b). Of course, this notion does not depend on how the graph is represented. We will call *proper coloring*, or simply *coloring*, a labelling of the vertices so that the condition stated above is verified. Conversely, when this condition is not necessarily verified, we will simply speak of *labelling*.




(a) A 2-coloring of the cube (b) A 2-coloring of the cube

Figure 13: Coloring of the cube with two colors

In case of a cube, we cannot use less than two colors. We say that the *chromatic number* of the cube is 2. More generally, the chromatic number of a graph $G$ is the minimal number of colors one need in order to properly color this graph. Figure 14 shows a 3-coloring of Petersen's graph. This graph cannot be properly colored with less than 3 colors so, its chromatic number is 3. Determining the chromatic number of a graph is a hard problem in general[15].

The four colors theorem states that the chromatic number of a planar graph is at most 4. We need to wait 1976, which is more that one century after the Guthrie brothers found the conjecture, to finally have a correct proof thanks to Kenneth Appel and Wolfgang Haken ([3]). For the first time, the proof is computer assisted. This may be problematic: how to be sure that the computer is right despite a proof by case analysis of 1478 cases and more than 600 pages when printed[16]? Later, Robertson, Sanders, Seymour and Thomas will simplify

[15]This problem is NP-complete.
[16]By the way, a mistake has been found in the original proof!

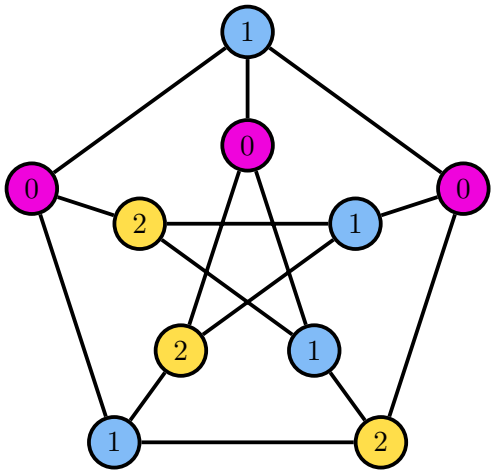



Figure 14: A 3-coloring of Petersen's graph

the proof leaving only 633 cases. Nowadays, this result remains mysterious and we do not fully understand why the theorem is true. According to Paul Erdös, the four colors theorem is a "subtle problem but not a complex one", and a simple proof[17] should exists because, according to him, the class of planar graphs is a subset of the class of graphs to consider for this theorem. A simple proof of this famous result would constitute a breakthrough in computer science.

Graph coloring proves to be useful for many optimization problems. This is probably why this problem is still widely studied. We provide here a few examples. Suppose one wants to organize exams in a university with many rooms and many courses. Of course, two exams concerning the same student cannot take place at the same time. How can we organize the exams in an optimal way? Define $G$ to be the graph whose vertices are the exams and so that two exams are connected by an edge if, and only if, one student at least must attend those two exams. In any coloring, the vertices of the same color are exams that can take place at the same time. Hence, a coloring achieving $\chi(G)$ gives an optimal schedule for the exams.

Let us see another example, which is in fact very similar: the seating plan. Suppose one wants to make a seating plan for a wedding so that no pair of guests who dislike each other are at the same table. (Unfortunately, this seems to be quite common.) Again, we can use graphs to model this problem. The vertices are the guests and two guests are connected by an edge if, and only if, they dislike each other. A table must be a stable set of the graph. Hence, a coloring of the graph reaching the minimal number of colors gives a seating plan that minimizes the number of required tables.

Finally, suppose one wants to create a phone network. A frequency range must be allocated to each antenna. We would like to minimize the number of frequency ranges since it comes with a cost. However, two antennas that are nearby must not share the same

[17] A proof from the Book!

frequency range in order not to interfere. We can define a graph whose vertices are the antenna and so that two antenna are connected by an edge if, and only if, the are nearby. The chromatic number of this graph is the minimal number of required frequency ranges.

Since the chromatic number is hard to compute, we use to seek lower and upper bounds. For instance:

**Theorem.** Let $G$ be a graph, $\omega(G)$ the size of its largest clique and $\Delta(G)$ its maximum degree. We have that

$$\omega(G) \leq \chi(G) \leq \Delta(G) + 1$$

Unfortunately, $\chi(G)$ can be arbitrary far from those bounds. Indeed, there exists triangle free graphs with arbitrary large chromatic number (see [25]) and, moreover, a graph composed of one vertex with $n$ neighbours has a chromatic number of 2 but maximum degree of $n$.

The graph coloring problem is hard because, although the constraints are local, the minimality of the number of colors depends on the whole graph. Hence, working only with subgraphs cannot be enough in general[18]. Conversely, the notion of *minor*[19] of a graph seems promising. Let us cite the famous Hadwiger conjecture ([18]), opened since 1943. Let us denote by $\mathcal{H}(G)$ the Hadwiger number of $G$, that is the least integer $k$ such that $G$ admits the complete graph on $k$ vertices for minor.

**Conjecture (Hadwiger).** For every graph $G$, $\chi(G) \leq \mathcal{H}(G)$.

## The main ideas of this thesis

Proving that a graph $G$ can be colored with $k$ colors is one thing. Showing that this number is minimal is another. One way to do so is by proving one cannot color $G$ with $k-1$ colors. This allows to determine the chromatic number of $G$ "from below". This is the starting point of this thesis. More generally, we would like, whenever $\chi(G) > k$, a certificate of non $k$-colorabiliy for $G$. Such a certificate could be several things. For instance, if $G$ contains a clique of size $k+1$, then this clique is a proof, a certificate, that $\chi(G) > k$. Figure 15 shows a graph that is not 3-colorable because it contains a clique of size 4 inside the dotted ellipse.

Unfortunately, it is not always possible to find a subgraph that can be a certificate. In this thesis, we will present a generic method to certify that a graph is not $k$-colorable. Our work is related to the publications of Bayer ([5]), De Loera ([12], [13]) and Li, Lowenstein and Omar ([6]). The common idea through those articles is to use multivariate polynomials to encode the problem of the 3-colorability of a graph. Indeed, the Nullstellensatz theorem of Hilbert (1.5.1) provides a certificate in case $G$ is not $k$-colorable. This certificate is, however, a family of polynomials which is a purely algebraic object. We will prove that it is possible to create a "natural" extension of $G$ in which such an algebraic certificate has a

[18] If it were the case, computing the chromatic number of a graph would be a polynomial time problem, and so we would have P = NP...

[19] A minor of a graph $G$ is a graph we can obtain from $G$ after applying the following transformations, delete an isolated vertex, delete and edge, contract an edge.

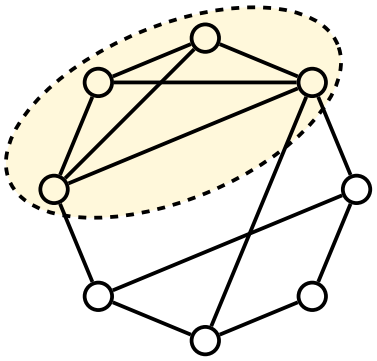


Figure 15: A graph that contains a clique of size 4

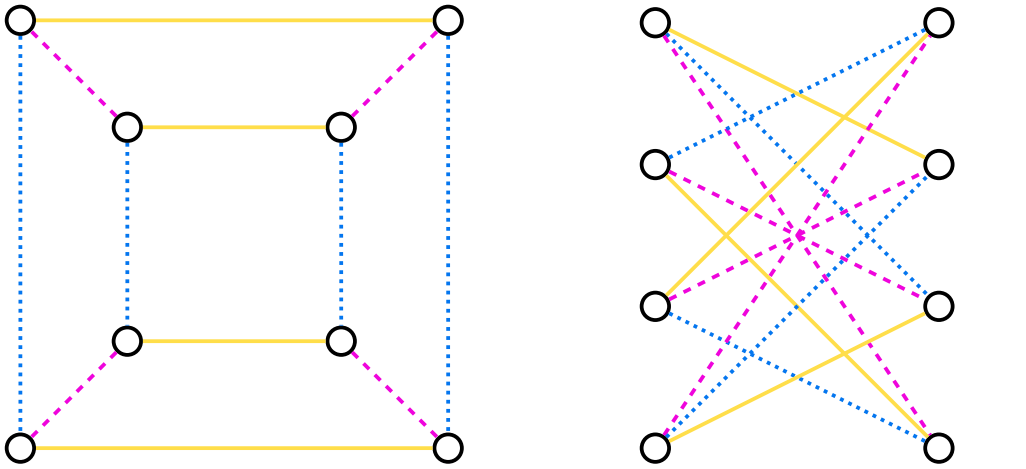
combinatorial interpretation. For instance, to study the 3-colorability of a graph $G$, we can define a graph denoted by $3^G$ that satisfies $\chi(G) = 3 \Leftrightarrow \chi\left(3^G\right) = 3$ (see Section 1.3). We shall see that we can defined several such extensions in case $k$ is not a prime number. We will discuss the differences between those extensions in Section 1.4.

Having studied those graph extensions that we call *power graphs*, we discovered a connection with what we named *Fourier analysis on graphs*. In order to illustrate this concept, let us introduce a new way to color graphs: the *edge-coloring*. We must now chose one color per edge and satisfy the condition that no pair of adjacent edges share the same color. Of course, this problem is not fundamentally different from the vertex-coloring that we have seen previously since an edge-coloring of a graph is a vertex-coloring of its line graph[20]. Figure 16a shows a 3-edge-coloring of the cube. We can also represent this coloring on a bipartite representation of the cube (see Figure 16b).

Our idea is to use the bipartite representation and the following remark: an edge-coloring of a bipartite graph is correct if, and only if, the constraints are satisfied both on the right and on the left. In other words, an edge-coloring of a bipartite graph is good if, and only if, two incident edges on the right (resp. on the left) always have different colors. This can be expressed with an inner product: define $f_L$ to be the vector of size $3^{m/2}$ ($m$ being the number of edges of the graph) indexed by all the possible 3-edge-labellings and which has a 1 in front of a proper edge-labelling from the left perspective, and a 0 otherwise. In an analogous way, we define $f_R$ to be the characteristic vector of the good 3-edge-colorings from the right perspective. By construction, $\langle f_L, f_R \rangle$ is the number of good 3-edge-colorings of $G$. Then, to prove that $G$ admits a 3-edge-coloring, it suffices to prove that this inner product is non zero. A formal introduction of this is made in Section 2.1.

Rather than computing directly this inner product, we compute $\left\langle \widetilde{f_L}, \widetilde{f_R} \right\rangle$ where $\widetilde{\cdot}$ designates the multiplication with some appropriate Fourier matrix (see Section 2.2). Those matrices have the nice property of being hermitian so $\langle f_L, f_R \rangle = \left\langle \widetilde{f_L}, \widetilde{f_R} \right\rangle$. In some cases,

[20]The line graph of a graph $G$, denoted by $\mathcal{L}(G)$, has the edges of $G$ as vertex set. Moreover, two vertices of $\mathcal{L}(G)$ are connected by an edge if, and only if, the corresponding edges are adjacent in $G$.



(a) 3-coloring of the edges of the cube (b) 3-coloring of the edges of the cube

Figure 16: Two representations of an edge-coloring of the cube with three colors

we have a simple argument to assess that this last inner product is non zero. Our method also works with non bipartite graphs up to some changes (see for instance Proposition 2.1.2) and with vertex coloring as well. Using our tools, we made a new simple and elegant proof of Fleischner and Stiebitz theorem ([16]) in Section 2.3.1.

The Fourier analysis on graphs developed in this thesis has a strong connection with power graphs. The Fourier transforms of the good colorings form a basis of the linear space of the *precoloring* which are functions that admits a simple characterization on power graphs. For more details, please refer to Section 2.2.5.

Finally, there are several natural questions about power graphs. In particular, what are the properties of $G$ that are also true in its different power graphs? How a small edit of $G$ translates in its power graphs? Those questions are not trivial and many of them remains open. When researching the effect of edge editings on power graphs, we have studied the cograph editing problem: Given a graph $G$, how can we edit $G$ (that is, revert some adjacency relations), in an optimal way in terms of execution time but also in terms of number of edited edges in order to make $G$ a graph with no induced path of length 4? An introduction of those edition problems is available at Section 3.1. We have improved a result of Havet et al ([17]) going from a cubic kernel for this problem to a "quasi-quadratic" kernel[21]. Our article has been accepted in *Discrete Applied Maths* and should be published soon.

[21] Our kernel is in $O\left(k^2 \log k\right)$.

## Algebraic proofs on graphs: an introduction

In order to put in perspective the methods developed in this thesis, this section contains a short survey on how polynomials have been used in graph theory. All the results presented here are based on a theorem called *combinatorial Nullstellensatz*. Rather than trying to be exhaustive in the proofs, we give the intuition and explain how algebraic proofs on graphs work in general. Roughly speaking, the idea is to introduce a multivariate polynomial whose roots are solutions of our problem. The combinatorial Nullstellensatz gives conditions on the roots and allows us to conclude by contradiction.

**Theorem** (combinatorial Nullstellensatz)**.** Let $\mathbb{K}$ be a field, $n \in \mathbb{N}^*$ and $P \in \mathbb{K}[X_1, \ldots, X_n]$. Let $S_1, \ldots, S_n$ be finite subsets of $\mathbb{K}$. If $P$ vanishes on $S_1 \times \cdots \times S_n$, then

$$P \in \left\langle \prod_{s \in S_i} (X_i - s) \right\rangle_{i \in [\![ 1 \ ; \ n ]\!]}$$

Moreover, $P$ can be written $\displaystyle P = \sum_{i=1}^{n} \left( \prod_{s \in S_i} (X_i - s) \right) H_i$

with $\forall i \in [\![ 1 \ ; \ n ]\!] \qquad \deg(H_i) \leq \deg P - |S_i|$

*Remark.* In case one of the $S_i$ is empty, the product $S_1 \times \cdots \times S_n$ is empty. Hence, the ideal generated by the $\prod_{s \in S_i} (X_i - s)$ contains 1 so it is equal to $\mathbb{K}[X_1, \ldots, X_n]$.

This theorem generalizes the well known following result on univariate polynomials:

**Theorem.** Let $\mathbb{K}$ be a field and $P \in \mathbb{K}[X]$. If $\alpha \in \mathbb{K}$ satisfies $P(\alpha) = 0$, then

$$(X - \alpha) \mid P$$

The proof of the combinatorial Nullstellensatz can be done by induction. It relies of the fact that a polynomial of $\mathbb{K}[X_1, \ldots, X_{n+1}]$ is a polynomial in $X_{n+1}$ whose coefficients are elements of $\mathbb{K}[X_1, \ldots, X_n]$. In other words,

$$\mathbb{K}[X_1, \ldots, X_{n+1}] = \mathbb{K}[X_1, \ldots, X_n][X_{n+1}]$$

The core idea is to use the well known fact that, for univariate polynomials, the zero polynomial is the only one that has more roots than its degree. This is true even if the coefficients are polynomials[22]. A proof of the combinatorial Nullstellensatz can be found in [1] where Alon gives several applications to graph theory. He notably proves the following theorem that generalizes a result which has been conjectured by Berge and Sauer and then proved by Taśkinov in [33]: Every 4-regular graph contains a 3-regular subgraph.

**Theorem.** Let $p$ be a prime number. Every graph with average degree bigger than $2p - 2$ and maximum degree at most $2p - 1$ contains a $p$-regular subgraph.

[22] An element of $\mathbb{K}[X_1, \ldots, X_n]$ is, in particular, an element of $\mathbb{K}(X_1, \ldots, X_n)$, the field of the algebraic fractions in $X_1, \ldots, X_n$.

*Proof.* Let $p$ be a prime number and $G = (V, E)$ be a graph with average degree bigger than $2p - 2$ and maximum degree at most $2p - 1$. Let $m = |E|$. We consider the ring of polynomials $\mathbb{Z}_p[X_1, \ldots, X_m]$. Let us define

$$P = \prod_{v \in V} \left(1 - \left(\sum_{e \ni v} X_e\right)^{p-1}\right) - \prod_{e \in E} (1 - X_e)$$

We abuse notation here and consider that $e = i$ where $i$ is the index of the edge $e$. As we will see later, almost every notion studied in this thesis, such as the rank of an adjacency matrix, are independent of the numbering chosen for the vertices (or edges) of the graph. Let us define

$$Q = \prod_{v \in V} \left(1 - \left(\sum_{e \ni v} X_e\right)^{p-1}\right) \qquad \text{and} \qquad R = \prod_{e \in E} (1 - X_e)$$

*Remark.* The following calculus are made in $\mathbb{Z}_p$. Hence, every sums and every products are modulo $p$.

Observe that, $(x_1, \ldots, x_m) \in \{0, 1\}^m$ satisfies $\prod_{v \in V} \left(1 - \left(\sum_{e \ni v} x_e\right)^{p-1}\right) = 0$ if, and only if,

$$\exists v \in V \qquad \sum_{e \ni v} x_e \neq 0$$

Indeed, $\mathbb{Z}_p$ is an integral domain which implies that $\prod_{v \in V} \left(1 - \left(\sum_{e \ni v} x_e\right)^{p-1}\right)$ is null if, and only if, one of its terms, at least, is null. This is equivalent to the existence of $v \in V$ such that

$$\left(\sum_{e \ni v} x_e\right)^{p-1} = 1$$

Since $p$ is prime, $(\mathbb{Z}_p{}^*, \times)$ is a finite group of order $p - 1$. Moreover, the $x_e$ lies into $\{0, 1\}$. Hence, Lagrange's theorem[23] gives that it is equivalent to $\sum_{e \ni v} x_e \neq 0$. However, such a sum is not null in $\mathbb{Z}_p$ if, and only if, its number of non zero terms is not divisible by $p$. Assume by contradiction that there exists $(x_1, \ldots, x_m) \in \{0, 1\}^m$ such that $Q(x_1, \ldots, x_m) \neq 0$. Consider the subgraph formed by the edges $e \in E$ such that $x_e = 1$. By what we just did, in such a subgraph, the degree of every vertex is a multiple of $p$. Since the maximum degree of $G$ is $2p - 1$, every vertex has either degree 0 or degree $p$.

Let us now prove the existence of $(x_1, \ldots, x_m) \in \{0, 1\}^m$ such that $Q(x_1, \ldots, x_m) \neq 0$. Assume by contradiction that $P$ vanishes on $\{0, 1\}^m$. Hence, by the combinatorial Nullstellensatz, $P$ can be written

$$P = \sum_{i=1}^{m} X_i(X_i - 1)H_i$$

with $H_i \in \mathbb{Z}_p[X_1, \cdots, X_m]$ such that

$$\forall i \in [\![ 1 \ ; \ m ]\!] \qquad \deg(X_i(X_i - 1)H_i) \leq \deg(P)$$

Observe that $\deg(Q) \leq (p - 1)\,|V|$. Yet $(p - 1)\,|V| < m$. Indeed, the condition on the average degree of $G$ translates to

[23] In this case, this is Fermat's little theorem.

$$\frac{1}{|V|}\sum_{v\in V}\deg(v) > 2p-2$$

where, by the handshaking lemma, $\quad m > (p-1)\,|V|$

However, $\deg(R) = m$. As a consequence, the coefficient of the monomial $\prod_{i=1}^{m} X_i$ in $P$ is $(-1)^{m+1}$. Let us denote, as it will be done in Section 2.2.4, $\left(X^{(x_1,\dots,x_m)}\right)^*(P)$ the coefficient of $\prod_{i=1}^{m} {X_i}^{x_i}$ in $P$. We have that

$$\left(X^{(1,\dots,1)}\right)^*(P) = (-1)^{m+1}$$

Hence, $$\sum_{i=1}^{m}\left(X^{(1,\dots,1)}\right)^*(X_i(X_i-1)H_i) = (-1)^{m+1}$$

Let us write $m_i = (1,\dots,1,0,1,\dots,1)$ the $m$-tuple of $\{0,1\}^m$ which is zero only on coordinate $i$. There exists $i \in [\![ 1\ ;\ m ]\!]$ such that

$$(X^{m_i})^*(H_i) \neq 0$$

then $$\deg(H_i) \geq m-1$$

so $$\deg(X_i(X_i-1)H_i) \geq m+1$$

which is a contradiction. As a consequence, there exists $(x_1,\dots,x_m) \in \{0,1\}^m$ such that $P(x_1,\dots,x_m) \neq 0$. Moreover, since $P(0,\dots,0) = 0$ (and $1 \neq 0$ in $\mathbb{Z}_p$), we have that $(x_1,\dots,x_m) \in \{0,1\}^m \setminus \{(0,\dots,0)\}$. Hence, $R(x_1,\dots,x_m) = 0$. So $Q(x_1,\dots,x_m) \neq 0$, which concludes the proof. □

*Remark.*

- The polynomial $R$ has only a technical purpose in this proof. It aims at making the degree of $P$ big enough in order to use the combinatorial Nullstellensatz. As a matter of fact, other polynomials could have been used for that proof. Choosing an appropriate polynomial in order to make an algebraic proof easier is crucial. This question will be addressed in this thesis and constitutes an important research axis.

- The proof is not constructive in the sense that one cannot use it to build such a subgraph. Indeed, this is a proof of existence by contradiction. As we will see, it is common for the proofs in this thesis.

We now give the main ideas of the proof of Fleischner and Stiebitz's theorem (see [16]). A new proof, using the tools developed in this thesis, will be made in Section 2.3.1. Like Fleischner and Stiebitz, we use, at some point, a counting argument. In our proof, this counting argument is based on a lemma from Petrov who also made a proof of Fleischner and Stiebitz's theorem (see [30]).

**Theorem** (Fleischner and Stiebitz)**.** Every graph that decomposes into a Hamiltonian cycle and a vertex disjoint union of triangles is 3-choosable.

The notion of *choosability* is defined in the following way. Given a graph $G$, a total function $f \in \mathbb{N}^{V(G)}$, we say that $G$ is *$f$-choosable* if, and only if, for every family of sets $(S_v)_{v\in V(G)}$ such that

$$\forall v \in V(G) \qquad |S_v| = f(v)$$

there exists a coloring $c$ of $G$ that satisfies

$$\forall v \in V(G) \qquad c(v) \in S_v$$

In other words, given $f(v)$ possible colors for every vertex $v \in V$, one can choose one color for each in order to make a proper coloring of $G$. A graph is said to be *$k$-choosable* (with $k \in \mathbb{N}$) if, and only if, it is $f$-choosable where $f$ is the function constant to $k$. A $k$-choosable graph is, in particular, $k$-colorable (one just has to take $S_v = [\![ 0 \ ; \ k-1 ]\!]$ for every $v \in V(G)$). However, the converse is false in general: the complete bipartite graph $K_{3,3}$ is 2-colorable but not 2-choosable. Fleischner and Stiebitz's theorem is then stronger than the initial conjecture made by Erdös in 1990. Indeed, Erdös only claimed that such a graph is 3-colorable. Another proof of that result, that does not use the combinatorial Nullstellensatz, has been made in 1994 by Sachs (see [31]).

We denote by $D = (V, E)$ the directed graph obtained from $G$ by orienting the Hamiltonian cycle and every triangles cyclically. The main idea of Fleischner and Stiebitz's proof is to consider such an orientation $D$ of $G$ and to introduce the following polynomial:

$$P_D = \prod_{(u,v)\in E} (X_u - X_v)$$

Let us denote by $EE(D)$ (resp. $EO(D)$) the number of Eulerian subgraphs which have an even (resp. odd) number of edges. Thanks to some counting arguments, Fleischner and Stiebitz show in [16], that

$$\left| \left( X^{(1,\dots,1)} \right)^* (P_D) \right| = |EE(D) - EO(D)|$$

and that, moreover, $EE(D) - EO(D) = 2$ [4]. Hence, the coefficient of $X^{(1,\dots,1)}$ in $P_D$ is non zero. As before, we show, using the combinatorial Nullstellensatz, that $P_D$ cannot vanish on every point of $\{0,1,2\}^n$.

Indeed, assume by contradiction that $P_D$ vanishes on $\{0,1,2\}^n$. Then, by the combinatorial Nullstellensatz, $P_D$ can be written

$$P_D = \sum_{i=1}^{n} X_i(X_i - 1)(X_i - 2)H_i$$

with $$\forall i \in [\![ 1 \ ; \ n ]\!] \qquad \deg(H_i) \leq \deg(P_D) - 3$$

Let us denote, as earlier, $n_i = (1, \dots, 1, 0, 1, \dots, 1)$ the $n$-tuple of $\{0,1\}^n$ which has exactly one zero on coordinate $i$. Since $\left( X^{(1,\dots,1)} \right)^* (P_D) \neq 0$, there exists $i \in [\![ 1 \ ; \ n ]\!]$ such that $(X^{n_i})^* (H_i) \neq 0$. Again, this contradicts the hypothesis on the degree of $H_i$.

*Remark.* A proper coloring for a directed graph is the same as a proper coloring for the underlying undirected graph. Actually, if $G$ is an undirected graph and $D$ is an orientation of $G$, then we can define

$$P_G = \prod_{(u,v)\in E(G)} (X_u - X_v) \qquad \text{and} \qquad P_D = \prod_{(u,v)\in E(D)} (X_u - X_v)$$

We have that $$P_G = (-1)^{|E(D)|} {P_D}^2$$
As a consequence, $P_G$ and $P_D$ have the same roots. However, using a directed version of the graph simplifies the proof of the counting argument.

Actually, a significant part of Fleischner and Stiebitz's proof relies on the following result of Alon and Tarsi (see [2]) :

**Theorem.** Let $D = (V, E)$ be a directed graph such that $EE(D) \neq EO(D)$. Then, $D$ is $f$-choosable with

$$f : \left\{ \begin{array}{ccc} V & \to & \mathbb{N} \\ v & \mapsto & d_v + 1 \end{array} \right.$$

where $d_v$ is the outdegree of $v \in V$.

*Proof.* Define $P_D = \prod_{(u,v)\in E} (X_u - X_v)$. Without loss of generality, we assume that the vertices of $D$ are the elements of $[\![ 1 \ ; \ n ]\!]$. As before,

$$\left| \left( X^{(d_1,\ldots,d_n)} \right)^* (P_D) \right| = |EE(D) - EO(D)|$$

which proves that the coefficient of $X^{(d_1,\ldots,d_n)}$ in $P_D$ is non zero. For every $i \in [\![ 1 \ ; \ n ]\!]$, let $S_i$ be a set of size $d_i + 1$. Assume by contradiction that $P_D$ vanishes on every point of $S_1 \times \cdots \times S_n$. Then, by the combinatorial Nullstellensatz, $P_D$ can be written

$$P_D = \sum_{i=1}^{n} \left( \prod_{s\in S_i} (X_i - s) \right) H_i$$

with $$\forall i \in [\![ 1 \ ; \ n ]\!] \qquad \deg(H_i) \leq \deg P_D - |S_i|$$
Since $\left( X^{(d_1,\ldots,d_n)} \right)^* (P_D) \neq 0$, there exists $i \in [\![ 1 \ ; \ n ]\!]$ such that

$$\left( X^{(d_1,\ldots,d_n)} \right)^* \left( \left( \prod_{s\in S_i} (X_i - s) \right) H_i \right) \neq 0$$

which leads to a contradiction by considering the degree of $H_i$. □

A simple corollary of that result is that a graph $G$ of maximum degree $\Delta$ is $\Delta + 1$-choosable so, in particular, $\Delta + 1$-colorable. This is part of the Brooks' theorem. Besides, the complete proof of Brooks' theorem using the combinatorial Nullstellensatz has been made by Hladkýa, Král and Schauz (see [22]).

The ideas of Alon and Tarsi have really been fruitful, and not only for usual graph coloring. For instance, Norine, Wong and Zhu used Alon and Tarsi ideas in order to prove some results on $(p, q)$-list coloring (see [28]). If $(p, q) \in \mathbb{N}^2$ satisfies $p > q$, we call $(p, q)$-*coloring* of a graph $G$ a $p$-coloring that satisfies an additional constraint on the distance between colors: two adjacent vertices must have colors at distance at least $q$. However, such a definition has side effects which break the symmetry we usually have on colors. In order to make a better definition, we consider $\mathbb{Z}_p$ as the set of colors and define the following distance:

$$d : \left\{ \begin{array}{ccc} [\![ 0 \ ; \ p-1 ]\!]^2 & \to & \mathbb{R} \\ (i, j) & \mapsto & \min \left( |i - j| , p - |i - j| \right) \end{array} \right.$$

Intuitively, it is the length of the shortest path between $i$ and $j$ if one represents the elements of $\mathbb{Z}_p$ as equally distributed points of a circle. Hence, a $(p, q)$-coloring of some graph $G$ is a coloring of $G$ with elements of $\mathbb{Z}_p$ such that two vertices that are connected by an edge have colors at distance at least $q$ for the distance $d$. For $q = 1$ this is the usual definition of a $p$-coloring.

We can also define the notion of $f$-$(p, q)$-*choosability* when $f$ is bounded by $p$. Norine, Wong et Zhu give an extension of the above result in [28]. Once again, the proof relies on the combinatorial Nullstellensatz.

The proofs made in this thesis follow the general idea of the works presented here. However, our work is innovative and offers a different point of view on those algebraic proofs. One of the main novelty is the introduction of an object that is, somehow, the dual of a polynomial that encodes the coloring problem (and more generally, problems on graphs that can be expressed with polynomials): *precolorings* (see Section 1.10). One of the difficulties of the previous proofs is the choice of a good polynomial to encode the problem. The same difficulty arises in the choice of good precolorings. Nevertheless, we give hints to choose them wisely. This is, perhaps, an exciting new path to explore.

After those years of doctoral studies, it is now time to write a final dot to this work. I realize that this is only the beginning of that exploration. There is so much left to do!

We hope that, despite some heavy formalism, which is unfortunately mandatory due to the complexity of the mathematical objects manipulated in this thesis, the reading of this manuscript will be pleasant and inspiring. We hope that other mathematicians and computer scientists will pursue the work humbly started here.

Finally, those years of doctoral studies are the final act of a long scholarship and this manuscript, the last examination. We thank the jury members for accepting to review this thesis despite the natural apprehension that this causes to any student.

> "The hardship of an examination is useful and fair, and despite easy declamations, he who has not overcome it will not overcome any."
>
> Paul Valéry

# Chapter 0

# Basic definitions

This section contains some common definitions. We will frequently refer to it when appropriate all along this thesis so the reader is invited to skip linear reading of this part.

### 0.0.1 General algebra

**Definition 0.0.1.** Let $G$ be a group and $H \subseteq G$. The *subgroup generated by $H$ on $G$* is the smallest (for the inclusion) subgroup of $G$ that contains $H$. We denote it by $\langle H \rangle$.

If a subgroup is generated by a finite set, we say that it is a subgroup of *finite* type.

**Definition 0.0.2.** Let $\mathcal{A}$ be a ring and $S \subseteq \mathcal{A}$. The *ideal generated by $S$ on $\mathcal{A}$* is the smallest (for the inclusion) ideal of $\mathcal{A}$ that contains $S$. We denote it by $\langle S \rangle$.

*Remark.* In case of a ring, these two notions do not necessarily coincide. For instance, the subgroup generated by 1 on $\mathbb{F}_p[X]$ is finite (it is $\mathbb{F}_p$) whereas the ideal generated by 1 on $\mathbb{F}_p[X]$ is infinite (it is $\mathbb{F}_p[X]$).

**Definition 0.0.3** (characteristic)**.** Let $\mathcal{A}$ be a ring. The *characteristic* of $\mathcal{A}$ is the unique $\xi \in \mathbb{N}$ such that $\operatorname{Ker} \phi = \xi\mathbb{Z}$ where

$$\phi : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathcal{A} \\ k & \mapsto & k \cdot 1_{\mathcal{A}} \end{array} \right.$$

**Definition 0.0.4** (integral domain)**.** A ring $\mathcal{A}$ is said to be an *integral domain* whenever $\mathcal{A} \neq \{0\}$, $\mathcal{A}$ is commutative and

$$\forall a, b \in \mathcal{A} \qquad ab = 0 \Rightarrow a = 0 \vee b = 0$$

**Theorem 0.0.5.** Let $k \in \mathbb{N}$. If $k$ cannot be written $k = p^\ell$ with $p$ prime and $\ell \geq 1$, then there is no field of cardinality $k$. Otherwise, there exists a unique (up to isomorphism) field of cardinality $k$ that we denote by $\mathbb{F}_k$. It's characteristic is $p$.

**Definition 0.0.6** (module)**.** Let $(\mathcal{A}, +, \times)$ be a ring and $(M, +)$ be an Abelian group. We say that $(M, +, \cdot)$ is an $\mathcal{A}$-*module* (or a *left* $\mathcal{A}$-*module*) whenever

- $\forall a \in \mathcal{A} \quad \forall x, y \in M \qquad a \cdot (x + y) = a \cdot x + a \cdot y$
- $\forall a, b \in \mathcal{A} \quad \forall x \in M \qquad (a + b) \cdot x = a \cdot x + b \cdot x$
- $\forall x \in M \qquad 1_{\mathcal{A}} \cdot x = x$
- $\forall a, b \in \mathcal{A} \quad \forall x \in M \qquad (a \times b) \cdot x = a \cdot (b \cdot x)$

### 0.0.2 Graph theory

**Definition 0.0.7.** A *directed graph* is a pair of sets $(V, E)$ such that $E \subseteq V^2$. Such a graph is said to be *simple* whenever

$$\forall v \in V \qquad (v, v) \notin E$$

The graph is said to be *undirected* whenever

$$\forall u, v \in V \qquad (u, v) \in E \Leftrightarrow (v, u) \in E$$

In this case, we will write indifferently $uv$ or $vu$ for the edge $(u, v)$ or $(v, u)$.

*Remark.* Unless otherwise stated, all the graphs in this thesis are simple and undirected.

**Notation.** Let $G = (V, E)$ be an undirected graph. For $v \in V$ and $e \in E$, we write $v \in e$ for

$$\exists u \in V \quad e = (v, u) \vee e = (u, v)$$

**Definition 0.0.8.** Let $k \in \mathbb{N}$, the complete graph on $k$ vertices, denoted by $K_k$ is the graph $\Big(\llbracket 1 \ ; \ k \rrbracket, \llbracket 1 \ ; \ k \rrbracket^2 \setminus \{(i, i) \colon i \in \llbracket 1 \ ; \ k \rrbracket\}\Big)$.

**Definition 0.0.9** (graph factor)**.** A *graph factor* of a graph $G$ is a spanning subgraph or, in other words, a subgraph that has the same vertex set as $G$. Such a subgraph is called $k$-*factor* if it is $k$-regular.

**Definition 0.0.10** (Eulerian graph)**.** A graph is said to be *Eulerian* if each of its vertices has even degree.

**Definition 0.0.11** (Eulerian circuit)**.** A graph has an Eulerian circuit if there exists a closed walk that uses every edge exactly once.

**Proposition 0.0.12.** A graph is Eulerian if and only if it has an Eulerian circuit.

**Definition 0.0.13** (Eulerian orientation)**.** A graph $G$ has an *Eulerian orientation* if and only if there exists an orientation of its edges so that for every vertex, the in-degree is equal to the out-degree.

*Remark.* In particular, if a graph has an Eulerian orientation then it is Eulerian. The converse also holds.

**Example.**

- A 1-factor is a perfect matching
- A 2-factor is a set of cycles that spans the vertex set. We also call it a *cycle factor*.

**Definition 0.0.14** (graph morphism)**.** Let $G = (V, E)$ and $G' = (V', E')$ be two graphs. We say that the total function $f : V \to V'$ is a *graph homomorphism* (or simply a *graph morphism*) from $G$ to $G'$ whenever

$$\forall u, v \in V \quad uv \in E \Rightarrow f(u)f(v) \in E'$$

In other words, $f$ maps an edge of $G$ to an edge of $G'$. We say that $f$ is an *isomorphism* if $f$ is bijective and $f^{-1}$ is a graph morphism (from $G'$ to $G$).

**Notation.** If there exists a graph isomorphism between $G$ and $G'$, we will write $G \simeq G'$.

*Warning.* In general, a bijective morphism (even in another context than in graph theory), is not an isomorphism. Indeed, the inverse function may not be a morphism!

*Remark.* Most of the time, two isomorphic graphs will be considered equal. Indeed, in this thesis, we are interested only by the structure of graphs which is preserved by graph isomorphisms.

**Definition 0.0.15** (graph coloring)**.** Let $G$ be a simple graph and $k \geq 1$ be an integer. We say that $\rho : V(G) \to [\![ 0 ; k-1 ]\!]$ is a *$k$-coloring* of $G$ (or, a *proper $k$-coloring* of $G$) if and only if

$$\forall u, v \in V(G) \qquad uv \in E(G) \Rightarrow \rho(u) \neq \rho(v)$$

The integers used to label the vertices are called *colors*. This terminology is related to the history of combinatorics.

*Remark.* A graph $k$-coloring of $G$ is actually a graph morphism from $G$ to $K_k$, the complete graph with $k$ vertices.

**Definition 0.0.16** (chromatic number)**.** For any graph $G$, the chromatic number of $G$, denoted by $\chi(G)$, is the smallest number of colors required to properly color $G$.

**Definition 0.0.17** (vertex-transitive graph)**.** A graph $G = (V, E)$ is said to be *vertex-transitive* whenever for every pair of vertices $u, v \in V$, there exists a graph isomorphism $f : V \to V$ from $G$ to $G$[1] such that $f(u) = v$.

### 0.0.3 Modular arithmetic

Recall that for every $n \in \mathbb{N}^*$, the relation defined on $\mathbb{Z}$ by

$$\forall k, \ell \in \mathbb{Z} \quad k \sim \ell \Leftrightarrow k - \ell \in n\mathbb{Z}$$

is an equivalence relation. The set $\mathbb{Z}_n$ has a natural ring structure. We will often need to convert an integer to its class of equivalence modulo $n$. Here are three useful functions to achieve this.

[1] We call such an isomorphism, a *automorphism*.

**Definition 0.0.18.** The operator *modulo* will be written with the infix notation. For every $i \in \mathbb{Z}$ and every $n \in \mathbb{N}^*$, the modulo $n$ of $i$ is the remainder of the euclidean division of $i$ by $n$. We denote it by $i \,\%\, n$. More formally, $\%$ is a total function from $\mathbb{Z} \times \mathbb{N}^*$ such that for every $(i, n) \in \mathbb{Z} \times \mathbb{N}^*$, $i \,\%\, n = \%(i, n)$ is the unique $r \in [\![ 0 \ ; \ n-1 ]\!]$ such that $i - r \in n\mathbb{Z}$.

Two integer $i, j \in \mathbb{Z}$ that satisfy $i \,\%\, n = j \,\%\, n$ are said to be *equal modulo* $n$. We will denote it by

$$i = j \,[n]$$

**Definition 0.0.19.** Let $n \in \mathbb{N}^*$. The cast modulo $n$ associates to an integer $i$ its class of equivalence modulo $n$ in the quotient $\mathbb{Z}_n = {}^{\mathbb{Z}}/_{n\mathbb{Z}}$. We denote its class by $\bar{i}^n$. More formally,

$$\bar{\cdot}^n : \left\{ \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}_n \\ i & \mapsto & i + n\mathbb{Z} \end{array} \right.$$

**Definition 0.0.20.** Let $n \in \mathbb{N}^*$ and $i + n\mathbb{Z}$ be a class of equivalence modulo $n$. The uncast of $i\mathbb{Z}$ associates a canonical integer $j = \underline{i}_n$ such that $\bar{j}^n = i + n\mathbb{Z}$.

$$\underline{\cdot}_n : \left\{ \begin{array}{ccc} \mathbb{Z}_n & \to & [\![ 0 \ ; \ n-1 ]\!] \\ i + n\mathbb{Z} & \mapsto & i \,\%\, n \end{array} \right.$$

### 0.0.4 Linear algebra

In this section, $\mathcal{A}$ is a ring and $\mathbb{K}$ a field.

**Definition 0.0.21.** We say that a matrix has *full column rank* when the dimension of its image (linear space spanned by its columns) is equal to its number of rows. In other words, the dimension of the image is maximum. We say that a matrix has *full row rank* when its transpose has full column rank.

*Warning* 0.0.22. This terminology is different from the usual one. Usually, the column (resp. row) rank of a matrix is the dimension of the space spanned by its columns (resp. rows). This is the same here. However, a matrix is usually said to have full column rank (resp. full row rank) whenever its columns (resp. rows) are linearly independent. So, the linear map canonically associated (resp. canonically associated to the transposed of the matrix) is injective.

In this thesis, full column rank (resp. full row rank) means that the space spanned by the columns (resp. rows) has maximal (full) dimension. Hence, it is equal to the number of rows (resp. columns). In this thesis, full columns rank (resp. full row rank) means that the matrix is surjective (resp. injective).

**Definition 0.0.23** (Kronecker product)**.** Let $n, m, p, q \geq 1$ be integers and $A \in \mathscr{M}_{n,k}(\mathcal{A})$, $B \in \mathscr{M}_{p,q}(\mathcal{A})$. The *Kronecker product* (or *tensor product*) $A \otimes B$ is the $np \times kq$ block matrix

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1k}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nk}B \end{bmatrix}$$

**Properties 1.** The $\otimes$ operator is bilinear, associative, non-commutative.

**Proposition 0.0.24.** Let $n, k, p, q, m, \ell \geq 1$ be integers and $A \in \mathscr{M}_{n,k}(\mathcal{A})$, $B \in \mathscr{M}_{p,q}(\mathcal{A})$, $C \in \mathscr{M}_{k,m}(\mathcal{A})$ and $D \in \mathscr{M}_{q,\ell}(\mathcal{A})$. Then,

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$

*Remark.* Observe that the only restriction in Proposition 0.0.24 is that the matrix products $AC$ and $BD$ must be defined.

**Definition 0.0.25.** Let $F$ and $G$ be two sublinear spaces of a linear space $E$. We say that the sum $F+G$ is *direct* (and write it $F \oplus G$) whenever for every $x \in F+G$ there is a unique way to write $x = f + g$ with $f \in F$ and $g \in G$.

### 0.0.5 Some useful abuses

Abuses of language and/or notations are almost always evil. However, in some particular cases it may make things clearer.

- We say that a graph $H$ is included in a graph $G$ ($H \subseteq G$) whenever there exists a subgraph of $G$ that is homomorphic to $H$.
- We will often omit to define the order of the rows and the columns of incidence matrices. This is because we are only interested in the rank so it does not matter.
- The vectors of $\mathbb{K}^n$ will be sometimes represented as column vectors (which is, in my opinion, the most natural way to draw them), or sometimes as row vectors (as it is more convenient to draw them in a paragraph). However, we will always be cautious that the matrix vector product are well defined.
- In the context of power graphs, since $G \subseteq {\Gamma_k}^G$, we will sometimes confound $v \in V(G)$ and its canonical map into ${\Gamma_k}^G$. We will do the same of abuse for the edges of $G$ as they naturally map to edges in ${\Gamma_k}^G$. This should not disturb the reader as the context should always be clear. Besides, it will often be convenient to think about edges of ${\Gamma_k}^G$ as being edges of $G$.
- A vector of $\mathbb{K}^k$ will also be confounded with a map from $[\![ 0 \ ; \ k-1 ]\!]$ to $\mathbb{K}$.

# Chapter 1

# Power graphs

A connected graph $G$ on $n$ vertices is non-bipartite if and only if its incidence matrix (vertices versus edges) has rank $n$ over the reals. More generally, if the set of cliques of size $k$ is rich enough so that the incidence matrix of vertices versus copies of $K_k$ has rank $n$, the graph $G$ is not $k$-colorable. However, the existence of such a "clique certificate" is far from being equivalent to the non $k$-colorability. In this chapter, we introduce a graph ${\mathbb{Z}_k}^G$, inspired from graph reconfiguration, which has the property that $G$ is not $k$-colorable if and only if ${\mathbb{Z}_k}^G$ has a $k$-clique certificate. This can be seen as a graph interpretation of Hilbert's Nullstellensatz certificate for non $k$-colorability. However, even though the $k$-colorability of $G$ is equivalent to the $k$-colorability of ${\mathbb{Z}_k}^G$ when $k$ is a prime, this equivalence fails for instance when $k = 4$. But, when $k$ is a power of a prime number, $G$ is $k$-colorable if and only if another graph, ${\mathbb{F}_k}^G$ is $k$-colorable. This indicates that, for instance, the natural object to investigate 4-colorability is the reconfiguration graph based on $\mathbb{F}_4$ rather than the usual one based on the classical interpretation of colorability by polynomials. We discuss the properties of these reconfiguration graphs at the end of this chapter.

## 1.1 Introduction

A $k$-coloring of a graph $G$ on $n$ vertices is a mapping from the vertex set of $G$ into $[\![ 0 \ ; \ k-1 ]\!]$ or any set of $k$ elements. A coloring $c$ is said to be a *proper coloring* if every edge is colored by two distinct colors. A very popular approach to colorability is the study of reconfiguration where one forms a graph over proper colorings by letting an edge between two of them when they differ on one vertex. A good introduction to reconfiguration graphs can be found in [27] and in [34]. We adopt a similar point of view by considering the set of all $k$-labellings of $G$ (rather than restricting to proper colorings) and letting an edge between two labellings $x$ and $x'$ of $G$ with elements of $\mathbb{Z}_k$ whenever they differ on two vertices $u, v$ which forms an edge of $G$ and such that $x(u) - x'(u) = x'(v) - x(v)\,[k]$, in other words, if $x'$ is obtained from $x$ by transferring some weight along the edge $uv$ (A formal definition will be made in 1.3.1.). We denote this graph by ${\mathbb{Z}_k}^G$. Observe that, potentially, a different graph could have been obtained if the equality $x(u) - x'(u) = x'(v) - x(v)$ would not have

been computed modulo $k$ but on another group $\Gamma$ (we would write the graph $\Gamma^G$ as we will see later). This (exponential size) reconfiguration graph ${\mathbb{Z}_k}^G$ happens to be a very natural object to investigate since, as we prove in Proposition 1.5.6, the set of cliques of size $k$ in ${\mathbb{Z}_k}^G$ is full rank over the vertices (that has rank equal to $k^n$) whenever $G$ is not $k$-colorable. In other words, when a graph is not $k$-colorable, there exists an associated exponential size graph which is not $k$-colorable for some rather "obvious" reason (the existence of a clique certificate).

Note that ${\mathbb{Z}_k}^G$ is a vertex-transitive graph, and thus the existence of a clique certificate is equivalent to the existence of a linear combination of cliques which is equal to a single vertex[1]. The reader familiar with the interpretation of $k$-colorability by multivariate polynomials will recognize here the equation $\sum Q_i P_i = 1$ and the classical Nullstellensatz certificates of non $k$-colorability. And this is indeed the case: ${\mathbb{Z}_k}^G$ is exactly the underlying graph structure of the usual polynomial approach. The goal of this chapter is to investigate, from the graph theory point of view, this reconfiguration-flavored graph.

Here is the first natural question to ask: is $\chi(G) > k$ equivalent to $\chi({\mathbb{Z}_k}^G) > k$? This is indeed the case when $k$ is a prime number, but surprisingly this equivalence fails even for $k = 4$ and it turns out that the right object to consider in this case is not ${\mathbb{Z}_4}^G$ but instead ${\mathbb{F}_4}^G$ (the field with 4 elements). We show in this chapter that $\chi(G) > k$ is equivalent to $\chi({\mathbb{F}_k}^G) > k$ for finite fields, and that non $k$-colorability of $G$ can be shown by a clique certificate of ${\mathbb{F}_k}^G$. This indicates for instance that the right power graph underlying four colorability might be ${\mathbb{F}_4}^G$.

The rest of this chapter is dedicated to the general properties of these graphs.

## 1.2 Clique certificates

In the following, $\mathbb{K}$ designates an arbitrary field[2].

### 1.2.1 Incidence matrices

Let $E = \{e_1, \ldots, e_n\}$ be a set and $F = \{f_1, \ldots, f_k\}$ be a set of subsets of $E$. The *incidence matrix* of $E$ *versus* $F$ is a $n \times k$ matrix $M = (m_{i,j})$ with $n = |E|$ and $k = |F|$ such that

$$\forall (i,j) \in [\![ 1 \ ; \ n ]\!] \times [\![ 1 \ ; \ k ]\!] \qquad m_{i,j} = \begin{cases} 1 & \text{if and only if} \quad e_i \in f_j \\ 0 & \text{otherwise} \end{cases}$$

**Example.**

- Given a graph $G$, we can consider the incidence matrix of its vertices versus its edges.
- In an affine space over a finite field, we can consider the matrix of the points versus the lines.

[1] This is an abuse, a vector with exactly one 1 and $k-1$ zeros can be confound with the vertex of $G$ that corresponds to the coordinate of the 1. See Lemma 1.3.2.

[2] Note to french readers: In English, every field is, by default, assumed to be commutative. In this thesis, we will always consider commutative fields.

*Remark.* Writing "the incidence matrix of $G$" is actually a bit inappropriate as we would need to specify the order of the rows and columns of the matrix. However, we will almost always spare ourselves from doing this as we will only be interested in the rank of such matrix. Also, in order to have lighter notations and when the context is clear, we will write $\operatorname{Im} M$, $\operatorname{rk} M$ instead of the heavy $\operatorname{Im}_{\mathbb{K}} M$ and $\operatorname{rk}_{\mathbb{K}} M$ to designate the image and the rank of $M$ in the field $\mathbb{K}$.

### 1.2.2 Link with colorability

Let us start with an easy case. Assume one wants to show that some graph $G$ is not bipartite. Consider the incidence matrix $M_2$ of the vertices versus the edges. Let us show that if $M_2$ has full column rank (see Def 0.0.21 and Warning 0.0.22), then $G$ is not bipartite. Assume for the sake of contradiction that $G = (V, E)$ is bipartite. We write $V = A \uplus B$ such that every edge is between $A$ and $B$. Now consider a linear combination of columns of $M_2$ and observe that the sum of the coefficients over all vertices of $A$ is the same as the sum on $B$. Hence, $M_2$ cannot have full column rank because, for instance, we cannot create a vector such that all coordinates but one are zero.

Observe that this works in any field. The key point is that the color classes of a coloring are stables sets that partition the set of vertices. We will now see how to generalize this result.

**Definition 1.2.1.** We define $\mathcal{K}_r(G)$ to be the set of all the subgraphs of $G$ that are $r$-cliques. Let us denote by $M_r(G)$ (or simply $M_r$) the incidence matrix of $V(G)$ versus $\mathcal{K}_r(G)$.

**Notation.** Let $E$ and $F$ be two sets. For every $e \in E$, we denote by $\mathbb{1}_e$ the total function from $E$ to $F$ defined by

$$\forall x \in E \qquad \mathbb{1}_e(x) = \begin{cases} 1 & \text{if} \quad x = e \\ 0 & \text{otherwise} \end{cases}$$

**Proposition 1.2.2.** Let $r \geq 1$ be an integer and $G$ be a graph. If there exists $v \in V(G)$ such that $\mathbb{1}_v \in \operatorname{Im} M_r$, then $\chi(G) > r$.

*Proof.* Assume for the sake of contradiction that $G$ has a proper $r$-coloring. The idea is to partition the vertices of $G$ into monochromatic stable sets. Such a partition of the vertices naturally translates into a partition of the rows of $M_r$. Since every $r$-clique has exactly $r$ colors, any linear combination of the columns of $M_r$ has the same weight on each monochromatic part. This contradicts the fact that there exists $v \in V(G)$ such that $\mathbb{1}_v \in \operatorname{Im} M_r$. □

We will see in Example 1.2.3 that the converse does not always hold. Actually, the matrix $M_r$ may be empty! For instance, there exists triangle-free graphs whose chromatic number is 4 (see [25]). Even though, it could be that $\chi(G) > r$ and that $M_r(G)$ does not have any $\mathbb{1}_v$ in its image. In case there exists a $v \in V(G)$ such that $\mathbb{1}_v \in \operatorname{Im}(M_r(G))$, any linear combination of the columns of $M_r(G)$ that gives $\mathbb{1}_v$ is called *$r$-clique certificate in* $\mathbb{K}$.

Indeed, such a combination is a proof that $G$ is not $r$-colorable. We say that $v$ is the *center of the certificate*.

**Example.** In Figure 1.1 we draw an example of a 3-clique certificate with weights in $\mathbb{F}_2$. Every triangle has weight 1. In the end, every vertex but the bottom one sums to 0. More generally, if every vertex of a graph $G$ but one is in an even number of triangles, then $G$ has a 3-clique certificate (in $\mathbb{F}_2$) hence is not 3-colorable.

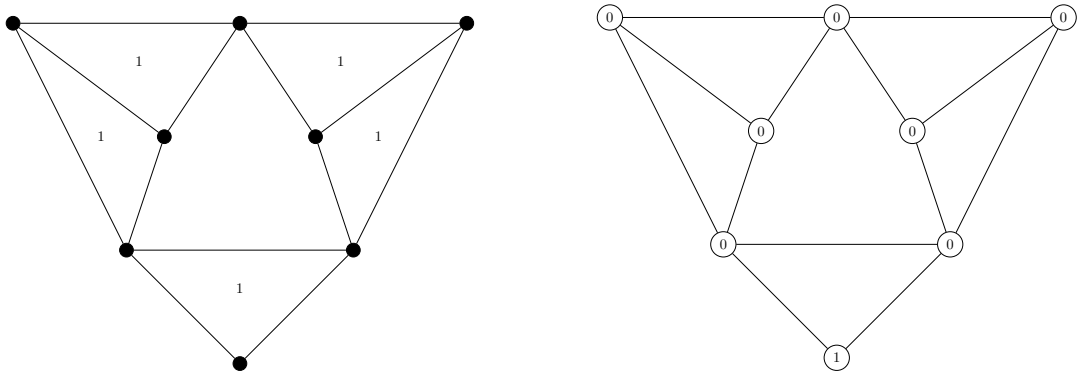



Figure 1.1: A 3-clique certificate in $\mathbb{F}_2$

The existence of a clique certificate may depend on the underlying field. Consider for instance the 2-clique certificate of a triangle. The matrix $M_2(\triangle)$ is represented in Figure 1.2 with an example of a 2-clique certificate.

$$M_2(\triangle) = \begin{array}{c} 0 \\ 1 \\ 2 \end{array} \begin{array}{c} \left[\begin{array}{ccc} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right] \\ \begin{array}{ccc} 01 & 02 & 12 \end{array} \end{array}$$

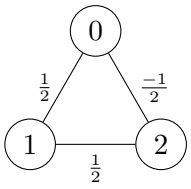


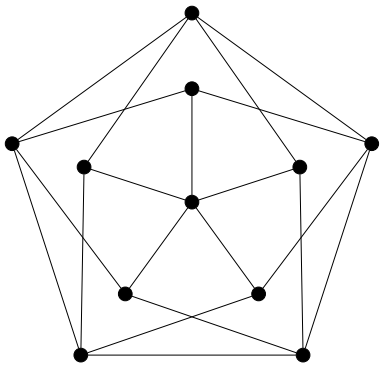

Figure 1.2: A 2-clique certificate in $\mathbb{R}$

The rank of $M_2(\triangle)$ is 2 in $\mathbb{F}_2$ but 3 is $\mathbb{R}$. Hence, there exists a 2-clique certificate in $\mathbb{R}$ but not in $\mathbb{F}_2$. Indeed, if a linear combination of the columns of $M_2(\triangle)$ in $\mathbb{F}_2$ would give $\mathbb{1}_0$ for instance, then, by symmetry, we would also have $\mathbb{1}_1$ and $\mathbb{1}_2$ which would contradict the fact that the rank of $M_2$ in $\mathbb{F}_2$ is 2.

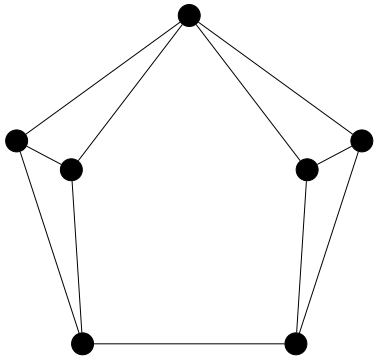
So, the choice of the underlying field for matrices is crucial when it comes to clique-certificates. Note that Proposition 1.2.2 only gives a sufficient condition for $G$ to be not $r$-colorable. Hence, it suffices to find a field[3] $\mathbb{K}$ such that $\mathrm{Im}_{\mathbb{K}} M_r(G)$ does not contain any $\mathbb{1}_v$ for $v \in V$. However, this does not always exists as we will see in Example 1.2.3.

[3] Actually, we may even weaken the algebraic structure by taking a ring instead of a field. However, being able to divide in the end is useful to avoid technical details latter. The only parameter that matters is the

**Example 1.2.3.** The Grötzsch's graph (see Figure 1.3a) has no triangle. Hence, there is no 3-clique certificate even though it is not 3-colorable (see [25]). The Moser spindle graph (see Figure 1.3b) has triangles but its matrix $M_3$ satisfies that for all $v \in V$, $\mathbb{1}_v \notin \mathrm{Im}_{\mathbb{R}} M_3$. However, the Moser spindle graph is not 3-colorable.

