# Nouvelles applications des surfaces rationnelles et surfaces de Kummer généralisées sur des corps finis à la cryptographie à base de couplages et à la théorie des codes BCH

Dmitrii Koshelev

Thèse de doctorat

NNT: 2021UPASM001

université PARIS-SACLAY

# Nouvelles applications des surfaces rationnelles et surfaces de Kummer généralisées sur des corps finis à la cryptographie à base de couplages et à la théorie des codes BCH

*New applications of rational and generalized Kummer surfaces over finite fields in pairing-based cryptography and in the theory of BCH codes*

**Thèse de doctorat de l'université Paris-Saclay**

École doctorale n° 574, Mathématiques Hadamard (EDMH)
Spécialité de doctorat: mathématiques appliquées
Unité de recherche: Université Paris-Saclay, UVSQ, CNRS, Laboratoire de mathématiques de Versailles, 78000, Versailles, France
Référent: Université de Versailles Saint-Quentin-en-Yvelines

**Thèse présentée et soutenue à Paris-Saclay, le 09/02/2021, par**

**Dmitrii Koshelev**

## Composition du jury

| | |
|---|---|
| **M. Christophe Ritzenthaler**<br>Professeur des universités, Université de Rennes 1, Institut de Recherche Mathématique de Rennes | Président |
| **M. Marc Hindry**<br>Professeur, Université Denis Diderot Paris VII, Institut de Mathématiques de Jussieu | Rapporteur et Examinateur |
| **M. Marc Perret**<br>Professeur, Université de Toulouse-Jean Jaurès, Institut de Mathématiques de Toulouse | Rapporteur et Examinateur |
| **Mme Ekaterina Amerik**<br>Professeur, Université Paris-Saclay | Examinatrice |
| **Mme Nadia El Mrabet**<br>Maitre assistant, École des Mines de Saint-Étienne, antenne de Gardanne | Examinatrice |
| **M. Benjamin Smith**<br>Chargé de recherche, École Polytechnique, INRIA Saclay | Examinateur |

## Direction de la thèse

| | |
|---|---|
| **M. Michael Tsfasman**<br>Directeur de recherche, UVSQ | Directeur de thèse |

# Remerciements

Je voudrais exprimer ma profonde gratitude à mon directeur de thèse M. Tsfasman pour sa formidable aide tout au long de la période de mes études à l'école doctorale. Je lui suis reconnaissant de l'opportunité de discuter régulièrement de divers problèmes scientifiques et de ses précieux commentaires concernant leurs solutions et la rédaction des résultats obtenus. J'apprécie particulièrement le soutien qu'il m'a apporté lors de ma migration et adaptation en France. Il m'a aussi permis de choisir des tâches en fonction de mes préférences, ce qui a contribué à un dévélopment plus complet de mon potentiel scientifique. De plus, on ne peut pas manquer de noter son rôle important dans la recherche de diverses sources de financement pour mon travail. Le principal soutien a certainement été apporté par la Fondation Mathématique Jacques Hadamard (FMJH). Je suis très reconnaissant à ses représentants C. D'Epenoux, F. Paulin, P. Pansu et V. Sécherre pour la confiance qui m'a été accordée et que j'espère avoir justifiée. Grâce à cette fondation, mon grand rêve d'étudier en France s'est réalisé, ce qui a grandement changé ma vie pour le mieux. Enfin, je remercie D. Zvonkine pour son aide à la correction de ma traduction en français du début de cette thèse.

# Contents

# Chapter 1

# Introduction

Des méthodes de la *géométrie algébrique* [1] sur des corps finis sont utilisées avec succès en *cryptographie à clé publique* [2] et dans *la théorie des codes correcteurs d'erreurs* [3]. Les domaines tels que la *cryptographie elliptique* [4] et la théorie des codes géométriques algébriques (AG) [5], qui sont apparus à peu près au même moment dans les années 1980, en sont la preuve la plus frappante.

Initialement cryptographie elliptique concernait uniquement le *problème du logarithme discret* [2, Partie V] dans le groupe des points d'une *courbe elliptique* [6]. À de rares exceptions près, il n'existe à ce jour aucun algorithme rapide pour résoudre ce problème, contrairement aux problèmes tout aussi populaires du logarithme discret dans le groupe multiplicatif d'un corps fini et de la *factorisation entière* [2, Partie VI]. Les sous-domaines basés sur des couplages et des isogénies de courbes elliptiques se sont ensuite démarqués. Par exemple, la *cryptographie à base de couplages* [7] est récemment devenue l'un des fondements pour créer de diverses *crypto-monnaies* [8]. À son tour, la *cryptographie à base d'isogénies* [9] est un type de la *cryptographie post-quantique* [10] qui devient de plus en plus pertinente en relation avec l'émergence potentielle d'un *ordinateur quantique multi-qubit*.

Des codes de géométrie algébrique sont une généralisation naturelle des *codes de Reed–Solomon* [3, Chapitre 10]. Ils n'étaient à l'origine considérés que sur des courbes algébriques. En particulier, il existe des *tours de courbes (modulaires)* [11, §5.3, §7.4] qui permettent de construire *des familles de codes asymptotiquement bonnes* [12, Chapitre 5] en améliorant partiellement la *borne de Varshamov–Gilbert* [13, §8.4]. Par la suite, il s'est avéré que des codes AG sur certaines surfaces algébriques et même sur des variétés de dimension supérieure sont également assez bons (voir [11, Chapitre 11]). Cependant, leur inconvénient reste le manque de méthodes de décodage efficaces, ainsi qu'une description simple à la disposition d'ingénieurs sans connaissance approfondie de la géométrie algébrique.

Cette thèse est consacrée à trois tâches indépendantes, dont deux (§1.1, §1.2) se rapportent à la cryptographie elliptique, et la troisième (§1.3) à la théorie des

codes de géométrie algébrique. Certains des résultats obtenus ont été publiés dans les articles [14], [15], [16] et [17]. Les autres sont en cours de révision. En outre, l'auteur a fait des exposés dans les conférences "Arithmétique, Géométrie, Cryptographie et Théorie des Codes" (AGCCT 2019) à Marseille et "Current Trends in Cryptology" (CTCrypt 2020) à la région de Moscou.

## 1.1 Compression de points de courbes elliptiques

De nos jours, sans aucun doute, la cryptographie elliptique est largement utilisée en pratique [18]. Dans beaucoup de ses protocoles, il faut une *méthode de compression* pour les points d'une courbe elliptique $E$ sur un corps fini $\mathbb{F}_q$ de caractéristique $p$. Ceci est fait pour une transmission rapide de l'information sur un canal de communication ou pour son stockage compact dans la mémoire. Il existe une méthode classique qui considère un $\mathbb{F}_q$-point de $E \subset \mathbb{A}^2_{(x,y)}$ comme la coordonnée $x$ (ou $y$ [19]) avec 1 (resp. 2) bits pour récupérer de manière unique l'autre coordonnée en résolvant l'équation quadratique (resp. cubique) sur $\mathbb{F}_q$. Voir des variantes de cette méthode pour $p = 2$ dans [20], [21].

Considérons une courbe elliptique de la forme $E_b\colon y^2 = x^3 + b$ pour $b \in \mathbb{F}_q^*$ (de $j$-invariant 0). Comme on le sait, elle est ordinaire si et seulement si $p \equiv 1 \pmod 3$. Malgé la légère accélération [22] de la méthode rho de Pollard pour ces courbes, elles sont devenues très populaires en cryptographie elliptique. Ceci est confirmé par les standards WAP WTLS [23, Table 8], SEC 2 [24, §2] et différentes technologies telles que des crypto-monnaies (par exemple, la courbe Secp256k1 [25] est utilisée dans Bitcoin).

La raison principale pour cela est l'existence sur $E_b$ de l'automorphisme $[\omega]\colon (x, y) \mapsto (\omega x, y)$ d'ordre 3, où $\omega := \sqrt[3]{1} \in \mathbb{F}_p$, $\omega \neq 1$, c'est-à-dire $\omega^2 + \omega + 1 = 0$. Donc pour la multiplication scalaire plus rapide sur la courbe $E_b$ nous pouvons appliquer la soi-disant *décomposition GLV* [26]. En même temps, dans [27], il est suggéré de considérer également des courbes $E_b$ sur $\mathbb{F}_{q^2}$, car pour de tels corps, nous pouvons appliquer la *décomposition GLS* [26] (une amélioration de GLV). Il est à noter, cependant, que la décomposition GLS est également appliquée à des courbes elliptiques avec $j \neq 0$. L'exemple le plus connu est la courbe Four$\mathbb{Q}$ [29] proposée par Microsoft. Voir [30, §8] pour une comparaison de l'efficacité des approches GLV-GLS implémentées pour quelques courbes, y compris certaines avec $j = 0$.

En raison de nombreuses applications intéressantes telles que la *cryptographie basée sur l'identité* [31] ou des schémas de signature courte et de percées dans le calcul de couplages [32], la cryptographie à base de couplages devient une alternative de plus en plus populaire à la cryptographie elliptique classique. En effet, voir, par exemple, les documents des organisations IEEE [33], ISO/IEC [34], [35], FIDO [36], W3C [37] et les produits d'entreprises célèbres telles que ZECC [38],

Intel [39], Ethereum Foundation [40].

Comme d'habitude en cryptographie, une courbe elliptique $E/\mathbb{F}_q$ (en pratique $q = p$ toujours) est supposée avoir un sous-groupe $G \subset E(\mathbb{F}_q)$ d'ordre premier grand $\ell \neq p$. Le *degré de plongement* de $E$ (par rapport à $\ell$) est, par définition, le degré d'extension $k := [\mathbb{F}_q(\mu_\ell) : \mathbb{F}_q]$. De plus, soit $E'$ une tordue pour $E$ de degré $d \mid k$ (voir, par exemple, [7, §2.3.6]) et $G' \subset E'(\mathbb{F}_{q^{k/d}})$ le sous-groupe d'ordre $\ell$. En vertu de [110, Théorème 9] ce dernier existe au moins si $2, 3 \nmid |E_b(\mathbb{F}_q)|$. Des couplages (de type 2 [32, §2.3.2]) sont principalement pris sous la forme

$$G \times G' \to \mu_\ell \subset \mathbb{F}_{q^k}^* \quad [41, §7.3],$$

où $k$ est le plus petit nombre possible tel que le problème du logarithme discret dans $\mathbb{F}_{q^k}^*$ soit difficile, mais $d$ soit, à l'inverse, le plus grand nombre possible. C'est un fait classique que $d \leqslant 6$ et cette borne n'est atteinte que par les courbes elliptiques $E_b$.

Parmi celles-ci, les *courbes de Barreto–Naehrig* (BN) [42], [43, §2] et *Barreto–Lynn–Scott* (BLS12) [44] de degré de plongement $k = 12$ sont souvent utilisées dans la pratique pour le moment. Les courbes BN ont également $k = 12$, c'est-à-dire $k/d = 2$. Dernièrement, le choix le plus populaire pour le niveau de sécurité de 128 bits est la $\mathbb{F}_p$-courbe BLS12-381 [38], où $p \equiv 3 \pmod 4$, $p \equiv 10 \pmod{27}$ et $\lceil \log_2(p) \rceil = 381$.

Ainsi il sera utile de trouver une méthode de compression pour les $\mathbb{F}_{q^2}$-points des courbes $E_b/\mathbb{F}_{q^2}$ telle que la décompression correspondante soit beaucoup plus rapide que l'extraction d'une racine carrée dans $\mathbb{F}_{q^2}$. On voit facilement que cette dernière peut être accomplie en extrayant 2 racines carrées dans $\mathbb{F}_q$ (pour plus de détails voir [45]). Malgré le fait connu que pour $q \not\equiv 1 \pmod 8$ une racine carrée dans $\mathbb{F}_q$ est calculée par une seule exponentiation dans $\mathbb{F}_q$, c'est quand même une opération assez laborieuse.

Le chapitre 2 propose une nouvelle méthode de compression de points (à $2\lceil \log_2(q) \rceil + 3$ bits) nécessitant (en phase de décompression) d'extraire une seule racine cubique dans $\mathbb{F}_q$. Pour $q \not\equiv 1 \pmod{27}$ cela peut aussi être fait par une exponentiation dans $\mathbb{F}_q$ (voir [46, Proposition 1]), donc notre méthode est environ deux fois plus rapide que la méthode classique avec la coordonnée $x$ (a fortiori, $y$).

Notre approche est basée sur la $\mathbb{F}_q$-*rationalité* [47, §6.6] de la *surface de Kummer généralisée* $GK_b := R_b/[\omega]_2$ de la *restriction (descente) de Weil* $R_b := \mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E_b)$ [48, §3.2] par rapport à l'automorphisme $[\omega]_2 := \mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}([\omega])$ d'ordre 3. Plus précisément, nous appliquons la théorie des *fibrations en coniques* [49], [50] (c'est-à-dire des coniques sur le corps de fonctions $\mathbb{F}_q(t)$) pour obtenir des formules aussi bien explicites que simples d'un $\mathbb{F}_q$-isomorphisme birationnel entre $GK_b$ et $\mathbb{A}^2$. La nouvelle méthode de compression consiste à appliquer ces formules.

Pour retrouver le point de départ de $E_b(\mathbb{F}_{q^2}) = R_b(\mathbb{F}_q)$ par la méthode de décompression correspondante nous devons, étant donné un point de $GK_b(\mathbb{F}_q)$, cal-

culer l'un de ses antécédents par l'application naturelle $\varrho\colon R_b \to GK_b$ de degré 3, c'est-à-dire résoudre une équation cubique sur $\mathbb{F}_q$. Puisque $\omega \in \mathbb{F}_q$, un avantage des courbes $E_b$ est que l'application pull-back $\varrho^*$ est en fait une *extension de Kummer*, c'est-à-dire que le corps $\mathbb{F}_q(R_b)$ est généré par une racine cubique d'une fonction rationnelle de $\mathbb{F}_q(GK_b)$.

La compression simultanée de deux points $(x_0, y_0), (x_1, y_1)$ de $E(\mathbb{F}_q)$ (dite *compression de points double*) est aussi utile. Cela apparaît, par exemple, dans des protocoles à base de couplages de *preuves à divulgation nulle de connaissance non interactives*. L'un des travaux récents les plus notables dans ce domaine est [51].

La compression de points double a déjà été discutée dans [52] non seulement pour $j(E) = 0$, mais d'une manière légèrement différente. Dans cet article, les auteurs n'essaient pas de compresser des points de manière aussi compact que possible. Au lieu de cela, ils trouvent des formules transformant les coordonnées $x_0, y_0, x_1, y_1$ en trois éléments du corps $\mathbb{F}_q$. L'avantage de leur approche est la rapidité, car elle ne doit résoudre aucune équation en phase de décompression.

Il y a aussi sur $E_b/\mathbb{F}_q$ l'automorphisme $[-\omega]\colon (x, y) \mapsto (\omega x, -y)$ d'ordre 6. Considérons la surface de Kummer généralisée $GK'_b := E_b^2/[-\omega]^{\times 2}$. Contrairement à $GK_b$, la $\mathbb{F}_q$-rationalité de $GK'_b$ est facilement établie sans techniques de la géométrie algébrique. Comme ci-dessus, pour retrouver le point de départ appartenant à $E_b^2(\mathbb{F}_q)$ à partir d'un point donné de $GK'_b(\mathbb{F}_q)$ nous calculons l'un de ses antécédents par l'application naturelle $E_b^2 \to GK'_b$ de degré 6. C'est aussi une application de Kummer, c'est-à-dire que le corps $\mathbb{F}_q(E_b^2)$ est généré par une racine sixième d'une fonction rationnelle de $\mathbb{F}_q(GK'_b)$.

Ainsi en phase de décompression il suffit d'extraire dans $\mathbb{F}_q$ une racine sixième d'un élément de $\mathbb{F}_q$. D'après [7, §5.1.7], [46, §4] pour $q \equiv 3 \pmod 4$, $q \not\equiv 1 \pmod{27}$ ceci peut être implémenté au moyen d'une seule exponentiation dans $\mathbb{F}_q$. Nous décrivons en détail notre méthode de compression-décompression (à $2\lceil \log_2(q) \rceil + 4$ bits) dans le chapitre 3.

De plus, pour $E_b/\mathbb{F}_{q^2}$ l'application $[-\omega]$ naturellement induit l'automorphisme $-[\omega]_2 = [-\omega]_2\colon R_b \xrightarrow{\sim} R_b$ d'ordre 6. Conformément à [53, §8] la $\mathbb{F}_q$-rationalité de $GK_b = R_b/[\omega]_2$ entraîne la $\mathbb{F}_q$-rationalité de la surface de Kummer généralisée $R_b/[-\omega]_2 \simeq_{\mathbb{F}_q} GK_b/[-1]$. Cependant, ce fait ne fournit pas des formules explicites d'un $\mathbb{F}_q$-isomorphisme birationnel $R_b/[-\omega]_2 \xrightarrow{\sim} \mathbb{A}^2$. Néanmoins, de telles formules peuvent être facilement dérivées de la même manière que pour $GK'_b$ (pour plus de détails, voir §3.3).

Un résultat similaire a été obtenu dans le mémoire de master de l'auteur [54] pour la compression de points des deux jacobiennes $J_b$ [55] sur les corps $\mathbb{F}_{2^e}$, où $b \in \mathbb{F}_2$ et $2, 3 \nmid e$. Ce sont deux uniques (à une $\mathbb{F}_{2^e}$-isogénie près) surfaces abéliennes simples supersingulières qui ont le plus grand degré de plongement possible $k = 12$.

Nous avons prouvé la $\mathbb{F}_2$-rationalité de la surface de Kummer (habituelle) $K := J_b/[-1]$ et même obtenu des formules explicites d'un $\mathbb{F}_2$-isomorphisme birationnel entre $K$ et $\mathbb{A}^2$ en utilisant aussi la théorie des fibrations en coniques, mais d'une manière différente.

Enfin, en nous appuyant sur les résultats établis, nous osons formuler la conjecture 2.30 à propos de la $\mathbb{F}_q$-rationalité des $\mathbb{F}_q$-surfaces de Kummer généralisées qui sont géométriquement rationnelles.

## 1.2 Hachage vers des courbes elliptiques

Depuis son invention au début des années 2000, la cryptographie à base de couplages (sur une courbe elliptique $E\colon y^2 = f(x)$ sur un corps fini $\mathbb{F}_q$ de caractéristique $p > 3$) devient de plus en plus populaire chaque année. L'une de dernières revues de standards, produits commerciaux et bibliothèques pour ce type de la cryptographie est donnée dans [56, §4.1].

De nombreux protocoles à base de couplages (et certains protocoles de PAKE [7, §8.2.2]) utilisent une application $h\colon \mathbb{F}_q \to E(\mathbb{F}_q)$ efficacement calculable (en aucun cas un homomorphisme de groupes) souvent appelée *hachage* ou *encodage*. Elle ne doit pas être nécessairement injective ou surjective, mais l'image $\mathrm{Im}(h)$ plus grande est bien sûr meilleure. Les revues de ce sujet sont présentées dans [7, Chapitre 8], [57].

Certainement, nous pouvons simplement changer (par exemple, aléatoirement) quelques bits d'un élément donné $a \in \mathbb{F}_q$ de sorte à ce que $\sqrt{f(a)} \in \mathbb{F}_q$. Bien que cette propriété soit vraie pour environ une valeur de $a$ sur deux (voir, e.g., [7, §8.2.1]), cette approche est néanmoins vulnérable aux *attaques temporelles* [7, §8.2.2]. Une autre méthode évidente consiste en la multiplication scalaire $a \mapsto [a]P$ pour un point fixe $P \in E(\mathbb{F}_q)$. Malgré son caractère déterministe, elle est aussi peu sûre [7, §8.1].

Il existe de nombreuses constructions sûres (du moins à première vue) du hachage déterministe souhaité, telles que le hachage de Boneh–Franklin (bijectif) [58, §5.2] pour les courbes supersingulières de $j(E) = 0$, le hachage de Icart [59] pour $q \equiv 2 \pmod 3$ ou Elligator 2 [60, §5] à condition que $2 \mid \#E(\mathbb{F}_q)$ et $j(E) \neq 1728$. Cependant, la méthode unique valable pour $E$ et $\mathbb{F}_q$ arbitraires a été proposée dans [61] (basée sur [62, Théorème 14.1]) et améliorée dans [63]. Maintenant, elle est souvent appelée en l'honneur de ses auteurs: *Shallue, van de Woestijne* et aussi parfois *Ulas*.

La méthode SWU consiste à paramétrer une $\mathbb{F}_q$-*courbe rationnelle* $C$ (éventuellement singulière) [64, §4.1] sur un $\mathbb{F}_q$-*threefold de Calabi–Yau* $T$ (voir, e.g., [65]). Ce dernier est une résolution minimale des singularités de certain *threefold de Kummer généralisé* (étudié dans [66, §4.2], [67, §4], [68, §4.1.1]), à savoir du quo-

tient géométrique de $E^3$ sous une action de $(\mathbb{Z}/2)^2$. En regardant la définition, on obtient le modèle affine

$$T\colon y^2 = f(x_0)f(x_1)f(x_2) \quad \subset \quad \mathbb{A}^4_{(x_0,x_1,x_2,y)},$$

où $(x_i, y_i)$ sont trois points généraux de $E$ et $y := y_0y_1y_2$. Pour un point donné $P \in C(\mathbb{F}_q)$ la valeur $f(a_i)$ d'au moins une coordonnée $a_i := x_i(P)$ est un résidu quadratique dans $\mathbb{F}_q$. On obtient donc les points $\left(a_i, \pm\sqrt{f(a_i)}\right) \in E(\mathbb{F}_q)$.

Selon [69, Théorème 2], le threefold $T$ n'est pas uniréglé [70, Chapitre 4], mais peut être présenté sous la forme $(K \times E)/(\mathbb{Z}/2)$ (voir [71]), où $K$ est la *surface de Kummer* de $E^2$ (voir, e.g., [72, §4]). En vertu de ce dernier et du théorème de Bogomolov–Tschinkel [72, Théorème 1.1] la surface $K$ et donc le threefold $T$ sont recouverts sur $\overline{\mathbb{F}_q}$ par des courbes rationnelles. Nous soulignons que sur le corps $\mathbb{C}$ (contrairement à une caractéristique première) cela conduirait à une contradiction.

De plus, pour un non-résidu quadratique $c \in \mathbb{F}_q$ (pas nécessairement de l'image $f(\mathbb{F}_q)$) considérons la surface

$$K'\colon y^2 = f(x_0)f(x_1)c \quad \subset \quad \mathbb{A}^3_{(x_0,x_1,y)}.$$

Comme on peut voir, c'est la $\mathbb{F}_q$-tordue quadratique de $K$ qui elle-même est la surface de Kummer de $E \times E'$, où $E'\colon y^2 = f(x)c$ est la $\mathbb{F}_q$-tordue quadratique de $E$ (voir, e.g., [7, §2.3.6]).

Si dans la méthode SWU nous prenons une $\mathbb{F}_q$-courbe rationnelle sur $K'$, on obtient ce que l'on appelle la *méthode SWU simplifiée* [73, §7]. En comparaison avec la méthode SWU (classique), elle permet d'éviter un test de résiduosité quadratique dans $\mathbb{F}_q$ qui est une opération assez pénible en cryptographie en ce qui concerne des attaques temporelles (pour plus de détails, voir [7, §8.4.2]). En fait, nous montrons dans §6.1 que la méthode SWU simplifiée peut être implémentée sans aucun test de résiduosité quadratique.

Néanmoins, malgré le théorème de Bogomolov–Tschinkel, la recherche d'une $\mathbb{F}_q$-courbe rationnelle $C$ sur $K'$ (contrairement à $T$) n'est pas une tâche très simple. Pour $j(E) \neq 0, 1728$ une courbe désirée (même pour une plus grande classe de surfaces de Kummer) a d'abord été construite dans [74] (voir aussi [75], [76, §2]). Fait intéressant, les articles [74], [77, §1] utilisent alors $C$ pour prouver certains résultats arithmétiques sur le corps $\mathbb{Q}$.

Cependant, en cryptographie à base de couplages, des courbes *pairing-friendly* [7, Chapitre 4] de $j(E) = 0, 1728$ sont seulement intéressantes. Ceci est dû à l'existence de tordues de haut degré pour elles, ce qui conduit au calcul de couplages plus rapide [7, §3.3]. Dans [78, §4.3] pour une courbe $E$ avec $j(E) = 0$ sur le corps $\mathbb{F}_p$ (resp. $\mathbb{F}_{p^2}$) il est proposé d'utiliser une $\mathbb{F}_p$-isogénie (resp. $\mathbb{F}_{p^2}$-isogénie) verticale $\mathcal{E} \to E$ de degré 11 (resp. 3) de certaine courbe elliptique auxiliaire $\mathcal{E}$ avec $j(\mathcal{E}) \neq 0, 1728$. Malheureusement, cette approche dépend fortement de $\mathbb{F}_q$,

c'est-à-dire que dans certains cas, il n'y a pas de $\mathbb{F}_q$-isogénie désirée de petit degré, qui pourrait être calculée rapidement.

Dans le chapitre 4 nous résolvons le problème de la construction d'une $\mathbb{F}_q$-courbe rationnelle $C \subset K'$ pour toutes les $\mathbb{F}_q$-courbes elliptiques $E_a\colon y^2 = x^3 - ax$ avec $j = 1728$. L'exemple le plus célèbre de ces courbes pairing-friendly est les courbes de Kachisa–Schaefer–Scott (KSS) de degré de plongement 16 (voir [79, Exemple 4.2]) qui sont devenues (selon [80], [81], [82]) une alternative populaire pour celles de $j = 0$. Nous soulignons encore une fois qu'avant nous, la méthode SWU (classique), à notre connaissance, était le seul moyen de produire un hachage $h\colon \mathbb{F}_q \to E_a(\mathbb{F}_q)$ indépendamment de $\mathbb{F}_q$.

Il est à noter que pour dériver $C$, nous utilisons activement (entre autres) la théorie de la *restriction (descente) de Weil* [83, §8.1] pour des courbes elliptiques par rapport à l'extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. La communauté cryptographique connaît cette opération comme un instrument de cryptanalyse [4, §22.3].

Fait intéressant, les coefficients de nos fonctions définissant une paramétrisation propre de $C$ sont presque entièrement des puissances de 2 et 3. Cela permet de calculer très rapidement le hachage correspondant $h\colon \mathbb{F}_q \to E_a(\mathbb{F}_q)$. Enfin, remarquons qu'au pire $h$ est une application 8:1 $\big($ainsi que le hachage SWU (classique)$\big)$, c'est-à-dire que pour chaque point de $E_a(\mathbb{F}_q)$ son antécédent par $h$ contient au plus 8 éléments.

Ci-après, nous nous concentrons sur le cas de la $\mathbb{F}_q$-courbe elliptique $E_b\colon y_0^2 = x_0^3 - b$ (i.e., $E_{-b}$ dans la notation de §1.1), dont le $j$-invariant est 0. Pour le moment, les courbes $E_b$ les plus utilisées ont la restriction $\sqrt[3]{b} \notin \mathbb{F}_q$, i.e., $2 \nmid |E_b(\mathbb{F}_q)|$. Puisque $E_b$ est supposée être ordinaire, nous avons $q \equiv 1 \pmod 3$, c'est-à-dire $\omega := (-1 + \sqrt{-3})/2$ (en d'autres mots, $\omega^3 = 1$, $\omega \neq 1$) se trouve dans $\mathbb{F}_q$.

Notons ensuite la surface de Kummer du produit direct $E_b \times E_b'$ au moyen de $\mathcal{K}_2$, où, comme d'habitude, $E_b'$ est la $\mathbb{F}_q$-tordue quadratique de $E_b$. Prenons n'importe quel élément $c \in (\mathbb{F}_q^*)^3$ tel que $c \notin (\mathbb{F}_q^*)^2$. Par la deuxième hypothèse sur $c$ nous obtenons les équations

$$E_b'\colon cy_1^2 = x_1^3 - b, \qquad \mathcal{K}_2\colon (x_1^3 - b)t^2 = c(x_0^3 - b) \quad \subset \quad \mathbb{A}^3_{(x_0,x_1,t)},$$

où $t := y_0/y_1$.

Il y a sur $\mathcal{K}_2$ la fibration elliptique naturelle $(x_0, x_1, t) \mapsto t$ (appelée *fibration d'Inose* [84]), cependant nous ne connaissons aucune de ses $\mathbb{F}_q$-sections. Au lieu de cela, nous appliquons le changement de base $t \mapsto t^3$ et obtenons la surface elliptique

$$\mathcal{K}_6\colon (x_1^3 - b)t^6 = c(x_0^3 - b) \quad \subset \quad \mathbb{A}^3_{(x_0,x_1,t)}$$

ayant la section $\mathcal{O} := (t^2 : \sqrt[3]{c} : 0) \in \mathbb{P}^2_{(X_0:X_1:X_2)}$, où $x_0 = X_0/X_2$, $x_1 = X_1/X_2$.

La surface $\mathcal{K}_6$ est parfois appelée *surface de Kuwata* [85] (voir aussi [86], [87], [88], [89]). Il convient de noter que $\mathcal{K}_2$, $\mathcal{K}_6$ sont des surfaces $K3$ (voir, e.g., [90, §12]). De plus, conformément à [89, Théorème 8.1] elles sont *singulières* [84], [90, §13], [91], c'est-à-dire que leur $\overline{\mathbb{F}_q}$-nombres de Picard sont égaux à 20 (le plus élevé possible pour des surfaces $K3$ ordinaires). Au fait, le $\mathbb{F}_q$-nombre de Picard de $\mathcal{K}_2$ est égal à 8 (voir, par exemple, §4.2) qui est le plus petit possible pour les surfaces de Kummer du produit direct de deux $\mathbb{F}_q$-courbes elliptiques.

A cause du théorème de Lüroth [1, Example IV.2.5.5] chaque $\mathbb{F}_q$-courbe rationnelle sur $\mathcal{K}_6$ donne (au moyen de $t \mapsto t^3$) la $\mathbb{F}_q$-courbe rationnelle sur $\mathcal{K}_2$. A cet égard, il est naturel d'étudier le *groupe de Mordell–Weil* $\mathrm{MW}(\mathcal{K}_6)$ (voir [90, §6]) et dériver explicitement l'un de ses éléments non nuls (dont la hauteur canonique [90, §11.6] est la plus basse possible). Cette approche est déployée dans [74, §1], [77, §1], où toute courbe elliptique de $j \neq 0, 1728$ est prise au lieu de $E_b$.

Pour plus de clarté on notera par $\mathrm{MW}\big(\overline{\mathcal{K}_6}\big)$ le groupe de Mordell–Weil de toutes les sections de $\mathcal{K}_6$ (pas nécessairement définies sur $\mathbb{F}_q$). D'après [88, §1], [89, Lemma 6.2] nous avons $\mathrm{MW}\big(\overline{\mathcal{K}_6}\big) \simeq \mathbb{Z}^6 \oplus \mathbb{Z}/3$. En particulier, le sous-groupe de torsion est généré par l'une des deux sections $(t^2 : \omega^j \sqrt[3]{c} : 0)$, où $j \in \{1, 2\}$. En revanche, nous prouvons dans le chapitre 5 que $\mathrm{MW}(\mathcal{K}_6) \simeq \mathbb{Z}/3$, c'est-à-dire le $\mathbb{F}_q$-rang de Mordell–Weil de $\mathcal{K}_6$ est égal à 0. Puisque les sections de torsion sont à l'infini (i.e., sur la droite $X_2 = 0$), nous ne pouvons pas malheureusement les utiliser pour construire un hachage $h \colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$ par la méthode SWU simplifiée.

Néanmoins, dans le chapitre 6 il est produit un hachage SWU simplifié $h$ vers les $\mathbb{F}_q$-courbes elliptique $E_b$ ayant une $\mathbb{F}_{q^2}$-isogénie verticale de degré 5 $\big($au moins si $2, 3 \nmid \log_p(q)\big)$. Pour faire ça, nous agissons de la même manière comme dans le cas des courbes elliptiques avec $j$-invariant 1728 (ayant toujours une $\mathbb{F}_{q^2}$-isogénie verticale de degré 2), mais avec des formules plus lourdes.

En particulier, la condition souhaitée est remplie pour les $\mathbb{F}_p$-courbes BN512 et BN638 de [36, §4.1] (la première est aussi de [34, Partie 5]), où les nombres dans la notation sont égaux à $\lceil \log_2(p) \rceil$. De telles longueurs de bits pour la cryptographie à base de couplages deviendront actuelles à l'avenir, ces courbes sont donc potentiellement utiles. En factorisant les discriminants de l'endomorphisme de Frobenius (sur $\mathbb{F}_p$) des courbes, on voit que le plus petit degré d'une $\mathbb{F}_p$-isogénie verticale pour BN512 (resp. BN638) est 1291 (resp. 1523). Par conséquent, l'idée de [78, §4.3] ne fonctionne pas ici.

Enfin, dans le chapitre nous expliquons aussi pourquoi il ne reste que le cas d'une $\mathbb{F}_{q^2}$-isogénie verticale de degré 7 vers (de) $E_b$, pour lequel, apparemment, il est possible de construire un hachage SWU simplifié $h$ de la même manière, en effectuant le raisonnement indépendamment de $q$, c'est-à-dire sur un corps de nombres.

## 1.3 Codes toriques non déployés

Il existe la théorie bien développée des soi-disant *codes toriques* [12, Chapitre 8], c'est-à-dire des codes de géométrie algébrique (de Goppa) sur des *variétés toriques* [92] (de dimension $d$ sur un corps fini $\mathbb{F}_q$). Ces codes ont été découverts dans [93], [94] comme une généralisation des codes de Reed–Solomon (pour $d = 1$). Les codes toriques sont des codes cycliques $d$-dimensionnels (également connus sous le nom de codes multicycliques ou abéliens) [95], [96]. Malgré cela, des méthodes de décodage suffisamment rapides pour eux ne sont pas connues. Des méthodes peu efficaces sont présentées dans [97, §5].

En plus de *tores algébriques* et de variétés toriques habituels (i.e., déployés), il y a ceux qui sont *non déployés* (sur $\mathbb{F}_q$) [98]. Il est donc naturel de considérer des codes de géométrie algébrique sur ces dernières, ce que nous avons commencé à faire dans le chapitre 7. Nous les appelons *codes toriques non déployés*. Dans ce chapitre, on suppose partout que les variétés toriques sont lisses, cependant il n'y a aucun obstacle à considérer des codes toriques non déployés sur des variétés toriques singulières (voir le chapitre 8).

Les nouveaux codes ont certains avantages. Premièrement, les $\mathbb{F}_q$-groupes des points de tores non déployés sont souvent cycliques, donc les codes correspondants se révèlent être des *codes cycliques (à racines simples)* [3, Chapitre 7]. De plus, certains d'entre eux sont même *réversibles* [99]. Deuxièmement, les tores non déployés contiennent plus de $\mathbb{F}_q$-points que le tore déployé, c'est-à-dire plus de $(q-1)^d$. En d'autres termes, les codes toriques non déployés sont plus longs que les codes déployés, ils peuvent donc avoir une meilleure capacité de correction d'erreurs. Enfin, de nombreux codes classiques tels que les codes de Reed–Solomon doublement étendus [5, §4.4.1] et les codes de Reed–Muller cycliques (ainsi que leur analogue projectif [100]) sont équivalents à certains codes toriques non déployés.

De plus, il est merveilleux que plusieurs codes toriques non déployés soient des *codes BCH* [3, §9]. Par conséquent, à notre avis, ils ont plus de chances d'être utilisés dans la pratique que d'autres codes de géométrie algébrique sur des surfaces.

Il existe la classification bien connue des *surfaces toriques de del Pezzo* (éventuellement singulières) [101]. Ils correspondent bijectivement (à une équivalence près) aux soi-disant *polygones réflexifs* [92, §8.3]. Il y a exactement 16 tels polygones [92, Théorème 8.3.7], mais seulement 5 d'entre eux (du figure 8.1) sont assez "symétriques", c'est-à-dire qu'ils ont une action intégrale d'ordre supérieur à 2. La dernière condition semble nécessaire pour construire de bons codes toriques non déployés.

Les codes toriques non déployés $\mathcal{C}_8$, $\mathcal{C}_9$ (les tables 8.3 et 8.4) associés aux polygones lisses $Pol_8$, $Pol_9$ ont déjà été considérés, par exemple, dans [102, Proposition 4.7], [100, §2] respectivement. À leur tour, dans les paragraphes 7.2.3 et 8.3, nous

étudions les codes $q$-aires toriques non déployés à bas débit $\mathcal{C}_3$, $\mathcal{C}_4$, $\mathcal{C}_6$ qui sont associés aux polygones restants, à savoir $Pol_3$, $Pol_4$, $Pol_6$ respectivement. Ces polygones correspondent aux surfaces toriques de del Pezzo de degrés 3, 4, 6 et de $\mathbb{F}_q$-nombre de Picard 1 (voir la table 8.1). Au fait, les deux premiers d'entre eux sont des surfaces singulières, dont les points singuliers sont $\mathbb{F}_q$-conjugués.

Nos codes s'avèrent être des codes BCH avec la distance minimale $d$ suffisamment grande. En effet, nous prouvons que $d - d^* \geqslant q - \lfloor 2\sqrt{q} \rfloor - 1$, où $d^*$ est la distance assignée. En d'autres termes, nous améliorons considérablement la borne BCH. D'autre part, le défaut de la borne de Griesmer pour les nouveaux codes est $\leqslant \lfloor 2\sqrt{q} \rfloor - 1$ qui semble également être assez bonne. Il est à noter que pour une meilleure estimation de $d$, nous utilisons activement la théorie des courbes elliptiques sur des corps finis.