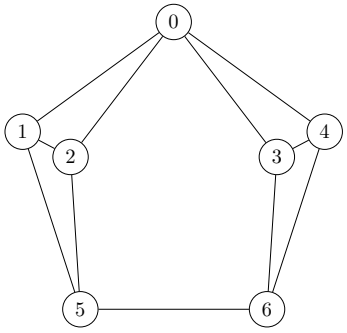


(a) The Grötzsch's graph



(b) The Moser Spindle graph

The Moser Spindle graph has chromatic number 4. However, we can show that it has no 3-clique certificate in $\mathbb{R}$. To prove this, it suffices to check that the equation $M_3 X = \mathbb{1}_i$ has no solution for $X \in \mathbb{R}^7$ for any $i \in [\![ 0 \ ; \ 6 ]\!]$.




$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{array}{c} \\ 012 \end{array} \begin{array}{c} \\ 034 \end{array} \begin{array}{c} \\ 125 \end{array} \begin{array}{c} \\ 346 \end{array}$$

Figure 1.4: Moser Spindle graph and its matrix $M_3$

characteristic of the field. Since it cannot be any number (the characteristic of a field is either zero or a prime number), one may want to consider clique certificates in rings rather than in fields. The matrices form a module and not a linear space which makes the study of the rank more complicated... Anyway, this is only for clique-certificates. The new kind of certificates that are studied in this thesis are not more general if one consider values in rings by Corollary 1.7.2.

## 1.3 Power graphs

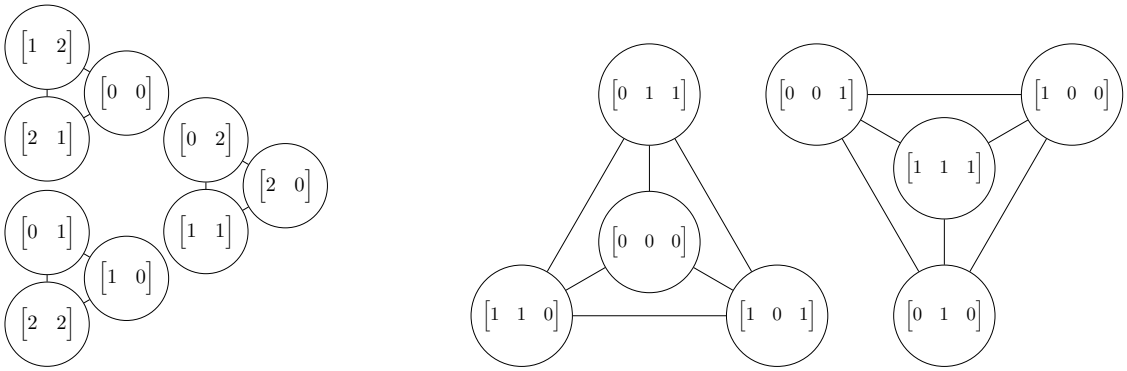
In this section, $\Gamma_k$ designates either $\mathbb{Z}_k$ or, if $k$ is a power of a prime number, the field with $k$ elements $\mathbb{F}_k$.

**Definition 1.3.1** (${\Gamma_k}^G$)**.** Let $k \geq 2$ and $G$ be graph. We define the graph ${\Gamma_k}^G$ by

- $V\left({\Gamma_k}^G\right) = {\Gamma_k}^{V(G)}$
- For every $(x, y) \in V\left({\Gamma_k}^G\right)^2$, $(x, y) \in E\left({\Gamma_k}^G\right)$ if and only if there exists $(u, v) \in E$ such that

  i) $\forall w \in V(G) \setminus \{u, v\} \qquad x(w) = y(w)$
  ii) $x(u) - y(u) \neq 0$
  iii) $x(u) - y(u) = y(v) - x(v)$

We denote the total functions from $V(G)$ to $\Gamma_k$ (the vertices of ${\Gamma_k}^G$) by vectors of size $|V(G)|$ whose values are in $\Gamma_k$. This is quite convenient to represent power graphs. Examples are given in Figure 1.5.




(a) The graph $\mathbb{Z}_3{}^{\bullet-\bullet}$ (b) The graph $\mathbb{Z}_2{}^{\triangle}$

Figure 1.5: Examples of power graphs

*Remark.*

- When $k = p$ is prime, we have that ${\mathbb{F}_p}^G = {\mathbb{Z}_p}^G$ since $\mathbb{F}_p = \mathbb{Z}_p$. In such case, we write $p^G$.
- When $k = p^\ell$ with $p$ prime and $\ell \geq 1$, both ${\mathbb{Z}_k}^G$ and ${\mathbb{F}_k}^G$ are defined but we will see later that they are not isomorphic in general.
- We can reformulate the condition for $cc'$ to be an edge of ${\Gamma_k}^G$ as

$$\exists uv \in E(G) \quad \exists a \in \Gamma_k \setminus \{0\} \qquad c' - c = a\,(\mathbb{1}_u - \mathbb{1}_v)$$

**Lemma 1.3.2.** For every $k \geq 2$, the graph $G$ is an induced subgraph of ${\Gamma_k}^G$.

*Proof.* The vertices of $G$ can be seen as vertices of ${\Gamma_k}^G$. Indeed, one can identify $u \in V(G)$ and $\mathbb{1}_u \in V\left({\Gamma_k}^G\right)$. Now take $uv \in E(G)$ and observe that

$$\mathbb{1}_u - \mathbb{1}_v = 1 \cdot (\mathbb{1}_u - \mathbb{1}_v)$$

Hence, $G$ is an induced subgraph of ${\Gamma_k}^G$. □

**Corollary 1.3.3.** In particular, $\chi(G) \leq \chi\left({\Gamma_k}^G\right)$.

One can wonder whether the converse inequality holds. As we can see on Figure 1.5b, it is false in general since $\chi(\triangle) = 3$ and $\chi\left({\mathbb{Z}_2}^{\triangle}\right) = 4$. However, is it true that $\chi(G) = k$ if and only if $\chi\left({\Gamma_k}^G\right) = k$? We will see in Section 1.4 that the answer depends on $\Gamma_k$ being a field or not. However, we will prove that $G$ is not $k$-colorable if and only if ${\Gamma_k}^G$ has some certificate. Such a certificate will be called *edge-clique certificate*.

### 1.3.1 Edge-clique certificates

We have seen in Section 1.2 a sufficient condition for a graph $G = (V, E)$ to be not $k$-colorable using its cliques of size $k$. However, the condition was not necessary in general (see Example 1.2.3). We define here a similar notion in the context of power graphs: the edge-clique certificates. Our goal is to have an equivalence between the non $k$-colorability of $G$ and the existence of an edge-clique certificate in ${\Gamma_k}^G$.

**Definition 1.3.4** (edge-clique certificate)**.** For $x, d \in {\Gamma_k}^V$, we call *d-line* a set of the form

$$L_x(d) = \{x + \lambda\, d \colon \lambda \in \Gamma_k\}$$

In the case $d = 0$, any 0-line is a point and we call it a *trivial line*. If $d = \mathbb{1}_u - \mathbb{1}_v$ with $uv \in E$, we call any $(\mathbb{1}_u - \mathbb{1}_v)$-line an *edge-clique*. Observe that edge-cliques are $k$-cliques of ${\Gamma_k}^G$.

An *edge-clique certificate* is a weight function on the edge-cliques such that every vertex but one (which we call the *center*) sums to zero. It is a $k$-clique certificate of ${\Gamma_k}^G$ that uses only $k$-cliques that are edge-cliques.

*Remark* 1.3.5. Thanks to the group structure of ${\Gamma_k}^V$, if there exists an edge-clique certificate, we can choose its center to be any point. Indeed, applying a translation to an edge-clique certificate gives an edge-clique certificate[4]. In particular, ${\Gamma_k}^G$ has an edge-clique certificate if and only if the incidence matrix of ${\Gamma_k}^V$ versus the edge-cliques has full row rank.

**Theorem 1.3.6.** Let $k \geq 2$ and $G$ be a graph. $G$ is not $k$-colorable if and only if ${\Gamma_k}^G$ has an edge-clique certificate.

This result can be surprising as edge-cliques are more constrained objects than cliques. Indeed, any edge-clique of ${\Gamma_k}^G$ is a $k$-clique but the converse is false in general (for $k \geq 3$, consider any $k$-clique of $G$). However, the $k$-clique certificate is now to be found in ${\Gamma_k}^G$ rather than $G$. Intuitively, we have more freedom since ${\Gamma_k}^G$ is a much bigger graph than $G$! The purpose of the next four sections is to establish the Theorem 1.3.6.

## 1.4 Differences between ${\mathbb{Z}_q}^G$ and ${\mathbb{F}_q}^G$

When $q$ is a non trivial power of a prime number $p$ (namely, $q = p^\ell$ with $\ell \geq 1$), we have defined two objects: ${\mathbb{Z}_q}^G$ which is always defined and ${\mathbb{F}_q}^G$ which exists only in this context since the cardinality of a finite field is always a power of a prime number (see Theorem 0.0.5). When $q = p$, these two objects are identical as $\mathbb{Z}_p = \mathbb{F}_p$. However, when $\ell \geq 2$, $\mathbb{Z}_q$ and $\mathbb{F}_q$ are not isomorphic: the characteristic of the first one is $q$ but the characteristic of the second one is $p$. In this section, we discuss the differences between these two objects. First, let us prove the following theorem:

**Theorem 1.4.1.** For any graph $G$, any $q$ that is a non trivial power of a prime, we have that ${\mathbb{F}_q}^G$ is $q$-colorable if and only if $G$ is $q$-colorable.

More precisely we will show how we can build a $q$-coloring of ${\mathbb{F}_q}^G$ from a $q$-coloring of $G = (V, E)$.

**Definition 1.4.2** (linear coloring)**.** For $c \in {\mathbb{F}_q}^V$, we define a labelling of ${\mathbb{F}_q}^G$ $c^* : {\mathbb{F}_q}^V \to \mathbb{F}_q$ by

$$\forall x \in {\mathbb{F}_q}^V \quad c^*(x) = \langle c, x \rangle$$

where $\langle c, x \rangle = \sum_{i=1}^{n} x_i c_i$ is the usual inner product[5] of ${\mathbb{F}_q}^n$ seen as a $\mathbb{F}_q$-linear space.

**Lemma 1.4.3.** For every $c \in {\mathbb{F}_q}^V$, the labelling $c$ is a proper coloring of $G$ if and only if $c^*$ is a proper coloring of ${\mathbb{F}_q}^G$.

[4]Actually, the graph ${\Gamma_k}^G$ is vertex-transitive and for every $u, v \in V\left({\Gamma_k}^G\right)$, there is a unique graph automorphism of ${\Gamma_k}^G$ that sends $u$ to $v$: this is the translation of vector $v - u$.

[5]Beware that we are working with finite fields and not $\mathbb{R}$ or $\mathbb{C}$. In particular, this inner product has isotropic vectors!

*Proof.* Take $v \in V$ and $c \in \mathbb{F}_q{}^V$. Observe that $c^*(\mathbb{1}_v) = \langle c, \mathbb{1}_v \rangle = c(v)$. So, if $c^*$ is a proper $q$-coloring of $\mathbb{F}_q{}^G$, then $c$ is a proper $q$-coloring of $G$ because $G \subseteq \mathbb{F}_q{}^G$ by Lemma 1.3.2. Conversely, assume that $c \in \mathbb{F}_q{}^V$ is a proper $q$-coloring of $G$. Let $xx' \in E\left(\mathbb{F}_q{}^G\right)$. By definition of $\mathbb{F}_q{}^G$,

$$\exists uv \in E \quad \exists a \in \mathbb{F}_q \setminus \{0\} \qquad x' - x = a(\mathbb{1}_u - \mathbb{1}_v)$$

so we have that

$$\begin{aligned} c^*(x') - c^*(x) &= \langle c, a(\mathbb{1}_u - \mathbb{1}_v) \rangle \\ &= a\left(\langle c, \mathbb{1}_u \rangle - \langle c, \mathbb{1}_v \rangle\right) \\ &= a\left(c(u) - c(v)\right) \end{aligned}$$

Since $c$ is a proper $q$-coloring of $G$, we have that $c(u) - c(v) \neq 0$. Since $a \neq 0$ and $\mathbb{F}_q$ is a field (which is an integral domain), $a(c(u) - c(v)) \neq 0$. Hence, $c^*(x') \neq c^*(x)$ and since this is true for any edge $xx'$ of $\mathbb{F}_q{}^G$, $c^*$ is a proper $q$-coloring of $\mathbb{F}_q{}^G$. □

This concludes the proof of Theorem 1.4.1. Indeed, we have that $\chi(G) \leq \chi\left(\mathbb{F}_q{}^G\right)$ by Corollary 1.3.3 and since we know how to extend a $q$-coloring of $G$ to $\mathbb{F}_q{}^G$ we also have that $\chi(G) \geq \chi\left(\mathbb{F}_q{}^G\right)$.

*Remark* 1.4.4.

- The proof of this result allows us to extend any proper $q$-coloring of $G$ to a proper $q$-coloring of $\mathbb{F}_q{}^G$ using the linear map $c \mapsto c^*$ defined in the proof. One can wonder what are the $q$-colorings of $\mathbb{F}_q{}^G$ and whether or not we can derive them from those of $G$. We investigate these questions in Section 1.8.
- Beware that this proof only works for the $q$-colorings of $\mathbb{F}_q{}^G$. Recall that we can see on Figure 1.5b that $\chi\left(2^{\triangle}\right) = 4$.
- The fact that $q$ is a power of a prime number is used to ensure that $\mathbb{F}_q$ is a field. In the proof of Lemma 1.4.3, we would not be able to obtain that $a(c(u) - c(v)) \neq 0$ if we were not in an integral domain. For instance, $\mathbb{F}_4{}^{K_4}$ is 4-colorable but if we consider instead $\mathbb{Z}_4{}^{K_4}$, then the previous proof does not work anymore because $\mathbb{Z}_4$ is not an integral domain. In particular, $2 \times 2 = 0$ although $2 \neq 0$. Actually, this graph is not 4-colorable:

**Proposition 1.4.5.** The graph $\mathbb{Z}_4{}^{K_4}$ is not 4-colorable.

*Proof.* Let us try to 4-color $\mathbb{Z}_4{}^{K_4}$. We restrict ourselves to the connected component of $\begin{bmatrix}0 & 0 & 0 & 0\end{bmatrix}$. Without loss of generality, we can assume that 0000 is white (For clarity, we will not draw the vector's bracket.). Consider the subgraph $H$ of $\mathbb{Z}_4{}^{K_4}$ defined in Figure 1.6. Since every vertex is connected by an edge to 0000, we have only three colors left. Up to a permutation of these colors, there is only one way to 3-color $H$ (see Figure 1.6).
Now, observe that each vertex with two 2's and two 0's is included into a triangle with vertices which have two 0's at the same position, one 1 and one 3. Hence, there are two possible choices represented on Figures 1.7a and 1.7b.

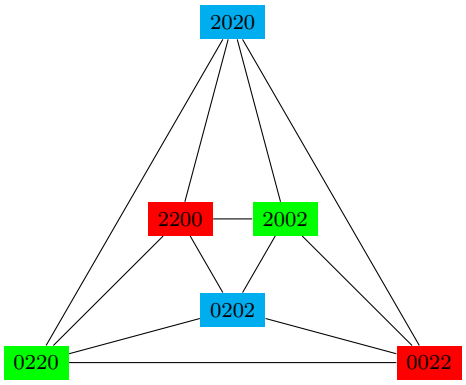



Figure 1.6: 3-coloring of a subgraph $H$ of ${\mathbb{Z}_4}^{K_4}$


(a) $H_1$ (b) $H_2$

Figure 1.7: Two choices for the colors of 3001 and 1003

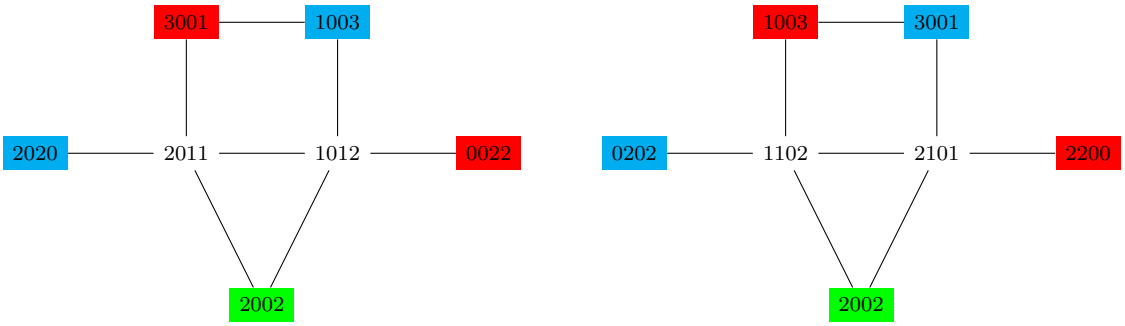
Assume that the coloring is as in graph $H_1$ (Figure 1.7a). Consider the subgraph $G_1$ (Figure 1.8a) to obtain a contradiction. Indeed, both 2011 and 1012 must be colored white. If the coloring is as in graph $H_2$ (Figure 1.7b), take the subgraph $G_2$ (Figure 1.8b).

□

So, the result of Theorem 1.4.1 is not true in general if we replace ${\mathbb{F}_q}^G$ by ${\Gamma_q}^G$, even if $q$ is a power of a prime number. We explained in Remark 1.4.4 that we cannot extend a proper $q$-coloring of $G$ to a proper $q$-coloring of ${\mathbb{Z}_q}^G$ with the "inner product trick" if $\mathbb{Z}_q$ is not a field[6]. Moreover, we just proved in Proposition 1.4.5 that we can have $\chi\left({\mathbb{Z}_k}^G\right) > k$ even if $\chi(G) = k$. We don't know the chromatic number of ${\mathbb{Z}_k}^{K_k}$ even for $k = 4$. Although this could be done by a brute force algorithm, we would rather like to have a deeper understanding of Proposition 1.4.5 an be able to know (or, at least to have a lower bound on) the chromatic number of ${\mathbb{Z}_k}^{K_k}$.

To conclude this section, let us point out that although we will prove that Theorem 1.3.6 is true for both ${\mathbb{Z}_k}^G$ and ${\mathbb{F}_q}^G$, we will see in Section 1.5 and Section 1.7 that the proofs differ. It may be relevant to try to unify these proofs but we didn't work it out yet.

[6]Since $\mathbb{Z}_q$ is a finite ring, it is an integral domain if and only if it is a field.




(a) $G_1$ (b) $G_2$

Figure 1.8: The colorings of $G_1$ and $G_2$ cannot be extended as 4-colorings

## 1.5 Nullstellensatz certificates

In this section, we introduce the notion of Nullstellensatz certificate of non $k$-colorability and explain the link with edge-clique certificates in power graphs. We recall here Hilbert's Nullstellensatz theorem.

**Theorem 1.5.1** (Nullstellensatz)**.** Let $n \geq 1$ and $\ell \geq 1$ be integers, $\mathbb{K}$ be an algebraically closed field and $P_1, \ldots, P_\ell \in \mathbb{K}[X_1, \ldots, X_n]$. The following points are equivalent:

i) $\forall x \in \mathbb{K} \quad \exists i \in [\![ 1 \ ; \ \ell ]\!] \quad P_i(x) \neq 0$

ii) $\exists Q_1, \ldots, Q_\ell \in \mathbb{K}[X_1, \ldots, X_n] \quad \sum_{i=1}^{\ell} Q_i P_i = 1$

*Remark.* In other words, the polynomials $P_1, \ldots, P_\ell$ have a common root in $\mathbb{K}$ if and only if the ideal generated by $P_1, \ldots, P_\ell$ is not $\mathbb{K}[X_1, \ldots, X_n]$.

In the following, $\mathbb{K}$ is a field assumed to be algebraically closed. In particular, $\mathbb{K}$ has $k^{\text{th}}$ roots of unity for any $k \geq 1$. Namely, one can think of $\mathbb{K}$ as being the field of complex numbers $\mathbb{C}$.

### 1.5.1 The $k$-coloring ideal

Given a graph $G$ and an integer $k \geq 2$, we want to express the problem of the $k$-colorability of $G$ using polynomial equations. There are many ways to do it like in [5], [21], [12] or [6]. The method we use is inspired from [13] and [6]. We assume the vertices of $G$ to be integers between 1 and $n$. We use the following polynomials[7] for every $i \in V$ and every $ij \in E$:

[7] It is a slightly different formulation than Bayer's (see [5]).

$$P_i = {X_i}^k - 1$$
$$P_{ij} = X_i \frac{{X_i}^k - {X_j}^k}{X_i - X_j}$$

Observe that $P_{ij}$ is indeed a polynomial since

$$P_{ij} = X_i \sum_{\ell=0}^{k-1} {X_i}^{k-1-\ell} {X_j}^{\ell} = {X_i}^k + {X_i}^{k-1} X_j + \cdots + {X_i}^2 {X_j}^{k-2} + X_i {X_j}^{k-1}$$

Moreover, it is a sum of monomials of degree $k$ in $\mathbb{K}[X_1, \ldots, X_n]$.

Let us denote by $S$ the following system of equations:

$$S = \{P_i = 0\}_{i \in V} \cup \{P_{ij} = 0\}_{ij \in E}$$

We define as in [13] the *$k$-coloring ideal of $G$*, denoted by $\mathcal{I}_k(G)$, to be the ideal generated by the $P_i$'s and $P_{ij}$'s. We will see, provided that the characteristic of $\mathbb{K}$ does not divide $k$, that this algebraic structure captures the $k$-colorability problem on $G$.

**Theorem 1.5.2** (Bayer [5])**.** Let $\mathbb{K}$ be an algebraically closed field of characteristic not dividing $k$. We assume that $\mathbb{K}$ has $k$ roots of unity. For any graph $G$, $G$ is not $k$-colorable if and only if

$$\mathcal{I}_k(G) = \mathbb{K}[X_1, \ldots, X_n]$$

Although this proof is not new (see [5]), we found relevant to do it here.

*Proof.* First, notice that by Hilbert's Nullstellensatz, $\mathcal{I}_k(G) = \mathbb{K}[X_1, \ldots, X_n]$ if and only if $S$ has no solution (that is, our polynomials do not have a common root).

Let us assume that $G$ is $k$-colorable and consider a proper $k$-coloring of $G$ using the $k^{\text{th}}$ roots of unity for the colors. Let $x_i$ denote the color of vertex $i$. First, by definition, $P_i(x_1, \ldots, x_n) = 0$ for every $i \in [\![ 1 \ ; \ n ]\!]$. Now let $ij \in E$. Since $x_i \neq 0$ for every $i \in [\![ 1 \ ; \ n ]\!]$,

$$P_{ij}(x_1, \ldots, x_n) = x_i \sum_{\ell=0}^{k-1} {x_i}^{k-1-\ell} {x_j}^{\ell} = {x_i}^k \sum_{\ell=0}^{k-1} \left(\frac{x_j}{x_i}\right)^{\ell}$$

so this last sum is zero as $x_i \neq x_j$. Hence, $(x_1, \ldots, x_n)$ is a solution of $S$.

Conversely, assume that $(x_1, \ldots, x_n)$ is a solution of $S$. Let us show that the coloring that maps vertex $i$ to $x_i$ for every $i \in [\![ 1 \ ; \ n ]\!]$ is a proper coloring of $G$. Notice that for all $i$, $x_i$ is a $k^{\text{th}}$ root of unity as $P_i(x_1, \ldots, x_n) = 0$. Take $ij \in E$ and assume for the sake of contradiction that $x_i = x_j$. Then,

$$P_{ij}(x_1, \ldots, x_n) = {x_i}^k \sum_{\ell=0}^{k-1} \left(\frac{x_j}{x_i}\right)^{\ell} = 1 \times k \cdot 1$$

which is not null because the characteristic of $\mathbb{K}$ does not divide $k$. This contradicts the fact that $(x_1, \ldots, x_n)$ is a solution of $S$. □

Hence, by Hilbert's Nullstellensatz, a graph $G$ is $k$-colorable if and only if the associated polynomials $P_i$'s and $P_{ij}$'s have a common root in $\mathbb{K}^n$ and any such root provides a proper coloring for $G$.

**Example.** We can encode the 2-colorability problem of $K_3$ with the following polynomials:

$$P_1 := {X_1}^2 - 1 \qquad P_2 := {X_2}^2 - 1 \qquad P_3 := {X_3}^2 - 1$$
$$P_{1,2} := {X_1}^2 + X_1X_2 \quad P_{2,3} := {X_2}^2 + X_2X_3 \quad P_{3,1} := {X_3}^2 + X_1X_3$$

Here is a Nullstellensatz certificate for this system:

$$Q_1 = 0 \qquad Q_2 = 0 \qquad Q_3 = -{X_3}^2 - 1$$
$$Q_{1,2} = {X_3}^2 + \frac{X_2X_3}{2} \qquad Q_{2,3} = \frac{{X_3}^2}{2}$$
$$Q_{3,1} = {X_3}^2 - \frac{X_2X_3}{2} - X_1X_3 - \frac{X_1X_2}{2} - \frac{{X_2}^2}{2}$$

### 1.5.2 Nullstellensatz and edge-clique certificates

We now explain the link between Nullstellensatz certificates and edge-clique certificates in a power graph. Let $\mathcal{R} := \mathbb{K}[X_1, \ldots, X_n]$. The next definition is derived from [13]. Define the system of equations $S' := \{P_{ij} = 0\}_{ij \in E}$ over the ring

$$\mathcal{R}' := \frac{\mathbb{K}[X_1, \ldots, X_n]}{\left\langle {X_1}^k - 1, \ldots, {X_n}^k - 1 \right\rangle}$$

*Remark.* Observe that, intuitively, $\mathcal{R}'$ is nothing but $\mathcal{R}$ where every exponent are taken modulo $k$.

**Definition 1.5.3** (Nullstellensatz certificate in $\mathcal{R}$)**.** Let $G$ be a non $k$-colorable graph. We call *Nullstellensatz certificate of non $k$-colorability for $G$ in $\mathcal{R}$* any set of polynomials $\{Q_i\}_{i \in V} \cup \{Q_{ij}\}_{ij \in E}$ such that

$$\sum_{i \in V} Q_i \, P_i + \sum_{ij \in E} Q_{ij} \, P_{ij} = 1$$

where the polynomials $P_i$ and $P_{ij}$ are the elements of $S$ defined above.

**Definition 1.5.4** (Nullstellensatz certificate in $\mathcal{R}'$)**.** Let $G$ be a non $k$-colorable graph. We call *Nullstellensatz certificate of non $k$-colorability for $G$ in $\mathcal{R}'$* any set of polynomials $\{Q_{ij}\}_{ij \in E}$ such that

$$\sum_{ij \in E} Q_{ij} \, P_{ij} = 1$$

where the polynomials $P_{ij}$ are the elements of $S'$ defined above.

*Remark.* If $S$ (resp $S'$) has a solution, then $G$ has no Nullstellensatz certificate in $\mathcal{R}$ (resp in $\mathcal{R}'$).

We will see that the existence of a Nullstellensatz certificate of non $k$-colorability for $G$ in $\mathcal{R}$ or in $\mathcal{R}'$ is equivalent to $\chi(G) > k$. In the following, the *degree* of a Nullstellensatz certificate is the maximum degree of all the monomials involved in the $Q_i$'s and $Q_{i,j}$'s.

*Warning.* Since $\mathcal{R}'$ is not $\mathbb{K}[X_1, \ldots, X_n]$, Hilbert's Nullstellensatz theorem does not apply. However, we still call for convenience *Nullstellensatz certificate* any set of elements $Q_{ij} \in \mathcal{R}'$ such that the equality $\sum_{i,j} Q_{ij}P_{ij} = 1$ holds in $\mathcal{R}'$.

Recall that $S = \{P_i = 0\}_{i \in V} \cup \{P_{ij} = 0\}_{ij \in E}$ and $S' = \{P_{ij} = 0\}_{ij \in E}$. The system of equations $S'$ is equivalent to $S$ in the sense of the next proposition.

**Proposition 1.5.5.** The system $S$ has a solution over $\mathcal{R}$ if and only if $S'$ has a solution over $\mathcal{R}'$. Moreover, $S$ has a Nullstellensatz certificate if and only if $S'$ has one.

*Proof.* Observe that any solution of $S$ is a solution of $S'$. Moreover, if $S$ has a Nullstellensatz certificate over $\mathcal{R}$ then, mapping this certificate to $\mathcal{R}'$ gives a certificate for $S'$ in $\mathcal{R}'$. Indeed, this is true because there is a ring homomorphism from $\mathcal{R}$ to $\mathcal{R}'$ that sends every $P_i$'s to zero.

Now assume that $S'$ has a Nullstellensatz certificate. This implies in particular that $S'$ has no solution over ${\mathbb{U}_k}^n$. Hence, $S$ cannot have a solution over $\mathbb{C}^n$ since any solution of $S$ over $\mathbb{C}^n$ would actually be a solution over ${\mathbb{U}_k}^n$. So, by Hilbert's Nullstellensatz, $S$ has a Nullstellensatz certificate.

Finally, if $S'$ has a solution over $\mathcal{R}'$ then it does not have any Nullstellensatz certificate so neither do $S$. Hence, by Hilbert's Nullstellensatz, $S$ has a solution. □

*Remark.* We can easily compute a Nullstellensatz certificate for $S'$ if we are provided one for $S$. Indeed, there is a natural ring homomorphism $\psi : \mathcal{R} \to \mathcal{R}'$ defined by

$$\forall i_1, \ldots, i_n \in [\![ 0 \,;\, n-1 ]\!] \quad \forall j \in \mathbb{N} \qquad \psi\left({X_i}^j\right) = {X_i}^{j\%k}$$

However, it is not clear how to translate a Nullstellensatz certificate for $S'$ into one for $S$: the proof of Proposition 1.5.5 gives no clue on how to do so.

In the following, we only consider a Nullstellensatz certificate of non $k$-colorability for a graph $G$ in $\mathcal{R}'$. We now show that such a certificate and an edge-clique certificate in ${\mathbb{Z}_k}^G$ are somehow isomorphic.

**Proposition 1.5.6.** For any integer $k \geq 2$, $G$ is non $k$-colorable if and only if ${\mathbb{Z}_k}^G$ has an edge-clique certificate.

*Proof.* Observe that in $\mathcal{R}'$, all the exponents are between 0 and $k-1$. Hence, the monomials that can be involved are the elements of the set

$$\mathscr{M} := \left\{ {X_1}^{i_1} \cdots {X_n}^{i_n} : i_1, \ldots, i_n \in [\![ 0 \,;\, k-1 ]\!] \right\}$$

Assume that $G$ has a Nullstellensatz certificate $\{Q_{ij}\}_{ij \in E}$. For all $ij \in E$, write

$$Q_{ij} = \sum_{M \in \mathscr{M}} \alpha_M^{(ij)} \cdot M$$

We have that

$$\sum_{ij \in E} Q_{ij}P_{ij} = \sum_{M \in \mathscr{M}} \sum_{ij \in E} \alpha_M^{(ij)} \cdot MP_{ij} = 1$$

Let us show that $MP_{ij}$ can be seen as an edge-clique in ${\mathbb{Z}_k}^G$. Define

$$\phi : \begin{cases} \mathscr{M} & \to & {\mathbb{Z}_k}^V \\ {X_1}^{i_1} \cdots {X_n}^{i_n} & \mapsto & (i_1, \ldots, i_n) \end{cases}$$

This is a group isomorphism. Observe that in $\mathcal{R}'$,

$$MP_{ij} = M + M{X_i}^{k-1}X_j + M{X_i}^{k-2}{X_j}^2 + \cdots MX_i{X_j}^{k-1}$$

If we apply $\phi$ to every term of this sum, we have every point of the edge clique containing $\phi(M)$ in the direction of the edge $ij$. We will write $(\phi(M), ij)$ to designate such edge-clique. If $G$ has a Nullstellensatz certificate, then ${\mathbb{Z}_k}^G$ has an edge-clique certificate. Indeed, for every edge clique $(\phi(M), ij)$ we can take the weight $\alpha_M^{(ij)}$. Thanks, to the equality

$$\sum_{ij \in E} Q_{ij}P_{ij} = \sum_{M \in \mathscr{M}} \sum_{ij \in E} \alpha_M^{(ij)} \cdot MP_{ij} = 1 = \phi^{-1}(0, \cdots, 0)$$

the function that maps $(\phi(M), ij)$ to $\alpha_M^{(ij)}$ is an edge-clique certificate whose center is $(0, \ldots, 0)$.

Conversely, let $f$ be an edge-clique certificate. Up to translating, we can assume it's center to be $(0, \ldots, 0)$. We write $f(x, ij)$ for the weight of the unique edge-clique directed by $ij$ and containing $x$. Define for every $ij \in E$

$$Q_{ij} := \sum_{M \in \mathscr{M}} f\left(\phi(M), ij\right)\, M$$

and let us check that $\{Q_{ij}\}_{ij \in E}$ is a Nullstellensatz certificate.

$$\begin{aligned} \sum_{ij \in E} Q_{ij}P_{ij} &= \sum_{ij \in E} \sum_{M \in \mathscr{M}} f\left(\phi(M), ij\right)\, M\, P_{ij} \\ &= \sum_{M \in \mathscr{M}} \sum_{ij \in E} f\left(\phi(M), ij\right) \sum_{\ell=0}^{k-1} M\, {X_i}^{k-\ell}\, {X_j}^{\ell} \end{aligned}$$

For every $M \in \mathcal{M}$ and every $ij \in E$, let us define

$$M_{ij} = \left\{ M' \in \mathscr{M} \colon \exists \ell \in [\![ 0\ ;\ k-1 ]\!] \quad M = M'\, {X_i}^{k-\ell}\, {X_j}^{\ell} \right\}$$

We then have that $\displaystyle\sum_{ij \in E} Q_{ij}P_{ij} = \sum_{M \in \mathscr{M}} \sum_{ij \in E} \sum_{M' \in M_{ij}} f\left(\phi(M'), ij\right)\, M$

Indeed, $f\left(\phi\left(M'\, {X_i}^{k-\ell}\, {X_j}^{\ell}\right), ij\right) = f\left(\phi(M'), ij\right)$. Hence, the coefficient of a monomial $M$ in the sum $\displaystyle\sum_{ij \in E} Q_{ij}P_{ij}$ is the sum of all $f(x, ij)$ where $(x, ij)$ is an edge-clique containing $\phi(M)$. This implies that the coefficient in front of $M$ is always zero except when $M = 1$. □

This concludes the proof of Theorem 1.3.6 in the particular case of $\Gamma_k$ being $\mathbb{Z}_k$. We prove in the next two sections the case where $\Gamma_k$ is a finite field.

One can wonder why this proof does not apply to $\mathbb{F}_k$. Actually, the function $\phi$ cannot be defined anymore as the exponents of a monomial naturaly map to $\mathbb{Z}_k$ but not to $\mathbb{F}_k$. Surprisingly, the result of Theorem 1.3.6 is still true for $\Gamma_k$ being $\mathbb{F}_k$ but our proof is completely different. We do not know any natural way to turn an edge-clique certificate for ${\mathbb{F}_k}^G$ into a Nullstellensatz certificate neither we do for the converse. Intuitively, we would have to consider polynomials whose exponents take values in $\mathbb{F}_k$ rather than in $\mathbb{Z}_k$. Obviously, there is no analogous theorem to Hilbert's Nullstellensatz in such context.

## 1.6 A general geometry result

In order to prove Theorem 1.3.6 in the case where $\Gamma_k$ is a finite field, we cannot use polynomials and Nullstellensatz anymore. Indeed, when $k = p^\ell$ with $p$ a prime number and $\ell \geq 2$, $\mathbb{F}_{p^\ell}$ and $\mathbb{Z}_{p^\ell}$ are different objects (the characteristic of $\mathbb{Z}_{p^\ell}$ is $p^\ell$ whereas $\mathbb{F}_{p^\ell}$ has characteristic $p$) and powers of monomials do not translate naturally into $\mathbb{F}_k$. However, power graphs of the form ${\mathbb{F}_k}^G$ have, in some sense, more structure than these of the form ${\mathbb{Z}_k}^G$. The set of vertices of the former is a linear space (over $\mathbb{F}_k$) whereas the later has a weaker structure of module (over $\mathbb{Z}_k$). Hence, we can have a geometric interpretation of ${\mathbb{F}_k}^G$. The edge-cliques can be seen as lines. Finding an edge-clique certificate in ${\mathbb{F}_k}^G$ amounts to find a set of weighted lines in ${\mathbb{F}_k}^n$ with some properties. The edge-cliques are mapped to lines but not every line is mapped to an edge-clique. This is why some of the lines of ${\mathbb{F}_k}^n$ will be "forbidden".

In this section we characterize the set of directions $\mathcal{D}$ of an affine space over a finite field such that the affine lines of direction in $\mathcal{D}$ span the space. In other words, the incidence matrix of the points of the space versus the affine lines of direction in $\mathcal{D}$ has full column rank. This result will be useful to study the certificate of non $q$-colorability for ${\mathbb{F}_q}^G$ in Section 1.7. Indeed, the "authorized" directions will be those corresponding the edge-cliques.

For all this section, we fix a prime number $p$, $\ell \geq 1$ and $r \geq 2$ two positive integers and we let $q = p^\ell$.

**Definition 1.6.1** (d-line)**.** Let $\Gamma$ be a ring and $E$ a module on $\Gamma$. For $x, d \in \Gamma^E$, we call *d-line* a set of the form $L_x(d) = \{x + \lambda\, d \colon \lambda \in \Gamma\}$. We say that $L_x(d)$ is a *non trivial affine line* whenever $d \neq 0$.

**Lemma 1.6.2.** Let $E$ be an affine space over the finite field $\mathbb{F}_q$ of dimension 2 with $q = p^\ell$ where $p$ a prime number and $\ell \geq 1$. For every field $\mathbb{K}$ of characteristic $\xi \neq p$, the non trivial affine lines of $E$ are full rank in $\mathbb{K}$. More precisely, the matrix of $E$ versus the non trivial affine lines has full column rank in $\mathbb{K}$.

*Proof.* Let $M$ be the incidence matrix of the elements of $E$ (called "points") versus the non trivial affine lines. More formally, we consider an enumeration $\{x_1, \ldots, x_r\}$ of the points and an enumeration of the non trivial affine lines $\{\ell_1, \ldots, \ell_s\}$ and we define $M = (m_{ij}) \in \mathscr{M}_{r,s}(\mathbb{K})$ by

$$\forall i \in [\![ 1 \,;\, r ]\!] \quad \forall j \in [\![ 1 \,;\, s ]\!] \qquad m_{ij} = \begin{cases} 1 & \text{if} \quad x_i \in \ell_j \\ 0 & \text{otherwise} \end{cases}$$

We will show that $M$ has rank $r$. If we sum all the columns corresponding to some partition of the space into lines[8], we get that ${}^{\mathrm{t}}\begin{bmatrix} 1 & \cdots & 1 \end{bmatrix} \in \mathbb{K}^r$. Now consider a point $x_i \in E$. Without loss of generality, we can assume that $i = 1$. If we sum every columns of $M$ corresponding to a line containing $x_1$, we obtain, since $r = q^2$,

$${}^{\mathrm{t}}\begin{bmatrix} \dfrac{r-1}{q-1} & 1 & \cdots & 1 \end{bmatrix} = {}^{\mathrm{t}}\begin{bmatrix} q+1 & 1 & \cdots & 1 \end{bmatrix}$$

[8]For instance, since $E$ is a plane, one can consider all the "horizontal" lines. Actually, given a direction, the lines with that directions form a partition of $E$.

So, $${}^{\mathrm{t}}\begin{bmatrix} q+1 & 1 & \cdots & 1 \end{bmatrix} - {}^{\mathrm{t}}\begin{bmatrix} 1 & \cdots & 1 \end{bmatrix} = {}^{\mathrm{t}}\begin{bmatrix} q & 0 & \cdots & 0 \end{bmatrix}$$
Then, since $\xi \neq p$, this last vector is non zero. We can do this for every point which proves that $M$ has full column rank hence $\operatorname{rk} M = r$. □

We will now see how this result can be generalized. First, let us prove a useful corollary:

**Corollary 1.6.3.** If a function $S : E \to \mathbb{K}$ sums to zero on every non trivial line of $E$ then $S = 0$.

*Proof.* If we see $S$ as a row of size $r$ then, by hypothesis, $S\,M = 0$. By Lemma 1.6.2, $M$ has rank $r$ hence ${}^{\mathrm{t}}M$ is injective so $S = 0$. □

We consider a set $\mathcal{D} \subseteq {\mathbb{F}_q}^n \setminus \{0\}$. The underlying idea is that $\mathcal{D}$ represents the allowed directions of the affine space ${\mathbb{F}_q}^n$. We denote by $\mathcal{A}(\mathcal{D})$ the incidence matrix of ${\mathbb{F}_q}^n$ versus the affine lines of ${\mathbb{F}_q}^n$ directed by an element of $\mathcal{D}$.

**Lemma 1.6.4.** Let $\mathbb{K}$ be a field of characteristic $\xi$ with $\xi \neq p$. $\mathcal{A}(\mathcal{D})$ has full column rank in $\mathbb{K}$ if and only if, for every hyperplane $H$ of ${\mathbb{F}_q}^n$, $H \cap \mathcal{D} \neq \varnothing$.

*Proof.* Assume that there exists a hyperplane $H$ of ${\mathbb{F}_q}^n$ such that $H \cap \mathcal{D} = \varnothing$. By Corollary A.1.10, $H = \operatorname{Ker} \langle c, \bullet \rangle$ for some $c \in {\mathbb{F}_q}^n$.

*Remark.* This is not the Riesz representation theorem! Indeed, the linear space are not real or complex but on the finite field $\mathbb{F}_q$. Although the result is similar, the proof differ in particular because $\xi$ may be equal to 2 (see Lemma A.1.8 and Proposition A.1.6).

Now consider a $d$-line $L_x(d)$ for some $x \in {\mathbb{F}_q}^n$ and $d \in \mathcal{D}$. Since $\langle c, d \rangle \neq 0$, we have that
$$\forall u, v \in L_x(d) \qquad u \neq v \Rightarrow \langle c, u \rangle \neq \langle c, v \rangle$$
Indeed, if $u, v \in L_x(d)$ with $u \neq v$, then we can write $u = v + \lambda\, d$ with $\lambda \neq 0$. Hence, $\langle c, u \rangle = \langle c, v \rangle + \lambda \langle c, d \rangle$ and since $\lambda \neq 0$ and $\langle c, d \rangle \neq 0$, we must[9] have that $\langle c, u \rangle \neq \langle c, v \rangle$. Define for every $\lambda \in \mathbb{F}_q$ and every $c \in {\mathbb{F}_q}^n$,
$$I_c(\lambda) := \{x \in {\mathbb{F}_q}^n \colon \langle c, x \rangle = \lambda\}$$
and let us consider, for a fixed $c \in {\mathbb{F}_q}^n$, the $q$-partition of ${\mathbb{F}_q}^n$ given by $\{I_c(\lambda) \colon \lambda \in \mathbb{F}_q\}$. Observe that for every $d \in \mathcal{D}$, a $d$-line has exactly one point in each[10] $I_c(\lambda)$. Hence, any linear combination of the columns of $\mathcal{A}(\mathcal{D})$ has the same sum on each $I_c(\lambda)$. So $\mathcal{A}(\mathcal{D})$ has not full column rank.

*Remark.* This is the same argument that we used in 1.2.2.

Now, if $A(\mathcal{D})$ has not full column rank, then, by Corollary A.1.15, there exists a non zero function $S : {\mathbb{F}_q}^n \to \mathbb{K}$ such that $S$ sums to zero on every $d$-line for $d \in \mathcal{D}$ (that is, if one sees $S$ as a row matrix, $S\,\mathcal{A}(\mathcal{D}) = 0$). Our goal is to find some vector $c \in {\mathbb{F}_q}^n$ such that $\langle c, d \rangle \neq 0$ for every $d \in \mathcal{D}$. To do so, let us divide the elements of ${\mathbb{F}_q}^n$ into three types:

[9] Observe that we use here the fact that ${\mathbb{F}_q}^n$ is an integral domain... This would not be true on any ring!
[10] This is because the map from $\mathbb{F}_q$ to $\mathbb{F}_q$ defined by $\lambda \mapsto \langle c, x \rangle + \lambda \langle c, d \rangle$ is injective.

- the set $S_2$ of $x$ (called *type* 2 *elements*) for which $S$ sums to zero on every $x$-line:

$$S_2 = \left\{ x \in {\mathbb{F}_q}^n \setminus \{0\} \colon \forall c \in {\mathbb{F}_q}^r \quad \sum_{\lambda \in \mathbb{F}_q} S(c + \lambda\, x) = 0 \right\}$$

- the set $S_3$ of $x$ (called *type* 3 *elements*) such that $S$ is constant on every $x$-line:

$$S_3 = \{ x \in {\mathbb{F}_q}^n \colon \forall c \in {\mathbb{F}_q}^r \, \forall \lambda \in \mathbb{F}_q \quad S(c + \lambda\, x) = S(c) \}$$

- the set $S_1$ of every others (called *type* 1 *elements*):

$$S_1 = {\mathbb{F}_q}^n \setminus (S_2 \cup S_3)$$

First, we show that if $S_2 \cap S_3 \neq \varnothing$ then $S = 0$. Indeed, consider $x \in S_2 \cap S_3$ and observe that for every $c \in {\mathbb{F}_q}^n$,

$$0 = \sum_{\lambda \in \mathbb{F}_q} S(c + \lambda x) = q S(c)$$

so $S(c) = 0$ since $\xi$ does not divide $q$. Moreover, observe that $S_3$ is a linear subspace of ${\mathbb{F}_q}^n$. Indeed, $S_3 \subseteq {\mathbb{F}_q}^n$, $0 \in S_3$ and if $x, y \in S_3$, $\lambda \in \mathbb{F}_q$, then for every $c \in {\mathbb{F}_q}^n$ and every $\mu \in \mathbb{F}_q$,

$$\begin{aligned} S\left(c + \mu\ (\lambda\, x + y)\right) &= S(c + \mu\, \lambda\, x + \mu\, y) \\ &= S(c + \mu\, \lambda x) && \text{(since } y \in S_3\text{)} \\ &= S(c) && \text{(since } x \in S_3\text{)} \end{aligned}$$

Hence, $S_3$ is a linear subspace of ${\mathbb{F}_q}^n$. Finally, observe that what we just did is true for every function $S : {\mathbb{F}_q}^n \to \mathbb{K}$ such that $S\mathcal{A}(\mathcal{D}) = 0$.

Observe that Corollary A.1.15 does not explicitly gives a function $S$ nor that it says how many such functions exists. For our proof, we would like that $S_1 = \varnothing$. The idea is, starting from any function $S$ provided by Corollary A.1.15 (that is, such that $S\,\mathcal{A}(\mathcal{D}) = 0$), we can define a new function $S'$ satisfying $S'\,\mathcal{A}(\mathcal{D}) = 0$ and such that ${S'}_1 = \varnothing$. More precisely, we will now describe an algorithm to make every element of type 1 becoming an element of type 3. Let us define, $S^{(0)} = S$ and for every $i \in \mathbb{N}$, if ${S^{(i)}}_1$ (the set of elements of type 1 of the function $S^{(i)}$) is non empty then pick $x_i \in {S^{(i)}}_1$ and define $S^{(i+1)}$ by

$$\forall y \in {\mathbb{F}_q}^n \quad S^{(i+1)}(y) = \sum_{\lambda \in \mathbb{F}_q} S^{(i)}(y + \lambda\, x_i)$$

otherwise, let $S^{(i+1)} = S^{(i)}$. The idea is to take an element of type 1 for $S^{(i)}$ and to make it becoming of type 3 by taking the "average" over each $x_i$-line.

*Remark.* Of course, this procedure depends on the choice of $x_i$. However, the only thing that matters is that it ends with a function $S^{(i_0)}$ satisfying ${S^{(i_0)}}_1 = \varnothing$. This is shown by the following Claim.

**Claim 1.6.5.** There exists $i_0 \in \mathbb{N}$ such that

- ${\mathbb{F}_q}^n = {S^{(i_0)}}_2 \cup {S^{(i_0)}}_3$
- $S^{(i_0)} \neq 0$
- ${S^{(i_0)}}_3$ is a hyperplane

*Proof.* First, notice that for every $i \in \mathbb{N}$, if $x_i$ exists (which means ${S^{(i)}}_1 \neq \varnothing$), then $x_n \in {S^{(i+1)}}_3$. Indeed, let $c \in {\mathbb{F}_q}^n$, $\lambda \in \mathbb{F}_q$ and observe that

$$S^{(i+1)}(c + \lambda\, x_i) = \sum_{\mu \in \mathbb{F}_q} S^{(i)}(c + \lambda\, x_i + \mu\, x_i) = \sum_{\mu \in \mathbb{F}_q} S^{(i)}(c + \mu\, x_i) = S^{(i+1)}(c)$$

Second, if $y \in {S^{(i)}}_2$ then $y \in {S^{(i+1)}}_2$. Indeed, if $S^{(i+1)} = S^{(i)}$ there is nothing to do and if not, let $c \in {\mathbb{F}_q}^n$,

$$\begin{aligned}
\sum_{\lambda \in \mathbb{F}_q} S^{(i+1)}(c + \lambda\, y) &= \sum_{\lambda \in \mathbb{F}_q} \sum_{\mu \in \mathbb{F}_q} S^{(i)}(c + \lambda\, y + \mu x_i) \\
&= \sum_{\mu \in \mathbb{F}_q} \sum_{\lambda \in \mathbb{F}_q} S^{(i)}(c + \mu\, x_i + \lambda\, y) && (\mathbb{F}_q \text{ is finite}) \\
&= \sum_{\mu \in \mathbb{F}_q} 0 && (y \text{ has type 2}) \\
\sum_{\lambda \in \mathbb{F}_q} S^{(i+1)}(c + \lambda\, y) &= 0
\end{aligned}$$

Finally, if $y \in {S^{(i)}}_3$ then $y \in {S^{(i+1)}}_3$. Indeed, if $S^{(i+1)} = S^{(i)}$ there is nothing to do and if not, let $c \in {\mathbb{F}_q}^n$ and $\lambda \in \mathbb{F}_q$,

$$\begin{aligned}
S^{(i+1)}(c + \lambda\, y) &= \sum_{\mu \in \mathbb{F}_q} S^{(i)}(c + \lambda\, y + \mu\, x_i) \\
&= \sum_{\mu \in \mathbb{F}_q} S^{(i)}(c + \mu\, x_i) && (\text{since } y \in {S^{(i)}}_3) \\
&= S^{(i+1)}(c)
\end{aligned}$$

Hence, our procedure can only make the number of type 1 elements decrease. Since there is a finite number of such elements, this procedure terminates. Let $i_0$ be the smallest integer such that $S^{(i_0)} = S^{(i_0+1)}$. Notice that this $i_0$ may depends on the choice we made for the $x_i$'s.

Let us show that if $S \neq 0$ then $S^{(i_0)} \neq 0$. Assume for the sake of contradiction that it is not the case, then $i_0 \geq 1$ and we have that

$$\forall c \in {\mathbb{F}_q}^n \qquad \sum_{\lambda \in \mathbb{F}_q} S^{(i_0-1)}(c + \lambda\, x_{i_0-1}) = 0$$

Then, every $x_{i_0-1}$-line sums to zero for $S^{(i_0-1)}$ which means that $x_{i_0-1} \in {S^{(i_0-1)}}_2$ which is a contradiction since ${S^{(i_0-1)}}_2 \cap {S^{(i_0-1)}}_1 = \varnothing$.

Let us now show that ${S^{(i_0)}}_3$ is a hyperplane. Consider $x \in {S^{(i_0)}}_2$. As $x \neq 0$, it suffices to prove that ${\mathbb{F}_q}^n = {S^{(i_0)}}_3 \oplus \mathbb{F}_q x$ (see Def 0.0.25). First, observe that ${S^{(i_0)}}_3 \cap {S^{(i_0)}}_2 = \varnothing$ since $S^{(i_0)} \neq 0$. Second, we show that ${\mathbb{F}_q}^n = {S^{(i_0)}}_3 + \mathbb{F}_q x$. Consider $y \in {\mathbb{F}_q}^n$. If $y \in \mathbb{F}_q x$ or if $y \in {S^{(i_0)}}_3$ then there is nothing to do. If not, take $c \in {\mathbb{F}_q}^n$ such that $S^{(i_0)}(c) \neq 0$ and define

$$P = \{c + a\, x + b\, y \,:\, a, b \in \mathbb{F}_q\}$$

The affine space $P$ has dimension 2 because $y \notin \mathbb{F}_q x$ and $x \neq 0$. Moreover, $S^{(i_0)}$ is not zero on the plane $P$. So, according to Corollary 1.6.3, there exists a non trivial line of this plane on which $S^{(i_0)}$ does not sum to zero. Let $c' + \mathbb{F}_q\,(a\, x + b\, y)$ be such a line. It must be that $a\, x + b\, y \in {S^{(i_0)}}_3$ as we have ${S^{(i_0)}}_1 = \varnothing$. Observe that $b \neq 0$ since otherwise we would have $a\, x \in {S^{(i_0)}}_3$ and because it is a linear subspace, $x \in {S^{(i_0)}}_3$ (since $a \neq 0$) which is not the case.

Hence, $$y \in \frac{-a}{b}\, x + {S^{(i_0)}}_3$$

□

Finally, observe that the hyperplane ${S^{(i_0)}}_3$ does not contain any element of $\mathcal{D}$ because $\mathcal{D} \subseteq {S^{(0)}}_2$ and the procedure cannot make element of type 2 becoming of type 3. This concludes the proof of Lemma 1.6.4. □

## 1.7 The case of ${\mathbb{F}_q}^G$

In this Section, we conclude the proof of Theorem 1.3.6 by dealing with the special case of $\Gamma_k$ being a finite field of cardinality not a prime number. We already know by Theorem 1.4.1 that $G$ is $q$-colorable if and only if ${\mathbb{F}_q}^G$ is $q$-colorable. We will prove that, as for ${\mathbb{Z}_k}^G$, there exists an edge-clique certificate in ${\mathbb{F}_q}^G$ if and only if $G$ is not $q$-colorable. However this time, such an edge-clique certificate will not translate nicely into a Nullstellensatz certificate. Indeed, we would need to allow exponents in $\mathbb{F}_q$ for our polynomials and so to define other addition and multiplication laws on polynomials. In such context, we do not know if Hilbert's Nullstellensatz theorem holds in general. Although this would be an interesting question to investigate, in particular if one wants to come up with a simpler proof for Theorem 1.3.6, the study of ${\mathbb{F}_q}^G$ remains relevant since opposite to ${\mathbb{Z}_k}^G$ with $k$ not prime, the absence of an edge-clique certificate implies that ${\mathbb{F}_q}^G$ is $q$-colorable (see Prop 1.4.5).

**Theorem 1.7.1.** Let $q = p^\ell$ where $p$ is a prime number and $\ell \geq 1$ is an integer. Let $G$ be a graph and $\mathbb{K}$ a field of characteristic $\xi \neq p$. We have that $G$ is not $q$-colorable if and only if its power graph ${\mathbb{F}_q}^G$ has an edge-clique certificate in $\mathbb{K}$.

*Proof.* We will show that, opposite to graphs in general, if ${\mathbb{F}_q}^G$ is not $q$-colorable, then it has an edge-clique certificate. Let $G$ be a connected graph with at least one edge. The integer $n$ always denotes the number of vertices of $G$. Let us consider the set

$$\mathcal{D} = \{\mathbb{1}_u - \mathbb{1}_v \colon uv \in E(G)\}$$

and the matrix $\mathcal{A}(\mathcal{D})$ to be the matrix of ${\mathbb{F}_q}^V$ versus the edge-cliques of ${\mathbb{F}_q}^G$. This is exactly the matrix of the points of ${\mathbb{F}_q}^n$ versus the $d$-lines, with $d \in \mathcal{D}$.

First, if ${\mathbb{F}_q}^G$ has an edge-clique certificate, then $\mathcal{A}(\mathcal{D})$ and so $M_q\left({\mathbb{F}_q}^G\right)$ has full column rank. Hence, we know by Proposition 1.2.2 that ${\mathbb{F}_q}^G$ is not $q$-colorable. So $G$ cannot be $q$-colorable by Lemma 1.4.3.