Le code $\mathcal{C}_6$ est indépendamment découvert dans [103, §4.2]. En même temps, à notre connaissance, les codes $\mathcal{C}_3$, $\mathcal{C}_4$ n'ont pas du tout été étudiés avant nous. Cependant, des codes AG sur certaines surfaces lisses cubiques et quartiques de del Pezzo sont décrits dans [103, §6], [104], [105, §4.1, §5.1] et [106].

# Part I

# Point compression for elliptic curves

# Chapter 2

# Point compression for elliptic $\mathbb{F}_{q^2}$-curves of $j$-invariant of 0

## 2.1 Background

### 2.1.1 Cubic polynomials

In this paragraph we recall some known facts about cubic polynomials. Consider a polynomial $x^3 + \alpha x^2 + \beta x + \gamma$ over a field $k$ of characteristic $p \neq 2, 3$. After the variable change $x := y - \alpha/3$, we obtain the polynomial

$$f(y) := y^3 + cy + d, \qquad \text{where} \qquad c := \beta - \frac{\alpha^2}{3}, \qquad d := \gamma - \frac{\alpha\beta}{3} + \frac{2\alpha^3}{27}.$$

Let $G \hookrightarrow S_3$ be the Galois group of the splitting field of $f$ over $k$. Further, for $a \in k$ we denote by $\left(\frac{a}{k}\right)$ the Legendre symbol, however in the case of a finite field $k = \mathbb{F}_q$ we also use the notation $\left(\frac{a}{q}\right)$.

**Lemma 2.1** ([107, §2]). *The discriminant of $f$ is equal to $\Delta = -4c^3 - 27d^2$ and*

$$\left(\frac{\Delta}{k}\right) = \begin{cases} 0 & \text{if} \quad f \text{ has a multiple root,} \\ 1 & \text{if} \quad G = 1 \text{ or } G \simeq \mathbb{Z}/3, \\ -1 & \text{if} \quad G \simeq \mathbb{Z}/2 \text{ or } G \simeq S_3. \end{cases}$$

**Theorem 2.2** (Cardano's formula [107, Theorem 2.5]). *The roots of $f$ are equal to $R_+ + R_-$, where*

$$R_\pm := \sqrt[3]{-\frac{d}{2} \pm \sqrt{D}}, \qquad D := -\frac{\Delta}{108} = \frac{c^3}{27} + \frac{d^2}{4}, \qquad R_+ R_- = -\frac{c}{3}.$$

One can see that for general $c$, $d$ finding roots of $f$ (by this formula) consists in extracting 1 square root and 2 cubic ones.

Throughout the thesis we denote by $\omega$ a fixed primitive 3-th root of unity, which is obviously equal to $(-1+\sqrt{-3})/2$. From Cardano's formula we immediately obtain

**Lemma 2.3.** *Assume that $\omega \in k^*$, i.e., $\left(\frac{-3}{k}\right) = 1$. Then a cubic extension of $k$ is Galois (and hence cyclic) iff it is Kummer, i.e., it has the form $k(\sqrt[3]{a})$ for some $a \in k^*$ such that $a \notin (k^*)^3$.*

Note that for $k = \mathbb{F}_q$ the condition $\omega \in \mathbb{F}_q^*$ is also equivalent to $q \equiv 1 \pmod 3$.

To formulate the next theorem we need to recall a definition of the Lucas sequence $v_n = v_n(a,b)$ for $a, b \in k$ and $n \in \mathbb{N}$:

$$v_0 := 2, \qquad v_1 := b, \qquad v_n := bv_{n-1} - av_{n-2}.$$

**Theorem 2.4** ([19, Theorem 2])**.**
*Assume that $k = \mathbb{F}_p$, $c, d \neq 0$, and $\left(\frac{\Delta}{p}\right) = -1$. Then the unique $\mathbb{F}_p$-root of $f$ equals*

$$-\frac{(3c)^{-(p/3)} v_n(C,D)}{3}, \qquad \text{where} \qquad C := -27c^3, \qquad D := -27d, \qquad n := \frac{p + 2\left(\frac{p}{3}\right)}{3}.$$

**Lemma 2.5** ([19, Remark 2])**.** *For $a \in \mathbb{F}_q^*$ we obtain:*

$$a \notin (\mathbb{F}_q^*)^3 \qquad \text{if and only if} \qquad q \equiv 1 \pmod 3 \quad \text{and} \quad a^{(q-1)/3} \neq 1.$$

*Moreover, if $a \in (\mathbb{F}_q^*)^3$, then*

$$\sqrt[3]{a} = \begin{cases} a^{(2q-1)/3} & \text{if} \quad q \equiv 2 \pmod 3, \\ [46, \text{Proposition 1}] & \text{if} \quad q \equiv 1 \pmod 9 \text{ and } q \not\equiv 1 \pmod{27}, \\ a^{-(q-4)/9} & \text{if} \quad q \equiv 4 \pmod 9, \\ a^{(q+2)/9} & \text{if} \quad q \equiv 7 \pmod 9. \end{cases}$$

Algorithms of exponentiation in $\mathbb{F}_q$ and extracting cubic roots in $\mathbb{F}_q$ for $q \equiv 1 \pmod{27}$ can be found, for example, in [108, §3.4] and [46] respectively. At the same time, for extracting square roots in $\mathbb{F}_p$ see [108, §12.5.1].

### 2.1.2 Elliptic curves of $j$-invariant 0

Consider a finite field $\mathbb{F}_q$, where $q = p^e$, $e \in \mathbb{N}$, and $p$ (>3) is a prime. In this paragraph we review elliptic curves $\overline{E_b} \subset \mathbb{P}^2$ (of $j = 0$) given by the affine model

$$E_b \colon y^2 = x^3 + b \quad \subset \quad \mathbb{A}^2_{(x,y)}$$

for $b \in \mathbb{F}_q^*$. In other words, $\overline{E_b} = E_b \cup \{\mathcal{O}\}$, where $\mathcal{O} := (0:1:0)$. Unless otherwise specified we will identify $E_b$ and $\overline{E_b}$ for the sake of simplicity. Curves $E_b$ are discussed, for example, in [27]. They have the order 3 automorphism

$$[\omega]\colon E_b \xrightarrow{\sim} E_b, \qquad (x,y) \mapsto (\omega x, y)$$

with fixed point set

$$\mathrm{Fix}([\omega]) = \big\{\mathcal{O}, (0, \pm\sqrt{b})\big\}.$$

Let us recall some well known results.

**Theorem 2.6** ([6, Example V.4.4]). *A curve $E_b$ is ordinary if and only if $p \equiv 1 \pmod 3$.*

Hereafter we will assume this condition, because results of the chapter have immediate applications only for discrete logarithm cryptography, where supersingular elliptic curves are weak.

**Theorem 2.7** ([43, Proposition 1.50], [43, Example 1.112]).

1. *Curves $E_b$ are isomorphic to each other at most over $\mathbb{F}_{q^6}$ by the map*

$$\varphi_{b,b'}\colon E_b \xrightarrow{\sim} E_{b'}, \qquad (x,y) \mapsto (\sqrt[3]{\beta}x, \sqrt{\beta}y),$$

   *where $\beta := b'/b$. Besides, for $\alpha \in \mathbb{F}_q$ such that $\alpha \notin (\mathbb{F}_q^*)^2$, $\alpha \notin (\mathbb{F}_q^*)^3$ the curves $E_{\alpha^i}$ $(i \in \mathbb{Z}/6)$ are unique ones of $j = 0$ (up to an $\mathbb{F}_q$-isomorphism).*

2. *The endomorphism ring of curves $E_b$ (and only of them) is that of Eisenstein integers:*

$$\mathrm{End}(E_b) \simeq \mathbb{Z}[\omega] \ \subset\ \mathbb{Q}\big(\sqrt{-3}\big),$$

   *where $\omega = \sqrt[3]{1} \in \mathbb{C}^*$ (such that $\omega \neq 1$) corresponds to the automorphism $[\omega]$. In particular,*

$$\mathrm{Aut}(E_b) \simeq \langle -\omega \rangle \simeq \mathbb{Z}/6.$$

Let us recall some things about the ring of Eisenstein integers. First, there is the unique decomposition $p = \pi\overline{\pi}$ such that $\pi = n + m\omega$ is a prime in $\mathbb{Z}[\omega]$ and $\pi \equiv 2 \pmod 3$. Besides, for a number $a \in \mathbb{Z}[\omega]\backslash(\pi)$ its 6-th power residue symbol $\left(\frac{a}{\pi}\right)_6$ is, by definition, the 6-th root of unity that is congruent to $a^{\frac{p-1}{6}}$ modulo $\pi$. We will denote by $t_q$ (by $f_q$) trace (respectively conductor) of the Frobenius map $\pi_q = \pi^e$ on $E_b/\mathbb{F}_q$. In other words, $f_q$ is conductor of the order $\mathbb{Z}[\pi_q] \subset \mathbb{Z}[\omega]$. In particular,

$$t_q^2 - 4q = -3f_q^2 \qquad \text{and hence} \qquad \pi_q, \overline{\pi_q} = \frac{t_q \pm f_q\sqrt{-3}}{2},$$

where $\overline{\pi_q} = \overline{\pi}^e$ is the Verschiebung map on $E_b/\mathbb{F}_q$. Finally, let

$$n_b := |E_b(\mathbb{F}_q)| = q + 1 - t_q.$$

**Theorem 2.8** ([27, Theorem 2], [43, Proposition 1.57])**.**

1. *For $q = p$ we obtain:*

$$t_p = -\overline{\left(\frac{4b}{\pi}\right)_6}\pi - \left(\frac{4b}{\pi}\right)_6\overline{\pi} \quad \in \quad \Big\{\pm(n+m),\ \pm(2n-m),\ \pm(n-2m)\Big\}.$$

2. *If $E_{b'}$ is a twist of $E_b$ of degree $d$, then its trace is equal to*

$$t'_q = \begin{cases} -t_q & \text{if} \quad d = 2, \\ \dfrac{\pm 3f_q - t_q}{2} & \text{if} \quad d = 3, \\ \dfrac{\pm 3f_q + t_q}{2} & \text{if} \quad d = 6. \end{cases}$$

*Moreover, for any curve $E_b$ all cases occur.*

Consequently, applying both parts of this theorem, we can immediately compute the trace $t_q$ (and then the order $n_b$) of any curve $E_b/\mathbb{F}_q$.

**Theorem 2.9** ([110, Theorem 9])**.** *Let $\alpha$ be as in Theorem 2.7. If $2, 3 \nmid n_b$, then*

$$E_b(\mathbb{F}_{q^6}) \simeq \bigoplus_{i \in \mathbb{Z}/6} E_{\alpha^i}(\mathbb{F}_q).$$

*Moreover, if $\mathbb{F}_q(E_b[\ell]) = \mathbb{F}_{q^6}$ for some prime $\ell \mid n_b$, then $E_b$ has the unique sextic twist $E_{b'}/\mathbb{F}_q$ such that $\ell \mid n_{b'}$. In other words,*

$$E_b[\ell] = E_b(\mathbb{F}_q)[\ell] \times \varphi_{b,b'}^{-1}(G'), \qquad \textit{where} \qquad G' := E_{b'}(\mathbb{F}_q)[\ell].$$

**The Weil restriction of $E_b/\mathbb{F}_{p^2}$**

For simplicity suppose $p \equiv 3 \pmod 4$, i.e., $i := \sqrt{-1} \notin \mathbb{F}_p$. Also, let $b := b_0 + b_1 i$ and $N_b := b_0^2 + b_1^2$ for some $b_0, b_1 \in \mathbb{F}_p$. Then the Weil restriction [48, §3.2] of $E_b \subset \mathbb{A}^2_{(x,y)}$ (with respect to the extension $\mathbb{F}_{p^2}/\mathbb{F}_p$) is equal to

$$R_b := \begin{cases} y_0^2 - y_1^2 = x_0^3 - 3x_0x_1^2 + b_0, \\ 2y_0y_1 = -x_1^3 + 3x_0^2x_1 + b_1 \end{cases} \quad \subset \quad \mathbb{A}^4_{(x_0,x_1,y_0,y_1)}.$$

Besides, we denote by $\overline{R_b} \hookrightarrow \mathbb{P}^8$ the Weil restriction of $\overline{E_b} \subset \mathbb{P}^2$, recalling that $\overline{R_b} \simeq \overline{E_b} \times \overline{E_{b^p}}$ over $\mathbb{F}_{p^2}$.

Further, consider the restriction of $[\omega]$, i.e., the order 3 automorphism

$$[\omega]_2 \colon R_b \xrightarrow{\sim} R_b, \qquad (x_0, x_1, y_0, y_1) \mapsto (\omega x_0, \omega x_1, y_0, y_1).$$

Its fixed point set

$$\mathrm{Fix}([\omega]_2) = \big\{(0,0,y_0,y_1) \;\mid\; y_0^2 - y_1^2 = b_0,\ 2y_0y_1 = b_1\big\}.$$

Over $\overline{\mathbb{F}_p}$ it obviously consists of exactly 4 points, and besides, $\mathrm{Fix}([\omega]_2)(\mathbb{F}_p) = \varnothing$ if and only if $\left(\frac{b}{p^2}\right) = -1$. At the same time, the continuation $[\omega]_2 \colon \overline{R_b} \xrightarrow{\sim} \overline{R_b}$ has exactly 9 fixed $\overline{\mathbb{F}_p}$-points. The similar analysis can be also carried out for the involution

$$[-1] \colon R_b \xrightarrow{\sim} R_b, \qquad (x_0, x_1, y_0, y_1) \mapsto (x_0, x_1, -y_0, -y_1).$$

### 2.1.3 Generalized Kummer surfaces

Let $A$ be an abelian surface over a perfect field $k$ of characteristic $p$ and $\sigma$ be its automorphism as a group variety. The quotient $A/\sigma$ (or its minimal resolution of singularities) is called *generalized Kummer surface*. The theory of geometric quotients is well represented in [111]. For $\sigma = [-1]$ this is just *Kummer surface* $K_A$. Besides, we will denote by $\varrho \colon A \to A/\sigma$ the quotient morphism, which is of degree $\mathrm{ord}(\sigma)$.

Let us recall some rationality properties of generalized Kummer surfaces.

**Theorem 2.10** ([112, Theorem A], [113, Theorem 1.3]). *For $k = \overline{k}$ we obtain:*

1. *If $p > 2$, $p \not\equiv 1 \pmod{12}$, then $A$ is supersingular $\Leftrightarrow$ $K_A$ is a Zariski surface* [114];
2. *If $p = 2$, then $A$ is supersingular $\Leftrightarrow$ $K_A$ is a rational surface.*

**Theorem 2.11** ([115, Table 6], [116, §2]). *For $k = \mathbb{C}$ there are only two abelian surfaces having $\sigma$ of a prime order such that the generalized Kummer surface is rational. These are:*

1. *The direct square $E_1^2$ with $\sigma = [\omega]^{\times 2}$ of order 3;*
2. *The Jacobian $J_1$ of the genus 2 curve given by the affine model $y^2 = x^5 + 1$ with $\sigma$ (of order 5) induced from the curve automorphism $(x, y) \mapsto (x\sqrt[5]{1}, y)$.*

In fact, $J_1$ is the unique simple abelian surface $A$ having $\sigma$ with the rational quotient $A/\sigma$ even if we omit the prime condition on $\mathrm{ord}(\sigma)$.

**Theorem 2.12** ([117, Theorem 2.11]). *Assume that $k = \overline{k}$, $\dim\big(\mathrm{Fix}(\sigma)\big) = 0$, and at least one of singularities on $A/\sigma$ is not a node. Then $A/\sigma$ is a rational surface.*

Recently, a sort of classification for automorphism groups of abelian surfaces over a finite field $\mathbb{F}_q$ appeared in [118]. Nevertheless, almost nothing is known about $\mathbb{F}_q$-rationality of generalized Kummer surfaces unlike their $\overline{\mathbb{F}_q}$-unirationality in some cases (see [117]).

**The surface $GK_b$**

We keep the notation of §2.1.2. Consider the generalized Kummer surface $\overline{GK_b} := \overline{R_b}/[\omega]_2$ and its open subset $GK_b := R_b/[\omega]_2$. Besides, we will need the polynomials

$$\alpha(t) := 3t^2 - 1, \qquad \beta(t) := t(t^2 - 3),$$

$$f(t) \;:=\; -b_0\alpha(t) + b_1\beta(t) \;=\; b_1t^3 - 3b_0t^2 - 3b_1t + b_0.$$

Note that the discriminant of $f/b_1$ is equal to $\Delta = 2^2 3^3 N_b^2/b_1^4$ and hence $\left(\frac{\Delta}{p}\right) = -1$. By Lemma 2.1 there is the decomposition $f = \lambda\gamma$ into linear $\lambda$ and $\mathbb{F}_p$-irreducible quadratic $\gamma$ polynomials over $\mathbb{F}_p$. For uniqueness we suppose $\gamma$ to be reduced. This decomposition (or, equivalently, the unique $\mathbb{F}_p$-root of $f$) can be found, for example, by means of Theorem 2.4.

**Theorem 2.13.** *The surface $GK_b$ has the affine model*

$$\alpha(t)(y_0^2 - y_1^2) - 2\beta(t)y_0y_1 + f(t) \quad \subset \quad \mathbb{A}^3_{(t,y_0,y_1)}.$$

*By identifying $GK_b$ with this model, the corresponding quotient map takes the form*

$$\varrho\colon R_b \dashrightarrow GK_b, \qquad (x_0, x_1, y_0, y_1) \mapsto \left(\frac{x_0}{x_1}, y_0, y_1\right).$$

*Proof.* It is well known that $\mathbb{F}_p(GK_b) = \mathbb{F}_p(R_b)^{[\omega]_2}$, that is rational functions on $GK_b$ are $[\omega]_2$-invariant ones on $R_b$. Also, consider the field

$$F := \mathbb{F}_p(t, y_0, y_1) \subset \mathbb{F}_p(GK_b), \qquad \text{where} \qquad t := \frac{x_0}{x_1}.$$

Note that $F(x_1) = \mathbb{F}_p(R_b)$, because $x_0 = tx_1$. Since $x_1^3 = (2y_0y_1 - b_1)/\alpha(t)$, the extension degree $[\mathbb{F}_p(R_b) : F] \leqslant 3$. At the same time, $[\mathbb{F}_p(R_b) : \mathbb{F}_p(GK_b)] = 3$ according to the Artin theorem from the Galois theory. Thus $F = \mathbb{F}_p(GK_b)$. Finally, looking at the equations of $R_b$ and the equalities

$$\frac{y_0^2 - y_1^2 - b_0}{2y_0y_1 - b_1} = \frac{x_0^3 - 3x_0x_1^2}{-x_1^3 + 3x_0^2x_1} = \frac{(x_0^3 - 3x_0x_1^2)/x_1^3}{(-x_1^3 + 3x_0^2x_1)/x_1^3} = \frac{\beta(t)}{\alpha(t)},$$

we obtain the aforementioned polynomial. There are no another dependencies between the coordinates $t, y_0, y_1$, because $GK_b$ is a surface. □

It is known [119, Example 8.10] that the image of $\mathrm{Fix}([\omega]_2) \subset \overline{R_b}$ under $\varrho$ is the singular locus of $\overline{GK_b}$ and all its 9 singularities are cyclic quotient ones of type $\frac{1}{3}(1,1)$ (see, e.g., [119, Appendix]).

Later it will be more practical to consider the closure of $GK_b$ in $\mathbb{A}^1_t \times \mathbb{P}^2_{(y_0:y_1:y_2)}$, keeping the same notation. In this case the quotient map takes the form

$$\varrho\colon R_b \dashrightarrow GK_b, \qquad (x_0, x_1, y_0, y_1) \mapsto \left(\frac{x_0}{x_1}, (y_0 : y_1 : 1)\right).$$

An inverse image of $\varrho$ is represented, for example, as

$$\big(t,(y_0:y_1:y_2)\big)\mapsto\big(tX_1,X_1,Y_0,Y_1\big),$$

where

$$X_1:=\sqrt[3]{\frac{2Y_0Y_1-b_1}{\alpha(t)}},\qquad Y_0:=\frac{y_0}{y_2},\qquad Y_1:=\frac{y_1}{y_2}.$$

In other words, these formulas give the map $\varrho^{-1}$ from $GK_b$ to the set-theoretic quotient of $R_b$ by $[\omega]_2$.

### 2.1.4 Conic bundles (conics over the rational function field)

In this paragraph we will recall some facts about conic bundles. For a deeper look, see [49], [50]. Let $(x_0:x_1)$ be homogenous coordinates of $\mathbb{P}^1$ and $t:=x_0/x_1$. As usual, we denote a point $(t_0:1)$ just by $t_0$ and the point $(1:0)$ by $\infty$.

Consider a projective irreducible (possibly singular) surface $S$ over a finite field $\mathbb{F}_q$ of characteristic $p>2$. We call a non-constant $\mathbb{F}_q$-morphism $\pi\colon S\to\mathbb{P}^1$ *conic bundle* if for general $t_0\in\mathbb{P}^1$ the fibre $\pi^{-1}(t_0)$ is a non-degenerate conic. The latter means an irreducible (or, equivalently, non-singular) algebraic $\mathbb{F}_q(t_0)$-curve of degree 2. As usually, a $\mathbb{F}_q$-section of $\pi$ is a $\mathbb{F}_q$-morphism $\sigma\colon\mathbb{P}^1\to S$ such that $\pi\circ\sigma=\mathrm{id}$.

It is clear that $\pi$ corresponds to its general fibre $F_\pi$, which is a non-degenerate conic over the univariate function field $\mathbb{F}_q(t)$. And besides, $\mathbb{F}_q$-sections of $\pi$ correspond to $\mathbb{F}_q(t)$-points on $F_\pi$. For one another conic bundle $\pi'\colon S'\to\mathbb{P}^1$ any birational $\mathbb{F}_q$-isomorphism $\varphi\colon S\xrightarrow{\sim}S'$ (such that $\pi=\pi'\circ\varphi$) corresponds to an $\mathbb{F}_q(t)$-isomorphism (i.e., a transformation in $\mathbb{P}^2$) of their general fibers $\varphi_{\pi,\pi'}\colon F_\pi\xrightarrow{\sim}F_{\pi'}$, and vice versa. If the general fibre $F_\pi$ is *isotropic*, i.e., it has $\mathbb{F}_q(t)$-point, then $S$ is obviously an $\mathbb{F}_q$-rational surface. Inverse is not true (see, for example, Theorem 2.26).

Suppose $S$ to be a non-singular surface. A conic bundle $\pi$ is called *relatively* $\mathbb{F}_q$-*minimal* if $S$ has no $\mathbb{F}_q$-orbits of pairwise disjoint exceptional $(-1)$-curves in fibers of $\pi$. In other words, the surface $S$ can not be contracted over $\mathbb{F}_q$ with respect to $\pi$. A conic bundle may have several relatively $\mathbb{F}_q$-minimal models, however the Frobenius action on each of them is the same.

**Theorem 2.14** (Iskovskih)**.** *Suppose $\pi\colon S\to\mathbb{P}^1$ to be a relatively $\mathbb{F}_q$-minimal conic bundle. Then we obtain:*

1. *The number of degenerate fibres of $\pi$ (over $\overline{\mathbb{F}_q}$) is equal to $8-K^2$, where $K$ is a canonical divisor of $S$;*

2. *The surface $S$ is $\mathbb{F}_q$-rational if and only if $K^2 \geqslant 5$, i.e., there is no more than 3 degenerate fibers.*

3. *If $K^2 \in \{5, 6\}$, then $S$ is a del Pezzo surface. Moreover, $S$ is unique among all relatively $\mathbb{F}_q$-minimal conic bundles of degree $K^2$.*

It is well known that every surface having conic bundle can be reduced by means of some birational $\mathbb{F}_q$-isomorphism to the form

$$S = F(x_0, x_1)y_0^2 + G(x_0, x_1)y_1^2 + H(x_0, x_1)y_2^2 \quad \subset \quad \mathbb{P}^1_{(x_0:x_1)} \times \mathbb{P}^2_{(y_0:y_1:y_2)},$$

where $F, G, H$ are non-zero homogenous $\mathbb{F}_q$-polynomials of the same degree. The conic bundle itself is transformed into the projection $\pi\colon S \to \mathbb{P}^1_{(x_0:x_1)}$. The product $\Delta := FGH$ is called *discriminant* of $\pi$. After a simple check we obtain

**Lemma 2.15.** *For $t_0 \in \mathbb{P}^1$ the following is true:*

1. *The fibre of $\pi$ over $t_0$ is degenerate $\Leftrightarrow \Delta(t_0) = 0$;*

2. *The fibre of $\pi$ over $t_0$ contains a singular point on $S \Leftrightarrow t_0$ is a multiple root of $\Delta$;*

3. *Singular curves on $S$ may only be double fibers of $\pi$.*

Further, it is clear that the surface $S$ has the non-singular $\mathbb{F}_q$-model

$$S_{f,g,h} := f(t)y_0^2 + g(t)y_1^2 + h(t)y_2^2 \quad \subset \quad \mathbb{A}^1_t \times \mathbb{P}^2_{(y_0:y_1:y_2)},$$

where $f, g, h$ are non-zero (possibly $\mathbb{F}_q$-reducible) square-free polynomials having no common roots in pairs. We will also call the projection $S_{f,g,h} \to \mathbb{A}^1_t$ (induced from $\pi$) a conic bundle despite the fact that $S_{f,g,h}$ is not a projective surface. Thus its general fibre can be written as

$$Q_{\alpha,\beta} := y_0^2 + \alpha(t)y_1^2 + \beta(t)y_2^2, \qquad \text{where} \qquad \alpha(t) := \frac{g(t)}{f(t)}, \qquad \beta(t) := \frac{h(t)}{f(t)}.$$

**Lemma 2.16** ([120, Theorem 3.7])**.** *The conic bundle $S_{f,g,h} \to \mathbb{A}^1_t$ has an $\mathbb{F}_q$-section if and only if the following identities on the Legendre symbols are satisfied:*

$$\left(\frac{-fg}{h}\right) = \left(\frac{-fh}{g}\right) = \left(\frac{-gh}{f}\right) = 1.$$

A quite efficient algorithm for finding an $\mathbb{F}_q$-section of a conic bundle can be found, for example, in [121].

We recall that for functions $\alpha, \beta \in \mathbb{F}_q(t)^*$ their (*quadratic*) *Hilbert symbol at* $t_0 \in \mathbb{P}^1$ is the Legendre one

$$(\alpha, \beta)_{t_0} := \left(\frac{e(\alpha,\beta)}{\mathbb{F}_q(t_0)}\right), \qquad \text{where} \qquad e(\alpha,\beta) := (-1)^{ab}\frac{\alpha^b}{\beta^a}(t_0) \ \in \ \mathbb{F}_q(t_0)^*$$

and $a$, $b$ are orders at $t_0$ of $\alpha$, $\beta$ respectively. The following theorem is very useful despite the fact that it is not constructive.

**Theorem 2.17** ([49, Example 3.7])**.** *Fix two more functions $\alpha', \beta' \in \mathbb{F}_q(t)^*$. Then the conics $Q_{\alpha,\beta}$, $Q_{\alpha',\beta'}$ are $\mathbb{F}_q(t)$-isomorphic if and only if for all $t_0 \in \mathbb{P}^1$ we have that $(\alpha,\beta)_{t_0} = (\alpha',\beta')_{t_0}$.*

## 2.2 Auxiliary results

Throughout this paragraph $p$ denotes a prime such that $p \equiv 3 \pmod 4$, $p > 3$.

### 2.2.1 Cubic $\mathbb{F}_p$-surfaces $S_h$ with two $\mathbb{F}_p$-nodes

We will study some singular cubic surfaces with 16 lines, which occur in §2.2.2, §2.3. The general theory of singular cubic ones (over a non-closed field) can be found, for example, in [101, Part I].

**Lemma 2.18.** *For $h = h_1 t + h_0 \in \mathbb{F}_p[t]$ with $h_1 \neq 0$ consider a cubic surface*

$$S_h := x^2 y - (t^2 + y^2)y - (h_1 t + h_0 y)z^2 \quad \subset \quad \mathbb{P}^3_{(x:y:z:t)}.$$

*It has only two singular points $P_\pm := (\pm 1 : 0 : 0 : 1)$ and they are nodes (i.e., of type $\mathrm{A}_1$). In particular, the surface $S_h$ is $\mathbb{F}_p$-rational.*

*Proof.* The partial derivatives of $S_h$ are equal to

$$\frac{\partial S_h}{\partial x} = 2xy, \qquad \frac{\partial S_h}{\partial y} = x^2 - (t^2 + 3y^2) - h_0 z^2,$$
$$\frac{\partial S_h}{\partial z} = -2(h_1 t + h_0 y)z, \qquad \frac{\partial S_h}{\partial t} = -2ty - h_1 z^2.$$

Besides, after the translation

$$\tau_{P_\pm} : (x : y : z : t) \mapsto (\pm x - t : y : z : t), \qquad \tau^{-1}_{P_\pm} : (x : y : z : t) \mapsto \big(\pm(x + t) : y : z : t\big)$$

the tangent cone of

$$S_{h,O} := \tau_{P_\pm}(S_h) \ = \ x^2 y + 2xty - y^3 - (h_1 t + h_0 y)z^2$$

at the origin $O = \tau_{P_\pm}(P_\pm)$ of $\mathbb{A}^3_{(x,y,z)}$ has the form

$$\mathrm{T}_O(S_{h,O}) = 2xy - h_1 z^2.$$

Therefore the points $P_\pm$ are nodes and the projection from one of them is the birational $\mathbb{F}_p$-isomorphism $pr\colon S_h \xrightarrow{\sim} \mathbb{A}^2$. □

Let $N_h := h_0^2 + h_1^2$ and note that

$$S_{h,O} \cap \mathrm{T}_O(S_{h,O}) = L_{P_+,P_-} \cup M_O,$$

where

$$L_{P_+,P_-} := \mathbb{V}(y,z), \qquad M_O := \begin{cases} h_1 x = \big(h_0 \pm \sqrt{N_h}\big) y, \\ h_1 z = \pm\sqrt{2h_1 xy}. \end{cases}$$

Here $M_O$ is the union of 4 lines, i.e., the signs $\pm$ are taken independently. Consider the projection from $O$ and its inverse map:

$$pr_O\colon S_{h,O} \xrightarrow{\sim} \mathbb{A}^2_{(u,v)}, \qquad (x:y:z:t) \mapsto \Big(\frac{x}{y}, \frac{z}{y}\Big),$$

$$pr_O^{-1}\colon \mathbb{A}^2_{(u,v)} \xrightarrow{\sim} S_{h,O}, \qquad (u,v) \mapsto (uY : Y : vY : T),$$

where

$$Y := h_1 v^2 - 2u, \qquad T := u^2 - h_0 v^2 - 1.$$

Note that $pr_O$, $pr_O^{-1}$ are isomorphisms on the open subsets

$$U_O := S_{h,O} \backslash \big(\mathrm{T}_O(S_{h,O}) \cup L_\infty\big), \qquad V := \mathbb{A}^2_{(u,v)} \backslash \mathbb{V}(Y),$$

where $L_\infty := \mathbb{V}(y,t)$. Thus the maps

$$pr = pr_O \circ \tau_{P_\pm}\colon S_h \xrightarrow{\sim} \mathbb{A}^2, \qquad pr^{-1} = \tau_{P_\pm}^{-1} \circ pr_O^{-1}\colon \mathbb{A}^2 \xrightarrow{\sim} S_h$$

are those on the open subsets $V$ and

$$U := \tau_{P_\pm}^{-1}(U_O) = S_h \backslash \big(\mathrm{T}_{P_\pm}(S_h) \cup L_\infty\big),$$

where

$$\mathrm{T}_{P_\pm}(S_h) = \tau_{P_\pm}^{-1}(S'_h) \;=\; \pm 2(x+t)y - h_1 z^2.$$

Thus we proved

**Lemma 2.19.** *If* $\left(\frac{N_h}{p}\right) = -1$, *then* $pr\colon U(\mathbb{F}_p) \xrightarrow{\sim} V(\mathbb{F}_p)$, *where*

$$U(\mathbb{F}_p) = S_h(\mathbb{F}_p) \backslash \mathbb{V}(y), \qquad V(\mathbb{F}_p) = \mathbb{A}^2(\mathbb{F}_p) \backslash \mathbb{V}(Y).$$

We are also interested in the involution

$$[-1]\colon S_h \xrightarrow{\sim} S_h, \qquad (x:y:z:t) \mapsto (x:y:-z:t),$$

the meaning of which is explained in Remark 2.25. Let $P \in S_h \backslash \mathrm{T}_\infty(S_h)$ be a point outside the tangent plane

$$\mathrm{T}_\infty(S_h) = h_1 t + h_0 y \qquad \text{at} \qquad \infty := (0:0:1:0) \in S_h.$$

In geometric terms the point $[-1](P)$ is the third intersection one of the surface $S_h$ and the line $L_{\infty,P}$ passing through $\infty$ and $P$ (see also [109, Proposition II.12.13]). In other words,

$$S_h \cdot L_{\infty,P} = \infty + P + [-1](P).$$

### 2.2.2 A conic bundle $\pi$ on $S_h$

We save the notation of §2.2.1. In §2.3 we will encounter the projection $\pi\colon S_h \to \mathbb{P}^1_{(y:t)}$ from the line $L_\infty$, which is a conic bundle. The surfaces $S_h$ and

$$S'_h := x^2 - (t^2+1)y^2 - (h_1 t + h_0)z^2 \quad \subset \quad \mathbb{A}^1_t \times \mathbb{P}^2_{(x:y:z)}$$

are obviously equal for $y \neq 0$ on both ones. Moreover, after inducing the maps $\pi, pr, [-1]$ on $S'_h$ they respectively become the projection $\pi'\colon S'_h \to \mathbb{A}^1_t$,

$$pr'\colon S'_h \xrightarrow{\sim} \mathbb{A}^2_{(u,v)}, \qquad \big(t, (x:y:z)\big) \mapsto \Big(\pm\frac{x}{y} - t, \frac{z}{y}\Big),$$

and

$$[-1]\colon S'_h \xrightarrow{\sim} S'_h, \qquad \big(t, (x:y:z)\big) \mapsto \big(t, (x:y:-z)\big).$$

Besides,

$$(pr')^{-1}\colon \mathbb{A}^2_{(u,v)} \xrightarrow{\sim} S'_h, \qquad (u,v) \mapsto \Big(\frac{T}{Y}, \big(\pm(uY+T):Y:vY\big)\Big),$$

where

$$Y := h_1 v^2 - 2u, \qquad T := u^2 - h_0 v^2 - 1.$$

For compactness we will sometimes use the notation $g(t) := t^2 + 1$.

**Lemma 2.20.** *The conic bundle $\pi'$ has an $\mathbb{F}_p$-section $\Leftrightarrow \left(\frac{N_h}{p}\right) = 1$.*

*Proof.* According to Lemma 2.16 there is an $\mathbb{F}_p$-section for $\pi'$ if and only if

$$\left(\frac{g}{h}\right) = \left(\frac{h}{g}\right) = \left(\frac{-gh}{1}\right) = 1.$$

The last equality is obviously true. Also, note that

$$\left(\frac{g}{h}\right) = \left(\frac{g(h_0/h_1)}{p}\right) = \left(\frac{N_h}{p}\right).$$

Finally, the second equality is, by definition, the existence of an $\mathbb{F}_p$-polynomial $r(t) = r_1 t + r_0$ such that $g \mid h - r^2$. The remainder of dividing $h - r^2$ by $g$ equals

$$(h_1 - 2r_0 r_1)t + (h_0 - r_0^2 + r_1^2),$$

hence we obtain the equation system

$$\begin{cases} r_0 = \dfrac{h_1}{2r_1}, \\ 4r_1^4 + 4h_0 r_1^2 - h_1^2 = 0. \end{cases}$$

Therefore $r_1^2 = R_\pm$, where

$$R_\pm := \frac{-h_0 \pm \sqrt{N_h}}{2}, \qquad R_+ R_- = -\frac{h_1^2}{4}.$$

If $\left(\frac{N_h}{p}\right) = 1$, then the above system is solvable. Indeed, $R_\pm \in \mathbb{F}_p$ and exactly one of these elements is a quadratic residue in $\mathbb{F}_p$. □

Provided $\left(\frac{N_h}{p}\right) = -1$ we see that $pr' \colon U(\mathbb{F}_p) \xrightarrow{\sim} V(\mathbb{F}_p)$ by analogy with Lemma 2.19. For the next theorem consider the lines

$$L_\pm := h_1 x \pm y\sqrt{N_h}, \qquad M_\pm := x - z\sqrt{h(\pm i)}, \qquad M_\pm^{(1)} = x + z\sqrt{h(\pm i)}.$$

**Theorem 2.21.** *If* $\left(\frac{N_h}{p}\right) = -1$, *then:*

1. *The degenerate fibers of* $\pi'$ *over* $t \neq \infty$ *are represented in Figure* 2.1;
2. *The fibre of* $\pi'$ *over* $\infty$ *is the double one with the unique surface singular point* $(1:0:0)$, *which is of type* $\mathrm{A}_3$;
3. *The relatively* $\mathbb{F}_p$*-minimal model of* $S'_h$ *is a del Pezzo surface of degree* 5.

*Proof.* The first fact is immediately checked. To prove the second one we write out the surface $S'_h$ (locally over $\overline{\mathbb{F}_p}$) as

$$s^2 - (1+s^2)y^2 - (1 + \frac{h_0}{h_1}s)sz^2 \quad \subset \quad \mathbb{A}^3_{(y,z,s)}.$$

To obtain the surface $\mathbb{V}(s^2+y^2+z^4)$ it remains to apply the analytical change of variables

$$(y,z,s)\mapsto\Big(Ay,Bz,s+\frac{(Bz)^2}{2}\Big),$$

where

$$A=\sqrt{-(1+s^2)},\quad B=\sqrt{-(1+\frac{h_0}{h_1}s)}\quad\in\quad\overline{\mathbb{F}_p}[[s]].$$

Finally, the third fact follows from the Iskovskih theorem 2.14 and $\mathbb{F}_p$-rationality of $S_h$ (see Lemma 2.18). □

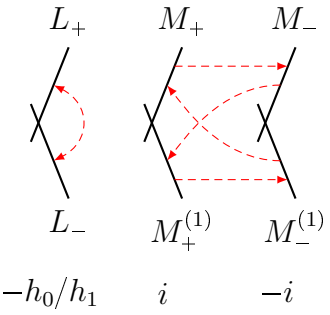


Figure 2.1: The Frobenius action on degenerate fibers of the conic bundle $\pi'\colon S'_h\to\mathbb{A}^1_t$

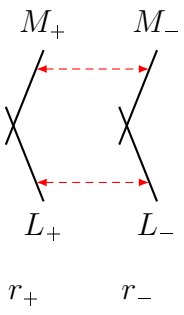


Figure 2.2: Pairs of $\mathbb{F}_p$-conjugate lines lying in two $\mathbb{F}_p$-conjugate degenerate fibers

Hereafter we will identify $(S_h,\pi,pr)$ and $(S'_h,\pi',pr')$, saving for simplicity only the first notation.

### 2.2.3 Blowing down components of degenerate fibres for $\pi$

According to [49, §3] we have explicit formulas for contracting one of $\mathbb{F}_p$-lines of a degenerate $\mathbb{F}_p$-fibre. We will also need to explicitly contract one of the pairs of $\mathbb{F}_p$-conjugate lines $L_\pm$ (or $M_\pm$) lying in two $\mathbb{F}_p$-conjugate degenerate fibers over roots $r_\pm$ of some $\mathbb{F}_p$-irreducible quadratic polynomial. This is done in Lemma 2.22 in a particular case, which is sufficient for our purposes. For better comprehension of the described situation see Figure 2.2.

For any polynomial $h\in\mathbb{F}_p[t]$ consider the surface

$$S_h:=x^2-(t^2+1)y^2-h(t)z^2\quad\subset\quad\mathbb{A}^1_t\times\mathbb{P}^2_{(x:y:z)}.$$

As usual, the projection $\pi\colon S_h\to\mathbb{A}^1_t$ is a conic bundle.

**Lemma 2.22.** *Let $q(t) := t^2 + ct + d \in \mathbb{F}_p[t]$ with roots $r_\pm$ and discriminant $D = c^2 - 4d$ such that $\left(\frac{D}{p}\right) = -1$. Also, let $h \in \mathbb{F}_p[t]$ and $s_\pm := r_\pm^2 + 1$ provided that $q \mid h$ and $\left(\frac{s_\pm}{p^2}\right) = 1$. If $c \neq 0$ or $\big(c = 0$ and $d - 1 \in (\mathbb{F}_p^*)^2\big)$, then for some $u \in \mathbb{F}_p^*$ there is a birational $\mathbb{F}_p$-isomorphism (respecting the conic bundles)*

$$\varphi_q \colon S_h \xrightarrow{\sim} S_{u\frac{h}{q}} \qquad \text{such that} \qquad \varphi_q \colon S_h(\mathbb{F}_p) \xrightarrow{\sim} S_{u\frac{h}{q}}(\mathbb{F}_p).$$

*Proof.* We propose to start the searching a desired transformation in the form

$$\psi_q := \begin{cases} x_2 := (b_0 + b_1 t)x - y, \\ y_2 := -x + (a_0 + a_1 t)y, \\ z_2 := a_1 b_1 q(t) z, \end{cases} \qquad \psi_q^{-1} = \begin{cases} x := (a_0 + a_1 t)x_2 + y_2, \\ y := x_2 + (b_0 + b_1 t)y_2, \\ z := z_2, \end{cases}$$

where $\det(\psi_q^{-1}) = a_1 b_1 q(t)$ and $a_0, b_0 \in \mathbb{F}_p$, $a_1, b_1 \in \mathbb{F}_p^*$. After substitution $\psi_q^{-1}$ into $S_h$ and division by $q(t)$ the coefficients of the monomials $x_2^2$, $x_2 y_2$, $y_2^2$ we obtain (with the help of Magma [122]) the remainders

$$\begin{aligned} &(a_0^2 - a_1^2 d + d - 1)x_2^2, && (2a_0 a_1 - a_1^2 c + c)x_2^2 t, \\ &2(a_0 + b_0 d - b_0 - b_1 c d)x_2 y_2, && 2\big(a_1 + b_0 c - b_1(c^2 - d + 1)\big)x_2 y_2 t, \end{aligned}$$

$$\begin{aligned} &\big(d b_0^2 - b_0^2 - 2cdb_0 b_1 + d(c^2 - d + 1)b_1^2 + 1\big)y_2^2, \\ &\big(c b_0^2 - 2(c^2 - d + 1)b_0 b_1 + c(c^2 - 2d + 1)b_1^2\big)y_2^2 t \end{aligned}$$

and the non-zero quotients $ux_2^2$, $v(t)x_2 y_2$, $w(t)y_2^2$, where

$$\begin{aligned} u &:= a_1^2 - 1, \\ v(t) &:= 2(-b_1 t + b_1 c - b_0), \\ w(t) &:= -b_1^2 t^2 + b_1(-2b_0 + b_1 c)t - b_0^2 + 2b_0 b_1 c - b_1^2(c^2 - d + 1). \end{aligned}$$

Consider the trace and norm:

$$T := \mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(s_\pm) = c^2 - 2d + 2, \qquad N := \mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(s_\pm) = c^2 + d^2 - 2d + 1.$$

Because of $\left(\frac{s_\pm}{p^2}\right) = 1$ we get $\left(\frac{N}{p}\right) = 1$. Also, it is easily checked that $T^2 - c^2 D = 4N$.

The system of reminders has two $\mathbb{F}_p$-solutions:

$$\begin{aligned} a_0 &:= c\frac{(d+1)Nb_1^2 + 1 - d}{2Nb_1}, && a_1 := \frac{TNb_1^2 - c^2}{2Nb_1}, \\ b_0 &:= c\frac{Nb_1^2 + 1}{2Nb_1}, && b_1 := \pm\sqrt{\beta}, \end{aligned}$$

where

if $c \neq 0$, then $\beta$ is exactly one (due to $\left(\frac{D}{p}\right) = -1$) of the roots

$$\frac{T \pm 2\sqrt{N}}{ND} \in \mathbb{F}_p^* \qquad \text{of} \qquad DN^2X^2 - 2TNX + c^2 \in \mathbb{F}_p[X]$$

such that $\left(\frac{\beta}{p}\right) = 1$;

if $c = 0$ and $d - 1 \in (\mathbb{F}_p^*)^2$, then $\beta := \frac{1}{d(d-1)}$ and moreover $\left(\frac{\beta}{p}\right) = 1$.

Therefore

$$\psi_q \colon S_h \xrightarrow{\simeq} S', \qquad \text{where} \qquad S' := ux_2^2 + v(t)x_2y_2 + w(t)y_2^2 - \frac{h(t)}{q(t)}z_2^2.$$

Note that $u, a_1 \neq 0$. Thus after the $\mathbb{F}_p$-transformation $\chi_q \colon S' \xrightarrow{\simeq} S_{u\frac{h}{q}}$ given by

$$\chi_q := \begin{cases} x_3 := ux_2 + \dfrac{v(t)}{2}y_2, \\ y_3 := a_1b_1y_2, \\ z_3 := z_2, \end{cases} \qquad \chi_q^{-1} = \begin{cases} x_2 := \dfrac{a_1b_1}{u}x_3 - \dfrac{v(t)}{2u}y_3, \\ y_2 := y_3, \\ z_2 := a_1b_1z_3, \end{cases}$$

(where $\det(\chi_q) = ua_1b_1$) we obtain the desired surface $S_{u\frac{h}{q}}$, i.e., $\varphi_q := \chi_q \circ \psi_q$ satisfies the theorem conditions. □

Without loss of generality let $(\sqrt{s_+})^p = -\sqrt{s_-}$. Then under the conditions of Lemma 2.22 as the lines of Figure 2.2 one takes

$$L_\pm = \begin{cases} x \pm \sqrt{s_\pm}y = 0, \\ t = r_\pm, \end{cases} \qquad M_\pm = \begin{cases} x \mp \sqrt{s_\pm}y = 0, \\ t = r_\pm. \end{cases}$$

**Corollary 2.23.** *If $c = 0$ and $d - 1 \in (\mathbb{F}_p^*)^2$ in the previous lemma, then the condition $\left(\frac{s_\pm}{p^2}\right) = 1$ is automatically fulfilled. Thus, letting $\delta := \sqrt{d(d-1)} \in \mathbb{F}_p^*$, we obtain:*

$$u = -\frac{1}{d}, \qquad v(t) = \mp\frac{2t}{\delta}, \qquad w(t) = -\frac{t^2 - d + 1}{\delta^2}$$

*(in particular, $\left(\frac{u}{p}\right) = -1$) and (up to multiplication by elements of $\mathbb{F}_p^*$)*

$$\psi_q = \begin{cases} x_2 := \pm\dfrac{t}{\delta}x - y, \\ y_2 := -x \mp \dfrac{(d-1)t}{\delta}y, \\ z_2 := -\dfrac{q(t)}{d}z, \end{cases} \qquad \psi_q^{-1} = \begin{cases} x := \mp\dfrac{(d-1)t}{\delta}x_2 + y_2, \\ y := x_2 \pm \dfrac{t}{\delta}y_2, \\ z := z_2, \end{cases}$$

$$\chi_q = \begin{cases} x_3 := x_2 \pm \dfrac{dt}{\delta}y_2, \\ y_3 := y_2, \\ z_3 := -dz_2, \end{cases} \qquad \chi_q^{-1} = \begin{cases} x_2 := x_3 \mp \dfrac{dt}{\delta}y_3, \\ y_2 := y_3, \\ z_2 := -\dfrac{1}{d}z_3. \end{cases}$$

*Proof.* It is immediately checked that

$$s_\pm = 1 - d, \qquad D = -4d, \qquad T = -2(d-1), \qquad N = (d-1)^2, \qquad \beta = \frac{1}{\delta^2}$$

and all other values are as stated. □

## 2.3 New point compression method

We will freely use notation of previous paragraphs. Below $p$ will be a prime such that $p \equiv 1 \pmod 3$, $p \equiv 3 \pmod 4$. Consider the following ordinary elliptic $\mathbb{F}_{p^2}$-curve, its Weil restriction (with respect to $\mathbb{F}_{p^2}/\mathbb{F}_p$), and the generalized Kummer $\mathbb{F}_p$-surface respectively:

$$E_b \subset \mathbb{A}^2_{(x:y)}, \qquad R_b \subset \mathbb{A}^4_{(x_0,x_1,y_0,y_1)}, \qquad GK_b \subset \mathbb{A}^1_t \times \mathbb{P}^2_{(y_0:y_1:y_2)}.$$

Note that the projection $\pi\colon GK_b \to \mathbb{A}^1_t$ is a conic bundle. In this paragraph we prove $\mathbb{F}_p$-rationality of $GK_b$, which leads to the creation of our compression method for $\mathbb{F}_{p^2}$-points of $E_b$. We also discuss some technical details of its implementation.

**Remark 2.24.** *If $\sqrt{b} = a_0 + a_1 i$ for some $a_0, a_1 \in \mathbb{F}_p$, then the general fibre of $\pi$ contains the point $(a_0 : a_1 : 1)$ and the projection from it obviously gives a birational $\mathbb{F}_p$-isomorphism between $GK_b$ and $\mathbb{A}^2$. In fact, this case does not happen in pairing-based cryptography, otherwise by Theorem 2.7 the curve $E_b$ would not be a sextic $\mathbb{F}_{p^2}$-twist for any initial $\mathbb{F}_p$-curve $E_{b'}$. Thus we can always assume that $\left(\frac{b}{p^2}\right) = -1$, in particular $b_0, b_1 \neq 0$.*

First, we reduce $GK_b$ to a diagonal form by the map $\sigma\colon GK_b \xrightarrow{\sim} S_{\alpha f}$ given by

$$\sigma := \begin{cases} x := \beta(t)y_0 + \alpha(t)y_1, \\ y := g(t)y_0, \\ z := y_2, \end{cases} \qquad \sigma^{-1} = \begin{cases} y_0 := \alpha(t)y, \\ y_1 := g(t)x - \beta(t)y, \\ y_2 := \alpha(t)g(t)z, \end{cases}$$

where $\det(\sigma) = \alpha(t)g(t)$. In particular, $\sigma$ respects the conic bundle $\pi$ and $\sigma\colon GK_b(\mathbb{F}_p) \xrightarrow{\sim} S_{\alpha f}(\mathbb{F}_p)$. Next we successively apply Corollary 2.23 and Lemma 2.22 to contract pairs of $\mathbb{F}_p$-conjugate lines lying in the fibres of $\pi$ over roots of the $\mathbb{F}_p$-irreducible polynomials $\alpha$, $\gamma$ respectively. More precisely, this is done by means of the maps

$$\varphi_{\alpha/3}\colon S_{\alpha f} \xrightarrow{\sim} S_{9f}, \qquad \varphi_\gamma\colon S_{9f} \xrightarrow{\sim} S_h,$$

where $h(t) = 9u\lambda(t)$ for some $u \in \mathbb{F}_p^*$. The cubic surface $S_h$ is $\mathbb{F}_p$-rational by the projection $pr$ from any of its two nodes (see Lemma 2.18). Thus we obtain the

maps

$$\theta := \varphi_\gamma \circ \varphi_{\alpha/3} \circ \sigma \colon GK_b \xrightarrow{\sim} S_h, \qquad \tau := pr \circ \theta \colon GK_b \xrightarrow{\sim} \mathbb{A}^2,$$
$$\theta_\varrho := \theta \circ \varrho \colon R_b \dashrightarrow S_h, \qquad \tau_\varrho := \tau \circ \varrho \colon R_b \dashrightarrow \mathbb{A}^2.$$

By analogy with $\varrho^{-1}$ we also have the map $\theta_\varrho^{-1}$ (resp. $\tau_\varrho^{-1}$) from $S_h$ (resp. $\mathbb{A}^2$) to the set-theoretic quotient of $R_b$ by $[\omega]_2$.

**Remark 2.25.** *It is immediately checked that by $\theta_\varrho$ the involution $[-1]\colon R_b \xrightarrow{\sim} R_b$ is induced to the cubic surface $S_h$ as the involution $[-1]$ from §2.2.1, §2.2.2. Similarly, on $S_h$ there is the double map $[2]$. It would be very interesting to also understand its geometric picture.*

According to Lemma 2.20 we can assume that $\left(\frac{N_h}{p}\right) = -1$, otherwise the conic bundle $\pi$ on $S_h$ (or, equivalently, on $GK_b$) has an $\mathbb{F}_p$-section. However, we do not claim that only this case occurs in practice, although it seems more likely. Taking into account Lemma 2.19 we sum up the main result of this article in

**Theorem 2.26.** *For a prime $p$ such that $p \equiv 1 \pmod 3$, $p \equiv 3 \pmod 4$ the generalized Kummer surface $GK_b$ is $\mathbb{F}_p$-rational. More precisely, assume that the conic bundle $\pi$ on $GK_b$ has no an $\mathbb{F}_p$-section, in particular $\left(\frac{b}{p^2}\right) = -1$. Then we have the birational $\mathbb{F}_p$-isomorphism*

$$\tau \colon GK_b \xrightarrow{\sim} \mathbb{A}^2 \qquad \textit{such that} \qquad \tau \colon GK_b(\mathbb{F}_p) \hookrightarrow \mathbb{A}^2(\mathbb{F}_p).$$

Another constructive proof of the $\mathbb{F}_p$-rationality could consist in applying the theory of adjoints [120, §5]. However, in our opinion, the approach using conic bundles is more simple and elegant.

The map $\varrho$ is not defined for $x_1 = 0$. We extend it to this case as follows. Let

$$R_{b,\infty} := R_b \cap \mathbb{V}(x_1) = \begin{cases} 2y_0y_1 = b_1, \\ y_0^2 - y_1^2 = x_0^3 + b_0. \end{cases} \subset \mathbb{A}^3_{(x_0,y_0,y_1)},$$

$$Q_b := 4y_0^2(y_0^2 - x_0^3 - b_0) - b_1^2 \subset \mathbb{A}^2_{(x_0,y_0)}.$$

Then the projection $\varrho_\infty \colon R_{b,\infty} \xrightarrow{\sim} Q_b$ to $(x_0, y_0)$ is a birational $\mathbb{F}_p$-isomorphism with the inverse one

$$\varrho_\infty^{-1} \colon Q_b \xrightarrow{\sim} R_{b,\infty}, \qquad \varrho_\infty^{-1} \colon (x_0, y_0) \mapsto \left(x_0, y_0, \frac{b_1}{2y_0}\right).$$

It is obvious that $\varrho_\infty$ is an isomorphism if $y_0 \neq 0$ both on $R_{b,\infty}$ and $Q_b$. In particular, this is fulfilled for $b_1 \neq 0$.

Similarly, the map $pr$ is not defined for $y = 0$. Let

$$S_{h,\infty} := x^2 - (h_1 t + h_0) z^2 \quad \subset \quad \mathbb{A}^3_{(t,x,z)}.$$

Then the projection $pr_\infty \colon S_{h,\infty} \xrightarrow{\sim} \mathbb{A}^2_{(x,z)}$ is a birational $\mathbb{F}_p$-isomorphism with the inverse one

$$pr_\infty^{-1} \colon \mathbb{A}^2_{(x,z)} \xrightarrow{\sim} S_{h,\infty}, \qquad (x,z) \mapsto \Big(x, z, \frac{x^2 - h_0 z^2}{h_1 z^2}\Big).$$

As a result, in the case $\left(\frac{N_h}{p}\right) = -1$ we obtain the compression map

$$\mathrm{com}_b \colon \overline{E_b}(\mathbb{F}_{p^2}) \hookrightarrow \mathbb{F}_p^2 \times \mathbb{F}_2^3, \quad \mathrm{com}_b(P) := \begin{cases} \big(\varrho_\infty(P), (0,0,0)\big) & \text{if} \quad x_1(P) = 0, \\ \big((0,0), (0,0,1)\big) & \text{if} \quad P = \mathcal{O}, \\ \big((pr_\infty \circ \theta_\varrho)(P), (v,0)\big) & \text{if} \quad y\big(\theta_\varrho(P)\big) = 0, \\ \big(\tau_\varrho(P), (v,1)\big) & \text{otherwise}, \end{cases}$$

where $v \in \{(0,1), (1,0), (1,1)\}$ is the position number of $x_1(P) \in \mathbb{F}_p^*$ in the representative set $\{\omega^i x_1(P) \pmod p\}_{i=0}^2$ ordered with respect to the usual numerical order. Therefore the corresponding decompression map has the form

$$\mathrm{com}_b^{-1} \colon \mathrm{Im}(\mathrm{com}_b) \twoheadrightarrow \overline{E_b}(\mathbb{F}_{p^2}), \quad \mathrm{com}_b^{-1}\big(Q, w\big) = \begin{cases} \varrho_\infty^{-1}(Q) & \text{if} \quad w = (0,0,0), \\ \mathcal{O} & \text{if} \quad w = (0,0,1), \\ (\theta_\varrho^{-1} \circ pr_\infty^{-1})(Q) & \text{if} \quad w = (v,0), \\ \tau_\varrho^{-1}(Q) & \text{if} \quad w = (v,1), \end{cases}$$

where in the two last cases the image of $\mathrm{com}_b^{-1}$ is uniquely defined by the value $v$.

### 2.3.1 Usage of the method for some curves (including BLS12-381)

In this paragraph we instantiate the new point compression method in the case $b_0 = b_1$. In particular, this condition is fulfilled for the curve BLS12-381 [38], which is one the most popular pairing-friendly curves today according to [56, Table 1]. For this curve

$$p \equiv 10 \pmod{27}, \qquad p \equiv 3 \pmod 4, \qquad \lceil \log_2(p) \rceil = 381, \qquad b = 4(1+i).$$

The former allows to extract a cubic root in $\mathbb{F}_p$ by means of 1 exponentiation in $\mathbb{F}_p$ (see Lemma 2.5). More generally, for $b_0 = b_1$ we obtain:

$$N_b = 2b_1^2, \quad \lambda(t) = b_1(t+1), \quad \gamma(t) = t^2 - 4t + 1, \quad r_\pm = 2 \pm \sqrt{-3}i, \quad s_\pm = 4r_\pm.$$

In particular, $\left(\frac{s_\pm}{p^2}\right) = 1$, because the norm $\mathrm{N}(r_\pm) = 1$. As usually, we will suppose that $\left(\frac{b}{p^2}\right) = -1$ (i.e., $\left(\frac{2}{p}\right) = -1$), hence according to the known formula $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ [108, Theorem 12.1.iv] we have $p \equiv 3 \pmod 8$.

We say that an arbitrary map has (on the average) an algebraic complexity

$$n_S S + n_{M_c} M_c + n_M M + n_I I + n_{CR} CR$$

if (for most arguments) it can be computed by means of $n_S$ squarings, $n_{M_c}$ multiplications by a constant, $n_M$ general ones (with different non-constant multiples), $n_I$ inversions and $n_{CR}$ cubic roots, where all operations are in $\mathbb{F}_p$. Additions and subtractions in $\mathbb{F}_p$ are not considered, because they are very easy to compute. We also do not take account (in $n_{M_c}$) for multiplications by a constant $c \in \mathbb{F}_p$ such that $c \pmod p \leqslant 6$, because they are not more difficult than few additions. Implementation details of the most operations mentioned see, for example, in [108].

Next we specify the maps $\varphi_{\alpha/3}$ and $\varphi_\gamma$, multiplying them by some elements of $\mathbb{F}_p^*$ to reduce their algebraic complexity.

**Corollary 2.27.** *For $q = \alpha/3$ the value $\delta = 2/3$ and hence Corollary 2.23 takes the form:*

$$u = 3, \qquad v(t) = \mp 3t, \qquad w(t) = -3\Big(\frac{3}{4}t^2 + 1\Big)$$

*and*

$$\psi_q = \begin{cases} x_2 := \pm 3tx - 2y, \\ y_2 := -2x \pm 4ty, \\ z_2 := 2\alpha(t)z, \end{cases} \qquad \psi_q^{-1} = \begin{cases} x := \pm 4tx_2 + 2y_2, \\ y := 2x_2 \pm 3ty_2, \\ z := 2z_2, \end{cases}$$

$$\chi_q = \begin{cases} x_3 := 6x_2 \mp 3ty_2, \\ y_3 := 6y_2, \\ z_3 := 2z_2, \end{cases} \qquad \chi_q^{-1} = \begin{cases} x_2 := 2x_3 \pm ty_3, \\ y_2 := 2y_3, \\ z_2 := 6z_3. \end{cases}$$

**Corollary 2.28.** *For $q = \gamma$ Lemma 2.22 takes the form:*

$$u = -\frac{1}{3}, \qquad v(t) = \mp\frac{t-1}{\sqrt{6}}, \qquad w(t) = -\frac{t^2 - 6t + 1}{24}$$

*and*

$$\psi_q = \begin{cases} x_2 := \pm\frac{\sqrt{6}}{2}(5-t)x + 6y, \\ y_2 := 6x \pm 2\sqrt{6}(1+t)y, \\ z_2 := q(t)z, \end{cases} \qquad \psi_q^{-1} = \begin{cases} x := \mp\frac{2}{\sqrt{6}}(1+t)x_2 + y_2, \\ y := x_2 \mp \frac{1}{2\sqrt{6}}(5-t)y_2, \\ z := z_2, \end{cases}$$

$$\chi_q = \begin{cases} x_3 := 2x_2 \mp \frac{\sqrt{6}}{2}(1-t)y_2, \\ y_3 := y_2, \\ z_3 := -6z_2, \end{cases} \qquad \chi_q^{-1} = \begin{cases} x_2 := -3x_3 \mp \frac{3\sqrt{6}}{2}(1-t)y_3, \\ y_2 := -6y_3, \\ z_2 := z_3. \end{cases}$$

It is easily seen that after applying $\varphi_\gamma$ we obtain the surface $S_h$ with $h(t) = -3b_1(t+1)$. In particular, $\left(\frac{N_h}{p}\right) = -1$. To make sure in correctness of the above formulas see our code [122] in the language of the computer algebra system Magma.

**Lemma 2.29.** *The maps* $\mathrm{com}_b$, $\mathrm{com}_b^{-1}$ *respectively have an algebraic complexity*

$$3S + 5M_c + 14M + 2I \qquad \textit{and} \qquad 4S + 6M_c + 18M + 3I + CR.$$

*Proof.* It is easily checked that the basic maps forming $\mathrm{com}_b$, $\mathrm{com}_b^{-1}$ have an algebraic complexity as in Table 2.1. Therefore we know that of the maps $\tau_\varrho$, $\tau_\varrho^{-1}$. Exactly these functions are computed for most arguments. It remains to note that for finding $v \in \mathbb{F}_2^2$ (during computation of $\mathrm{com}_b$) it is necessary to accomplish two multiplications by the constants $\omega$, $\omega^2$. And vice versa, this is also done to recover the initial value of $x_1$-coordinate (during computation of $\mathrm{com}_b^{-1}$). □

| map | $\varrho_\infty$ | $pr_\infty$ | $\varrho$ | $\sigma$ | $\varphi_{\alpha/3}$ | $\varphi_\gamma$ | $pr$ | $\varrho_\infty^{-1}$ |
|---|---|---|---|---|---|---|---|---|
| alg. complexity | 0 | 0 | $I$ | $S+4M$ | $S+4M$ | $S+3M_c+4M$ | $2M+I$ | $M_c+I$ |

| $pr_\infty^{-1}$ | $\varrho^{-1}$ | $\sigma^{-1}$ | $\varphi_{\alpha/3}^{-1}$ | $\varphi_\gamma^{-1}$ | $pr^{-1}$ |
|---|---|---|---|---|---|
| $2S+M_c+M+I$ | $S+4M+2I+CR$ | $S+6M$ | $3M$ | $3M_c+3M$ | $2S+M_c+2M+I$ |

Table 2.1: An algebraic complexity of the maps

## 2.4 Further questions

We end the chapter by some comments about possible generalizations of our point compression method. First of all, in addition to Theorem 2.26 the author has already proved in [54] a similar one about $\mathbb{F}_2$-rationality of the (usual) Kummer surface of some two supersingular Jacobians [55] of dimension 2. Thus we are feel free to formulate

**Conjecture 2.30.** *Let $A$ be an abelian surface over a finite field $\mathbb{F}_q$ and $\sigma$ be its $\mathbb{F}_q$-automorphism. If the generalized Kummer surface $A/\sigma$ is geometrically rational, then it is also $\mathbb{F}_q$-rational.*

We do not see any problems to extend the new point compression method to the Weil restriction $\mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E_b)$ for any finite field $\mathbb{F}_q$ such that $q \equiv 1 \pmod 3$ and $p > 3$. Besides, our approach could be immediately applied to $A_{b,b'} := E_b \times E_{b'}$ for any $b, b' \in \mathbb{F}_q^*$. Nevertheless, in this chapter we focused on the surface $R_b$, because compression of its points seemed to us more difficult and important for practice. Finally, according to Theorem 2.11 the Jacobian of a hyperelliptic curve $y^2 = x^5 + b$ (for $b \in \mathbb{F}_q^*$, $q \equiv 1 \pmod 5$, and $p > 5$) seems to also have the $\mathbb{F}_q$-rational generalized Kummer surface.

The task of point compression for $A_{b,b'}$ (so-called *double point compression*) is also reasonable. It has already been discussed (in a slightly different way) in [52] for the direct square $E^2$ of any elliptic curve $E/\mathbb{F}_q$. In that article authors do not try to compress points as compact as possible. Instead of this they find an $\mathbb{F}_q$-model of $E^2$ in $\mathbb{A}^3$ and the corresponding birational $\mathbb{F}_q$-isomorphism. The advantage of their approach is speed, because it should not solve equations at the decompression stage.

Double point compression also occurs [123] in supersingular isogeny-based cryptography [124]. The main difference from classical one is the need to compress points of a *superspecial* abelian surface $E^2$ for any supersingular elliptic curve $E/\mathbb{F}_{p^2}$ of trace $2p$ (or $-2p$). Therefore our approach does not spread immediately to this case.

Up to now we have focused only on the rationality problem of a generalized Kummer surface. However there is also another possible method to compress points of a superspecial abelian surface $E^2/\mathbb{F}_{p^2}$. According to Theorem 2.10 its Kummer surface $K$ is a so-called Zariski surface [114] for $p \not\equiv 1 \pmod{12}$. This means the existence of a purely inseparable map $K \dashrightarrow \mathbb{A}^2$ (or, equivalently, $\mathbb{A}^2 \dashrightarrow K$) of degree $p$. We stress that computation of such a map (and its inverse image) is very fast and usually even trivial. But, unfortunately, the known proof of the mentioned theorem is valid only over $\overline{\mathbb{F}_p}$ and it is absolutely not constructive.

It is very natural to think about compression for points of $m$-dimensional abelian varieties, where $m > 2$. *Multiple point compression*, i.e., that for a direct power $E^m$ of an elliptic curve $E/\mathbb{F}_q$ is discussed in [125] by analogy with double one. At the same time, by the Weil descent attack [48, §3.2], [126] it may be dangerous to consider elliptic curves over $\mathbb{F}_{q^m}$ for classical elliptic cryptography. However, in pairing-based one optimal embedding degree $k$ will exceed 12 in the near future. Therefore we will have to use twists (of degree $d$) defined over $\mathbb{F}_{q^m}$, where $m = k/d$.

According to [41, §8.2] for most $k > 12$ the curves $E_b$ are still the most pairing-

friendly, because there are methods to generate such curves with a quite large prime subgroup of $E_b(\mathbb{F}_q)$. Unfortunately, for $m > 2$ the generalized Kummer variety corresponding to the order 3 automorphism $[\omega]_m := \mathrm{R}_{\mathbb{F}_{q^m}/\mathbb{F}_q}([\omega])$ on the Weil restriction $R_{b,m} := \mathrm{R}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(E_b)$ is no longer rational [119, Lemma 8.11] even over $\overline{\mathbb{F}_q}$. Nevertheless, for $m = 3$ (resp. $m \in \{4, 5\}$) geometrical rationality is proved in [127, Theorem 1.4.(1)] (conjectured in [128, Questions 1.3, 1.4]) for the quotient of $R_{b,m}$ by the order 6 automorphism $-[\omega]_m$. Thus instead of $m$ exponentiations in $\mathbb{F}_q$ it is sufficient to accomplish only 2 ones.

# Chapter 3

# Double point compression for elliptic $\mathbb{F}_q$-curves of $j$-invariant 0

## 3.1 Double compression

For the sake of generality we will consider any pair of elliptic $\mathbb{F}_q$-curves of $j$-invariant 0, where $q \equiv 1 \pmod 3$, i.e., $\omega \in \mathbb{F}_q$. Namely, for $i = 0, 1$ let $E_i \colon y_i^2 = x_i^3 + b_i$, that is $E_{b_i}$ in our old notation. These curves are isomorphic at most over $\mathbb{F}_{q^6}$ by the map

$$\varphi \colon E_0 \xrightarrow{\sim} E_1, \qquad (x_0, y_0) \mapsto \big(\sqrt[3]{\beta} x_0, \sqrt{\beta} y_0\big),$$

where $\beta := b_1/b_0$. Also, for $k \in \mathbb{Z}/6$ let $\varphi_k := \varphi \circ [-\omega]^k = [-\omega]^k \circ \varphi$ and

$$S_i := \big\{(x_i, y_i) \in E_i \mid x_i y_i = 0\big\} \cup \big\{(0 : 1 : 0)\big\} \quad \subset \quad E_i[2] \cup E_i[3].$$

Using the fractions

$$X := \frac{x_0}{x_1}, \qquad Y := \frac{y_0}{y_1},$$

we obtain the compression map

$$\mathrm{com} \colon (E_0 \times E_1)(\mathbb{F}_q) \setminus S_0 \times S_1 \quad \hookrightarrow \quad \mathbb{F}_q^2 \times \mathbb{Z}/6 \times \mathbb{Z}/2,$$

$$\mathrm{com}(P_0, P_1) := \begin{cases} \big(X, Y, n, 0\big) & \text{if} \quad \forall k \in \mathbb{Z}/6 \colon \varphi_k(P_0) \neq P_1, \\ \big(x_0, y_0, k, 1\big) & \text{if} \quad \exists k \in \mathbb{Z}/6 \colon \varphi_k(P_0) = P_1, \end{cases}$$

where $n \in \mathbb{Z}/6$ is the position number of $z := x_1 y_1 \in \mathbb{F}_q^*$ in the set $\big\{(-1)^i \omega^j z\big\}_{i=0,j=0}^{1,2}$ ordered with respect to some order in $\mathbb{F}_q^*$. For example, in the case $q = p$ this can be the usual numerical one. Note that the condition $\varphi_k(P_0) = P_1$ is possible only if the isomorphism $\varphi$ is defined over $\mathbb{F}_q$, that is $\sqrt[6]{\beta} \in \mathbb{F}_q$. Finally, if it is necessary, points from $(S_0 \times S_1)(\mathbb{F}_q)$ can be separately processed, using few additional bits.

## 3.2 Double decompression

Let $u := x_1^3$, $v := y_1^2$, and $Z := u^2v^3 = z^6$. Since $x_0 = Xx_1$, we have $x_0^3 = X^3u$. Hence

$$Y^2 = \frac{y_0^2}{y_1^2} = \frac{x_0^3 + b_0}{x_1^3 + b_1} = \frac{X^3u + b_0}{u + b_1}$$

and

$$u = \frac{b_0 - b_1Y^2}{Y^2 - X^3}, \qquad v = u + b_1.$$

Using the number $n \in \mathbb{Z}/6$, we can extract the original sixth root

$$z = x_1y_1 = \sqrt[3]{u}\sqrt{v} = \sqrt[6]{Z} = \sqrt[3]{\sqrt{Z}}.$$

For $q \equiv 3 \pmod 4$, $q \not\equiv 1 \pmod{27}$ according to [7, §5.1.7], [46, §4]

$$a := \sqrt{Z} = \pm Z^{\frac{q+1}{4}}, \qquad \sqrt[3]{a} = \theta a^e, \qquad \text{hence} \qquad z = \pm\theta Z^{e\frac{q+1}{4}}$$

for some $\theta \in \mathbb{F}_q^*$, $\theta^9 = 1$ and $e \in \mathbb{Z}/(q-1)$. Moreover, $e$ has an explicit simple expression depending only on $q$. We eventually obtain the equalities

$$x_1 = f_n(X,Y) := \frac{uv}{z^2}, \qquad y_1 = g_n(X,Y) := \frac{z}{x_1}.$$

If $Y^2 = X^3$, then

$$\frac{x_0^3 + b_0}{x_1^3 + b_1} = \frac{x_0^3}{x_1^3} \quad \Leftrightarrow \quad b_0x_1^3 = b_1x_0^3 \quad \Leftrightarrow \quad \exists j \in \mathbb{Z}/3\colon x_1 = \omega^j\sqrt[3]{\beta}x_0.$$

This means that $\varphi_k(P_0) = P_1$ for $k \in \{j, j+3\}$. Thus the decompression map has the form

$$\mathrm{com}^{-1}\colon \mathrm{Im}(\mathrm{com}) \quad \rightarrowtail \quad (E_0 \times E_1)(\mathbb{F}_q) \setminus S_0 \times S_1,$$

$$\mathrm{com}^{-1}\big(t, s, m, bit\big) = \begin{cases} (tf_m, sg_m, f_m, g_m) & \text{if} \quad bit = 0, \\ \big((t,s), \varphi_m(t,s)\big) & \text{if} \quad bit = 1, \end{cases}$$

where $f_m := f_m(t,s)$, $g_m := g_m(t,s)$.

**Remark 3.1.** *Although the new point compression-decompression method contains a lot of inversion operations in the field $\mathbb{F}_q$, this is often harmless in regard to timing attacks* [7, §8.2.2, §12.1.1]. *The point is that this type of conversion is mainly applied to public data.*

## 3.3 Extension of the compression technique

Our approach still works well for compressing $\mathbb{F}_{q^2}$-points on the curve $E_b\colon y^2 = x^3 + b$, where $b \in \mathbb{F}_{q^2}^*$. As usual, for simplicity we take $q \equiv 3 \pmod 4$, i.e., $i := \sqrt{-1} \notin \mathbb{F}_q$. Let $b = b_0 + b_1 i$ (such that $b_0, b_1 \in \mathbb{F}_q$) and

$$x = x_0 + x_1 i, \qquad y = y_0 + y_1 i, \qquad X := \frac{x_0}{x_1}, \qquad Y := \frac{y_0}{y_1}.$$

Building on the equations of the Weil restriction $R_b = \mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(E_b)$ (see §2.1.2), we obtain

$$u := x_1^3 = \frac{2b_0 Y - b_1 \gamma(Y)}{\alpha(X)\gamma(Y) - 2\beta(X)Y}, \qquad v := y_1^2 = \frac{\beta(X)u + b_0}{\gamma(Y)},$$

where

$$\alpha(X) := 3X^2 - 1, \qquad \beta(X) := X(X^2 - 3), \qquad \gamma(Y) := Y^2 - 1.$$

As above, the degenerate cases (whenever the denominator of $X$, $Y$, $u$, or $v$ equals 0) can be easily handled independently.

Finally, consider an elliptic $\mathbb{F}_{q^2}$-curve $E_a\colon y^2 = x^3 + ax$ of $j$-invariant 1728, where $q \equiv 1 \pmod 4$. According to [7, Example 2.28] the latter condition is necessary for the ordinariness of $E_a$. Our technique also remains to be valid for compressing $\mathbb{F}_q$-points of $E_a^2$ (if $a \in \mathbb{F}_q^*$) and $\mathbb{F}_{q^2}$-points of $E_a$, because there is on $E_a$ the $\mathbb{F}_q$-automorphism $[i]\colon (x, y) \mapsto (-x, iy)$ of order 4. However in the second case one needs to take another basis of the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$.