Conversely, let us assume that ${\mathbb{F}_q}^G$ has no edge-clique certificate. Consider the matrix $\mathcal{A}(\mathcal{D})$ which does not have full column rank since we assume that ${\mathbb{F}_q}^G$ has no edge-clique certificate. So, by Lemma 1.6.4, there exists a hyperplane $H$ of ${\mathbb{F}_q}^n$ such that $H \cap \mathcal{D} = \varnothing$. By Corollary A.1.10, there exists $c \in {\mathbb{F}_q}^n$ such that $H = \operatorname{Ker}\langle c, \bullet\rangle$. For every $uv \in E(G)$, since $u - v \in \mathcal{D}$, we must have that $\langle c, u - v\rangle \neq 0$. So $c$ is a proper coloring of $G$. □

This concludes the proof of Theorem 1.3.6 in the case of $\Gamma_k$ being $\mathbb{F}_q$. Since the case $\Gamma_k = \mathbb{Z}_k$ has been done in Section 1.5, we have proved the Theorem 1.3.6.

This proof can be quite surprising as we didn't explicitly build the coloring $c$. However, this proof is constructive! Indeed, the proof of Proposition A.1.6 is constructive (We can build a basis of ${\mathbb{F}_q}^n$ that is orthogonal for $\langle \bullet, \bullet \rangle$.) as the one of Lemma A.1.8 (provided a basis of ${\mathbb{F}_q}^n$). Moreover, the proof of Lemma A.1.14 is also constructive and we used an algorithm to make every type 1 element becoming element of type 3 in the proof of Lemma 1.6.4. Hence, one just has to compute a basis of ${S^{i_0}}_3$ (like in the proof of Proposition A.1.6) in order to find a vector $c$ such that ${S^{i_0}}_3 = \mathrm{Ker}\, \langle c, \bullet \rangle$. Obviously, this would end in a terrible algorithm to compute a proper coloring of a graph. In particular, although determining kernels can be done in polynomial time, the matrices at stake here ($S$ and $\mathcal{A}(\mathcal{D})$) have a size which is exponential in $n$.

**Corollary 1.7.2.** If the graph ${\mathbb{F}_q}^G$ has an edge-clique certificate with weights in a field of characteristic not $p$, then it has an edge-clique certificate with weights in any field of characteristic not $p$.

*Proof.* Let us assume ${\mathbb{F}_q}^G$ has an edge-clique certificate with weights in a field $\mathbb{K}_1$ of characteristic $\xi_1$ with $\xi_1 \neq p$. By theorem 1.7.1, this implies $G$ is not $q$-colorable. Hence, for any field $\mathbb{K}_2$ of characteristic $\xi_2 \neq p$, there exists an edge-clique certificate for ${\mathbb{F}_q}^G$ in $\mathbb{K}_2$ by theorem 1.7.1. □

*Remark* 1.7.3. Changing the field may give completely different certificates! This means the vertices and edge-cliques involved may not be the same. Actually, there is no edge-clique certificate in $\mathbb{R}$ for ${3^{K_4}}$ on the subgraph composed of the vertices of support less than 3 whereas there is one in $\mathbb{F}_2$. We know this thanks to our program (see E.1).

## 1.8 Some properties of power graphs

In this section, we present some properties of power graphs. We show that surprisingly, there exists no graph $G$ such that $\chi\left(2^G\right) = 3$. Since it is difficult to have a good intuition on these objects, we study small examples (mainly powers of 2). We prove some results on the properties that are transferred from $G$ to ${\Gamma_k}^G$.

### 1.8.1 Basic properties

**Proposition 1.8.1.** If $G$ is connected and non empty, then ${\Gamma_k}^G$ has exactly $k$ connected components.

*Proof.* Let $G$ be a connected and non empty graph. Consider the linear form $\phi : {\Gamma_k}^V \to \Gamma_k$ defined by

$$\forall (x_1, \ldots, x_n) \in {\Gamma_k}^V \qquad \phi(x_i, \ldots, x_n) = \sum_{i=1}^{n} x_i$$

Observe that $\phi$ is constant on a connected component of ${\Gamma_k}^G$. Moreover, since $G$ is non empty, $\phi$ is surjective so ${\Gamma_k}^G$ has at least $k$ connected components.

Moreover, since $G$ is connected, for any $\lambda \in \Gamma_k$, any pair of vertices in $\phi^{-1}(\lambda)$ can be connected with a path in ${\Gamma_k}^G$.

This last point may not be that obvious. First, consider $u, v \in V(G)$. These vertices are naturally mapped into ${\Gamma_k}^G$ (one just has to send $u$ to $\mathbb{1}_u$ as in the proof of Lemma 1.3.2. Since $G$ is connected, there exists a path from $u$ to $v$ in $G$. Let us consider a minimal path in term of distance so that there is no loop. We consider the edges involved following the path and starting from $u$. Namely, we have the edges

$$u_0u_1, \dots, u_{k-1}u_k \in E(G) \qquad \text{with } u_0 = u \text{ and } u_k = v$$

Define for all $i \in [\![ 0 \ ; \ k-1 ]\!]$, $e_i = \mathbb{1}_{u_{i+1}} - \mathbb{1}_{u_i}$ and observe that

$$\mathbb{1}_v = \mathbb{1}_u + \sum_{i=0}^{k-1} e_i$$

Since $e_i \in E\left({\Gamma_k}^G\right)$ for every $i \in [\![ 0 \ ; \ k-1 ]\!]$, this proves that there is a path from $\mathbb{1}_u$ to $\mathbb{1}_v$ in ${\Gamma_k}^G$. Actually, this path naturally translates to a path between $\lambda\mathbb{1}_u$ and $\lambda\mathbb{1}_v$ in the connected component $\phi^{-1}(\lambda)$ whatever is $\lambda$.

*Remark.* This path is nothing but the original path with a translation.

Now, to conclude the proof, let us consider two vertices $x$ and $y$ of the same connected component of ${\Gamma_k}^G$, say, $\phi^{-1}(\lambda)$. Let us see $x$ and $y$ as column vectors of size $n$ and let $i$ be the first[11] index where $x$ and $y$ differ. Since their sum is the same (equal to $\lambda$), there must exists an index $j > i$ such that $x_j \neq y_j$. Since $i$ and $j$ are connected in $G$, and thanks to what we just did, we can "transfer weight". More precisely, there exists a path in ${\Gamma_k}^G$ from $x$ to $x'$ such that $x$ and $x'$ are the same up to index $j-1$ and such that $x'$ and $y$ are the same from index $j$ to the end. By induction, there exists a path from $x$ to $y$ in ${\Gamma_k}^G$. □

Let us see a simple example. One of the most trivial we can do is $2^{K_3}$. It is represented on Figure 1.9. This graph has indeed two connected components and, which may be a bit surprising, each of these components is a $K_4$.

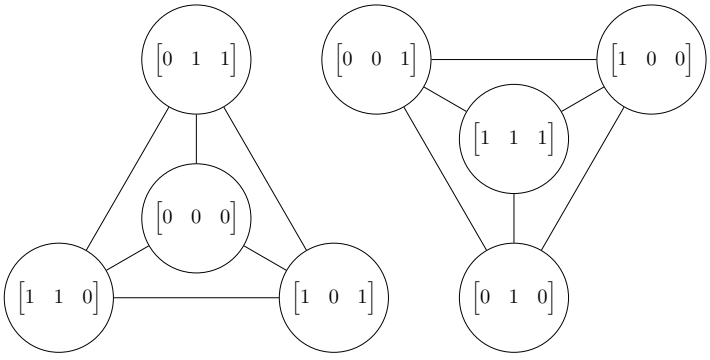



Figure 1.9: The graph ${\mathbb{Z}_2}^{\triangle}$

[11] Up to down or down to up, it does not matter...

*Remark.* When one study the power graphs of the form $2^G$, it is convenient to think of the vertices of $2^G$ as sets of elements of $V$ with the law "+" being the symmetric difference. In such context, it may be convenient to call the symmetric difference "union modulo 2".

Actually, the chromatic number of a graph of the form $2^G$ cannot be 3.

**Theorem 1.8.2.** For any graph $G$, either $2^G$ is bipartite or $\chi\left(2^G\right) \geq 4$.

To prove this theorem, we study the case of $2^C$ where $C$ is an odd cycle. Indeed, a graph is bipartite if and only if it has no odd cycle. Our goal is to find a subgraph of $2^C$ which is not 3-colorable.

Let us define $C$ by

- $V(C) = \{x_0, \ldots, x_{2n}\}$
- For every $i, j \in [\![ 0 \ ; \ 2n ]\!]$, $x_i x_j \in E(C)$ if and only if $i = j+1 \ [2] n+1$ or $j = i+1 \ [2] n+1$.

In what follows, all the indices are taken modulo $2n+1$ and the "+" operation is the symmetric difference[12]. Let us define

- $C^0 = (\{x_i\})_{i \in [\![ 0 \ ; \ 2n ]\!]}$
- $\forall k \in [\![ 1 \ ; \ n ]\!] \qquad C^k = \left(C^{k-1}(i) \Delta \{x_{i-k}, x_{i+k}\}\right)_{i \in [\![ 0 \ ; \ 2n ]\!]}$

We then define $G_n$ by

- $V(G_n) = \{C^k(i) \colon k \in [\![ 0 \ ; \ n ]\!] \quad i \in [\![ 0 \ ; \ 2n ]\!]\}$
- For every $u, v \in V(G_n)$, $uv \in E(G_n)$ if and only if

$$\exists i \in [\![ 0 \ ; \ 2n ]\!] \quad u \Delta v = \{x_i, x_{i+1}\}$$

*Remark.*

- Two vertices are connected in $G_n$ if and only if their symmetric difference is a set of two elements whose indices are consecutive modulo $2n+1$.
- $C^n(0) = \cdots = C^n(2n)$

**Example 1.8.3.** We have that $G_1 = K_4$ and, for $n = 2$, $G_2$ is the famous Grötzsch graph. Drawings of $G_2$ and $G_3$ can be found on Figure 1.10.

[12] This is due to the modulo 2. We have that $\begin{bmatrix} 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \end{bmatrix}$ and similarly, $\{x, y\} \Delta \{y\} = \{x\}$.

**Proposition 1.8.4.** For every $n \geq 1$, $\chi(G_n) = 4$.

*Proof.* The Figure 1.10 may be helpful to understand the following proof. First, we will prove that $\chi(G_n) \leq 4$. To do so, we will build a 4-coloring of $G_n$. Let us start by choosing a 3-coloring $\rho$ of the external odd cycle $\{x_0\}, \ldots, \{x_{2n}\}$. Let us extend $\rho$ this way:

$$\forall k \in [\![ 1 \ ; \ n-1 ]\!] \quad \forall i \in [\![ 0 \ ; \ 2n ]\!] \qquad \rho\left(C^k(i)\right) = \rho\left(C^{k-1}(i)\right)$$

and chose an arbitrary new color for the last vertex. We now check that $\rho$ is a proper 4-coloring of $G_n$.

- First, the external cycle is properly colored by definition.
- The last vertex ($C^n(0) = \cdots = C^n(2n)$) is the only one in its color class hence any edge involving this vertex is properly colored.
- The remaining edges are always between two consecutive levels (between a vertex of $C^k$ and a vertex of $C^{k+1}$). By construction, those vertices are well colored.

Let us now show that $\chi(G_n) > 3$. Assume for the sake of contradiction that there exists a proper 3-coloring $c$ of $G$. Observe that for every color, there exists a vertex of the external cycle with this color whose neighborhood has every other colors. This is because an odd cycle is not 2-colorable. Indeed, the negation of this sentence would allow us to remove one color on the external cycle which cannot be done. Hence, the subgraph induced by $C^1(0), \ldots, C^1(2n)$ has every colors. Observe now that the subgraph induced by $C^1(0), C^2(0), C^1(1), C^2(1), \ldots, C^1(2n), C^2(2n)$ is an even cycle. Moreover, there is a vertex of each color on $C^1(0), \ldots, C^1(2n)$ so, between two distinct colors (say 0 and 1) on level 1, there is an odd number of vertices on this cycle so there must exists a vertex with color 2 in between. Hence, the level 2 ($C^2(0), \ldots, C^2(2n)$) has every colors. By induction, it follows that the level $n-1$ has every colors. Since the last vertex is connected to every vertices of level $n-1$, we need an extra fourth color. □

**Example 1.8.5.** Proper 4-colorings for $G_2$ and $G_3$ can be found on Figure 1.10.

**Lemma 1.8.6.** For any $n \geq 1$, the graph $2^{C_{2n+1}}$ contains $G_n$ as an induced subgraph.

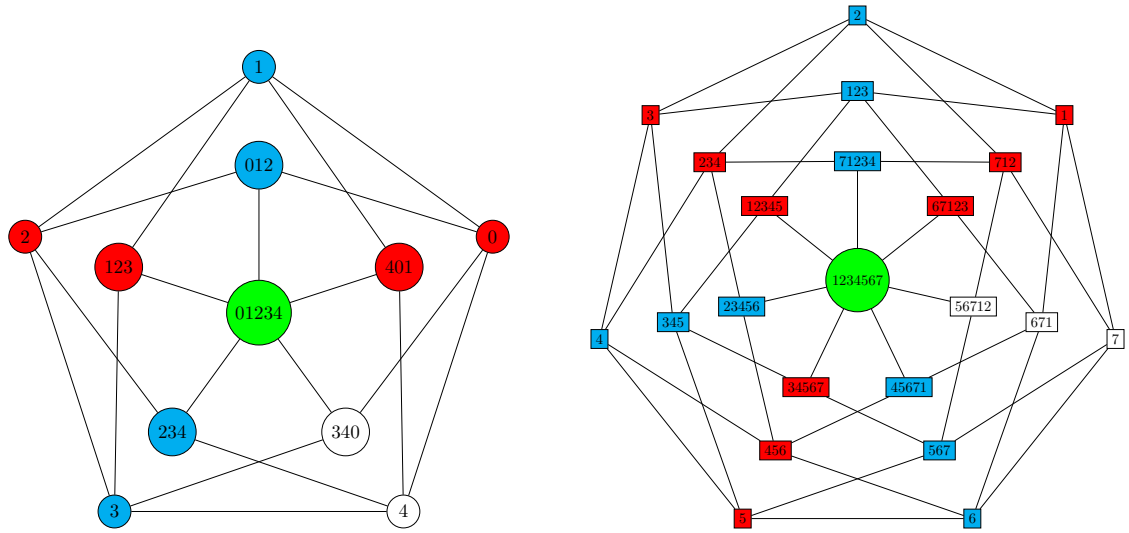
*Proof.* Consider an odd cycle $C_{2n+1} = x_0, \ldots, x_{2n}$. All the indices are taken modulo $2n+1$. Again, we use the set representation for vertices of $2^{C_{2n+1}}$ as it is more convenient for writing the proof. First, $C_{2n+1} \subseteq 2^{C_{2n+1}}$ by Lemma 1.3.2. For any $i \in [\![ 0 \ ; \ 2n ]\!]$, the vertex $\{x_{i-1}, x_i, x_{i+1}\}$ belongs to $2^{C_{2n+1}}$ and is connected by an edge to $\{x_{i-1}\}$ and to $\{x_{i+1}\}$ (because $x_{i-1}, x_i$ and $x_i, x_{i+1}$ are edges of $C_{2n+1}$). Define

$$C^0 = (\{x_i\})_{i \in [\![ 0 \ ; \ 2n ]\!]}$$

and $$\forall k \in [\![ 1 \ ; \ n ]\!] \quad C^k = \left(C^{k-1}(i) \Delta \{x_{i-k}, x_{i+k}\}\right)_{i \in [\![ 0 \ ; \ 2n ]\!]}$$

By construction, we have that

$$\forall k \in [\![ 0 \ ; \ n ]\!] \quad \forall i \in [\![ 0 \ ; \ 2n ]\!] \qquad C^k(i) \in V\left(2^{C_{2n+1}}\right)$$




(a) A 4-coloring of the Grötzsch graph

(b) A 4-coloring of $G_3$

Figure 1.10: Proper 4-colorings of $G_2$ and $G_3$

Observe that

$$\forall k \in [\![ 0 \ ; \ n ]\!] \quad \forall i \in [\![ 0 \ ; \ 2n ]\!] \qquad C^k(i) = C^k(i+1)\Delta\{x_{i-k}, x_{i+1+k}\}$$

$$\begin{aligned} \forall k \in [\![ 1 \ ; \ n ]\!] \quad \forall i \in [\![ 0 \ ; \ 2n ]\!] \qquad C^k(i) &= C^{k-1}(i+1)\Delta\{x_{i-k}, x_{i+1+k}\}\Delta\{x_{i-k}, x_{i+k}\} \\ &= C^{k-1}(i+1)\Delta\{x_{i+k}, x_{i+1+k}\} \end{aligned}$$

hence $\forall k \in [\![ 1 \ ; \ n ]\!] \quad \forall i \in [\![ 0 \ ; \ 2n ]\!] \qquad C^k(i)\, C^{k-1}(i+1) \in E\left(2^{C_{2n+1}}\right)$

which concludes the proof that $G_n$ is an induced subgraph of $2^{C_{2n+1}}$. □

We can now make a proof of Theorem 1.8.2. Observe that $2^G$ is bipartite if and only if $G$ is bipartite by Theorem 1.7.1. Now, if $G$ is not bipartite then it has an odd cycle and so $2^G$ contains $G_n$ as an induced subgraph for some $n \geq 1$ by Lemma 1.8.6. Finally, such subgraph has a chromatic number equals to 4 by Prop 1.8.4.

The result of Theorem 1.8.2 may be surprising if the reader wrongly remember Theorem 1.4.1 as "$G$ and ${\mathbb{F}_q}^G$ have the same chromatic number". As we have seen in the case of $K_3$ and $2^{K_3}$ (see Figure 1.5b), this is not true. Which is true however is that ${\mathbb{F}_q}^G$ is $q$ colorable if and only if $G$ is $q$-colorable. In other words, ${\mathbb{F}_q}^G$ is pertinent only for the $q$-coloring problem on $G$, not any other coloring problem.

A natural question though is "what other properties remains true when we go from $G$ to one of its power graphs?". If one wants to investigate these issues, there is a lot to do. We just scratched the surface.

### 1.8.2 Odd girth

Intuitively, for a non bipartite graph $G$, its shortest non trivial odd cycle is the smallest certificate of its non 2-colorability. We know by Theorem 1.7.1 that $2^G$ is bipartite if and only if $G$ is bipartite. It is then natural to ask whether $2^G$ has, in case $G$ is not bipartite, a shorter odd cycle. We will prove it is not the case. In other word, the odd girth is preserved.

**Definition 1.8.7.** For any graph $G$ we define the odd girth of G as the length of the shortest odd cycle included in $G$. More formally,

$$\mathrm{og}(G) = \inf_{k \in \mathbb{N}^*} \{2k+1 \colon C_{2k+1} \subseteq G\}$$

*Remark.* We have that $\mathrm{og}(G) = +\infty$ if and only if $G$ is bipartite.

**Proposition 1.8.8.** For any graph $G$, $\mathrm{og}(G) = \mathrm{og}(2^G)$.

*Proof.* First, since $G \subseteq 2^G$ by Lemma 1.3.2, we have that $\mathrm{og}(2^G) \leq \mathrm{og}(G)$. If $\mathrm{og}(G) = +\infty$, then $G$ is bipartite hence $2^G$ is bipartite by Theorem 1.4.1 so $\mathrm{og}(2^G) = +\infty$. We now assume $+\infty > \mathrm{og}(G)$ so $\mathrm{og}(G) \geq 3$. Let us define $p = (\mathrm{og}(G) - 1)/2$ and assume for the sake of contradiction that $2^G$ has a cycle of length $2\ell + 1$ with $\ell < p$. Without loss of generality, we assume that this cycle goes through 0 (one just has to translate the cycle). So, there exists $e_1, \ldots, e_{2\ell+1} \in E(G)$ such that this cycle is of the form

$$0, e_1, e_1 + e_2, \ldots, \sum_{i=1}^{2\ell} e_i$$

with $\sum_{i=1}^{2\ell+1} e_i = 0$. Now, in the sum $\sum_{i=1}^{2\ell+1} e_i$, there may be repeating terms. Define $I$ to be the set of terms that appear an odd number of time in this sum. More formally,

$$I := \{e_i \colon i \in [\![ 1 \ ; \ 2\ell + 1 ]\!] \quad |\{j \in [\![ 1 \ ; \ 2\ell + 1 ]\!] \ e_j = e_i\}| \equiv 1 \ [2]\}$$

Observe that $I$ is of odd size since we started from an odd cycle. Indeed, if $|I|$ is even then the $e_i$'s in $I$ contributes to an even number of terms in $\sum_{i=1}^{2\ell+1} e_i$ and the $e_i$'s not in $I$, to another even number of terms which contradicts the fact that this sum has an odd number of terms. Let us rewrite the distinct elements of $I$ as $e_1, \ldots, e_k$. For every $i \in [\![ 1 \ ; \ k ]\!]$, there exists $u_i u_{i+1} \in E(G)$ such that $e_i = u_i + u_{i+1}$. Let $e'_1 = e_1$. Since $\sum_{i=1}^{k} e_i = 0$ and since the $e_i$'s are pairwise distinct, there exists $j \in [\![ 1 \ ; \ k ]\!] \setminus \{1\}$ such that $e_j = u_j + u_2$. Define $e'_2 = e_j$ and iterate this algorithm until you meet $u_1$ that is, until $e'_{k_0} = u_{k_0 - 1} + u_1$. We have that $\sum_{i=1}^{k_0} e'_i = 0$.

- If $k_0$ is odd, we have an odd cycle of $G$ of size $k_0 < \mathrm{og}(G)$ which is a contradiction.
- Otherwise, we start again the algorithm with $I'$ equals $I \setminus \{e'_1, \ldots, e'_{k_0}\}$.

Since $|I|$ is odd, at some point, we will have an odd cycle of $G$ of size strictly less that its odd girth which is a contradiction. □

*Remark.*

- This result is false in general for even cycles. Indeed, consider $C_6 = u_0, \dots, u_5$ and observe that $2^{C_6}$ contains the cycle $0, e_1, e_1+e_2, e_2$ with $e_1 = u_0+u_1$ and $e_2 = u_2+u_3$. Actually, for any $G$ with at least two edges, $2^G$ has a $C_4$.
- This theorem does not hold for $3^G$. Indeed, there is always triangles in $3^G$ (provided $G$ has at least one edge) even if $G$ is bipartite or triangle free.

### 1.8.3 Graphs' logarithms

If $G$ and $G'$ are isomorphic (which we write $G \simeq G'$), then for any $k \geq 2$, ${\Gamma_k}^G \simeq {\Gamma_k}^{G'}$. The proof is straightforward. In the following, we prove the converse which is far from being obvious.

**Theorem 1.8.9.** Let $G$ and $G'$ be two graphs and $k \geq 2$. If ${\Gamma_k}^G \simeq {\Gamma_k}^{G'}$ then $G \simeq G'$.

*Proof.* Assume that ${\Gamma_k}^G \simeq {\Gamma_k}^{G'}$. By definition, there exists a graph isomorphism

$$f : {\Gamma_k}^V \to {\Gamma_k}^{V'}$$

for ${\Gamma_k}^G$ to ${\Gamma_k}^{G'}$ which implies in particular that $k^{|V|} = k^{|V'|}$ and so that $|V| = |V'|$. Let $\epsilon_1$ be the vector $\begin{bmatrix}1 & 0 & \cdots & 0\end{bmatrix} \in {\Gamma_k}^{|V|}$. We fix an ordering of the vertices of $G$ and of the vertices of $G'$. Then, $\epsilon_1$ can be seen as $\mathbb{1}_{v_1}$ (a vertex of ${\Gamma_k}^G$) or $\mathbb{1}_{v'_1}$ (a vertex of ${\Gamma_k}^{G'}$). First, we explain why we can assume without loss of generality that $f(\epsilon_1) = \epsilon_1$. Indeed, for every $c \in {\Gamma_k}^{|V|}$, if we define $f_c$ to be $f + c$, then $f_c$ is a graph morphism from ${\Gamma_k}^G$ to ${\Gamma_k}^{G'}$ as for every $xy \in E\left({\Gamma_k}^G\right)$,

$$(f_c(x), f_c(y)) = (f(x), f(y)) + (c, c)$$

which is an edge of ${\Gamma_k}^{G'}$ as $(f(x), f(y)) \in E\left({\Gamma_k}^{G'}\right)$. Moreover, $f_c$ is a bijection and ${f_c}^{-1} = f^{-1}(\bullet - c)$ is a graph morphism as a composed function of graph morphisms. Hence, up to considering $f' = f - f(\epsilon_1) + \epsilon_1$, we can assume that $f(\epsilon_1) = \epsilon_1$.

Since $f$ is a graph isomorphism, it preserves the distances so the neighborhood of $\epsilon_1$ in ${\Gamma_k}^G$ is sent to the neighborhood of $f(\epsilon_1) = \epsilon_1$ in ${\Gamma_k}^{G'}$. This means that

$$\{\mathbb{1}_v : v \in V\} = \{\mathbb{1}_{v'} : v' \in V'\}$$

This allows us to define $h : V' \to V$ that associate to each $v' \in V'$ the unique $v \in V$ such that $f(\mathbb{1}_v) = \mathbb{1}_{v'}$.

We can now check that $h$ is a graph isomorphism from $G'$ to $G$. Let $u'v' \in E(G')$. Since $f^{-1}$ is a graph morphism,

$$f^{-1}(\mathbb{1}_{u'}) f^{-1}(\mathbb{1}_{v'}) = \mathbb{1}_{h(u')}\mathbb{1}_{h(v')} \in E\left({\Gamma_k}^G\right)$$

so $h(u')h(v') \in E(G)$. Moreover, since $f_{|N(\epsilon_1)}$ is a bijection, $h$ is also a bijection. Using the fact that $f$ is a graph morphism, one can check that $h^{-1}$ is also a graph morphism. □

### 1.8.4 Colorings of power graphs

We proved in Lemma 1.4.3 that any $q$-coloring of $G$ can be extended to a $q$-coloring of ${\mathbb{F}_q}^G$. Recall that this is false in general for ${\Gamma_k}^G$ (see Proposition 1.4.5). The question whether ${\mathbb{F}_q}^G$ can have other $q$-colorings is natural. Namely, does ${\mathbb{F}_q}^G$ have $q$-colorings that are not linear extensions of colorings of $G$? Stated this way, this answer is trivial since ${\mathbb{F}_q}^G$ has (at least) $q$ connected components. We could just chose two different $q$-colorings for $G$ and extend the first one on one connected component and the second one on the others. Moreover, if $\chi$ is a $q$-coloring of ${\mathbb{F}_q}^G$, $\chi + \lambda$ is a proper $q$-coloring of ${\mathbb{F}_q}^G$ for any $\lambda \in \mathbb{F}_q$. Hence, the interesting question is: given a $q$-colorable connected graph $G$, does there exist a proper $q$-coloring of one connected component of ${\mathbb{F}_q}^G$ (say the component of the vertices whose sum is zero) that is not an affine extension of a $q$-coloring of $G$?

We will see in this section that the answer is "no" for $q = 2$ or $q = 3$ but "yes" if $q$ is any other prime number. When $q$ is a non trivial power of a prime number, the question is open.

**Notation.** We denote by $\mathrm{C}_0\left({\mathbb{F}_q}^G\right)$ the component of ${\mathbb{F}_q}^G$ composed by the vertices that sum to zero. More formally,

$$\mathrm{C}_0 := \left\{ v \in {\mathbb{F}_q}^{V(G)} \colon \sum_{i=1}^{n} v_i = 0 \right\}$$

**Theorem 1.8.10.** If $G$ is a connected graph, then any 3-coloring of $\mathrm{C}_0\left(3^G\right)$ is an affine extension of a 3-coloring of $G$.

Let us prove this theorem. Let $G$ be a connected 3-colorable graph and $\chi$ be a 3-coloring of $\mathrm{C}_0\left(3^G\right)$. First of all, observe that without loss of generality, we can assume that $\chi(0) = 0$. Indeed, if it is not the case, define $\chi' = \chi - \chi(0)$ and show it is linear so that $\chi$ is affine.

**Notation.** For $e = uv \in E(G)$, we abuse notations and denote by $e$ the vector $\mathbb{1}_u - \mathbb{1}_v$ for convenience.

**Claim 1.8.11.** $\forall v \in \mathrm{C}_0\left(3^G\right) \quad \forall e, e' \in E(G) \qquad \chi(v) + \chi(v + e - e') + \chi(v + e' - e) = 0$

*Proof.* This is a simple check on the 4 proper colorings of the induced graph composed by the vertices $v$, $v+e$, $v-e$, $v+e'$, $v-e'$, $v+e+e'$, $v+e-e'$, $v+e'-e$, $v-e-e'$. A drawing of this subgraph can be found on Figure 1.11. Basically, every row and every column forms a triangle.
Finding a proper 3-coloring of this subgraph is nothing but solving some kind of "sudoku game". Without loss of generality, $\chi(v) = 0$ and we have only two possibilities left (see Figure 1.11).
In both cases, the equality $\chi(v) + \chi(v + e - e') + \chi(v + e' - e) = 0$ is satisfied. □

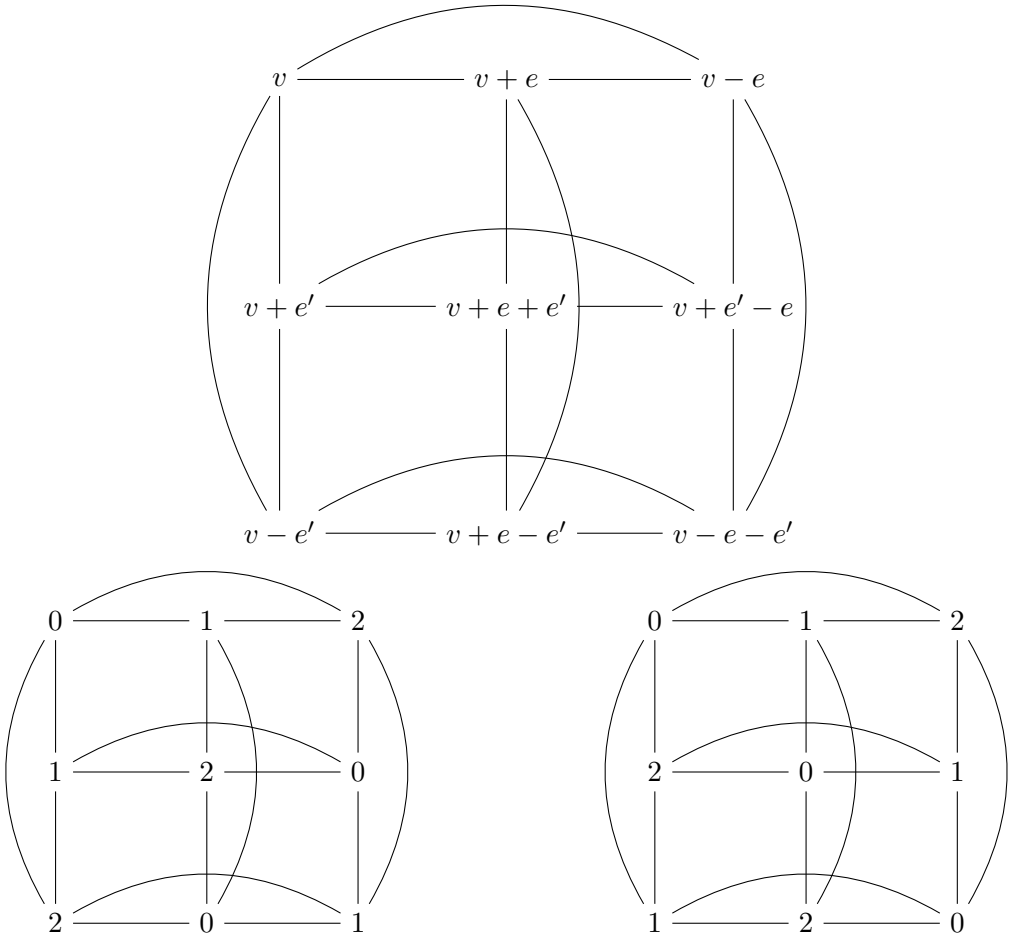



Figure 1.11: Two kind of 3-colorings for a subgraph of $3^G$

Now, take $e, e' \in E(G)$ and observe that since $\chi$ sums to zero on every edge-clique, we have that

$$\begin{cases} \chi(e) + \chi(e+e') + \chi(e-e') = 0 \\ \chi(e') + \chi(e'+e) + \chi(e'-e) = 0 \end{cases}$$

hence $$\chi(e+e') = \chi(e) + \chi(e') + \chi(e-e') + \chi(e'-e) = \chi(e) + \chi(e')$$

because $$\chi(0) + \chi(0+e-e') + \chi(0-e+e') = 0$$

by Claim 1.8.11 with $v = 0$.

**Claim 1.8.12.** For any $k \in \mathbb{N}$, for any $e_1, \ldots, e_k \in E(G)$,

$$\chi\left(\sum_{i=1}^{k} e_i\right) = \sum_{i=1}^{k} \chi(e_i)$$

*Proof.* We do an induction on $k$. For $k \in \{0, 1, 2\}$ the result is true by what we have done above. Consider $k \geq 3$ and assume the result to be true for any $k' < k$. Let $e_1, \ldots, e_k \in E(G)$. We have that

$$\chi\left(\sum_{i=2}^{k} e_i\right) + \chi\left(\sum_{i=1}^{k} e_i\right) + \chi\left(e_1 + \sum_{i=1}^{k} e_i\right) = 0$$

because this is a sum on and edge-clique (directed by $e_1$). The same goes for an edge-clique directed by $e_2$ so

$$\chi\left(e_1 + \sum_{i=3}^{k} e_i\right) + \chi\left(\sum_{i=1}^{k} e_i\right) + \chi\left(e_2 + \sum_{i=1}^{k} e_i\right) = 0$$

hence $$\chi\left(\sum_{i=1}^{k} e_i\right) = \chi\left(\sum_{i=2}^{k} e_i\right) + \chi\left(e_1 + \sum_{i=3}^{k} e_i\right) + \chi\left(e_1 + \sum_{i=1}^{k} e_i\right) + \chi\left(e_2 + \sum_{i=1}^{k} e_i\right)$$

but since $$\chi\left(e_1 + \sum_{i=1}^{k} e_i\right) + \chi\left(e_2 + \sum_{i=1}^{k} e_i\right) = -\chi\left(\sum_{i=3}^{k} e_i\right)$$

by Claim 1.8.11 with $v = \sum_{i=3}^{k} e_i$, $e = e_1$ and $e' = e_2$, we have that

$$\chi\left(\sum_{i=1}^{k} e_i\right) = \chi\left(\sum_{i=2}^{k} e_i\right) + \chi\left(e_1 + \sum_{i=3}^{k} e_i\right) - \chi\left(\sum_{i=3}^{k} e_i\right)$$

By the induction hypothesis,

- $\chi\left(e_1 + \sum_{i=3}^{k} e_i\right) = \chi(e_1) + \sum_{i=3}^{k} \chi(e_i)$
- $\chi\left(\sum_{i=3}^{k} e_i\right) = \sum_{i=3}^{k} \chi(e_i)$
- $\chi\left(\sum_{i=2}^{k} e_i\right) = \sum_{i=2}^{k} \chi(e_i)$

so $$\chi\left(\sum_{i=1}^{k} e_i\right) = \sum_{i=1}^{k} \chi(e_i)$$

Hence, $\chi$ is additive on $\{\mathbb{1}_u - \mathbb{1}_v \colon uv \in E(G)\}$. □

We will now prove that $\chi$ is additive on ${\Gamma_k}^{V(G)}$ by using this last property on paths of $G$. Let $u, v \in \mathrm{C}_0\left(3^G\right)$. Since $G$ is connected, $\mathrm{C}_0\left(3^G\right)$ is a connected component (see Proposition 1.8.1) so there exists $e_1, \ldots, e_s \in E(G)$ and ${e_1}', \ldots, {e_t}' \in E(G)$ such that

$$u = \sum_{i=1}^{s} e_i \qquad \text{and} \qquad v = \sum_{i=1}^{t} {e_i}'$$

Hence,
$$\begin{aligned}\chi(u+v) &= \chi\left(\sum_{i=1}^{s} e_i + \sum_{i=1}^{t} {e_i}'\right)\\ &= \sum_{i=1}^{s}\chi(e_i) + \sum_{i=1}^{t}\chi({e_i}') && \text{by Claim 1.8.12}\\ &= \chi\left(\sum_{i=1}^{s} e_i\right) + \chi\left(\sum_{i=1}^{t} {e_i}'\right) && \text{again by Claim 1.8.12}\\ &= \chi(u) + \chi(v)\end{aligned}$$

Then, we have that $\forall u, v \in \mathrm{C}_0\left(3^G\right) \qquad \chi(u+v) = \chi(u) + \chi(v)$

Moreover, since for every $e \in E(G)$, $\{0, e, -e\}$ is an edge-clique and because $\chi(0) = 0$, we have that $\chi(-e) = -\chi(e)$. Hence,

$$\forall v \in \mathrm{C}_0\left(3^G\right) \qquad \chi(-v) = -\chi(v)$$

which concludes the proof of Theorem 1.8.10.

*Remark.* The same result is true for the 2-colorings of $2^G$. A short proof is provided below.

**Proposition 1.8.13.** If $G$ is a connected graph, then any 2-coloring of $\mathrm{C}_0\left(2^G\right)$ is an affine extension of a 2-coloring of $G$.

*Proof.* Let $\chi$ be a 2-coloring of $\mathrm{C}_0\left(2^G\right)$. Without loss of generality, we assume that $\chi(0) = 0$. Observe that $\chi$ sums to 1 on every edge-clique that is

$$\forall v \in 2^V \quad \forall e \in E(G) \qquad \chi(v) + \chi(v+e) = 1$$

In particular, since $\chi(0) = 0$,

$$\forall e \in E(G) \qquad \chi(e) = 1$$

For $e, e' \in E(G)$, $\chi(e) + \chi(e+e') = 1$ so $\chi(e+e') = 0 = 1+1 = \chi(e) + \chi(e')$. By induction, for $e_1, \ldots, e_k \in E(G)$,

$$\chi\left(\sum_{i=1}^{k} e_i\right) = \begin{cases} 1 & \text{if } k \text{ is odd} \\ 0 & \text{otherwise} \end{cases}$$

so $\chi\left(\sum_{i=1}^{k} e_i\right) = \sum_{i=1}^{k}\chi(e_i)$.

Since $G$ is connected, we show as in the proof of Theorem 1.8.10 that,

$$\forall u, v \in \mathrm{C}_0\left(2^G\right) \qquad \chi(u+v) = \chi(u) + \chi(v)$$

Since the ground field is $\mathbb{F}_2$, this suffices to prove the result. □

**Proposition 1.8.14.** For any $k \geq 4$, there exists $G$ such that $\mathrm{C}_0\left({\mathbb{Z}_k}^G\right)$ has a proper $k$-coloring which is not an affine extension of a proper $k$-coloring of $G$.

*Proof.* Take $G = (V, E)$ any edge-critical $k$-chromatic graph. Consider a $k$-coloring $c$ of $G$ and define $\chi = \langle c, \bullet \rangle$ the linear extension of $c$ on ${\mathbb{Z}_k}^G$ (see Definition 1.4.2). For any $i \in [\![\, 0 \,;\, k-1 \,]\!]$, define $S_i := \left\{ a \in {\mathbb{Z}_k}^V : \chi(a) = i \right\}$ and let $\chi' : {\mathbb{Z}_k}^V \to \mathbb{Z}_k$ be defined by

$$\forall a \in {\mathbb{Z}_k}^V \qquad \chi'(a) = \begin{cases} 0 & \text{if } a \in S_0 \\ 1 & \text{if } a \in S_1 \\ 3 & \text{if } a \in S_2 \\ 2 & \text{if } a \in S_3 \\ j & \text{if } a \in S_j \quad \text{for any } j \in [\![ 4 \ ; \ k-1 ]\!] \end{cases}$$

Observe that $\chi'$ is a proper $k$-coloring of $\mathrm{C}_0\left({\mathbb{Z}_k}^G\right)$ since we just renamed the colors of $\chi$. Moreover, if $\chi'$ is an affine extension of a proper coloring of $G$ then $\chi'$ is linear since $\chi'(0) = 0$. Consider now $a, b \in \mathrm{C}_0\left({\mathbb{Z}_k}^V\right)$ such that $\chi(a) = 1$ and $\chi(b) = 3$ which exists since $G$ is edge-critical and there is a copy of $G$ inside $\mathrm{C}_0\left({\mathbb{Z}_k}^G\right)$. We then have that $\chi'(a+b) = 4$ but $\chi'(a) = 1$ and $\chi'(b) = 2$ so $\chi'$ is not linear which concludes the proof. □

*Remark.* The counter example we gave is a bit disappointing as it is still an affine extension of a 4-coloring of $G$ up to colors permutation. The question of the existence of other $k$-colorings for ${\mathbb{Z}_k}^V$ is open.

### 1.8.5 Structures of the cliques

When $k$ is a power of a prime number, we have introduced two objects to study the $k$-colorability problem: ${\mathbb{Z}_k}^G$ and ${\mathbb{F}_k}^G$. We know by Proposition 1.4.5 that (for a fixed $G$), those graphs are not isomorphic in general. In particular, even though ${\mathbb{F}_k}^G$ has an edge-clique certificate if and only if it is not $k$-colorable (see Theorem 1.7.1), this equivalence is false in general for ${\mathbb{Z}_k}^G$. Indeed, by Proposition 1.4.5, the graph ${\mathbb{Z}_4}^{K_4}$ is not 4-colorable but it cannot have any edge-clique certificate as it would provide a Nullstellensatz[13] certificate for $K_4$. However, we know by Proposition 1.5.6 that ${\mathbb{Z}_k}^G$ has an edge-clique certificate whenever $G$ is not $k$-colorable (and, as we just said, this is a Nullstellensatz certificate). A natural question is whether ${\mathbb{Z}_k}^G$ has a clique-certificate when it is itself not $k$-colorable. In this subsection, we prove this to be false in general. In order to establish this result, we will consider the particular case of ${\Gamma_k}^{K_k}$ (with $\Gamma_k$ being either $\mathbb{Z}_k$ or $\mathbb{F}_k$ when defined) and explore the structure of the $k$-cliques of ${\Gamma_k}^{K_k}$.

**Theorem 1.8.15.** Let $k \geq 2$ be an integer and $\Gamma_k$ be either $\mathbb{Z}_k$ or, when defined, $\mathbb{F}_k$. The $k$-cliques of ${\Gamma_k}^{K_k}$ are either

- edge-cliques
- or homothetic translations of the canonical copy of $K_k$. More precisely, if $\epsilon_i$ is the $i^{\text{th}}$ vector of the canonical basis of ${\Gamma_k}^{K_k}$, then there exists $\lambda \in \Gamma_k$ and $t \in {\Gamma_k}^k$ such that

$$\{a_1, \ldots, a_k\} + t = \lambda \{\epsilon_1, \ldots, \epsilon_k\}$$

*Proof.* Let $a_1, \ldots, a_k$ be a subgraph of ${\Gamma_k}^{K_k}$ that is a $k$-clique. Define for all $i, j \in [\![ 1 \ ; \ k ]\!]$ with $i < j$, $x_{ij} := a_j - a_i$. First, let us show that if three points among $a_1, \ldots, a_k$ belongs

[13] This would be a Nullstellensatz certificate in the quotient described in Section 1.5.2. By Proposition 1.5.5, this contradicts the fact that $K_4$ is 4-coloriable.

to the same edge-clique, then $a_1, \dots, a_k$ is an edge-clique. Assume that three points, say $a_1, a_2$ and $a_3$, belong to the same edge-clique. Observe that in general, for any graph $G$, two vertices of ${\Gamma_k}^G$ are connected by an edge if and only if they belong to the same connected component $\mathrm{C}_\lambda\left({\Gamma_k}^G\right)$ for $\lambda \in \Gamma_k$ and if they differ on exactly two coordinates. Without loss of generality, we assume that $x_{12} = \mu\left(\mathbb{1}_{v_1} - \mathbb{1}_{v_2}\right)$ for some $\mu \in \Gamma_k \setminus \{0\}$. Hence, $x_{23} = \lambda\left(\mathbb{1}_{v_1} - \mathbb{1}_{v_2}\right)$ for some $\lambda \in \Gamma_k \setminus \{0\}$ and $a_1, a_2, a_3$ are equal on coordinates $3, \dots, k$. Since $a_1 a_4 \in E\left({\Gamma_k}^{K_k}\right)$, there are exactly two coordinates $i$ and $j$ (say $i < j$) where $a_1$ and $a_4$ differ. We will show that $x_{12}$ and $x_{14}$ are collinear. Assume for the sake of contradiction that $\{i, j\} \neq \{1, 2\}$.

- Assume that $i, j \geq 3$. Since $a_1$ and $a_2$ are equal on coordinates $3, \dots, k$, $a_4$ and $a_2$ differ on coordinates $i$ and $j$. Hence, $a_1, a_2$ and $a_4$ belong to the same edge-clique directed by the edge $x_{14}$. However, two distinct edge-clique cannot share more than one point so it must be that $x_{12}$ and $x_{14}$ are collinear.
- Assume that $i \in \{1, 2\}$ and $j \geq 3$. Take $i = 1$ for instance (the case $i = 2$ is analogous). Observe that $a_4$ and $a_2$ differ on position $j$. If $a_4$ and $a_2$ differ on 1, then $a_4$ and $a_2$ are identical on coordinate 2 so $a_1$ and $a_2$ are equal on coordinate 2 which is a contradiction. Hence, $a_4$ and $a_2$ differ on coordinates 2 and $j$. For the same reason, $a_4$ and $a_3$ differ on coordinates 2 and $j$. However, this implies that $a_4, a_3$ and $a_2$ are all equal on coordinate 1 which is again a contradiction.

Hence, $a_4$ and $a_1$ differ on coordinates 1 and 2 so $x_{12}$ and $x_{14}$ are collinear. This implies that $a_1, a_2, a_3$ and $a_4$ belong to the same edge-clique. Since we can do the same reasoning for $a_5, \dots, a_k$, in the end, we have that $a_1, \dots, a_k$ is an edge-clique.

We now assume that $a_1, \dots, a_k$ is a clique that is not an edge-clique. By what we just did, this implies that $x_{1,2}, \dots, x_{1,k}$ are pairwise not collinear. Then, for every $i \in [\![ 1 \ ; \ k ]\!]$, $x_{1,i}, \dots, x_{i-1,i}, x_{i,i+1}, \dots, x_{i,k}$ are pairwise not collinear. Then, every direction can be found in $\{x_{ij} \colon i, j \in [\![ 1 \ ; \ k ]\!] \text{ with } i < j\}$. We write

$$x_{ij} = \lambda_{ij}\left(\mathbb{1}_{u_{ij}} - \mathbb{1}_{v_{ij}}\right)$$

with $\lambda_{ij} \in \Gamma_k$ and $u_{ij}, v_{ij} \in V(K_k)$. First, observe that the $\lambda_{ij}$ must be the same, up to a $-1$ factor. To prove this, simply consider the triangles, as we did previously. The three edges implied in a triangle must have (up to some sign change), the same $\lambda$.

Denote by $\epsilon_i$ the $i^{\text{th}}$ vector of the canonical basis of ${\Gamma_k}^k$. Define $t$ by

$$t = -a_1 + \lambda\epsilon_1$$

We will show that $$\{a_1, \dots, a_k\} = \lambda\{\epsilon_1, \dots, \epsilon_k\} - t$$

Of course, $a_1 + t = \lambda\epsilon_1$. Since we have every directions among the $x_{ij}$, there exists $i$ and $j$ such that

$$a_1 + x_{ij} = \lambda\epsilon_2$$

so $$t + a_1 - a_i + a_j = \lambda\epsilon_2$$

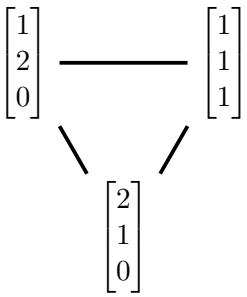
Suppose by contradiction that 1,$i$ and $j$ are all different (that is, $|\{1, i, j\}| = 3$). Then, in particular, $a_i \neq a_1$ so we can write

$$t + a_1 - (t + a_i) = a_1 - a_i = \lambda (\mathbb{1}_u - \mathbb{1}_v)$$

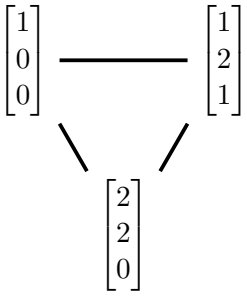
for some $u$ and $v$. Since $t + a_1 - a_i + a_j = \lambda\epsilon_2$, it must be that $t + a_j$ has its support within $\{2, u, v\}$. Moreover, $t + a_1$ and $t + a_j$ are connected by an edge so $|\{1, 2, u, v\}| = 2$. Hence,

- either $u = 1$ and $v = 2$ but in that case, $t + a_j = -\lambda\epsilon_1 + 2\lambda\epsilon_2$ and $t + a_i = \lambda\epsilon_2$ which leads to $a_1$, $a_i$ and $a_j$ to be on the same edge-clique: contradiction
- or $u = 2$ and $v = 1$ but then $t+a_j = \lambda\epsilon_1 = t+a_1$ which leads to $a_j = a_1$: contradiction.

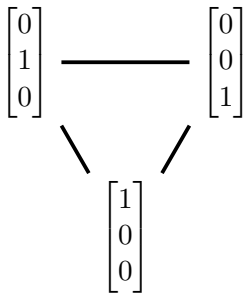
Then, either $j$ or $i$ is equal to 1. If $i = 1$, then we have $t+a_1-a_1+a_j = \lambda\epsilon_1$ so $t+a_j = \lambda\epsilon_2$. However, if $j = 1$, then $t + a_1 + a_1 - a_i = \lambda\epsilon_2$ and we cannot conclude that $t + a_i = \lambda\epsilon_2$. It is actually false. Consider the following example which represents a clique in $3^{K_3}$:



This is not an edge-clique and, indeed, every possible direction is used. If we take $t = \epsilon_1 - {}^{\mathrm{t}}\begin{bmatrix}1 & 2 & 0\end{bmatrix}$, this leads us to



which is problematic. The point is, we cannot send any vertex to $\lambda\epsilon_1$: we must choose it wisely. For instance, in our example, if we use $t = {}^{\mathrm{t}}\begin{bmatrix}2 & 2 & 0\end{bmatrix}$, the translation by $t$ gives:




Let us say that, once we have fixed a $\lambda$ (namely, we chose between $\lambda$ and $-\lambda$), a vertex $a_i$ among $a_1, \dots, a_k$ is *nice* if and only if $a_i$ satisfies that for every $j \in [\![ 1 \ ; \ k ]\!] \setminus \{i\}$,

$$a_j - a_i = \lambda \left( \mathbb{1}_{u_{ij}} - \mathbb{1}_{v_{ij}} \right)$$

with $u_{ij} < v_{ij}$.

**Fact 1.8.16.** There exists a vertex among $a_1, \dots, a_k$ which is *nice*.

*Proof.* It suffices to notice that, since every directions exists in $\{a_j - a_i \colon 1 \leq i < j \leq k\}$,

$$\left\{ \lambda \left( \mathbb{1}_{u_i} - \mathbb{1}_{u_j} \right) : 1 \leq i < j \leq k \right\} = \{a_j - a_i \colon 1 \leq i < j \leq k\}$$

Hence, renaming the $a_i$'s is the same as choosing a permutation of the vertices of the ground graph. □

Without loss of generality, we may assume that $a_1$ is nice. We define $t = -a_1 + \lambda\epsilon_1$. Recall that we proved that there exists $i, j \in [\![ 1 \ ; \ k ]\!]$ such that

$$t + a_1 - a_i + a_j = \lambda\epsilon_2$$

and that, either $i = 1$ or $j = 1$. Then, since $a_1$ is nice, it must be that $i = 1$ and so $t + a_j = \lambda\epsilon_2$. Indeed, if $j = 1$, then $t + a_1 + a_1 - a_i = \lambda\epsilon_2$ so

$$a_i - a_1 = \lambda\epsilon_2 - \lambda\epsilon_1$$

which contradicts the fact that $a_1$ is nice.

We can now iterate the construction: there exists an edge $a_s - a_r$ with $s > r$ such that

$$t + a_1 - a_r + a_s = \lambda\epsilon_3$$

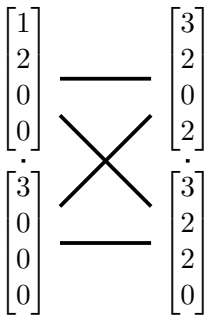
For the same reason as previously, either $r = 1$ or $s = 1$. The fact that $a_1$ is nice allow us to discard the case $s = 1$.

In the end, we have that

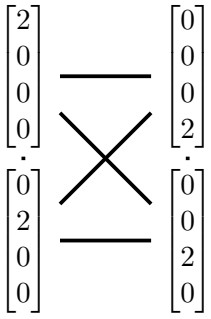
$$\{a_1, \dots, a_k\} = \lambda \{\epsilon_1, \dots, \epsilon_k\} - t$$

□

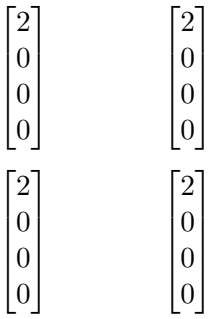
In case $\{a_1, \dots, a_k\}$ is not an edge-clique, it is not entirely true to speak of homothetic translation. Indeed, we may not be able to divide by $\lambda$ if $\Gamma_k$ is not a field. For instance, consider the following clique in ${\mathbb{Z}_4}^{K_4}$:



We can check that this is not an edge-clique (and that every directions are involved). We fix $\lambda = 2$ and observe that vertex ${}^{\mathrm{t}}\begin{bmatrix}1 & 2 & 0 & 0\end{bmatrix}$ is nice. So, we may translate using $t = {}^{\mathrm{t}}\begin{bmatrix}1 & 2 & 0 & 0\end{bmatrix}$ which leads to



In such case, we cannot divide by two as it is not invertible in $\mathbb{Z}_4$. One may wonder if we can make some clever trick like multiplying by $\lambda$ before taking the translation $t$. However, precisely because $\lambda$ may not be invertible, it fails. For instance, multiplying by 2 the previous example leads to



which is obviously not a clique since all the vertices "collapsed" to ${}^{\mathrm{t}}\begin{bmatrix}2 & 0 & 0 & 0\end{bmatrix}$. This example can be generalized to every ${\mathbb{Z}_k}^{K_k}$ whenever $k$ is not a power of a prime number.

**Corollary 1.8.17.** Let $k \geq 2$ and $\Gamma_k$ be either $\mathbb{Z}_k$ or, when defined, $\mathbb{F}_k$. There is no $k+1$-clique in ${\Gamma_k}^{K_k}$.

*Proof.* Suppose $a_1, \ldots, a_{k+1}$ is a clique of size $k+1$ of ${\Gamma_k}^{K_k}$. First, let us show that it does not contain an edge-clique. By contradiction assume without loss of generality that $a_1, \ldots, a_k$ is an edge-clique directed by $\mathbb{1}_{v_1} - \mathbb{1}_{v_2}$ (hence the weight transfer is done on the two first coordinate). Let $i, j$ be the coordinate on which $a_1$ and $a_{k+1}$ disagree ($i < j$).

- If $i = 1$ and $j = 2$ then $a_{k+1}$ belongs to the edge-clique $a_1, \ldots, a_k$ which is a contradiction as an edge-clique has cardinality $k$.
- If $i, j \geq 3$ then $a_{k+1}$ and $a_2$ have 4 different coordinates so they cannot be connected by an edge which is a contradiction.
- If $i \in \{1, 2\}$ (say $i = 1$) and $j \geq 3$ (say $j = 3$) then, since $a_{k+1}$ and $a_1$ are the same on coordinate 2, $a_{k+1}$ and $a_2$ must differ on coordinates 2 and 3 or on coordinates 1 and 2. The latter is not possible since $a_{k+1}$ would then belong to the edge-clique $a_1, \ldots, a_k$. Then, either $a_2$ and $a_{k+1}$ differ on coordinate 1 and we have a contradiction, or $a_3$ and $a_{k+1}$ differ on coordinates 1, 2 and 3 which is, again, a contradiction.