# Part II

# Hashing to elliptic curves

# Chapter 4

# Hashing to elliptic $\mathbb{F}_q$-curves of $j$-invariant 1728

## 4.1 Weil restriction of an elliptic $\mathbb{F}_{q^2}$-curve

In this paragraph we freely use some terms from the language of abelian varieties (for details see [129]). For a prime $p > 3$ and any its power $q$ consider the finite field extension $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{\gamma})$, where $\gamma \in \mathbb{F}_q$, $\sqrt{\gamma} \notin \mathbb{F}_q$, and hence $(\sqrt{\gamma})^q = -\sqrt{\gamma}$. Besides, for $i \in \{0, 1\}$ consider two elliptic $\mathbb{F}_{q^2}$-curves $\overline{E_i}$ given by the affine Weierstrass forms

$$E_i \colon y_i^2 = x_i^3 + a^{q^i} x_i + b^{q^i} \quad \subset \quad \mathbb{A}^2_{(x_i, y_i)}.$$

In other words, $\overline{E_i} = E_i \sqcup \{P_\infty\} \subset \mathbb{P}^2$, where $P_\infty := (0 : 1 : 0)$. These curves are obviously isogenous by means of the Frobenius maps $\mathrm{Fr} \colon E_0 \to E_1$, $\mathrm{Fr} \colon E_1 \to E_0$ over $\mathbb{F}_q$ and $j(E_0) = j(E_1)^q$.

Consider the Weil restriction $R_i$ (resp. $\overline{R_i}$) of $E_i$ (resp. $\overline{E_i}$) with respect to $\mathbb{F}_{q^2}/\mathbb{F}_q$ (see, e.g., [83, §8.1]). We stress that $\overline{R_i} \not\simeq R_i \cup \{P_\infty\}$ even over $\overline{\mathbb{F}_q}$, however we will identify $E_i$ (resp. $R_i$) with $\overline{E_i}$ (resp. $\overline{R_i}$) for simplicity of the notation. Let $A := E_0 \times E_1$ and

$$a := a_0 + a_1\sqrt{\gamma}, \qquad b := b_0 + b_1\sqrt{\gamma}, \qquad x_0 := u_0 + u_1\sqrt{\gamma}, \qquad y_0 := v_0 + v_1\sqrt{\gamma},$$

where $a_0, a_1, b_0, b_1 \in \mathbb{F}_q$. By definition $R_i(\mathbb{F}_q) = E_i(\mathbb{F}_{q^2})$ and

$$R_i \colon \begin{cases} v_0^2 + \gamma v_1^2 = u_0^3 + 3\gamma u_0 u_1^2 + a_0 u_0 + (-1)^i a_1 \gamma u_1 + b_0, \\ 2v_0 v_1 = \gamma u_1^3 + 3u_0^2 u_1 + a_0 u_1 + (-1)^i (a_1 u_0 + b_1) \end{cases} \quad \subset \quad \mathbb{A}^4_{(u_0, v_0, u_1, v_1)}.$$

Although $j$-invariants of the curves $E_i$ may be different (i.e., $j(E_i) \notin \mathbb{F}_q$), we always have the involution

$$s \colon \mathbb{A}^4 \xrightarrow{\sim} \mathbb{A}^4, \qquad (u_0, v_0, u_1, v_1) \mapsto (u_0, v_0, -u_1, -v_1)$$

such that $s\colon R_0 \xrightarrow{\sim} R_1$ and $s|_{R_0(\mathbb{F}_q)} = \mathrm{Fr}|_{E_0(\mathbb{F}_{q^2})}$. Thus we will also identify $R_0$ with $R_1$, omitting the index. Besides, there is an $\mathbb{F}_{q^2}$-isomorphism

$$\theta\colon \mathbb{A}^4_{(u_0,v_0,u_1,v_1)} \xrightarrow{\sim} \mathbb{A}^4_{(x_0,y_0,x_1,y_1)} \qquad \text{s.t.} \qquad \theta\colon R \xrightarrow{\sim} A$$

given by the matrix

$$\theta := \begin{pmatrix} 1 & 0 & \sqrt{\gamma} & 0 \\ 0 & 1 & 0 & \sqrt{\gamma} \\ 1 & 0 & -\sqrt{\gamma} & 0 \\ 0 & 1 & 0 & -\sqrt{\gamma} \end{pmatrix}, \qquad \text{where} \qquad \theta^{-1} = \frac{1}{2\sqrt{\gamma}} \begin{pmatrix} \sqrt{\gamma} & 0 & \sqrt{\gamma} & 0 \\ 0 & \sqrt{\gamma} & 0 & \sqrt{\gamma} \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

Consider the permutation

$$s' := \theta \circ s \circ \theta^{-1}\colon \mathbb{A}^4 \xrightarrow{\sim} \mathbb{A}^4, \qquad (x_0, y_0, x_1, y_1) \mapsto (x_1, y_1, x_0, y_0)$$

and the "twisted" Frobenius endomorphism

$$\pi\colon \mathbb{A}^4 \to \mathbb{A}^4, \qquad (x_0, y_0, x_1, y_1) \mapsto (x_1^q, y_1^q, x_0^q, y_0^q) \qquad \text{s.t.} \qquad \pi\colon A \to A.$$

It is easily checked that $\theta^{-1} \circ \pi \circ \theta$ is the (usual) Frobenius endomorphism. Thus $\pi$-invariant (hence $\mathbb{F}_{q^2}$-rational) curves $C \subset A$ and maps $\varphi\colon A \dashrightarrow \mathbb{A}^4_{(x_0,y_0,x_1,y_1)}$ correspond to $\mathbb{F}_q$-ones

$$\theta^{-1}(C) \subset R, \qquad \theta^{-1} \circ \varphi \circ \theta\colon R \dashrightarrow \mathbb{A}^4_{(u_0,v_0,u_1,v_1)}.$$

This means that

$$C = s'\big(C^{(1)}\big), \qquad \varphi = \big(\varphi_{x_0}, \varphi_{y_0}, \varphi^{(1)}_{x_0} \circ s', \varphi^{(1)}_{y_0} \circ s'\big),$$

where $C^{(1)}$ is the $\mathbb{F}_q$-conjugate curve to $C$ and $\varphi^{(1)}_{x_0}, \varphi^{(1)}_{y_0}$ are the $\mathbb{F}_q$-conjugate functions to some $\varphi_{x_0}, \varphi_{y_0} \in \mathbb{F}_{q^2}(A)$.

It is also worth noting that on $A$ there are natural involutions $[-1]$ and $[-1]^i \times [-1]^{i+1}$ (for $i \in \{0, 1\}$), which are transformed to $R$ by $\theta$ as

$$\begin{aligned} &(u_0, v_0, u_1, v_1) \mapsto (u_0, -v_0, u_1, -v_1), \\ &(u_0, v_0, u_1, v_1) \mapsto \Big(u_0,\ (-1)^i\sqrt{\gamma}v_1,\ u_1,\ (-1)^i(\sqrt{\gamma})^{-1}v_0\Big) \end{aligned}$$

respectively.

Hereafter we assume that $a, b \in \mathbb{F}_q$ (i.e., $E := E_0 = E_1$). In this case $s' \colon E^2 \xrightarrow{\sim} E^2$. Let $\Delta, \Delta' \subset E^2$ be the diagonal and antidiagonal respectively. Besides, we have the quadratic $\mathbb{F}_q$-twist of $E$:

$$E' \colon \gamma y^2 = x^3 + ax + b, \qquad \sigma \colon E' \xrightarrow{\sim} E, \qquad (x, y) \mapsto (x, \sqrt{\gamma} y).$$

The curves $E, E'$ are naturally embedded in $R$ as

$$\theta^{-1}(\Delta) = R \cap \{u_1 = v_1 = 0\} = E, \qquad \theta^{-1}(\Delta') = R \cap \{u_1 = v_0 = 0\} = E'.$$

Consider the exact sequences

$$0 \to E \hookrightarrow R \xrightarrow{\tau'} E' \to 0, \qquad 0 \to E' \hookrightarrow R \xrightarrow{\tau} E \to 0,$$

of $\mathbb{F}_q$-(homo)morphisms, where $\tau := [1] + s$, $\tau' := [1] - s$. Note that $\tau|_{R(\mathbb{F}_q)}$ is just the trace map on $E$ with respect to $\mathbb{F}_{q^2}/\mathbb{F}_q$. As a result, we obtain the $\mathbb{F}_q$-rational $(2,2)$-isogeny

$$\chi := \tau \times \tau' \colon R \to E \times E' \qquad \text{with} \qquad \ker(\chi) = E \cap E' = E[2] = E'[2].$$

Finally, the $(2,2)$-isogenies

$$\psi := \chi \circ \theta^{-1} \colon E^2 \to E \times E', \qquad \psi = \begin{pmatrix} 1 & 1 \\ \sigma^{-1} & -\sigma^{-1} \end{pmatrix}$$

and $\widehat{\chi} \colon E \times E' \to R$ (dual to $\chi$) have the kernels

$$\ker(\psi) = \Delta \cap \Delta' = \Delta[2] = \Delta'[2], \qquad \ker(\widehat{\chi}) = \Gamma \cap \Gamma' = \Gamma[2] = \Gamma'[2],$$

where $\Gamma$, $\Gamma'$ are the graphs of $\sigma$ and $-\sigma = \mathrm{Fr} \circ \sigma \circ \mathrm{Fr}^{-1}$ respectively.

**Theorem 4.1.** *It is easily checked that* $(\mathrm{Fr} \times \mathrm{Fr}) \circ \psi = \psi \circ \pi$. *In particular,* $\pi$*-invariant points and curves on* $E^2$ *are transformed by means of* $\psi$ *to* $\mathbb{F}_q$*-ones on* $E \times E'$.

## 4.2 Kummer surfaces

In this paragraph we handle some concepts of two-dimensional algebraic geometry, which can be found, for example, in [1, Chapter V]. For $i \in \{0, 1\}$ consider any two elliptic $\mathbb{F}_q$-curves $\overline{E_i} \subset \mathbb{P}^2$ given by the Weierstrass forms

$$E_i \colon y_i^2 = f_i(x_i) := x_i^3 + a_i x_i + b_i \quad \subset \quad \mathbb{A}^2_{(x_i, y_i)}$$

and their direct product

$$A := E_0 \times E_1 \subset \mathbb{A}^4_{(x_0,y_0,x_1,y_1)}, \qquad \overline{A} = \overline{E_0} \times \overline{E_1} \hookrightarrow \mathbb{P}^8,$$

where the second map is the Segre embedding. For $j \in \{0,1,2\}$ let $r_j$ (resp. $s_j$) are roots of $f_0$ (resp. $f_1$) and $P_{r_j} := (r_j, 0)$ (resp. $P_{s_j} := (s_j, 0)$) are order 2 points on $E_0$ (resp. $E_1$). Also, let $\infty := (1:0)$ and $P_\infty := (0:1:0)$. Note that

$$\overline{A} = A \ \sqcup \ \big(\overline{E_0} \times \{P_\infty\} \ \cup \ \{P_\infty\} \times \overline{E_1}\big).$$

Hereafter we will identify $E_0$, $\overline{E_0}$, $\overline{E_0} \times \{P_\infty\}$ (resp. $E_1$, $\overline{E_1}$, $\{P_\infty\} \times \overline{E_1}$), and $A$, $\overline{A}$.

By definition, the *Kummer surface* $K_A$ of $A$ (see, e.g., [72, §4]) is the minimal singularity resolution $bl$ of the geometric quotient $A/[-1]$, which is sometimes called (*singular*) *Kummer surface*. In other words, $bl$ is blowing up 16 nodes, which form the image of $A[2]$ to $A/[-1]$. If $E_0 \simeq E_1$, then at least over $\overline{\mathbb{F}_q}$ the Kummer surface $K_A$ is birationally isomorphic to a quartic in $\mathbb{P}^3$ with 12 nodes. It is so-called *desmic surface*, which is related to the *desmic system* of three tetrahedrons (for more details see, e.g., [130, §B.5.2]).

There are also natural models

$$\begin{aligned} A/[-1]\colon y^2 = f_0(x_0)f_1(x_1) \quad &\subset \quad \mathbb{A}^3_{(x_0,x_1,y)}, \\ K_A\colon y_0^2 f_1(x_1) = y_1^2 f_0(x_0) \quad &\subset \quad \mathbb{A}^2_{(x_0,x_1)} \times \mathbb{P}^1_{(y_0:y_1)} \end{aligned}$$

and the two-sheeted maps

$$\begin{aligned} &\rho\colon A \to A/[-1], \quad (x_0,y_0,x_1,y_1) \mapsto (x_0, x_1, y_0y_1), \\ &\rho'\colon A \dashrightarrow K_A, \qquad (x_0,y_0,x_1,y_1) \mapsto \big((x_0,x_1),(y_0:y_1)\big). \end{aligned}$$

Therefore blowing up and blowing down maps

$$bl = \rho \circ (\rho')^{-1}\colon K_A \to A/[-1], \qquad bl^{-1} = \rho' \circ \rho^{-1}\colon A/[-1] \dashrightarrow K_A$$

have the form

$$\begin{aligned} &\big((x_0,x_1),(y_0:y_1)\big) \mapsto \Big(x_0, x_1, f_1(x_1)\frac{y_0}{y_1}\Big) = \Big(x_0, x_1, f_0(x_0)\frac{y_1}{y_0}\Big), \\ &(x_0,x_1,y) \mapsto \Big((x_0,x_1),\big(y : f_1(x_1)\big)\Big) = \Big((x_0,x_1),\big(f_0(x_0) : y\big)\Big) \end{aligned}$$

respectively. Further, the involutions $[1]\times[-1]$, $[-1]\times[1]$ on $A$ are induced to $A/[-1]$ as $(x_0,x_1,y) \mapsto (x_0,x_1,-y)$. Since $E_i/[-1] = \mathbb{P}^1$, the quotient of $A/[-1]$ under this new involution is $\mathbb{P}^1 \times \mathbb{P}^1$ and the corresponding natural map is denoted by $pr$. In simple words, it is the projection to the coordinates $x_0, x_1$.

For $r \in \{r_0, r_1, r_2, \infty\}$, $s \in \{s_0, s_1, s_2, \infty\}$ let

$$L_r := \rho(\{P_r\} \times E_1), \qquad M_s := \rho(E_0 \times \{P_s\})$$

and $E_{r,s}$ be the exceptional $(-2)$-curve on $K_A$ corresponding to the point $\rho(P_r, P_s)$. For $r, s \neq \infty$ it is easily seen that

$$L_r = \{x_0 = r, y = 0\}, \qquad M_s = \{x_1 = s, y = 0\}, \qquad E_{r,s} = \{x_0 = r, x_1 = s\}.$$

Since $Ram := \bigsqcup_{r,s}(L_r \cup M_s)$ is exactly the ramification locus of $pr$, we will identify the lines $L_r$, $pr(L_r)$ and $M_s$, $pr(M_s)$. Note that

$$\overline{A}/[-1] = A/[-1] \sqcup (L_\infty \cup M_\infty), \qquad \mathbb{P}^1 \times \mathbb{P}^1 = \mathbb{A}^2_{(x_0,x_1)} \sqcup (L_\infty \cup M_\infty).$$

It is well known that $K_A$ is a K3 surface [131], i.e., its canonical class and the first cohomology space $\mathrm{H}^1(K_A, \mathcal{O}_{K_A})$ of the structure sheaf $\mathcal{O}_{K_A}$ are zero. According to [132, §2.8.4] and [131, §17.2], [133, Proposition 3.1] we have:

$$\mathrm{NS}(A) \simeq \mathbb{Z}[E_0, E_1] \oplus \mathrm{Hom}(E_0, E_1) \qquad \mathrm{NS}(K_A) \simeq \mathrm{Pic}(K_A) \simeq \mathrm{NS}(A) \oplus \mathbb{Z}[\{E_{r,s}\}]^{\mathrm{Fr}}$$

In particular, ranks of these free groups (i.e., Picard $\mathbb{F}_q$-numbers) satisfy the inequalities

$$2 \leqslant \rho(A) \leqslant 6, \qquad 8 \leqslant \rho(K_A) \leqslant 22$$

If $\rho(A) = 2$, then the curves $E_0, E_1$ are not isogenous over $\mathbb{F}_q$. At the same time, from $\rho(A) = 6$ it follows that $E_0, E_1$ are supersingular [133, §2] and the surface $K_A$ is geometrically unirational [131, Remark 18.3.14].

For an absolutely irreducible (possibly singular) $\mathbb{F}_q$-curve $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ (s.t. $C \nsubseteq Ram$) we denote by $r_C$ the count of branches $B$ [134, §4.3] on $C$ such that the intersection number $\mathrm{I}_P(B, Ram)$ is odd, where $P$ is the centre of $B$. It is known that branches on $C$ are in the natural bijective correspondence with points of the singularity resolution of $C$, i.e., with discrete valuations of the function field $\overline{\mathbb{F}_q}(C)$. Denoting by $\nu$ the discrete valuation corresponding to $B$, by virtue of [75, §1] we get

$$\mathrm{I}_P(B, Ram) = \begin{cases} \nu\big(f_0(x_0) f_1(x_1)\big) & \text{if} \quad P \in \mathbb{A}^2_{(x_0,x_1)}, \\ \nu\big(1/(x_0 x_1)\big) & \text{if} \quad P \in L_\infty \cup M_\infty. \end{cases} \tag{4.1}$$

Thus in order to calculate the value $r_C$ we can choose any of the two given equivalent notions.

**Theorem 4.2** ([75, Proposition 1.2.3]). *Suppose that $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ is a rational $\mathbb{F}_q$-curve. Let $D := pr^{-1}(C)$ and $k$ be one of the fields $\mathbb{F}_q, \mathbb{F}_{q^2}$.*

1. *If $r_C = 0$, then $D$ consists of two absolutely irreducible rational curves $D_0, D_1$ defined at most over $\mathbb{F}_{q^2}$. Moreover, $D$ is reducible over $k$ if and only if $y = \sqrt{f_0(x_0)f_1(x_1)} \in k(C)$. In this case $pr\colon D_0 \to C$, $pr\colon D_1 \to C$ are birational $k$-morphisms.*

2. *If $r_C > 0$, then $D$ is an absolutely irreducible (possibly singular) $\mathbb{F}_q$-curve of geometric genus $r_C/2 - 1$ (in particular, $2 \mid r_C$). Moreover, for $r_C > 2$ the curve $D$ is hyperelliptic.*

**Theorem 4.3** ([72, Lemma 4.1], [75, §2.1])**.**

1. *A curve $D \subset A/[-1]$ is rational if and only if $H := \rho^{-1}(D) \subset A$ is a (possibly singular) hyperelliptic curve such that the hyperelliptic involution on $H$ is the restriction of $[-1]$.*

2. *Moreover, if the image $C := pr(D)$ is of bidegree $(1,1)$ and $r_C = 2$, then geometric genus $g(H) = 2$ and $H$ also has a non-hyperelliptic involution $i$ such that $H/i = E_0$, $H/-i = E_1$ (such hyperelliptic curves are studied in detail, e.g., in [135]).*

Suppose that $E_0, E_1$ are $\mathbb{F}_q$-conjugate elliptic $\mathbb{F}_{q^2}$-curves as in §4.1 (hence we will use its notation). Let $K_R$ be the Kummer surface of the Weil restriction $R$ and

$$Q := K_R/\big\langle [1]\times[-1]\big\rangle \;=\; R/\big\langle [1]\times[-1], [-1]\times[1]\big\rangle.$$

Looking at the transformation $\theta\colon R \xrightarrow{\sim} A$, we see that in affine coordinates the natural two-sheeted maps have the form

$$\begin{aligned} &\rho\colon R \to R/[-1], \quad (u_0, v_0, u_1, v_1) \mapsto (u_0, u_1, v_0^2 - \gamma v_1^2),\\ &pr\colon R/[-1] \to Q, \quad (u_0, u_1, v) \mapsto (u_0, u_1). \end{aligned}$$

Besides, denote by $\overline{\theta}$, $\overline{\overline{\theta}}$ isomorphisms over $\mathbb{F}_{q^2}$ that are the restrictions of $\theta$ to $R/[-1] \subset \mathbb{A}^3_{(u_0,u_1,v)}$ and $Q$ respectively. Thus we obtain the commutative diagram

$$\begin{array}{ccc} R & \overset{\theta}{\xrightarrow{\sim}} & A \\ \rho\downarrow & & \downarrow\rho \\ R/[-1] & \overset{\overline{\theta}}{\xrightarrow{\sim}} & A/[-1] \\ pr\downarrow & & \downarrow pr \\ Q & \overset{\overline{\overline{\theta}}}{\xrightarrow{\sim}} & \mathbb{P}^1\times\mathbb{P}^1 \end{array}$$

Note that $\overline{\overline{\theta}} = (u_0 + u_1\sqrt{\gamma}, u_0 - u_1\sqrt{\gamma})$ is the standard transformation between affine open subsets of the elliptic and hyperbolic quadratic surfaces (see, e.g., Theorem 7.21). As a result, $Q$ is the first one, which is also the Weil restriction of $\mathbb{P}^1$ with respect to $\mathbb{F}_{q^2}/\mathbb{F}_q$ [83, Exercise 8.1.6.iii]. Finally, $\overline{\theta}$ is given by the same formulas as $\overline{\overline{\theta}}$ with the coordinate $v$ remaining in place (i.e. $y := v$).

## 4.3 A rational curve on the Kummer surface

We will often use notation and results from §4.1-4.2. Consider a finite field $\mathbb{F}_q$ of characteristic $p > 3$. We are interested in elliptic $\mathbb{F}_q$-curves $E_a\colon y^2 = f(x) := x^3 - ax$ of $j$-invariant 1728. According to [6, Example V.4.5] they are ordinary if and only if $p \equiv 1 \pmod 4$, i.e., $\sqrt{-1} \in \mathbb{F}_p$. For definiteness, we will suppose this condition, because for pairing-based cryptography supersingular curves are insecure at the moment.

Any two $\mathbb{F}_q$-curves of $j = 1728$ are isomorphic (at most over $\mathbb{F}_{q^4}$) by the map

$$E_a \xrightarrow{\sim} E_{a'}, \qquad (x, y) \mapsto (\sqrt{\alpha}x, \sqrt[4]{\alpha^3}y),$$

where $\alpha := a'/a$. From now on we assume that $\sqrt{a} \notin \mathbb{F}_q$ (hence $\sqrt[4]{a} \notin \mathbb{F}_{q^2}$). Therefore the curves $E_{a^i}$ (for $i \in \mathbb{Z}/4$) are unique ones (up to $\mathbb{F}_q$-isomorphism) of $j = 1728$. For $E_1, E_a$ there are the quadratic $\mathbb{F}_q$-twists

$$E_1'\colon ay^2 = x^3 - x, \qquad E_a'\colon ay^2 = x^3 - ax$$

and the corresponding $\mathbb{F}_{q^2}$-isomorphisms $\sigma\colon E_1' \xrightarrow{\sim} E_1$, $\sigma\colon E_a' \xrightarrow{\sim} E_a$. It is obvious that

$$E_1' \xrightarrow{\sim} E_{a^2}, \qquad E_a' \xrightarrow{\sim} E_{a^3}, \qquad (x, y) \mapsto (ax, a^2y).$$

The curves $E_{a^i}$ are pairwise non-isogenous over $\mathbb{F}_q$ [7, Proposition 2.5]. Hence, in particular, the Picard $\mathbb{F}_q$-numbers of the Kummer surfaces $K_{E_1 \times E_1'}$ and $K_{E_a \times E_a'}$ are equal to 18 and 12 respectively. In this paragraph we focus on constructing a rational $\mathbb{F}_q$-curve only on $K_{E_a \times E_a'}$, because this is more difficult than analogous task for $K_{E_1 \times E_1'}$.

Obviously,

$$E_a[2] = E_a'[2] = \{P_0, P_\pm, P_\infty\}, \qquad P_0 := (0, 0), \qquad P_\pm := (\pm\sqrt{a}, 0).$$

According to the Vélu formulas [2, §25.1.1] we obtain:

$$E_a/\langle P_0\rangle \simeq_{\mathbb{F}_q} E_a, \qquad E_\pm := E_a/\langle P_\pm\rangle\colon\ y^2 = x^3 - 11ax \mp 14a\sqrt{a},$$

where $j(E_\pm) = 287496$, and the corresponding vertical dual to each other 2-isogenies

$$\widehat{\varphi_\pm}\colon E_a \to E_\pm, \qquad \varphi_\pm\colon E_\pm \to E_a$$

have the form

$$\widehat{\varphi_\pm} = \begin{cases} x := x + \dfrac{2a}{x \mp \sqrt{a}}, \\ y := \Big(1 - \dfrac{2a}{(x \mp \sqrt{a})^2}\Big) y, \end{cases} \qquad \varphi_\pm = \begin{cases} x := \Big(x + \dfrac{a}{x \pm 2\sqrt{a}}\Big)/4, \\ y := \Big(1 - \dfrac{a}{(x \pm 2\sqrt{a})^2}\Big) y/8. \end{cases}$$

For compactness we will often use the value $\alpha_\pm := 1 \pm 2\sqrt{2}$. Note that

$$E_+[2] = \big\{Q_0^{(0)}, Q_\pm^{(0)}, P_\infty\big\}, \qquad E_-[2] = \big\{Q_0^{(1)}, Q_\pm^{(1)}, P_\infty\big\},$$

where

$$Q_0^{(i)} := \big((-1)^{(i+1)} 2\sqrt{a}, 0\big), \qquad Q_\pm^{(i)} := \big((-1)^i \alpha_\pm \sqrt{a}, 0\big).$$

Clearly,

$$\begin{aligned} \widehat{\varphi_+}(P_0) = \widehat{\varphi_+}(P_-) &= Q_0^{(0)}, & \varphi_+\big(Q_\pm^{(0)}\big) &= P_+, \\ \widehat{\varphi_-}(P_0) = \widehat{\varphi_-}(P_+) &= Q_0^{(1)}, & \varphi_-\big(Q_\pm^{(1)}\big) &= P_- \end{aligned}$$

and hence

$$E_a = E_+/\big\langle Q_0^{(0)} \big\rangle = E_-/\big\langle Q_0^{(1)} \big\rangle.$$

Finally, letting

$$A_\pm := E_+ \times E_-, \qquad A_a := E_a \times E_a, \qquad A'_a := E_a \times E'_a,$$

consider the dual to each other $(2,2)$-isogenies

$$\widehat{\varphi} := \widehat{\varphi_+} \times \widehat{\varphi_-} \colon\ A_a \to A_\pm, \qquad \varphi := \varphi_+ \times \varphi_- \colon\ A_\pm \to A_a,$$

which are $\pi$-invariant.

Next, let

$$\begin{aligned} \overline{\varphi} &:= \rho \circ \varphi \circ \rho^{-1} \colon\ A_\pm/[-1] \to A_a/[-1], & \overline{\psi} &:= \rho \circ \psi \circ \rho^{-1} \colon\ A_a/[-1] \to A'_a/[-1], \\ \overline{\overline{\varphi}} &:= pr \circ \overline{\varphi} \circ pr^{-1} \colon\ \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1, & \overline{\overline{\psi}} &:= pr \circ \overline{\psi} \colon\ A_a/[-1] \to \mathbb{P}^1 \times \mathbb{P}^1, \end{aligned}$$

where $\psi$ is taken from §4.1. These maps form a commutative diagram represented in Figure 4.4. Note that $\overline{\psi}$ does not descend to any map $\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1 \times \mathbb{P}^1$. Looking at the formulas of the isogeny $\varphi$, we obtain:

$$\overline{\varphi} = \begin{cases} x_0 := \Big(x_0 + \dfrac{a}{x_0 + 2\sqrt{a}}\Big)/4, \\ x_1 := \Big(x_1 + \dfrac{a}{x_1 - 2\sqrt{a}}\Big)/4, \\ y := \Big(1 - \dfrac{a}{(x_0 + 2\sqrt{a})^2}\Big)\Big(1 - \dfrac{a}{(x_1 - 2\sqrt{a})^2}\Big) y/64. \end{cases}$$

At the same time, using the famous formulas of addition and subtraction on elliptic curves (see, e.g., [2, §9.1]) yields:

$$\overline{\overline{\psi}} = \begin{cases} x_0 = \dfrac{x_0^2x_1 + x_0x_1^2 - a(x_0+x_1) - 2y}{(x_0-x_1)^2}, \\ x_1 = \dfrac{x_0^2x_1 + x_0x_1^2 - a(x_0+x_1) + 2y}{(x_0-x_1)^2}. \end{cases}$$

Below we will often use the computer algebra system Magma to produce equations or formulas and check theoretical facts (see the corresponding code in [136]). Consider on $\mathbb{A}^2_{(x_0,x_1)} \subset \mathbb{P}^1 \times \mathbb{P}^1$ the $\pi$-invariant conic

$$C_1 \colon 6x_0x_1 - 11\sqrt{a}x_0 + 11\sqrt{a}x_1 - 20a,$$

which is the unique bidegree $(1,1)$ curve passing through the points

$$\big(-2\sqrt{a},\ 2\sqrt{a}\big), \qquad \big(\alpha_+\sqrt{a},\ -\alpha_-\sqrt{a}\big), \qquad \big(\alpha_-\sqrt{a},\ -\alpha_+\sqrt{a}\big).$$

Using Magma, one can compute the defining polynomial of $C_2 := \overline{\overline{\varphi}}(C_1)$, namely

$$C_2 \colon 24x_0^2x_1 + 25\sqrt{a}x_0^2 - 24x_0x_1^2 - 62\sqrt{a}x_0x_1 - 40ax_0 + 25\sqrt{a}x_1^2 + 40ax_1 + 16a\sqrt{a}.$$

This is a $\pi$-invariant cubic (of bidegree $(2,2)$) having the node $(\sqrt{a}, -\sqrt{a})$.

Looking at Formula (4.1) or Figures 4.1, 4.2 of $C_1, C_2$ respectively, we obtain $r_{C_1} = r_{C_2} = 2$. Therefore by Theorem 4.2 the $\pi$-invariant curves

$$D_1 := pr^{-1}(C_1) \ \subset\ A_\pm/[-1], \qquad D_2 := pr^{-1}(C_2) = \overline{\varphi}(D_1) \ \subset\ A_a/[-1]$$

are rational. It turns out that the restriction $\overline{\overline{\varphi}} \colon C_1 \to C_2$ (and hence $\overline{\varphi} \colon D_1 \to D_2$ by [64, Lemmas 2.41, 2.42]) is invertible. Indeed, Magma gives the formulas

$$(\overline{\overline{\varphi}})^{-1} \colon C_2 \dashrightarrow C_1, \qquad (\overline{\overline{\varphi}})^{-1} = \begin{cases} x_0 := \dfrac{24x_0^2 - 24x_0x_1 - 49\sqrt{a}x_0 + 25\sqrt{a}x_1 + 26a}{6(x_0 - \sqrt{a})}, \\ x_1 := \dfrac{11\sqrt{a}x_0 + \sqrt{a}x_1 - 10a}{6(x_0 - \sqrt{a})}. \end{cases}$$

Finally, denote by $C_2^{(1)}$ (resp. $D_2^{(1)} = pr^{-1}\big(C_2^{(1)}\big)$) the curve $\mathbb{F}_q$-conjugate to $C_2$ (resp. $D_2$).

Again, by means of Magma we get the image $C_8 := \overline{\overline{\psi}}(D_2) = \overline{\overline{\psi}}\big(D_2^{(1)}\big)$ (see Figure 4.3) given by the symmetric $\mathbb{F}_q$-polynomial

$$C_8\colon 5764801a^3s_1^8 - 921984a^2s_1^6s_2^2 + 3471884416a^3s_1^6s_2 + 6914880000a^4s_1^6 + 36864as_1^4s_2^4 -$$
$$6463336448a^2s_1^4s_2^3 + 216401113088a^3s_1^4s_2^2 - 1634869760000a^4s_1^4s_2 + 2073600000000a^5s_1^4 +$$
$$966524928as_1^2s_2^5 - 3811311616a^2s_1^2s_2^4 - 941125009408a^3s_1^2s_2^3 + 10180198400000a^4s_1^2s_2^2 -$$
$$14745600000000a^5s_1^2s_2 - 37748736s_2^7 + 1124073472as_2^6 - 56463720448a^2s_2^5 +$$
$$757642297344a^3s_2^4 - 15920005120000a^4s_2^3 + 26214400000000a^5s_2^2,$$

where $s_1 := x_0 + x_1$, $s_2 := x_0x_1$ are the elementary symmetric polynomials. Note that $\operatorname{bideg}(C_8) = (8,8)$. Since $r_{C_8} = 0$ (see [136] or Figure 4.3) it follows from Theorem 4.2 that the inverse image $pr^{-1}(C_8)$ consists of two different rational curves $D_8 := \overline{\psi}(D_2)$ and $D_8' := \overline{\psi}\big(D_2^{(1)}\big)$ such that the restrictions $pr\colon D_8 \to C_8$, $pr\colon D_8' \to C_8$ are birational. Moreover, $D_8, D_8'$ are defined over the field $\mathbb{F}_q$, since $D_2, D_2^{(1)}$ are $\pi$-invariant. This is an immediate corollary from Theorem 4.1.

Such the long way to obtain a rational $\mathbb{F}_q$-curve on $A_a'/[-1]$ is justified by the following lemma, which can be checked by a reasonable exhaustive search.

**Lemma 4.4.** *Let $C \subset \mathbb{P}^1 \times \mathbb{P}^1$ be an absolutely irreducible $\mathbb{F}_q$-invariant (resp. $\pi$-invariant) $(1,1)$-curve such that $r_C \in \{0,2\}$ with respect to $\{\pm\sqrt{a}, 0, \infty\}$. Then $r_C = 0$ and $pr^{-1}(C) \subset A_a'/[-1]$ (resp. $pr^{-1}(C) \subset A_a/[-1]$) consists of two $\mathbb{F}_q$-conjugate (resp. $\pi$-conjugate) curves.*

Further, according to the Magma computation we obtain

**Lemma 4.5.**

1. *The curve $C_8 \subset \mathbb{P}^1 \times \mathbb{P}^1$ has exactly 42 singular points, where $(0,0)$, $(\infty,\infty)$ are unique ones from the ramification locus Ram.*
2. *The point $(0,0)$ is a non-ordinary singularity of multiplicity 4 with two different tangents (each one of multiplicity 2).*
3. *The point $(\infty,\infty)$ is a node, whose tangents are the lines $L_\infty, M_\infty$. Moreover, this point is an inflexion one with respect to each of the two local branches.*

By Theorem 4.3 the inverse images

$$H_i := \rho^{-1}(D_i), \qquad H_2^{(1)} := \rho^{-1}\big(D_2^{(1)}\big), \qquad H_8' := \rho^{-1}(D_8'),$$

where $i \in \{1,2,8\}$, are hyperelliptic curves. Note that the maps

$$\varphi\colon H_1 \to H_2, \qquad \psi\colon H_2 \to H_8, \qquad \psi\colon H_2^{(1)} \to H_8'$$

are birational and hence all these curves have geometric genus 2 and a non-hyperelliptic involution. We now have everything to represent Figure 4.5.