So, a clique of size $k+1$ in ${\Gamma_k}^{K_k}$ cannot contain an edge-clique. By Theorem 1.8.15, the cliques of size $k$ in $a_1, \ldots, a_{k+1}$ are homothetic translations of the canonical $k$-clique of ${\Gamma_k}^{K_k}$. One just has to check that there is no $k+1$-clique in the distance one neighborhood of this canonical $k$-clique. Indeed, assume there is one vertex $v$ connected by an edge to $\begin{bmatrix}1 & 0^{k-1}\end{bmatrix} \ldots \begin{bmatrix}0^{k-1} & 1\end{bmatrix}$, then $v$ and $\begin{bmatrix}1 & 0^{k-1}\end{bmatrix}$ must be equal on $k-2$ coordinates say for instance the last ones. But in such case, $v$ cannot be connected by an edge to $\begin{bmatrix}0^{k-1} & 1\end{bmatrix}$.

*Remark.* We implicitly assumed $k \geq 3$ in the proof. However, it is easy to check that the result is true for $2^{K_2}$.

□

## 1.9 Generalizations

In this section, we explore an extension of the coloring problem using graph homomorphisms. If there is a graph homomorphism from $G$ to $H$, we denote it by $G \xrightarrow{f} H$ or even $G \to H$.

**Proposition 1.9.1.** A graph $G$ can be colored with $k$ colors if and only if $G \to K_k$.

*Proof.* Assume that $G \xrightarrow{f} K_k$. Notice that any proper coloring for $K_k$ gives a proper coloring for $G$. Indeed, for $u \in V(G)$, one just has to take the color of $f(u)$. This proves that $\chi(G) \leq k$.

Now, if we can color $G$ with $k$ colors, then we can map $G$ to $K_k$ using the coloring we have on $G$. This gives a graph homomorphism. □

*Remark.* More generally, we have shown that if $G \to H$ then $\chi(G) \leq \chi(H)$.

Hence, the existence of a graph homomorphism between two graphs can be seen as a more general problem than graph coloring.

### 1.9.1 Cayley graphs

Since power graphs are useful to study chromatic numbers, one can be tempted to consider a power graph of some power graph. The following results show that doing it does not necessarily lead to a more interesting structure if one wants to study chromatic numbers.

In order to have a very general result, we study the case of $\Gamma^G$ where $\Gamma$ is a finite Abelian group. We will use the additive notation.

**Definition 1.9.2** (Cayley graph)**.** Let $\Gamma$ be an Abelian group and $\Delta$ be a symmetric[14] subset of $\Gamma$. We define the graph $H = \mathscr{C}(\Gamma, \Delta)$ by

$$V(H) = \Gamma \qquad \text{and} \qquad E(H) = \left\{(u, v) \in \Gamma^2 \colon u - v \in \Delta\right\}$$

**Definition 1.9.3.** Let $G$ be a connected graph and $H = \mathscr{C}(\Gamma, \Delta)$. We define the graph $H^G$ by

- $V\left(H^G\right) = \Gamma^{V(G)}$
- $xy \in E\left(H^G\right)$ if and only if there exists $uv \in E(G)$ such that

  i) $\forall w \in V(G) - \{u, v\} \qquad x(w) = y(w)$
  ii) $x(u) - y(u) \in \Delta$
  iii) $x(u) - y(u) = y(v) - x(v)$

*Remark.* This definition is very similar to Definition 1.3.1. Actually, the graph ${\Gamma_k}^G$ is a particular case of $\mathscr{C}(\Gamma, \Delta)^G$ where $\Gamma = \Gamma_k$ and $\Delta = \Gamma_k \setminus \{0\}$.

**Proposition 1.9.4.** Let $H = \mathscr{C}(\Gamma, \Delta)$ be a Cayley graph with $\Gamma$ a finite Abelian group. For any graph $G$,

$$H^{H^G} \to H^G$$

*Proof.* Let us first recall the famous result on the structure of finite type Abelian groups.

**Theorem 1.9.5** (Kronecker)**.** Let $Gr$ be a finite type Abelian group. There exists a unique $n \in \mathbb{N}$ and a unique sequence (up to ordering) $a_1, \ldots, a_r$ such that $a_{i+1} \,|\, a_i$ for every $i \in [\![ 1 \,;\, r-1 ]\!]$ and that we have the group isomorphism

$$Gr \simeq \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r} \times \mathbb{Z}^n$$

[14] $\forall x \in \Gamma \qquad x \in \Delta \Rightarrow -x \in \Delta$

Let us prove the result in the particular case where $\Gamma$ is a group of the form

$$\Gamma = \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}$$

and $\Delta$ is any symmetric set of $\mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}$. Once it is done, we will use Kronecker's theorem in order to have the general result. Define

$$f : \left\{ \begin{array}{ccc} \Gamma^{\Gamma^V} & \to & \Gamma^V \\ \phi & \mapsto & \sum\limits_{x \in \Gamma^V} \phi(x) x \end{array} \right.$$

where we use the usual scalar multiplication that makes $\Gamma^V$ a module on $\Gamma$.

Consider $\phi\psi \in E\left(H^{H^G}\right)$. By definition, there exists $xy \in E(H^G)$ and $uv \in E(G)$ such that

- $\forall z \in V\left(H^G\right) \setminus \{x, y\} \quad \phi(z) = \psi(z)$
- $\psi(x) - \phi(x) \in \Delta$
- $\psi(x) - \phi(x) = \phi(y) - \psi(y)$
- $\forall w \in V \setminus \{u, v\} \quad x(w) = y(w)$
- $x(u) - y(u) \in \Delta$
- $x(u) - y(u) = y(v) - x(v)$

Let us show that $f(\phi)f(\psi) \in E(H^G)$.

$$\begin{aligned} f(\psi) - f(\phi) &= \sum_{\gamma \in \Gamma^V} (\psi(\gamma) - \phi(\gamma))\gamma \\ &= (\psi(x) - \phi(x))x + (\psi(y) - \phi(y))y \\ &= (\psi(x) - \phi(x))(x - y) \end{aligned}$$

Hence, $\forall w \in V \setminus \{u, v\} \quad f(\psi)(w) = f(\phi)(w)$

Moreover,
$$\begin{aligned} f(\psi)(u) - f(\phi)(u) &= (\psi(x) - \phi(x))(x(u) - y(u)) \\ &= (\psi(x) - \phi(x))(y(v) - x(v)) \\ &= f(\phi)(v) - f(\psi)(v) \end{aligned}$$

which concludes the proof that $f(\phi)f(\psi) \in E\left(H^G\right)$.

Consider now an arbitrary finite Abelian group $\Gamma$. We know by Kronecker's theorem (see 1.9.5) that there exists a group isomorphism

$$g \ : \ \Gamma \ \to \ \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}$$

with[15] $a_{i+1} \,|\, a_i$ for every $i \in [\![ 1 \,;\, r-1 ]\!]$. In order to prove the general statement, it suffices to show that for any graph $G$ and any symmetric set $\Delta$ of $\Gamma$, there exists a graph homomorphism

[15] This is useful to have the unicity in Theorem 1.9.5. We do not actually need it in our proof.

$$\widetilde{g} \ : \ \mathscr{C}\left(\Gamma, \Delta\right)^G \to \mathscr{C}\left(\mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}, \widetilde{g}(\Delta)\right)^G$$

In the following, we will replace $\mathscr{C}(\Gamma, \Delta)$ by $\Gamma$ to avoid the use of heavy notation. The set $\Delta$, as we will see, plays no role in the proof.

Define $$\widetilde{g} : \left\{ \begin{array}{ccc} \Gamma^V & \to & \left(\mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}\right)^V \\ x & \mapsto & g \circ x \end{array} \right.$$

Let us show that $\widetilde{g}$ is a graph isomorphism. Take $xy \in E\left(\Gamma^G\right)$. By definition, there exists $uv \in E(G)$ such that

- $\forall w \in V \setminus \{u, v\} \quad x(w) = y(w)$
- $x(u) - y(u) \in \Delta$
- $x(u) - y(u) = y(v) - x(v)$

Observe that for every $w \in V \setminus \{u, v\}$,

$$\widetilde{g}(x)(w) = g(x(w)) = g(y(w)) = \widetilde{g}(y)(w)$$

Moreover,
$$\begin{aligned} \widetilde{g}(x)(u) - \widetilde{g}(y)(u) &= g(x(u)) - g(y(u)) \\ &= g(x(u) - y(u)) && \text{since } g \text{ is a morphism} \\ &= g(y(v) - x(v)) \\ &= g(y(v)) - g(x(v)) && \text{since } g \text{ is a morphism} \\ \widetilde{g}(x)(u) - \widetilde{g}(y)(u) &= \widetilde{g}(y)(v) - \widetilde{g}(x)(v) \end{aligned}$$

Hence, $\widetilde{g}(x)\widetilde{g}(y)$ is an edge of $\left(\mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}\right)^G$.

Conversely, observe that $\widetilde{g}^{-1} = g^{-1} \circ x$. Since $g^{-1}$ is a group morphism, it follows by what we just did that that $\widetilde{g}^{-1}$ is also a graph homomorphism.

Since what we did is true for every graph $G$, we have the following graph homomorphisms:

$$\begin{aligned} \Gamma^{\Gamma^G} &\to \left(\mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}\right)^{\Gamma^G} \\ &\to \left(\mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}\right)^{\left(\mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}\right)^G} && \text{by Prop A.1.2} \\ &\to \left(\mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_r}\right)^G \\ &\to \Gamma^G \end{aligned}$$

□

**Corollary 1.9.6.** For any finite Abelian group and any graph $G$,

$$\Gamma^{\cdot^{\cdot^{\Gamma^G}}} \to \Gamma^G$$

*Remark.* Recall that we have chosen to omit the symmetric set $\Delta$ in our notations. The symmetric set involved in the Cayley graph of the right is the image of $\Delta$ by the group isomorphism.

**Corollary 1.9.7.** Let $q$ be a non trivial power of a prime number and $G$ be a graph.

$$\mathbb{F}_q^{\cdot^{\cdot^{\mathbb{F}_q{}^G}}} \to \mathbb{F}_q{}^G$$

Recall that we always have $\chi(G) \leq \chi({\mathbb{F}_q}^G)$ because $G \subseteq {\mathbb{F}_q}^G$. However, $\chi\left({\mathbb{F}_q}^{{\mathbb{F}_q}^G}\right) \leq \chi\left({\mathbb{F}_q}^G\right)$ by Lemma 1.4.3. So, the chromatic number cannot increase by taking iterated exponents.

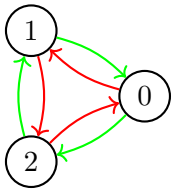
### 1.9.2 From $k$-coloring to $H$-coloring

In this section, we propose a definition of $H^G$ for any edge-labelled graph $H$ and any graph $G$. This very general definition unifies those of ${\mathbb{Z}_k}^G$ and ${\mathbb{F}_q}^G$. As we will see, the notation $H^G$ is not entirely complete as we need an edge-labelling on $H$ in order to define $H^G$. The idea is to have a similar tool as ${\mathbb{Z}_k}^G$ or ${\mathbb{F}_q}^G$ for the $H$-coloring problem that is, is there a graph homomorphism that sends $G$ to $H$. This is indeed a generalization of the $k$-coloring problem as a graph $G$ is $k$-colorable if and only if there is a graph homomorphism from $G$ to $K_k$ (see Proposition 1.9.1).

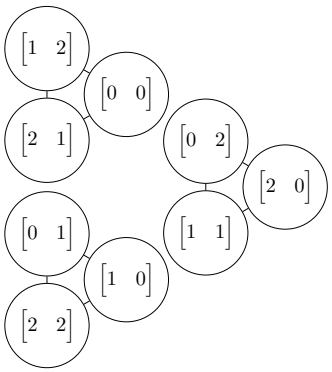
**Definition 1.9.8.** Let $H$ be a directed simple graph, $c_H$ an edge-labelling of $H$ and $G$ a graph (directed or not). We define the directed simple graph $H^G$ by:

- $V\left(H^G\right) = V(H)^{V(G)}$
- $(c, c') \in E\left(H^G\right)$ if and only if there exists $(u, v) \in E(G)$ such that
  - $\forall w \in V(G) \setminus \{u, v\} \quad c'(w) = c(w)$
  - $(c'(u), c(u)) \in E(H) \quad$ and $\quad (c(v), c'(v)) \in E(H)$
  - $c_H(c'(u), c(u)) = c_H(c(v), c'(v))$

**Example.**




(a) Some graph $H$




(b) The graph $H^{\bullet - \bullet}$

Here is how we can define ${\mathbb{Z}_k}^G$ as a special case of this general definition:

**Definition 1.9.9** (${\mathbb{Z}_k}^G$)**.** Let $k \geq 1$ be an integer. We see $K_k$ as the simple complete undirected graph on $\mathbb{Z}_k$ and $c_{K_k}$ to be the map:

$$c_{K_k} : \left\{ \begin{array}{ccc} E(K_k) & \to & \mathbb{Z}_k \\ (x,y) & \mapsto & x-y \end{array} \right.$$

**Proposition 1.9.10.** For every graph $G$, ${K_k}^G = {\mathbb{Z}_k}^G$.

Here is how we can define ${\mathbb{F}_q}^G$ as a special case of this general definition:

**Definition 1.9.11** (${\mathbb{F}_q}^G$)**.** Let $q = p^\ell$ with $\ell \in \mathbb{N}^*$ and $p$ a prime number. We define $L_q$ by

- $V(L_q) = \mathbb{F}_q$
- $(x,y) \in E(L_q) \Leftrightarrow x \neq y$
- $c_{L_q} : \left\{ \begin{array}{ccc} E(L_q) & \to & \mathbb{F}_q \\ (x,y) & \mapsto & x-y \end{array} \right.$

**Proposition 1.9.12.** For every graph $G$, ${L_q}^G = {\mathbb{F}_q}^G$.

The attentive reader may observe that in Definitions 1.9.9 and 1.9.11 are very similar. Actually, whenever $q$ is a power of a prime number, the graphs $H_q$ and $L_q$ are isomorphic. One may think that ${H_q}^G$ and ${L_q}^G$ are also isomorphic for any graph $G$ but we know by Proposition 1.4.5 that this is false. This may seem contradictory with the proof of Proposition 1.9.4 as we used, at some point, a morphism between $\Gamma$ and $\mathbb{Z}_{a_1} \times \cdots \mathbb{Z}_{a_r}$ to conclude that ${\Gamma^\Gamma}^G \to (\mathbb{Z}_{a_1} \times \cdots \mathbb{Z}_{a_r})^{{(\mathbb{Z}_{a_1} \times \cdots \mathbb{Z}_{a_r})}^G}$. It is not. Indeed, in that proof, $g$ was a group isomorphism and not only a graph homomorphism. In general, there is no group isomorphism between $\mathbb{Z}_q$ and $\mathbb{F}_q$ (except when $q$ is prime).

## 1.10 Some edge-clique certificates

In this section, we will prove some general results and then show how they can be used in order to compute edge-clique certificates in practice. First, we introduce a new concept called precolorings which are dual objects of the edge-clique certificates. Basically, a precoloring is a weight function on ${\Gamma_k}^V$ such that every edge-clique has a global weight of zero. We will show that there exists a non trivial precoloring if and only if there exists no edge-clique certificate. Moreover, we will prove that we can easily construct a basis of the linear space of precolorings which behaves well with the inner product.

**Definition 1.10.1** (precoloring)**.** Let $G = (V, E)$ be a graph and $\mathbb{K}$ be a field of characteristic $\xi$ such that $\xi \nmid k$. A function $f : {\Gamma_k}^V \to \mathbb{K}$ is a precoloring of ${\Gamma_k}^G$ in $\mathbb{K}$ if and only if

$$\forall x \in {\Gamma_k}^V \quad \forall uv \in E \qquad \sum_{\lambda \in \Gamma_k} f\left(x + \lambda\left(\mathbb{1}_u - \mathbb{1}_v\right)\right) = 0$$

In other words, $f$ sums to zero on every edge-clique.

*Remark.* Observe that if $\xi \mid k$, then the function constant to 1 sums to zero on every edge-cliques. Actually, in such case, any constant function would be a precoloring. We forbid that $\xi \mid k$ as otherwise the next Proposition would be pointless.

We will now see how precolorings are related to edge-clique certificates. The short proof of the next Proposition is enlightening. Recall that *non trivial precoloring* means a precoloring that is not the null function.

**Proposition 1.10.2.** Let $G = (V, E)$ be a graph and $\mathbb{K}$ a field of characteristic $\xi$ such that $\xi \not| k$. There exists a non trivial precoloring of ${\Gamma_k}^G$ in $\mathbb{K}$ if and only if ${\Gamma_k}^G$ has no edge-clique certificate.

*Proof.* Let $M$ be the incidence matrix of the edge-cliques of ${\Gamma_k}^G$ versus the vertices of ${\Gamma_k}^G$. Observe that $\mathrm{Ker}_{\mathbb{K}}({}^{\mathrm{t}}M)$ is the linear space of the precolorings. Moreover, by Fact A.1.13,

$$\mathrm{Ker}_{\mathbb{K}}({}^{\mathrm{t}}M) = \mathrm{Im}_{\mathbb{K}}(M)^{\perp}$$

so
$$\mathrm{Ker}_{\mathbb{K}} = \{0\} \Leftrightarrow \mathrm{Im}_{\mathbb{K}} M = \mathbb{K}^{k^{|V|}}$$

because $\langle \bullet, \bullet \rangle$ is non degenerate.

The fact that ${\Gamma_k}^G$ has no edge-clique certificate is equivalent to $\mathrm{Im}_{\mathbb{K}} M \neq \mathbb{K}^{k^{|V|}}$ so $\mathrm{Ker}_{\mathbb{K}}({}^{\mathrm{t}}M) \neq \{0\}$ hence the result. □

### 1.10.1 A basis for the precolorings in $\mathbb{F}_2$

In this section, we restrict ourselves to the case of $3^G$ with $\mathbb{K} = \mathbb{F}_2$.

Recall that a precoloring in $\mathbb{F}_2$ is a map $f : {\mathbb{F}_3}^V \to \mathbb{F}_2$ such that $f$ sums to zero on every edge-clique. The space of precolorings is the kernel of $M$, the incidence matrix of the edge-cliques versus the vertices of $3^G$. In what follows, we will provide a useful basis of the precolorings.

Consider $G = (V, E)$ to be a graph with $n \geq 1$ vertices. Let $x_1, \ldots, x_k$ be all the different directions of ${\mathbb{F}_3}^V$. We have that $k = (3^n - 1)/2$. Define

$$f^0_{x_i} : \left\{ \begin{array}{ccc} {\mathbb{F}_3}^V & \to & \mathbb{F}_2 \\ u & \mapsto & \overline{\langle u, x_i \rangle} \end{array} \right. \quad \text{and} \quad f^1_{x_i} : \left\{ \begin{array}{ccc} {\mathbb{F}_3}^V & \to & \mathbb{F}_2 \\ u & \mapsto & \overline{\langle u, x_i \rangle + 1} \end{array} \right.$$

where $\bar{\cdot} : \mathbb{F}_3 \to \mathbb{F}_2$ is the cast function from $\mathbb{F}_3$ to $\mathbb{F}_2$ defined by

$$\forall i \in \mathbb{F}_3 \qquad \bar{i} = \left\{ \begin{array}{ll} 0 & \text{if } i = 0 \\ 1 & \text{otherwise} \end{array} \right.$$

**Notation.** We denote by $\mathbf{1}$ the function constant to 1.

**Theorem 1.10.3.** The family $(\mathbf{1}, f^0_{x_1}, f^1_{x_1}, \ldots, f^0_{x_k}, f^1_{x_k})$ is a basis of the linear space of the functions from ${\mathbb{F}_3}^V$ to $\mathbb{F}_2$.

*Proof.* We will start by showing that these vectors are linearly independent. To do so, we use the inner product. Then, we prove that the family is a basis by cardinality.

First, in order to compute the inner product of any pair of vectors in that family, we introduce the notion of $z$-orbit. For $z \in {\mathbb{F}_3}^V \setminus \{0\}$, we call $z$-orbit any set $\{u, u + z, u - z\}$

where $u \in {\mathbb{F}_3}^V$. For every $u, v \in {\mathbb{F}_3}^V$, we write $u \sim_z v$ whenever $u$ and $v$ belongs to the same $z$-orbit. More formally,

$$u \sim_z v \Leftrightarrow \exists \lambda \in \mathbb{F}_3 \quad u = v + \lambda z$$

Observe that for any $z \in {\mathbb{F}_3}^V$, $\sim_z$ is an equivalence relation. Hence, the set ${\mathbb{F}_3}^V$ can be partitioned with $z$-orbits each of which having 3 elements. We can now compute the inner product between any two vectors of the family using a relevant $z$-orbit.

**Fact 1.10.4.**

i) $\langle \mathbf{1}, \mathbf{1} \rangle = 1$

ii) $\forall i \in [\![ 1 \ ; \ k ]\!] \quad \forall j \in \{0, 1\} \qquad \left\langle \mathbf{1}, f^j_{x_i} \right\rangle = 0$

iii) $\forall i, j \in [\![ 1 \ ; \ k ]\!] \qquad i \neq j \Rightarrow \left\langle f^0_{x_i}, f^0_{x_j} \right\rangle = \left\langle f^1_{x_i}, f^0_{x_j} \right\rangle = \left\langle f^0_{x_i}, f^1_{x_j} \right\rangle = \left\langle f^1_{x_i}, f^1_{x_j} \right\rangle = 0$

iv) $\forall i \in [\![ 1 \ ; \ k ]\!] \qquad \left\langle f^0_{x_i}, f^1_{x_i} \right\rangle = 1$

*Proof.* The first point is true because ${\mathbb{F}_3}^V$ has an odd number of elements since $V \neq \varnothing$. For the second one, consider $z \in {\mathbb{F}_3}^V \setminus \{x_i\}^\perp$. It is possible because $\langle \bullet, \bullet \rangle$ is non degenerate and $x_i \neq 0$ so $\{x_i\}^\perp \neq {\mathbb{F}_3}^V$. On any $z$-orbit, both $f^0_{x_i}$ and $f^1_{x_i}$ sums to zero. The point iii) can be proved using the same trick. Consider $z \perp x_i$ and $z \not\perp x_j$. Such a $z$ exists by Proposition A.1.12. On the $z$-orbits, $f^0_{x_i}$ and $f^1_{x_i}$ are constant whereas $f^0_{x_j}$ and $f^1_{x_j}$ sums to zero. Let us now detail the last point. Consider $z \perp x_i$ and $z \neq 0$. For every $u \in {\mathbb{F}_3}^V$,

$$f^0_{x_i}(u) f^1_{x_i}(u) + f^0_{x_i}(u+z) f^1_{x_i}(u+z) + f^0_{x_i}(u-z) f^1_{x_i}(u-z) = 3 f^0_{x_i}(u) f^1_{x_i}(u)$$

Moreover,

- if $\langle x_i, u \rangle = 0$, then $f^0_{x_i}(u) f^1_{x_i}(u) = 0$
- if $\langle x_i, u \rangle = 1$, then $f^0_{x_i}(u) f^1_{x_i}(u) = 1$
- if $\langle x_i, u \rangle = 2$, then $f^0_{x_i}(u) f^1_{x_i}(u) = 0$

Since there is an odd number $(3^{n-1})$ of elements $u \in {\mathbb{F}_3}^V$ such that $\langle x_i, u \rangle = 1$, we have that $\left\langle f^0_{x_i}, f^1_{x_i} \right\rangle = 1$. □

Let us show that the vectors of $(\mathbf{1}, f^0_{x_1}, f^1_{x_1}, \ldots, f^0_{x_k}, f^1_{x_k})$ are linearly independent. Let

$$g := a \cdot \mathbf{1} + \sum_{i=1}^{k} \left( a^0_i \cdot f^0_{x_i} + a^1_i \cdot f^1_{x_i} \right)$$

and assume that $g = 0$. By Fact 1.10.4, we have that

- $0 = \langle \mathbf{1}, g \rangle = a$
- $\forall i \in [\![ 1 \ ; \ k ]\!] \qquad 0 = \left\langle f^0_{x_i}, g \right\rangle = a^1_{x_i} \qquad \text{and} \qquad 0 = \left\langle f^1_{x_i}, g \right\rangle = a^0_{x_i}$

Hence, the vectors of the family $(\mathbf{1}, f^0_{x_1}, f^1_{x_1}, \ldots, f^0_{x_k}, f^1_{x_k})$ are linearly independent. Since there are $1 + 2 \times k = 3^n$ vectors, it is a basis of the linear space of the total functions from ${\mathbb{F}_3}^V$ to $\mathbb{F}_2$. □

**Corollary 1.10.5.** Consider all the colorings of $G$ among $x_1, \ldots, x_k$ say, without loss of generality, $x_1, \ldots, x_r$. The family $(f^0_{x_1}, f^1_{x_1}, \ldots, f^0_{x_r}, f^1_{x_r})$ is a basis of the precolorings.

*Proof.* Let $f$ be a precoloring. Observe that $\langle \mathbf{1}, f \rangle = 0$ since $f$ sums to zero on every edge-clique so in particular, $f$ sums to zero on any $z$-orbits where $z = \mathbb{1}_u - \mathbb{1}_v$ with $uv \in E$. Consider $i \in [\![ 1 \ ; \ k ]\!]$ such that $x_i$ is not a proper coloring of $G$. There exists $uv \in E$ such that $x_i(u) = x_i(v)$. On any edge-clique directed by $uv$, $f^0_{x_i}$ and $f^1_{x_i}$ are constant. Hence, $\left\langle f^0_{x_i}, f \right\rangle = 0 = \left\langle f^1_{x_i}, f \right\rangle$. However, if $x_i$ is a proper coloring of $G$ then $f^0_{x_i}$ and $f^1_{x_i}$ are precolorings. □

### 1.10.2 Some tools for finding edge-clique certificates

In this section, we present some results useful to study edge-clique certificates on concrete examples. First, we prove two general results that we will use to create some widgets. These widgets can be seen as elementary pieces to build an edge-clique certificate.

In the following, $M$ designates the incidence matrix of ${\mathbb{F}_3}^V$ versus the edge-cliques of $3^G$. Each column of $M$ has $3^n - 3$ zeros and 3 ones. We denote by $\mathrm{GC}_3(G)$ the set of all total functions from $V$ to $\mathbb{F}_3$ that are proper 3-colorings of $G$.

**Theorem 1.10.6.** Let $x, y$ be two distinct vertices of $G$. Define $t := -\mathbb{1}_x - \mathbb{1}_y \in {\mathbb{F}_3}^V$ and $X_t := \mathbb{1}_{\mathbb{1}_x} + \mathbb{1}_{\mathbb{1}_y} + \mathbb{1}_t \in {\mathbb{F}_2}^{{\mathbb{F}_3}^V}$. We have that

$$X_t \in \mathrm{Im}_{\mathbb{F}_2} M \Leftrightarrow \forall c \in \mathrm{GC}_3(G) \quad c(x) \neq c(y)$$

*Proof.* Let us start by proving that

$$\exists c \in \mathrm{GC}_3(G) \quad c(x) = c(y) \Rightarrow X_t \notin \mathrm{Im}_{\mathbb{F}_2} M$$

Take $c \in \mathrm{GC}_3(G)$ such that $c(x) = c(y)$. Up to permuting colors, we can assume that $c(x) = 1$. Recall that $\mathrm{Im}_{\mathbb{F}_2} M = \left(\mathrm{Ker}_{\mathbb{F}_2} {}^{\mathrm{t}}M\right)^{\perp}$ by Fact A.1.13. Moreover, $\mathrm{Ker}_{\mathbb{F}_2} {}^{\mathrm{t}}M$ is the space of all precolorings. Consider the precoloring

$$f_c : \left\{ \begin{array}{ccc} {\mathbb{F}_3}^V & \to & \mathbb{F}_2 \\ u & \mapsto & \overline{\langle c, u \rangle} \end{array} \right.$$

We have that

$$\begin{aligned} \langle f_c, X_t \rangle &= f_c(\mathbb{1}_x) + f_c(\mathbb{1}_y) + f_c(-\mathbb{1}_x - \mathbb{1}_y) \\ &= \overline{\langle c, \mathbb{1}_x \rangle} + \overline{\langle c, \mathbb{1}_y \rangle} + \overline{\langle c, -\mathbb{1}_x - \mathbb{1}_y \rangle} \\ &= \overline{c(x)} + \overline{c(y)} + \overline{-c(x) - c(y)} \\ &= 0 + \overline{c(x) + c(y)} \\ \langle f_c, X_t \rangle &= 1 \end{aligned}$$

This implies, by Fact A.1.13, that $X_t \notin \left(\mathrm{Ker}_{\mathbb{F}_2} {}^{\mathrm{t}}M\right)^{\perp}$ hence $X_t \notin \mathrm{Im}_{\mathbb{F}_2} M$.

We will now show that

$$\forall x \in \mathrm{GC}_3(G) \quad c(x) \neq c(y) \Rightarrow X_t \in \mathrm{Im}_{\mathbb{F}_2} M$$

By Corollary 1.10.5, there exists $c_1, \dots, c_r \in \mathrm{GC}_3(G)$ such that $(f^0_{c_1}, f^1_{c_1}, \dots, f^0_{c_r}, f^1_{c_r})$ is a basis of $\mathrm{Ker}_{\mathbb{F}_2}{}^{\mathrm{t}}M$.

$$\forall i \in [\![ 1 \ ; \ r ]\!] \qquad \left\langle f^0_{c_i}, X_t \right\rangle = \overline{\langle c_i, \mathbb{1}_x \rangle} + \overline{\langle c_i, \mathbb{1}_y \rangle} + \overline{\langle c_i, -\mathbb{1}_x - \mathbb{1}_y \rangle}$$

- If $c_i(x) \neq 0$ and $c_i(y) \neq 0$, then $\overline{\langle c_i, \mathbb{1}_x \rangle} = 1 = \overline{\langle c_i, \mathbb{1}_y \rangle}$ and $\overline{\langle c_i, -\mathbb{1}_x - \mathbb{1}_y \rangle} = \overline{-c_i(x) - c_i(y)} = 0$ since $c_i(x) \neq c_i(y)$.
- Otherwise, assume, without loss of generality, that $c_i(x) = 0$ and $c_i(y) \neq 0$. We have $\overline{\langle c_i, \mathbb{1}_x \rangle} = 0$, $\overline{\langle c_i, \mathbb{1}_y \rangle} = 1$ and $\overline{\langle c_i, -\mathbb{1}_x - \mathbb{1}_y \rangle} = 1$.

In both case, the sum is zero. This proves that $X_t \in \left(\mathrm{Ker}_{\mathbb{F}_2}{}^{\mathrm{t}}M\right)^{\perp}$ so $X_t \in \mathrm{Im}_{\mathbb{F}_2} M$ by Fact A.1.13.

*Remark.* If $\mathrm{Ker}_{\mathbb{F}_2}{}^{\mathrm{t}}M = \{0\}$ (which is the case if and only if the graph is not 3-colorable), then $\mathrm{Im}_{\mathbb{F}_2} M = {\mathbb{F}_2}^{{\mathbb{F}_3}^V}$ so we still have that $X_t \in \mathrm{Im}_{\mathbb{F}_2} M$.

□

*Remark.* In the particular case where $xy \in E$, the vector $X_t$ is a column of $M$.

**Proposition 1.10.7.** Let $x, y$ be two distinct vertices of $G$. For every $u \in V$, let $Y^{x,y}_u$ be the characteristic vector of the set $\{\mathbb{1}_x - \mathbb{1}_u, \mathbb{1}_y - \mathbb{1}_u\}$. Namely,

$$Y^{x,y}_u = \mathbb{1}_{\mathbb{1}_x - \mathbb{1}_v} + \mathbb{1}_{\mathbb{1}_y - \mathbb{1}_u}$$

We have that

$$\forall c \in \mathrm{GC}_3(G) \quad c(x) = c(y) \Leftrightarrow \forall u \in V \quad Y^{x,y}_u \in \mathrm{Im}_{\mathbb{F}_2} M$$

*Proof.* Recall that, by Fact A.1.13, $\mathrm{Im}_{\mathbb{F}_2} M = \left(\mathrm{Ker}_{\mathbb{F}_2}{}^{\mathrm{t}}M\right)^{\perp}$. By Corollary 1.10.5, there exists $c_1, \dots, c_r \in \mathrm{GC}_3(G)$ such that $(f^0_{c_1}, f^1_{c_1}, \dots, f^0_{c_r}, f^1_{c_r})$ is a basis of $\mathrm{Ker}_{\mathbb{F}_2}{}^{\mathrm{t}}M$. Observe that for all $c \in \mathrm{GC}_3(G)$,

$$\left\langle f^0_c, Y^{x,y}_u \right\rangle = \overline{\langle c, \mathbb{1}_x - \mathbb{1}_u \rangle} + \overline{\langle c, \mathbb{1}_y - \mathbb{1}_u \rangle} = \overline{c(x) - c(u)} + \overline{c(y) - c(u)}$$

Assume that for all $c \in \mathrm{GC}_3(G)$, $c(x) = c(y)$. Consider $c \in \mathrm{GC}_3(G)$. Since $c(x) = c(y)$, it follows that $\overline{c(x) - c(u)} = \overline{c(y) - c(u)}$ hence $\left\langle f^0_{c_i}, Y^{x,y}_u \right\rangle = 0$. The same reasoning shows that $\left\langle f^1_{c_i}, Y^{x,y}_u \right\rangle = 0$. This proves that $Y^{x,y}_u \in \mathrm{Im}_{\mathbb{F}_2} M$.

Conversely, assume that $Y^{x,y}_u \in \mathrm{Im}_{\mathbb{F}_2} M$ for every $u \in V$. Consider $c \in \mathrm{GC}_3(G)$ and fix $u \in V$. Since $\mathrm{Im}_{\mathbb{F}_2} M = \mathrm{Ker}_{\mathbb{F}_2}{}^{\mathrm{t}}M^{\perp}$, $f^0_c \perp Y^{x,y}_u$ and $f^1_c \perp Y^{x,y}_u$. Hence,

$$\overline{c(x) - c(u)} = \overline{c(y) - c(u)} \qquad \text{and} \qquad \overline{c(x) - c(u) + 1} = \overline{c(y) - c(u) + 1}$$

Assume for the sake of contradiction that $c(x) \neq c(y)$. Observe that $c(x) - c(u) \neq 0$. Indeed, since $\overline{c(x) - c(u)} = \overline{c(y) - c(u)}$, this would imply that $c(y) - c(u) = 0$ so $c(x) = c(y)$. Suppose without loss of generality that $c(x) - c(u) = 1$. Then, $c(y) - c(u) = 2$ so $\overline{c(y) - c(u) + 1} = 0$ and $\overline{c(x) - c(u) + 1} = 1$ which is a contradiction. In the end, we proved that $c(x) = c(y)$. □

### 1.10.3 Concrete examples of edge-clique certificates

In this section, we explain how to build edge-clique certificates for non 3-colorable graphs called Moser spindles. A Moser spindle is a cycle of diamond closed by an edge. Examples of such graphs are given on Figure 1.13.

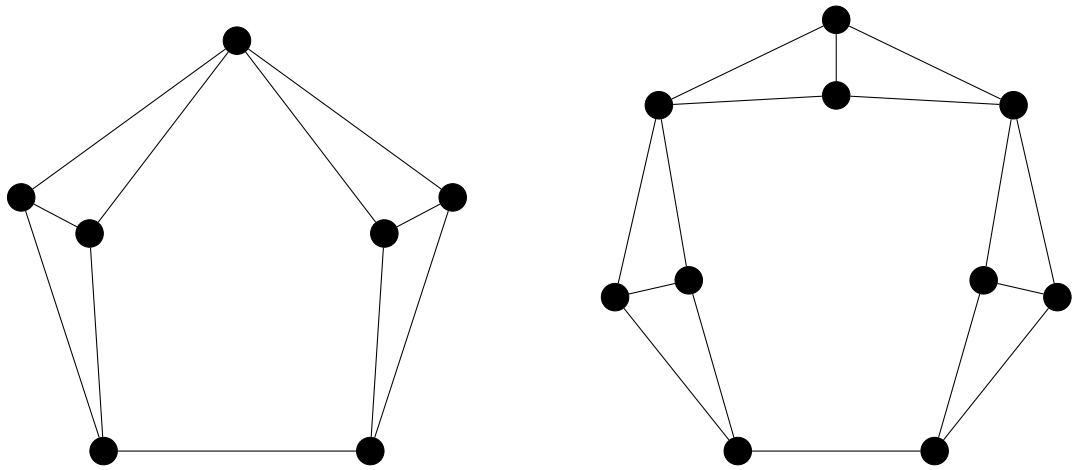


Figure 1.13: Moser Spindle

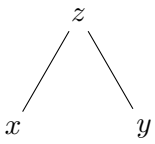
In order to explicitly give an edge-clique certificate, we start by creating two widgets. Consider a graph $G$ with 3 vertices $x, y$ and $z$. The pair $x, y$ is dominated by $z$. This means that $G$ contains the edges $xz$ and $yz$. We order the vertices lexicographically. For instance, 210 designates the vertex of $3^G$ where $x$ has weight 2, $y$ has weight 1 and $z$ has weight 0. In order to have a graphical representation of the certificate, we will use the following drawing conventions:

- For any vertex of $3^G$ with exactly one vertex $x$ weighted 2, one vertex $y$ weighted 1 and every other weighted zero, we draw an arrow from $x$ to $y$.
- For any vertex of $3^G$ with exactly $\ell$ vertices weighted 1 (resp 2), every other weighted zero, we draw a convex $\ell$-polygon whose vertices are the vertices weighted 1 with a plus inside (resp a minus).
- In the following, an edge clique will designate a weight function ${\mathbb{F}_3}^V \to \mathbb{F}_2$ that is 0 everywhere except on three aligned vertices where it is 1. Hence, summing edge cliques means summing those functions.

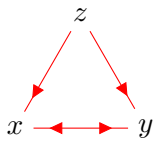
Let us sum two edge-cliques that contain 111 (so $x, y$ and $z$ all have weight 1):

$$\{111, 210, 012\} \qquad \text{and} \qquad \{111, 120, 102\}$$

The sum function is zero on 111 and 1 on the four other points (120, 102, 210, and 012). With the drawing convention stated above, we can represent this sum function (called widget) by Figure 1.14b.




(a) dominated pair

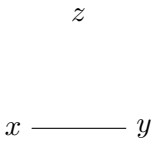



(b) widget 1

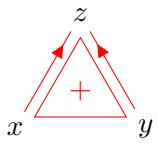
Figure 1.14: Widget 1

Consider now an edge $xy$ plus an isolated vertex $z$. We can build the following widget thanks to the edge-clique

$$\{111, 201, 021\}$$



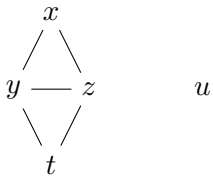

(a) edge



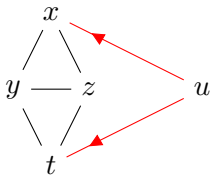

(b) widget 2

Figure 1.15: Widget 2

Let us now give a way to create a last widget. Consider a diamond plus an isolated vertex $u$ as in Figure 1.16. Observe that every 3-coloring $c$ of this diamond satisfies $c(x) = c(t)$. Hence, by Proposition 1.10.7, we can build the widget represented on Figure 1.15. However, this proposition does not tell how to build such widget. In particular, we don't know how many edge-clique are involved and what is the minimal support.




(a) diamond plus vertex




(b) widget 3

Figure 1.16: Widget 3

Here is how we can build this widget. Consider the 8 following edge-cliques. We have written the directions on the right.

$$\begin{array}{ll} \{22002, 10002, 01002\} & xy \\ \{22002, 21102, 20202\} & yz \\ \\ \{11202, 02202, 20202\} & xy \\ \{11202, 01002, 21102\} & xz \\ \\ \{02022, 01002, 00012\} & yt \\ \{02022, 01122, 00222\} & yz \\ \\ \{01212, 01122, 01002\} & zt \\ \{01212, 00222, 02202\} & yt \end{array}$$

After summing those 8 edge-clique in $\mathbb{F}_2$, we are left with 10002 and 00012 which corresponds to the drawing on Figure 1.16.

Let us see how we can apply this result. In what follows, we will produce an edge-clique certificate for the Moser spindle graph with two diamonds. The proof can easily be generalized for any Moser spindle. In order to make it simpler, let us add a new isolated vertex that we call $u$. This is represented on Figure 1.17.

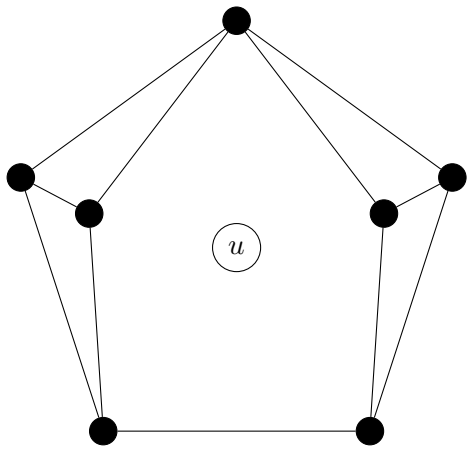



Figure 1.17: Moser Spindle

Let us sum two diamond widgets as described in Figure 1.18.

In order to conclude, one just has to use the "edge-widget" (see Figure 1.14b). In the end, we have only one point in $3^G$ with non zero coordinates: $\mathbb{1}_{u,5,6}$. This is the center of the edge-clique certificate.

Can we get rid of vertex $u$? Observe that removing $u$ does not remove any edge-clique since $u$ is isolated. Hence, projecting the edge-clique certificate on ${\mathbb{F}_2}^{V\setminus\{u\}}$ gives an edge-clique certificate for the initial graph.

Let us see how to build an edge-clique certificate for an odd wheel. For every triangle,

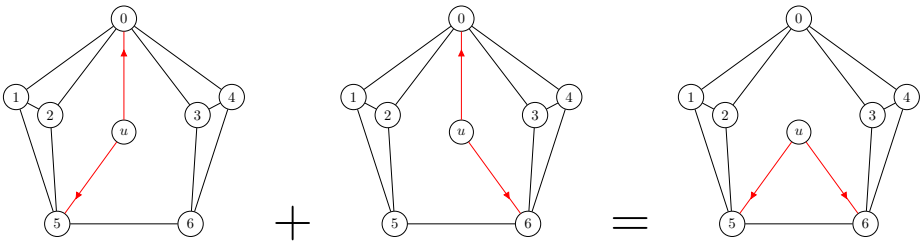
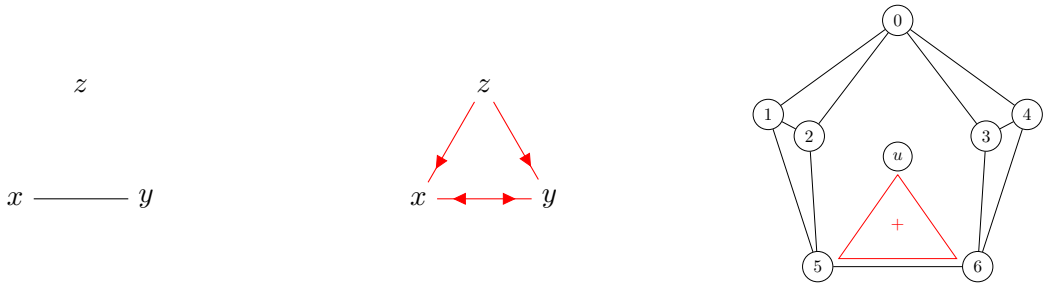
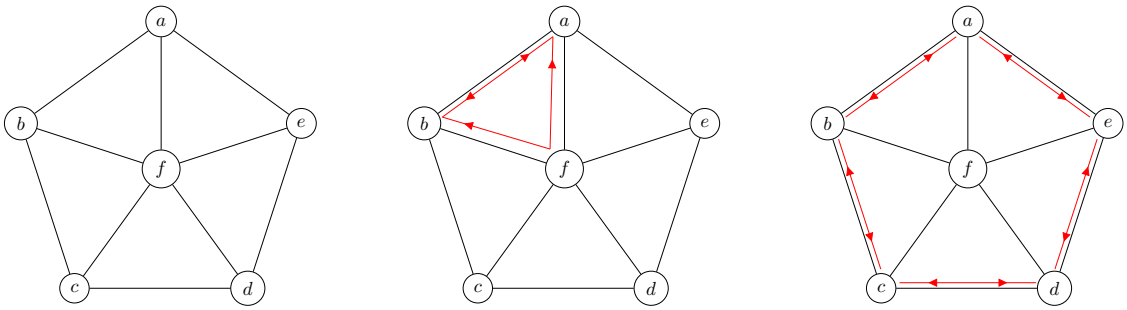



Figure 1.18: Sum of two diamond widgets




we use the widget 1. Summing those 5 widgets gives a cycle of double red arrows because the arrows along the radius cancel mod 2 (see Figure 1.19).




(a) The graph $W_5$ (b) Widget 1 (c) Sum

Figure 1.19: Building an edge-clique certificate for a wheel

Finally, observe that for any edge $uv$, the $(\mathbb{1}_u - \mathbb{1}_v)$-line containing the zero of ${\mathbb{F}_3}^V$ creates a double red arrow between $u$ and $v$ and put weight 1 on zero. Hence, we can cancel this cycle of double red arrows and retrieve weight $1+1+1+1+1=1$ on zero which is the center of our edge-clique certificate.

*Remark.* We used every edges of the odd wheel. It was expected since such graph is edge-critical: removing any edge make it 3-colorable.

### 1.10.4 Edge-clique certificates and homology

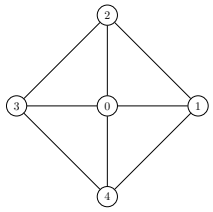
In this section, we discuss the link between coloring and homology. To do so, we need first to associate a simplicial complex to every graph. This can be done thanks to the concept of dominated pairs, dominated triples and more generally, dominated $n$-uples. Basically, a dominated *$n$-uple* is a set of $n$ vertices that are all linked to another one. Under some hypothesis on the $n$-uples, we can prove lower bounds on the chromatic number. If this lower bound is tight ($\chi(G)-1$), we say that the graph is not $\chi(G)-1$-colorable for *homological reasons*. For 3-colorable graphs that are not 4-colorable for homological reasons, we proved that there exists an edge-clique certificate of minimal degree. The converse is an open question, as for the general problem of $k$-coloring.

**Definition 1.10.8.** Let $G$ be a graph. For any integer $n \in \mathbb{N}$, we define

$$D_n = \left\{ \{x_1, \ldots, x_n\} \in \tbinom{V}{n} \colon \exists d \in V \quad \forall i \in [\![ 1 \ ; \ n ]\!] \qquad dx_i \in E \right\}$$

In other words, $D_n$ is the set of subsets of size $n$ of vertices that have a common neighbour. We call the elements of $D_n$ *dominated $n$-sets*. When $n = 3$, we call it a *dominated pair* and when $n = 3$, a *dominated triple*.

**Example 1.10.9.**




(a) The graph $W_4$

$D_0 = \{\varnothing\}$
$D_1 = \{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}\}$
$D_2 = \{\{01\}, \{02\}, \{03\}, \{04\}, \{12\}, \{13\}, \{14\}, \{23\}, \{24\}, \{34\}\}$
$D_3 = \{\{013\}, \{024\}, \{123\}, \{124\}, \{134\}, \{234\}\}$
$D_4 = \{\{1234\}\}$
$D_5 = \varnothing$

Figure 1.20: The graph $W_4$ and its dominated sets

Observe that in a dominated $(n+1)$-set, there are $n+1$ dominated $n$-sets.

*Remark.* The set $\{D_n \colon n \in \mathbb{N}\}$ is called the neighborhood complex of $G$.

For every $n \geq 1$ such that $D_n \neq \varnothing$ and $D_{n-1} \neq \varnothing$, let us define $M_n$ to be the incidence matrix of $D_{n-1}$ versus $D_n$.

**Example 1.10.10.** Here are the matrices $M_2$ and $M_3$ for the graph $W_4$ represented on Figure 1.20a.

$$M_2 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccccccccc} 01 & 02 & 03 & 04 & 12 & 13 & 14 & 23 & 24 & 34 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

$$M_3 = \begin{array}{c} \\ 01 \\ 02 \\ 03 \\ 04 \\ 12 \\ 13 \\ 14 \\ 23 \\ 24 \\ 34 \end{array} \begin{array}{c} \begin{array}{cccccc} 013 & 024 & 123 & 124 & 134 & 234 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

*Remark.*

- We have that[16] $D_0 = \{\varnothing\}$.
- If $G$ has no isolated vertex, then $D_1 = V$. In such a case, $M_1$ is a row matrix of size $|V|$ that is full of 1's.

In the following, we consider $\mathbb{F}_2$ for the ground field of every matrices. Hence, we simply write $\operatorname{Im} M$ for $\operatorname{Im}_{\mathbb{F}_2} M$ and $\operatorname{Ker} M$ for $\operatorname{Ker}_{\mathbb{F}_2} M$.

**Proposition 1.10.11.** For every $n \geq 2$ such that $M_n$ is defined, we have that

$$M_{n-1} \times M_n = 0$$

*Proof.* Consider a row of $M_{n-1}$ and a column of $M_n$. Our goal is to prove that the inner product (in $\mathbb{F}_2$) of this row and this column is zero. The row of $M_{n-1}$ is indexed by a dominated $(n-2)$-set $\{x_1, \ldots, x_{n-2}\}$. If the dominated $n$-set that is the index of the column of $M_n$ we consider does not contain $\{x_1, \ldots, x_{n-2}\}$, then the inner product is a sum of zeros. Otherwise, let us denote by $\{x_1, \ldots, x_{n-2}, x_{n-1}, x_n\}$ the dominated $n$-set that is the index of the column of $M_n$ that we consider. We have that $\{x_1, \ldots, x_{n-2}, x_{n-1}\}$ and $\{x_1, \ldots, x_{n-2}, x_n\}$ are dominated $(n-1)$-sets. Hence, in the sum defining the inner product, there are exactly two 1's. □

*Remark.* We proved something a bit stronger: there are either zero 1's or exactly two 1's in the sum defining the product of a row of $M_{n-1}$ by a column of $M_n$.

So we know that $\operatorname{Im} M_n \subseteq \operatorname{Ker} M_{n-1}$. In the following, we are interested in the case where this inclusion is an equality. For every $n \geq 1$ such that $M_n$ is defined, let $H_n$ be the property

$$\forall i \in [\![ 1 \ ; \ n ]\!] \qquad \operatorname{Im} M_i = \operatorname{Ker} M_{i-1}$$

[16] Except if $V = \varnothing$, then $D_0 = \varnothing$.

To illustrate this, let us give an interpretation of the properties $H_2$ and $H_3$.

1. The property $H_2$ expresses the fact that the graph $(D_1, D_2)$ is connected.
2. The property $H_3$ expresses the fact that any cycle of dominated pairs can be obtained by a sum (in $\mathbb{F}_2$) of dominated triples.

Indeed, $\operatorname{Ker} M_1$ is the set of weight functions $w$ from $D_1$ to $\mathbb{F}_2$ that sums to zero *i.e* so that $\sum_{v \in D_1} w(v) = 0$. Moreover, $\operatorname{Im} M_2$ is the linear space generated by the set of weight functions $w$ from $D_1$ to $\mathbb{F}_2$ so that $w$ is zero everywhere except on $x$ and $y$ so that $xy$ is a dominated pair. Observe that indeed, $\operatorname{Im} M_2 \subseteq \operatorname{Ker} M_1$. If $(D_1, D_2)$ is connected then $\operatorname{Ker} M_1 \subseteq \operatorname{Im} M_2$ and under the hypothesis that $\operatorname{Ker} M_1 \subseteq \operatorname{Im} M_2$, then $(D_1, D_2)$ is connected.

The following result is not new. However, in order to generalize it, we wanted to find an algebraic proof. Surprisingly, we found a proof that does not rely on the underlying graph.

**Proposition 1.10.12.** If $H_2$ (and thus $H_1$) holds for graph $G$, then $\chi(G) \geq 3$.

*Proof.* Let $G$ be a connected graph such that properties $H_1$ and $H_2$ hold. First, observe that implicitly, the fact that matrix $M_1$ is defined tells us that $D_1 \neq \varnothing$. Hence, $\chi(G) \geq 2$. Moreover, we can assume without loss of generality that $G$ has no isolated vertex so that $D_1 = V$. Assume for the sake of contradiction that there exists a 2-coloring for $G$. Without loss of generality, we can assume the colors to be the elements of ${\mathbb{F}_2}^2$ $(0,1)$ and $(1,0)$. Let $c : D_1 \to {\mathbb{F}_2}^2$ be such a coloring. We can naturally extend $c$ to a linear map from ${\mathbb{F}_2}^n$ to ${\mathbb{F}_2}^2$. To do so, we define $L_c : {\mathbb{F}_2}^n \to {\mathbb{F}_2}^2$ to be the unique linear map such that

$$\forall v \in V \qquad L_c(\mathbb{1}_v) = c(v)$$

Let us denote by $C$ the matrix of $L_c$ in the canonical basis (that is the basis of ${\mathbb{F}_2}^n$ composed by the vectors of the form $\mathbb{1}_v$ for every $v \in V$). Since $\chi(G) \geq 2$, the rank of $C$ must be at least 2.

Observe that $CM_2 = 0$. Indeed, given a dominated pair, its two vertices must have the same color. So, $\operatorname{Im} M_2 \subseteq \operatorname{Ker} C$.

Thanks to the rank theorem, $\operatorname{rk} c = n - \dim(\operatorname{Ker} c)$

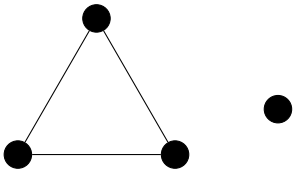
However, the hypothesis $H_2$ implies

$$\operatorname{rk} M_2 = \dim(\operatorname{Ker} M_1) = \operatorname{rk} M_1 - 1 = n - 1$$

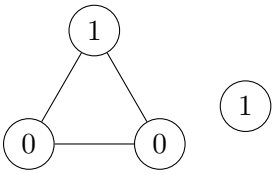
Hence, $\operatorname{rk} c \leq 1$ which is absurd. □

If the bound of Proposition 1.10.12 is tight, we say that $G$ is not 2-colorable (*i.e* not bipartite) *for homological reasons*.

One can wonder whether a non bipartite graph is always non bipartite for homological reasons. The answer is "no" in general. Consider for instance the graph on Figure 1.21a. It is non bipartite but the weight distribution represented on Figure 1.21b cannot be obtained by a sum (in $\mathbb{F}_2$) of dominated pairs. However, this is a not relevant as the graph is not connected: we used the part of the graph this is bipartite to argue that $\operatorname{Ker} M_1 \not\subseteq \operatorname{Im} M_2$. The answer is "yes" for connected non bipartite graph.



(a) Some non bipartite graph




(b) Some weight function in $\operatorname{Ker} M_1 \setminus \operatorname{Im} M_2$

Figure 1.21: Non connected graphs can be non bipartite not for homological reasons

**Proposition 1.10.13.** For every connected graph $G$, if $G$ is not bipartite, then it is for homological reasons.

*Proof.* First, observe that the square of an odd cycle is an odd cycle of the same length. Our goal is to show that for every vertex $v$ of $V = D_1$, there exists a path in $(D_1, D_2)$ that connects $v$ to an odd cycle. Since the graph is connected an non bipartite, we know that there exists an odd cycle. Let $C$ be a closest odd cycle for $v$ in $G$.

- If $v \in V(C)$, there is nothing to do.
- Otherwise, there exists a path of odd length (we count the vertices) that connects $v$ to a vertex $c$ of $C$. The dominated pairs of this path is a path from $v$ to $c$ in $(D_1, D_2)$.

Hence, $(D_1, D_2)$ is connected so the property $H_2$ is true for $G$. □

**Proposition 1.10.14.** If $H_3$ holds (and thus $H_2$ and $H_1$) for the graph $G$, then $\chi(G) \geq 4$. Moreover, $G$ has a Nullstellensatz certificate of degree 3.

*Proof.* Let $G$ be a connected graph and let us assume that $H_1$, $H_2$ and $H_3$ hold for $G$. Thanks to Proposition 1.10.12 we know that $\chi(G) \geq 3$ so in particular, $G$ has an odd cycle, say $v_0, \ldots, v_{2\ell}$.

Our goal is to find an edge-clique certificate for $3^G$ in $\mathbb{F}_2$. To do so, we will use the fact that every cycle of dominated pairs is a sum of dominated triples (this is the hypothesis $H_3$). We will use the monomial notation from section 1.5 for the vertices of $3^G$. First, recall that for every dominated pair $xy$, we have the widget of Figure 1.14. Consider now a dominated triple $xyz$. Since such dominated triple contains three dominated pair, we can build the widget represented on Figure 1.22.

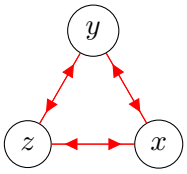
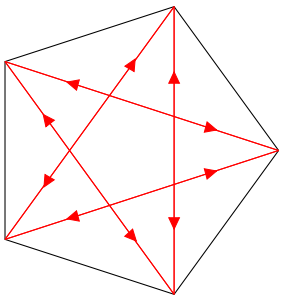
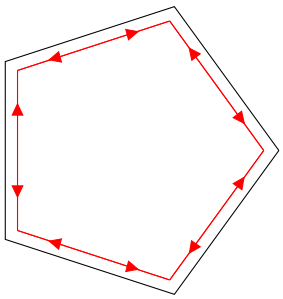



Figure 1.22: Widget given by a dominated triple

Now observe that the square of an odd cycle is a cycle of dominated pairs of same length. Hence, thanks to the hypothesis $H_3$, it is a sum of dominated triples. This gives us the widget drawn on Figure 1.23a (we took a $C_5$ for the example). For every dominated pair, we use the dominated pair widget (Figure 1.14). In the end, we have the pattern drawn on Figure 1.23b.



(a) Widget given by the square of a $C_5$



(b) Remaining widget

Figure 1.23: Widget for a graph $G$ with a $C_5$ so that $G$ satisfies $H_3$

Observe that for every $i \in [\![ 0 \ ; \ 2\ell ]\!]$, the set $\{1, x_i x_{i+1}{}^2, x_i{}^2 x_{i+1}\}$ is an edge-clique (we consider the indices modulo $2\ell$). Hence, by summing all these edge-cliques along the cycle, the only vertex with non zero weight is the vertex 1 (every vertices of the cycle cancel modulo 2 and there are an odd number of edge-cliques so, in the end, only vertex 1 remains). This means there is an edge-clique certificate in $3^G$ whose center is 1.

Moreover, all the monomials used in the proof are of degree 3. Hence, in the end, the corresponding Nullstellensatz certificate has degree 3. □

Notice that this proof relies on a particular structure within the graph that is the square of an odd cycle. This is a problem because one cannot use the same technique if one wants to show that $H_4(G) \Rightarrow \chi(G) \geq 5$. Indeed, there is no standard certificate of non 3-colorability. Unfortunately, we did not manage to find out an algebraic proof as for Proposition 1.10.14.

As for Proposition 1.10.12, we say that $G$ is not 3-colorable for *homological reasons* whenever $H_3(G)$ holds. However, contrary to what we proved in Proposition 1.10.13, there exists graphs that not 3-colorable but this is not for homological reasons. One of the simplest we can think about (we found it in [6]) is the so called Moser Spindle graph (see Figure 1.13).

## 1.11 From the Nullstellensatz to Fourier

Let us consider the ring

$$\mathbb{C}_{k,n} = \frac{\mathbb{C}[X_1, \ldots, X_n]}{\left\langle {X_i}^k - 1 \right\rangle_{i \in [\![ 1 \ ; \ n ]\!]}}$$

as defined in Section 1.5. Recall that for any graph $G = (V, E)$, the polynomials defined for every $ij \in E$ by

$$P_{ij} = \frac{{X_i}^k - {X_j}^k}{X_i - X_j}$$

have no common root in ${\mathbb{U}_k}^n$ if and only if $G$ is not $k$-colorable. Let us assume that for every $x \in {\mathbb{U}_k}^n$, there exists an element of $\mathbb{C}_{k,n}$, say $\phi_{k,n}(x)$, such that

$$\forall y \in {\mathbb{U}_k}^n \qquad \phi_{k,n}(x)(y) = \begin{cases} 1 & \text{if} \quad x = y \\ 0 & \text{otherwise} \end{cases}$$

We will see in Proposition 2.2.18 that it is indeed the case. Moreover, we will see in Corollary 2.2.19 that the image of $P \in \ \mathbb{C}_{k,n}$ on ${\mathbb{U}_k}^n$ fully characterizes $P$. Thanks to those results, we can make an elementary proof of the Nullstellensatz theorem in the specific case we are interested in.

For any $P \in \mathbb{C}_{k,n}$, define $\sup P$ to be the set of elements of ${\mathbb{U}_k}^n$ on which $P$ is not null. More formally,

$$\sup P = \{x \in {\mathbb{U}_k}^n \colon P(x) \neq 0\}$$

Define

$$P = \sum_{ij \in E} \sum_{y \in \sup P_{ij}} \phi_{k,n}(y)$$

and observe that $P \in \langle P_{ij} \rangle_{ij \in E}$. Indeed,

$$\forall x \in {\mathbb{U}_k}^n \qquad P(x) = \sum_{ij \in E} P_{ij}(x) \sum_{y \in \sup P_{ij}} \frac{1}{P_{ij}(y)} \phi_{k,n}(y)(x)$$

so, by unicity (see Corollary 2.2.19),

$$P = \sum_{ij \in E} P_{ij} \sum_{y \in \sup P_{ij}} \frac{1}{P_{ij}(y)} \phi_{k,n}(y)$$

which proves that $P \in \langle P_{ij} \rangle_{ij \in E}$. Moreover,

$$\sup P = \bigcup_{ij \in E} \sup P_{ij} = {\mathbb{U}_k}^n \setminus \mathrm{GC}_k(G)$$

Indeed, for every $x \in {\mathbb{U}_k}^n$,

$$\begin{aligned} P(x) &= \sum_{ij \in E} \sum_{y \in \sup P_{ij}} \phi_{k,n}(y)(x) \\ &= \sum_{ij \in E} \sum_{y \in \sup P_{ij}} \delta_y(x) \\ &= \sum_{ij \in E} \mathbb{1}_{\sup P_{ij}}(x) \end{aligned}$$

and as we have seen in 1.5, $\bigcap_{ij \in E} ({\mathbb{U}_k}^n \setminus \sup P_{ij}) = \mathrm{GC}_k(G)$

Now, we will prove that there exists a Nullstellensatz certificate in $\mathbb{C}_{k,n}$ for the $P_{ij}$'s if and only if $G$ is not $k$-colorable. We have that

$$\begin{aligned}\mathrm{GC}_k(G) = \varnothing &\Leftrightarrow \sup P = {\mathbb{U}_k}^n \\ &\Leftrightarrow P \times \sum_{x \in \sup P} \frac{1}{P(x)} \phi_{k,n}(x) = 1 \quad \text{(by unicity (2.2.19))} \\ &\Leftrightarrow 1 \in \langle P_{ij} \rangle_{ij \in E}\end{aligned}$$

For the last equivalence, if $1 \in \langle P_{ij} \rangle_{ij \in E}$, then $\bigcup_{ij \in E} \sup P_{ij} = {\mathbb{U}_k}^n$ and so $\sup P = {\mathbb{U}_k}^n$. Actually we can even derive a Nullstellensatz certificate if we push the calculus a bit further. Under the hypothesis that $G$ is not $k$-colorable, we have that

$$\begin{aligned}1 &= P \times \sum_{x \in {\mathbb{U}_k}^n} \frac{1}{P(x)} \phi_{k,n}(x) \\ &= \sum_{ij \in E} P_{ij} \sum_{y \in \sup P_{ij}} \frac{1}{P_{ij}(y)} \phi_{k,n}(y) \times \sum_{x \in {\mathbb{U}_k}^n} \frac{1}{P(x)} \phi_{k,n}(x) \\ &= \sum_{ij \in E} P_{ij} \times \left( \sum_{y \in \sup P_{ij}} \frac{1}{P_{ij}(y)} \phi_{k,n}(y) \sum_{x \in {\mathbb{U}_k}^n} \frac{1}{P(x)} \phi_{k,n}(x) \right) \\ 1 &= \sum_{ij \in E} P_{ij} \times \left( \sum_{y \in \sup P_{ij}(y)} \frac{1}{P(y) P_{ij}(y)} \phi_{k,n}(y) \right)\end{aligned}$$

since $\phi_{k,n}(x) \times \phi_{k,n}(y) = \delta_y(x) \phi_{k,n}(x)$ by Proposition 2.2.18. Hence,

$$1 = \sum_{ij \in E} P_{ij} \times \left( \sum_{y \in \sup P_{ij}} \frac{1}{P_{ij}(y) \left| \{ \ell p \in E \colon P_{\ell m}(y) \neq 0 \} \right|} \phi_{k,n}(y) \right)$$

So, we have that $\sum_{ij \in E} P_{ij} Q_{ij} = 1$ with

$$Q_{ij} = \sum_{y \in \sup P_{ij}} \frac{1}{P_{ij}(y) \left| \{ \ell p \in E \colon P_{\ell m}(y) \neq 0 \} \right|} \phi_{k,n}(y)$$

*Remark.* Observe that $\{ \ell p \in E \colon P_{\ell p}(y) \neq 0 \}$ is the set of edges that are not well colored by $y$.

*Remark.* We did not use the algebraic expression of the $P_{ij}$'s nor did we used the good colorings! This is because what we have done is generic: it works for any system of polynomial equation in $\mathbb{C}_{k,n}$. It actually works in any field of characteristic zero and with $k^{\text{th}}$ roots of unity.

One can wonder how we could effectively compute $Q_{ij}$. With the expression we just gave, it suffices to know the decomposition of $\phi_{k,n}(y)$ on the basis $\mathcal{M}$ for every $y \in {\mathbb{U}_k}^n \setminus \mathrm{GC}_k(G)$. Let us emphasize here that there are two natural ways to represent an element of $\mathbb{C}_{k,n}$. First, we can give its coordinates on the basis $\mathcal{M}$. For an element $Q \in \mathbb{C}_{k,n}$, this corresponds to the vector $\mathcal{M}^*(Q)$ defined by

$$\mathcal{M}^*(Q) = [X^*(Q)]_{X \in \mathcal{M}}$$

where $X^*(Q)$ is the coefficient of the monomial $X$ in $Q$.

*Remark.* We implicitly assume the lexicographic order here.

There is, however, another natural way to fully describe an element $Q \in \mathbb{C}_{k,n}$. Indeed, we know by Corollary 2.2.19 that an element of $\mathbb{C}_{k,n}$ is characterized by its image on ${\mathbb{U}_k}^n$. Hence, $Q$ can be represented by the vector $\mathrm{I}(Q)$ defined by

$$\mathrm{I}(Q) = [Q(x)]_{x \in {\mathbb{U}_k}^n}$$

*Remark.* Again, we do not specify the order of the rows here. In practice, the lexicographic order of the exponents is useful.

Observe that $\phi_{k,n}(y)$ is easy to describe with the latter way but the values of the former, that are given by $\mathcal{M}^*(\phi_{k,n}(y))$, are unclear. Let us see how we can compute this last vector. Given an element $Q \in \mathbb{C}_{k,n}$, we would like a way to go from $\mathrm{I}(Q)$ to $\mathcal{M}^*(Q)$. To do so, it is natural to introduce a matrix whose rows are the vectors $\mathrm{I}(X)$ for $X \in \mathcal{M}$. Let us define $F'_{k,n}$ by

$$F'_{k,n} = [\mathrm{I}(X)(x)]_{(X,x) \in \mathcal{M} \times {\mathbb{U}_k}^n}$$

**Example.** With $k = n = 2$, we have that

$$F'_{2,2} = \begin{array}{c} \begin{matrix} (1,1) & (1,-1) & (-1,1) & (1,1) \end{matrix} \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \end{array} \begin{matrix} 1 \\ Y \\ X \\ XY \end{matrix}$$

*Remark.* We used the lexicographic order on the exponent of the elements of ${\mathbb{U}_2}^2$. For instance, $(1,1) < (1,-1)$ since $(1,1) = ((-1)^0, (-1)^0)$ and $(1,-1) = ((-1)^0, (-1)^1)$. This is the same for the rows, we use the fact that $X = X^1Y^0$ and $Y = X^0Y^1$ so $X$ comes after $Y$.

Such matrices have nice properties. In particular, up to renormalization they are unitary. This is why we prefer to define $F_{k,n}$ by

$$F_{k,n} = \frac{1}{\sqrt{k}^n} \, [\mathrm{I}(X)(x)]_{(X,x) \in \mathcal{M} \times {\mathbb{U}_k}^n}$$

This is why we will study how to use those matrices for graph coloring problems in the next section.

Now $\mathcal{M}^*(\phi_{k,n}(y))$ is nothing but the transpose of the row of $F_{k,n}$ that corresponds to $y$ (up to the renormalization coefficient $\sqrt{k}^n$). By linearity,

$$\mathcal{M}^*(P) = \sum_{ij \in E} \sum_{y \in \sup P_{ij}} \mathcal{M}^*(\phi_{k,n})(y)$$

So, $G$ is not $k$-colorable if and only if $\sup P = {\mathbb{U}_k}^n$.

# Chapter 2

# Fourier analysis on graphs

In this chapter, we present a new method to prove combinatorial results. This technique relies on some kind of discrete Fourier transform and can be applied to a bunch of problems: existence of a $k$-coloring, existence of a perfect matching, of a large enough stable set etc. First, we illustrate how this proof method works in Section 2.1 by proving some simple and already known results. Namely, we show the existence of a cycle factor in 4-regular graphs. In a nutshell, the idea is to come up with an inner product of two vectors which is not null if and only if a solution exists and then to argue that the inner product is indeed not null. This can often be done in numerous ways, some being more clever than others which makes this part of the proof quite challenging. Then, the beautiful idea is to change the inner product using a Fourier matrix. Such matrix being unitary, the result of the inner product is the same. However, this allows us to have a completely different viewpoint on the problem since the vectors involved in the inner product are now the *Fourier transform* of the original vectors. This proof sketch is completely new and in our opinion, quite promising even though we do not have breakthrough results yet. Even so, we came up with a new proof of the cycle + triangle conjecture (see [16], [30] and 2.3.1) thanks to this method. The proof is very short once the reader has assimilated our theory. Surprisingly, some simple results like Petersen's theorem on the existence of a perfect matching in a bridgeless cubic graph (see [29]) seem to be very difficult to prove even though our proof sketch can easily be applied. Finally, our method is non constructive in the sense that it only proves that objects (3-colorings, perfect matchings etc.) exist but one cannot build such objects with to the Fourier proof.

## 2.1 Introductive problems

In this section, we will prove the existence of a cycle factor for some class of graphs. The purpose is not the results themselves (they are already known and even quite easy to show) but the proof sketch. Indeed, the proof method we invented, say the "Fourier method", can be applied to many combinatorial problems (existence of a perfect matching, of a cycle factor, of a 3-coloring etc.). This section should help the reader to understand what is the

scope of application for our Fourier method. We try to keep the examples as simple as possible by deferring calculus in appendix.

**Proposition 2.1.1.** Every 4-regular bipartite graph has a cycle factor.

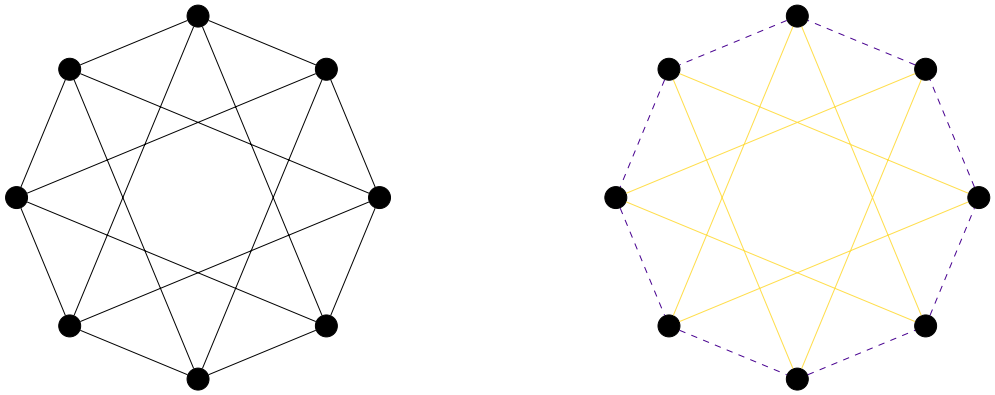


Figure 2.1: The complete bipartite graph $K_{4,4}$ and a cycle factor in dotted purple

The usual proof is straightforward. Since every vertex of $G$ has even degree, there exists an Eulerian circuit for each connected component, hence an Eulerian orientation. Consider all edges that are oriented from one side of the bipartition to the other: it gives disjoint union of cycles that span the vertex set. More generally, Petersen proved in [29] that every $2k$-regular graph has a factorization into two $k$-factors.

Despite this result is not new, we will now see how to prove it using our Fourier method. This will be a good illustration of how Fourier based proofs work. In the following proof, we will not write every calculus details (this can be found in Appendix, see C.1.1) as the purpose is only to indicate what is our sketch proof. One can wonder why we took the strong hypothesis of $G$ being 4-regular (instead of simply $G$ being Eulerian). This is to be able the use some tensor product. It will become clear in the proof.

*Proof.* Let $G = (A \uplus B, E)$ be a 4-regular bipartite graph. Our goal is to show that there exists a choice of edges such that every vertex has exactly 2 chosen edges. More formally, we want to prove that there exists $x : E \to \mathbb{F}_2$ such that

$$\forall v \in V \quad |\{e \in E : v \in e \wedge x(e) = 1\}| = 2 \tag{2.1}$$

The idea is to split the constraints among the bipartition. This is fundamental when it comes to Fourier based proof because we need an inner product somewhere. So, let us define two functions $f_A, f_B : {\mathbb{F}_2}^E \to \mathbb{C}$ by

$$\forall x \in {\mathbb{F}_2}^E \qquad f_A(x) = \begin{cases} 1 & \text{if} \quad \forall v \in A \quad |\{e \in E : v \in e \wedge x(e) = 1\}| = 2 \\ 0 & \text{otherwise} \end{cases}$$

and $$\forall x \in {\mathbb{F}_2}^E \qquad f_B(x) = \begin{cases} 1 & \text{if} \quad \forall v \in B \quad |\{e \in E : v \in e \wedge x(e) = 1\}| = 2 \\ 0 & \text{otherwise} \end{cases}$$

There exists a function $x$ that fulfills the condition 2.1 if and only if $\langle f_A, f_B\rangle \neq 0$. Actually, $\langle f_A, f_B\rangle$ is exactly the number of such functions hence the number of cycle factors.

However, computing directly this inner product seems to be of little interest as it is exactly the same than just counting the cycle factors. Rather than doing this, we will change the inner product using a unitary matrix. We choose a specific one, the Fourier matrix. We will see later why this choice is sound. Essentially, this is because Fourier behave well with the tensor product. Hence, the idea is to compute $\left\langle \widehat{f_A}, \widehat{f_B}\right\rangle$ instead of $\langle f_A, f_B\rangle$ where the $\widehat{\cdot}$ symbol designates the result of the matrix vector product of an appropriate Fourier matrix and $f_A$. This idea is the core of our Fourier method. By changing the inner product, we now have a completely different viewpoint on the sum used for the inner product. Our hope is then to find a simple argument to justify that this inner product is not zero.

The details of the computation of $\widehat{f_A}$ and $\widehat{f_B}$ are not relevant in this introduction. They can be found in appendix in the detailed proof of Prop C.1.1. However, we will now explain the method used.

Obviously, we cannot compute directly a matrix vector product of the Fourier matrix and $f_A$ as the size of $f_A$ is a variable (It is equal to $2^{2n}$ where $n$ is the number of vertices of $G$.). So, the idea is first to compute $\widehat{f_{A_1}}$ where $f_{A_1}$ is the function $f_A$ in the particular case where $|A| = 1$. Then observe that $f_A = {f_{A_1}}^{\otimes n/2}$. Since Fourier matrices behave well with tensor product, we have that $\widehat{f_A} = \widehat{f_{A_1}}^{\otimes n/2}$ which gives

$$\forall x \in {\mathbb{F}_2}^E\ \widehat{f_A}(x) = \begin{cases} \frac{1}{2^n}\, 6^{|A_0(x)|+|A_4(x)|}(-2)^{|A_2(x)|} & \text{if } \forall v \in A\, v \in A_0(x) \cup A_2(x) \cup A_4(x) \\ 0 & \text{otherwise} \end{cases}$$

where for every $i \in [\![ 0\ ;\ 4 ]\!]$, $A_i(x)$ is the set of vertices of degree $i$ in $x$. More formally,

$$A_i(x) := \{v \in A\colon\ |\{e \in E\colon v \in e \wedge x(e) = 1\}| = i\}$$

Since $A$ and $B$ plays symmetric roles, we have that

$$\forall x \in {\mathbb{F}_2}^E\ \widehat{f_B}(x) = \begin{cases} \frac{1}{2^n}\, 6^{|B_0(x)|+|B_4(x)|}(-2)^{|B_2(x)|} & \text{if } \forall v \in B\, v \in B_0(x) \cup B_2(x) \cup B_4(x) \\ 0 & \text{otherwise} \end{cases}$$

where $B_i$ is the analogue of $A_i$. We can now compute the inner product:

$$\langle f_A, f_B\rangle = \left\langle \widehat{f_A}, \widehat{f_B}\right\rangle = \sum_{x \in {\mathbb{F}_2}^E} \widehat{f_A}(x)\widehat{f_B}(x)$$

We now need to come up with a simple argument to say that this inner product is non zero. Recall that it suffices to prove that $G$ has a cycle factor because the value of $\langle f_A, f_B\rangle$ is exactly the number of cycle factors of $G$. We will actually prove that every non zero term in the sum are non negative.

Observe that if $\widehat{f_A}(x) \neq 0$ and $\widehat{f_B}(x) \neq 0$, then $\widehat{f_A}(x)$ (resp $\widehat{f_B}(x)$) is negative if and only if $|x|_1 = 2\,[4]$ that is if and only if there is an odd number of degree 2 vertices in $x$. Hence, $\widehat{f_A}(x)$ and $\widehat{f_B}(x)$ both have the same sign so the inner product is a sum of non negative terms. In order to prove that this sum is non zero, we just have to provide one strictly positive term: $x = 0$ for instance. □

Recall that $\langle f_A, f_B \rangle = \sum_{x \in {\mathbb{F}_2}^E} f_A(x) f_B(x)$ is exactly the number of cycle factors. Moreover, a term of this sum, $f_A(x)f_B(x)$ is either 0 or 1 so it is non negative. However, finding such a term that is strictly positive (so $x$ such that $f_A(x)f_B(x) = 1$) is finding a cycle factor! Once we have the Fourier transforms, we also have, at least for this proof, that $\left\langle \widehat{f_A}, \widehat{f_B} \right\rangle = \sum_{x \in {\mathbb{F}_2}^E} \widehat{f_A}(x)\widehat{f_B}(x)$ is a sum of non negative terms but this time, it is easy to find a strictly positive term as $x = 0$ suits. Observe that moreover, this proof is not constructive in the sense that it does not provide a cycle factor. We cannot even try to build one from the proof! We only know that a cycle factor exists since the inner product is not null.

Finally, we relied on the fact that the graph $G$ is bipartite in order to define the inner product. This is essential for our proof method to work because we need an inner product somewhere. We will now give another example to show how to deal with non bipartite graphs.

**Proposition 2.1.2.** Every 4-regular graph has an Eulerian orientation.

Again, there exists a simple proof of this result. More generally, every Eulerian graph has an Eulerian orientation. It has been proved by Hierholzer (see [20]) that a connected graph is Eulerian if and only if it has an Eulerian circuit. One can simply consider each connected component of some 4-regular graph, take an Eulerian circuit on each and choose an orientation for every circuits. It provides an Eulerian orientation.

We will see how to prove this result using our Fourier method. This time, the graph is not bipartite anymore. First, let us start with a definition that will be useful for this proof and later on.

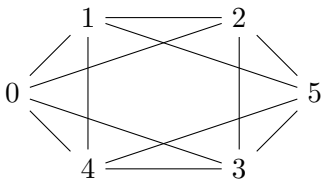
**Definition 2.1.3.** Let $G = (V, E)$ be a graph. Define the subdivided graph $G_\bullet = (V_\bullet, E_\bullet)$ of $G$ by

- $V_\bullet = V \uplus E$
- $E_\bullet = \{ve \colon v \in V \wedge e \in E \wedge v \in e\}$

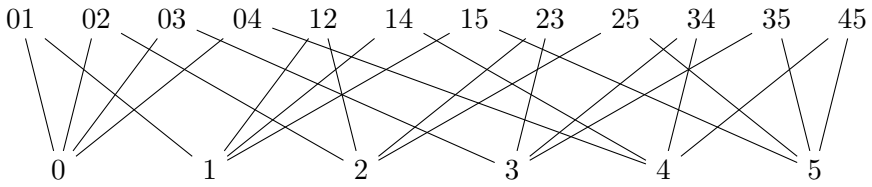
*Remark.* The graph $G_\bullet$ is always bipartite. Again, this is mandatory so that we can use the inner product trick.

*Proof.* Let $G = (V, E)$ be a 4-regular graph. Our goal is to split the problem as a conjunction of constraints: one on each side of the bipartite graph $G_\bullet$. Observe that $G$ has an Eulerian orientation if and only if there exists a function $x : E_\bullet \to \mathbb{F}_2$ such that

- every $v \in V$ is adjacent to exactly two edges $e$ and $e'$ so that $ve$ and $ve'$ are labelled 1
- every edge $e \in E$ has exactly one of its endpoints $v$ such that $ve$ is labelled 1




(a) Some 4-regular graph $G$




(b) Its corresponding graph $G_\bullet$

Figure 2.2: Subdivision of a graph

More formally this correspond to the following pair of conditions:

$$\begin{array}{ll} \forall v \in V & |\{e \in E \colon v \in e \wedge x(ve) = 1\}| = 2 \\ \forall e \in E & |\{v \in V \colon v \in e \wedge x(ve) = 1\}| = 1 \end{array} \tag{2.2}$$

Indeed, if such a function exists, then we orient the edge $e = uv$ according to the following rule:

- $u \to v$ if $x(ue) = 1$ (and so $x(ve) = 0$)
- $v \to u$ otherwise

Every edge $e \in E$ has a well defined orientation because $x$ satisfies that

$$|\{v \in V \colon v \in e \wedge x(ve)\}| = 1$$

and every vertex $v \in V$ has its indegree equals to 2 because

$$|\{e \in E \colon v \in e \wedge x(ve) = 1\}| = 2$$

Conversely, given an Eulerian orientation, we define $x(ue) = 1$ if an only if $e = uv$ with $u \to v$ and 0 otherwise. Such an $x$ satisfies the conditions 2.2.

Let us now prove that there exists such a function $x$. Define $f_V, f_E : {\mathbb{F}_2}^{E_\bullet} \to \mathbb{C}$ by

$$\forall x \in {\mathbb{F}_2}^{E_\bullet} \qquad f_V(x) = \begin{cases} 1 & \text{if} \quad \forall v \in V \quad |\{e \in E \colon v \in e \wedge x(e) = 1\}| = 2 \\ 0 & \text{otherwise} \end{cases}$$

and $$\forall x \in {\mathbb{F}_2}^{E_\bullet} \qquad f_E(x) = \begin{cases} 1 & \text{if} \quad \forall e \in E \quad |\{v \in V \colon v \in e \wedge x(e) = 1\}| = 1 \\ 0 & \text{otherwise} \end{cases}$$

Our goal is to show that the inner product $\langle f_V, f_E \rangle$ is non zero. Indeed, by definition,

$$\langle f_V, f_E \rangle = \sum_{x \in {\mathbb{F}_2}^{E_\bullet}} f_V(x) f_E(x)$$

For $f_V(x)f_E(x)$ to be non zero, we need that $x$ fulfills the two conditions 2.2. Such an $x$ provides an Eulerian orientation as we explained above. Moreover, $f_V(x)f_E(x)$ is either 0 or 1. So, $\langle f_V, f_E\rangle$ is exactly the number of Eulerian orientations of $G$.

Now that we have an inner product, we will compute the Fourier transform of our two vectors $f_V$ and $F_E$. We already have computed $\widehat{f_V}$ in the proof of Proposition 2.1.1 so we only have to deal with $\widehat{f_E}$. Again, the trick is to look at what happen when $|E| = 1$ and denote $f_E$ by $f_{E_1}$ in this case. Then, we use the fact that Fourier matrices behave nicely with tensor product:

$$\widehat{f_E} = \widehat{f_{E_1}^{\otimes m}} = \widehat{f_{E_1}}^{\otimes m}$$

The details can be found in Appendix (see C.1.2). In the end, we have that

$$\forall x \in {\mathbb{F}_2}^{E_\bullet} \qquad f_E(x) = \begin{cases} \frac{1}{2^m}(-1)^{|x|_1/2} & \text{if} \quad \forall e \in E \qquad \sum_{v\in e} x(ve) = 0 \\ 0 & \text{otherwise} \end{cases}$$

Moreover, recall that

$$\forall x \in {\mathbb{F}_2}^{E_\bullet}\ \widehat{f_V}(x) = \begin{cases} \frac{1}{2^{2n}}\, 6^{|V_0(x)|+|V_4(x)|}(-2)^{|V_2(x)|} & \text{if } \forall v \in V\ v \in V_0(x) \cup V_2(x) \cup V_4(x) \\ 0 & \text{otherwise} \end{cases}$$

where for every $i \in [\![ 0\ ;\ 4 ]\!]$, $V_i(x)$ is the set of vertices of degree $i$ in $x$. More formally,

$$V_i(x) := \{v \in V\colon\ |\{e \in E\colon v \in e \wedge x(e) = 1\}| = i\}$$

This is the very same calculus we made in the proof of Proposition 2.1.1. (Note the $2^{2n}$ instead of $2^n$, it is not a mistake since this time we work with $G_\bullet$ rather than $G$.)

So, we can compute $\left\langle \widehat{f_V}, \widehat{f_E} \right\rangle$ which we know to be equal to $\langle f_V, f_E\rangle$, the number of cycle factors of $G$. For $\widehat{f_E}(x)$ to be non zero, $x$ must satisfies that every edge $e \in E$ is monochromatic in $x$. Let us call $\Gamma$ the set of such $x$. If $x \in \Gamma$ then $\widehat{f_E}(x) = 1/2^m(-1)^{|x|_1/2}$. Hence,

$$\left\langle \widehat{f_V}, \widehat{f_E} \right\rangle = \sum_{x\in {\mathbb{F}_2}^{E_\bullet}} \widehat{f_V}(x)\, \widehat{f_E}(x) = \frac{1}{2^m} \sum_{x\in\Gamma} \widehat{f_V}(x)(-1)^{\frac{|x|_1}{2}}$$

Observe that $\widehat{f_V}(x)(-1)^{\frac{|x|_1}{2}}$ is always positive. Indeed,

- either $|x|_1 = 0\,[4]$ and there is an even number of bichromatic vertices $v \in V$ so $\widehat{f_V}(x) \geq 0$
- or $|x|_1 = 2\,[4]$ and there is an odd number of bichromatic vertices $v \in V$ so $\widehat{f_V}(x) \leq 0$

Hence, $\left\langle \widehat{f_V}, \widehat{f_E} \right\rangle$ is a sum of non negative terms. Moreover, $\widehat{f_V}(0)\widehat{f_E}(0) = 6^n/2^{m+2n} > 0$ which concludes the proof. □

What we did is very similar to the proof of Proposition 2.1.1. However, it is interesting to know that other choices could have been made for the functions $f_V$ and $f_E$. For instance, we could have defined $f_E$ by

$$\forall x \in {\mathbb{F}_2}^{E^\bullet} \qquad f_E(x) = \begin{cases} 1 & \text{if } \forall e \in E \quad \sum_{e \ni v} x(e) = 0 \\ 0 & \text{otherwise} \end{cases}$$

One can check that there exists a Eulerian orientation of $G$ if and only if there exists $x \in {\mathbb{F}_2}^{E^\bullet}$ such that both $f_V(x)$ and $f_E(x)$ are not null. Indeed, such an $x$ provide a cycle factor and since the graph is 4-regular, we can easily derive an Eulerian orientation. There is no difficulty to compute $\widehat{f_E}$ is this case. However this time, the sum of the inner product $\left\langle \widehat{f_V}, \widehat{f_E} \right\rangle$ contains positive and negative terms and it is not clear how to show that the inner product is not null.

In the next section, we will properly define Fourier matrices and see some general properties of the Fourier transform in this context. We will also explain what are the link between the precolorings (see 1.10.1), the Nullstellensatz (see 1.5) and this Fourier theory.

## 2.2 Definition and basic properties

Consider an integer $k \geq 1$ and a field $\mathbb{K}$ with $k^{\text{th}}$ root of unity. We denote by $w_k$ the $k^{\text{th}}$ root of unity. We define the Fourier matrix $F_k$ by

$$F_k = \frac{1}{\sqrt{k}} \left( {w_k}^{ij} \right)_{i,j \in [\![ 0 \ ; \ k-1 ]\!]}$$

Then, for every $n \geq 1$, we let $\qquad F_{k,n} = {F_k}^{\otimes n} = \bigotimes_{i=1}^{n} F_k$

Consider the lexicographic order $<_{\text{lex}}$ on ${\mathbb{Z}_k}^n$ and let $x_0 <_{\text{lex}} x_1 <_{\text{lex}} \cdots <_{\text{lex}} x_{k^n-1}$ be the distinct elements of ${\mathbb{Z}_k}^n$. We have that

$$F_{k,n} = \frac{1}{\sqrt{k^n}} \left( {\omega_k}^{\langle x_i, x_j \rangle} \right)_{i,j \in [\![ 0 \ ; \ k^n-1 ]\!]}$$

In the following, we will conveniently forget about the order on the elements and simply write

$$F_{k,n} = \frac{1}{\sqrt{k^n}} \left( {w_k}^{\langle x,y \rangle} \right)_{x,y \in {\mathbb{Z}_k}^n}$$

**Example 2.2.1.** Let us index the rows with $(0,0), (0,1), (1,0)$ and $(1,1)$ (which are the vectors of $\mathbb{Z}_2$ taken in lexicographic order) and use the same indices for the columns. On can check that

$$F_{2,2} = \frac{1}{\sqrt{2}} \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Now, for every $n \geq 1$ and every $k \geq 1$, the ($k^{\text{th}}$-)Fourier transform is the application

$$\widehat{\cdot} : \begin{cases} \mathbb{K}^{k^n} & \to & \mathbb{K}^{k^n} \\ x & \mapsto & F_{k,n}\, x \end{cases}$$

**Properties 2.2.2.**

i) $\forall x \in \mathbb{K}^{k^n} \qquad \widehat{\widehat{x}} = x$

ii) $\forall \lambda \in \mathbb{K} \quad \forall x, y \in \mathbb{K}^{k^n} \qquad \widehat{\lambda x + y} = \lambda \widehat{x} + \widehat{y}$

iii) ${F_{k,n}}^* = {F_{k,n}}^{-1}$

iv) $\forall x, y \in \mathbb{K}^{k^n} \quad \langle x, y \rangle = \langle \widehat{x}, \widehat{y} \rangle$

**Proposition 2.2.3.** Let $k \geq 2$. Define $f : {\mathbb{Z}_k}^2 \to \mathbb{C}$ by

$$\forall (x_0, x_1) \in {\mathbb{Z}_k}^2 \quad f(x_0, x_1) = \begin{cases} 1 & \text{if} \quad x_0 = x_1 \\ 0 & \text{otherwise} \end{cases}$$

Then,
$$\forall x \in {\mathbb{Z}_k}^2 \quad \widehat{f}(x_0, x_1) = \begin{cases} k & \text{if} \quad x_0 + x_1 = 0 \\ 0 & \text{otherwise} \end{cases}$$

*Remark* 2.2.4. Up to a factor, the Fourier transform of the equality is the characteristic function of the pairs that sums to zero.

### 2.2.1 Notes about the tensor product

Physicists (and more specifically those working in quantum mechanics) use the "braket" notation. This consists of denoting by $|\phi\rangle$ the column vector $\phi$ and by $\langle\phi|$ its conjugate transpose (hence a row vector). With those notations, $\langle\phi|\phi\rangle$ is the square (hermitian) norm of $\phi$ and $|\phi\rangle\langle\phi|$ is a rank one matrix: the projector on $\mathbb{C} \cdot |\phi\rangle$ that sends $\phi$ to $\langle\phi|\phi\rangle |\phi\rangle$.

**Example 2.2.5.**

$$|x\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{so} \quad |x\rangle\langle x| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad \langle x|x\rangle = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 1$$

**Notation.**

- The canonical basis of $\mathbb{C}^2$ is denoted by $(|0\rangle, |1\rangle)$.
- The tensor product $|a\rangle \otimes |b\rangle$ is usually denoted by $|ab\rangle$.
- Hence, the canonical basis of $\mathbb{C}^{2^n}$ can be written

$$(|0\cdots0\rangle, |0\cdots01\rangle, \ldots, |1\cdots1\rangle)$$

One just has to count in basis 2 with $n$ digits.

One matrix is also very important in quantum mechanics: the Hadamard matrix. It is exactly our Fourier matrix $F_2$. Hence, if $H_n$ is the Hadamard matrix of size $2^n$, we have that $H_n = F_{2,n} = {F_2}^{\otimes n}$.

Observe that for instance, $\widehat{|000\rangle}$, the Fourier transform of ${}^{\mathrm{t}}\begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$ (first vector of the canonical basis of $\mathbb{C}^3$) is exactly $H_3 |000\rangle$. More generaly,

$$\forall x_1, \ldots, x_n \in \{0; 1\}^n \qquad \widehat{|x_1 \cdots x_n\rangle} = H_n |x_1 \cdots x_n\rangle$$

### 2.2.2 Uncertainty principle

The uncertainty principle is a well known result in Fourier analysis. It has fundamental applications in quantum mechanics. Namely, the position and the momentum of some particle (say, an electron) cannot be both known with arbitrary precision. The more certainty we have on its position in the space, the less we have on its velocity. This is due to the wave nature of object (at least, according to the quantum mechanics) and is a mathematical theorem. We will see that there exists an analogous theorem for discrete Fourier transform. Intuitively, the more solution there exists to a combinatorial problem, the simpler the Fourier transform. By "simpler" we mean small support.

The proof of the following result can be found in [14]. We do it here (with small changes) for consistency.

**Proposition 2.2.6.** Let $k \geq 2$. For every $X \in \mathbb{C}^k$, $|\sup X|\,|\sup F_k X| \geq k$.

*Proof.* Let $X \in \mathbb{C}^k$. We define $t = |\sup X|$ to be the number of non zero coefficients of $X$. We denote these coefficients by $x_{i_0}, \ldots, x_{i_{t-1}}$. Our goal is to prove that $\widehat{X} = F_k X$ cannot have $t$ consecutive zeros. By "consecutive" we mean here "consecutive modulo $k$". In other words, if $\widehat{X} = {}^{\mathrm{t}}\begin{bmatrix} y_0 & \cdots & y_k \end{bmatrix}$ then

$$\forall i \in [\![ 0\ ;\ k-1 ]\!] \quad \{y_{i\,\%\,k}, \ldots, y_{i+t-1\,\%\,k}\} \neq \{0\}$$

For convenience, all indices are taken modulo $k$ in the following. Assume for contradiction that $\widehat{X}$ has $t$ consecutive zeros $y_i, \ldots, y_{i+t-1}$. Define $A$ to be the matrix $F_k$ where we remove every rows but these of indices $i, \ldots, i+t-1$ and every columns but these of indices $i_0, \ldots, i_{t-1}$. Hence,

$$\begin{bmatrix} {\omega_k}^{ii_0} & \cdots & {\omega_k}^{ii_{t-1}} \\ \vdots & & \vdots \\ {\omega_k}^{(i+t-1)i_0} & \cdots & {\omega_k}^{(i+t-1)i_{t-1}} \end{bmatrix} \begin{bmatrix} x_{i_0} \\ \vdots \\ x_{i_{t-1}} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

However this is not possible. Indeed, this matrix is the transpose of a Vandermonde matrix and the scalars ${\omega_k}^{i_0}, \ldots, {\omega_k}^{i_{t-1}}$ are pairwise distinct since $i_0, \ldots, i_{t-1} \in [\![ 0\ ;\ k-1 ]\!]$ hence it is invertible. □

We would like to extend this result to Fourier matrix of the form $F_{k,n}$ with $n \geq 2$. One can wonder whether this result is true in general that is if for every $k \geq 2$, every $n \geq 1$ and every $X \in \mathbb{C}^{k^n}$,

$$|\sup X| \left|\sup \widehat{X}\right| \geq k^n$$

For sure, the argument used in the previous proof does not work anymore: a submatrix (with consecutive rows) of $F_{k,n}$ (for $n \geq 2$) may not be invertible.

**Example 2.2.7.** Consider $X = {}^{\mathrm{t}}\begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix}$. We have that

$$\widehat{X} = F_{2,2} X = {}^{\mathrm{t}}\begin{bmatrix} 1 & 0 & 0 & -1 \end{bmatrix}$$

which have $|\sup X| = 2$ consecutive zeros. Observe that $X$ is not a tensor product.

**Corollary 2.2.8.** Let $X_1, \dots, X_n \in \mathbb{C}^k$. Define $X = \bigotimes_{i=1}^{n} X_i$. We have that

$$|\sup X| \left|\sup \widehat{X}\right| \geq k^n$$

*Proof.* By the mixed product property (Proposition 0.0.24) of the Kronecker product,

$$\left|\sup \widehat{X}\right| = \left|\sup \bigotimes_{i=1}^{n} \widehat{X_i}\right| = \prod_{i=1}^{n} \left|\sup \widehat{X_i}\right|$$

so, by Proposition 2.2.6,

$$|\sup X| \left|\sup \widehat{X}\right| = \prod_{i=1}^{n} |\sup X_i| \left|\sup \widehat{X_i}\right| \geq \prod_{i=1}^{n} k = k^n$$

□

### 2.2.3 Link with precolorings

We explain here the link between the precolorings that have been defined in Chapter 1.1 (see Definition 1.10.1) and the discrete Fourier transform defined above. Let us first recall the definition of a precoloring in the case we are interested in here.

**Definition 2.2.9.** Let $G = (V, E)$ be a graph and $k \geq 2$ an integer. We say that the total function $f : {\mathbb{Z}_k}^V \to \mathbb{C}$ is a precoloring of ${\mathbb{Z}_k}^G$ in $\mathbb{C}$ if and only if

$$\forall x \in {\mathbb{Z}_k}^V \quad \forall uv \in E \qquad \sum_{\lambda \in \mathbb{Z}_k} f\left(x + \lambda\left(\mathbf{1}_u - \mathbb{1}_v\right)\right) = 0$$

*Remark* 2.2.10. We could make a more general definition by replacing $\mathbb{Z}_k$ with some finite group and $\mathbb{C}$ with any field of appropriate characteristic. However, this would not be useful for Fourier related object.

**Proposition 2.2.11.** Let $G = (V, E)$ be a graph such that $E \neq \varnothing$ and $k \geq 2$ be an integer. The family of vectors $\left(\widehat{|x\rangle}\right)_{x \in \mathrm{GC}_k(G)}$ is a basis for the linear space of the precolorings of ${\mathbb{Z}_k}^G$ in $\mathbb{C}$.

*Remark.* We abuse notations here. For $x \in {\mathbb{Z}_k}^V$, there is a canonical vector $X \in {\mathbb{Z}_k}^V$ associated to $x$ if we fix an order on $V$. Namely, if $V = \{v_0, \dots, v_{n-1}\}$, then $X = {}^{\mathrm{t}}\begin{bmatrix} x(v_0) & \cdots & x(v_{n-1}) \end{bmatrix}$.

*Proof.* First, observe that if $x \in \mathrm{GC}_k(G)$ then $\widehat{|x\rangle}$ is a precoloring of ${\mathbb{Z}_k}^G$ in $\mathbb{C}$. Indeed, take $y \in {\mathbb{Z}_k}^V$ and $uv \in E$. We have that

$$\sum_{\lambda \in \mathbb{Z}_k} \widehat{|x\rangle}\left(y + \lambda\left(\mathbb{1}_u - \mathbb{1}_v\right)\right) = \sum_{\lambda \in \mathbb{Z}_k} {\omega_k}^{\langle x, y + \lambda(\mathbb{1}_u - \mathbb{1}_v)\rangle} = {\omega_k}^{\langle x, y\rangle} \sum_{\lambda \in \mathbb{Z}_k} {\omega_k}^{\lambda(x(u) - x(v))} = 0$$

since $x(u) - x(v) \neq 0\,[k]$ by hypothesis.

Lastly, let $x \in {\mathbb{Z}_k}^V \setminus \mathrm{GC}_k(G)$. There exists $uv \in E$ such that $x(u) = x(v)$ so

$$\forall y \in {\mathbb{Z}_k}^V \, \forall \lambda \in \mathbb{Z}_k \quad \widehat{|x\rangle}\left(y + \lambda(\mathbb{1}_u - \mathbb{1}_v)\right) = {\omega_k}^{\langle x|y\rangle} \, {\omega_k}^{\lambda(x(u) - x(v))} = {\omega_k}^{\langle x|y\rangle}$$

So, if $f$ is a precoloring of ${\mathbb{Z}_k}^G$ in $\mathbb{C}$, then

$$\forall y \in {\mathbb{Z}_k}^V \quad \sum_{\lambda \in \mathbb{Z}_k} f\left(y + \lambda\left(\mathbb{1}_u - \mathbb{1}_v\right)\right) \widehat{|x\rangle}\left(y + \lambda\left(\mathbb{1}_u - \mathbb{1}_v\right)\right) = 0$$

which proves that $\left\langle f, \widehat{|x\rangle} \right\rangle = 0$. Since $\left(\widehat{|x\rangle}\right)_{x\in\mathbb{Z}^V}$ is an orthonormal basis of $\mathbb{C}^{k^n}$, we have the result. □

This result is fundamental! It provides deep understanding of what precolorings are. With this new point of view, it is easy to see why a non zero inner product of two precolorings is a proof of the existence of a coloring: they must share an element of the basis $\left(\widehat{|x\rangle}\right)_{x\in \mathrm{GC}_k(G)}$. This result also provides an easy way to find precolorings for a given graph: one just has to take any linear combination of these basis vectors. This offers a useful freedom as in many cases, there is probably a pair of precolorings that make the inner product easier to understand. Moreover, we can use this result to find precolorings of small graphs of one class of graphs (for instance, on the triangle and $C_5$) and then extrapolate for the whole class (in our example, for odd cycles) using the original definition of precolorings.

This result is similar to Corollary 1.10.5. However, the objects are very different. Indeed, in Proposition 2.2.11, the precolorings are precolorings of ${\Gamma_k}^G$ in $\mathbb{C}$ whereas in Corollary 1.10.5, we deal with precolorings of $3^G$ in $\mathbb{F}_2$. The field matters as we cannot really define Fourier matrices in $\mathbb{F}_2$[1]. Despite this technical issue, we still have that the proper 3-colorings somehow provide a basis of the precoloring of $3^G$ in $\mathbb{F}_2$ but our proofs are really different. Further investigations would be useful to generalize these results in any finite field. However, our proof of Proposition 2.2.11 cannot be easily transposed to the case of precolorings of ${\Gamma_k}^G$ to $\mathbb{F}_q$.

### 2.2.4 Link between polynomials and precolorings

Let $\mathbb{K}$ be a field, $\mathcal{A}$ be a $\mathbb{K}$-algebra and $n \in \mathbb{N}^*$. For every $a \in \mathcal{A}^n$, the total function

$$\phi_a : \begin{cases} \mathcal{A}[X_1, \ldots, X_n] & \to & \mathcal{A} \\ P & \mapsto & P(a) \end{cases}$$

is an algebra homomorphism. Indeed,

- $\forall \lambda \in \mathbb{K} \quad \forall P, Q \in \mathcal{A}[X_1, \ldots, X_n] \qquad \phi_a(\lambda P + Q) = \lambda\phi(P) + \phi(Q)$
- $\forall P, Q \in \mathcal{A}[X_1, \ldots, X_n] \qquad \phi_a(PQ) = \phi_a(P)\phi_a(Q)$
- $\phi_a(1) = 1(a) = 1$

However, although $\mathcal{A}_{k,n}$ is an algebra, the evaluation function $\phi_a$ from $\mathcal{A}_{k,n}$ to $\mathcal{A}$ may not be an algebra homomorphism. Here is a counterexample for $k = 2$ and $n = 1$.

$$\phi_2(X-1) \times \phi_2(X+1) = 1 \times 3 = 3$$

but $$\phi_2((X+1)(X-1)) = \phi_2\left(X^2-1\right) = \phi_2(0) = 0$$

*Remark.* The question of an evaluation function being or not an algebra homomorphism amounts to know whether the evaluation and the operations on the polynomial ring commute.

[1] Actually, to define Fourier matrices we need the field to have a primitive $k^{\text{th}}$ root of unity. In $\mathbb{F}_2$, such matrix is always full of ones...

**Proposition 2.2.12.** Let $k, n \in \mathbb{N}^*$. For every $a \in {\mathbb{Z}_k}^n$, $\phi_{\overline{a}}$ is an algebra homomorphism.

*Proof.* Recall that the set

$$\mathcal{A}_{k,n} = \frac{\mathbb{C}[X_1, \ldots, X_n]}{\left\langle {X_i}^k - 1 \right\rangle_{i \in [\![ 1 \ ; \ n ]\!]}}$$

is the quotient of $\mathbb{C}[X_1, \ldots, X_n]$ by the equivalence relation $\sim$ defined by

$$\forall f, g \in \mathbb{C}[X_1, \ldots, X_n] \quad f \sim g \Leftrightarrow f - g \in I$$

where $I$ is the ideal generated by $\left\{ {X_i}^k - 1 \colon i \in [\![ 1 \ ; \ n ]\!] \right\}$. Let us define

$$\pi : \left\{ \begin{array}{ccc} \mathbb{C}[X_1, \ldots, X_n] & \to & \mathcal{A}_{k,n} \\ f & \mapsto & f + I \end{array} \right.$$

It is a surjective algebra homomorphism. We have that

$$\forall a \in {\mathbb{Z}_k}^n \, \forall f \in \mathbb{C}[X_1, \ldots, X_n] \quad \pi(f)(\overline{a}) = f(\overline{a})$$

Indeed, let $a \in {\mathbb{Z}_k}^n$. If $f, g \in \mathbb{C}[X_1, \ldots, X_n]$ satisfy $f \sim g$ then $f(\overline{a}) = g(\overline{a})$ since $f = g + h$ with $h \in I$ thus $h(\overline{a}) = 0$. Then, every element $g \in \pi(f)$ satisfies $g(\overline{a}) = f(\overline{a})$. This implies that $\pi(f)(\overline{a})$ is well defined as the common image of $\overline{a}$ by every elements of $f + I$. So,

$$\forall a \in {\mathbb{Z}_k}^n \quad \forall f \in \mathbb{C}[X_1, \ldots, X_n] \qquad \pi(f)(\overline{a}) = f(\overline{a})$$

Now let $P, Q \in \mathcal{A}_{k,n}$. There exists $f, g \in \mathbb{C}[X_1, \ldots, X_n]$ such that $P = \pi(f)$ and $Q = \pi(g)$. For $a \in {\mathbb{Z}_k}^n$, we have that

$$\phi_{\overline{a}}(P + Q) = \phi_{\overline{a}}\left(\pi(f) + \pi(g)\right) = \phi_{\overline{a}}\left(\pi(f + g)\right) = \pi(f + g)(\overline{a})$$

By what we did above, $\pi(f + g)(\overline{a}) = (f + g)(\overline{a})$ so

$$\phi_{\overline{a}}(P + Q) = (f + g)(\overline{a}) = f(\overline{a}) + g(\overline{a}) = \pi(f)(\overline{a}) + \pi(g)(\overline{a}) = \phi_{\overline{a}}\left(\pi(f)\right) + \phi_{\overline{a}}\left(\pi(g)\right)$$

Moreover, $$\phi_{\overline{a}}(P \times Q) = \phi_{\overline{a}}\left(\pi(f) \times \pi(g)\right) = \pi(f \times g)(\overline{a})$$

Again, since the evaluation function in $\overline{a}$ is an algebra homomorphism for $a \in {\mathbb{Z}_k}^n$, we have that $\pi(f \times g)(\overline{a}) = (f \times g)(\overline{a})$. Hence,

$$\phi_{\overline{a}}(P \times Q) = (f \times g)(\overline{a}) = f(\overline{a}) \times g(\overline{a}) = \pi(f)(\overline{a}) \times \pi(g)(\overline{a}) = \phi_{\overline{a}}(P) \times \phi_{\overline{a}}(Q)$$

□

**Corollary 2.2.13.** $\forall \ell \geq 1 \quad \forall x \in {\mathbb{Z}_k}^n \qquad \phi_{k,n}(x)^\ell = \phi_{k,n}(x)$

*Proof.* We know by Proposition 2.2.18 that $\phi_{k,n}(x)$ is the only element of $\mathcal{A}_{k,n}$ that satisfies

$$\forall y \in {\mathbb{Z}_k}^n \quad \phi_{k,n}(x)(\overline{y}) = \delta_x(y)$$

By Proposition 2.2.12, $\phi_{k,n}(x)^\ell$ also satisfies this property □

**Notation.** For $x \in {\mathbb{Z}_k}^n$, we designate the monomial $\prod_{i=0}^{n-1} {X_i}^{\frac{x_i}{n}}$ by $X^x$.

For $P \in \mathcal{A}_{k,n}$, we denote by $\left(X^x\right)^*(P)$ the coefficient of $X^x$ in $P$ in the basis $\left(X^x\right)_{x \in {\mathbb{Z}_k}^n}$.

**Proposition 2.2.14.** The total function

$$\Psi_{k,n} : \left\{ \begin{array}{ccc} \mathcal{A}_{k,n} & \to & \mathbb{C}^{{\mathbb{Z}_k}^n} \\ P & \mapsto & \left(x \mapsto \left(X^x\right)^*(P)\right) \end{array} \right.$$

is a linear isomorphism.

*Proof.* The fact that $\Psi_{k,n}$ is linear is a direct consequence of the fact that $(X^x)^*$ is linear for every $x \in {\mathbb{Z}_k}^n$.

Observe that if $\Psi_{k,n}(P) = 0$ for some $P \in \mathcal{A}_{k,n}$, then $(X^x)^*(P) = 0$ for every $x \in {\mathbb{Z}_k}^n$ so $P = 0$. Moreover, $\dim \mathcal{A}_{k,n} = k^n = \dim \mathbb{C}^{{\mathbb{Z}_k}^n}$ so $\Psi_{k,n}$ is a linear isomorphism. □

**Proposition 2.2.15.** Let $P \in \mathcal{A}_{k,n}$. If $P$ satisfies

$$\forall a \in {\mathbb{Z}_k}^n \setminus \mathrm{GC}_k(G) \quad P(\overline{a}) = 0$$

where $\overline{a} = ({\omega_k}^{a_1}, \ldots, {\omega_k}^{a_n})$, then $\Psi_{k,n}(P)$ is a precoloring.

*Proof.* Let $c \in {\mathbb{Z}_k}^n$ and $uv \in E$. We write $f_P := \Psi_{k,n}(P)$.

$$\sum_{\lambda \in \mathbb{Z}_k} f_P\left(c + \lambda\left(\mathbb{1}_u - \mathbb{1}_v\right)\right) = 0 \Leftrightarrow \langle P, Q_{c,uv}\rangle = 0$$

with $Q_{c,uv} = \sum_{\lambda \in \mathbb{Z}_k} X^{c+\lambda(\mathbb{1}_u - \mathbb{1}_v)}$. Observe that for every $x \in {\mathbb{Z}_k}^n$,

- either $x(u) = x(v)$ and then $P(\overline{x}) = 0$
- or $x(u) \neq x(v)$ and then $Q_{c,uv}(\overline{x}) = 0$

hence $PQ_{c,uv}(\overline{x}) = 0$ for every $x \in {\mathbb{Z}_k}^n$. It follows that $\langle P, Q_{c,uv}\rangle = 0$. □

*Remark* 2.2.16. The converse is false in general. For instance, consider a non empty graph with no edge. For every $P \in \mathcal{A}_{k,n} \setminus \{0\}$, we have that $\Psi_{k,n}(P)$ is a precoloring. We can also provide a counterexample on the graph with one edge. Take $P = X + Y$. The roots of $P$ among ${\mathbb{U}_2}^2$ are exactly the good colorings of the edge: $(1,-1)$ and $(-1,1)$. However, $f_P := \Psi_{k,n}(P)$ verifies $f_P((0,1)) + f_P((1,0)) = 1 + 1$ so $f_P$ is not a precoloring in $\mathbb{C}$.