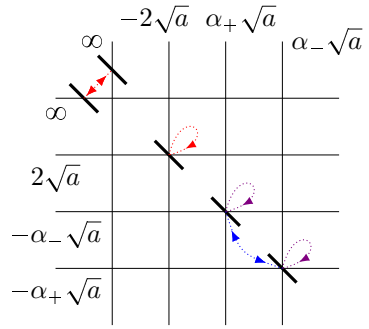


Figure 4.1: The curve $C_1$

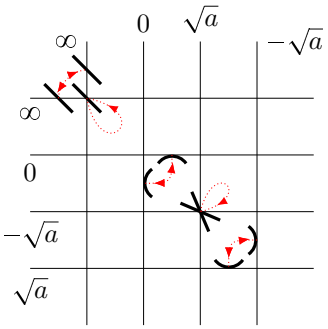


Figure 4.2: The curve $C_2$

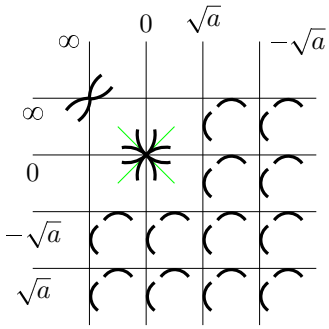


Figure 4.3: The curve $C_8$

Dotted arrows denote the action of the endomorphism $\pi$: blue ones if $\sqrt{2} \in \mathbb{F}_q$, violet ones if $\sqrt{2} \notin \mathbb{F}_q$, and red ones in both cases. Also, the green lines are two tangents to $C_8$ at $(0,0)$.

$$\begin{array}{ccccc} A_\pm & \xrightarrow{\varphi} & A_a & \xrightarrow{\psi} & A'_a \\ \rho\downarrow & & \rho\downarrow & & \downarrow\rho \\ A_\pm/[-1] & \xrightarrow{\overline{\varphi}} & A_a/[-1] & \xrightarrow{\overline{\psi}} & A'_a/[-1] \\ & & & \searrow^{\overline{\overline{\psi}}} & \\ pr\downarrow & & pr\downarrow & & \downarrow pr \\ \mathbb{P}^1\times\mathbb{P}^1 & \xrightarrow{\overline{\overline{\varphi}}} & \mathbb{P}^1\times\mathbb{P}^1 & & \mathbb{P}^1\times\mathbb{P}^1 \end{array}$$

Figure 4.4

$$\begin{array}{ccccc} H_1 & \xrightarrow{\varphi} & H_2 & \xrightarrow{\psi} & H_8 \\ \rho\downarrow & & \rho\downarrow & & \downarrow\rho \\ D_1 & \xrightarrow{\overline{\varphi}} & D_2 & \xrightarrow{\overline{\psi}} & D_8 \\ & & & \searrow^{\overline{\overline{\psi}}} & \\ pr\downarrow & & pr\downarrow & & \downarrow pr \\ C_1 & \xrightarrow{\overline{\overline{\varphi}}} & C_2 & & C_8 \end{array}$$

Figure 4.5

### 4.3.1 Proper $\mathbb{F}_q$-parametrization of the curve

Now we are going to parametrize the curve $C_8$. Note that $C_1$ has the $\pi$-invariant point $(-5/3\sqrt{a},\ 5/3\sqrt{a})$ and the projection from it gives:

$$pr_{C_1} : C_1 \dashrightarrow \mathbb{A}^1_x, \qquad x := \frac{3\sqrt{a}(x_0+x_1)}{3(x_0-x_1)+10\sqrt{a}}$$

such that

$$pr^{-1}_{C_1} : \mathbb{A}^1_x \dashrightarrow C_1, \qquad pr^{-1}_{C_1} = \begin{cases} x_0 := \dfrac{-5\sqrt{a}x+6a}{3(x-\sqrt{a})}, \\ x_1 := \dfrac{5\sqrt{a}x+6a}{3(x+\sqrt{a})}. \end{cases}$$

Substituting (with the help of Magma) the last formulas in the equation of $A_{\pm}/[-1]$, we obtain the $\mathbb{F}_q$-curve

$$D_1' \colon 3^6x^6y^2 + 2^6a^3x^6 - 3^7ax^4y^2 - 2^43^2a^4x^4 + 3^7a^2x^2y^2 + 3^4a^5x^2 - 3^6a^3y^2 \quad \subset \quad \mathbb{A}^2_{(x,y)}.$$

Thus there are birational isomorphisms

$$\chi := pr_{C_1} \times \mathrm{id}_y \colon D_1 \xrightarrow{\sim} D_1', \qquad \chi^{-1} = pr_{C_1}^{-1} \times \mathrm{id}_y \colon D_1' \xrightarrow{\sim} D_1.$$

Further, Magma allows to compute the anticanonical map from $D_1'$ to the $\mathbb{F}_q$-conic

$$Q \colon 2^6a^3u^2 + 3^6v^2 - 2^6a^4 \quad \subset \quad \mathbb{A}^2_{(u,v)}$$

given by the $\mathbb{F}_q$-formulas

$$\varphi_{-K} \colon D_1' \xrightarrow{\sim} Q, \qquad \varphi_{-K} = \begin{cases} u := x, \\ v := \dfrac{2^3a^3(3^2a - 2^3x^2)x}{3^6(x^2 - a)y} \end{cases}$$

such that

$$\varphi_{-K}^{-1} \colon Q \xrightarrow{\sim} D_1', \qquad \varphi_{-K}^{-1} = \begin{cases} x := u, \\ y := \dfrac{(2^3u^2 - 3^2a)uv}{2^3(u^2 - a)^2}. \end{cases}$$

Finally, the projection from the point $(2^3a^2/3^3, 0) \in Q(\mathbb{F}_q)$ has the form

$$pr_Q \colon Q \xrightarrow{\sim} \mathbb{A}^1_t, \qquad t := \frac{3^3v - 2^3a^2}{3^3u}$$

such that

$$pr_Q^{-1} \colon \mathbb{A}^1_t \xrightarrow{\sim} Q, \qquad pr_Q^{-1} = \begin{cases} u := \dfrac{-2^43^3a^2t}{2^6a^3 + 3^6t^2}, \\ v := \dfrac{2^3a^2(2^6a^3 - 3^6t^2)}{3^3(2^6a^3 + 3^6t^2)}. \end{cases}$$

Thus we obtain the $\mathbb{F}_q$-rational map

$$par := \overline{\overline{\psi}} \circ \overline{\varphi} \circ \chi^{-1} \circ \varphi_{-K}^{-1} \circ pr_Q^{-1} \colon \ \mathbb{A}^1_t \dashrightarrow C_8.$$

Magma allows to simplify its defining functions as follows:

$$par = \begin{cases} x_0 := \dfrac{(3^8t^2 + 2^6a^3)^2 g(t)}{2^{14}3^2a^4(3^7t^2 - 2^6a^3)^2 t}, \\ x_1 := \dfrac{(3^4t^2 + 2^6a^3)^2 g(t)}{2^8 3^6 a(3^5t^2 - 2^6a^3)^2 t^3}, \end{cases} \quad \text{where} \quad g(t) := t^2(3^{12}t^2 - 2^7 3^4 7a^3) + 2^{12}a^6.$$

It is easily seen that $g(t)$ has no multiple roots and the functions are in the reduced form, that is the numerators and denominators have no common roots. By [64, Theorem 4.21] we get

**Theorem 4.6.** *The map par (or, equivalently, $\overline{\overline{\psi}}|_{D_2}$) is birational.*

Another proof consists in applying the projection formula [70, §1.2] with respect to $\overline{\overline{\psi}}$. Interestingly, according to [64, Corollary 6.14] the curve $C_8$ is not polynomial, i.e., it cannot be parametrized by two polynomials (even over $\overline{\mathbb{F}_q}$). Finally, the inverse map $par^{-1}\colon C_8 \xrightarrow{\sim} \mathbb{A}^1_t$ and the maps $pr^{-1} \circ par\colon \mathbb{A}^1_t \xrightarrow{\sim} D_8, D_8'$ (or, equivalently, the functions $\pm\sqrt{af(x_0)f(x_1)} \in \mathbb{F}_q(t)$) can be also computed, but we do not write out them here for the sake of compactness (as above, see the Magma code [136]).

## 4.4 Remarks and conclusions

Let us keep a notation of previous paragraphs. First of all, we would like to deal with the case $\sqrt{a} \in \mathbb{F}_q$ (in fact, it is sufficient to take $a = 1$). Let $E'_-, E'_a$ be the quadratic $\mathbb{F}_q$-twists of $E_-, E_a$ respectively (by the $\mathbb{F}_{q^2}$-isomorphism $\sigma$) and

$$A'_\pm := E_+ \times E'_-, \qquad A'_a := E_a \times E'_a.$$

By means of

$$[1]\times\sigma\colon A'_\pm \xrightarrow{\simeq} A_\pm, \qquad [1]\times\sigma\colon A'_a \xrightarrow{\simeq} A_a$$

the morphisms $\varphi, \overline{\varphi}$ are identically transformed to

$$A'_\pm \to A'_a, \qquad A'_\pm/[-1] \to A'_a/[-1]$$

respectively, hence we save the notation. Finally, for $i \in \{1, 2\}$ consider the $\mathbb{F}_q$-curves

$$H'_i := ([1]\times\sigma^{-1})(H_i), \qquad D'_i := \rho(H'_i) = pr^{-1}(C_i).$$

Thus $D_2' = \overline{\varphi}(D_1')$ is a desired rational $\mathbb{F}_q$-curve on the Kummer surface of $A_a'$ and we obtain the commutative diagrams

$$\begin{array}{ccc} A'_{\pm} & \stackrel{\varphi}{\to} & A'_a \\ \rho\downarrow & & \downarrow\rho \\ A'_{\pm}/[-1] & \stackrel{\overline{\varphi}}{\to} & A'_a/[-1] \\ pr\downarrow & & \downarrow pr \\ \mathbb{P}^1\times\mathbb{P}^1 & \stackrel{\overline{\overline{\varphi}}}{\to} & \mathbb{P}^1\times\mathbb{P}^1 \end{array} \qquad \begin{array}{ccc} H_1' & \stackrel{\varphi}{\to} & H_2' \\ \rho\downarrow & & \downarrow\rho \\ D_1' & \stackrel{\overline{\varphi}}{\to} & D_2' \\ pr\downarrow & & \downarrow pr \\ C_1 & \stackrel{\overline{\overline{\varphi}}}{\to} & C_2 \end{array}$$

Now we return to the more interesting case $\sqrt{a} \notin \mathbb{F}_q$. In particular, under the condition $q \equiv 5 \pmod 8$ it is sufficient to take $a \in \{2, 8\}$, because it is known that the Legendre symbol

$$\left(\frac{2}{p}\right) = 2^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if} \quad p \equiv 1, 7 \pmod 8, \\ -1 & \text{if} \quad p \equiv 3, 5 \pmod 8, \end{cases} \qquad \left(\frac{2}{q}\right) = \begin{cases} 1 & \text{if} \quad 2 \mid \log_p(q), \\ \left(\frac{2}{p}\right) & \text{if} \quad 2 \nmid \log_p(q). \end{cases}$$

Fortunately, for $q \not\equiv 1 \pmod 8$ a square root in $\mathbb{F}_q$ can be computed by means of one exponentiation in $\mathbb{F}_q$ (see, e.g., [7, §5.1.7]), hence the simplified SWU method can be implemented quite efficiently.

It is time to clarify which sign of the square root $y = \sqrt{r}$ (for a quadratic residue $r \in \mathbb{F}_q^*$) should be chosen by default. Let $\mathbb{F}_q = \mathbb{F}_p(\gamma)$ and $y = \sum_{i=0}^{n-1} y_i\gamma^i \in \mathbb{F}_q^*$, where $0 \leqslant y_i < p$. If $i_0$ is the minimal index with $y_{i_0} \neq 0$, then we take $y$ such that the value from $\{y_{i_0}, p - y_{i_0}\}$ is even (or odd). Another way is to compare when the value is greater than $(p-1)/2$.

Let $U := \mathbb{P}^1 \backslash par^{-1}(Ram)$ and

$$h' \colon C_8(\mathbb{F}_q)\backslash Ram \to E_a(\mathbb{F}_q)\backslash E_a[2], \qquad (x_0, x_1) \mapsto \begin{cases} \big(x_0, \sqrt{f(x_0)}\big) & \text{if} \quad \sqrt{f(x_0)} \in \mathbb{F}_q, \\ \big(x_1, -\sqrt{f(x_1)}\big) & \text{if} \quad \sqrt{f(x_1)} \in \mathbb{F}_q. \end{cases}$$

Thus the parametrization $par \colon \mathbb{P}^1 \to C_8$ from §4.3.1 induces the hashing

$$h := h' \circ par \colon U(\mathbb{F}_q) \to E_a(\mathbb{F}_q).$$

Of course, we could extend $h$ to all the field $\mathbb{F}_q$, but let us simplify the paragraph, not dealing with the exceptional cases. The defining polynomial of $C_8$ is symmetric, hence both points $\pm h(t)$ are in the image of $h$. More precisely, it can be checked that $h\big(2^6a^3/(3^6t)\big) = -h(t)$. Finally, since the curve $C_8$ is of bidegree $(8, 8)$, for any point $P \in E_a(\mathbb{F}_q)$ it follows that $|h^{-1}(P)| \leqslant 8$.

**Theorem 4.7.** *We have the bounds*

$$\frac{q-54}{8} \leqslant |\mathrm{Im}(h)| \leqslant |E_a(\mathbb{F}_q)| - 2.$$

*Proof.* By the adjunction formula [1, Exercise V.1.3.a] arithmetic genus $p_a = 49$ for the curve $C_8 \subset \mathbb{P}^1 \times \mathbb{P}^1$, because a canonical divisor $K_{\mathbb{P}^1 \times \mathbb{P}^1}$ is of bidegree $-(2,2)$. Besides, for a point $P \in C_8(\mathbb{F}_q)$ consider the values

$$\alpha_P := \left|par^{-1}(P)(\mathbb{F}_q)\right|, \qquad \delta'_P := \begin{cases} 0 & \text{if} \quad \alpha_P = 0, \\ \alpha_P - 1, & \text{otherwise,} \end{cases}$$

and $\delta_P$ [1, Example V.3.9.3]. Using [137, Lemma 2.2], Theorem 4.6 and [1, Example V.3.9.2], we obtain the inequalities

$$\left|par\big(\mathbb{P}^1(\mathbb{F}_q)\big)\right| \;=\; q+1-\sum_{P \in C_8(\mathbb{F}_q)} \delta'_P \;\geqslant\; q+1-\sum_{P \in C_8(\mathbb{F}_q)} \delta_P \;\geqslant\; q+1-p_a \;=\; q-48.$$

Thus

$$\frac{q-54}{8} \leqslant \frac{\left|par\big(\mathbb{P}^1(\mathbb{F}_q)\big)\right| - \left|(C_8 \cap Ram)(\mathbb{F}_q)\right|}{8} \leqslant |\mathrm{Im}(h)|$$

and the upper bound is trivial. □

To be more precise the formula for $|E_a(\mathbb{F}_q)|$ is given in [7, Proposition 2.5], [138, Theorem 18.5]. The lower bound can be probably improved by the Chebotarev density theorem (in the function field case) as well as this is done for some other hashings (see [139, §3.2]).

We say that an arbitrary map has an *algebraic* (*worst-case*) *complexity*

$$n_S S + n_{M_c} M_c + n_M M + n_I I + n_{QRT} QRT + n_{SR} SR$$

if for all arguments it can be computed by means of (at most) $n_S$ squarings, $n_{M_c}$ multiplications by a constant $c \in \mathbb{F}_q$, $n_M$ general ones (with different non-constant multiples), $n_I$ inversions, $n_{QRT}$ quadratic residuosity tests, and $n_{SR}$ square roots, where all operations are in $\mathbb{F}_q$. Additions and subtractions in $\mathbb{F}_q$ are not considered, because they are very easy to compute. We also do not take account (in $n_{M_c}$) for multiplications by a constant $c \in \mathbb{F}_p$ such that $c \pmod p \leqslant 7$, because they are not more difficult than few additions. Implementation details of the operations mentioned see, for example, in [4, Chapter II], [7, §5.1].

**Lemma 4.8.** *The hashing $h$ has an algebraic complexity*

$$7S + 2M_c + 10M + 2I + QRT + SR.$$

*Proof.* It is easily checked that the functions $g(t), x_0(t), x_1(t)$ forming the parametrization *par* have an algebraic complexity

$$S + M, \qquad 2S + M_c + 3M + I, \qquad 2S + M_c + 4M + I$$

respectively (the value $t^2$ is supposed to be known before calculating $x_0(t), x_1(t)$). In addition to $f(x_0)$ in the worst case (i.e., if $\sqrt{f(x_0)} \notin \mathbb{F}_q$) we must also compute $f(x_1)$. Each of these two substitutions is accomplished by $S + M$ operations. We emphasize once again that the quadratic residuosity test is unique. It remains to extract one square root $\sqrt{f(x_0)}$ or $\sqrt{f(x_1)}$. Thus we obtain the desired algebraic complexity for $h$. □

In pairing-based cryptography non-supersingular (i.e., for $p \equiv 1 \pmod 3$) elliptic $\mathbb{F}_q$-curves $E_b\colon y^2 = x^3 - b$ of $j$-invariant 0 are only used in practice at the moment [56, Table 1]. Thus it is tempting to generalize the simplified SWU method to them. More precisely, there is the following

**Problem 4.9.** *Let $E_b$ be any elliptic $\mathbb{F}_q$-curve of $j = 0$ and $E'_b$ be its quadratic $\mathbb{F}_q$-twist. How to explicitly construct a rational $\mathbb{F}_q$-curve $D$ on the Kummer surface $K'_b$ of the direct product $E_b \times E'_b$ such that bidegree of the image $C := pr(D) \subset \mathbb{P}^1 \times \mathbb{P}^1$ does not depend on $\mathbb{F}_q$?*

Unfortunately, the approach of this work does not allow to resolve this problem, because in the case $\sqrt[3]{b} \notin \mathbb{F}_q$ it seems that there is no natural $\mathbb{F}_{q^2}$-isogeny from some elliptic curve of $j \neq 0$, that is an ascending $\mathbb{F}_{q^2}$-isogeny to $E_b$.

# Chapter 5

# Finiteness of the Mordell–Weil groups of some elliptic $\mathbb{F}_q$-surfaces of $j$-invariant 0

The theory of elliptic surfaces over $\mathbb{P}^1$ (i.e., elliptic curves over the function field in one variable $t$) is well represented, for example, in [90] (and in [132] for the case of a finite field $\mathbb{F}_q$). By abuse of notation, we will denote an elliptic $\mathbb{F}_q$-surface $S$ and its generic $\mathbb{F}_q(t)$-fiber by the same letter. Besides, let us identify $S$ with its (unique) Kodaira–Néron model.

**Theorem 5.1.** *The Mordell–Weil group* $\mathrm{MW}(\mathcal{K}_6)$ *is isomorphic to* $\mathbb{Z}/3$.

*Proof.* First of all, we transform $\mathcal{K}_6$ (with $\mathcal{O}$ as the zero section) to its globally minimal [90, §8.2] Weierstrass form

$$\mathcal{E}\colon y^2 = x^3 + \left(\frac{t^6 - c}{2b^2}\right)^2$$

by means of the $\mathbb{F}_q(t)$-isomorphism

$$\varphi\colon \mathcal{K}_6 \xrightarrow{\sim} \mathcal{E}, \qquad \varphi^{-1}\colon \mathcal{E} \xrightarrow{\sim} \mathcal{K}_6,$$

$$\varphi = \begin{cases} x := \dfrac{t^6 - c}{b(x_0\sqrt[3]{c} - t^2 x_1)}, \\ y := \dfrac{\sqrt{-3}(x_0\sqrt[3]{c} + t^2 x_1)}{-2b} \cdot x, \end{cases} \qquad \varphi^{-1} = \begin{cases} x_0 := \dfrac{2b^2 y - \sqrt{-3}(t^6 - c)}{-2\sqrt{-3} \cdot b\sqrt[3]{c} \cdot x}, \\ x_1 := \dfrac{2b^2 y + \sqrt{-3}(t^6 - c)}{-2\sqrt{-3} \cdot bt^2 \cdot x}. \end{cases}$$

These formulas are verified in [140].

Also, for $j \in \mathbb{Z}/6$ consider the elliptic surfaces given by globally minimal Weierstrass forms

$$\mathcal{E}_j \colon y^2 = x^3 + t^j \left(\frac{t-c}{2b^2}\right)^2.$$

Note that $\mathcal{E}_j$ is a Weierstrass form for $\mathcal{E}_{4-j}$ minimal at $t = \infty$. By [90, §4.10] the surfaces $\mathcal{E}_0, \mathcal{E}_1, \mathcal{E}_2$ are geometrically rational, but $\mathcal{E}_5$ is, in turn, $K3$ one. Besides, according to [141, Lemma 2.1] we have the following identities between Mordell–Weil ranks:

$$\operatorname{rk}(\mathcal{E}) = \sum_{j=0}^{5} \operatorname{rk}(\mathcal{E}_j), \qquad \operatorname{rk}\big(\bar{\mathcal{E}}\big) = \sum_{j=0}^{5} \operatorname{rk}\big(\bar{\mathcal{E}}_j\big).$$

Let $\rho\big(\bar{\mathcal{E}}_j\big)$ be the Picard $\overline{\mathbb{F}_q}$-number of $\mathcal{E}_j$. Using Tate's algorithm [90, §4.2] (also see [140]), the main theorem of [142], and the Shioda–Tate formula [132, §3.5], we immediately obtain all cells of Table 5.1 except for $\operatorname{MW}\big(\bar{\mathcal{E}}_5\big)$, $\rho\big(\bar{\mathcal{E}}_5\big)$. Since $\operatorname{rk}\big(\bar{\mathcal{E}}\big) = 6$, we also get $\operatorname{rk}\big(\bar{\mathcal{E}}_5\big) = 0$ and, as a result, $\mathcal{E}_5$ is a singular $K3$ surface. Moreover, $\mathcal{E}_5$ is so-called *extremal* elliptic surface, hence by the row 297 of [143, Table 2] we have $\operatorname{MW}\big(\bar{\mathcal{E}}_5\big)_{tor} = 0$. Thus Table 5.1 is completely filled.

It remains to prove that $\operatorname{rk}(\mathcal{E}_1) = \operatorname{rk}(\mathcal{E}_2) = 0$. For $k \in \mathbb{Z}/3$ consider the sections

$$P_k := \left(\frac{\omega^k(t-c)}{-b\sqrt[3]{4b}},\ \frac{\sqrt{c}(t-c)}{2b^2}\right), \qquad Q_k := \left(\frac{\omega^k \sqrt[3]{c}\cdot t}{b\sqrt[3]{b}},\ \frac{t^2+ct}{2b^2}\right)$$

of $\mathcal{E}_1$ and $\mathcal{E}_2$ respectively. Since each triple have the same $y$-coordinate, we obviously get

$$P_0 + P_1 + P_2 = \mathcal{O}, \qquad Q_0 + Q_1 + Q_2 = \mathcal{O}.$$

The canonical height matrices

$$\hat{h}_{L_1} = \begin{pmatrix} 1/3 & -1/6 \\ -1/6 & 1/3 \end{pmatrix}, \qquad \hat{h}_{L_2} = \begin{pmatrix} 2/3 & -1/3 \\ -1/3 & 2/3 \end{pmatrix}$$

on the lattices $L_1 := \langle P_0, P_1 \rangle$ and $L_2 := \langle Q_0, Q_1 \rangle$ are not hard to derive, looking at [144, Theorem 8.6]. Instead, we use in [140] one of Magma functions in order to reduce the amount of computations. The given matrices are non-degenerate, hence, in particular, the sections $P_0, P_1$ (resp. $Q_0, Q_1$) are linearly independent.

Besides, we have the following possible Frobenius actions Fr on $L_1$:

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$$

if the third power residue symbol $\left(\frac{4b}{q}\right)_3 = 1, \omega, \omega^2$ respectively. In turn, the Frobenius Fr on $L_2$ is given by one of matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

if $\left(\frac{b}{q}\right)_3 = 1, \omega, \omega^2$ respectively. However the first case is ruled out by our assumption. In all remaining cases,

$$\mathrm{rk}(\mathcal{E}_1) = \mathrm{rk}\big(L_1^{\mathrm{Fr}}\big) = 0, \qquad \mathrm{rk}(\mathcal{E}_2) = \mathrm{rk}\big(L_2^{\mathrm{Fr}}\big) = 0,$$

where $L_1^{\mathrm{Fr}}$, $L_2^{\mathrm{Fr}}$ are the sublattices of Fr-invariants. Thus the theorem is proved. □

| $\mathcal{E}_j$ | singular fibers | lattice T | $\mathrm{MW}(\bar{\mathcal{E}}_j)$ | $\rho(\bar{\mathcal{E}}_j)$ |
|---|---|---|---|---|
| $\mathcal{E}_0$ | IV, IV* | $\mathrm{A}_2 \oplus \mathrm{E}_6$ | $\mathbb{Z}/3$ | 10 |
| $\mathcal{E}_1$ | II, IV, $\mathrm{I}_0^*$ | $\mathrm{A}_2 \oplus \mathrm{D}_4$ | $\mathbb{Z}^2$ | |
| $\mathcal{E}_2$ | 3·IV | $\mathrm{A}_2^{\oplus 3}$ | $\mathbb{Z}^2 \oplus \mathbb{Z}/3$ | |
| $\mathcal{E}_5$ | IV, 2·II* | $\mathrm{A}_2 \oplus \mathrm{E}_8^{\oplus 2}$ | 0 | 20 |

Table 5.1: The surfaces $\mathcal{E}_j$, where $\mathcal{E}_0 \simeq_{\mathbb{F}_q(t)} \mathcal{E}_4$, $\mathcal{E}_1 \simeq_{\mathbb{F}_q(t)} \mathcal{E}_3$

**Remark 5.2.** *As we see in the proof, if* $\left(\frac{b}{q}\right)_3 = 1$, *then* $L_2^{\mathrm{Fr}} = L_2$. *At the same time, since* $\mathrm{rk}\big(L_1^{\mathrm{Fr}}\big) = 0$ *as before, we have* $\mathrm{rk}(\mathcal{K}_6) = 2$ *in this case.*

Since the base change $t \mapsto t^3$ obviously transforms an affine (i.e., $X_2 \neq 0$) $\mathbb{F}_q$-section of $\mathcal{K}_2$ to that of $\mathcal{K}_6$, we also establish

**Corollary 5.3.** *The elliptic* $\mathbb{F}_q$*-surface* $\mathcal{K}_2$ *is not Jacobian, that is it has no an* $\mathbb{F}_q$*-section.*

## 5.1 Further questions

Let us shortly discuss what other Jacobian elliptic $\mathbb{F}_q$-fibrations can be potentially used to construct a rational $\mathbb{F}_q$-curve on the Kummer surface $\mathcal{K}_2$. First, it is very natural to formulate

**Problem 5.4.** *Is there a number* $n \in \mathbb{N}$ *such that the Mordell–Weil group* $\mathrm{MW}(\mathcal{K}_{6n})$ *of the elliptic surface*

$$\mathcal{K}_{6n} \colon (x_1^3 - b)t^{6n} = c(x_0^3 - b) \quad \subset \quad \mathbb{A}^3_{(x_0,x_1,t)}$$

(*with* $(t^{2n} : \sqrt[3]{c} : 0)$ *as the zero section*) *is of non-zero rank?*

The base change $t \mapsto t^{3n}$ allows to transfer rational $\mathbb{F}_q$-curves on $\mathcal{K}_{6n}$ to rational ones on $\mathcal{K}_2$. As well as for $\mathcal{K}_6$ we verify in [140] that

$$y^2 = x^3 + \left(\frac{t^{6n} - c}{2b^2}\right)^2$$

is a globally minimal Weierstrass form for $\mathcal{K}_{6n}$. Therefore the arithmetic genus of its Kodaira–Néron model is equal to $2n$ and hence for $n > 1$ we deal with a surface of Kodaira dimension one.

We also can consider elliptic fibrations immediately on $\mathcal{K}_2$. All of them are classified (without explicit formulas) in [145, Table 1.3] over an algebraically closed field. This is a good question which ones are Jacobian $\mathbb{F}_q$-fibrations. Finally, one may wonder about the existence of another dominant rational maps from (elliptic) $K3$ surfaces onto $\mathcal{K}_2$. This topic is highlighted, for example, in [146, §3].

# Chapter 6

# Hashing to elliptic $\mathbb{F}_q$-curves of $j$-invariant 0 having a vertical $\mathbb{F}_{q^2}$-isogeny of small degree

Let $\mathbb{F}_p$ be a prime finite field ($p > 5$) and $E_b\colon y_0^2 = x_0^3 + b$ be an elliptic $\mathbb{F}_p$-curve of $j$-invariant 0. For definiteness, we will suppose that $E_b$ is an ordinary curve. According to [6, Example V.4.4] this condition means that $p \equiv 1 \pmod 3$, i.e., $\omega := \sqrt[3]{1} \in \mathbb{F}_p$, where $\omega \neq 1$. Also, for $c \in \mathbb{F}_p^*$ (such that $\sqrt{c} \notin \mathbb{F}_p$) let $E'_b\colon y_1^2 = c(x_1^3 + b)$ be the (unique) quadratic $\mathbb{F}_p$-twist of $E_b$ and

$$K'_b\colon y^2 = c(x_0^3 + b)(x_1^3 + b) \quad \subset \quad \mathbb{A}^3_{(x_0,x_1,y)}.$$

be the Kummer surface of the direct product $E_b \times E'_b$.

Let us give a strict mathematical definition. *Simplified SWU hashing* is any non-constant rational $\mathbb{F}_p$-map $h_{SWU}\colon \mathbb{A}^1 \dashrightarrow K'_b$, that is an $\mathbb{F}_p$-parametrization of any rational curve on $K'_b$. It is known that $h_{SWU}$ induces a (usual) hashing $h\colon \mathbb{F}_p \to E_b(\mathbb{F}_p)$ (a constant-time implementation is represented in §6.1). We know from Chapter 5 that finding $h_{SWU}$ is generally considered a difficult task only if $\sqrt[3]{b} \notin \mathbb{F}_p$, that is $2 \nmid |E_b(\mathbb{F}_p)|$. Therefore for definiteness, it is further assumed that this condition is met.

The quotient by the point $(0, \sqrt{b}) \in E_b(\mathbb{F}_{p^2})$ always gives the (unique) $\mathbb{F}_p$-endomorphism of degree 3 on $E_b$. If $\sqrt[3]{4b} \in \mathbb{F}_p$, then the curve $E_b$ also has a *vertical* $\mathbb{F}_p$*-isogeny* (see its definition in [9, Proposition 36]) of degree 3 onto the curve of $j = -2^{15}5^33$ [147, Table 1], since the 3-division polynomial of $E_b$ equals $\psi_3(x) = 3x(x^3 + 4b)$. In this case, the problem of constructing $h_{SWU}$ is obviously reduced to the analogous problem already solved for $j \neq 0$ (see, e.g, [78]). In particular, this reduction applies to the curve BN256 from [148], earlier quite popular in the industry. Thus we will assume that $\sqrt[3]{4b} \notin \mathbb{F}_p$.

As we know from Chapter 4, to construct $h_{SWU}$ it is sufficient that the curve $E_b$ has a vertical $\mathbb{F}_{p^2}$-isogeny. Moreover, if its degree is lower, then the computation of $h_{SWU}$ (and hence $h$) is more efficient in practice. This chapter is devoted to the case of degree 5.

Let $t_1$ be the $\mathbb{F}_p$-trace and $D_1 = t_1^2 - 4p$ be the $\mathbb{F}_p$-discriminant of $E_b$. Since the $\mathbb{F}_{p^2}$-trace $t_2 = t_1^2 - 2p$, then the $\mathbb{F}_{p^2}$-discriminant $D_2 = t_2^2 - 4p^2 = t_1^2 D_1$. According to [9, Proposition 37] the curve $E_b$ has a vertical $\mathbb{F}_{p^2}$-isogeny of degree 5, undefined over $\mathbb{F}_p$, (we denote it by $\phi_+ \colon E_+ \to E_b$) if and only if $5 \mid t_1$. Moreover, in this case $E_b$ does not have $\mathbb{F}_p$-isogenies of degree 5, because 5 cannot simultaneously divide $t_1$ and $D_1$. By the way, $E_b$ never has horizontal isogenies (or, equivalently for $j = 0$, endomorphisms) of degree 5. Finally, it is easy to check that quite popular Barreto–Naehrig (BN) curves [7, Example 4.2] cannot have $\mathbb{F}_p$-isogenies of degree 5 at all.

The 5-division polynomial of the curve $E_b$ equals

$$\psi_5(x) = f_5(x^3), \qquad \text{where} \qquad f_5(z) := 5z^4 + 380bz^3 - 240b^2z^2 - 1600b^3z - 256b^4.$$

We get that any point of order 5 on $E_b$ has the form $P = \left(\sqrt[3]{z_i}, \sqrt{z_i + b}\right)$, where $z_i \in \mathbb{F}_{p^4}^*$ $(0 \leqslant i \leqslant 3)$ are roots of the polynomial $f_5$. If $P$ generates an $\mathbb{F}_{p^2}$-invariant subgroup (of the form $G = \{\mathcal{O},\ \pm P,\ \pm 2P\}$), then obviously $\sqrt[3]{z_i} \in \mathbb{F}_{p^4}^*$ and $P \in E_b(\mathbb{F}_{p^8})$. Using Ferrari's method for expressing the roots $z_i$ in radicals, it is easy to show that under the condition $\sqrt{5} \notin \mathbb{F}_p$ (in particular, if $5 \mid t_1$, this is true for all BN curves) we have $z_i \notin \mathbb{F}_{p^2}$. Therefore $G$ is not $\mathbb{F}_p$-invariant and the norm of $z_i$ equals $\mathrm{N}_{\mathbb{F}_{p^4}/\mathbb{F}_p}(z_i) = -2^8 b^4/5$. As a consequence, $\sqrt[3]{4b/5} \in \mathbb{F}_p$ and hence $\sqrt[3]{5} \notin \mathbb{F}_p$. The case $\sqrt{5} \in \mathbb{F}_p$ is expected to be simpler, hence we omit it.

In fact, it is enough to put $b = 10$. Indeed, since $\sqrt[3]{b/10} \in \mathbb{F}_p$, the curves $E_b$, $E_{10}$ are isomorphic at most over $\mathbb{F}_{p^2}$. Therefore the surfaces $K_b'$, $K_{10}'$ are isomorphic over $\mathbb{F}_p$.

Let $E_-$ be the curve $\mathbb{F}_p$-conjugate to $E_+$, that is $j(E_-) = j(E_+)^p$. Similarly, $\varphi_- \colon E_- \to E_b$ is the isogeny $\mathbb{F}_p$-conjugate to $\varphi_+$, that is $\varphi_- = \mathrm{Fr} \circ \varphi_+ \circ \mathrm{Fr}^{-1}$, where Fr is the Frobenius endomorphism. An explicit form of the dual isogenies $\widehat{\varphi_\pm} \colon E_b \to E_\pm$ and then isogenies $\varphi_\pm$ can be easily found, using Velu's formulas [9, Proposition 38]. Besides, let us clarify Figure 6.1. We denote by $K_\pm$ (resp. $K_b$) the Kummer surface of the direct product $E_+ \times E_-$ (resp. $E_b \times E_b$). In addition, $\varphi := (\varphi_+, \varphi_-)$, the isogeny $\psi$ is defined in §4.1, and $\rho$ is the natural quotient map. Finally, $\overline{\varphi}$ (resp. $\overline{\psi}$) is the restriction of $\varphi$ (resp. $\psi$) to the Kummer surfaces.

Due to [147, Table 2], by substituting 0 in the *modular polynomial* [149, Exercise 2.18] of level 5, we obtain

$$\Phi_5(0, j) = H_D(j)^3, \qquad \text{where} \qquad H_D(j) = j^2 + 654403829760 \cdot j + 5209253090426880$$

$$\begin{array}{ccccc} E_+ \times E_- & \stackrel{\varphi}{\to} & E_b \times E_b & \stackrel{\psi}{\to} & E_b \times E'_b \\ \rho \downarrow & & \rho \downarrow & & \downarrow \rho \\ K_\pm & \stackrel{\overline{\varphi}}{\to} & K_b & \stackrel{\overline{\psi}}{\to} & K'_b \end{array}$$

Figure 6.1

is the *Hilbert class polynomial* [149, §II.6] of discriminant $D = -5^2 3$. Its roots equal

$$j_\pm := j(E_\pm) = \pm 146329141248 \cdot \sqrt{5} - 327201914880.$$

The ideal class group [9, Proposition 51] of the field $\mathbb{Q}(\sqrt{5})$ is known to be trivial, that is its integer ring $\mathbb{Z}[(1+\sqrt{5})/2]$ is a unique factorization domain. Therefore the curves $E_\pm$, considered over $\mathbb{Q}(\sqrt{5})$, have a *global minimal model* [150]. It turns out that the latter is a short Weierstrass form, for instance

$$E_\pm \colon y^2 = x^3 + (\pm 540\sqrt{5} - 1500)x - (\pm 12600\sqrt{5} - 26050),$$

whose the discriminant is factored into prime elements as follows:

$$\Delta(E_\pm) = -2^6 3^3 (\pm 72\sqrt{5} + 161)(\sqrt{5})^8.$$

Using the computer algebra system Magma, we obtain in [151] a non-trivial map $\chi \colon \mathbb{A}^1 \dashrightarrow K_\pm$ invariant under the "twisted" Frobenius endomorphism from §4.1. The arguments given when finding it are almost the same as those of §4.3.1. Thus we have the map

$$h_{SWU} := \overline{\psi} \circ \overline{\varphi} \circ \chi = \big(x_0(t), x_1(t), y(t)\big),$$

which is also explicitly written out in [151]. Here $x_0(t), x_1(t)$ are rational $\mathbb{F}_p$-functions of the variable $t$ of degree 20 and $y(t)$ is that of degree 60. An explanation of why $h_{SWU}$ is defined over $\mathbb{F}_p$ is given in §4.1. Finally, using Theorem 4.2.1 and [64, §6.1.2], one can easily check that it is birational with its own image.

Let's summarize the main result of the chapter.

**Theorem 6.1.** *If an ordinary elliptic $\mathbb{F}_p$-curve $E_b$ has an $\mathbb{F}_{p^2}$-isogeny of degree 5, then (except for a finite number of $p$) there is a simplified SWU hashing $h_{SWU} \colon \mathbb{A}^1 \dashrightarrow K'_b$. Moreover, the latter can be found explicitly.*

According to [147, Tables 1, 2] there are exactly 5 non-maximal (i.e., $\subsetneq \mathbb{Z}[\omega]$) orders of the quadratic field $\mathbb{Q}(\sqrt{-3})$, having class number 1 or 2. Their conductors are 2, 3 and 4, 5, 7 respectively. Thus there remains only the case of a vertical $\mathbb{F}_{p^2}$-isogeny of degree 7 to (from) $E_b$, for which, apparently, it is possible to construct

$h_{SWU}$ in a similar way, carrying out reasoning regardless of $p$, that is over a number field.

Finally, we emphasize that all the above arguments remain valid for an elliptic curve $E_b$ over any finite field $\mathbb{F}_q$ of characteristic $p$ such that $2,3 \nmid \log_p(q)$ and $p \equiv 1 \pmod 3$. In turn, we do not expect significant obstacles to extend Theorem 6.1 if at least one of the last restrictions does not hold.