### 2.2.5 Link with the Nullstellensatz

Let $k, n \in \mathbb{N}^*$. We will associate an element of

$$\mathcal{A}_{k,n} = \frac{\mathbb{C}[X_1, \ldots, X_n]}{\left\langle {X_i}^k - 1 \right\rangle_{i \in [\![1\ ;\ n]\!]}}$$

to each element of ${\mathbb{Z}_k}^n$ using the Fourier matrix $F_{k,n}$. One natural way to do so is with the following definition:

$$\phi_{k,n} : \left\{ \begin{array}{ccc} {\mathbb{Z}_k}^n & \to & \mathcal{A}_{k,n} \\ x & \mapsto & \frac{1}{\sqrt{k}^n} \sum\limits_{y \in {\mathbb{Z}_k}^n} [F_{k,n}]_{x,y} \prod\limits_{i=1}^{n} {X_i}^{\frac{-y_i}{n}} \end{array} \right.$$

**Example 2.2.17.** For convenience, we denote $X_1$ by $X$ when $n = 1$ and $X_2$ by $Y$ when $n = 2$.

$$\phi_{2,2}(0,1) = \frac{1}{4}\left(1 - Y + X - XY\right) \qquad \phi_{3,1}(1) = \frac{1}{3}\left(1 + \mathrm{j}X^2 + \bar{\mathrm{j}}X\right)$$

**Proposition 2.2.18.** For every $k, n \in \mathbb{N}^*$ and every $x \in {\mathbb{Z}_k}^n$, $\phi_{k,n}(x)$ is the only element of $\mathcal{A}_{k,n}$ that satisfies

$$\forall y \in {\mathbb{Z}_k}^n \quad \phi_{k,n}(x)(\overline{y}) = \begin{cases} 1 & \text{if} \quad x = 0 \\ 0 & \text{otherwise} \end{cases}$$

where $\overline{y} = ({\omega_k}^{y_1}, \ldots, {\omega_k}^{y_n})$.

*Proof.* For $z \in {\mathbb{Z}_k}^n$,

$$\begin{aligned} \phi_{k,n}(x)(\overline{z}) &= \left( \frac{1}{\sqrt{k}^n} \sum_{y \in {\mathbb{Z}_k}^n} [F_{k,n}]_{x,y} \prod_{i=1}^{n} {X_i}^{\overline{-y_i}_k} \right)(z) \\ &= \frac{1}{\sqrt{k}^n} \sum_{y \in {\mathbb{Z}_k}^n} \frac{1}{\sqrt{k}^n} {\omega_k}^{\langle x,y \rangle} \prod_{i=1}^{n} ({\omega_k}^{z_i})^{-y_i} \text{ by Proposition 2.2.12} \\ &= \frac{1}{k^n} \sum_{y \in {\mathbb{Z}_k}^n} {\omega_k}^{\langle x,y \rangle} {\omega_k}^{\sum_{i=1}^{n} z_i \times (-y_i)} \\ &= \frac{1}{k^n} \sum_{y \in {\mathbb{Z}_k}^n} {\omega_k}^{\langle x,y \rangle} {\omega_k}^{\langle -z,y \rangle} \\ \phi_{k,n}(x)(\overline{z}) &= \frac{1}{k^n} \sum_{y \in {\mathbb{Z}_k}^n} {\omega_k}^{\langle x-z,y \rangle} \end{aligned}$$

Hence, either $x = z$ and $\phi_{k,n}(x)(\overline{z}) = 1$ or $x \neq z$ and $\sum_{y \in {\mathbb{Z}_k}^n} {\omega_k}^{\langle x-z,y \rangle} = 0$. Indeed, for every $s \in {\mathbb{Z}_k}^n \setminus \{0\}$, we have that

$$\forall i \in \mathbb{Z}_k \quad |\{y \in {\mathbb{Z}_k}^n \colon \langle s, y \rangle = i\}| = k^{n-1}$$

Let us now prove that $(\phi_{k,n}(x))_{x \in {\mathbb{Z}_k}^n}$ is a basis of $\mathcal{A}_{k,n}$. First, we show that these vectors are linearly independent. Assume that

$$\sum_{x \in {\mathbb{Z}_k}^n} \alpha_x \, \phi_{k,n}(x) = 0$$

where $\alpha_x \in \mathbb{C}$ for every $x \in {\mathbb{Z}_k}^n$. Since $\phi_{k,n}(x)$ satisfies

$$\forall y \in {\mathbb{Z}_k}^n \quad \phi_{k,n}(x)(\overline{y}) = \delta_x(y)$$

we have that $\alpha_x = 0$ for every $x \in {\mathbb{Z}_k}^n$. Moreover, $\mathcal{A}_{k,n}$ is a $\mathbb{C}$-linear space of dimension $k^n$. This proves that $(\phi_{k,n}(x))_{x \in {\mathbb{Z}_k}^n}$ is a basis (called *Fourier basis*) of $\mathcal{A}_{k,n}$.

Now, for every $P \in \mathcal{A}_{k,n}$ there exists a unique family $(\alpha_x)_{x \in {\mathbb{Z}_k}^n}$ of $\mathbb{C}$ such that

$$P = \sum_{x \in {\mathbb{Z}_k}^n} \alpha_x \, \phi_{k,n}(x)$$

By evaluating $P$ on $(\overline{x})_{x \in {\mathbb{Z}_k}^n}$, we get that

$$\forall P \in \mathcal{A}_{k,n} \quad P = \sum_{x \in {\mathbb{Z}_k}^n} P(\overline{x}) \, \phi_{k,n}(x)$$

□

**Corollary 2.2.19.** For every family of complex numbers $(\alpha_x)_{x \in {\mathbb{Z}_k}^n}$ there exists exactly one element of $\mathcal{A}_{k,n}$ that satisfies

$$\forall x \in {\mathbb{Z}_k}^n \quad P(\overline{x}) = \alpha_x$$

*Remark.* This is nothing but polynomial interpolation on the $k^{\text{th}}$ roots of unity.

We have already made a proof for the Nullstellensatz in $\mathcal{A}_{k,n}$ in Section 1.5 for the particular case of Bayer's system (see Prop 1.5.2). Recall that $\mathcal{A}_{k,n}$ is not a ring of polynomials that satisfies the hypothesis of Hilbert's Nullstellensatz (it is not even an integral domain). However, this proof relies on the general Nullstellensatz theorem. We will see here an elementary proof of the Nullstellensatz theorem in $\mathcal{A}_{k,n}$ that uses Fourier.

**Theorem 2.2.20** (Nullstellensatz in $\mathcal{A}_{k,n}$)**.** Let $S \subseteq \mathcal{A}_{k,n}$ be a finite set. The elements of $S$ have a common root in ${\mathbb{U}_k}^n$ if and only if $\langle S \rangle \neq \mathcal{A}_{k,n}$.

*Proof.* Let $\mathscr{S}_S = \{x \in {\mathbb{Z}_k}^n \colon \forall P \in S \quad P(\overline{x}) = 0\}$. If $\langle S \rangle = \mathcal{A}_{k,n}$ then $1 \in \langle S \rangle$ and so $\mathscr{S}_S = \varnothing$. Conversely, let us assume that $\mathscr{S}_S = \varnothing$ and define for every $P \in S$

$$\sup P = \{x \in {\mathbb{Z}_k}^n \colon P(\overline{x}) \neq 0\} \qquad R_P = \sum_{x \in \sup P} \phi_{k,n}(x)$$

Observe that $R_p \in \langle P \rangle$ since $\quad R_P = P \times \sum_{x \in \sup P} \dfrac{1}{P(\overline{x})} \phi_{k,n}(x)$

by the interpolation result stated in Corollary 2.2.19. Let $R = \sum_{P \in S} R_P$ which is well defined as $S$ is finite. Observe that

$$\forall x \in {\mathbb{Z}_k}^n \quad R(\overline{x}) = |\{P \in S \colon x \in \sup P\}|$$

Since $\mathscr{S}_S = \varnothing$, $R$ has no root so $R \times \sum_{x \in {\mathbb{Z}_k}^n} \dfrac{1}{R(\overline{x})} \phi_{k,n} = 1$ hence $1 \in \langle S \rangle$ which concludes the proof. □

## 2.3 Some results using Fourier

### 2.3.1 Cycle + triangles

In July 1990, Paul Erdős proposed the following problem at the Julius Petersen Graph Theory Conference: given a graph $G$ on $3n$ vertices that is composed of a disjoint union of $n$ pairwise vertex disjoint triangles and a Hamiltonian cycle, is it true that $G$ is 3-colorable? In 1992, Fleischner and Stiebitz proved (see [16]) the so called "cycle plus triangles conjecture" using a result of Alon and Tarsi (see [2]).

In this section, we provide a new proof of this result using our theory of Fourier precolorings. The key idea is to use some combinatorial lemma of Fedor (see [30]) in order to prove that some inner product is not zero.

**Theorem 2.3.1.** Every 4-regular graph formed by a Hamiltonian cycle and $\ell$ pairwise vertex disjoint triangles is 3-colorable.

Examples of such graphs are given on Figure 2.3. In the following we will talk of the Hamiltonian cycle to refer to the "external" cycle. Of course, being Hamiltonian is not a property of the cycle itself but it will be convenient to distinguish the external cycle from the other cycles (and in particular, from the triangles).

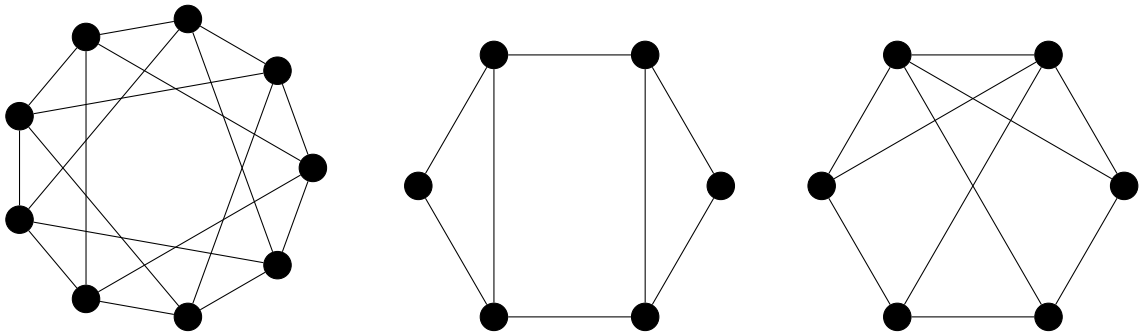


Figure 2.3: Examples of graphs of the form "cycle + triangles"

*Proof.* This problem is naturally expressed as the conjunction of two constraints: both the Hamiltonian cycle and the triangles must be properly colored. Hence, we want to find precolorings for the family of triangles and for the Hamiltonian cycle.

We will provide a family of precolorings for cycles of any length. Hence, it will be useful for the Hamiltonian cycle and for one triangle. Since the triangles are pairwise vertex disjoint, we can use the tensor product to make a precoloring for the family of triangles out of a precoloring for one triangle.

Computing a precoloring for a cycle of arbitrary length with Fourier can be surprisingly challenging. However, it is rather easy to check that a given complex function is indeed a precoloring by using the Definition 1.10.1. Here is a good one we found after many trials:

Let $n \geq 3$ and $C_n$ be the cycle on $n$ vertices that is $(V(C_n), E(C_n))$ where

$$V(C_n) = \mathbb{Z}_n \qquad \text{and} \qquad E(C_n) = \{\{i, i+1\} \colon i \in \mathbb{Z}_n\}$$

First, our precoloring will be non zero on $x \in {\mathbb{F}_3}^{\mathbb{Z}_n}$ if and only if 1 and 2 "alternates". This means that if $x(i) \neq 0$ then the next non zero coefficient $x(j)$ must satisfy $x(i) + x(j) = 0$. Figure 2.4 illustrates this. More formally, for every $x \in {\mathbb{F}_3}^{\mathbb{Z}_n}$, we define $N^x_{\neq 0} : \mathbb{Z}_n \to \mathbb{Z}_n$ by

$$\forall i \in \mathbb{Z}_n \quad N^x_{\neq 0}(i) = \begin{cases} i + \overline{\min_{j \in \mathbb{N}^*} \{x(i + \overline{j}^n) \neq 0\}}^n & \text{if} \quad \exists j \in \mathbb{Z}_n \quad x(j) \neq 0 \\ i & \text{otherwise} \end{cases}$$

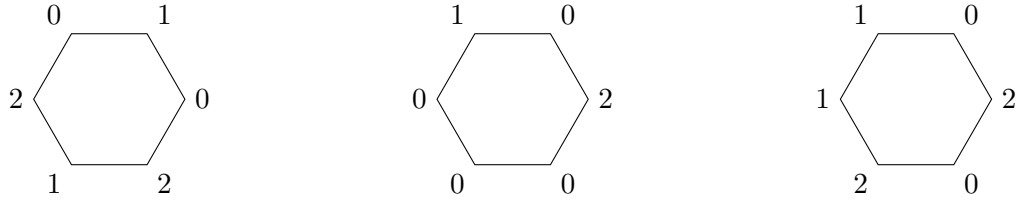



Figure 2.4: Example of configuration where 1 and 2 alternate and where they do not

Then, if $n$ is even, we define

$$\mathrm{SGC}_3(C_n) := \left\{ x \in {\mathbb{F}_3}^{\mathbb{Z}_n} : \forall i \in \mathbb{Z}_n \quad x(i) \neq 0 \Rightarrow x(i) + x\left(N^x_{\neq 0}(i)\right) = 0 \right\}$$

and if $n$ is odd,

$$\mathrm{SGC}_3(C_n) := \left\{ x \in {\mathbb{F}_3}^{\mathbb{Z}_n} \setminus \{0\} : \forall i \in \mathbb{Z}_n \quad x(i) \neq 0 \Rightarrow x(i) + x\left(N^x_{\neq 0}(i)\right) = 0 \right\}$$

*Remark.* SGC stands for "semi good colorings". This is the support of our precoloring. In some sense, semi good colorings are the Fourier pendant of proper colorings. Observe that

$$\forall x \in \mathrm{SGC}_3(C_n) \qquad \sum_{i \in \mathbb{Z}_n} x(i) = 0$$

Moreover, $\mathrm{SGC}_3(C_n)$ contains 0 if and only if $n$ is even.

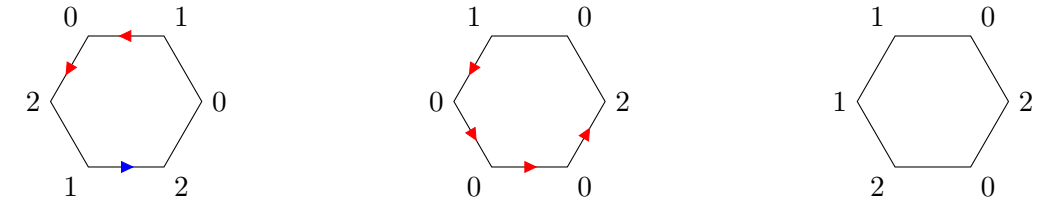
Finally, we define the $n^{\text{th}}$ Bousquet precoloring by $B_n : {\mathbb{F}_3}^{\mathbb{Z}_n} \to \mathbb{C}$ by

$$\forall x \in {\mathbb{F}_3}^{\mathbb{Z}_n} \quad B_n(x) = \begin{cases} 0 & \text{if} \quad x \notin \mathrm{SGC}_3(C_n) \\ 1 + (-1)^n & \text{if } x = 0 \\ \displaystyle\prod_{i \in x^{-1}(\{1\})} (-1)^{\overline{N^x_{\neq 0}(i) - i}^{\,n}} & \text{otherwise} \end{cases}$$

*Remark.* The cast is not just for the sake of being formal. Consider for instance the labelling of $C_3$ given by $x = {}^{\mathrm{t}}\begin{bmatrix} 0 & 2 & 1 \end{bmatrix}$. We have that $x^{-1}(\{1\}) = \{2\}$ and $N^x_{\neq 0}(2) - 2 = 1 - 2$. Since 3 is odd, we cannot take any integer congruent to $-1$ modulo 3 for the exponent as, for instance, $(-1)^{-1} \neq (-1)^2$. In other words, the implicit ordering given by the cyclic order on $\mathbb{Z}_n$ matters. For instance, $B_3\left({}^{\mathrm{t}}\begin{bmatrix} 0 & 1 & 2 \end{bmatrix}\right) \neq B_3\left({}^{\mathrm{t}}\begin{bmatrix} 0 & 2 & 1 \end{bmatrix}\right)$, the first labelling being "direct" and the second one "indirect".

Here is the intuition behind this definition. For $B_n(x)$ to be non zero, 1 and 2 must alternates along the cycle. Then, for every couple of consecutive non zero values $(1, 2)$, compute the edge distance between this 1 and this 2 and multiply by $(-1)$ to this distance.

Let us give some examples. First, our definition implicitly makes the assumption that the cycle is oriented. This is ensured by the fact that vertices are elements of $\mathbb{Z}_n$ which has a natural cyclic order. We give examples on Figure 2.5. In these examples, the orientation is trigonometric. Hence, for each 1, we go counterclockwise to the next 2 and count the number of edges. These edges have arrows on Figure 2.5. We sum up these distances for every 1: this is the exponent of the $-1$. Of course, if 1 and 2 do not alternate then the Bousquet value is 0.




$B_6(x) = (-1)^{2+1} = -1$ $\quad$ $B_6(x) = (-1)^4 = 1$ $\quad$ $B_6(x) = 0$

Figure 2.5: Examples of value for Bousquet precoloring

Let us check that $B_n$ is indeed a precoloring in $\mathbb{C}$ for $C_n$. Our goal is to prove that

$$\forall x \in {\mathbb{F}_3}^{V(C_n)} \quad \forall uv \in E(C_n) \quad B_n(x) + B_n(x + \mathbb{1}_u - \mathbb{1}_v) + B_n(x + \mathbb{1}_v - \mathbb{1}_u) = 0$$

Let $uv \in E(C_n)$. Without loss of generality, we assume that $u = i$ and $v = i + 1$. By definition,

- $B_n(0) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ 2 & \text{otherwise} \end{cases}$
- $B_n(\mathbb{1}_u - \mathbb{1}_v) = (-1)^1 = -1$
- $B_n(\mathbb{1}_v - \mathbb{1}_u) = (-1)^{\overbrace{i+1+n-1-(i+1)}^{n}} = (-1)^{\overbrace{n-1}^{n}} = \begin{cases} 1 & \text{if } n \text{ is odd} \\ -1 & \text{otherwise} \end{cases}$

So $B_n(0) + B_n(\mathbb{1}_u - \mathbb{1}_v) + B_n(\mathbb{1}_v - \mathbb{1}_u) = 0$. Now take $w = i + 2$. The case $w = i - 1$ is analog. We have that

- $B_n(\mathbb{1}_u - \mathbb{1}_v) = -1$
- $B_n(\mathbb{1}_u - \mathbb{1}_v + \mathbb{1}_v - \mathbb{1}_w) = 1$
- $B_n(\mathbb{1}_u - \mathbb{1}_v - \mathbb{1}_v + \mathbb{1}_w) = B_n(\mathbb{1}_u + \mathbb{1}_v + \mathbb{1}_w) = 0$

So it sums to zero. Consider now $x \in {\mathbb{F}_3}^{\mathbb{Z}_n}$ such that $B_n(x) \neq 0$. We also assume that $0 \notin \{x, x + \mathbb{1}_u - \mathbb{1}_v, x + \mathbb{1}_v - \mathbb{1}_u\}$ since we have already done the other cases above. Define $a$ and $b$ to be respectively the first previous non zero vertex of $u$ and the first next non zero vertex of $v$. Namely,

$$b = N^x_{\neq 0}(v) \qquad \text{and} \qquad N^x_{\neq 0}(a) = b$$

Observe that $a \neq u$ and $a \neq v$ as $x(u) = x(v) = 0$. Moreover, $a \neq b$ since $x$ must have at least 2 non zero values. Assume that $x(u) = x(v) = 0$. First, we deal with case $x(a) = 1$ and $x(b) = 2$. Figure 2.6 helps to understand what happens on the edge-clique $\{x + \lambda(\mathbb{1}_u - \mathbb{1}_v) \colon \lambda \in \mathbb{F}_3\} = \{x, x', x''\}$.

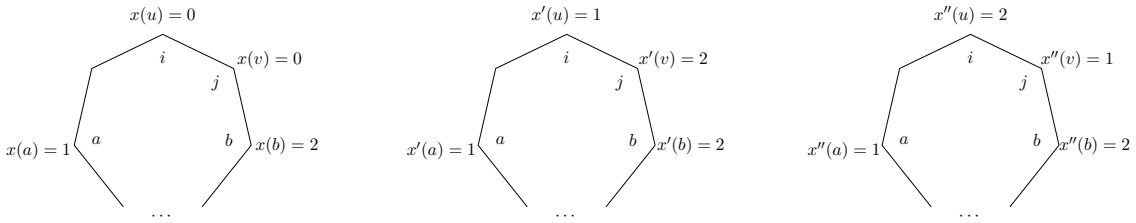



Figure 2.6: Representation of the edge-clique $\{x, x', x''\}$

We have that $B_n(x + \mathbb{1}_u - \mathbb{1}_v) = 0$ since 1 and 2 do not alternate along the cycle and that $B_n(x + \mathbb{1}_v - \mathbb{1}_u) = B_n(x) \times (-1)$ so

$$B_n(x) + B_n(x + \mathbb{1}_u - \mathbb{1}_v) + B_n(x + \mathbb{1}_v - \mathbb{1}_u) = 0$$

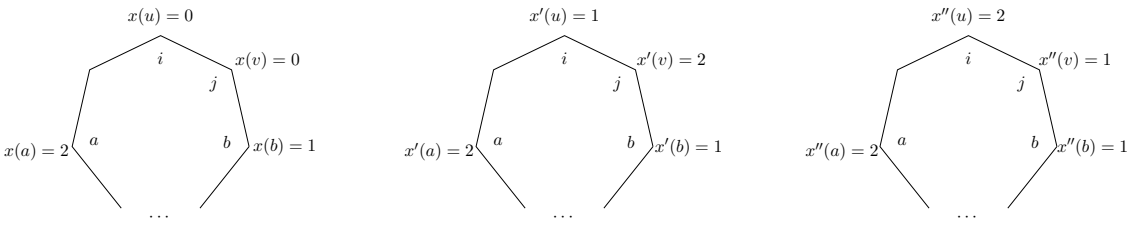



Figure 2.7: Representation of the edge-clique $\{x, x', x''\}$

The case $x(a) = 2$ and $x(b) = 1$ is analogous. Figure 2.7 should be self-explanatory.

We now have to deal with the case $x(u) \neq 0$ and $x(v) \neq 0$. Without loss of generality, we assume that $x(u) = 1$ and $x(v) = 2$. Figure 2.8 helps to understand what happen. Since we assumed that $B_n(x) \neq 0$, we must have that $x(a) = 2$ and $x(b) = 1$ otherwise 1 and 2 do not alternate. In this last case also we can check that the sum is zero on the edge-clique.

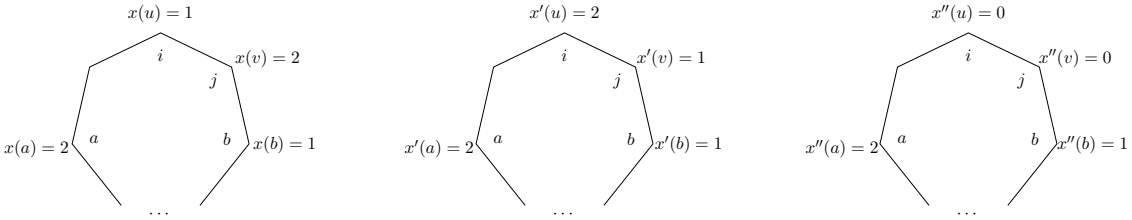



Figure 2.8: Representation of the edge-clique $\{x, x', x''\}$

So, let us define $f_0 = B_3$. By what we just did, this is a precoloring for one triangle. Since the triangles are pairwise vertex disjoint, the function $f_\triangle = {f_0}^{\otimes \ell}$ is a precoloring for the family of triangles.

Recall that our goal is to prove that $\langle f_\triangle, B_n \rangle \neq 0$. We will now prove that $\langle f_\triangle, B_n \rangle \neq 0$. First, for $B_n(x)$ to be non zero, $x$ must have as many 1's than 2's and it must be non zero. Moreover, we have that

$$\forall x \in {\mathbb{F}_3}^{\mathbb{Z}_n} \qquad f_\triangle(-x)B_n(-x) = f_\triangle(x)B_n(x)$$

Indeed, let $x \in {\mathbb{F}_3}^{\mathbb{Z}_n}$. If $n$ is even then

$$f_\triangle(-x) = f_\triangle(x) \qquad \text{and} \qquad B_n(-x) = B_n(x)$$

If $n$ is odd then

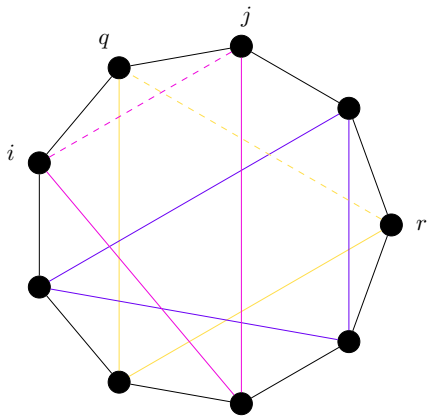
$$f_\triangle(-x) = -f_\triangle(x) \qquad \text{and} \qquad B_n(-x) = -B_n(x)$$

Hence, if $\Gamma$ is the quotient set of $\{x \in {\mathbb{F}_3}^{\mathbb{Z}_n} : f_\triangle(x)B_n(x) \neq 0\}$ by the equivalence relation $\equiv$ defined by

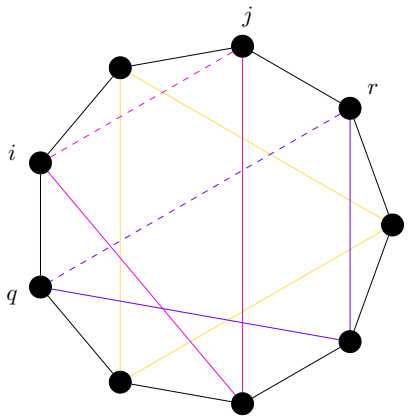
$$\forall x, y \in {\mathbb{F}_3}^{\mathbb{Z}_n} \qquad x \equiv y \Leftrightarrow \exists \lambda \in {\mathbb{F}_3}^* \quad x = \lambda y$$

then $\langle f_\triangle, B_n \rangle = 2 \sum_{x \in \Gamma} f_\triangle(x)B_n(x)$ since $0 \notin \Gamma$.

In order to prove that this sum of $+1$ and $-1$ is non zero, it suffices to show that it has an odd number of terms. We will use here a result of F. Petrov [30]:




(a) Two crossing edges in dotted




(b) Two non crossing edges in dotted

Figure 2.9: Crossing and non crossing edges

**Theorem** (Petrov)**.** Let $V = \biguplus_{i=0}^{\ell-1} V_i$ be a finite set partitioned onto disjoint subsets $V_i$ of odd sizes. Let $G$ be a graph on a ground set $V$ such that each $V_i$ is an independent set in $G$ and each subgraph induced on $V_i \uplus V_j$ is Eulerian. There exists an odd number of subsets $U \subset V$ that satisfy

- $\forall i \in [\![ 0 \,;\, \ell - 1 ]\!] \quad |U \cap V_i| = 1$
- $G[U]$ is Eulerian

For every $i \in [\![ 0 \,;\, \ell - 1 ]\!]$, we define $V_i$ to be the set of edges of the triangle $T_i$ and $V_p := \biguplus_{i=0}^{\ell-1} V_i$. For $ij, qr \in V_p$, we say that the edges $ij$ and $qr$ are *crossing* if and only if either

- $\min\limits_{k\in\mathbb{N}^*} \left(\overline{i+k}^{\,n} = j\right) > \min\limits_{k\in\mathbb{N}^*} \left(\overline{i+k}^{\,n} = q\right)$ and $\min\limits_{k\in\mathbb{N}^*} \left(\overline{i+k}^{\,n} = j\right) < \min\limits_{k\in\mathbb{N}^*} \left(\overline{i+k}^{\,n} = r\right)$
- or $\min\limits_{k\in\mathbb{N}^*} \left(\overline{i+k}^{\,n} = j\right) > \min\limits_{k\in\mathbb{N}^*} \left(\overline{i+k}^{\,n} = r\right)$ and $\min\limits_{k\in\mathbb{N}^*} \left(\overline{i+k}^{\,n} = j\right) < \min\limits_{k\in\mathbb{N}^*} \left(\overline{i+k}^{\,n} = q\right)$

Figure 2.9 shows examples of edges crossing and not crossing. This corresponds to the intuitive notion when the Hamiltonian cycle is drawn as a circle and such that every edges of the triangles are inside. Let $E_p$ be the set of crossing edges. The graph $G_p = (V_p, E_p)$ satisfies

- $V_p = \biguplus_{i=0}^{\ell-1} V_i$
- for every $i \in [\![ 0 \,;\, \ell - 1 ]\!]$, $V_i$ is a stable set

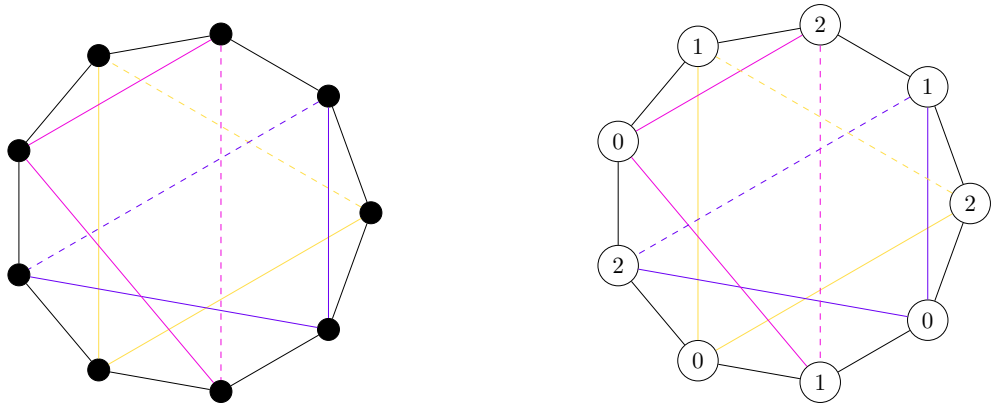
- for every $i, j \in [\![ 0 \ ; \ \ell - 1 ]\!]$ distinct, $G_p[V_i \cup V_j]$ is Eulerian

By Theorem 2.3.1, there is an odd number of $U \subset V_p$ such that

- $\forall i \in [\![ 0 \ ; \ \ell - 1 ]\!] \quad |U \cap V_i| = 1$
- $G_p[U]$ is Eulerian

Observe that such a set $U$ gives an $x \in \Gamma$. Indeed, $U$ contains exactly one edge per triangle. For every $i \in [\![ 0 \ ; \ \ell - 1 ]\!]$, let $v_i$ be the vertex in $T_i$ that does not belong to this edge. We define $x(v_i) = 0$. Take the edge $uv \in U \cap V_i$ and define $x(u) = 1$ and $x(v) = 2$. There is a unique way to choose labels for the remaining vertices so that 1 and 2 alternates along the cycle. This is true because $G_p[U]$ is Eulerian. Hence, such a set $U$ defines one element of $\Gamma$. Conversely, every element $x \in \Gamma$ defines such a set $U$. Indeed, let $y \in {\mathbb{F}_3}^{\mathbb{Z}_n}$ be a representing element of $x$. By definition, 1 and 2 alternates along the cycle and every triangle is properly colored. We define $U$ to be the set of $1-2$ edges: this is a Petrov set. The result is illustrated by Figure 2.10.

*Remark.* Observe that a Petrov set $U$ does not necessarily give a proper coloring of $G$. For instance, the set $U$ represented with the dotted edges on Figure 2.10b is a valid Petrov set.




(a) Some valid Petrov configuration (b) Some valid Petrov configuration

Figure 2.10: A Petrov configuration gives two non zero terms of the inner product

Hence, there is an odd number of terms in the sum $\sum_{x \in \Gamma} f_\triangle(x) B_n(x)$ and moreover, $f_\triangle(x) B_n(x) = \pm 1$ for every $x \in \Gamma$. So, it cannot be zero and the inner product $\langle f_\triangle, B_n \rangle \neq 0$ which concludes the proof. □

### 2.3.2 Further investigation on cycle + triangles

In the proof of Theorem 2.3.1, we used the precoloring $f_0 = g_3$ which is nothing but the Bousquet precoloring in the particular case of a cycle of length 3. One can check that

$$f_0 = -\mathrm{i}\left(|012\rangle + |120\rangle + |201\rangle - |021\rangle - |210\rangle - |102\rangle\right)$$

A proof of this fact is given in Proposition C.1.3. It has this particularity to use every base vector (see Proposition 2.2.11). Although we did not define the precoloring $B_n$ for the (Hamiltonian) cycle in terms of Fourier decomposition, we know by Proposition 2.2.11 that $B_n$ has such a decomposition on the basis of proper 3-colorings of $C_n$. However, it could have been that we were unlucky and that $\langle f_\triangle, B_n\rangle$ have been zero despite the fact that there exists a proper 3-coloring of $G$. Indeed, take for instance $n = 6$ and consider the graph depicted on Figure 2.11.

**Example.** Define $f = |001122\rangle$ and $g = |010102\rangle$. The functions $f$ and $g$ are respectively (non zero) precolorings of the triangles and of $C_6$. However, $\langle f, g\rangle = 0$ since $(|x\rangle)_{x\in\mathbb{F}_3{}^6}$ is an orthogonal basis of $\mathbb{C}^{\mathbb{F}_3{}^6}$.

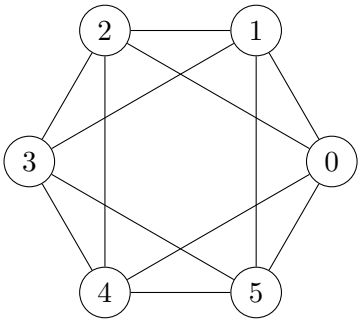
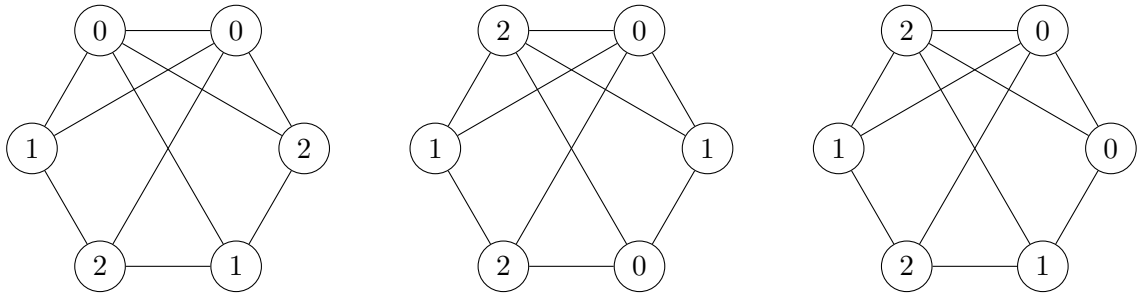



Figure 2.11: Some 3-colorable graph

One can wonder whether the sum $\sum_{x\in\Gamma} f_\triangle(x)B_n(x)$ has only non negative terms as for the proof of Propositions 2.1.1 and 2.1.2. If this were true, we would have a sum of $+1$ which would be counting the number of labelling that are Bousquet on both the Hamiltonian cycle and on every triangle. This is actually not the case in general. A counter example can be found on Figure 2.12.




$f_\triangle(x)B_6(x) = 1 \times 1$ $f_\triangle(x)B_6(x) = 1 \times (-1)$ $f_\triangle(x)B_6(x) = (-1) \times 1$

Figure 2.12: The inner product $\langle f_\triangle, B_n \rangle$ may have positive and negative terms

## 2.4 Further investigations on Fourier

In order to investigate the Fourier method, I created some programs in C++ to compute inner products. In particular, in case $G$ is bipartite, the sum

$$\sum_{x \in \mathrm{SGC}_3(G)} 2^{\Delta_1(x)}(-1)^{\Delta_3(x)}$$

counts (up to normalization), the number of 3-edge colorings of $G$. However, the fact that $G$ is bipartite is not necessary to define this sum. Hence, my program can compute it for any cubic graph. Surprisingly, the result is always non negative. This leads us to the intuition that this sum counts something. We did prove the following result:

**Proposition 2.4.1.** For any cubic graph $G$,

$$\sum_{x \in \mathrm{SGC}_3(G)} 2^{\Delta_1(x)}(-1)^{\Delta_3(x)} = 3^{\frac{n}{2}} \sum_{\mathcal{C} \in \mathrm{cf}(G)} 2^{\mathrm{cc}(\mathcal{C})}$$

where $\mathrm{cf}(G)$ is the set of all cycle factors of $G$ and, for $\mathcal{C} \in \mathrm{cf}(G)$, $\mathrm{cc}(\mathcal{C})$ is the number of connected components of $\mathcal{C}$.

When writing this thesis, I found a very simple proof of that result using Fourier! Hence, we completely dropped the (quite long and technical) combinatorial proof.

*Proof.* The idea is to work with $G_\bullet$ rather that $G$. Recall that $G_\bullet$ is $G$ where all edges have been subdivided once (see 2.1.3). As a matter of fact, $G_\bullet$ is bipartite. Define $f_V : {\mathbb{F}_3}^{E_\bullet} \to \mathbb{C}$ and $f_E : {\mathbb{F}_3}^{E_\bullet} \to \mathbb{C}$ by

$$\forall x \in {\mathbb{F}_3}^{E_\bullet} \qquad f_V(x) = \begin{cases} 1 & \text{if} \quad \forall v \in V \quad |\{x(e) \colon e \ni v\}| = 3 \\ 0 & \text{otherwise} \end{cases}$$

and

$$\forall x \in {\mathbb{F}_3}^{E_\bullet} \qquad f_E(x) = \begin{cases} 1 & \text{if} \quad \forall v \in E \quad \sum_{e \ni v} x(e) = 0 \\ 0 & \text{otherwise} \end{cases}$$

Observe that $\langle f_V, f_E\rangle$ is the number of 3-edge labellings of $G_\bullet$ such that

- every degree 3 vertex is properly colored
- every degree 2 vertex is incident to either one edge labelled 1 and one edge labelled 2 or to two edges labelled 0.

Fix a cycle factor of $G$. Since $G$ is cubic, the edges that are not in this cycle factor form a perfect matching. We want to build $x \in {\mathbb{F}_3}^{E_\bullet}$ that satisfies the two previous points. Label $(0,0)$ the edges (seen in $G$) of the perfect matching. For each of the remaining cycle, pick an edge and choose whether it is $(1,2)$ or $(2,1)$. There is only one way to complete $x$. Hence, starting from a cycle factor $\mathcal{C} \in \mathrm{cc}(G)$, there are $2^{\mathrm{cc}(\mathcal{C})}$ corresponding $x$. Conversely, for every $x \in {\mathbb{F}_3}^{E_\bullet}$ that satisfies the two previous points, the monochromatic edges form a perfect matching and each cycle is determined by the image of one of its edges. Figure 2.13 may be helpful to visualize what happens. This proves that

$$\langle f_V, f_E\rangle = \sum_{\mathcal{C}\in \mathrm{cf}(G)} 2^{\mathrm{cc}(\mathcal{C})}$$

We now have to deal with $\left\langle \widehat{f_V}, \widehat{f_E}\right\rangle$ in order to achieve the proof. Let us compute $\widehat{f_V}$ and $\widehat{f_E}$. Once again, we use the fact that the constraints are the same on every degree 3 vertex so the tensor product trick can be used. First, consider the base case of a single degree 3 vertex. Namely, we take $G_1$ to be a claw. Our aim is to compute $\widehat{f_{V_1}} = F_{3,3} f_{V_1}$ where

$$f_{V_1} : \left\{ \begin{array}{ccc} {\mathbb{F}_3}^3 & \to & \mathbb{C} \\ (x_0,x_1,x_2) & \mapsto & \left\{ \begin{array}{lll} 1 & \text{if} & |\{x_0,x_1,x_2\}| = 3 \\ 0 & \text{otherwise} & \end{array} \right. \end{array} \right.$$

Let $c = (0,1,2)$. Observe that the 6 proper edge-colorings of $G_1$ can be partitioned into

$$\{c, c+\mathbf{1}, c-\mathbf{1}\} \uplus \{-c, -c+\mathbf{1}, -c-\mathbf{1}\}$$

Let $x = (x_0,x_1,x_2) \in {\mathbb{F}_3}^3$. Observe that if $x_0+x_1+x_2 \neq 0$ then $\widehat{f_{V_1}}(x) = 0$. Indeed,

$$\mathrm{j}^{\langle x,c\rangle} + \mathrm{j}^{\langle x,c+\mathbf{1}\rangle} + \mathrm{j}^{\langle x,c-\mathbf{1}\rangle} = \mathrm{j}^{\langle x,c\rangle}\left(1 + \mathrm{j}^{\langle x,\mathbf{1}\rangle} + \mathrm{j}^{-\langle x,\mathbf{1}\rangle}\right) = 0$$

and

$$\mathrm{j}^{\langle x,-c\rangle} + \mathrm{j}^{\langle x,-c+\mathbf{1}\rangle} + \mathrm{j}^{\langle x,-c-\mathbf{1}\rangle} = 0$$

as $\langle x, \mathbf{1}\rangle \neq 0$. Now if $x_0+x_1+x_2 = 0$,

$$\begin{aligned} \sqrt{3}^3 \widehat{f_{V_1}}(x) &= \mathrm{j}^{\langle x,c\rangle} + \mathrm{j}^{\langle x,c+\mathbf{1}\rangle} + \mathrm{j}^{\langle x,c-\mathbf{1}\rangle} + \mathrm{j}^{\langle x,-c\rangle} + \mathrm{j}^{\langle x,-c+\mathbf{1}\rangle} + \mathrm{j}^{\langle x,-c-\mathbf{1}\rangle} \\ &= 3\mathrm{j}^{\langle x,c\rangle} + 3\mathrm{j}^{-\langle x,c\rangle} \\ &= 6\,\mathrm{Re}\left(\mathrm{j}^{\langle x,c\rangle}\right) \end{aligned}$$

Since $x_0+x_1+x_2 = 0$, $x$ is either monochromatic or trichromatic.

- If $x$ is monochromatic then $\mathrm{Re}\left(\mathrm{j}^{\langle x,c\rangle}\right) = 1$ so $\sqrt{3}^2 \widehat{f_{V_1}}(x) = 6$.
- If $x$ is trichromatic then $\mathrm{Re}\left(\mathrm{j}^{\langle x,c\rangle}\right) = -1/2$ so $\sqrt{3}^3 \widehat{f_{V_1}}(x) = -3$.

Hence, the tensor product gives

$$\forall x \in {\mathbb{F}_3}^{E_\bullet}\ \widehat{f_V}(x) = \begin{cases} \frac{1}{\sqrt{3}^{2m}}\, 6^{\Delta_1(x)}(-3)^{\Delta_3(x)} & \text{if } \forall v \in V(G_\bullet)\ \deg(v) = 3 \Rightarrow \sum_{e \ni v} x(e) = 0 \\ 0 & \text{otherwise} \end{cases}$$

where $\Delta_1(x)$ (resp $\Delta_3(x)$) is the set of degree 3 vertices of $G_\bullet$ that are monochromatic (resp trichromatic). Now, since $G$ is cubic, $m = 3n/2$ so

$$\forall x \in {\mathbb{F}_3}^{E_\bullet} \qquad \widehat{f_{V_1}}(x) \neq 0 \Rightarrow \widehat{f_V}(x) = 3^{\frac{-n}{2}} 2^{\Delta_1(x)}(-1)^{\Delta_3(x)}$$

Let us now compute $\widehat{f_E}$. As usual, we start by the case of a single degree 2 vertex. Let $G_1$ be the graph $P_3$. By Prop 2.2.3, we have that

$$\forall x \in {\mathbb{F}_3}^2 \qquad \sqrt{3}^2 \widehat{f_{E_1}}(x_0, x_1) = \begin{cases} 3 & \text{if} \quad x_0 = x_1 \\ 0 & \text{otherwise} \end{cases}$$

Hence,

$$\forall x \in {\mathbb{F}_3}^{E_\bullet} \qquad \sqrt{3}^{2m} \widehat{f_E}(x) = \begin{cases} 3^m & \text{if} \quad \forall v \in E \quad |\{x(e) \colon e \in E_\bullet \wedge e \ni v\}| = 1 \\ 0 & \text{otherwise} \end{cases}$$

Let us compute $\left\langle \widehat{f_V}, \widehat{f_E} \right\rangle$. Observe that for every $x \in {\mathbb{F}_3}^{E_\bullet}$, $\widehat{f_V}(x)\widehat{f_E}(x) \neq 0$ if and only if every degree 3 vertex is either monochromatic of trichromatic and every degree 2 vertex is monochromatic. In such case, $x$ can be thought of as a semi good edge coloring of $G$ (see Figure 2.13).

$$\begin{aligned} \left\langle \widehat{f_V}, \widehat{f_E} \right\rangle &= 3^{\frac{-n}{2}} \times \frac{1}{\sqrt{3}^{2m}} \sum_{x \in \mathrm{SGC}_3(G)} 2^{\Delta_1(x)}(-1)^{\Delta_3(x)} 3^m \\ &= 3^{\frac{-n}{2}} \sum_{x \in \mathrm{SGC}_3(G)} 2^{\Delta_1(x)}(-1)^{\Delta_3(x)} \end{aligned}$$

which concludes the proof as $\left\langle \widehat{f_V}, \widehat{f_E} \right\rangle = \langle f_V, f_E \rangle$.

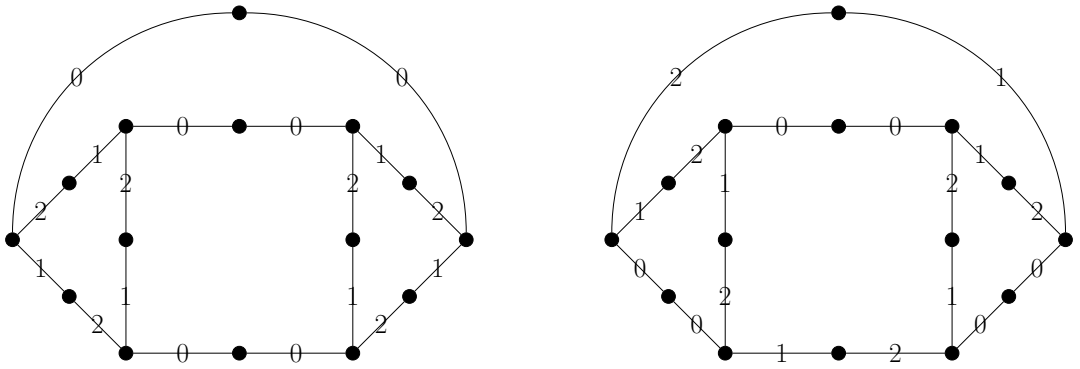


Figure 2.13: Some valid Fourier labelling for the subdivided prism

□

# Chapter 3

# A kernel for cograph edge editing

Our study of the power graphs has lead us to the Fourier analysis on graphs introduced in Section 2.1. We proved that those graphs have interesting properties as in Theorem 1.8.15 or in Theorem 1.4.1. It is natural to wonder which other properties of the ground graphs are also true for its power graphs. For instance, is the pathwidth, treewidth, clique-with, "whatever"-width an invariant? What about the homology of a power graph given the homology of its ground graph[1]? Although natural, those questions are far from being trivial because power graphs are hard to understand in a combinatorial way. Another natural question is the following: what if we slightly change the ground graph? How are its power graphs affected? Assume for instance that one wants to make $G$ a cograph, that is a graph with no induced $P_4$, a simple and well studied class of graphs. The goal is to edit as few edges of $G$ as possible. How does this translate into, say, ${\mathbb{Z}_{\chi(G)}}^G$? This question is, again, quite difficult. We did study the cograph editing problem with this in mind. We found a $O(k^2 \log k)$ vertex kernel for cograph edge editing. This improves the cubic kernel found by Guillemot, Havet, Paul and Perez [17] which involved four reduction rules. We generalize one of their rules, based on packing of induced paths of length four, by introducing $t$-modules, which are modules up to $t$ edge modifications. The key fact is that large $t$-modules cannot be edited more than $t$ times, and this allows to obtain a near quadratic kernel. The extra $\log k$ factor seems tricky to remove as it is necessary in the combinatorial lemma on trees which is central in our proof.

[1]Recall that the so called "ground graph" is unique by Theorem 1.8.9.

## 3.1 Introduction

A particularly large class of graph algorithmic questions can be seen as modification problems. Such problems are defined by a target class of graphs $\mathcal{C}$ and the types of modifications allowed on a graph, such as vertex deletion or edge addition for example. The question is, given an input graph $G$, to find the minimum number of such modifications to be performed on $G$ in order to obtain a graph $H \in \mathcal{C}$. For instance, the very popular vertex-cover problem can be seen as a vertex deletion problem in which one wants to reach the class of edgeless graphs. Also, the feedback-vertex-set problem can be seen as vertex deletion toward the class of forests.

In these two examples, allowing vertex additions would not make sense as adding vertices would not help to reach the target class. The situation is the same for all hereditary target classes, i.e. classes closed by induced subgraphs, which turns out to be a property shared by the vast majority of the target classes considered in modification problems (see [24] for example). For the case of edge modification problems, which we consider here, the situation is quite different as both deletion and addition of edges may help in order to reach some hereditary target class. Consequently, three kinds of edge modification problems are classically considered: the deletion problem, in which only deletion of edges is allowed, the completion problem, allowing only addition of edges and the editing problem, where both addition and deletion are allowed. The question asked by edge modification problems is very natural in the sense that one can assume that the input graph $G$ is a noisy version of a graph $H$ of $\mathcal{C}$ in which a small set $S$ of $k$ pairs of vertices has been modified [26]. This is the reason why several edge modification problems are successfully used in practice to analyse real-world datasets. As an example of this success, the community detection problem, which is a central topic in complex networks analysis, is formalised by the *cluster editing* problem [32], which asks whether it is possible to edit at most $k$ pairs of vertices to make the input graph a disjoint union of cliques, also known as *cluster graphs*.

Unfortunately, most edge modification problems, including *cluster editing*, are $NP$-hard, even if the target class is very simple [26]. One striking example of this is the $NP$-hardness of the editing problem toward the class of graphs that are the disjoint union of a single clique and an independent set, called *clique + independent set*. In order to deal with this difficulty of computation, edge modification problems have often been studied in the framework of parameterized complexity, see [11] for a survey on the topic. In this framework, the complexity one wants to reach is $f(k)n^c$, where $c$ is a constant and $k$ the maximum number of edits allowed in the decision problem, and not the obvious $O(n^k)$ one can obtain by brute force. A common technique to design such algorithms, called FPT (for *Fixed Parameter Tractable*), is kernelization. A kernel is a preprocessing algorithm aiming at reducing in polynomial time (in $n$) the instance of a problem to an equivalent instance of size bounded by $f(k)$. Such a kernel is said to be polynomial whenever its size $f(k)$ is (at most) polynomial in $k$. It is well-known that a problem is FPT if and only if it has a kernel [15], but not all FPT problems admit a kernel of polynomial size [7] (under some complexity hypothesis). The research for compact kernels for edge modification problems

is very flourishing [11] and has achieved remarkable results. For example, there exists a $2k$ vertex kernel for cluster editing [8, 9] and very recently, [4] designed a sublinear vertex kernel for edge deletion to clique + independent set, which is the first and, up to this day only, sublinear vertex kernel for an edge modification problem.

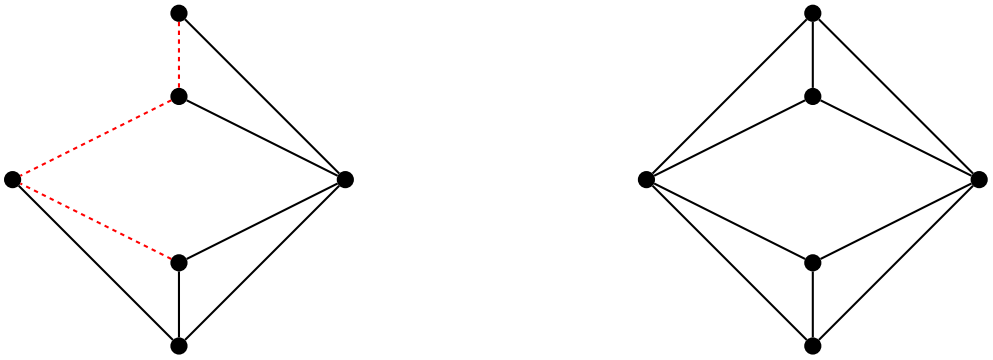
Here, we aim at designing a kernel for the editing problem toward the class of cographs, which is a proper and natural generalisation of the two classes mentioned above. Indeed, cographs are the graphs obtained from single vertices under the closure of two operations: the disjoint union of graphs and their complete union[2]. Equivalently, they can also be defined as the graphs with no induced $P_4$ (path on four vertices). Then, the purpose of the editing problem is that no induced path on four vertices can be found in the edited graph $H$. Cographs have received a huge amount of attention in algorithmic graph theory and have been shown to admit very efficient solutions to various problems. For instance, Liu et al prove in [23] that the cograph editing problem is FPT. More recently, Hellmuth et al designed in [19] an FPT algorithm for the cograph editing problem that operates on the modular decomposition of the input graph. Related to our concern here, Guillemot et al [17] proved that all the three edge modification problems toward the class of cographs admit a cubic vertex kernel. This kernel size may still appear a bit large compared to the linear and sublinear vertex kernels mentioned above for two subclasses of cographs, but the solution proposed in [17] to reach this cubic size is actually already far from being obvious. Nevertheless, there may still be some room for improvement as it seems that the cubic size instances provided in [17] in which none of the reduction rules apply can be reduced further. This is the goal of this paper. Our hope is that a finer analysis of this (rather simple) problem could provide some new reduction rules, maybe useful for other classes. Our main idea is to provide tools in order to roughly localize where edits should happen. More precisely, we provide upper bounds on the number of edits performed across a cut $(X, V \setminus X)$. For this, we relax the notion of module to some approximate version ($t$-module), and argue that not too many edits can cross a $t$-module. One very nice property of the resulting reduction rule is that it can apply independently of the possibly large value of $k$, which is crucial in practice to reduce difficult instances.

## 3.2 Notations

Let $G = (V, E)$ be a graph and $S$ be a subset of pairs of vertices of $G$. We call *edit of $G$ by $S$* the graph $G'$ obtained from $G$ by changing the adjacency relation of the elements of $S$, i.e. $G'$ differs from $G$ for every pair of vertices in $S$ and coincides for the pairs not in $S$. More formally, $G' = (V, E \triangle S)$. Since all the graphs that we will consider are simple graphs, such a set $S$ will always satisfy that $(x, y) \in S$ if and only if $(y, x) \in S$. The general editing problem for a fixed class $\mathcal{C}$ of graphs is, given an input graph $G$ and an integer $k$, to ask for the existence of an edit $H$ of $G$ by some set of pairs $S$ of size at most $k$ such that $H \in \mathcal{C}$. This is the parameterized version of *$\mathcal{C}$-editing problem*.

[2]The complete union of two graphs $G_1$ and $G_2$ is their disjoint union plus all the possible edges between $G_1$ and $G_2$.

In this paper we are interested in the case where $\mathcal{C}$ is the class of cographs. A *cograph* is a graph which does not contain any induced $P_4$ (where $P_4$ is the path on four vertices). Figure 3.1 shows an example of a cograph and an example of a graph that is not a cograph with an induced $P_4$ in dotted red.



(a) not a cograph (induced $P_4$ in dotted red) (b) a cograph

Figure 3.1: Example of a cograph and a counter example

Observe that $H$ is an edit of $G$ by $S$ whenever $G$ is an edit of $H$ by $S$. Taking the opposite point of view will be useful as we understand better the structure of $H$ since it is a cograph. Though, all along this paper $H$ is a cograph on vertex set $V$ and $G$ is an edge editing of $H$ by a set $S$ of pairs of vertices of size at most $k$. Given a subset $X$ of vertices, we denote by $\delta(X)$ the set of pairs of vertices $xy$ where $x \in X$ and $y \notin X$. The set of neighbors of a vertex $x$ is denoted by $N(x)$ and if $X \subseteq V$, $N(X) = \bigcup_{x \in X} N(x)$. When $X$ is a subset of vertices of a graph $G$, we denote by $G[X]$ the subgraph induced by $G$ on $X$.

Since cographs are exactly the graphs that can be built from isolated vertices using only fulljoins ($\oplus$) and disjoint unions ($+$), the most useful characterization of cographs is their *cotree*. Precisely, for any cograph $H$, there exists a rooted tree $T$ whose leaves are identified to the vertices of $H$ and whose internal vertices have at least two children and are labelled by $+$ or $\oplus$. Such tree explains how the cograph can be built as a sequence of disjoint unions and fulljoins starting from isolated vertices. Moreover, two vertices $x, y$ form an edge of $H$ if and only if their closest ancestor is labelled $\oplus$. A proof of this result can be found in [10]. There are several possible choices for this tree $T$, but there is a canonical one if every child of a node labelled $+$ has label $\oplus$ and every child of a node labelled $\oplus$ has label $+$ (see [10]). For instance, the cotree of a clique has a unique internal node labelled $\oplus$. Another cotree for a less specific example is shown on Figure 3.2.