## 6.1 Simplified SWU hashing in constant time

We would like to explain how a simplified SWU hashing $h_{SWU}\colon \mathbb{A}^1 \dashrightarrow K'_b$ gives a (usual) hashing $h\colon \mathbb{F}_q \to E_b(\mathbb{F}_q)$. In fact, any elliptic curve of $j \neq 1728$ can be next considered instead of $E_b$. In practice, one almost always takes $q \equiv 3 \pmod 4$ (i.e., $\sqrt{-1} \notin \mathbb{F}_q$). Let $f_i := x_i^3 + b$ and $y := y_0 y_1$. Then the Kummer surface can be taken in the form $K'_b\colon y^2 = -f_0 f_1 \subset \mathbb{A}^3_{(x_0,x_1,y)}$. We denote by $U$ and $V$ respectively the domain of definition and the image for $h_{SWU}$. Also, let $\theta := f_0^{(q+1)/4}$. Consider the auxiliary map

$$h'\colon V(\mathbb{F}_q) \to E_b(\mathbb{F}_q), \qquad (x_0,x_1,y) \mapsto \begin{cases} (x_0,\theta) & \text{if} & \theta^2 = f_0, \\ (x_1, y/\theta) & \text{otherwise, i.e.,} & \theta^2 = -f_0. \end{cases}$$

Since

$$\theta^2 = f_0^{(q+1)/2} = f_0^{(q-1)/2} \cdot f_0 = \pm f_0,$$

this map is well defined everywhere on $V(\mathbb{F}_q)$. We can thus put

$$h := h' \circ h_{SWU}\colon U(\mathbb{F}_q) \to E_b(\mathbb{F}_q).$$

The set $\mathbb{F}_q \backslash U(\mathbb{F}_q)$ containing only $\mathbb{F}_q$-roots of the denominators of the functions $x_0(t), x_1(t), y(t)$ has insignificant cardinality ($\leqslant \deg(x_0) + \deg(x_1) + \deg(y) = 100$). Therefore, if necessary, the value of $h$ on its elements can be specified manually.

We emphasize that in the definition of $h'$ the Legendre symbol $\left(\frac{\cdot}{q}\right)$ (in other words, a quadratic residuosity test) in the field $\mathbb{F}_q$ does not appear. In turn, the element $\theta$ can be calculated without the inversion operation in $\mathbb{F}_q$ even if the function $x_0(t)$ is not polynomial (see [78, §4.2]). Therefore, by returning the value of $h$ in (weighted) projective coordinates, we entirely avoid inversions. Thus the hashing $h$ is *constant-time*, that is the computation time of its value is independent of an input argument.

The latter circumstance is considered a great advantage over the (universal) *SWU hashing* [7, §8.3.4, §8.4.2], which, on the contrary, generally requires the computation of two Legendre symbols. The point is that time-constant implementations protect cryptographic protocols against timing attacks [7, §8.2.2, §12.1.1]. And the operations $\left(\frac{\gamma}{q}\right)$, $\gamma^{-1}$ (for $\gamma \in \mathbb{F}_q^*$) are possible sources of such attacks.

Note that computing the Legendre symbol in $\mathbb{F}_q$ reduces to the same task in $\mathbb{F}_p$ using the obvious equality $\left(\frac{\gamma}{q}\right) = \left(\frac{\mathrm{N}(\gamma)}{p}\right)$, where $\mathrm{N}(\gamma)$ is the norm of $\gamma$ with respect to the extension $\mathbb{F}_q/\mathbb{F}_p$. There are two common methods for computing the Legendre symbol in $\mathbb{F}_p$. One uses Euler's criterion $\left(\frac{\gamma}{p}\right) = \gamma^{(p-1)/2}$ (for $\gamma \in \mathbb{F}_p^*$), but requires the very inefficient exponentiation operation in $\mathbb{F}_p$. The second is based on Gauss's quadratic reciprocity law $\left(\frac{\gamma}{\delta}\right)\left(\frac{\delta}{\gamma}\right) = (-1)^{(\gamma-1)(\delta-1)/4}$ for the Jacobi symbol (with odd $\gamma, \delta \in \mathbb{Z}$). This method is much more efficient, but difficult to implement in constant time. Identical conclusions are also made in [7, §2.2.9, §8.4.2].

In fact, the hashing $h\colon \mathbb{F}_q \to E_a(\mathbb{F}_q)$ (proposed in §4.4) to an elliptic $\mathbb{F}_q$-curve $E_a\colon y^2 = x^3 - ax$ (where $\sqrt{a} \notin \mathbb{F}_q$) of $j$-invariant 1728 can also be made constant-time. Let $q \equiv 1 \pmod 4$ (or, equivalently, $i := \sqrt{-1} \in \mathbb{F}_q$) and $q \not\equiv 1 \pmod 8$. In other words, $q \equiv 5 \pmod 8$. The first condition is necessary for the curve $E_a$ to be ordinary. And second is sufficient to implement the square root extraction in $\mathbb{F}_q$ by means of one exponentiation in $\mathbb{F}_q$. As it is easy to see, under the given conditions we have $\sqrt{i} \notin \mathbb{F}_q$.

Let $h_{SWU}\colon \mathbb{A}^1 \dashrightarrow K'_a$ be the simplified SWU hashing built in §4.3.1. We will assume that the Kummer surface is given in the form $K'_a\colon y^2 = if_0f_1 \subset \mathbb{A}^3_{(x_0,x_1,y)}$, where $f_i = x_i^3 - ax_i$. As above, $U$ and $V$ are respectively the domain of definition and the image for $h_{SWU}$. Also, let $\theta := f_0^{(q+3)/8}$. Consider the auxiliary map

$$h'\colon V(\mathbb{F}_q) \to E_a(\mathbb{F}_q), \qquad (x_0, x_1, y) \mapsto \begin{cases} \big(x_0, \theta\big) & \text{if} & \theta^2 = f_0, \\ \big(x_0, i\theta\big) & \text{if} & \theta^2 = -f_0, \\ \big(x_1, y/\theta\big) & \text{if} & \theta^2 = if_0, \\ \big(x_1, y/(i\theta)\big) & \text{otherwise, i.e.,} & \theta^2 = -if_0. \end{cases}$$

Since

$$\theta^2 = f_0^{(q+3)/4} = f_0^{(q-1)/4} \cdot f_0 \ \in \ \{\pm f_0, \pm i f_0\},$$

this map is well defined everywhere on $V(\mathbb{F}_q)$. Besides, the element $\theta$ can be computed without the inversion operation in $\mathbb{F}_q$. Indeed,

$$(u/v)^{(q+3)/8} = u^{(q+3)/8} v^{(7q-11)/8} = uv^3 (uv^7)^{(q-5)/8}$$

for any $u, v \in \mathbb{F}_q^*$. Thus we obtain the constant-time hashing

$$h = h' \circ h_{SWU}\colon U(\mathbb{F}_q) \to E_a(\mathbb{F}_q).$$

As before, the set $\mathbb{F}_q \backslash U(\mathbb{F}_q)$ can be processed separately.

# Part III

# Non-split toric codes

# Chapter 7

# Theory building in the smooth case

## 7.1 Toric geometry over finite fields

### 7.1.1 Algebraic tori

Let $\mathbb{F}_q$ be a finite field of order $q$ and characteristic $p$, $\overline{\mathbb{F}_q}$ be its algebraic closure, and $\mathbb{G}_m = \overline{\mathbb{F}_q}\backslash\{0\}$. By definition, an algebraic group $T$ over $\mathbb{F}_q$ is said to be an *algebraic torus* of dimension $d$ if there is an isomorphism of algebraic varieties $\phi\colon \mathbb{G}_m^d \xrightarrow{\sim} T$ defined over some extension $\mathbb{F}_{q^e}$. We can suppose $\phi$ to be an isomorphism in the category of algebraic groups [152, Theorem 7]. If such $e$ is minimal, then $\mathbb{F}_{q^e}$ is called the *splitting field* of the torus $T$. We call $T$ *split* if $e = 1$. Note that in the case of a cyclic group $T(\mathbb{F}_q)$ its order divides $q^e - 1$.

Let $x \in \mathbb{G}_m^d$, $m \in \mathbb{Z}^d$, and $\Phi \in \mathrm{GL}(d, \mathbb{Z})$. Throughout the chapter we stick to the notation

$$x^m = x_1^{m_1} \cdot \ldots \cdot x_d^{m_d}, \qquad \Phi(x) = \left(x^{\Phi_{\square,1}}, \cdots, x^{\Phi_{\square,d}}\right),$$

where $\Phi_{\square,j}$ is the $j$-th column of $\Phi$. Besides, we assume that $\Phi$ acts on $m$ from the left, that is $\Phi(m) = \Phi m$.

For a given $T$ consider its *lattices of characters* $M = \mathrm{Hom}_{\overline{\mathbb{F}_q}}(T, \mathbb{G}_m)$ and *cocharacters* $N = M^*$ with Frobenius actions $\Phi$, $\Phi^t \in \mathrm{GL}(d, \mathbb{Z})$ respectively. We recall that these matrices are conjugate in $\mathrm{GL}(d, \mathbb{Z})$. The order of $\Phi$ (i.e., $\Phi^t$) is equal to $e$, hence all eigenvalues of $\Phi$ (i.e., $\Phi^t$) are contained in $\mu_e = \{\zeta \in \overline{\mathbb{F}_q} \mid \zeta^e = 1\}$. *Rank* $r$ of $T$ is, by definition, rank of the invariant sublattice $M^\Phi$ (i.e., $N^{\Phi^t}$). The torus $T$ is called *isotropic* if $r > 0$, that is if it has non-trivial $\mathbb{F}_q$-(co)characters. Otherwise, $T$ is called *anisotropic*.

**Theorem 7.1** ([153, §2.1.7])**.** *The following properties are equivalent:*

1. *a torus $T$ is split,*

2. $r = d$,

3. *all (co)characters of* $T$ *are defined over* $\mathbb{F}_q$,

4. *all eigenvalues of* $\Phi$ *are equal to* 1.

**Theorem 7.2** ([152, §1]). *The map* $T \mapsto \Phi$ *is a bijection between the set of* $d$*-dimensional* $\mathbb{F}_q$*-tori split over* $\mathbb{F}_{q^e}$ *and that of matrices (up to a conjugation) from* $\mathrm{GL}(d,\mathbb{Z})$ *of order* $e$*. More precisely, under the inverse map a matrix* $\Phi$ *corresponds to the geometric quotient* $T_\Phi = \mathbb{G}_m^d/\Phi$.

**Theorem 7.3** ([152, §2]). *For a fixed* $d$ *there is only a finite (up to a conjugation) number of finite subgroups in* $\mathrm{GL}(d,\mathbb{Z})$*. In particular, there is only a finite number of* $d$*-dimensional* $\mathbb{F}_q$*-tori.*

**Theorem 7.4** ([98, §9.2], [153, §2.1.7]).

1. *A torus* $T$ *has the unique maximal split (resp. anisotropic)* $\mathbb{F}_q$*-subtorus* $T_s$ *(resp.* $T_a$*).*

2. *Moreover,* $T_sT_a = T$ *and* $|T_s \cap T_a| < \infty$*. In other words, the map*

$$T_s \times T_a \to T, \qquad (P_s, P_a) \mapsto P_s \cdot P_a$$

*is an* $\mathbb{F}_q$*-isogeny. In particular,*

$$|T(\mathbb{F}_q)| = (q-1)^r \cdot |T_a(\mathbb{F}_q)|.$$

3. *The tori* $T_s$ *and* $T_a$ *correspond to the lattices* $M^\Phi$ *and* $M/M^\Phi$ *with the naturally induced action* $\Phi$*. In particular,* $r = \dim(T_s)$ *and the splitting fields of* $T$ *and* $T_a$ *are equal.*

**Lemma 7.5** ([98, Theorem 9.1.1]). *The preimage* $\phi^{-1}\big(T(\mathbb{F}_q)\big)$ *is equal to "the eigenspace"*

$$\mathrm{E}_q(\Phi) = \{x \in \mathbb{G}_m^d(\mathbb{F}_{q^e}) \mid \Phi(x) = x^q\}$$

*associated with the eigenvalue* $q$*.*

More precisely, if $\alpha$ is a primitive element of $\mathbb{F}_{q^e}$, then

$$\mathbb{G}_m^d(\mathbb{F}_{q^e}) = \{(\alpha^{v_1}, \cdots, \alpha^{v_d}) \mid v_i \in \mathbb{Z}/(q^e - 1)\}$$

and

$$\mathrm{E}_q(\Phi) = \Big\{(\alpha^{v_1}, \cdots, \alpha^{v_d}) \,\Big|\, \sum_{i=1}^{d} \Phi_{i,j} v_i \equiv q v_j \pmod{q^e - 1}\Big\}.$$

**Lemma 7.6.** *Let $x \in \mathrm{E}_q(\Phi)$, $m \in M$, and $k$ be cardinality of the orbit of $m$ under $\Phi$. Then $x^{\Phi^s(m)} = x^{q^s m}$ for $0 \leqslant s \leqslant k-1$ (in particular, $x^m \in \mathbb{F}_{q^k}$).*

*Proof.* The proposition follows from the equality chain

$$x^{\Phi(m)} = \prod_{i=1}^{d} x_i^{\sum\limits_{j=1}^{d} \Phi_{i,j} m_j} = \prod_{j=1}^{d} \left( \prod_{i=1}^{d} x_i^{\Phi_{i,j}} \right)^{m_j} = \prod_{j=1}^{d} x_j^{q m_j} = x^{qm}.$$

□

**Theorem 7.7.** *It is true that*

$$|T(\mathbb{F}_q)| = \chi(q) \equiv \pm 1 \pmod{q}, \qquad \textit{where} \qquad \chi(\lambda) = \det(\lambda I - \Phi)$$

*is the characteristic polynomial of $\Phi$. Moreover, if a torus $T$ is non-split, then it has strictly more $\mathbb{F}_q$-points than the split one, that is*

$$|T(\mathbb{F}_q)| > (q-1)^d.$$

*Proof.* The first part is proved in [98, Theorem 9.1.2]. For the second one we repeat a proof suggested by Kunyavskii in a private letter. Let $\lambda_1, \cdots, \lambda_d$ be all eigenvalues of $\Phi$. By Theorem 7.1 at least one of them is different from 1. Thus we obtain the strict inequality

$$|T(\mathbb{F}_q)| = \chi(q) = \prod_{i=1}^{d} |q - \lambda_i| \ > \ \prod_{i=1}^{d} (q - |\lambda_i|) = (q-1)^d.$$

□

Let $n, m \in \mathbb{N}$, $m \mid n$ and $\mathrm{R}_{n,q}$ be the Weil scalar restriction of $\mathbb{G}_m$ with respect to an extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ (see, for example, [98, §3.12]). The universal property of the Weil restriction gives the *norm map* $\mathrm{N}_{n,m,q} \colon \mathrm{R}_{n,q} \to \mathrm{R}_{m,q}$ [154, §5], which is a surjective $\mathbb{F}_q$-homomorphism of the algebraic tori. In particular,

$$\mathrm{N}_{n,q} := \mathrm{N}_{n,1,q} \colon \mathrm{R}_{n,q} \to \mathbb{G}_m, \qquad \mathrm{N}_{n,q}(P) = P \cdot P^{(1)} \cdot \ldots \cdot P^{(n-1)}$$

is the usual norm map, i.e., the product of $n$ conjugate (over $\mathbb{F}_q$) points. Besides, according to [154, Lemma 5.1.ii] the restriction of $\mathrm{N}_{n,m,q}$ to the subgroup $\mathrm{R}_{n,q}(\mathbb{F}_q)$ is the norm map for the extension $\mathbb{F}_{q^n}/\mathbb{F}_{q^m}$. Finally, consider $\mathbb{F}_q$-tori

$$\mathrm{R}_{n,q}^{(m)} = \ker(\mathrm{N}_{n,m,q}), \qquad \mathrm{T}_{n,q} = \bigcap_{\substack{m \mid n, \\ m \neq n}} \mathrm{R}_{n,q}^{(m)}.$$

For $m = 1$ the former is called a *norm one torus*. It is interesting that for $n$ equal to a product of different primes, the groups $\mathrm{T}_{n,q}(\mathbb{F}_q)$ are used in discrete logarithm cryptography [154, §6].

**Theorem 7.8** ([153, §2.1.7], [154, §5])**.**

1. $(\mathrm{R}_{n,q})_a = \mathrm{R}^{(1)}_{n,q}$ *and hence* $\mathrm{T}_{n,q}$ *is an anisotropic torus;*
2. *The splitting fields of* $\mathrm{R}_{n,q}$, $\mathrm{R}^{(1)}_{n,q}$, *and* $\mathrm{T}_{n,q}$ *are equal to* $\mathbb{F}_{q^n}$;
3. $\dim(\mathrm{T}_{n,q}) = \varphi(n)$ *and* $\mathrm{T}_{n,q}(\mathbb{F}_q) \simeq \mathbb{Z}/\big(\Phi_n(q)\big)$, *where* $\varphi$ *is the Euler function and* $\Phi_n$ *is the* $n$*-th cyclotomic polynomial.*

**Algebraic tori of dimension** 1 **and** 2

**Theorem 7.9** ([155])**.** *There are only the following* 1*-dimensional algebraic* $\mathbb{F}_q$*-tori:*

| $T$ | $e$ | $r$ | $\Phi$ | $T(\mathbb{F}_q)$ |
|---|---|---|---|---|
| $\mathbb{G}_m$ | 1 | 1 | 1 | $\mathbb{Z}/(q-1)$ |
| $T_2 = \mathrm{R}^{(1)}_{2,q}$ | 2 | 0 | $-1$ | $\mathbb{Z}/(q+1)$ |

**Theorem 7.10** ([155])**.** *There are only the following* 2*-dimensional algebraic* $\mathbb{F}_q$*-tori:*

| $T$ | $e$ | $r$ | $\Phi \in \mathrm{GL}(M)$ | $T(\mathbb{F}_q)$ |
|---|---|---|---|---|
| $\mathbb{G}_m^2$ | 1 | 2 | $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ | $\big(\mathbb{Z}/(q-1)\big)^2$ |
| $T_{2.a} = T_2^2$ | 2 | 0 | $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ | $\big(\mathbb{Z}/(q+1)\big)^2$ |
| $T_{2.b} = \mathbb{G}_m \times T_2$ | 2 | 1 | $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ | $\mathbb{Z}/(q-1) \times \mathbb{Z}/(q+1)$ |
| $T_{2.c} = \mathrm{R}_{2,q}$ | 2 | 1 | $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ | $\mathbb{Z}/(q^2-1)$ |
| $T_3 = \mathrm{R}^{(1)}_{3,q}$ | 3 | 0 | $\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ | $\mathbb{Z}/(q^2+q+1)$ |
| $T_4 = \mathrm{R}_{2,q}\big(\mathrm{R}^{(1)}_{2,q^2}\big)$ | 4 | 0 | $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ | $\mathbb{Z}/(q^2+1)$ |
| $T_6 = \mathrm{T}_{6,q}$ | 6 | 0 | $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ | $\mathbb{Z}/(q^2-q+1)$ |

In Article [155] there are not the values $r$ and $T(\mathbb{F}_q)$, which are either obvious or follow from Theorem 7.8. Besides, in that article the torus $T_3$ (resp. $T_4$) is denoted by $T_4$ (resp. $T_5$). We changed the notation, because the extension degree $e$ for $T_3$ (resp. $T_4$) is equal to 3 (resp. 4). Also, we will denote the matrix $\Phi$ for a torus $T_i$ by $\Phi_i$.

Besides the classification, it is useful to know

**Theorem 7.11** ([156]). *All $\mathbb{F}_q$-tori of dimension 1 and 2 are rational over $\mathbb{F}_q$.*

### 7.1.2 Toric varieties

We keep the notation of §7.1.1. Suppose $T$ to be an $\mathbb{F}_q$-torus and $V$ to be a projective smooth $\mathbb{F}_q$-variety (of dimension $d$). We say that $V$ is a *toric variety* (with respect to $T$) if it contains $T$ as an open subset and the group operation on $T$ can be extended to an action of $T$ on $V$. It is called *split* if $T$ is split. Besides, let $V'$ be another toric variety with respect to some torus $T'$. Then a morphism $\phi\colon V \to V'$ is called a *morphism of toric varieties* if its restriction $\phi\colon T \to T'$ is a homomorphism.

**Theorem 7.12.** *Let $V$ be a projective smooth $\mathbb{F}_q$-variety with a faithful action of an $\mathbb{F}_q$-torus $T$ and the open orbit $U$. Then $T$ and $U$ are $\mathbb{F}_q$-isomorphic (under the action of $T$) and hence $V$ is a toric variety (with respect to $T$).*

*Proof.* The orbit $U$ is a $T$-torsor, hence $T$ and $U$ are isomorphic over $\overline{\mathbb{F}_q}$ and the variety $V$ is geometrically rational. By a theorem [157, §2] it has an $\mathbb{F}_q$-point. On the other hand, [158, Proposition 4] guarantees the existence of an $\mathbb{F}_q$-point on $U$ and thus $T$ and $U$ are $\mathbb{F}_q$-isomorphic. □

Throughout the chapter we will use the notation

$$M_{\mathbb{R}} = M \otimes_{\mathbb{Z}} \mathbb{R}, \qquad N_{\mathbb{R}} = N \otimes_{\mathbb{Z}} \mathbb{R},$$
$$\rho(V) = \operatorname{rank}\bigl(\operatorname{Pic}(V)\bigr), \qquad \overline{V} = V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q},$$

and $\operatorname{TDiv}(V)$ is the set of $T$-invariant $\mathbb{F}_q$-divisors on $V$. Turning to the standard terminology of the toric geometry (see, for example, [92]), consider the following sets:

**Poly:** Pairs $(P, \Phi)$, where $P \subset M_{\mathbb{R}}$ is a full-dimensional smooth convex lattice polytope and $\Phi \in \mathrm{GL}(M)$ is a finite order matrix such that $\Phi(P) = P$.

**Fan:** Triples $(\Sigma, \Phi, D)$, where $\Sigma$ is a projective smooth *fan* in $N_{\mathbb{R}}$, invariant under a finite order matrix $\Phi \in \mathrm{GL}(N)$. In other words, for any cone $\sigma \in \Sigma$ we have that $\Phi(\sigma) \in \Sigma$. Finally, $D$ is an (very) ample $\Phi$-invariant integral combination of rays from $\Sigma$.

**Split:** Triples $(V, \Phi, D)$, where $V$ is a split toric $\mathbb{F}_q$-variety, $\Phi$ is an automorphism of $V$ (as the toric variety), and $D \in \mathrm{TDiv}(V)$ is an (very) ample $\Phi$-divisor.

**Tor:** Triples $(V, T, D)$, where $V$ is a toric $\mathbb{F}_q$-variety with respect to an $\mathbb{F}_q$-torus $T$, and $D \in \mathrm{TDiv}(V)$ is an (very) ample divisor.

It is well known that these sets correspond to each other under the following maps (the split case is discussed in [92]):

1. The map
$$\mathbf{Poly} \to \mathbf{Fan}, \qquad (P, \Phi) \mapsto (\Sigma_P, \Phi^t, D_P),$$
where $\Sigma_P$ and $D_P$ are the corresponding to $P$ normal fan [92, Theorem 2.3.2] and integral ray combination [92, §4.2] respectively;

2. The map
$$\mathbf{Fan} \to \mathbf{Split}, \qquad (\Sigma, \Phi, D) \mapsto (V_\Sigma, \Phi, D),$$
where $V_\Sigma$ is the corresponding to $\Sigma$ split toric variety [92, §3.1] and $\Phi$ is an automorphism of $\mathbb{G}_m^d$ from §7.1.1 continued to $V_\Sigma$;

3. The map
$$\mathbf{Split} \to \mathbf{Tor}, \qquad (V_\Sigma, \Phi, D) \mapsto (V_{\Sigma,\Phi}, T_\Phi, D),$$
where
$$V_{\Sigma,\Phi} = V_\Sigma/\Phi, \qquad T_\Phi = \mathbb{G}_m^d/\Phi$$
are geometric quotients of $V_\Sigma$ and $\mathbb{G}_m^d$ by the automorphism $\Phi$. The toric variety $V_{\Sigma,\Phi}$ is called the *Demazure model* of the torus $T_\Phi$.

**Theorem 7.13** ([152, §1-2])**.**

1. *All $\mathbb{F}_q$-forms of $V_\Sigma$ (without a toric structure) are toric varieties, i.e., they look like $V_{\Sigma,\Phi}$ for $\Phi \in \mathrm{Aut}(\Sigma)$;*

2. *For $\Phi' \in \mathrm{Aut}(\Sigma)$ the varieties $V_{\Sigma,\Phi}$ $V_{\Sigma,\Phi'}$ are $\mathbb{F}_q$-isomorphic (as toric varieties) if and only if the matrices $\Phi$, $\Phi'$ are conjugate in $\mathrm{Aut}(\Sigma)$;*

3. *$V_\Sigma$, $V_{\Sigma,\Phi}$ are isomorphic over $\mathbb{F}_{q^e}$.*

*Conversely, consider a matrix $\Phi \in \mathrm{GL}(N)$ and the torus $T_\Phi$. There is a projective smooth fan in $N_\mathbb{R}$, invariant under $\Phi$. In other words, there is a toric $\mathbb{F}_q$-variety with respect to $T_\Phi$.*

Let $\Sigma^{\Phi^t}$ be the set of invariant cones of $\Sigma$ with respect to a matrix $\Phi^t \in \mathrm{Aut}(\Sigma)$. Also, for $\sigma \in \Sigma^{\Phi^t}$ we denote by $\sigma^* \subset M_\mathbb{R}$ the cone dual to $\sigma$ and by $T_{\Phi,\sigma}$ the torus corresponding to the restriction of $\Phi$ to the sublattice $M_\sigma = -\sigma^* \cap \sigma^* \cap M$ $\big($of dimension $d - \dim(\sigma)\big)$.

**Theorem 7.14** ([159, Theorem 1.3.2, Corollary 1.3.6]). *There is a natural bijective correspondence*

$$V_{\Sigma,\Phi}(\mathbb{F}_q) = \bigsqcup_{\sigma \in \Sigma^{\Phi^t}} T_{\Phi,\sigma}(\mathbb{F}_q).$$

*In particular, for an anisotropic torus $T_\Phi$ we have the equality $V_{\Sigma,\Phi}(\mathbb{F}_q) = T_\Phi(\mathbb{F}_q)$.*

**Theorem 7.15** ([152, §1]). *The natural embedding $\mathrm{Pic}(V_\Sigma) \hookrightarrow \mathrm{Pic}(\overline{V_\Sigma})$ is an isomorphism. In other words, any divisor on $\overline{V_\Sigma}$ is equivalent to some $\mathbb{F}_q$-divisor. At the same time, there is a natural isomorphism between $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$-module $\mathrm{Pic}(V_{\Sigma,\Phi} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^e})$ and $\Phi$-module $\mathrm{Pic}(V_\Sigma)$. In particular,*

$$\rho(V_{\Sigma,\Phi}) = \mathrm{rank}\big(\mathrm{Pic}(V_\Sigma)^\Phi\big).$$

**Theorem 7.16** ([98, Theorem 4.3.1], [159, §1.3]). *There is the exact sequence of $\Phi$-modules*

$$0 \to M \to \mathrm{TDiv}(V_\Sigma) \to \mathrm{Pic}(V_\Sigma) \to 0$$

*and, passing to invariants, we obtain the induced sequence of groups*

$$0 \to M^\Phi \to \mathrm{TDiv}(V_\Sigma)^\Phi \to \mathrm{Pic}(V_\Sigma)^\Phi \to \mathrm{Pic}(T_\Phi) \to 0.$$

*Moreover, the group*

$$\mathrm{Pic}(T_\Phi) \simeq \mathrm{H}^1(\Phi, M)$$

*is finite and hence the number of $\Phi^t$-orbits on $\Sigma(1)$ is equal to $r(T_\Phi) + \rho(V_{\Sigma,\Phi})$.*

Considering toric codes, we will be interested in the image of $\mathrm{TDiv}(V_\Sigma)^\Phi$ in $\mathrm{Pic}(V_\Sigma)^\Phi$, which we denote by $\mathrm{TPic}(V_\Sigma, \Phi)$. In particular,

$$\mathrm{TPic}(V_\Sigma, I) = \mathrm{Pic}(V_\Sigma).$$

### 7.1.3 Projective line $\mathbb{P}^1$ and some toric surfaces

It is well known that $\mathbb{P}^1$ is the unique one-dimensional projective smooth toric variety. Let $x, y$ be its homogeneous coordinates. Prime torus-invariant divisors on $\mathbb{P}^1$ are only the points $P_x = (0:1)$, $P_y = (1:0)$.

**Theorem 7.17** ([92, Example 2.4.10]). *The fan of $\mathbb{P}^1$ and all possible actions on it are represented in Figure* 7.1. *More precisely,*

$$\mathrm{Aut}(\Sigma_{\mathbb{P}^1}) = \langle -1 \rangle \simeq \mathbb{Z}/2.$$


$\Phi = 1$ $\Phi = -1$

Figure 7.1: Actions on primitive vectors of the fan $\Sigma_{\mathbb{P}^1}$

Besides, it is clear that

$$\mathrm{Pic}(\mathbb{P}^1) = \mathbb{Z}[P_y], \qquad \mathrm{TPic}(\mathbb{P}^1, -1) = \mathbb{Z}[D_{x,y}],$$

where $D_{x,y} = P_x + P_y$.

From now on we will talk about toric surfaces. And we will need the notation $\mathbb{V}(f_1, \cdots, f_n)$ for the algebraic variety generated by some family of $\mathbb{F}_q$-polynomials $f_1, \cdots, f_n$, $n \in \mathbb{N}$.

**Theorem 7.18** ([160, §4.1])**.** *A toric $\mathbb{F}_q$-surface can be obtained by a sequence of blowings up at $\mathbb{F}_q$-orbits of torus-invariant points, starting from $\mathbb{F}_q$-minimal surfaces, which are $\mathbb{F}_q$-forms of*

1. $\mathbb{P}^2$,
2. $\mathbb{P}^1 \times \mathbb{P}^1$,
3. *Hirzebruch surfaces $\mathbb{F}_m$ for $m > 1$,*
4. *the del Pezzo surface of degree 6 and Picard $\mathbb{F}_q$-number 1.*

**Projective plane $\mathbb{P}^2$.** Let us recall that forms (over any field) of $\mathbb{P}^2$ are called *Severi–Brauer surfaces*. According to Katz [157, §2] and Châtelet [161, Proposition 4.5.10] we have

**Lemma 7.19.** *There are no Severi–Brauer surfaces over $\mathbb{F}_q$ different from $\mathbb{P}^2$.*

Let $x, y, z$ be homogeneous coordinates of $\mathbb{P}^2$. It is well known that $\mathbb{P}^2$ is a split toric surface and all its prime torus-invariant divisors are the lines $L_x = \mathbb{V}(x)$, $L_y = \mathbb{V}(y)$, $L_z = \mathbb{V}(z)$.

**Theorem 7.20** ([92, Example 3.1.9])**.** *The fan of $\mathbb{P}^2$ and all possible actions on it (up to a conjugation) are represented in Figure 7.2. More precisely,*

$$\mathrm{Aut}(\Sigma_{\mathbb{P}^2}) = \langle \Phi_3^t \rangle \rtimes \langle \Phi_{2.c} \rangle \simeq S_3.$$

Finally, it is clear that

$$\mathrm{Pic}(\mathbb{P}^2) = \mathrm{TPic}(\mathbb{P}^2, \Phi_{2.c}) = \mathbb{Z}[L_z], \qquad \mathrm{TPic}(\mathbb{P}^2, \Phi_3) = \mathbb{Z}[D_{x,y,z}],$$

where $D_{x,y,z} = L_x + L_y + L_z$.

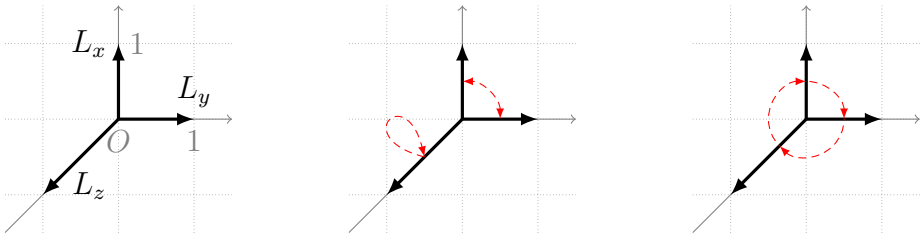


Figure 7.2: Actions on primitive vectors of the fan $\Sigma_{\mathbb{P}^2}$

**Quadratic surfaces.** Consider two different points $P_1, P_2 \in \mathbb{P}^2$ and the line $L$ between them. The successive blowings up at the points $P_1, P_2$ and the blowing down of the proper preimage of $L$ result in the surface $Q$. If $P_1, P_2$ are $\mathbb{F}_q$-points, then $Q$ is called the *hyperbolic quadratic $\mathbb{F}_q$-surface* $\mathcal{H}$. In turn, if $P_1, P_2$ are $\mathbb{F}_q$-conjugate, then $Q$ is called the *elliptic quadratic $\mathbb{F}_q$-surface* $\mathcal{E}$.

**Theorem 7.21.** *First, $\mathcal{E}$ is the unique non-trivial $\mathbb{F}_q$-form of $\mathcal{H}$. Besides, there are the following $\mathbb{F}_q$-isomorphisms:*

$$\mathcal{H} \simeq \mathbb{P}^1 \times \mathbb{P}^1 \simeq \mathbb{V}(xy - zt), \qquad \mathcal{E} \simeq \mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathbb{P}^1) \simeq \mathbb{V}\big(xy - Q(z,t)\big),$$

*where $x, y, z, t$ are homogeneous coordinates of $\mathbb{P}^3$, the surface $\mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathbb{P}^1)$ is a Weil scalar restriction, and*

$$Q(z,t) = \begin{cases} z^2 - at^2 & \big(\text{where } a \in \mathbb{F}_q^*,\ \sqrt{a} \notin \mathbb{F}_q\big) \quad \text{if } p \neq 2, \\ z^2 + zt + at^2 & \big(\text{where } a \in \mathbb{F}_q^*,\ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(a) = 1\big) \quad \text{if } p = 2. \end{cases}$$

*Proof.* The classification of $\mathbb{F}_q$-forms follows from [152, §3], [162, Lemma 15.3.1]. At the same time, the existence of isomorphisms is discussed, for example, in [163, §2.2.1], [164, Example 3.8]. □

Suppose $x, y$ and $u, v$ to be two pairs of homogeneous coordinates on $\mathbb{P}^1 \times \mathbb{P}^1$. The action $\mathbb{G}_m^2$ on $\mathcal{H}$ is naturally induced from the action $\mathbb{G}_m$ on $\mathbb{P}^1$ and corresponding prime $\mathbb{G}_m^2$-invariant divisors are the lines

$$L_x = \{P_x\} \times \mathbb{P}^1, \qquad L_y = \{P_y\} \times \mathbb{P}^1, \qquad L_u = \mathbb{P}^1 \times \{P_u\}, \qquad L_v = \mathbb{P}^1 \times \{P_v\}.$$

**Theorem 7.22** ([92, Example 3.1.12])**.** *The fan of $\mathcal{H}$ and all possible actions on it (up to a conjugation) are represented in Figure 7.3. More precisely,*

$$\mathrm{Aut}(\Sigma_{\mathcal{H}}) = \langle \Phi_4^t \rangle \rtimes \langle \Phi_{2.c} \rangle \simeq D_4.$$

Note that in geometric terms $\Phi_{2.c}$ is the involution $(P, Q) \mapsto (Q, P)$.

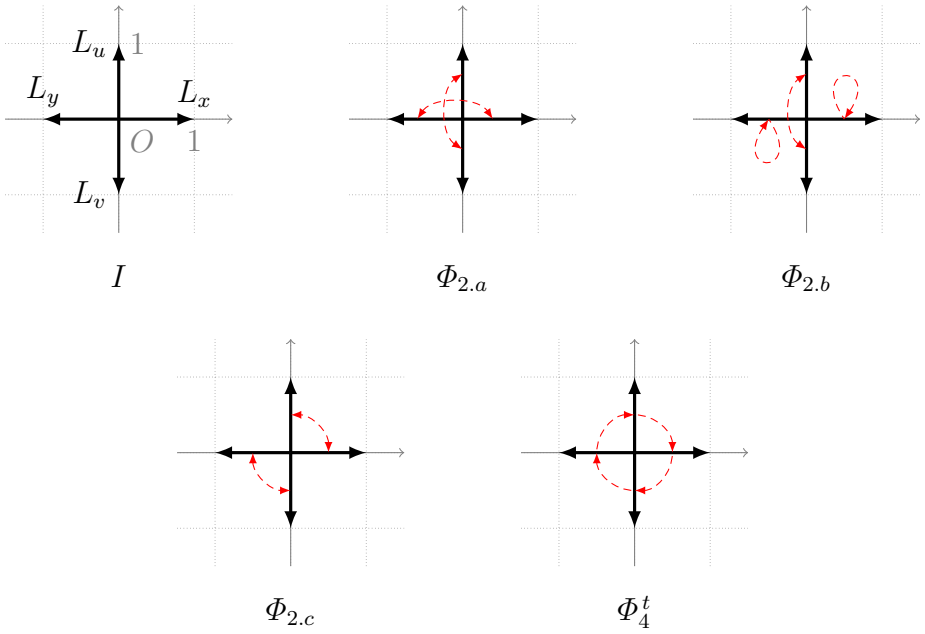


Figure 7.3: Actions on primitive vectors of the fan $\Sigma_{\mathcal{H}}$

**Lemma 7.23.** *We have $\mathbb{F}_q$-isomorphisms (without a toric structure)*

$$\mathcal{H} \simeq V_{\Sigma_{\mathcal{H}},\Phi_{2.a}} \simeq V_{\Sigma_{\mathcal{H}},\Phi_{2.b}}, \qquad \mathcal{E} \simeq V_{\Sigma_{\mathcal{H}},\Phi_{2.c}} \simeq V_{\Sigma_{\mathcal{H}},\Phi_4}.$$

*Proof.* It is sufficient to explicitly realize all toric $\mathbb{F}_q$-forms of $\mathcal{H}$. The first part of the lemma is obvious, because $\mathbb{P}^1 \times \mathbb{P}^1$ is a toric surface with respect to the tori $T_{2.a}$, $T_{2.b}$. On the other hand, by the universal property of Weil restriction the action of $\mathbb{G}_m$ (resp. $T_2$) on $\mathbb{P}^1$ is transferred to the action of $T_{2.c}$ (resp. $T_4$) on $\mathrm{R}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\mathbb{P}^1)$. Thus the second part is also true. □

Finally, it is easily proved that

$$\mathrm{Pic}(\mathcal{H}) = \mathbb{Z}[L_y] \oplus \mathbb{Z}[L_v], \quad \mathrm{TPic}(\mathcal{H},\Phi_{2.a}) = \mathbb{Z}[D_{x,y}] \oplus \mathbb{Z}[D_{u,v}], \quad \mathrm{TPic}(\mathcal{H},\Phi_{2.b}) = \mathbb{Z}[L_y] \oplus \mathbb{Z}[D_{u,v}],$$

$$\mathrm{Pic}(\mathcal{E}) = \mathrm{TPic}(\mathcal{H},\Phi_{2.c}) = \mathbb{Z}[D_{y,v}], \quad \mathrm{TPic}(\mathcal{H},\Phi_4) = \mathbb{Z}[D_{x,y,u,v}],$$

where

$$D_{x,y} = L_x + L_y, \quad D_{u,v} = L_u + L_v, \quad D_{y,v} = L_y + L_v, \quad D_{x,y,u,v} = D_{x,y} + D_{u,v}.$$

**Hirzebruch surfaces $\mathbb{F}_m$ for $m > 0$.** These surfaces are defined by the equation

$$\mathbb{F}_m = \mathbb{V}(u^m y - v^m x) \subset \mathbb{P}^2_{(x:y:z)} \times \mathbb{P}^1_{(u:v)}.$$

The projection $f\colon \mathbb{F}_m \to \mathbb{P}^1_{(u:v)}$ is the unique $\mathbb{P}^1$-fibration on $\mathbb{F}_m$. It is easily proved that there are no non-trivial $\mathbb{F}_q$-forms for $\mathbb{F}_m$ and the surface is split toric one. Its torus-invariant prime divisors have the form

$$F_u = \mathbb{V}(u,x), \qquad F_v = \mathbb{V}(v,y), \qquad \Sigma = \mathbb{V}(x,y), \qquad S = \mathbb{V}(\mathbb{F}_m, z).$$

The curves $F_u$, $F_v$ are fibers of $f$ over points $P_u$, $P_v \in \mathbb{P}^1$ respectively. On the other hand, the curves $\Sigma$, $S$ are the images of sections for $f$, whose self-intersections are equal to $-m$, $m$ respectively.

Consider the matrix

$$\Phi_{\mathbb{F}_m} = \begin{pmatrix} 1 & 0 \\ m & -1 \end{pmatrix} \in \mathrm{GL}(M),$$

noting that it is conjugate to $\Phi_{2.b}$ if $2 \mid m$, and to $\Phi_{2.c}$ if $2 \nmid m$.

**Theorem 7.24** ([92, Example 3.1.16])**.** *The fan of $\mathbb{F}_m$ and all possible actions on it are represented in Figure* 7.4*. More precisely,*

$$\mathrm{Aut}(\Sigma_{\mathbb{F}_m}) = \langle \Phi^t_{\mathbb{F}_m} \rangle \simeq \mathbb{Z}/2.$$

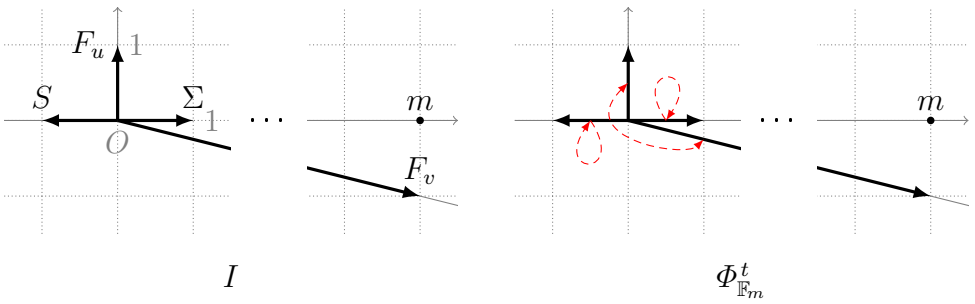


Figure 7.4: Actions on primitive vectors of the fan $\Sigma_{\mathbb{F}_m}$ for $m > 0$

Finally, it is easy to check that

$$\mathrm{Pic}(\mathbb{F}_m) = \mathbb{Z}[S] \oplus \mathbb{Z}[F_v], \qquad \mathrm{TPic}(\mathbb{F}_m, \Phi_{\mathbb{F}_m}) = \mathbb{Z}[S] \oplus \mathbb{Z}[D_m],$$

where

$$D_m = \begin{cases} F_u + F_v & \text{if } 2 \mid m, \\ \Sigma + \frac{m-1}{2}(F_u + F_v) & \text{if } 2 \nmid m, \end{cases} \qquad D_m \sim \begin{cases} 2F_v & \text{if } 2 \mid m, \\ S - F_v & \text{if } 2 \nmid m. \end{cases}$$

It is also worth noting that a divisor $r_1 S + r_2 F_v$ is (very) ample if and only if $r_1$, $r_2 > 0$.

### 7.1.4 Del Pezzo surfaces of degree 6

In this subsection we will use the above notation for $\mathbb{P}^2$ and basic facts from [152, §3]. Consider the points

$$P_x = (1:0:0), \qquad P_y = (0:1:0), \qquad P_z = (0:0:1).$$

It is well known that the simultaneous blowing up of $\mathbb{P}^2$ at these points is a *del Pezzo $\mathbb{F}_q$-surface* $\mathcal{D}_1$ of degree 6 and such one is unique over $\overline{\mathbb{F}_q}$. Besides, $\mathcal{D}_1$ is a toric surface, because the points $P_x$, $P_y$, $P_z$ are torus-invariant.

Let $E_x$, $E_y$, $E_z$ be the exceptional curves associated with the points $P_x$, $P_y$, $P_z$ respectively and $\widetilde{L}_x$, $\widetilde{L}_y$, $\widetilde{L}_z$ be the proper preimages of the lines $L_x$, $L_y$, $L_z$ respectively. These 6 curves are unique torus-invariant prime divisors on $\mathcal{D}_1$. Besides, the divisor

$$H_0 = E_x + E_y + E_z + \widetilde{L}_x + \widetilde{L}_y + \widetilde{L}_z$$

is anticanonical and gives $\mathbb{F}_q$-embedding of $\mathcal{D}_1$ in $\mathbb{P}^6$.

**Theorem 7.25.** *The fan of $\mathcal{D}_1$ and all possible actions on it are represented in Figure* 7.5*, where*

$$\Phi'_{2.c} = (-1)\Phi_{2.c} = \Phi_4\Phi_{2.c}\Phi_4^{-1}.$$

*More precisely,*

$$\mathrm{Aut}(\Sigma_{\mathcal{D}_1}) = \mathrm{Aut}(\Sigma_{\mathbb{P}^2}) \times \langle \Phi_{2.a} \rangle = \langle \Phi_6^t \rangle \rtimes \langle \Phi_{2.c} \rangle \cong D_6.$$

Note that in geometric terms $\Phi_{2.a}$ is the standard quadratic transformation

$$\mathbb{P}^2 \dashrightarrow \mathbb{P}^2, \qquad (x:y:z) \mapsto (yz:xz:xy) = (x^{-1}:y^{-1}:z^{-1})$$

lifted to $\mathcal{D}_1$.

We will denote by $\mathcal{D}_i$ (resp. $\mathcal{D}'_{2.c}$) the toric surface $V_{\Sigma_{\mathcal{D}_1},\Phi_i}$ (resp. $V_{\Sigma_{\mathcal{D}_1},\Phi'_{2.c}}$). We stress that the surfaces $\mathcal{D}_{2.c}$ and $\mathcal{D}'_{2.c}$ are not isomorphic over $\mathbb{F}_q$, but they both contain the torus $T_{2.c}$. Besides, for a toric surface $S$ let us denote by $\mathrm{Bl}_{a_1,\cdots,a_n}(S)$ a blowing up of $S$ at some $\mathbb{F}_q$-orbits (of cardinalities $a_1,\cdots,a_n, n \in \mathbb{N}$) of torus-invariant points. In general, this blowing up, of course, depends on a choice of $\mathbb{F}_q$-orbits with given cardinalities. According to Theorems 7.14, 7.16 and Figure 7.5 we have

**Theorem 7.26.** *All del Pezzo $\mathbb{F}_q$-surfaces of degree* 6 *are represented in Table* 7.1*. In particular, $\mathcal{D}_6$ is the unique $\mathbb{F}_q$-minimal surface among them.*

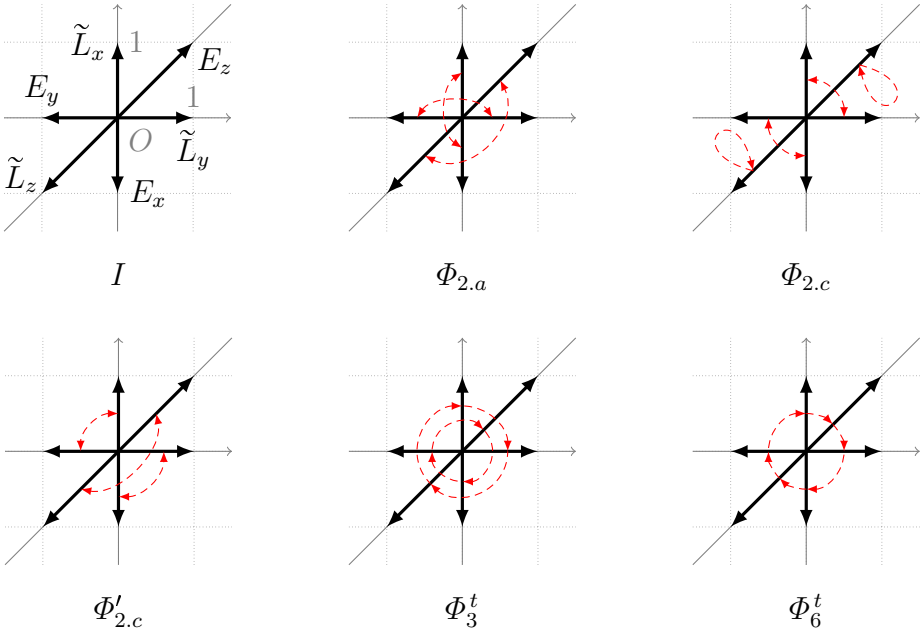


Figure 7.5: Actions on primitive vectors of the fan $\Sigma_{\mathcal{D}_1}$

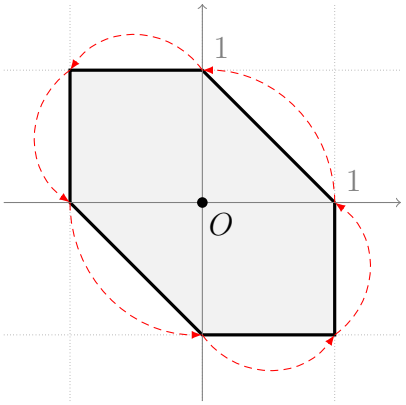


Figure 7.6: The polygon $P_{H_0}$ with the action $\Phi_6$

| $\mathcal{D}$ | $\lvert\mathcal{D}(\mathbb{F}_q)\rvert$ | $\rho(\mathcal{D})$ |
|---|---|---|
| $\mathcal{D}_1 = \mathrm{Bl}_{1,1,1}(\mathbb{P}^2) = \mathrm{Bl}_{1,1}(\mathcal{H})$ | $q^2+4q+1$ | 4 |
| $\mathcal{D}_{2.a} = \mathrm{Bl}_2(\mathcal{H})$ | $q^2+2q+1$ | 3 |
| $\mathcal{D}_{2.c} = \mathrm{Bl}_{1,2}(\mathbb{P}^2) = \mathrm{Bl}_{1,1}(\mathcal{E})$ | $q^2+2q+1$ | 3 |
| $\mathcal{D}'_{2.c} = \mathrm{Bl}_2(\mathcal{E})$ | $q^2+1$ | 2 |
| $\mathcal{D}_3 = \mathrm{Bl}_3(\mathbb{P}^2)$ | $q^2+q+1$ | 2 |
| $\mathcal{D}_6$ | $q^2-q+1$ | 1 |

Table 7.1: del Pezzo $\mathbb{F}_q$-surfaces of degree 6

From now on we focus on the surface $\mathcal{D}_6$, because toric codes on it seem to have the best parameters than those on other del Pezzo surfaces of degree 6. First of all,

$$\mathrm{Pic}(\mathcal{D}_6) = \mathrm{TPic}(\mathcal{D}_1, \Phi_6) = \mathbb{Z}[H_0]$$

and the polygon $P_{H_0}$ with the action $\Phi_6$ is represented in Figure 7.6. The following lemma is an elementary exercise.

**Lemma 7.27.** *For $r \in \mathbb{N}$ the set*

$$\{(0,0)\} \cup \{(i,j) \mid 1 \leqslant i;\ 0 \leqslant j;\ i+j \leqslant r\} \subset M$$

*consists of representatives for all orbits with respect to the action $\Phi_6$ on $P_{rH_0} \cap M$. Besides, non-zero points from this set represent orbits of cardinality 6. In particular,*

$$|P_{rH_0} \cap M| = 3r(r+1)+1.$$

Let $\mathbf{P} = \{P_1, P_2, P_3\}$ be a set of non-collinear $\mathbb{F}_q$-conjugate points on $\mathbb{P}^2$ and $\mathbf{Q} = \{Q_1, Q_2\}$ be that of different $\mathbb{F}_q$-conjugate points on $\mathbb{P}^2$. In particular, these 5 points are in general position, hence we can consider the uniquely defined non-degenerate conic $\mathcal{C}$ passing through them. For $i,j \in \{1,2,3\}$ $(i \neq j)$, $k \in \{1,2\}$ we denote by $\mathcal{L}_{i,j}$, $\mathcal{M}$, and $\mathcal{N}_{j,k}$ the lines passing through $P_i$, $P_j$, through $Q_1$, $Q_2$, and through $P_j$, $Q_k$ respectively. Besides, let

$$\mathcal{L} = \mathcal{L}_{1,2} + \mathcal{L}_{1,3} + \mathcal{L}_{2,3}, \qquad \mathcal{N} = \sum_{j,k=1}^{3,2} \mathcal{N}_{j,k}.$$

All mentioned geometric objects are represented in Figure 7.7.

Since the lines $\mathcal{N}_{j,k}$ are conjugate to each other and any toric $\mathbb{F}_q$-surface is uniquely defined by the Frobenius action on its prime torus-invariant divisors, we have

**Lemma 7.28.** *The surface $\mathcal{D}_6$ is obtained by the blowing up of $\mathbb{P}^2$ at the orbits $\mathbf{P}$, $\mathbf{Q}$ followed by the blowing down of the proper preimages $\widetilde{\mathcal{M}}$, $\widetilde{\mathcal{C}}$ of the curves $\mathcal{M}$, $\mathcal{C}$ respectively.*

We will denote by $\mathcal{B}$ the corresponding blowing up surface (which is del Pezzo one of degree 4) and by $\varphi_u$ (resp. $\varphi_d$) the blowing up (down) map. In other words, we have the diagram

$$\mathbb{P}^2 \xleftarrow{\varphi_u} \mathcal{B} \xrightarrow{\varphi_d} \mathcal{D}_6.$$

Besides, let

$$P_{\mathcal{M}} = \varphi_d(\widetilde{M}), \qquad P_{\mathcal{C}} = \varphi_d(\widetilde{C}), \qquad \varphi_{ud} = \varphi_u \circ \varphi_d^{-1},$$

and

$$\mathcal{L}' = \mathcal{L}'_{1,2} + \mathcal{L}'_{1,3} + \mathcal{L}'_{2,3}$$

be the proper preimage of $\mathcal{L}$ under $\varphi_{ud}$. Finally, let

$$E_{\mathbf{P}} = E_{P_1} + E_{P_2} + E_{P_3}, \qquad E_{\mathbf{Q}} = E_{Q_1} + E_{Q_2}$$

be the exceptional divisors associated with $\mathbf{P}$, $\mathbf{Q}$ respectively, and

$$E'_{\mathbf{P}} = (\varphi_d)_*(E_{\mathbf{P}}) = E'_{P_1} + E'_{P_2} + E'_{P_3}, \qquad E'_{\mathbf{Q}} = (\varphi_d)_*(E_{\mathbf{Q}}) = E'_{Q_1} + E'_{Q_2}.$$

For clarity see Figure 7.8. Note that there are the bijective correspondences

$$\mathcal{D}_6 \backslash (E'_{\mathbf{P}} \cup E'_{\mathbf{Q}}) \overset{\varphi_{ud}}{\xrightarrow{\sim}} \mathbb{P}^2 \backslash (\mathcal{M} \cup \mathcal{C}),$$

$$T_6(\mathbb{F}_q) \backslash \{P_{\mathcal{M}}, P_{\mathcal{C}}\} = \mathcal{D}_6(\mathbb{F}_q) \backslash \{P_{\mathcal{M}}, P_{\mathcal{C}}\} \overset{\varphi_{ud}}{\xrightarrow{\sim}} \mathbb{P}^2(\mathbb{F}_q) \backslash (\mathcal{M} \cup \mathcal{C}).$$

The lines $\mathcal{N}_{j,k}$ are not tangents to $\mathcal{C}$, hence their proper preimages $\widetilde{\mathcal{N}}_{j,k} \subset \mathcal{B}$ do not intersect $\widetilde{\mathcal{C}}$ (and $\widetilde{\mathcal{M}}$, of course). Therefore $\widetilde{\mathcal{N}}_{j,k} \overset{\varphi_d}{\xrightarrow{\sim}} \varphi_d(\widetilde{\mathcal{N}}_{j,k})$ and we will not make any difference in the notation. It is easily seen that $\widetilde{\mathcal{N}}_{j,k}$ are exceptional curves on $\mathcal{D}_6$ and thus

$$H_0 = \sum_{j,k=1}^{3,2} \widetilde{\mathcal{N}}_{j,k} \in \operatorname{Div}(\mathcal{D}_6) \quad \big(\text{or } \operatorname{Div}(\mathcal{B})\big).$$

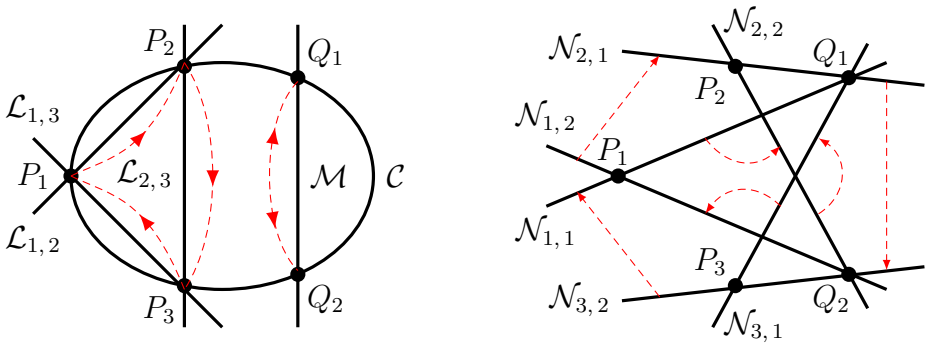


Figure 7.7: Points $P_j$, $Q_k$, lines $\mathcal{L}_{i,j}$, $\mathcal{M}$, $\mathcal{N}_{j,k}$, and the conic $\mathcal{C}$

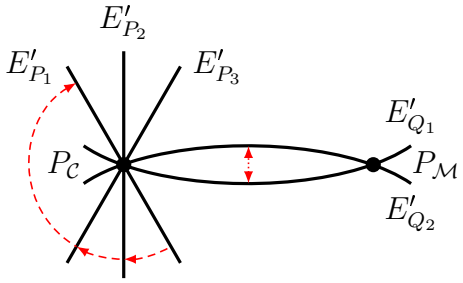


Figure 7.8: Points $P_{\mathcal{M}}$, $P_{\mathcal{C}}$ and curves $E'_{\mathbf{P}}$, $E'_{\mathbf{Q}}$

**Lemma 7.29.** *The set of hyperplane $\mathbb{F}_q$-sections on $\mathcal{D}_6 \subset \mathbb{P}^6$ has the form*

$$|H_0| = \varphi_{ud}^*(\mathbb{L}) - 2E'_{\mathbf{P}} - 3E'_{\mathbf{Q}},$$

*where the incomplete linear system*

$$\mathbb{L} = |\mathcal{N} - 2\mathbf{P} - 3\mathbf{Q}|,$$

*by definition, consists of plane (possibly reducible) $\mathbb{F}_q$-sextics passing through $\mathbf{P}$ with a multiplicity of 2 and through $\mathbf{Q}$ with a multiplicity of 3.*

*Proof.* Indeed, it is easily proved that

$$\varphi_u^*(\mathbb{L}) - 2E_{\mathbf{P}} - 3E_{\mathbf{Q}} = |\varphi_u^*(\mathcal{N}) - 2E_{\mathbf{P}} - 3E_{\mathbf{Q}}| = |H_0| \subset \mathrm{Div}(\mathcal{B}),$$

hence

$$\varphi_{ud}^*(\mathbb{L}) - 2E'_{\mathbf{P}} - 3E'_{\mathbf{Q}} = (\varphi_d)_*\big(\varphi_u^*(\mathbb{L}) - 2E_{\mathbf{P}} - 3E_{\mathbf{Q}}\big) = (\varphi_d)_*\big(|H_0|\big) = |H_0| \subset \mathrm{Div}(\mathcal{D}_6).$$

For better understanding of direct and inverse images of divisors on algebraic varieties see, for example, [1, §II.5-6, §IV.2]. □

According to the formula [1, Example V.3.9.2] (a version of the Plücker formula) for genus of an absolutely irreducible curve it is easy to check

**Lemma 7.30.** *There are only the following decompositions into irreducible components for $\mathbb{F}_q$-curves from $\mathbb{L}$:*

6: *A sextic with $\mu_{\mathbf{P}} = 2$, $\mu_{\mathbf{Q}} = 3$;*

$5 + \mathcal{M}$: *A quintic with $\mu_{\mathbf{P}} = \mu_{\mathbf{Q}} = 2$ and $\mathcal{M}$;*

$4 + \mathcal{C}$: *A quartic with $\mu_{\mathbf{P}} = 1$, $\mu_{\mathbf{Q}} = 2$ and $\mathcal{C}$;*

$3 + \mathcal{C} + \mathcal{M}$: *A cubic with $\mu_{\mathbf{P}} = \mu_{\mathbf{Q}} = 1$, $\mathcal{C}$, and $\mathcal{M}$;*

$2 + 2{\cdot}\mathcal{C}$: *A conic with $\mu_{\mathbf{P}} = 0$, $\mu_{\mathbf{Q}} = 1$ and two copies of $\mathcal{C}$;*

$2 + 2{\cdot}\mathcal{M} + \mathcal{C}$: *A conic with $\mu_{\mathbf{P}} = 1$, $\mu_{\mathbf{Q}} = 0$, two copies of $\mathcal{M}$, and $\mathcal{C}$;*

$2{\cdot}\mathcal{C} + \mathcal{M} + 1$: *Two copies of $\mathcal{C}$, $\mathcal{M}$, and a line;*

$\mathcal{M} + 1 + 2 + 2^{(1)}$: *The line $\mathcal{M}$, a line, and two $\mathbb{F}_q$-conjugate conics with $\mu_{\mathbf{P}} = 1$ such that $\mathcal{M}$ is the tangent to every one exactly at one point from $\mathbf{Q}$;*

$2' + 2 + 2^{(1)}$: *A conic and two $\mathbb{F}_q$-conjugate conics as in the previous case;*

$3{\cdot}\mathcal{C}$: *Three copies of $\mathcal{C}$;*

$2{\cdot}\mathcal{C} + 2{\cdot}\mathcal{M}$: *Two copies of $\mathcal{C}$ and two ones of $\mathcal{M}$;*

$\mathcal{L} + 3{\cdot}\mathcal{M}$: *The lines $\mathcal{L}_{i,j}$ and three copies of $\mathcal{M}$;*

$\mathcal{N}$: *The lines* $\mathcal{N}_{j,k}$*;*

Degenerate cases: *Other decompositions not containing* $\mathbb{F}_q$*-curves different from* $\mathcal{M}$ *and* $\mathcal{C}$*.*

*In particular, in all cases there is no more than one absolutely irreducible* $\mathbb{F}_q$*-curve (of geometric genus* $g \leqslant 1$*) different from* $\mathcal{M}$ *and* $\mathcal{C}$*. Moreover, for this curve* $g = 1$ *only in the cases* $6$*,* $5 + \mathcal{M}$*,* $4 + \mathcal{C}$*,* $3 + \mathcal{C} + \mathcal{M}$ *without singular points outside* $\mathbf{P}$ *and* $\mathbf{Q}$*.*

According to Lemmas 7.29, 7.30 and properties of blowings up [1, §V.3] we obtain

**Corollary 7.31.** *The full classification of hyperplane* $\mathbb{F}_q$*-sections on* $\mathcal{D}_6 \subset \mathbb{P}^6$ *is represented in Table* 7.2*.*

| $S \in \mathbb{L}$ | $H = \varphi_{ud}^*(S) - 2E'_{\mathbf{P}} - 3E'_{\mathbf{Q}}$ | $\lvert H(\mathbb{F}_q)\rvert$ | $\mu_{P_{\mathcal{M}}}(H)$ | $\mu_{P_{\mathcal{C}}}(H)$ |
|---|---|---|---|---|
| $6$ | an elliptic curve | [5, Th-m 3.3.12] | $0$ | $0$ |
| $5 + \mathcal{M}$ | or a rational one | or $\leqslant q + 2$ | $1$ | $0$ |
| $4 + \mathcal{C}$ | with a unique singular point | respectively | $0$ | $1$ |
| $3 + \mathcal{C} + \mathcal{M}$ | (of multiplicity 2) | | $1$ | $1$ |
| $2 + 2{\cdot}\mathcal{C}$ | a rational curve | $\leqslant q + 2$ | $0$ | $2$ |
| $2 + 2{\cdot}\mathcal{M} + \mathcal{C}$ | smooth outside $P_{\mathcal{M}}$, $P_{\mathcal{C}}$ | | $2$ | $1$ |
| $2{\cdot}\mathcal{C} + \mathcal{M} + 1$ | | | $1$ | $2$ |
| $\mathcal{M} + 1 + 2 + 2^{(1)}$ | three rational curves smooth outside | | $3$ | $2$ |
| $2' + 2 + 2^{(1)}$ | $P_{\mathcal{M}}$, $P_{\mathcal{C}}$; two of them are $\mathbb{F}_q$-conjugate | $\leqslant q + 4$ | $2$ | $2$ |
| $3{\cdot}\mathcal{C}$ | $E'_{\mathbf{P}}$ | $1$ | $0$ | $3$ |
| $2{\cdot}\mathcal{C} + 2{\cdot}\mathcal{M}$ | $E'_{\mathbf{Q}}$ | $2$ | $2$ | $2$ |
| $\mathcal{L} + 3{\cdot}\mathcal{M}$ | $\mathcal{L}'$ | $1$ | $3$ | $0$ |
| $\mathcal{N}$ | $H_0$ | $0$ | $0$ | $0$ |
| Degenerate cases | one or two $\mathbb{F}_q-$orbits of conjugate smooth rational curves | $\leqslant 4$ | | |

Table 7.2: Classification of hyperplane $\mathbb{F}_q$-sections on $\mathcal{D}_6 \subset \mathbb{P}^6$

**Corollary 7.32.** *For* $q \geqslant 5$ *every elliptic* $\mathbb{F}_q$*-curve is isomorphic over* $\mathbb{F}_q$ *to some hyperplane section on* $\mathcal{D}_6 \subset \mathbb{P}^6$*.*

*Proof.* On the one hand, the classification of elements from $|H_0|$ (Corollary 7.31) does not depend on choosing of the point sets $\mathbf{P}$, $\mathbf{Q}$. On the other hand, for $q \geqslant 5$ any elliptic $\mathbb{F}_q$-curve $E$ contains such sets. Indeed, let $S$ be the set of points from $E(\mathbb{F}_{q^3})$ that are collinear with their $\mathbb{F}_q$-conjugate ones. By the Bézout theorem the cardinality of this set is bounded by $3(q^2+q)$, because the equation of collinearity for three conjugate points is obviously of degree $q^2+q$. Applying the Hasse bound [5, §3.3.3], we see that

$$|E(\mathbb{F}_{q^3})\backslash S| \geqslant q^3 - 3q^2 - \lfloor 2q\sqrt{q}\rfloor - 3q + 1 > 0,$$

$$|E(\mathbb{F}_{q^2})\backslash E(\mathbb{F}_q)| \geqslant q^2 - 3q - \lfloor 2\sqrt{q}\rfloor > 0$$

for $q \geqslant 5$. □

## 7.2 Toric codes

### 7.2.1 Definition and main properties

This subsection is based on §7.1.1, §7.1.2. Consider a triple $(V,T,D) \in \mathbf{Tor}$ and corresponding ones $(V_\Sigma, \Phi, D) \in \mathbf{Split}$, $(P_D, \Phi) \in \mathbf{Poly}$. Suppose $\phi\colon V_\Sigma \xrightarrow{\sim} V$ to be an $\mathbb{F}_{q^e}$-isomorphism (of toric varieties) and $T(\mathbb{F}_q) = \{P_0, \cdots, P_{n-1}\}$.

The evaluation map

$$\mathrm{Ev}\colon \mathrm{H}^0(V,D) \to \mathbb{F}_q^n, \qquad \mathrm{Ev}(f) = \big(f(P_0), \cdots, f(P_{n-1})\big)$$

is well defined, because $T \cap \mathrm{Supp}(D) = \varnothing$. We will assume its injectivity, that is there is no $\mathbb{F}_q$-curve from the linear system $|D|$ that completely contains $T(\mathbb{F}_q)$. By definition, a *toric code* is the image

$$\mathcal{C}_q(V,T,D) = \mathrm{Im}(\mathrm{Ev}).$$

It is called *split* if the torus $T$ is split.

We would like to rewrite this definition more constructively. We recall that the usual Frobenius map on $V$ corresponds (by means of $\phi$) to the action $\Phi$ on $V_\Sigma$. At the same time,

$$\mathrm{H}^0(\overline{V},D) \overset{\phi^*}{\xrightarrow{\sim}} \mathrm{H}^0(\overline{V_\Sigma},D), \qquad \mathrm{H}^0(V_\Sigma,D) = \mathbb{F}_q[\{x^m \mid m \in P_D \cap M\}] \quad [92, \text{Prop. } 4.3.3].$$

Therefore $\phi^*$ is an isomorphism of $\mathbb{F}_q$-spaces $\mathrm{H}^0(V,D)$ and

$$\mathcal{L}(P_D,\Phi) := \mathrm{H}^0(\overline{V_\Sigma},D)^{\Phi^*} = \Big\{ \sum c_m x^m \;\Big|\; c_m \in \mathbb{F}_{q^e},\ c_m^q = c_{\Phi(m)} \Big\}.$$

Thus by Lemma 7.5 the code $\mathcal{C}_q(V,T,D)$ is also equal to the image of the evaluation map $\mathcal{L}(P_D,\Phi) \to \mathbb{F}_q^n$ at the points of $\mathrm{E}_q(\Phi)$, which we continue to denote by $P_0,\cdots,P_{n-1}$.

The code $\mathcal{C}_q(V,T,D)$ is non-degenerate and has no repetitions. Indeed, $D$ is a very ample divisor, hence for a basis $f_1,\cdots,f_k$ of $\mathrm{H}^0(V,D)$ the map

$$\varphi_D\colon V \hookrightarrow \mathbb{P}^{k-1}, \qquad \varphi_D(P) = \big(f_1(P) : \cdots : f_k(P)\big)$$

is a well-defined embedding. Therefore $\mathcal{C}_q(V,T,D)$ can be defined as an algebraic geometry (Goppa) code corresponding (in sense of [5, Theorem 1.1.6]) to the projective system $\varphi_D\big(T(\mathbb{F}_q)\big)$ without multiple points. Linearly equivalent divisors define equivalent Goppa codes, which justifies the appearance of the group $\mathrm{TPic}(V,\Phi)$.

**Remark 7.33.** *By definition, length $n$ and dimension $k$ of a code $\mathcal{C}_q(V,T,D)$ are equal to $|T(\mathbb{F}_q)|$ and $|P_D \cap M|$ respectively.*

**Theorem 7.34.** *Let $C = \mathcal{C}_q(V,T,D)$ and $C' = \mathcal{C}_{q^e}(V,\mathbb{G}_m^d,D)$. Then $C = \big(C'_{\mathrm{E}_q(\Phi)}\big)\big|_{\mathbb{F}_q}$. In other words, any toric code $C$ is the successive puncturing [5, §1.1.6] of the split toric code $C'$ at the coordinate set $\mathrm{E}_q(\Phi)$ and the restriction [5, §1.2.3] to $\mathbb{F}_q$.*

*Proof.* The equality follows from easily proved ones

$$C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^e} = C'_{\mathrm{E}_q(\Phi)}, \qquad \big(C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^e}\big)\big|_{\mathbb{F}_q} = C. \qquad \square$$

**Remark 7.35.** *The previous theorem allows us to think about non-split toric codes as high-dimensional analogue of BCH codes [5, §1.2.2]. However, the idea to consider subfield-subcodes of toric codes has already arisen in [165].*

Suppose $O(m_0),\cdots,O(m_{l-1})$ to be all orbits under the action of $\Phi$ on $P_D \cap M$, $k_i = |O(m_i)|$, and $\{b_{i,j}\}_{j=0}^{k_i-1}$ to be a basis of the $\mathbb{F}_q$-space $\mathbb{F}_{q^{k_i}}$. Besides, by $\mathrm{Tr}_{k_i,q}$ we denote the trace map with respect to an extension $\mathbb{F}_{q^{k_i}}/\mathbb{F}_q$.

It is easy to prove

**Lemma 7.36.** *The set*

$$\left\{ \sum_{s=0}^{k_i-1} b_{i,j}^{q^s} x^{\Phi^s(m_i)} \right\}_{i=0,\,j=0}^{l-1,\,k_i-1}$$

*is a basis of the $\mathbb{F}_q$-space $\mathcal{L}(P_D,\Phi)$.*

By Lemma 7.6 and previous one we immediately get

**Theorem 7.37.** *A generator matrix of a code $\mathcal{C}_q(V,T,D)$ has the form*

$$\begin{pmatrix} \mathrm{Tr}_{k_0,q}(b_{0,0}P_0^{m_0}) & \mathrm{Tr}_{k_0,q}(b_{0,0}P_1^{m_0}) & \cdots & \mathrm{Tr}_{k_0,q}(b_{0,0}P_{n-1}^{m_0}) \\ \mathrm{Tr}_{k_0,q}(b_{0,1}P_0^{m_0}) & \mathrm{Tr}_{k_0,q}(b_{0,1}P_1^{m_0}) & \cdots & \mathrm{Tr}_{k_0,q}(b_{0,1}P_{n-1}^{m_0}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_{k_{l-1},q}(b_{l-1,k_{l-1}-1}P_0^{m_{l-1}}) & \mathrm{Tr}_{k_{l-1},q}(b_{l-1,k_{l-1}-1}P_1^{m_{l-1}}) & \cdots & \mathrm{Tr}_{k_{l-1},q}(b_{l-1,k_{l-1}-1}P_{n-1}^{m_{l-1}}) \end{pmatrix}.$$

For the rest of this subsection we will suppose $T(\mathbb{F}_q) = \langle P \rangle \hookrightarrow \mathbb{F}_{q^e}^*$ to be a cyclic group, $P_s = P^s$ for $0 \leqslant s \leqslant n-1$, and $b_{i,j} = b_i^{q^j}$ is a normal basis of $\mathbb{F}_{q^{k_i}}/\mathbb{F}_q$ for $0 \leqslant i \leqslant l-1$. A proof of the following lemma can be easily obtained from that of [5, Proposition 4.1.22].

**Lemma 7.38.** *A code $\mathcal{C}_q(V,T,D)$ is a simple-root (i.e., $p \nmid n$) cyclic one.*

**Theorem 7.39.** *The parity-check polynomial of the cyclic code $\mathcal{C}_q(V,T,D)$ equals*

$$h(x) = \prod_{i=0}^{l-1} h_{P^{-m_i}}(x), \qquad \textit{where} \qquad h_{P^{-m_i}}(x) = \prod_{j=0}^{k_i-1} \left(x - P^{-\Phi^j(m_i)}\right)$$

*is the $\mathbb{F}_q$-minimal polynomial of $P^{-m_i}$.*

*Proof.* By definition, the parity-check polynomial is equal to the quotient of $x^n - 1$ by the generator polynomial $g$. At the same time, $g$ is equal to the greatest common divisor of basis polynomials

$$B_{i,j}(x) = \sum_{s=0}^{n-1} \mathrm{Tr}_{k_i,q}(b_i^{q^j} P^{sm_i}) x^s.$$

Let $n_{i,t} = \mathrm{ord}\left(P^{m_i(q^t-1)}\right)$ and

$$S_t = \sum_{s=0}^{n-1} \left(P^{m_i(q^t-1)}\right)^s = \frac{n}{n_{i,t}} \sum_{s=0}^{n_{i,t}-1} \left(P^{m_i(q^t-1)}\right)^s = \begin{cases} n = \pm 1 & \text{if } n_{i,t} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, $S_0 = n = \pm 1$. Thus

$$B_{i,j}(P^{-m_i}) = \sum_{t=0}^{k_i-1} b_i^{q^{j+t}} S_t \neq 0$$

and $h(P^{-m_i}) = 0$. Finally, $\deg(h_{P^{-m_i}}) = k_i$, hence $\deg(h) = k$, that is we found all roots of the polynomial $h$. □

We recall that a cyclic code is called *reversible* if its generator (or, equivalently, parity-check) polynomial is self-reciprocal.