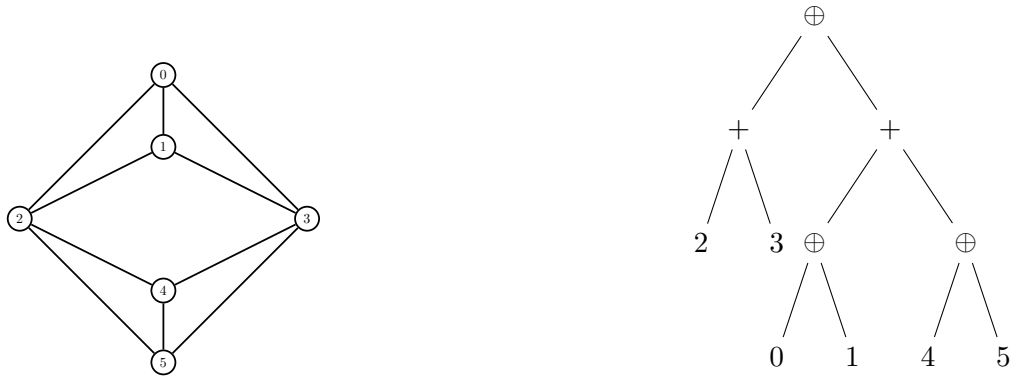



Figure 3.2: A cograph and its cotree

## 3.3 Reduction rules

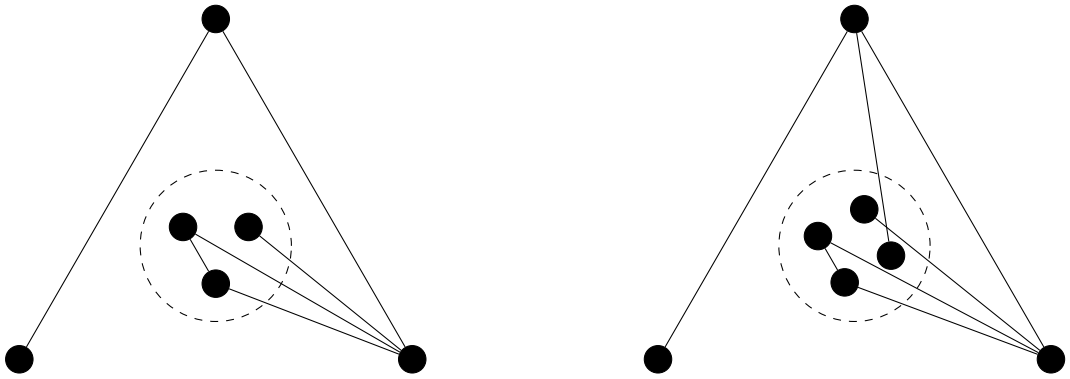
In [17], the authors show that the cograph editing problem has a cubic kernel. Their reduction rules are mainly based on two features: the induced copies of $P_4$ in $G$, and the modules of $G$. A *module* is a set of vertices $X$ such that all vertices in $X$ have the same neighborhood in $V \setminus X$. We say that two vertices are *twins* if they form a module. Figure 3.3a gives an example of a module in some graph and Figure 3.3b a counter example. In this counter example, observe that we can make the set $X$ inside the dotted circle a module by editing 2 edges. We say that $X$ is a 2-module since it is a module up to (at most) 2 edge edits. In order to define our new reduction rule, we will need this notion of $t$-module.

**Lemma 3.3.1.** Let $G = (V, E)$ be a graph and $X \subseteq V$ be a module of $G$. An induced $P_4$

- either is included in $X$
- or is included in $V \setminus X$
- or has exactly one vertex in $X$

*Proof.* Let $P$ be a $P_4$ that is an induced subgraph of $G$. Observe that $V(P) \cap X$ is a module of $P$. The modules of $P$ are the empty set, singletons and $P$ itself which proves the Lemma. □

The crucial fact shown in [17] is that for every module $X$ in $G$, one can assume that $X$ remains a module in some minimum cograph edit $H$. Here is a sketch of the argument. Assume that $S$ is a minimum cograph set of edits of $G$ so that $H = (V(G), E(G) \triangle S)$ and $X$ is a module of $G$. We consider a vertex $x \in X$ which is incident to the least number of pairs in $S \cap \delta(X)$. We now modify $S$ to $S'$ in such a way that all vertices in $X$ have the same neighborhood as $x$ in $V \setminus X$. The new graph $G' = (V(G), E(G) \triangle S')$ that we obtain has no $P_4$ since the only copy $C$ of some $P_4$ we could have created by modifying $S$ intersects both $X$ and $V \setminus X$. But $X$ is a module of $G'$, so $C$ has only one vertex in $X$



(a) a module (b) not a module

Figure 3.3: Example and counter example of modules

by Lemma 3.3.1, for instance $x$, which is impossible since $C$ would be an induced $P_4$ in $H$. Therefore this new edit has at most as many edited pairs as $S$ and leaves $X$ a module. In particular, if $X$ has size more than $k$, there is no edited pair in $\delta(X)$.

We are now ready to introduce our reduction rules to apply to $(G, k)$. We took the three first reduction rules of [17] (see Rule 5, Rule 6 and Rule 7) and slightly change them to fit our needs. In particular, we use the notion of comodule which proves to be convenient for writing our proof. A module $M$ is a *comodule* if either $N(M) = \varnothing$ or $N(M) = V \setminus M$. Despite the fact that our three first rules are a bit different from these of Guillemot et al, a graph $G$ is reduced under our three first rules whenever it is reduced under the rules of Guillemot et al. A proof of this fact can be found in Proposition 3.7.1. Moreover, up to adding an extra rule that is not useful for our kernel, the converse also holds (see Proposition 3.7.3).

*Reduction rule* 1. (comodule rule) If $G$ has a comodule $C$ which induces a cograph, remove $C$.

The safeness of this rule is clear since if we do not edit any pair incident to $C$, no $P_4$ can intersect $C$.

*Reduction rule* 2. (module reduction rule) If $G$ has a module $M$ of size $|M| > k+1$ inducing an independent set, reduce $M$ to size $k + 1$.

This rule is also safe since we can assume that $M$ remains a module, and since its size is at least $k + 1$, no pair of $\delta(M)$ can be edited.

*Reduction rule* 3. (module extraction rule) If $X$ is a module of $G$ which is not a comodule and such that $G[X]$ contains an edge, add a disjoint copy of $G[X]$ to $G$ (no edge between them) and replace the original $G[X]$ by an independent set of size $|X|$.

This is a very clever rule since it adds new vertices to $G$, which is precisely the opposite idea of kernelization! To understand its safeness, consider a module $X$ that is not a comodule and such that $G[X]$ contains an edge. Since $X$ is a module, we know by Lemma 3.3.1 that any induced $P_4$

- either is included in $X$
- or is included in $V \setminus X$
- or has exactly one vertex in $X$

The induced $P_4$ included in $X$ are kept by Rule 3 since we add a copy of $G[X]$ to the original graph. The induced $P_4$ included in $V \setminus X$ are unchanged. The induced $P_4$ crossing $X$ are still present after Rule 3 since we only remove internal edges of $X$ and by Lemma 3.3.1, such a $P_4$ has no edge inside $X$. Therefore, the cotree (see [10]) has been simplified since we "pushed $G[X]$ to its root".

After applying these three rules until none of them apply, the only modules of $G$ which are not independent sets are comodules. Hence we will always assume that our input $(G, k)$ is reduced under these rules before applying our new reduction rule.

The cubic kernel in [17] is obtained by adding a last rule: If $G$ has $k+1$ induced copies of $P_4$ pairwise only intersecting on vertices $x, y$, then edit $xy$ and decrease $k$ by 1. This rule is clearly safe since if $xy$ is not edited, some $P_4$ will survive. However, the fact that this rule is really different in nature from the others three leaves too much slack, and results in the cubic bound. The key is to be able to deduce that $xy$ must be edited, even though we only have $\ell + 1$ copies of $P_4$ where $\ell$ is smaller than $k$. We need for this to be able to say that fewer editions than $k$ are permitted in some zone of the graph $G$. Unsurprisingly, this can be achieved via a relaxation of the notion of module.

## 3.4 The fourth rule: budget and t-modules

The key here is to introduce some control on how many editions can be done across a cut. The *budget* of a set $X$ of $G$ is the minimum $b$ such that all minimum cograph edits $S$ of $G$ satisfy $|S \cap \delta(X)| \leq b$.

A *t-module* in $G$ is a set of vertices $X$ of $G$ such that by editing a set $T$ of at most $t$ pairs in $G$, we obtain $G'$ in which $X$ is a module. We usually assume that $T$ is minimal for this property, in particular $T$ is included in $\delta(X)$. Figure 3.3b shows a 2-module inside the dots.

**Lemma 3.4.1.** Let $X$ be a $t$-module such that $|X| > k + t$. If there exists a cograph edge editing set of size $k$, then the budget of $X$ is at most $t$.

*Proof.* Assume that there is an editing of $G$ by $T \subseteq \delta(X)$ with size at most $t$ in which $X$ is a module. Assume also that $H$ is a minimum cograph editing of $G$ by $S$ with size at most $k$. Since $|(S \cup T) \cap \delta(X)| \leq |S| + |T| \leq k + t$ and $|X| \geq k + t + 1$, there exists a vertex $x \in X$ which is not incident to any pair in $(S \cup T) \cap \delta(X)$. Consider now the set $S' := T \cup (S \setminus \delta(X))$ and denote by $G'$ the edition of $G$ by $S'$. Observe that $X$ is a module of $G'$. Indeed, all vertices of $X$ have the same neighborhood in $V \setminus X$ since they coincide with the one of $x$. Hence, by Lemma 3.3.1, the only copies of $P_4$ which intersects $\delta(X)$ have exactly one vertex in $X$ but this is impossible since there would be a $P_4$ in $H$ using $x$.

Indeed, $\delta(\{x\})$ is the same in $H$ and $G'$ since $x$ is not incident to any pair in $S$ nor $T$. So $G'$ is a cograph, and thus $|S'| \geq |S|$ so $t = |T| \geq |S \cap \delta(X)|$ which proves that the budget of $X$ is at most $t$. □

Note that testing if a set $X$ is a $t$-module with size at least $k + t + 1$ can be done in polynomial time since we can first guess the vertex $x \in X$ which is not incident to the edited edges, and then check if making $X$ a module with the same neighborhood as $x$ in $V \setminus X$ involves at most $t$ edits.

We now turn Lemma 3.4.1 into a reduction rule. A *nested $t$-module* of $G$ is a partition of its vertex set into five nonempty pairwise disjoint sets $A, B, C, K, I$ such that:

- The three sets $A$, $A \cup B$ and $A \cup B \cup C$ are $t$-modules and $A$ has size $|A| > k + t$.
- The set $B_\oplus$ is the subset of $B$ which is completely joined to $A$ and to $K$ and such that there is no edge between $I$ and $B_\oplus$.
- The set $B_+$ is the subset of $B$ which is completely joined to $K$ and such that there is no edge between $A$ and $B_+$ and no edge between $I$ and $B_+$.
- The set $C_\oplus$ is the subset of $C$ which is completely joined to $A \cup B$ and to $K$ and such that there is no edge between $I$ and $C_\oplus$.
- The set $C_+$ is the subset of $C$ which is completely joined to $K$ and such that there is no edge between $A \cup B$ and $C_+$ and no edge between $I$ and $C_+$.
- Each of the sets $B_\oplus, B_+, C_\oplus$ and $C_+$ have at least $3t + 1$ elements.

Figure 3.4 shows a representation of a nested $t$-module. Before stating the reduction rule, let us observe that if one can provide the sets $A, B, C, K$ and $I$, then the subsets $B_\oplus, C_\oplus, B_+, C_+$ are polynomial to compute.

*Reduction rule* 4. (nested $t$-module rule) If none of the three first rules apply and if $G$ has a nested $t$-module, edit every edge between $A$ and $I$ and every non-edge between $A$ and $K$.

**Lemma 3.4.2.** The nested $t$-module reduction rule is safe.

*Proof.* First, observe that if $t = 0$ then $A \cup B \cup C$ is a module which is not a comodule. Indeed, since $K \neq \varnothing$ and $B_\oplus \neq \varnothing$, there is an edge between $B_\oplus$ and $K$. Moreover, since $I \neq \varnothing$ and $B_\oplus \neq \varnothing$, there is a non edge between $B_\oplus$ and $I$. Thus, $A \cup B \cup C$ should have been reduced by Rule 3 since it is not an independent set as $A \neq \varnothing$ and $B_\oplus \neq \varnothing$ and $A \cap B_\oplus = \varnothing$. Now consider the case $t > 0$ and assume that there is an edge $xy$ with $x \in A$ and $y \in I$. Denote by $H$ a minimum cograph edition of $G$ by $S$ with size at most $k$. By Lemma 3.4.1, there are at most $t$ pairs of $S$ between $A$ and $C_\oplus \cup B_+$ ($A$ is a $t$-module of size $|A| > k + t$) and at most $t$ pairs of $S$ between $I$ and $C_\oplus \cup B_+$ ($A \cup B \cup C$ is a $t$-module of size $|A \cup B \cup C| > k + t$). We denote by $C'_\oplus$ (resp $B'_+$) the subset of $C_\oplus$ (resp $B_+$) which is not incident to one of these $2t$ pairs. These sets have size at least $t + 1$ as $|B_+| > 3t$ and

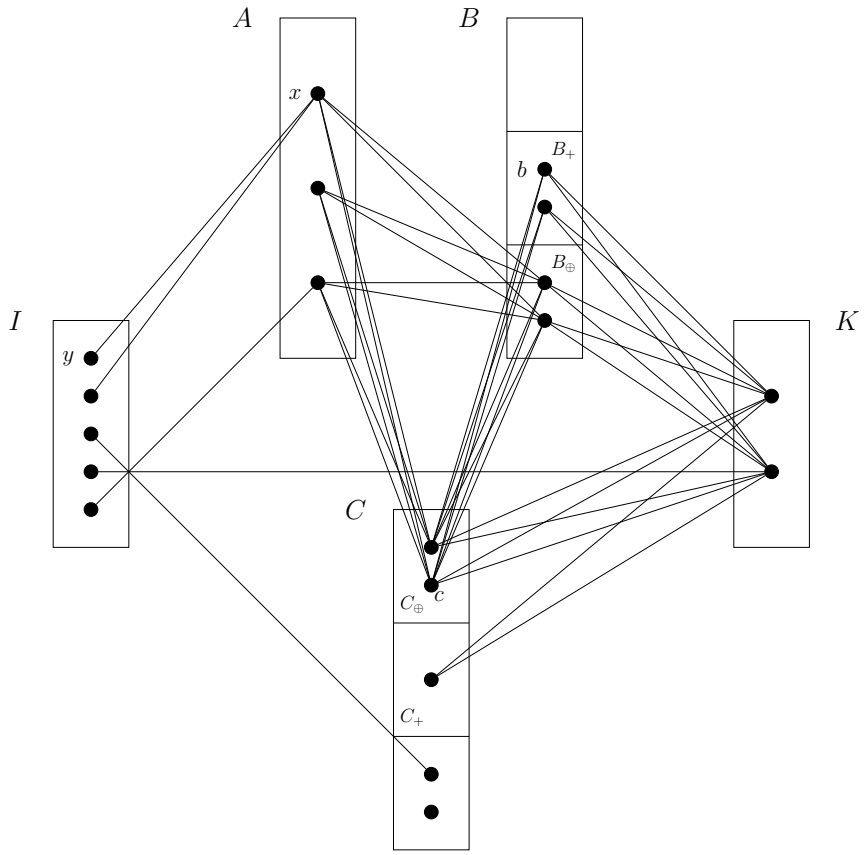



Figure 3.4: Structure of a nested $t$-module

$|C_\oplus| > 3t$. Since $A \cup B$ is also a $t$-module of size $|A \cup B| > k + t$, not every pair between $C'_\oplus$ and $B'_+$ are edited so there exists an edge $cb$ with $c \in C'_\oplus$ and $b \in B'_+$ such that $cb \notin S$. A representation of these vertices on a nested $t$-module can be found on Figure 3.4. In particular, the only pair of vertices inside $\{c, b, x, y\}$ which can be in $S$ is $xy$. Since $yxcb$ is an induced $P_4$, the pair $xy$ must belong to $S$. The same argument holds for any non-edge between $A$ and $K$ (replace $C_\oplus$ by $C_+$ and $B_+$ by $B_\oplus$ and consider $c \in C_+$ and $b \in B_\oplus$ such that $cb \notin S$). □

It is not clear that one can check if the nested $t$-module rule applies in polynomial time. However, it suffices to be able to correctly guess the sets $A, B, C, K$, and $I$. We will see later (in the proof of Claim 3.6.4) that this can be done in polynomial time.

Now that we have stated our four reduction rules, let us describe how our kernel works on input $G$.

1. Apply these four reduction rules in any order until none is applicable. This gives us a graph $G'$.
2. If $k$ is small (less than 560 as we will see in Corollary 3.6.5), do a brute force to check whether $G'$ can be made a cograph with less than $k$ edge editions.
3. If $|V(G')|$ is less than some bound in $k$ (a $O(k^2 \log k)$ that will be given in Corollary 3.6.5), return $G'$. If not, return any negative instance of size less than $k^2 \log k$ of the cograph $k$-editing problem (which is answering "no").

As we will see later, this algorithm runs in polynomial time in $n = |V(G)|$ so it is a kernel of size $O(k^2 \log k)$ for the cograph $k$-edge editing problem.

## 3.5 The combinatorial lemma

In a rooted tree (or forest), a path which starts from a node and ends in one of its descendants is a *descending path* (see Figure 3.5). We assume here that $T$ is a rooted tree or a forest which is edge-covered by a collection $\mathcal{P}$ consisting of $k$ descending paths $P_1, \ldots, P_k$. We do not assume that $\mathcal{P}$ is minimum, and there could be some multiple copies of the same path. Given some constant $c \geq 1$, we say that a descending path $Q$ which is a subpath of some $P_i$ with at least one edge is *$c$-sparse* if it intersects at most $|E(Q)|/c$ paths of $\mathcal{P}$ on at least one edge. We start by giving a sufficient condition for $T$ to have a $c$-sparse path in $\mathcal{P}$ in the particular case where $T$ is a path. This will be useful for our proof of Lemma 3.5.2.

**Lemma 3.5.1.** Let $T$ be a rooted tree which is a path and $\mathcal{P}$ be a set of $k$ (descending) paths that covers all the edges of $T$. If $|E(T)| \geq 4ck$ then there exists a $c$-sparse path $Q$.

*Proof.* Consider a minimum cover $\mathcal{C}$ of $T$ by some paths of $\mathcal{P}$. Free to reorder the paths, we assume that $\mathcal{C}$ is the set $P_1, \ldots, P_r$ and that the starting point of $P_i$ is an ascendant of the starting point of $P_j$ when $1 \leq i < j \leq r$. Note that since $\mathcal{C}$ is a minimum cover, $P_i$ is disjoint from $P_j$ whenever $1 \leq i < j - 1 \leq r$. Now we partition $\mathcal{C}$ into $\mathcal{C}_o$ (paths with odd indices) and $\mathcal{C}_e$ (paths with even indices). Without loss of generality, we assume that the sum of the numbers of edges of the paths in $\mathcal{C}_o$ is at least $2ck$. We will show that some path $P_i \in \mathcal{C}_o$ is $c$-sparse.

Assume by contradiction that every path $P_i \in \mathcal{C}_o$ is not $c$-sparse, and thus intersects $d_i$ paths of $\mathcal{P}$ with $d_i > |E(P_i)|/c$. By the fact that $\mathcal{C}$ is a minimum cover, no path in $\mathcal{P}$ intersects more than two paths in $\mathcal{C}_o$. Since the paths of $\mathcal{C}_o$ are disjoint, the total number of paths in $\mathcal{P}$ intersecting a path of $\mathcal{C}_o$ is at least

$$\sum_{i=1}^{r} \frac{d_i}{2} > \sum_{i=1}^{r} \frac{|E(P_i)|}{2c} \geq k$$

which is a contradiction. □

(a) a descending path (in dotted green) (b) not a descending path

Figure 3.5: A descending path in green and a non-descending path (in dotted red)

Figure 3.6: Example of a subdivided tree

If Lemma 3.5.1 would be true for trees, we could derive a quadratic kernel for cograph edge edition. Unfortunately the following tree provides a counter example: consider a balanced binary tree with $k$ leaves where $k$ is a power of 2. Now subdivide the two top edges $k/2$ times, the four next edges $k/4$ times, etc. In the end, the edge connected to the leaves are subdivided once. Figure 3.6 illustrates this procedure for $k = 8$.

The family $\mathcal{P}$ consists of all the $k$ root-leaf paths. The total size of the tree $T$ is[3] $\Omega(k \log_2 k)$. Let us prove that $T$ does not contain any 3-sparse path $Q$. By contradiction, assume that there exists a 3-sparse path $Q$. By definition, $Q$ is a subpath of some element of $\mathcal{P}$ hence it is a descending path. Denote by $u_0$ the first node of $Q$, by $x$ its last node and by $u_1$ its first node of degree 3 or $r$ if $r \in V(Q)$. For $u, u'$ two nodes of $Q$, we denote by $Q[u, u']$ the subpath of $Q$ delimited by $u$ and $u'$. Finally, let $d$ be the number of paths of $\mathcal{P}$ that $Q$ intersects on at least one edge. Figure 3.7 helps to understand the following counts. We have,

$$|E(Q)| = |E(Q[u_0, u_1])| + |E(Q[u_1, x])|$$

The idea is to count the number of nodes on this path. In the end, $|E(Q)|$ is equal to this number minus 1. The number of nodes can be decomposed as the original nodes (say $N_o$) plus the added nodes (say $N_+$).

- If $u_0 = u_1$, then $N_o$ is $k$ minus the depth of $u_1$. Hence, $N_o = \log_2(d) + 2$. To get $N_+$, one simply has to count the added vertices on the path $Q$:

$$N_+ = 1 + 2 + 4 + \cdots + d = \sum_{i=0}^{\log_2(d)} 2^i = 2d - 1$$

[3] More precisely, the tree has $k \log_2(k) + 2k - 1$ nodes.

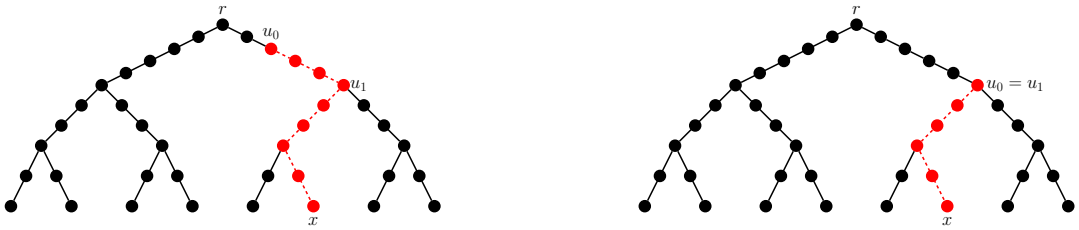



Figure 3.7: some non-3-sparse paths

In the end,
$$\begin{aligned} |E(Q)| &= |E(Q[u_1, x])| \\ &= N_o + N_+ - 1 \\ &= \log_2(d) + 2 + 2d - 1 - 1 \\ |E(Q)| &= \log_2(d) + 2d \end{aligned}$$
Hence, $|E(Q)| < 3d$ which is a contradiction.

- If $u_0 \neq u_1$, then
$$|E(Q[u_1, x])| = \log_2(d) + d - 1$$
(replace $2d$ by $d$ in the last count) and moreover, $|E(Q[u_0, u_1])| \leq d$. Hence,
$$|E(Q)| \leq d + \log_2(d) + d - 1 < 3d$$
which is a contradiction.

This proves that Lemma 3.5.1 is not true anymore when $T$ is not a path as we just provided a counter example for $c = 3$. Hence it seems that an extra $\log_2 k$ factor is needed for trees, and we indeed show that it suffices.

**Lemma 3.5.2.** Let $T$ be a forest and $\mathcal{P}$ be a set of $k$ descending paths that covers all edges of $T$. If $|E(T)| \geq 4ck(1 + \log_2 k)$ then there exists a $c$-sparse path $Q$.

*Proof.* We proceed by induction on $k$. The case $k = 1$ is clear since any subpath of $P_1$ with at least $c$ edges is $c$-sparse. If $T$ is a forest, say $T$ is composed by the trees $T_1, \ldots, T_r$ with $r \geq 2$, we define for all $1 \leq i \leq r$, the set $\mathcal{P}_i$ of the paths of $\mathcal{P}$ whose vertices belong to $T_i$ and we denote by $k_i$ the size of $\mathcal{P}_i$. Let us show that there exists $T_i$ such that $|E(T_i)| \geq 4ck_i(1 + \log_2 k_i)$. Assume by contradiction that for all $1 \leq i \leq r$, $|E(T_i)| < 4ck_i(1 + \log_2 k_i)$. Then
$$|E(T)| = \sum_{i=1}^{r} |E(T_i)| < 4c \sum_{i=1}^{r} k_i(1 + \log_2 k_i) = 4ck + 4c \sum_{i=1}^{r} k_i \log_2 k_i$$
Since $x \mapsto x \log_2 x$ is convex on $[\,1\,;k\,]$,
$$\forall x \in [\,1\,;k\,] \qquad x \log_2 x \leq \frac{k \log_2(k)}{k-1}(x-1)$$
hence
$$\begin{aligned} \sum_{i=1}^{r} k_i \log_2 k_i &\leq \frac{k \log_2 k}{k-1} \sum_{i=1}^{r} (k_i - 1) \\ &\leq k \log_2(k) \frac{k-r}{k-1} \\ &< k \log_2 k \qquad \text{(since } r \geq 2\text{)} \end{aligned}$$

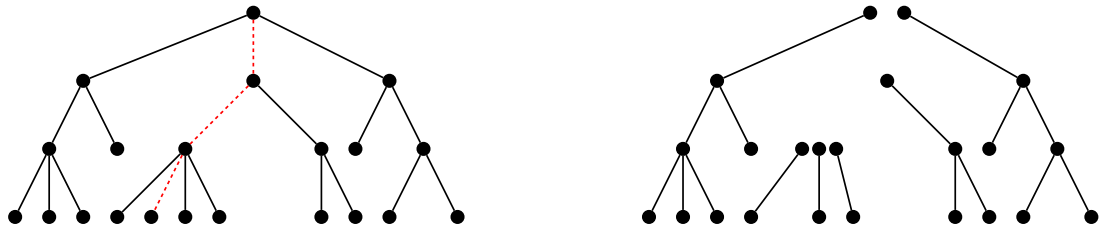


Figure 3.8: exploding a tree with path $R$ (in dotted red)

which leads to the contradiction $|E(T)| < 4ck(1+\log_2 k)$. We can now apply the induction hypothesis to $T_i$. In what follows, we assume $T$ to be a (rooted) tree.

Let us construct a descending path $R$ of $\mathcal{P}$ which starts at the root $r$ of $T$ and such that for every node $u \in R$, the child $v$ of $u$ whose subtree intersects the maximum number of paths of $\mathcal{P}$ is in $R$. In other words, $R$ follows the subtree that intersects the maximum number of paths of $\mathcal{P}$. If $R$ has at least $4ck$ edges, we conclude by Lemma 3.5.1. If not, we remove from $T$ every edge and every vertex of $R$ and for any node $u$ of $R$ and any $v$ child of $u$ in $T$ not in $R$, we add a new vertex $v'$ and add the edge $v'v$. We obtain a forest $F$ as illustrated on Figure 3.8. Observe that we can identify any new edge $v'v$ with the old edge $uv$ and thus every connected component in the new forest is edge covered by $\mathcal{P}$.

We denote by $C_1, \dots, C_p$ the connected components obtained. Observe that every component intersects at most $k/2$ paths of $\mathcal{P}$ by our choice of $R$. For $1 \le i \le p$ we denote by $k_i$ the number of paths of $\mathcal{P}$ intersecting the component $C_i$. There exist $1 \le i \le p$ so that $C_i$ has at least $4ck_i(1+\log_2 k_i)$ edges (hence we conclude by the induction hypothesis). Indeed, assume by contradiction that every $C_i$ has strictly less than $4ck_i(1+\log_2 k_i)$ edges, then the total number of edges in $T$ satisfies

$$|E(T)| < 4ck + \sum_{i=1}^{p} 4ck_i(1+\log_2 k_i) \qquad \text{with} \qquad \sum_{i=1}^{p} k_i \le k \quad \text{and} \quad k_i \le k/2 \text{ for all } i$$

Since $x \mapsto x\log_2 x$ is convex on $[\,1\,;k/2\,]$,

$$\forall x \in [\,1\,;k/2\,] \qquad x\log_2 x \le \frac{k/2\log_2(k/2)}{k/2-1}(x-1)$$

$$\text{so} \qquad \sum_{i=1}^{p} k_i \log_2 k_i \le \frac{k/2\,(\log_2(k)-1)}{k/2-1}\left(\sum_{i=1}^{p} k_i - p\right) \le \frac{k/2\,(\log_2(k)-1)}{k/2-1}(k-p)$$

$$\begin{aligned}\text{then} \qquad 4ck + \sum_{i=1}^{p} 4ck_i(1+\log_2 k_i) &\le 4ck + 4ck + 4c\,\frac{k\log_2(k)-k}{k-2}(k-p) \\ &\le 4ck + 4ck + 4c(k\log_2(k)-k) \qquad \text{since } p \ge 2 \\ &\le 4ck(1+\log_2 k)\end{aligned}$$

Thus $T$ has strictly less than $4ck(1+\log_2 k)$ edges, a contradiction. □

## 3.6 The $k^2 \log k$ kernel

In what follows, $k$ is an integer, $G$ has $n$ vertices and $H$ is a minimum cograph edit of $G$ by $S$ where $S$ has size at most $k$. Since our goal is to show a quasi-quadratic vertex kernel, we assume moreover that $n > k+1$, otherwise we would be done. Moreover, we assume that none of the first three rules apply to $G$. Our goal is to show that the fourth rule applies if $G$ is large enough (more than a quasi-quadratic function of $k$). A vertex of $G$ is *edited* if it belongs to some pair in $S$.

We consider $T$ to be the cotree of the cograph $H$. If $u$ is a node of $T$, the set of descendants of $u$ which are leaves is denoted by $De(u)$. We also see it as a set of vertices of $G$. We now define a particular subtree $T'$ of $T$ induced by the nodes $u$ such that $|De(u)| \geq k+2$. It is indeed a subtree since we have $De(u) \subseteq De(parent(u))$ for all node $u$ which is not the root of $T$.

**Lemma 3.6.1.** The tree $T'$ has at least $n/(k+1) - 2k$ nodes.

*Proof.* For $u \in V(T')$, we denote by $A_{T'}(u)$ the set of $x \in De(u)$ such that the path from $u$ to $x$ in $T$ does not contain any node of $T'$ except $u$. In other words, for a vertex $x \in V(G)$, we have that $x \in A_{T'}(u)$ if and only if $u$ is the closest ancestor of $x$ in $T$ that belongs to $T'$. Define

$$L(T') := \{u \in V(T') \mid A_{T'}(u) \neq \varnothing\}$$

For $u \in V(T')$, define $Be(u)$ (resp $Bn(u)$) to be the set of children $v$ of $u$ in $T$ such that $v \notin V(T')$ and $De(v)$ contains (resp does not contain) an edited vertex. Figure 3.9 illustrates this setting. Observe that

$$V(G) = \bigcup_{u \in L(T')} \left( \left( \bigcup_{v \in Be(u)} De(v) \right) \cup \left( \bigcup_{v \in Bn(u)} De(v) \right) \right)$$

Indeed, take $x \in V(G)$ and consider its closest ancestor $u$ in $T$ which belongs to $T'$. This is well defined since $V(T') \ni r$ as $n \geq k+2$. Let $v$ be the child of $u$ on this path (we could have $v = x$). By definition of $u$, we have that $v \notin V(T')$ and either $v \in Be(u)$ or $v \in Bn(u)$. In both case, $x \in De(v)$ so

$$V(G) \subseteq \bigcup_{u \in L(T')} \left( \left( \bigcup_{v \in Be(u)} De(v) \right) \cup \left( \bigcup_{v \in Bn(u)} De(v) \right) \right)$$

Observe that since there are at most $2k$ edited vertices and since for all $u \in L(T')$ and all $v \in Be(u)$, $|De(v)| \leq k+1$, we have that

$$\left| \bigcup_{u \in L(T')} \bigcup_{v \in Be(u)} De(v) \right| \leq 2k(k+1)$$

Hence

$$\left| \bigcup_{u \in L(T')} \bigcup_{v \in Bn(u)} De(v) \right| \geq n - 2k(k+1)$$

Observe that the sets involved in the union on $u \in L(T')$ are pairwise disjoint. Indeed, for all $x \in V(G)$ there exists a unique $u \in L(T')$ such that $x \in A_{T'}(u)$. So,

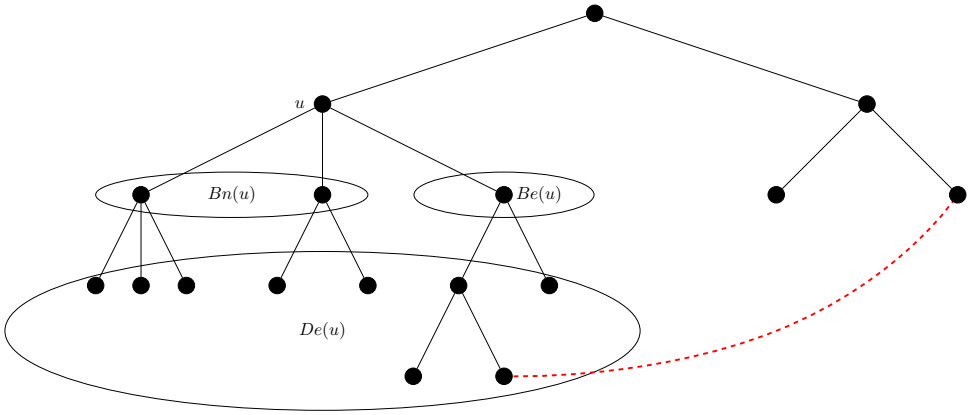



Figure 3.9: Structure of $T'$ with an edited edge in dotted red

$$\sum_{u \in L(T')} \left| \bigcup_{v \in Bn(u)} De(v) \right| \geq n - 2k(k+1)$$

Moreover, for all $u \in L(T')$, the set $\bigcup_{v \in Bn(u)} De(v)$ is a module as it does not contain any edited vertex. Moreover, it is not a comodule as it would have been removed by Rule 1. Hence, by Rule 2 and Rule 3, its size is at most $k+1$. Hence,

$$|V(T')| \geq |L(T')| \geq \frac{n - 2k(k+1)}{k+1} = \frac{n}{k+1} - 2k$$

□

The edited pairs $xy$ in $S$ can be analyzed with respect to the tree $T$. In particular, every pair $xy$ in $S$ corresponds to the path $P_{xy}$ of $T$ which connects the leaves $x$ and $y$. If we denote by $z$ the least common ancestor of $x$ and $y$ in $T$, we obtain two descending paths $P_{zx}$ and $P_{zy}$ which form an edge-partition of $P_{xy}$. There are at most $2k$ such descending paths in $T$ called *edit paths*.

**Lemma 3.6.2.** Every edge of $T'$ belongs to an edit path, except possibly $k$ edges incident to the root of $T'$.

*Proof.* Let $u \in V(T')$ and assume that $u$ is not the root of $T'$. Let $p$ be its parent node. Assume that the edge $up$ does not belong to any edit path. Then $De(u)$ is a module. By definition of $T'$, $|De(u)| \geq k+2 > k+1$ so $De(u)$ must be a comodule by Rules 2 and 3. Hence, $p$ is the root of $T'$. This proves that every edge of $T'$ not incident to its root belongs to an edit path. Moreover, $De(u)$ must contain an edited pair since it would have been removed by Rule 1 otherwise. Hence, $T'$ has at most $k$ edges which does not belong to an edit path and all of these edges are incident to its root. □

Let us denote by $T''$ the forest obtained from $T'$ when we remove the edges that does not belong to an edit path. By definition, $T''$ is edge covered by the edit paths.

**Theorem 3.6.3.** If $T''$ has a 51-sparse path with respect to the edit paths, then the nested $t$-module reduction rule applies to $G'$. Moreover, one can detect such a nested $t$-module in polynomial time.

*Proof.* Let $Q_0$ be a 51-sparse path with respect to the edit paths. Recall that by definition,

- $Q_0$ is a subpath of some edit path
- $Q_0$ intersects (on at least one edge) at most $\ell$ edit paths
- $1 \leq \ell \leq |E(Q_0)|/51$

We consider a subpath $Q$ of $Q_0$ with $|E(Q)| = 51\ell$ edges. For every node $u$ of $Q$ which is not the first or the last node (and hence has a descendant $u'$ in $Q$), we define $F_Q(u) = De(u) \setminus De(u')$. Such a node $u$ is said to be *free* if $F_Q(u)$ does not contain any edited vertex. In particular, $F_Q(u)$ is a module of $G$ which is not a comodule since $u$ is not the root of $T$ (it is not the first node of $Q$). Hence, by Rules 2 and 3, $F_Q(u)$ is an independent set. Let us prove that any non-free node $u \in V(Q)$ satisfies that $u\,parent(u)$ or $uu'$ belong to an edit path where $u'$ is the child of $u$ in $Q$. First, if there exists an edited pair $xy$ such that $x \in F_Q(u)$ and $y \in (V \setminus De(u)) \cup De(u')$ then

- either $y \in V \setminus De(u)$ in which case $P_{xy}$ intersects $Q$ on the edge $u\,parent(u)$
- or $y \in De(u')$ and so $P_{xy}$ intersects $Q$ on $uu'$.

In both cases, the edit path $P_{xy}$ intersects $Q$ hence intersects $Q_0$. Now, let us assume by contradiction that for every edited pair $xy$ such that $x \in F_Q(u)$, $y$ also belongs to $F_Q(u)$. Define

$$S' := \{xy \in S \mid x \notin F_Q(u) \vee y \notin F_Q(u)\}$$

and observe that $|S'| < |S|$ as there must exist an edited vertex in $F_Q(u)$. Denote by $G'$ the edition of $G$ by $S'$. Let us show that $G'$ is a cograph. Indeed, $G'$ coincide with $H$ except on $F_Q(u)$. Assume by contradiction that $G'[F_Q(u)]$ contains an induced $P_4$ say $x_1, x_2, x_3, x_4$. Since $F_Q(u)$ is an independent set in $H$ (recall that $T$ is the cotree of the cograph $H$), each of the pairs $x_1x_2, x_2x_3$ and $x_3x_4$ belong to $S$ as $S' \subseteq S$. So we could have made $G$ a cograph with fewer edits by removing $x_1x_2$ from $S$. Moreover, observe that there cannot be an induced $P_4$ in $G'$ crossing $F_Q(u)$. Indeed, $F_Q(u)$ is a module of $H$ (even an independent set) and $S \setminus S' \subseteq F_Q(u)^2$. So, $F_Q(u)$ is also a module of $G'$. By Lemma 3.3.1, if an induced $P_4$ crosses a module, then it has only one vertex inside this module. Hence, this $P_4$ is also an induced $P_4$ in $H$ as $S \setminus S' \subseteq F_Q(u)^2$. This contradicts the fact that $H$ is a cograph. Finally, $G'$ is a cograph which again contradicts the minimality of $S$.

This implies that $Q$ cannot have more than $2\ell$ non-free nodes since $Q_0$ intersects per definition exactly $\ell$ edit paths (two consecutive non-free nodes may correspond to the same intersection).

Consider a free node $u$ so that its child in $Q$ is also free and $u$ is labelled $\oplus$ (thus $u'$ is labelled $+$). Since $F_Q(u)$ and $F_Q(u')$ are independent sets, all vertices of $F_Q(u')$ are children

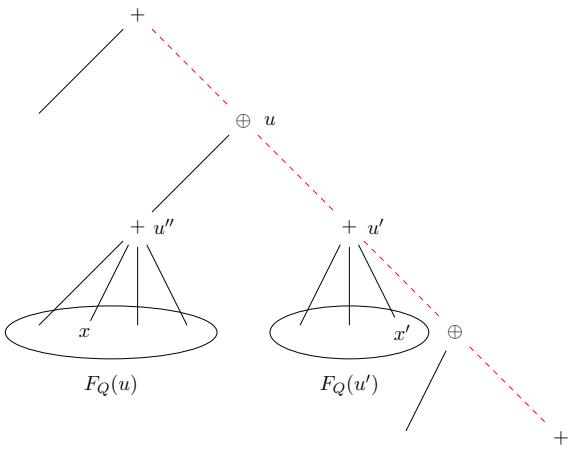



Figure 3.10: Consecutive free nodes in the path $Q$ drawn in dotted red

of $u'$ and all vertices of $F_Q(u)$ are children of $u''$, a child of $u$ not in $Q$ (Figure 3.10 illustrates this situation). Pick a vertex $x \in F_Q(u)$ and a vertex $x' \in F_Q(u')$. The crucial observation is that $V \setminus De(u)$ is exactly the set of vertices $y$ distinct from $x$ and $x'$ such that $\{x, x'\}$ is a module of $G[\{x, x', y\}]$. Indeed,

- the vertices of $V \setminus De(u)$ have this property as both $x$ and $x'$ are unedited and $u$ is labelled $\oplus$,
- the vertices in $De(u') \setminus \{x'\}$ are joined to $x$ and not to $x'$
- and the vertices of $F_Q(u) \setminus \{x\}$ are joined to $x'$ and not to $x$.

Hence, if one provides $x$ and $x'$, we can compute $De(u)$ in polynomial time (in $n$). In the following, we refer to such a couple $(u, u')$ in $Q$ as a *cut*.

**Fact 3.6.4.** There exists a cut in any subpath of $Q$ that has at least $8\ell$ edges.

*Proof.* Let $Q'$ be a subpath of $Q$ that has at least $8\ell$ edges. It suffices to show that there exists three consecutive nodes in $Q'$ that are free (either a sequence $+, \oplus, +$ or a sequence $\oplus, +, \oplus$). Assume by contradiction that every sequence of three consecutive nodes in $Q'$ contains a non-free node. Then, the number of intersections between $Q'$ and some edit paths is at least

$$\frac{1}{2} \times \frac{|V(Q')|}{3} \geq \frac{1}{2} \times \frac{8\ell}{3} = \frac{4\ell}{3} > \ell$$

which contradicts the fact that $Q_0$ intersects at most $\ell$ edits paths. □

We now pick three cuts $(u, u')$, $(v, v')$ and $(w, w')$ in $Q$ such that $(u, u')$ is chosen in the range $[\![ 43\ell \ ; \ 50\ell ]\!]$ (set of integers between $43\ell$ and $50\ell$) so among the $9\ell$ last nodes of $Q$ but not among the $\ell$ last ones, $(v, v')$ are in the middle of $Q$ (precisely chosen in the range

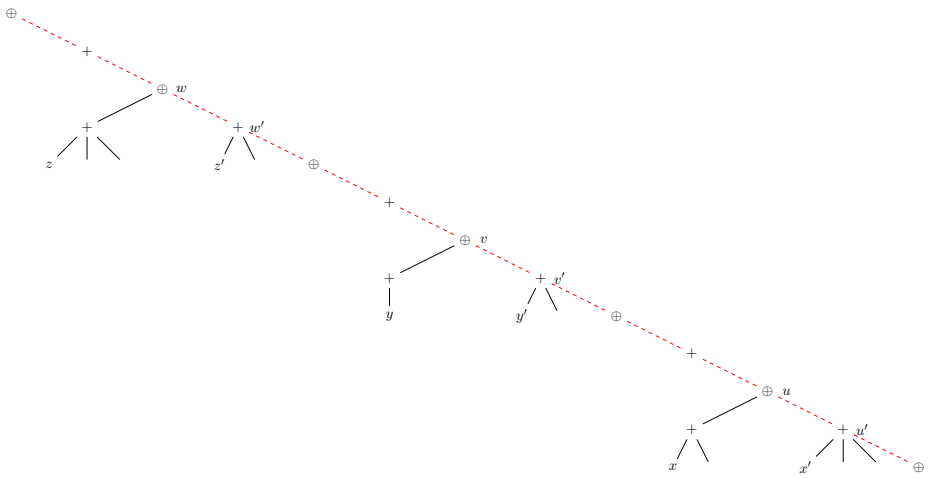



Figure 3.11: Representation of our nested $\ell$-module (the path $Q$ is in dotted red)

$[\![ 23\ell \ ; \ 30\ell ]\!]$) and $(w, w')$ are chosen in the first $10\ell$ nodes of $Q$ but not among the $2\ell$ first ones (in the range $[\![ 3\ell \ ; \ 10\ell ]\!]$). Take $x \in F_Q(u)$, $x' \in F_Q(u')$, $y \in F_Q(v)$, $y' \in F_Q(v')$, $z \in F_Q(w)$ and $z' \in F_Q(w')$. Define $A := De(u)$, then $B := De(v) \setminus A$ and finally $C := De(w) \setminus (A \cup B)$. The vertices of $V(G) \setminus (A \cup B \cup C)$ (which is equal to $V \setminus De(w)$) which are connected to $x$ form the set $K$, and the other vertices form the set $I$. Figure 3.11 illustrates how these elements are distributed on the tree $T$.

By construction, these five sets are pairwise disjoint. Moreover, $A, B$ and $C$ are nonempty. Let us check that $K \neq \varnothing$ and $I \neq \varnothing$. Since $w$ is not the first node of $Q$, it has a parent $p$ and $p$ is labelled $+$. Consider $t \in De(p) \setminus De(w)$ and observe that since $x$ is not edited, $t$ is not connected to $x$. Hence, $I \neq \varnothing$. Moreover, $p$ is not the first node of $Q$ (we took $w$ not among the first $2\ell$ nodes of $Q$) so it has a parent $p'$ and $p'$ is labelled $\oplus$. Consider $t' \in De(p') \setminus De(p)$ and observe that $t'$ is connected to $x$. Hence, $K \neq \varnothing$.

Observe that $A$, $A \cup B$ and $A \cup B \cup C$ are $\ell$-modules of size at least $k + \ell + 1$. Indeed, since $Q$ intersects at most $\ell$ edit paths, there is less than $\ell$ edges to edit to make any of them a module. Moreover, let us show that $A$ (hence $A \cup B$ and $A \cup B \cup C$) has at least $k + \ell + 1$ elements. Let $\gamma$ be the last node of $Q$. Since $\gamma \in V(T')$, we have that $|De(\gamma)| > k + 1$. Observe that $De(\gamma) \subseteq De(u) = A$ and that $u$ has at least $\ell$ descendants in $Q$ since we did not take $u$ among the last $\ell$ nodes of $Q$. So there exists $\ell - 1$ vertices of $G$ in $De(u) \setminus De(\gamma)$. Hence, $|A| \geq k + 1 + \ell$.

Another important point is that $A, B, C, K$ and $I$ can be constructed if one correctly guesses (in time $\mathrm{O}(n^6)$) the six vertices $x, x', y, y', z$ and $z'$. Indeed, we proved that $V \setminus A$ which is $V \setminus De(u)$ is exactly the set of vertices $t$ distinct from $x$ and $x'$ such that $\{x, x'\}$ is a module of $G[\{x, x', t\}]$. In other words, since both $x$ and $x'$ are not edited,

$$A = \{a \in V \mid ax \in E(G) \wedge ax' \notin E(G)\} \cup \{a \in V \mid ax \notin E(G) \wedge ax' \in E(G)\}$$

Similarly, $B$ and $C$ can be constructed in polynomial time given $y, y', z$ and $z'$.

Let us define the sets $B_\oplus, C_\oplus, B_+$ and $C_+$ as in the definition of nested $t$-module. We denote by $U_\oplus$ the subset of internal nodes of the subpath $Q[v', u]$ which are free and labelled $\oplus$. Since $Q[v', u]$ has at least $12\ell$ internal nodes and since there are at most $2\ell$ non-free nodes, the size of $U_\oplus$ is at least $12\ell/2 - 2\ell = 4\ell$. Observe that for any $\alpha \in U_\oplus$, $F_Q(\alpha)$ is completely joined to $K$ and to $A$ and there is no edge between $I$ and $F_Q(\alpha)$. Moreover, $F_Q(\alpha) \subseteq B$ by definition. Hence,

$$B_\oplus \supseteq \bigcup_{\alpha \in U_\oplus} F_Q(\alpha)$$

which proves that $|B_\oplus| \geq 4\ell > 3\ell$. We prove in a similar manner that the sets $B_+, C_\oplus$ and $C_+$ have size at least $3\ell + 1$. Recall that we can construct $B_\oplus, B_+, C_\oplus$ and $C_+$ in polynomial time if we are provided $A, B, C, K$ and $I$. Therefore, if indeed $A, B, C, K, I$ is a nested $\ell$-module, we can find it in polynomial time.

In order to show that the $t$-module rule applies, we need to check that there is at least one edge or one non-edge to edit. In other words, we have to prove that there is either an edge between $A$ and $I$ or a non-edge between $A$ and $K$ in $G$. Since $Q$ is an edit path, there exists $a \in A$ and $s \in V \setminus (A \cup B \cup C)$ such that $as \in S$. Since $V \setminus (A \cup B \cup C) = K \cup I$, either $s \in K$ and in that case $as$ is a non-edge in $G$ or $s \in I$ and $as$ is an edge. In both cases, the $t$-module rule applies. □

**Corollary 3.6.5.** Cograph editing has a vertex kernel of size $\mathrm{O}\left(k^2 \log k\right)$.

*Proof.* We assume that we apply the three first rules until none is applicable. We consider the cotree $T$ of $H$ and the forest $T''$ as previously defined. Recall that $T''$ is obtained from $T'$ by removing every edge of $T'$ which does not belong to an edit path. By Lemma 3.6.2, there are at most $k$ such edges. Since the value of $k$ can be supposed larger than some fixed constant, say $k \geq 560$ here (otherwise we conclude by brute force), we can assume that the number of edges in $T''$ is at least

$$\frac{n}{k+1} - 2k - 1 - k \geq \frac{409k^2(1 + \log_2 2k)}{k+1} - 3k - 1 \geq 408k(1 + \log_2 2k)$$

The forest $T''$ is covered by at most $2k$ edit paths, so, by Lemma 3.5.2, it contains a 51-sparse descending path, and we conclude by Theorem 3.6.3. If $k \geq 560$ and $n \geq 409k^2(1 + \log_2 2k)$ and if none of our four rules is applicable, we return any graph of size at most $409k^2(1 + \log_2 2k)$ which cannot be made a cograph with less than $k$ edge editions (this is returning « no »). Hence, we have designed a polynomial time (in $n$) algorithm that transforms any graph $G_{in}$ into a graph $G_{out}$ of size at most $409k^2(1 + \log_2 2k)$ such that $G_{in}$ and $G_{out}$ are equivalent instances of the cograph $k$ editing problem. □

## 3.7 Link with the rules by Guillemot et al

We reproduce here the three first reduction rules given by Guillemot et al in [17] for completeness.

*Reduction rule* 5. Remove the connected components of $G$ which are cographs.

*Reduction rule* 6. If $C = G_1 \oplus G_2$ is a connected component of $G$, then replace $C$ by $G_1 + G_2$.

*Reduction rule* 7. If $M$ is a non-trivial module of $G$ which is strictly contained in a connected component and is not an independent set of size at most $k+1$, then return the graph $G' + G[M]$ where $G'$ is obtained from $G$ by deleting $M$ and adding an independent set of size $\min\{|M|, k+1\}$ having the same neighborhood as $M$ in $G$.

We will see that if a graph is reduced under these three rules of Guillemot et al, it is also reduced under our three first rules.

**Proposition 3.7.1.** A graph $G$ is reduced for our three first rules whenever it is reduced under Rule 5, Rule 6 and Rule 7.

Let us first prove a simple property of comodules.

**Lemma 3.7.2.** Let $G$ be a graph and let $C$ be a comodule of $G$ such that $N(C) = V \setminus C$. Then,

$$G = G[C] \oplus G[V \setminus C]$$

Moreover, if $C \neq \varnothing$ and $C \neq V$, then $G$ is connected.

*Proof.* If $C = \varnothing$ or $V \setminus C = \varnothing$, then the equality is clear. Otherwise, take $x \in C$ and $y \in V \setminus C$. Since $N(C) = V \setminus C$, there exists $u \in C$ such that $uy \in E$. Since $C$ is a module, $xy \in E$. Hence,

$$G = G[C] \oplus G[V \setminus C]$$

Let us assume that $C \neq \varnothing$ and $C \neq V$. We will prove that $G$ is connected. Consider $u, v \in V$. Since $G = G[C] \oplus G[V \setminus C]$,

- if $u \in C$ and $v \in V \setminus C$, then we have that $uv \in E$,
- if $u \in C$ and $v \in C$, take $x \in V \setminus C$ and observe that $ux \in E$ and that $vx \in E$, hence, $u$ and $v$ are connected by a path.
- if $u \in V \setminus C$ and $v \in V \setminus C$, take $x \in C$ and observe that $vx \in E$ and $ux \in E$, hence, $u$ and $v$ are connected by a path.

□

Let us now prove Proposition 3.7.1.

*Proof.* Let $G$ be a graph that is reduced under Rule 5, Rule 6 and Rule 7.

Assume by contradiction that Rule 1 applies. Then, there exists a comodule $C$ that induces a cograph in $G$.

- If $N(C) = \varnothing$, then Rule 5 applies inside $C$ as $C$ is a disjoint union of connected components of $G$ (and $C \neq \varnothing$ since otherwise no rule applies to $C$): contradiction.

- Otherwise, $N(C) = V \setminus C$, we have, by Lemma 3.7.2 that

$$G = G[C] \oplus G[V \setminus C]$$

Moreover, since $C \neq V$ (otherwise Rule 5 applies) and $C \neq \varnothing$ (otherwise no rule applies to $C$), we have that $G$ is connected. Hence, Rule 6 applies: contradiction.

Assume by contradiction that Rule 2 applies. Then, there exists a module $M$ in $G$ such that $|M| > k + 1$ and $M$ is an independent set.

- If $N(M) = \varnothing$, then take any vertex $v \in M$ (again, $M \neq \varnothing$ as Rule 2 applies). Such a vertex is by itself a connected component of $G$ that induces a cograph. So, Rule 5 applies.

- Otherwise, since $M$ is a module,

$$\exists x \in V \setminus M \quad \forall v \in M \qquad vx \in E$$

Hence, $M$ is a non-trivial module that is not an independent set of size at most $k+1$ (we assumed that $|M| > k+1$) and $M$ is strictly contained in a connected component of $G$ so Rule 7 applies: contradiction.

Assume by contradiction that Rule 3 applies. Then, there exists a module $X$ of $G$ such that $X$ is not a comodule and $G[X]$ contains an edge. Since $X$ is a not a comodule, there exists $x, y \in V \setminus X$ such that

$$\forall v \in X \qquad vx \in E \wedge vy \notin E$$

Let $H$ be the connected component of $x$. We have that $X$ is strictly contained in $H$. Besides, $X$ is a non-trivial module and is not an independent set as $G[X]$ contains an edge. Hence, Rule 7 applies: contradiction. □

There exists graphs that are reduced under our three first reduction rules but not under Rule 5, Rule 6 and Rule 7. For instance, consider a graph that is a fulljoin between two $P_4$: it is reduced under our rules but Rule 6 applies. In order to have the equivalence, we can add the following rule:

*Reduction rule* 8. If $G = X \oplus Y$, replace $G$ by $X + Y$.

**Proposition 3.7.3.** Let $G$ be a graph. If $G$ is reduced under Rule 8, Rule 1, Rule 2 and Rule 3, then it is reduced under Rule 5, Rule 6 and Rule 7.

*Proof.* Let $G$ be a graph that is reduced under Rule 8, Rule 1, Rule 2 and Rule 3.

Assume by contradiction that Rule 5 applies. Then, $G$ has a connected component $C$ that is a cograph and Rule 1 applies: contradiction.

Assume by contradiction that Rule 6 applies. Then, there exists a connected component $C$ of $G$ such that

$$C = G_1 \oplus G_2$$

where $G_1$ and $G_2$ are subgraphs of $G$.

- If $C = G$ then Rule 8 applies: contradiction.
- Otherwise, $C$ is a comodule.
  - If $C$ is a cograph, then Rule 1 applies: contradiction.
  - Otherwise, $C$ has an induced $P_4$. Observe that $G_1$ and $G_2$ are modules. Hence, by Lemma 3.3.1, such a $P_4$ is either included in $G_1$ or included in $G_2$. Assume, without loss of generality that it is included in $G_1$. Then, $G_1$ is a module that is not a comodule and such that $G[G_1]$ contains an edge. Hence, Rule 3 applies: contradiction.

Assume by contradiction that Rule 7 applies. Then, there exists a non-trivial module $M$ strictly contains in a connected component of $G$ such that $M$ is not an independent set of size at most $k + 1$.

- If $M$ is an independent set, then $|M| > k + 1$ and Rule 2 applies: contradiction.
- Otherwise, $G[M]$ contains an edge.
  - If $M$ is a comodule, then, since $N(M) \neq \varnothing$, we have, by Lemma 3.7.2, that
    $$G = G[M] \oplus G[V \setminus M]$$
    and Rule 8 applies: contradiction.
  - Otherwise, $M$ is a module that is not a comodule and such that $G[M]$ contains an edge. Hence, Rule 3 applies: contradiction.

□

# Chapter 4

# Conclusion

In this thesis, we developed algebraic tools in order to study combinatorial problems on graphs, mainly about coloring.

First, we defined *power graphs*, a structure that enhances the ground graph $G$. We did study essentially to kinds of power graphs:

- ${\mathbb{Z}_k}^G$, in which Nullstellensatz certificates have a combinatorial meaning in terms of edge-cliques
- ${\mathbb{F}_q}^G$, when $q$ is a non trivial power of a prime number, which we proved to be a different object in general (see Proposition 1.4.5)

Those graphs have interesting properties in general and allow us to have, whenever $G$ is not $k$-colorable, a generic certificate of non $k$-colorability (see Theorem 1.3.6). However, in order to prove it, we made two distinct proofs: one for ${\mathbb{Z}_k}^G$ and another for ${\mathbb{F}_k}^G$. The former uses Nullstellensatz whereas the latter relies on the property that, in a field, a product of two non zero elements cannot be zero. Thanks to this property that we do not have in $\mathbb{Z}_k$ (except[1] if $k$ is prime), we proved that $\chi(G) \leq q \Leftrightarrow \chi\left({\mathbb{F}_q}^G\right) \leq q$ (see Theorem 1.4.1). We did study the structure of power graphs and did wonder about edge editing of those constrained structures. When working on edge editing, we improved a result of Guillemot et al ([17]) by providing a $O(k^2 \log k)$ kernel for the edge editing problem on cographs.

When studying the $k$-colorings of ${\Gamma_k}^G$, we found that this graph could also be used in order to prove colorability results. Indeed, one can make a certificate of absence of edge-clique certificate. This is what we called *precoloring*. The existence of a non zero precoloring for ${\mathbb{Z}_k}^G$ or ${\mathbb{F}_k}^G$ provides a proof that $\chi(G) \leq k$. Moreover, the set of all precolorings is a linear space. Finding a basis was then a natural goal.

We found such a basis for the precolorings in $\mathbb{C}$ (see Proposition 2.2.11) and discovered a link with Fourier matrices. The vectors of that basis are nothing but Fourier transform of the indicator vectors of the good $k$-colorings of $G$. Unfortunately, these vectors are hard

[1] A finite ring that is an integral domain is a field.

to understand and to manipulate as there support is maximal. However, by making some well chosen linear combinations, we managed to create rather simple precolorings for usual graphs like cycles.

This allows for a new proof method in case one wants to prove colorability results on graphs that naturally decompose as the union of two graphs $G_1 \cup G_2$ on the same vertex set. Indeed, if the inner product of two precolorings $f$ (for $G_1$) and $g$ (for $G_2$), is non zero, then, there must exists a $k$-labelling that is a proper coloring for both $G_1$ and $G_2$. Although promising, this method is hard to use in practice. Indeed, arguing that the inner product is non zero is the tricky part: we must find "good" precolorings, which is also hard. Moreover, it could be that we are unlucky and that the two chosen precolorings are orthogonal. Using this technique, we managed to prove the Erdös conjecture on cycle+triangle , which has already been proven by Fleischner and Stiebitz in [30].

We hope that, despite the fact that some proofs which are usually straightforward becomes hard with Fourier, this is because Fourier proofs are really different from combinatorial ones. Perhaps, some results which have complex combinatorial proofs will be easier with Fourier. The *uncertainty principle* allows us to hope that small support in the real worlds (which means, only a few solutions), translates to big support in the Fourier world.

# Appendix A

# Useful lemma

## A.1 Some useful lemma

### A.1.1 Definitions

**Definition A.1.1.** Let $E$ be a $\mathbb{K}$-linear space. A *bilinear form* is a map $\langle \bullet, \bullet \rangle : E \times E \to \mathbb{K}$ such that for every $x \in E$, both $\langle x, \bullet \rangle$ and $\langle \bullet, x \rangle$ are linear. We say that $\langle \bullet, \bullet \rangle$ is *symmetric* whenever

$$\forall x, y \in E \qquad \langle x, y \rangle = \langle y, x \rangle$$

We define $\operatorname{Ker} \langle \bullet, \bullet \rangle := \{x \in \mathbb{K}^n \colon \langle x, \bullet \rangle = 0\}$. We say that $\langle \bullet, \bullet \rangle$ is *non degenerate* whenever $\operatorname{Ker} \langle \bullet, \bullet \rangle = \{0\}$.

**Definition A.1.2.** Let $\mathbb{K}$ be a field and $n \geq 1$ an integer. We define the bilinear form $\langle \bullet, \bullet \rangle : \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ by

$$\forall ((x_1, \cdots, x_n), (y_1, \cdots, y_n)) \in \mathbb{K}^n \times \mathbb{K}^n \qquad \langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = \sum_{i=1}^{n} x_i y_i$$

**Fact A.1.3.** This bilinear form is symmetric and non degenerate.

*Warning.* This bilinear form could have non zero isotropic vectors (vectors $x$ such that $\langle x, x \rangle = 0$). For instance, consider the vector full of 1 on ${\mathbb{F}_p}^p$ with $p$ a prime number.

**Definition A.1.4.** Let $\mathbb{K}$ be a field, $E$ be a $\mathbb{K}$-linear space and $\langle \bullet, \bullet \rangle$ be a symmetric bilinear form on $E \times E$. If $F$ is a subspace of $E$, then we define the linear subspace

$$F^{\perp} = \left\{ x \in E \mid \langle x, \bullet \rangle_{|F} = 0 \right\}$$

**Notation.** If $x \in E$, we denote $\{x\}^{\perp}$ by $x^{\perp}$.

*Warning.* We always have that ${F^{\perp}}^{\perp} \supseteq F$ but without other assumptions on $\langle \bullet, \bullet \rangle$, it may be that $F \neq {F^{\perp}}^{\perp}$. Moreover, we could not have the usual property $E = F \oplus F^{\perp}$. However, if $\langle \bullet, \bullet \rangle$ is non degenerate and if $E$ has finite dimension, then ${F^{\perp}}^{\perp} = F$. If we also have that $\langle \bullet, \bullet \rangle$ has no isotropic vector then $E = F \oplus F^{\perp}$.

**Definition A.1.5.** Let $E$ be a $\mathbb{K}$-linear space and $\langle \bullet, \bullet \rangle$ a symmetric bilinear form. Let $(e_1, \dots, e_k)$ be a family of vectors of $E$. We say that the family $(e_1, \dots, e_k)$ is *orthogonal* whenever every pair or vectors of this family are orthogonal. More formally,

$$\forall i, j \in [\![ 1 \ ; \ k ]\!] \qquad i \neq j \Rightarrow \langle e_i, e_j \rangle = 0$$

**Notation.** When $x$ and $y$ are orthogonal (that is, satisfy $\langle x, y \rangle = 0$), we write $x \perp y$.

**Proposition A.1.6.** Let $E$ be a $\mathbb{K}$-linear space of finite dimension and $\langle \bullet, \bullet \rangle$ be a bilinear symmetric form. There exists an orthogonal basis for $\langle \bullet, \bullet \rangle$.

*Proof.* If $\langle \bullet, \bullet \rangle$ is the zero function then any basis of $E$ is fine. Assume $\langle \bullet, \bullet \rangle \neq 0$. We do an induction on the dimension $n$ of $E$.

If $n = 1$ then any basis of $E$ is fine. Assume the result to be true for every $\mathbb{K}$-linear spaces of dimension $n$. Consider a $\mathbb{K}$-linear space $E$ of dimension $n+1$. Let $v \in E \setminus \{0\}$. Since $\langle \bullet, \bullet \rangle$ is non degenerate and $v \neq 0$, $\langle v, \bullet \rangle$ is not the zero linear form. Hence, $H := \operatorname{Ker} \langle v, \bullet \rangle$ is a hyperplane. By induction hypothesis ($\langle \bullet, \bullet \rangle_{|H \times H}$ is a symmetric bilinear form), there exists an orthogonal basis of $H$, say $(e_1, \dots, e_n)$. Since $v \neq 0$ and $v \notin H$, $E = H \oplus \mathbb{K}v$. Hence, $(e_1, \dots, e_n, v)$ is a basis of $E$. Moreover, this basis is orthogonal by construction. □

**Definition A.1.7.** Let $E$ be a $\mathbb{K}$-linear space of finite dimension. We define $E^*$ to be the set of linear forms. In other words, $E^*$ is the set of every linear map from $E$ to $\mathbb{K}$.

*Remark.* The set $E^*$ is a $\mathbb{K}$-linear space.

**Lemma A.1.8.** Let $E$ be a $\mathbb{K}$-linear space of finite dimension and $\langle \bullet, \bullet \rangle$ be a non degenerate bilinear symmetric form.

$$\forall f \in E^* \quad \exists ! \, x \in E \qquad f = \langle x, \bullet \rangle$$

*Proof.* By Proposition A.1.6, there exists an orthogonal basis of $E$ $(e_1, \dots, e_n)$. For every $f \in E^*$ and every $x = \sum_{i=1}^{n} x_i e_i \in E$,

$$f(x) = \sum_{i=1}^{n} x_i f(e_i) = \sum_{i=1}^{n} f(e_i) x_i = \left( \sum_{i=1}^{n} f(e_i) {e_i}^* \right)(x)$$

where ${e_i}^*$ is the coordinate function on $e_i$. Since $\langle \bullet, \bullet \rangle$ is non degenerate and $(e_1, \dots, e_n)$ orthogonal, we have that

$$\forall i \in [\![ 1 \ ; \ n ]\!] \qquad \langle e_i, e_i \rangle \neq 0$$

Indeed, assume by contradiction that for some $i \in [\![ 1 \ ; \ n ]\!]$ we have that $\langle e_i, e_i \rangle = 0$. Then, since $e_i$ is orthogonal to every vector of the basis, $e_i \in E^{\perp}$. However, because $\langle \bullet, \bullet \rangle$ is non degenerate, this means $e_i = 0$ and so $(e_1, \dots, e_n)$ cannot be a basis of $E$. It follows that

$$\forall i \in [\![ 1 \ ; \ n ]\!] \qquad {e_i}^* = \frac{1}{\langle e_i, e_i \rangle} \langle e_i, \bullet \rangle$$

so

$$f = \sum_{i=1}^{n} f(e_i) \frac{1}{\langle e_i, e_i \rangle} \langle e_i, \bullet \rangle = \left\langle \sum_{i=1}^{n} f(e_i) \frac{1}{\langle e_i, e_i \rangle} e_i, \bullet \right\rangle$$

Assume that there exists $x, y \in E$ such that $f = \langle x, \bullet \rangle = \langle y, \bullet \rangle$. Then, $\langle x - y, \bullet \rangle = 0$ and so $x = y$ since $\langle \bullet, \bullet \rangle$ is non degenerate. □

*Warning.* This is not a corollary of the Riesz representation theorem! Indeed, our linear spaces are not over $\mathbb{R}$ or $\mathbb{C}$ and we assumed the dimension to be finite. Indeed, the existence of a basis is crucial in the proof.

**Corollary A.1.9.** Let $E$ be a $\mathbb{K}$-linear space of finite dimension and $\langle \bullet, \bullet \rangle$ a non degenerate symmetric bilinear form. The linear map $x \mapsto \langle x, \bullet \rangle$ is an isomorphism between $E$ and $E^*$.

**Corollary A.1.10.** Let $E$ be a $\mathbb{K}$-linear space of finite dimension and $\langle \bullet, \bullet \rangle$ a non degenerate symmetric bilinear form. For every hyperplane $H$ of $E$, there exists a vector $x \in E$ such that $H = \operatorname{Ker} \langle x, \bullet \rangle$.

**Proposition A.1.11.** Let $E$ be a $\mathbb{K}$-linear space of finite dimension and let $\langle \bullet, \bullet \rangle$ be a non degenerate bilinear symmetric form. For every linear subspace $F$, $F^{\perp\perp} = F$.

*Proof.* First, observe that $F \subseteq F^{\perp\perp}$. We will show that $\dim F^{\perp\perp} \leq \dim F$. To do so, let us consider an orthogonal basis $(e_1, \dots, e_p)$ of $F$ (which exists by Proposition A.1.6) and define

$$\phi : \left\{ \begin{array}{ccc} E & \to & F^{\perp *} \\ x & \mapsto & \langle x, \bullet \rangle_{|F^\perp} \end{array} \right. \qquad \text{and} \qquad \mathrm{p}_F : \left\{ \begin{array}{ccc} E & \to & F \\ x & \mapsto & \sum_{i=1}^{p} \langle e_i, x \rangle \, e_i \end{array} \right.$$

Observe that $F^\perp \subseteq \operatorname{Ker} \mathrm{p}_F$ and $\operatorname{Ker} \phi = F^{\perp\perp}$. We will now show that $\operatorname{Ker} \mathrm{p}_F = F^\perp$. Let $x \in \operatorname{Ker} \mathrm{p}_F$. Since $(e_1, \dots, e_p)$ is a free family, we have that

$$\forall i \in [\![ 1 \ ; \ p ]\!] \qquad \langle e_i, x \rangle = 0$$

hence $x \in F^\perp$. So, $F^\perp = \operatorname{Ker} \mathrm{p}_F$. Let us show that $\operatorname{rk} \phi = \dim F^\perp$. By Corollary A.1.9, $\dim F^{\perp *} = \dim F^\perp$ and moreover, $\operatorname{Im} \phi = F^{\perp *}$ so $\operatorname{rk} \phi = \dim F^{\perp *} = \dim F^\perp$. Hence, by rank theorem,

$$\dim F^{\perp\perp} = \dim E - \operatorname{rk} \phi = \dim E - \dim F^\perp = \operatorname{rk} \mathrm{p}_F \leq \dim F$$

□

**Proposition A.1.12.** Let $E$ be a $\mathbb{K}$-linear space of finite dimension and let $\langle \bullet, \bullet \rangle$ be a non degenerate bilinear symmetric form. For every $x, y \in E \setminus \{0\}$ such that $x \notin \mathbb{K}y$ and $y \notin \mathbb{K}x$, there exists $z \in x^\perp$ such that $z \not\perp y$.

*Proof.* Consider $x, y \in E \setminus \{0\}$ such that $x \notin \mathbb{K}y$ and $y \notin \mathbb{K}x$. Observe that $\mathbb{K}y \not\subseteq \mathbb{K}x$. Assume for the sake of contradiction that

$$\forall z \in x^\perp \qquad \langle z, y \rangle = 0$$

Observe that $x^\perp = (\mathbb{K}x)^\perp$. Hence we have that

$$(\mathbb{K}x)^\perp \subseteq (\mathbb{K}y)^\perp$$

then

$$(\mathbb{K}y)^{\perp\perp} \subseteq (\mathbb{K}x)^{\perp\perp}$$

by Proposition A.1.11, it follows that $\mathbb{K}y \subseteq \mathbb{K}x$ which is a contradiction. □

### A.1.2 Duality lemma

In the following, $\mathbb{K}$ will be a field and $k, n$ will be integers greater than 1.

**Fact A.1.13.** For any matrix $M \in \mathscr{M}_{n,k}(\mathbb{K})$, we have that

- $(\operatorname{Im} M)^{\perp} = \operatorname{Ker}{}^{\mathrm{t}}M$
- $\operatorname{Im} M = (\operatorname{Ker}{}^{\mathrm{t}}M)^{\perp}$

*Proof.* Let $M \in \mathscr{M}_{n,k}(\mathbb{K})$ and $y \in \mathbb{K}^n$. We denote by $C_1, \cdots, C_k$ the columns of $M$. We have that

$$\begin{aligned} y \in \operatorname{Ker}{}^{\mathrm{t}}M &\Leftrightarrow \forall i \in [\![ 1 \ ; \ k ]\!] \qquad \langle C_i, y \rangle = 0 \\ &\Leftrightarrow y \in (\operatorname{Im} M)^{\perp} \end{aligned}$$

Since $\langle \bullet, \bullet \rangle$ is non degenerate and the dimension of $\mathbb{K}^n$ is finite, we have $(\operatorname{Im} M)^{\perp\perp} = \operatorname{Im} M$ by Proposition A.1.11. □

**Lemma A.1.14.** Let $M \in \mathscr{M}_{n,k}(\mathbb{K})$. For every $y \in \mathbb{K}^n$, the equation of the variable $x$ "$Mx = y$" has a solution over $\mathbb{K}^k$ if and only if

$$\forall z \in \mathbb{K}^n \qquad {}^{\mathrm{t}}zM = 0 \Rightarrow {}^{\mathrm{t}}zy = 0$$

*Proof.* This equation has a solution if and only if $y \in \operatorname{Im} M$ but thanks to Fact A.1.13 this is equivalent to $y \in (\operatorname{Ker}{}^{\mathrm{t}}M)^{\perp}$. □

**Corollary A.1.15.** If a matrix $M \in \mathscr{M}_{n,k}(\mathbb{K})$ has not full column rank, then there exists $S \in \mathbb{K}^n \setminus \{0\}$ such that ${}^{\mathrm{t}}S\,M = 0$.

*Proof.* The fact that $M$ has not full column rank means that $\operatorname{Im} M \neq \mathbb{K}^n$. In particular, there exists a vector $x$ with exactly one non zero coordinate such that $x \notin \operatorname{Im} M$ (otherwise, we would have that $\operatorname{Im} M = \mathbb{K}^n$). By Lemma A.1.14, there exists $S \in \mathbb{K}^n$ such that ${}^{\mathrm{t}}SM = 0$ and ${}^{\mathrm{t}}Sx \neq 0$. In particular, $S \neq 0$. □

**Lemma A.1.16.** Let $p$ be a prime number, $\ell \geq 1$ an integer and $\mathbb{K}$ a field of characteristic $\xi$ such that $\xi \neq p$. Let $E$ be a $\mathbb{F}_{p^\ell}$-affine space of dimension 2. For every function $S : E \to \mathbb{K}$, if $S$ sums to zero on every non trivial line of $E$ then $S = 0$.

*Proof.* Let us write $m = |E|$ and $q = p^\ell$. We know that $m = q^2$. Let $k$ be the number of non trivial lines of $E$[1]. Consider an enumeration $\{x_1, \ldots, x_m\}$ of the points of $E$ and an enumeration $\{\ell_1, \ldots, \ell_k\}$ of the non trivial lines. Let $M$ be the incidence matrix of $\{x_1, \ldots, x_m\}$ versus $\{\ell_1, \ldots, \ell_k\}$. We will show that $M$ has rank $m$.

[1] More precisely we have that $k = \frac{\binom{q^2}{2}}{\binom{q}{2}} = q(q+1)$.

If we sum all the columns corresponding to some partition of the space[2], we get the vector

$$^{\mathrm{t}}\begin{bmatrix}1 & \cdots & 1\end{bmatrix} \in \mathbb{K}^m$$

Now consider a point $x_i \in E$. Without loss of generality, we can assume that $i = 1$. If we sum every columns of $M$ corresponding to lines containing $x_1$, we obtain the vector

$$^{\mathrm{t}}\begin{bmatrix}m-1 & 1 & \cdots & 1\\ q-1\end{bmatrix} = {}^{\mathrm{t}}\begin{bmatrix}q+1 & 1 & \cdots & 1\end{bmatrix}$$

So, the vector

$$^{\mathrm{t}}\begin{bmatrix}q+1 & 1 & \cdots & 1\end{bmatrix} - {}^{\mathrm{t}}\begin{bmatrix}1 & \cdots & 1\end{bmatrix} = {}^{\mathrm{t}}\begin{bmatrix}q & 0 & \cdots & 0\end{bmatrix}$$

belongs to $\operatorname{Im} M$. Moreover, since $\xi \neq p$, this last vector is non zero so $\epsilon_1 \in \operatorname{Im} M^\top$. We can do this for every vector of the standard basis which proves that $M$ has rank $m$. Therefore, the only solution of $Mx = \epsilon_i$ over $\mathbb{K}^m$ is zero which concludes the proof. □

*Remark.* Beware that this result may not hold if the characteristic of the field $\mathbb{K}$ is the same of the one of $\mathbb{F}_{p^\ell}$ (that is $p$). For a counter example consider

$$S : \begin{cases} \left(\mathbb{F}_{p^\ell}\right)^2 & \to & \mathbb{F}_{p^\ell} \\ x & \mapsto & 1 \end{cases}$$

**Proposition A.1.17.** Let $G$ and $G'$ be two isomorphic graphs. For every graph $H$ and every edge-labelling $c_H$ of $H$, the graphs $H^G$ and $H^{G'}$ defined with $c_H$ are isomorphic.

*Proof.* Let $f : V(G) \to V(G')$ be a graph isomorphism between $G$ and $G'$. Define

$$f^H : \begin{cases} V(H)^{V(G)} & \to & V(H)^{V(G')} \\ \phi & \mapsto & \phi \circ f^{-1} \end{cases}$$

and let us show that $f^H$ is a graph isomorphism between $H^G$ and $H^{G'}$.

Take $\phi\psi \in E\left(H^G\right)$. By definition, there exists $uv \in E(G)$ such that

$$\begin{cases} \forall w \in V - \{u, v\} \quad \phi(w) = \psi(w) \\ \phi(u)\psi(u) \in E(H) \\ \phi(v)\psi(v) \in E(H) \\ c_H\left(\psi(u), \phi(u)\right) = c_H\left(\phi(v), \psi(v)\right) \end{cases}$$

Observe that

$$\forall w \in V - \{u, v\} \quad f^H(\phi)(f(w)) = f^H(\psi)(f(w))$$

Moreover,

$$\begin{aligned} c_H(f^H(\psi)(f(u)), f^H(\phi)(f(u))) &= c_H(\psi(u), \phi(u)) \\ &= c_H(\phi(v), \psi(v)) \\ c_H(f^H(\psi)(f(u)), f^H(\phi)(f(u))) &= c_H(f^H(\phi)(f(v)), f^H(\psi)(f(v))) \end{aligned}$$

[2]For instance, since $E$ is a plane, one can consider all the "horizontal" lines.

Since $f$ is an isomorphism, this proves that $f^H$ is a bijective graph homomorphism between $H^G$ and $H^{G'}$. Moreover, the same calculus applied to $f^{H^{-1}} = \bullet \circ f$ proves that $f^{H^{-1}}$ is a graph homomorphism. □

# Appendix B

# Some Fourier matrices

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & \mathrm{j} & \bar{\mathrm{j}} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} \\ 1 & 1 & 1 & \mathrm{j} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 & \bar{\mathrm{j}} & 1 & \mathrm{j} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & 1 \\ 1 & 1 & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} \\ 1 & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \bar{\mathrm{j}} & \mathrm{j} & 1 & \mathrm{j} & 1 & \bar{\mathrm{j}} \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} \\ 1 & 1 & 1 & \mathrm{j} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 & \bar{\mathrm{j}} & 1 & \mathrm{j} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & 1 \\ 1 & 1 & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} \\ 1 & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \bar{\mathrm{j}} & \mathrm{j} & 1 & \mathrm{j} & 1 & \bar{\mathrm{j}} \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \mathrm{j} & 1 & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} \\ 1 & 1 & 1 & \mathrm{j} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & 1 & 1 & \mathrm{j} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & 1 & 1 & \mathrm{j} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 & \bar{\mathrm{j}} & 1 & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 & \bar{\mathrm{j}} & 1 & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 & \bar{\mathrm{j}} & 1 & \mathrm{j} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & 1 & 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & 1 & 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & 1 \\ 1 & 1 & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} & 1 & 1 & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} & 1 & 1 & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} \\ 1 & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 & 1 & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 & 1 & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \bar{\mathrm{j}} & \mathrm{j} & 1 & \mathrm{j} & 1 & \bar{\mathrm{j}} & 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 & \bar{\mathrm{j}} & 1 & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 & \bar{\mathrm{j}} & 1 & \mathrm{j} \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \mathrm{j} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} \\ 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} \\ 1 & 1 & 1 & \mathrm{j} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & 1 & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & 1 & 1 & \mathrm{j} & \mathrm{j} & \mathrm{j} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 & \bar{\mathrm{j}} & 1 & \mathrm{j} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & \mathrm{j} & 1 & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & 1 & 1 & \mathrm{j} & \bar{\mathrm{j}} & \mathrm{j} & \bar{\mathrm{j}} & 1 \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & 1 & \mathrm{j} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & 1 & \bar{\mathrm{j}} \\ 1 & 1 & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} & 1 & 1 & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} & 1 & 1 & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & \mathrm{j} \\ 1 & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} & \bar{\mathrm{j}} & 1 & \mathrm{j} \\ 1 & \bar{\mathrm{j}} & \mathrm{j} & \bar{\mathrm{j}} & \mathrm{j} & 1 & \mathrm{j} & 1 & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & 1 & \mathrm{j} & 1 & \bar{\mathrm{j}} & 1 & \bar{\mathrm{j}} & \mathrm{j} & \mathrm{j} & 1 & \bar{\mathrm{j}} & 1 & \bar{\mathrm{j}} & \mathrm{j} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \bar{\mathrm{j}} & \mathrm{j} & 1 \end{bmatrix}$$

# Appendix C

# Deferred proofs

## C.1 Detailed proof of the introductive problem of Section 2.1

**Proposition C.1.1.** Every simple 4-regular bipartite graph has a cycle factor.

*Proof.* Let $G = (A \uplus B, E)$ be a simple 4-regular bipartite graph. Our goal is to show that there exists a choice of edges such that every vertex has exactly 2 chosen edges. More formally, we want to prove that there exists $x : E \to \mathbb{F}_2$ such that

$$\forall v \in V \quad |\{e \in E \colon v \in e \wedge x(e) = 1\}| = 2 \tag{C.1}$$

The idea is to split the constraints among the bipartition. Let us define

$$f_A : \begin{cases} {\mathbb{F}_2}^E & \to & \mathbb{C} \\ x & \mapsto & \begin{cases} 1 & \text{if} \quad \forall v \in A \quad |\{e \in E \colon v \in e \wedge x(e) = 1\}| = 2 \\ 0 & \text{otherwise} \end{cases} \end{cases}$$

and

$$f_B : \begin{cases} {\mathbb{F}_2}^E & \to & \mathbb{C} \\ x & \mapsto & \begin{cases} 1 & \text{if} \quad \forall v \in B \quad |\{e \in E \colon v \in e \wedge x(e) = 1\}| = 2 \\ 0 & \text{otherwise} \end{cases} \end{cases}$$

There exists a function $x$ that fulfills the condition C.1 if and only if $\langle f_A, f_B \rangle \neq 0$. Actually, $\langle f_A, f_B \rangle$ is exactly the number of such functions hence the number of cycle factors.

The idea is to compute $\left\langle \widehat{f_A}, \widehat{f_B} \right\rangle$ instead of $\langle f_A, f_B \rangle$. We start by computing these two vectors. Let $x \in {\mathbb{F}_2}^E$. First, we prove that $\widehat{f_A}(x) = 0$ whenever $x$ has an odd number of ones (more formally, when $|x|_1 \in 2\mathbb{N} + 1$). Let us start by examining what happen on a single vertex, that is, in the hypothetical case where $|A| = 1$. We denote $f_A$ by $f_{A_1}$ and we let $\Gamma$ to be the set of $y \in {\mathbb{F}_2}^E$ that have exactly 2 ones. More formally,

$$\Gamma = \left\{ y \in {\mathbb{F}_2}^E \colon |\{e \in E \colon y(e) = 1\}| = 2 \right\}$$

Observe that if $y \in \Gamma$ then $\bar{y} = \mathbf{1} - y \in \Gamma$, $\bar{y} \neq y$ and $\langle x, y \rangle \neq \langle x, \bar{y} \rangle$ [2] since $x$ has an odd number of ones. Hence,

$$\widehat{f_{A_1}}(x) = \frac{1}{\sqrt{2}^4} \sum_{y \in \Gamma} (-1)^{\langle x, y \rangle} = 0$$

Moreover, the value $\widehat{f_{A_1}}(x)$ only depends on the number of ones in $x$ which we denote by $|x|_1$. We say that $v \in A$ is *monochromatic (in $x$)* if

- either $x(e) = 0$ for every $e \in E$ such that $e \ni v$
- or $x(e) = 1$ for every $e \in E$ such that $e \ni v$

and that $v$ is *bichromatic (in $x$)* if $v$ is not monochromatic. More generally, we say that $v$ has degree $k$ in $x$ if $v$ has degree $k$ in the subgraph obtained by removing the edges $e$ such that $x(e) = 0$. We have that

$$\forall x \in {\mathbb{F}_2}^E \quad 4\widehat{f_{A_1}}(x) = \begin{cases} 0 & \text{if} \quad |x|_1 \in 2\mathbb{N}+1 \\ 6 & \text{if} \quad |x|_1 = 0 \vee |x|_1 = 4 \\ -2 & \text{if} \quad |x|_1 = 2 \end{cases}$$

Now, observe that ${f_A} = {f_{A_1}}^{\otimes n/2}$ hence

$$\widehat{f_A} = F_{2,2n} f_A = {F_2}^{\otimes 2n} {f_{A_1}}^{\otimes n/2} = \left({F_2}^{\otimes 4} f_{A_1}\right)^{\otimes n/2} = \widehat{f_{A_1}}^{\otimes n/2}$$

so,

$$\forall x \in {\mathbb{F}_2}^E \, \widehat{f_A}(x) = \begin{cases} \dfrac{1}{2^n} 6^{|A_0(x)|+|A_4(x)|}(-2)^{|A_2(x)|} & \text{if } \forall v \in A \, v \in A_0(x) \cup A_2(x) \cup A_4(x) \\ 0 & \text{otherwise} \end{cases}$$

where for every $i \in [\![ 0 \,;\, 4 ]\!]$, $A_i(x)$ is the set of vertices of degree $i$ in $x$. More formally,

$$A_i(x) := \{v \in A \colon |\{e \in E \colon v \in e \wedge x(e) = 1\}| = i\}$$

Since $A$ and $B$ plays symmetric roles, we have that

$$\forall x \in {\mathbb{F}_2}^E \, \widehat{f_B}(x) = \begin{cases} \dfrac{1}{2^n} 6^{B_0(x)+B_4(x)}(-2)^{B_2(x)} & \text{if } \forall v \in B \, v \in B_0(x) \cup B_2(x) \cup B_4(x) \\ 0 & \text{otherwise} \end{cases}$$

where $B_i$ is the analog of $A_i$. We can now compute the inner product:

$$\langle f_A, f_B \rangle = \left\langle \widehat{f_A}, \widehat{f_B} \right\rangle = \sum_{x \in {\mathbb{F}_2}^E} \widehat{f_A}(x) \widehat{f_B}(x)$$

Observe that if $\widehat{f_A}(x) \neq 0$ and $\widehat{f_B}(x) \neq 0$, then $\widehat{f_A}(x)$ (resp $\widehat{f_B}(x)$) is negative if and only if $|x|_1 = 2\,[4]$ that is if and only if there is an odd number of degree 2 vertices in $x$. Hence, $\widehat{f_A}(x)$ and $\widehat{f_B}(x)$ both have the same sign so the inner product is a sum of non negative terms. In order to prove it is non zero, we just have to provide one strictly positive term: $x = 0$ for instance. □

**Proposition C.1.2.** Every 4-regular graph has an Eulerian orientation.

*Proof.* Let $G = (V, E)$ be a 4-regular graph. We consider the subdivided graph $G_\bullet$ (see Definition 2.1.3). Observe that $G$ has an Eulerian orientation if and only if there exists a function $x : E_\bullet \to \mathbb{F}_2$ such that

- every $v \in V$ is adjacent to exactly two edges $e$ and $e'$ so that $ve$ and $ve'$ are labelled 1
- every edge $e \in E$ has exactly one of its endpoints $v$ such that $ve$ is labelled 1

More formally this correspond to the following pair of conditions:

$$\begin{array}{ll} \forall v \in V & |\{e \in E \colon v \in e \wedge x(ve) = 1\}| = 2 \\ \forall e \in E & |\{v \in V \colon v \in e \wedge x(ve) = 1\}| = 1 \end{array} \tag{C.2}$$

Let us prove that there exists such a function $x$. Define $f_V, f_E : {\mathbb{F}_2}^{E\bullet} \to \mathbb{C}$ by

$$\forall x \in {\mathbb{F}_2}^{E\bullet} \qquad f_V(x) = \begin{cases} 1 & \text{if} \quad \forall v \in V \quad |\{e \in E \colon v \in e \wedge x(e) = 1\}| = 2 \\ 0 & \text{otherwise} \end{cases}$$

and $$\forall x \in {\mathbb{F}_2}^{E\bullet} \qquad f_E(x) = \begin{cases} 1 & \text{if} \quad \forall e \in E \quad |\{v \in V \colon v \in e \wedge x(e) = 1\}| = 1 \\ 0 & \text{otherwise} \end{cases}$$

Our goal is to show that the inner product $\langle f_V, f_E \rangle$ is non negative.

First, let us compute $\widehat{f_V} = F_{2,2m} f_V$ and $\widehat{f_E} = F_{2,2m} f_E$. We already have computed $\widehat{f_V}$ in the proof of Proposition C.1.1. We then examine the case of $f_E$ when $|E| = 1$ and denote $f_E$ by $f_{E_1}$.

$$\widehat{f_{E_1}} = \frac{1}{\sqrt{2}^2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix}$$

Since the constraints on each edge of $G$ are independent, we can use the tensor product. In the general setting, $f_E = {f_{E_1}}^{\otimes m}$ hence $\widehat{f_E} = {\widehat{f_{E_1}}}^{\otimes m}$. Moreover, we have that

$$\forall x \in {\mathbb{F}_2}^{E\bullet} \; \widehat{f_V}(x) = \begin{cases} \frac{1}{2^{2n}} 6^{|V_0(x)|+|V_4(x)|}(-2)^{|V_2(x)|} & \text{if } \forall v \in V \; v \in V_0(x) \cup V_2(x) \cup V_4(x) \\ 0 & \text{otherwise} \end{cases}$$

where for $i \in [\![ 0 \; ; \; 4 ]\!]$, $V_i(x)$ is the set of vertices of degree $i$ in $x$. More formally,

$$V_i(x) := \{v \in V \colon \; |\{e \in E \colon v \in e \wedge x(e) = 1\}| = i\}$$

This is the very same calculus we made in the proof of Proposition C.1.1. (Note the $2^{2n}$ instead of $2^n$, it is not a mistake since this time we take one tensor product per vertex of $G$.)

So, we can compute $\left\langle \widehat{f_V}, \widehat{f_E} \right\rangle$ which we know to be equal to $\langle f_V, f_E \rangle$, the number of cycle factors of $G$. For $\widehat{f_E}(x)$ to be non zero, $x$ must satisfies that every edge $e \in E$ is monochromatic in $x$. Let us call $\Gamma$ the set of such $x$. If $x \in \Gamma$ then $\widehat{f_E}(x) = 1/2^m (-1)^{|x|_1/2}$. Hence,

$$\left\langle \widehat{f_V}, \widehat{f_E} \right\rangle = \sum_{x \in {\mathbb{F}_2}^{E\bullet}} \widehat{f_V}(x) \, \widehat{f_E}(x) = \frac{1}{2^m} \sum_{x \in \Gamma} \widehat{f_V}(x) (-1)^{\frac{|x|_1}{2}}$$

Observe that $\widehat{f_V}(x)(-1)^{\frac{|x|_1}{2}}$ is always positive. Indeed,

- either $|x|_1 = 0[4]$ and there is an even number of bichromatic vertices $v \in V$ so $\widehat{f_V}(x) \geq 0$
- or $|x|_1 = 2\,[4]$ and there is an odd number of bichromatic vertices $v \in V$ so $\widehat{f_V}(x) \leq 0$

Hence, $\left\langle \widehat{f_V}, \widehat{f_E} \right\rangle$ is a sum of non negative terms. Moreover, $\widehat{f_V}(0)\widehat{f_E}(0) = 6^n/2^{m+2n} > 0$ which concludes the proof. □

**Proposition C.1.3.** The Bousquet precoloring $B_3$ satisfies

$$B_3 = -\mathrm{i}\left(|012\rangle + |120\rangle + |201\rangle - |021\rangle - |210\rangle - |102\rangle\right)$$

*Proof.* The Fourier matrix $F_{3,2}$ is already quite big ($27 \times 27$). It can be found in appendix (see B). Let us define

$$f_0 = -\mathrm{i}\left(|012\rangle + |120\rangle + |201\rangle - |021\rangle - |210\rangle - |102\rangle\right)$$

First, observe that $\forall x \in {\mathbb{F}_3}^{V(\triangle)} \quad \sum_{v \in V(\triangle)} x(v) \neq 0 \Rightarrow \widehat{f_0}(x) = 0$

Indeed, define $\mathrm{SGC}_3(\triangle) := \left\{ x \in {\mathbb{F}_3}^{V(\triangle)} : \sum_{v \in V(\triangle)} x(v) = 0 \right\}$

*Remark.* This stands for "semi-good 3-colorings".

We introduce the equivalence relation $\sim$ on ${\mathbb{F}_3}^{V(\triangle)}$ defined by

$$\forall x, y \in {\mathbb{F}_3}^{V(\triangle)} \qquad x \sim y \Leftrightarrow \exists \lambda \in \mathbb{F}_3 \quad x - y = \mathbf{1}$$

The set $\mathrm{GC}_3(\triangle)$ can be partitioned into two orbits for this equivalence relation. Moreover, if we fix $x \in {\mathbb{F}_3}^{V(\triangle)} \setminus \mathrm{SGC}_3(\triangle)$, then, for every $y \in \mathrm{GC}_3(\triangle)$,

$$\begin{aligned} \{\langle y + \lambda\mathbf{1}, x\rangle : \lambda \in \mathbb{F}_3\} &= \langle x, y\rangle + \{\lambda \langle \mathbf{1}, x\rangle : \lambda \in \mathbb{F}_3\} \\ &= \langle x, y\rangle + \mathbb{F}_3 \qquad (\text{as } \langle \mathbf{1}, x\rangle \in {\mathbb{F}_3}^*) \\ &= \mathbb{F}_3 \end{aligned}$$

so $\sum_{\lambda \in \mathbb{F}_3} \mathrm{j}^{\langle y + \lambda\mathbf{1}, x\rangle} = 0$ which proves that

$$\forall x \in {\mathbb{F}_3}^{V(\triangle)} \setminus \mathrm{SGC}_3(\triangle) \quad \widehat{f_0}(x) = 0$$

We now have to compute the value of $f_0$ on the semi-good colorings. By the calculus we just did, we know that

$$\{\langle y + \lambda\mathbf{1}, x\rangle : \lambda \in \mathbb{F}_3\} = \{\langle x, y\rangle\}$$

so $\forall x \in \mathrm{SGC}_3(\triangle) \quad \forall y \in \mathrm{GC}_3(\triangle) \qquad \sum_{\lambda \in \mathbb{F}_3} \mathrm{j}^{\langle y + \lambda\mathbf{1}, x\rangle} = 3\mathrm{j}^{\langle x, y\rangle}$

Take $x \in \mathrm{SGC}_3(\triangle)$. Recall that $\widehat{f_0}(x) = \dfrac{-\mathrm{i}}{\sqrt{3}^3} \sum_{y \in \mathrm{GC}_3(\triangle)} \mathrm{j}^{\langle x, y\rangle}$.

- If $x$ is monochromatic then $\widehat{f_0}(x) = -\mathrm{i}/\sqrt{3}^3(3 - 3) = 0$.
- Otherwise,

$$\widehat{f_0}(x) = \begin{cases} \dfrac{-\mathrm{i}}{\sqrt{3}^3}\left(3\bar{\mathrm{j}} - 3\mathrm{j}\right) = -1 & \text{if} \quad x \sim |012\rangle \\ \dfrac{-\mathrm{i}}{\sqrt{3}^3}\left(3\mathrm{j} - 3\bar{\mathrm{j}}\right) = 1 & \text{otherwise} \end{cases}$$

Finally, $\forall x \in {\mathbb{F}_3}^{V(\triangle)} \qquad \widehat{f_0}(x) = \begin{cases} 0 & \text{if} \quad x \notin \mathrm{SGC}_3(\triangle) \\ 0 & \text{if} \quad x \quad \text{is monochromatic} \\ 1 & \text{if} \quad x \not\sim |012\rangle \\ -1 & \text{otherwise} \end{cases}$

In other words, $\widehat{f_0}(x)$ is 0 if the triangle is not properly 3-colored and $+1$ or $-1$ depending on the orientation ($+1$ if "direct", $-1$ "indirect"). We can check that it is indeed a precoloring. For instance, see Figure C.1.

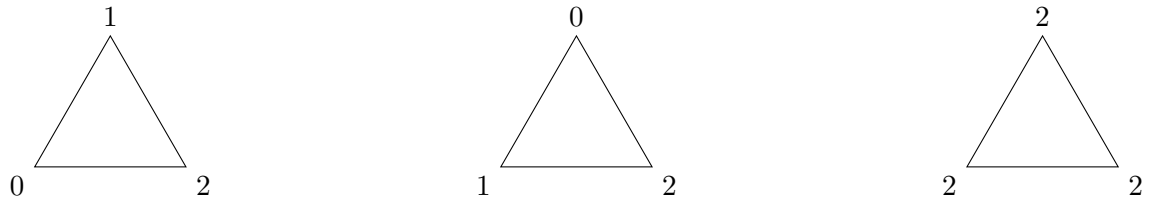



Figure C.1: The configuration of $\widehat{f_0}$ on some edge-clique

□

**Proposition C.1.4.** Let $n \geq 3$ be an odd integer. The support of the Bousquet precoloring $B_n$ is $2\,[4]$.

*Proof.* Let us count the number of labellings $x$ of $C_n$ that satisfies $B_n(x) \neq 0$. Such an $x$ must have an even number of 1 and 2 and these values must alternates along $C_n$. Let us assume that we have chosen the elements $v \in V(C_n)$ such that $x(v) = 0$. There must remain an even number of elements. Moreover, since $n$ is odd, $B_n(0) = 0$ so there must remain at least 2 elements. Once the zeros are chosen, there is two way to complete $x$ since 1 and 2 must alternates. Hence,

$$|\sup B_n| = 2 \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i}$$

The sum $\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor - 1} \binom{n}{2i}$ is equal to the number of subsets of $[\![\, 1 \,;\, n \,]\!]$ of even size. This number is even. Indeed, one can pair a subset $X$ of $[\![\, 1 \,;\, n \,]\!]$ of even size with its complement $[\![\, 1 \,;\, n \,]\!] \setminus X$ (and we always have that $X \neq [\![\, 1 \,;\, n \,]\!] \setminus X$ because $n \geq 1$. Hence, $|\sup B_n|$ is $2\,[4]$. □

# Appendix D

# Bestiary of precolorings

## D.1 Bestiary of precolorings

We give here a list of some useful precolorings.

### D.1.1 In general

**Definition D.1.1** (Universal/Charbit)**.** Take $G$ a directed[1] graph. Define

$$\Omega : \begin{cases} 2^E & \to & 3^V \\ \omega & \mapsto & \left[ \overline{\sum_{(u,v)\in E} \omega(u,v) - \sum_{(v,u)\in E} \omega(v,u)}^{3} \right]_{v\in V} \end{cases}$$

Where $\bar{\cdot}$ is the usual cast of $\mathbb{F}_2$ in $\mathbb{F}_3$.

We now define the Universal/Charbit precoloring by

$$\mathrm{Ch}_G : \begin{cases} 3^V & \to & \mathbb{Z} \\ x & \mapsto & \sum_{\omega\in\Omega^{-1}(x)} (-2)^{|\omega^{-1}(0)|} \end{cases}$$

*Remark.*

- For every $x \in 3^V$, either $x$ does not sum to zero and $\mathrm{Ch}_G(x) = 0$, or $x$ sums to zero and then $|\Omega^{-1}(x)| = |\Omega^{-1}(0)|$.
- In particular, the number of realisation of any semi good coloring on a cycle is 3.

**Proposition D.1.2.** For every graph $G$, $\mathcal{U}_G = (-1)^{|E|}\,\mathrm{Ch}_G$.

*Proof.* Let $G$ be a graph with $n$ vertices. Let's define

$$\mathcal{A} := \frac{\mathbb{K}[X_1, \cdots, X_n]}{\left\langle {X_i}^3 - 1 \right\rangle_{i\in[\![1\ ;\ n]\!]}}$$

[1] Actually the definition does not depend on the orientation but it is more convenient if we first orient $G$.

and $$P_G := \frac{1}{3^{|E|}} \prod_{ij \in E} \left(2 - X_i {X_j}^2 - {X_i}^2 X_j\right)$$

For every $x = (x_1, \ldots, x_n) \in 3^V$, we denote by $j^x$ the vector

$$j^x = (j^{x_1}, \cdots, j^{x_n})$$

Observe that $$\forall x \in 3^V \qquad P_G(j^x) \neq 0 \Leftrightarrow x \in GC(G)$$

More precisely, $$\forall x \in 3^V \qquad P_G(j^x) = \begin{cases} 1 & \text{if } x \in GC(G) \\ 0 & \text{otherwise} \end{cases}$$

Hence, $$P_G = \sum_{y \in GC(G)} \widehat{\mathbb{1}_y}$$

*Remark.* This last result is a direct consequence of Fourier interpolation. Observe that,

$$\forall x, y \in 3^V \qquad \widehat{\mathbb{1}_x} \cdot \widehat{\mathbb{1}_y} = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

So, $$\forall x \in 3^V \qquad P_G(j^x) = \widehat{\mathbb{1}_x} \cdot \sum_{y \in GC(G)} \widehat{\mathbb{1}_y}$$

We know that when we have such a polynomial $P$, then the function

$$f_P : \begin{cases} 3^V & \to & \mathbb{K} \\ x & \mapsto & [P]_x \end{cases}$$

where $[P]_x$ is the cœfficient of the monomial $x$, is a precoloring of $G$.

*Remark.* Actually, if $P = \sum \widehat{\mathbb{1}_y}$, then

$$f_P = x \mapsto \mathbb{1}_x \cdot \sum \widehat{\mathbb{1}_y}$$

So, for our polynomial $P_G$, we have that $f_{P_G} = \mathcal{U}_G$.

□

### D.1.2 Triangles

**Definition D.1.3** (Universal/Charbit)**.** $\mathcal{U}_\Delta$ :

$$\begin{cases} 3^V & \to & \mathbb{Z} \\ x & \mapsto & \begin{cases} 0 & \text{if } x \text{ does not sum to 0} \\ 2 & \text{if } x \text{ is monochromatic} \\ -1 & \text{otherwise (trichromatic)} \end{cases} \end{cases}$$

**Definition D.1.4** (The "$1j\bar{j}$")**.** We need first to be given an orientation of the triangles (cyclic order of the vertices).

$$f : \begin{cases} 3^V & \to & \mathbb{C} \\ x & \mapsto & \begin{cases} 0 & \text{if } x \text{ does not sum to 0} \\ 1 & \text{if } x \text{ is monochromatic} \\ j & \text{if trichromatic and direct} \\ \bar{j} & \text{if trichromatic and undirect} \end{cases} \end{cases}$$

### D.1.3 Cycles

**Definition D.1.5** (Bousquet)**.** Let $n \geq 3$ and $C_n$ be the cycle $(0, \ldots, n-1)$ where the vertices are in $\mathbb{Z}_n$. For every $x \in 3^{\mathbb{Z}_n}$, we define

$$N^x_{\neq 0} : \begin{cases} \mathbb{Z}_n & \to & \mathbb{Z}_n \\ i & \mapsto & \begin{cases} i & \text{if } x(i) = 0 \\ \overline{\inf\limits_{j \in \mathbb{N}^*} \{x(i+j) \neq 0\}}^n & \text{otherwise} \end{cases} \end{cases}$$

where $\overline{\cdot}^n$ is the usual injective ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_n$.

We define the Bousquet set of $C_n$ to be

$$B(C_n) := \{x \in 3^{\mathbb{Z}_n} \mid \forall i \in \mathbb{Z}_n \qquad x(i) \neq 0 \Rightarrow N^x_{\neq 0}(i) \neq x(i)\}$$

We now can define the Bousquet precoloring as

$$B_n : \begin{cases} 3^{\mathbb{Z}_n} & \to & \mathbb{Z} \\ x & \mapsto & \begin{cases} 0 & \text{if } x \notin B(C_n) - \{0\} \\ \prod\limits_{i \in x^{-1}(\{1\})} (-1)^{N^x_{\neq 0}(i)} \end{cases} \end{cases}$$

*Remark.*

- The Bousquet set is the set of labellings of $C_n$ such that 1 and 2 alternate along the cycle.
- One can observe that $B(C_n) \subseteq SGC(C_n)$. Hence, the Bousquet precoloring is, as every precoloring we consider, 0 on $3^V - SGC(G)$.
- The Bousquet precoloring has the particularity to be zero on zero.

# Appendix E

# Programs documentation

## E.1 Programs documentation

In this section, we give a short documentation of the programs we made. We also give some details about the algorithms involved.

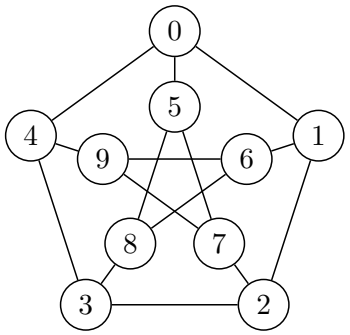
We chose to program using the C programming language (C89). We originally implemented simple programs in Python to explore power graphs but the time and memory consumption made us chose C for its ability to give control over the memory usage.

### E.1.1 A program to find edge-clique certificate

*Remark.* Our programs currently have no option to deal with ${\mathbb{F}_q}^G$ in general.

**Example E.1.1.** Here is an example of input file and the corresponding graph:

```
10
0-1
1-2
2-3
3-4
4-0
5-7
5-8
5-0
6-8
6-9
6-1
7-9
7-2
8-3
9-4
```




The field provided at the end of the command line is the field for the coefficients of

the edge-clique certificates. It can be either $\mathbb{F}_2$ (F2) or $\mathbb{R}$ (R). In the later, the program uses arbitrary precision arithmetic with the GMP library. This can be (very) memory consuming.

In order to find an edge-clique certificate, our programs list every possible edge-clique in the component of the vertices that sum to zero (remember that all these component are isomorphic) and build the incidence matrix $M$ of the vertices of ${\mathbb{Z}_k}^G$ versus these edge-cliques. Then, we use the Gauss elimination algorithm. This (very well known) algorithm consists in making elementary operation on the column of $M$ to obtain a matrix of the form

$$J_r = \begin{bmatrix} 1 & & & & & \\ 0 & \ddots & & & & \\ \vdots & & 1 & & & \\ \vdots & & & 0 & & \\ \vdots & & & & \ddots & \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 \end{bmatrix}$$

where $r = \operatorname{rk} M$ is the number of 1's on the diagonal. This algorithm also provide a matrix $R$ such that $M \times R = J_r$. The first column of $R$ is an edge-clique certificate.

Of course, the certificate we come up at the end depends on the order of the column of $M$. Everywhere else in this thesis, the order of the columns of such matrix is not specified as it has no impact on the results (on the rank in particular). Here however, the order is relevant since a permutation of the column of $M$ can result in a different edge-clique certificate. In order to find an edge-clique certificate of small degree and/or small support, the edge-cliques generated are limited at the step of creation of the power graph. To have an edge-clique certificate with a few edge-cliques as possible, we apply several rounds of Gauss pivoting. Before each round, we apply a random permutation on the columns of $M$. This can probably be improved.

# Bibliography


[1] Alon, N. Combinatorial nullstellensatz. *Combinatorics, Probability and Computing 8*, 1–2 (1999), 7–29.

[2] Alon, N., and Tarsi, M. Colorings and orientations of graphs. *Combinatorica 12* (1992), 125–134.

[3] Appel, K., and Haken, W. Every planar map is four colorable. Part I: Discharging. *Illinois Journal of Mathematics 21*, 3 (1977), 429 – 490.

[4] Bathie, G., Bousquet, N., and Pierron, T. (Sub)linear kernels for edge modification problems towards structured graph classes. *CoRR abs/2105.09566* (2021).

[5] Bayer, D. A. *The Division Algorithm and the Hilbert Scheme*. PhD thesis, Harvard University, USA, 1982. AAI8222588.

[6] Bo Li, Benjamin Lowenstein, M. O. Low degree nullstellensatz certificates for 3-colorability, 2015.

[7] Bodlaender, H. L., Downey, R. G., Fellows, M. R., and Hermelin, D. On problems without polynomial kernels. *J. Comput. Syst. Sci. 75*, 8 (2009), 423–434.

[8] Cao, Y., and Chen, J. Cluster editing: Kernelization based on edge cuts. *Algorithmica 64*, 1 (2012), 152–169.

[9] Chen, J., and Meng, J. A 2k kernel for the cluster editing problem. *J. Comput. Syst. Sci. 78*, 1 (2012), 211–220.

[10] Corneil, D., Lerchs, H., and Burlingham, L. Complement reducible graphs. *Discrete Applied Mathematics 3*, 3 (1981), 163–174.

[11] Crespelle, C., Drange, P. G., Fomin, F. V., and Golovach, P. A survey of parameterized algorithms and the complexity of edge modification. *Computer Science Review 48* (2023), 100556.

[12] de Leora, J. Gröbner bases and graph colorings. *Contributions to Algebra and Geometry 36* (1995), 89–96.

[13] De Loera, J. A., Margulies, S., Pernpeintner, M., Riedl, E., Rolnick, D., Spencer, G., Stasi, D., and Swenson, J. Graph-coloring ideals: Nullstellensatz certificates, gröbner bases for chordal graphs, and hardness of gröbner bases. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA, 2015), ISSAC '15, Association for Computing Machinery, p. 133–140.

[14] Donoho, D. L., and Stark, P. B. Uncertainty principles and signal recovery. *Siam Journal on Mathematical Analysis* (1989).

[15] Downey, R., Fellows, M., Fellows, M., Gries, D., and Schneider, F. *Parameterized Complexity*. Monographs in Computer Science. Springer New York, 1999.

[16] Fleischner, H., and Stiebitz, M. A solution to a colouring problem of P. Erdős. *Discrete Mathematics 101*, 1 (1992), 39–48.

[17] Guillemot, S., Paul, C., and Perez, A. *On the (Non-)existence of Polynomial Kernels for P l -free Edge Modification Problems*. Springer Berlin Heidelberg, 2010, p. 147–157.

[18] Hadwiger, H. Über eine klassifikation der streckenkomplexe. *Vierteljahrsschr* (1943), 133–142.

[19] Hellmuth, M., Fritz, A., Wieseke, N., and Stadler, P. F. Cograph editing: Merging modules is equivalent to editing p4's, 2019.

[20] Hierholzer, C., and Wiener, C. Ueber die möglichkeit, einen linienzug ohne wiederholung und ohne unterbrechung zu umfahren. *Mathematische Annalen 6* (1873), 30–32.

[21] Hillar, C. J., and Windfeldt, T. Algebraic characterization of uniquely vertex colorable graphs. *Journal of Combinatorial Theory, Series B 98*, 2 (2008), 400–414.

[22] Hladký, J., Král, D., and Schauz, U. Brooks' theorem via the alon-tarsi theorem. *Discret. Math. 310* (2010), 3426–3428.

[23] Liu, Y., Wang, J., Guo, J., and Chen, J. Complexity and parameterized algorithms for cograph editing. *Theoretical Computer Science 461* (2012), 45–54. 17th International Computing and Combinatorics Conference (COCOON 2011).

[24] Mancini, F. *Graph Modification Problems Related to Graph Classes*. PhD thesis, University of Bergen, Norway, 2008.

[25] Mycielski, J. Sur le coloriage des graphs. *Colloquium Mathematicae 3*, 2 (1955), 161–162.

[26] Natanzon, A., Shamir, R., and Sharan, R. Complexity classification of some edge modification problems. In *WG* (1999).