**Corollary 7.40.** *If $P_D$ is a centrally symmetric polytope (i.e., $-P_D = P_D$), then $\mathcal{C}_q(V, T, D)$ is a reversible code.*

Among centrally symmetric polytopes we want to highlight so-called *del Pezzo polytopes*, which are discussed in [158]. At the same time, the theory of cyclic reversible (or, equivalently, LCD) codes can be found in [99], [166], [167].

### 7.2.2 Toric codes on $\mathbb{P}^1$ and some toric surfaces

Let us keep the notation of §7.1.3.

**Theorem 7.41.** *The codes*

$$\mathrm{RS}_q(r) = \mathcal{C}_q(\mathbb{P}^1, \mathbb{G}_m, rP_y), \qquad \mathrm{PRS}_q(r) = \mathcal{C}_q(\mathbb{P}^1, T_2, \frac{r}{2}D_{x,y})$$

*are all possible (up to an equivalence) toric ones on $\mathbb{P}^1$ and their parameters are represented in Table* 7.3.

| | $n$ | $k$ | $d$ | restrictions | reference |
|---|---|---|---|---|---|
| $\mathrm{RS}_q(r)$ | $q-1$ | $r+1$ | $n-r$ | $0 < r < q-1$ | [5, §1.2.1] |
| $\mathrm{PRS}_q(r)$ | $q+1$ | | | $0 < r < q+1,\ 2 \mid r$ | [5, §4.4.1] |

Table 7.3: Toric codes on $\mathbb{P}^1$

The code $\mathrm{RS}_q(r)$ is known as a (*punctured*) *Reed–Solomon code*. And $\mathrm{PRS}_q(r)$ is equivalent to a so-called *projective* (*doubly extended*) *Reed–Solomon code*, because for even $r$ divisors $rP_y$ and $\frac{r}{2}D_{x,y}$ are equivalent. Moreover, according to Theorem 7.34 it is a BCH code (non-primitive non-narrow sense). Finally, the polytope of $\frac{r}{2}D_{x,y}$ is clearly the closed line segment $[-\frac{r}{2}, \frac{r}{2}]$, hence by Corollary 7.40 the code $\mathrm{PRS}_q(r)$ is reversible.

**Theorem 7.42.** *The codes*

$$\mathrm{SRM}_q(r) = \mathcal{C}_q(\mathbb{P}^2, \mathbb{G}_m^2, rL_z), \quad \mathrm{RM}_q(r) = \mathcal{C}_q(\mathbb{P}^2, T_{2.c}, rL_z), \quad \mathrm{PRM}_q(r) = \mathcal{C}_q(\mathbb{P}^2, T_3, \frac{r}{3}D_{x,y,z})$$

*are all possible (up to an equivalence) toric ones on $\mathbb{P}^2$ and their parameters are represented in Table* 7.4.

| | $n$ | $k$ | $d$ | restrictions | reference |
|---|---|---|---|---|---|
| $\mathrm{SRM}_q(r)$ | $(q-1)^2$ | $\frac{(r+1)(r+2)}{2}$ | $n-r(q-1)$ | $0<r<q-1$ | [94, Th-m 1.3] |
| $\mathrm{RM}_q(r)$ | $q^2-1$ | | $n-rq$ | $0<r<q$ | [168, §2-3] |
| $\mathrm{PRM}_q(r)$ | $q^2+q+1$ | | $n-(rq+1)$ | $0<r<q+1$, $3 \mid r$ | [100, §2] |

Table 7.4: Toric codes on $\mathbb{P}^2$

The code $\mathrm{RM}_q(r)$ is known as a (*punctured*) *Reed–Muller code*. And $\mathrm{PRM}_q(r)$ is equivalent to a so-called *projective Reed–Muller code*, because for $3 \mid r$ divisors $rL_z$ and $\frac{r}{3}D_{x,y,z}$ are equivalent.

**Theorem 7.43.** *The codes*

$$C_1 = \mathcal{C}_q(\mathcal{H}, \mathbb{G}_m^2, r_1L_y + r_2L_v), \quad C_{2.a} = \mathcal{C}_q(\mathcal{H}, T_{2.a}, \frac{r_1}{2}D_{x,y} + \frac{r_2}{2}D_{u,v}),$$

$$C_{2.b} = \mathcal{C}_q(\mathcal{H}, T_{2.b}, r_1L_y + \frac{r_2}{2}D_{u,v}), \quad C_{2.c} = \mathcal{C}_q(\mathcal{E}, T_{2.c}, rD_{y,v}), \quad C_4 = \mathcal{C}_q(\mathcal{E}, T_4, \frac{r}{2}D_{x,y,u,v})$$

*are all possible (up to an equivalence) toric ones on quadratic surfaces and their parameters are represented in Table* 7.5.

| | $n$ | $k$ | $d$ | restrictions | | reference |
|---|---|---|---|---|---|---|
| $C_1$ | $(q-1)^2$ | $(r_1+1)*$ $(r_2+1)$ | $(q-1-r_1)*$ $(q-1-r_2)$ | $0<r_1,r_2<q-1$ | | [94, Th-m 1.4] |
| $C_{2.a}$ | $(q+1)^2$ | | $(q+1-r_1)*$ $(q+1-r_2)$ | $0<r_1,r_2<q+1$, $2 \mid r_1$ | $2 \mid r_2$ | [102, Rem. 3.2] |
| $C_{2.b}$ | $q^2-1$ | | $(q-1-r_1)*$ $(q+1-r_2)$ | $0<r_1<q-1$, $0<r_2<q+1$ | | |
| $C_{2.c}$ | | $(r+1)^2$ | $n-r(q+1)$ | $0<r<q-1$ | | [102, Prop. 4.2] |
| $C_4$ | $q^2+1$ | | | $0<r<q$, $2 \mid r$ | | [102, Prop. 4.7] |

Table 7.5: Toric codes on quadratic surfaces

It is easily proved that

$$C_1 = \mathrm{RS}_q(r_1) \otimes \mathrm{RS}_q(r_2), \quad C_{2.a} = \mathrm{PRS}_q(r_1) \otimes \mathrm{PRS}_q(r_2), \quad C_{2.b} = \mathrm{RS}_q(r_1) \otimes \mathrm{PRS}_q(r_2),$$

where the symbol $\otimes$ denotes the tensor (Kronecker) product of codes. At the same time, $C_{2.c}$ is a primitive narrow-sense BCH code by [102, Proposition 4.2]. Finally, $C_4$ is a reversible code by Corollary 7.40, because the polygon of $\frac{r}{2}D_{x,y,u,v}$ is clearly the closed square $[-\frac{r}{2}, \frac{r}{2}] \times [-\frac{r}{2}, \frac{r}{2}]$.

**Lemma 7.44** ([94, Theorem 1.5]). *All possible (up to an equivalence) split toric codes on Hirzebruch surfaces $\mathbb{F}_m$ for $m > 0$ have the form*

$$\mathcal{C}_q(\mathbb{F}_m, \mathbb{G}_m^2, r_1 S + r_2 F_v), \qquad \text{where} \qquad 0 < r_1, r_2, mr_1 + r_2 < q - 1$$

*and their parameters are equal to*

$$n = (q-1)^2, \qquad k = \frac{(r_1+1)(mr_1+2r_2+2)}{2}, \qquad d = n - (q-1)(mr_1 + r_2).$$

**Remark 7.45.** *The author studied non-split toric codes on Hirzebruch surfaces and came to the conclusion that they are not of great interest.*

### 7.2.3 Toric codes on del Pezzo surfaces of degree 6

We keep the notation of §7.1.4, §7.2.1. Among all del Pezzo surfaces of degree 6 the surface $\mathcal{D}_6$ seems to be the most appropriate for considering on it toric codes, because its splitting field is the largest. In other words, this surface is "the most non-split". For comparison, see non-toric and split toric codes on the surface $\mathcal{D}_1$ in [104] and [169, Example 5.2] respectively.

Let $\beta \in \mathbb{F}_{q^6}^*$ be an element of order $n = q^2 - q + 1$ and $P_\beta = (\beta, \beta^q)$. It is clear that

$$\mathrm{E}_q(\Phi_6) = \langle P_\beta \rangle \simeq \langle \beta \rangle$$

and $P_\beta^{(i,j)} = \beta^{i+jq}$ for $(i,j) \in M$. We also recall that by $h_{\beta^i}$ one denotes the $\mathbb{F}_q$-minimal polynomial of the element $\beta^i$, where $0 \leqslant i \leqslant n-1$.

In the following theorem we use the value $N_q(1)$, that is the maximal possible number of $\mathbb{F}_q$-points on an elliptic curve. It is known that

$$N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor & \text{if } \sqrt{q} \notin \mathbb{N},\ p < q, \text{ and } p \mid \lfloor 2\sqrt{q} \rfloor, \\ q + \lfloor 2\sqrt{q} \rfloor + 1 & \text{otherwise.} \end{cases} \qquad [5, \text{Th-m } 3.4.49]$$

Elliptic curves, for which the number of $\mathbb{F}_q$-points attains $N_q(1)$ are called $\mathbb{F}_q$-*optimal* ($\mathbb{F}_q$-*maximal* if $\sqrt{q} \in \mathbb{N}$). Such curves are interesting in themselves, because algebraic geometry codes on them are so-called *almost MDS codes* with sufficiently large length [5, §4.4.2].

**Theorem 7.46.** *Consider $r \in \mathbb{N}$ such that $rN_q(1) < n$ and for any partition $r = \sum_{i=1}^m r_i > m$ (with $r_i \in \mathbb{N}$) we have the inequality*

$$m(q+1) + \lfloor 2\sqrt{q} \rfloor \sum_{i=1}^{m} g_i \leqslant rN_q(1), \qquad \text{where} \qquad g_i = 3r_i(r_i - 1) + 1.$$

*Then the toric code* $\mathcal{C}_{q,r} = \mathcal{C}_q(\mathcal{D}_6, T_6, rH_0)$ *has parameters*

$$n = q^2 - q + 1, \qquad k = 3r(r+1) + 1, \qquad d \geqslant n - rN_q(1).$$

*Moreover, if in the definition of* $\mathcal{C}_{q,r}$ *the point* $P_\beta$ *is taken as a generator of* $\mathrm{E}_q(\Phi_6)$, *then* $\mathcal{C}_{q,r}$ *is a cyclic reversible code with the parity-check polynomial*

$$h(x) = (x-1) \prod_{\substack{1 \leqslant i;\ 0 \leqslant j \\ i+j \leqslant r}} h_{\beta^{i+jq}}(x).$$

*Proof.* Length $n$ is obvious. First, we will estimate minimal distance $d$. Let $D = \sum_{i=1}^{m} C_i$ be the decomposition into $\mathbb{F}_q$-irreducible components for an element of the linear system $|rH_0|$. Picard group of the surface $\mathcal{D}_6$ is generated by $H_0$, hence $C_i \sim r_i H_0$, $r_i \in \mathbb{N}$, and $\sum_{i=1}^{m} r_i = r$. In particular, arithmetic genus $g_i$ of a curve $C_i$ is equal to $3r_i(r_i-1)+1$ (see, for example, [1, Exercise V.1.3]). Therefore by [170, Theorem 2.3] we obtain:

$$|C_i(\mathbb{F}_q)| \leqslant q + g_i\lfloor 2\sqrt{q} \rfloor + 1.$$

Moreover, if $r = m$ (i.e., $r_i = g_i = 1$ for $1 \leqslant i \leqslant m$), then $|C_i(\mathbb{F}_q)| \leqslant N_q(1)$ by Corollary 7.31. Thus

$$|D(\mathbb{F}_q)| \leqslant \sum_{i=1}^{m} |C_i(\mathbb{F}_q)| \leqslant rN_q(1)$$

and we get the desired bound on $d$, because $T(\mathbb{F}_q) = \mathcal{D}_6(\mathbb{F}_q)$. At the same time, dimension $k$ follows from Lemma 7.27 and the inequality $rN_q(1) < n$.

The cyclicity of $\mathcal{C}_{q,r}$ is true according to Lemma 7.38. The polygon $P_{rH_0} = rP_{H_0}$ (see Figure 7.6 for $r = 1$) is centrally symmetric, therefore the reversibility of $\mathcal{C}_{q,r}$ follows from Corollary 7.40. Finally, we get the desired parity-check polynomial by Lemma 7.27 and Theorem 7.39. □

From the last theorem and Corollary 7.32 we immediately obtain

**Corollary 7.47.** *For* $q \geqslant 5$ *the code* $\mathcal{C}_{q,1}$ *is an* $[n, 7, n - N_q(1)]_q$*-code.*

**Remark 7.48.** *For small* $q$ *the codes* $\mathcal{C}_{q,1}$ *have parameters*

$$[21, 7, 11]_5, \qquad [43, 7, 30]_7, \qquad [57, 7, 43]_8, \qquad [73, 7, 57]_9.$$

*The codes* $\mathcal{C}_{7,1}$, $\mathcal{C}_{8,1}$, $\mathcal{C}_{9,1}$ *have already been found (by a non-exhaustive computer search) in* [171], [172], [173] *respectively. According to the Brouwer–Grassl tables* [174] *they are currently known as the best ones for given* $q$, $n$, $k$. *Thus it seems that codes* $\mathcal{C}_{q,r}$ *(at least for* $r = 1$*) are also sufficiently good for bigger* $q$.

**Remark 7.49.** *By Corollaries* 7.31, 7.32 *and the Deuring–Waterhouse theorem* [5, Theorem 3.3.12] *we know all weights of a code* $\mathcal{C}_{q,1}$ *for* $q \geqslant 5$. *In particular, its codewords of the minimal weight (up to multiplication by an element of* $\mathbb{F}_q^*$*) bijectively correspond to* $\mathbb{F}_q$*-optimal elliptic curves from* $|H_0|$. *However, in this linear system there are many different (as sets) elliptic curves that are* $\mathbb{F}_q$*-isogenous, that is have equal number of* $\mathbb{F}_q$*-points.*

# Chapter 8

# Non-split toric BCH codes on singular del Pezzo surfaces

## 8.1 Toric del Pezzo surfaces and reflexive polygons

Let $\mathbb{F}_q$ be a finite field of characteristic $p$. Consider a toric (possibly singular) *del Pezzo surface* $S$ over $\mathbb{F}_q$, i.e., a toric one, whose anticanonical divisor $-K_S$ is an ample Cartier divisor. Let $\varphi_{min}\colon S' \to S$ be the minimal resolution of singularities. The surface $S'$ is a so-called *weak* (or *generalized*) *del Pezzo surface*. The self-intersection $K_S^2$ is said to be *degree* of $S$ (or $S'$). Besides, the *Fano index* of $S$ is the maximal number $i \in \mathbb{N}$ such that $K_S \sim iH$ for some Cartier divisor $H$ on $S$, which can be taken over $\mathbb{F}_q$. The theory of (not necessarily toric) del Pezzo surfaces (with more focus on $K_S^2 = 3, 4$) can be found, for example, in [101].

**Lemma 8.1** ([92, Proposition 11.2.8], [101, Proposition 0.6], [175, Figure 1])**.**

1. *$-K_S$ is very ample,* $\dim|-K_S| = K_S^2$*, and* $3 \leqslant K_S^2 \leqslant 9$;
2. *The surface $S$ may only have singularities of the types* $\mathrm{A}_1, \mathrm{A}_2, \mathrm{A}_3$ [92, Example 10.1.5];
3. *$\varphi_{min}$ is a crepant morphism, i.e., $K_{S'} := \varphi_{min}^*(K_S)$ is a canonical divisor.*

A lattice convex polygon $P \subset \mathbb{R}^2$ is said to be *reflexive* (or *Gorenstein*) if $O := (0,0)$ is its internal point and the dual (convex) polygon $P^\circ$ is also lattice. In this case, $P^\circ$ is obviously reflexive.

**Lemma 8.2** ([92, Exercise 2.3.5.a, Definition 2.3.12, Theorem 10.5.10])**.** *If $P$ is reflexive, then*

1. *$O$ is the unique internal point of $P$;*

2. *All vertices of $P$ are ray generators of the normal fan of $P^\circ$;*

3. $|P \cap \mathbb{Z}^2| + |P^\circ \cap \mathbb{Z}^2| = 14$.

**Theorem 8.3** ([92, Theorems 6.2.1, 8.3.4]). *The maps*

$$P \mapsto (S_P, D_P) \quad [92, §2.3, §4.2], \qquad (S, -K_S) \mapsto P_{-K_S} \quad [92, §4.3]$$

*are inverse to each other between reflexive polygons (up to an equivalence) and toric (possibly singular) del Pezzo surfaces provided with the anticanonical divisor that is the sum of all prime torus-invariant divisors.*

**Theorem 8.4** ([92, Theorem 8.3.7], [175, Figure 1]). *Up to an equivalence (isomorphism) there are exactly* 16 *reflexive polygons (split toric del Pezzo surfaces).*

It is immediately checked that all reflexive polygons having an action of maximal order greater than 2 are represented in Figure 8.1. For a polygon $Pol_i$ the subscript $i$ is the amount of integral points on its boundary. In turn, the superscript $t$ denotes the transposition operation of $\Phi_i$ as a matrix (of order $i$) in $\mathrm{GL}(2, \mathbb{Z})$. The corresponding non-split toric del Pezzo surfaces (with their Fano index) are contained in Table 8.1. We recall that the action $\Phi_i$ (or $\Phi_i^t$) complies with the Frobenius action on toric invariant curves and points of the surface. Finally, it is notable that all the five surfaces have Picard $\mathbb{F}_q$-number 1.

| № | (polygon, action) | toric surface | Fano index | (polygon$^\circ$, action$^t$) |
|---|---|---|---|---|
| 1 | $(Pol_3, \Phi_3^t)$ | $S_3$ (§8.1.1) | 1 | 5 |
| 2 | $(Pol_4, \Phi_4^t)$ | $S_4$ (§8.1.2) | | 4 |
| 3 | $(Pol_6, \Phi_6)$ | $\mathcal{D}_6$ (§7.1.4) | | 3 (up to an equivalence) |
| 4 | $(Pol_8, \Phi_4)$ | $\mathcal{E}$ (§7.1.3) | 2 | 2 |
| 5 | $(Pol_9, \Phi_3)$ | $\mathbb{P}^2$ | 3 | 1 |

Table 8.1: Toric del Pezzo surfaces with respect to the tori $T_3, T_4, T_6$.

**Lemma 8.5** ([92, Proposition 4.2.5, Exercises 4.3.2, 10.5.7.b]). *We have:*

1. *For $K_S^2 \leqslant 7$ the Fano index of $S$ is equal to* 1;

2. *Any smooth absolutely irreducible curve from $|-K_S|$ is elliptic;*

3. $\mathrm{Pic}(S)$ *is a free abelian group.*

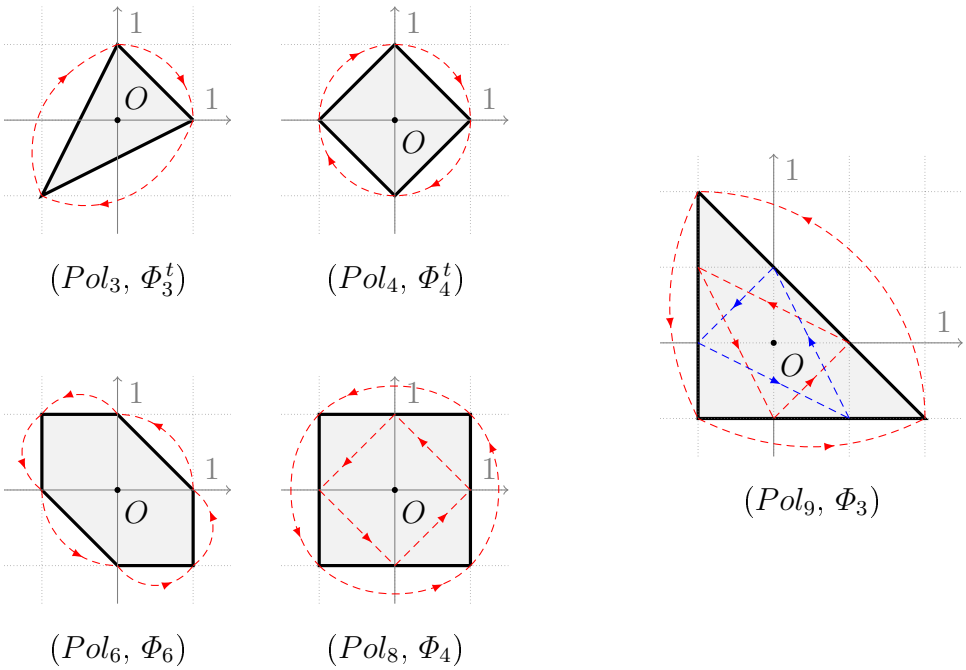


Figure 8.1: All reflexive polygons having an action (from Theorem 7.10) of maximal order greater than 2

### 8.1.1 Toric (singular) cubic surface in $\mathbb{P}^3$

Choose an element $\alpha \in \mathbb{F}_{q^3} \backslash \mathbb{F}_q$ and consider the so-called *norm cubic $\mathbb{F}_q$-surface*

$$S_3 \colon X_0 \cdot X_1 \cdot X_2 = x_3^3 \quad \subset \quad \mathbb{P}^3_{(x_0:x_1:x_2:x_3)} \qquad [159, \text{Example } 1.3.10],$$

where

$$X_0 := x_0 + \alpha x_1 + \alpha^2 x_2, \quad X_1 := x_0 + \alpha^q x_1 + \alpha^{2q} x_2, \quad X_2 := x_0 + \alpha^{q^2} x_1 + \alpha^{2q^2} x_2.$$

For $i \in \mathbb{Z}/3$ let

$$\begin{aligned} &\widehat{L}_i \colon X_i = x_3 = 0, && \widehat{P}_i := \widehat{L}_{i+1} \cap \widehat{L}_{i+2}, \\ &L_i := pr(\widehat{L}_i), && P_i := pr(\widehat{P}_i) = L_{i+1} \cap L_{i+2}, \end{aligned}$$

where $pr \colon S_3 \to \mathbb{P}^2_{(x_0:x_1:x_2)}$ is the well-defined projection of degree 3. Finally, let

$$\widehat{\mathbf{L}}_3 := \sum_{i=0}^{2} \widehat{L}_i, \qquad \mathbf{L}_3 := \sum_{i=0}^{2} L_i, \qquad \text{and} \qquad \mathbf{P}_3 := \{P_i\}_{i=0}^2.$$

**Remark 8.6.** *The surface $S_3$ is toric with respect to the torus $T_3 \simeq S_3 \backslash \{x_3 = 0\}$ (see Theorem 7.10) and the lines $\widehat{L}_i$ (resp. $\widehat{P}_i$) are the unique $T_3$-invariant curves (resp. points) on $S_3$. Moreover, they are $\mathbb{F}_q$-conjugate.*

**Lemma 8.7** ([175, Table 7])**.** *We have:*

1. *The points $\widehat{P}_i$ are the unique singularities on $S_3$ (of type $\mathrm{A}_2$);*
2. *$\varphi_{min} \colon S_3' \to S_3$ is the simultaneous blowing up at them;*
3. *$\widehat{L}_i$ are the unique lines on $S_3$.*

**Theorem 8.8** ([92, Exer. 8.3.8.c], [101, Exam. 0.7.b], [159, Exam. 1.3.10], [175, Table 7])**.**

1. *$S_3$ is the unique (up to an $\mathbb{F}_q$-isomorphism) toric del Pezzo surface of degree 3 with respect to the torus $T_3$;*
2. *$S_3$ is the non-split toric surface associated with the pair $(Pol_3, \Phi_3^t)$;*
3. *$S_3$ is the so-called fake projective plane* [176, Example 1.2]*, i.e., the quotient $\mathbb{P}^2/\sigma$ under a transformation $\sigma \in \mathrm{PGL}(3, \mathbb{F}_q)$ of order 3, whose fixed point set is $\mathbf{P}_3$;*

4. *$S_3'$ is the blowing up of the del Pezzo surface $\mathcal{D}_3$ of degree* 6 (*see* §7.1.4) *at one of the two triples*

$$\mathbf{Q}_3 = \{Q_0, Q_1, Q_2\}, \qquad \mathbf{Q}_3' = \{Q_0', Q_1', Q_2'\}$$

*of $\mathbb{F}_q$-conjugate $T_3$-invariant points.*

*Proof.* All statements can be found in the references, except that the action $\Phi_3^t$ on the polygon $Pol_3$ is the only one of order 3 $\big($up to a conjugation in $\mathrm{Aut}(Pol_3)\big)$. This fact is necessary in order to correctly pass from the split torus case (in those references) to that of $T_3$. □

From Theorem 7.16 or one of Statements 3, 4 of Theorem 8.8 it follows that the Picard $\mathbb{F}_q$-number of $S_3$ is equal to 1. Since the Fano index of $S_3$ is also 1, we obtain

**Lemma 8.9.** *The Picard $\mathbb{F}_q$-group of the surface $S_3$ is equal to*

$$\mathrm{Pic}(S_3) = \langle -K_{S_3} \rangle \simeq \mathbb{Z}.$$

For the sake of definiteness, we choose the triple $\mathbf{Q}_3$ and thus we deal with the diagram

$$S_3 \overset{\varphi_{min}}{\longleftarrow} S_3' \overset{bl_{\mathbf{Q}_3}}{\longrightarrow} \mathcal{D}_3 \overset{bl_{\mathbf{P}_3}}{\longrightarrow} \mathbb{P}^2,$$

where $bl_{\mathbf{Q}_3}$, $bl_{\mathbf{P}_3}$ are the blowing up maps at $\mathbf{Q}_3$, $\mathbf{P}_3$ respectively. Besides, let

$$\varphi := bl_{\mathbf{P}_3} \circ bl_{\mathbf{Q}_3} \circ \varphi_{min}^{-1} \qquad \varphi \colon S_3 \dashrightarrow \mathbb{P}^2.$$

**Corollary 8.10.** *The anticanonical linear system of $S_3$ is equal to*

$$|-K_{S_3}| = \varphi^*(\mathcal{L}) - 2\widehat{\mathbf{L}}_3, \qquad \textit{where} \qquad \mathcal{L} := |\mathbf{L}_3 - \mathbf{P}_3 - \mathbf{Q}_3|$$

*is the (incomplete) linear system of all (possibly reducible or singular) $\mathbb{F}_q$-cubics $C \subset \mathbb{P}^2$ passing through $\mathbf{P}_3$ such that $L_i$ is a tangent of $C$ at $P_{i+1}$ (resp. $P_{i+2}$ for the triple $\mathbf{Q}_3'$).*

For more clarity on what is going on, see Figures 8.2, 8.3, where arrows denote the Frobenius action. In the second figure $E_{P_i}$ are the exceptional curves associated with the points $P_i$ and $\widetilde{L}_i$ (resp. $\widetilde{C}$) are the proper preimages of $L_i$ (resp. $C \neq \mathbf{L}_3$) with respect to $bl_{\mathbf{P}_3}$. As usual, we also use the notations

$$E_{\mathbf{P}_3} := \sum_{i=0}^{2} E_{P_i} \qquad \text{and} \qquad \widetilde{\mathbf{L}}_3 := \sum_{i=0}^{2} \widetilde{L}_i.$$

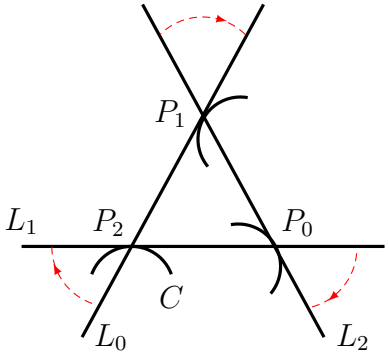


Figure 8.2: The lines $L_i \subset \mathbb{P}^2$ and a cubic $C \in \mathcal{L}$, $C \neq \mathbf{L}_3$

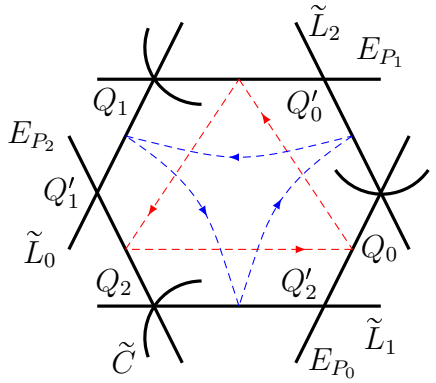


Figure 8.3: The curves $E_{P_i}, \widetilde{L}_i, \widetilde{C} \subset \mathcal{D}_3$

*Proof.* Let us freely use known identities for direct and inverse images of (possibly incomplete) linear systems on algebraic surfaces (see, e.g., [1, §II.5-6, §IV.2]). First,

$$bl^*_{\mathbf{P}_3}\big|\mathbf{L}_3 - \mathbf{P}_3\big| = \big|bl^*_{\mathbf{P}_3}(\mathbf{L}_3) - E_{\mathbf{P}_3}\big| + E_{\mathbf{P}_3} = \big|\widetilde{\mathbf{L}}_3 + E_{\mathbf{P}_3}\big| + E_{\mathbf{P}_3}.$$

Therefore

$$\mathcal{L}^* := bl^*_{\mathbf{P}_3}(\mathcal{L}) = \widetilde{\mathcal{L}} + E_{\mathbf{P}_3}, \qquad \text{where} \qquad \widetilde{\mathcal{L}} := \big|\widetilde{\mathbf{L}}_3 + E_{\mathbf{P}_3} - \mathbf{Q}_3\big|.$$

Next, let $E_{\mathbf{Q}_3}$ be the exceptional divisor associated with the point set $\mathbf{Q}_3$ and $\widetilde{\widetilde{\mathbf{L}}}_3$ (resp. $\widetilde{E}_{\mathbf{P}_3}$) be the proper preimage of $\widetilde{\mathbf{L}}_3$ (resp. $E_{\mathbf{P}_3}$) with respect to $bl_{\mathbf{Q}_3}$. We have:

$$bl^*_{\mathbf{Q}_3}\big(\widetilde{\mathcal{L}}\big) = \big|bl^*_{\mathbf{Q}_3}\big(\widetilde{\mathbf{L}}_3 + E_{\mathbf{P}_3}\big) - E_{\mathbf{Q}_3}\big| + E_{\mathbf{Q}_3} = \widetilde{\widetilde{\mathcal{L}}} + E_{\mathbf{Q}_3},$$

$$\mathcal{L}^{**} := bl^*_{\mathbf{Q}_3}(\mathcal{L}^*) = bl^*_{\mathbf{Q}_3}\big(\widetilde{\mathcal{L}}\big) + bl^*_{\mathbf{Q}_3}(E_{\mathbf{P}_3}) = \widetilde{\widetilde{\mathcal{L}}} + \widetilde{E}_{\mathbf{P}_3} + 2E_{\mathbf{Q}_3},$$

where $\widetilde{\widetilde{\mathcal{L}}} := \big|\widetilde{\widetilde{\mathbf{L}}}_3 + \widetilde{E}_{\mathbf{P}_3} + E_{\mathbf{Q}_3}\big|$.

From the identities

$$(\varphi_{min})_*\Big(\widetilde{\widetilde{\mathbf{L}}}_3\Big) = (\varphi_{min})_*\big(\widetilde{E}_{\mathbf{P}_3}\big) = 0, \qquad (\varphi_{min})_*(E_{\mathbf{Q}_3}) = \hat{\mathbf{L}}_3 \sim -K_{S_3}$$

it follows that

$$\varphi^*(\mathcal{L}) = (\varphi_{min})_*(\mathcal{L}^{**}) = (\varphi_{min})_*\Big(\widetilde{\widetilde{\mathcal{L}}}\Big) + (\varphi_{min})_*\big(\widetilde{E}_{\mathbf{P}_3} + 2E_{\mathbf{Q}_3}\big) = |-K_{S_3}| + 2\hat{\mathbf{L}}_3.$$

Finally, $\mathcal{L}$ has the geometric description declared in the corollary by virtue of [1, Exercise V.3.2]. □

One can easily check that

**Remark 8.11.** *Any $C \in \mathcal{L}$ different from $\mathbf{L}_3$ is an absolutely irreducible (possibly singular) $\mathbb{F}_q$-cubic.*

**Remark 8.12.** *Given $C \in \mathcal{L}$, the divisor $D := \varphi^*(C) - 2\hat{\mathbf{L}}_3$ is an elliptic curve if and only if $C$ is one too. Moreover, in this case $\varphi\colon D \to C$ is an isomorphism.*

**Lemma 8.13.** *Let $E \in \mathcal{L}$ be an elliptic $\mathbb{F}_q$-curve and $\mathcal{O} \in E(\mathbb{F}_{q^3})$ be one of its flexes, which, as is known, always exists over $\mathbb{F}_{q^3}$ (for details see* [177, Chapter 11]*). Then the $P_i$ are points of order 9 (with respect to $\mathcal{O}$ as the neutral element of the chord-tangent group law on $E$) such that $\langle P_0\rangle = \langle P_1\rangle = \langle P_2\rangle$.*

*Proof.* By definition of $\mathcal{L}$ in Corollary 8.10,

$$2P_0 + P_1 \;=\; 2P_1 + P_2 \;=\; 2P_2 + P_0 \;=\; \mathcal{O},$$

hence we see that

$$9P_0 = \mathcal{O}, \qquad 7P_0 = P_1, \qquad 4P_0 = P_2.$$

Similarly, $P_0$, $P_2$ (resp. $P_0$, $P_1$) are expressed through $P_1$ (resp. $P_2$). Finally, the points $P_i$ are of order 9, otherwise they would be equal. □

**Theorem 8.14.** *For any elliptic $\mathbb{F}_q$-curve $E \in |-K_{S_3}|$ the order $|E(\mathbb{F}_q)|$ is divisible by 3.*

*Proof.* The result is proved by exhibiting an $\mathbb{F}_q$-point of order 3 on $E$.

By Remark 8.12 we are in the conditions of the previous lemma, i.e., up to an $\mathbb{F}_q$-isomorphism $E \in \mathcal{L}$. This curve has the group structure with respect to any point $\mathcal{O}' \in E(\mathbb{F}_q) \neq \varnothing$ $\big($instead of a flex $\mathcal{O} \in E(\mathbb{F}_{q^3})\big)$ as the neutral element. It is well known that there is the group $\mathbb{F}_{q^3}$-isomorphism $\tau(P) := P + \mathcal{O}'$, $\tau\colon E \xrightarrow{\sim} E$. At the same time, $E$ has a Weierstrass form $W\colon y^2 + h(x)y = f(x)$ defined over $\mathbb{F}_q$, where $\deg(h) \leqslant 1$, $\deg(f) = 3$. Let $\sigma\colon E \xrightarrow{\sim} W$ be the corresponding $\mathbb{F}_q$-isomorphism such that $\sigma(\mathcal{O}')$ is the point at infinity.

Consider the $\mathbb{F}_{q^3}$-point $(x_0, y_0) := (\sigma \circ \tau)(3P_0)$ of order 3 on $W$. If $x_0 \in \mathbb{F}_q$ (e.g., this is true for $p = 3$), then $y_0 \in \mathbb{F}_{q^3} \cap \mathbb{F}_{q^2} = \mathbb{F}_q$ and all is proved. Otherwise the 3-division polynomial $\psi_3$ (see, e.g., [6, Exercise 3.7]) has exactly two $\mathbb{F}_q$-irreducible factors, namely the $\mathbb{F}_q$-minimal (cubic) polynomial of $x_0$ and $x - x_1$ for some $x_1 \in \mathbb{F}_q$. Note that the 3-torsion subgroup $W[3]$ is generated, for example, by the points $(x_0, y_0)$, $(x_0^q, y_0^q)$. Therefore $W[3] \subset W(\mathbb{F}_{q^3})$ and thus $(x_1, y_1) \in W(\mathbb{F}_q)[3]$ for an appropriate $y_1$. □

**Corollary 8.15.** *For $p = 3$ supersingular elliptic curves (i.e., of $j$-invariant 0)* [5, §2.4.3] *do not belong to $|-K_{S_3}|$.*

Finally, carefully analyzing small values $q$, we get the following result.

**Corollary 8.16.** *For $q \geqslant 3$ and any $\mathbb{F}_q$-divisor $D \in |-K_{S_3}|$ we have*

$$|\mathrm{Supp}(D)(\mathbb{F}_q)| \leqslant 3\lfloor N_q(1)/3 \rfloor,$$

*where the number $N_q(1)$ is given in Theorem* 8.32.

### 8.1.2 Toric (singular) intersection of two quadrics in $\mathbb{P}^4$

Let us fist suppose that $p > 2$. Choose quadratic non-residues $b \in \mathbb{F}_q$ and $a := a_0 + a_1\sqrt{b} \in \mathbb{F}_{q^2}$ (for some $a_0, a_1 \in \mathbb{F}_q$) and consider the following intersection of two $\mathbb{F}_q$-quadrics:

$$S_4 \colon \begin{cases} x_0^2 + bx_1^2 - a_0(y_0^2 + by_1^2) - 2a_1by_0y_1 = z^2, \\ \mathcal{E} \colon 2x_0x_1 - a_1(y_0^2 + by_1^2) - 2a_0y_0y_1 = 0 \end{cases} \quad \subset \quad \mathbb{P}^4_{(x_0:x_1:y_0:y_1:z)}.$$

Note that the affine open subset $U := S_4 \backslash \{z = 0\}$ is the Weil restriction (with respect to the extension $\mathbb{F}_{q^2}/\mathbb{F}_q$) of the $\mathbb{F}_{q^2}$-conic

$$C_2 \colon x^2 - ay^2 = 1 \ \subset \ \mathbb{A}^2_{(x,y)} \qquad \text{if} \qquad x = x_0 + x_1\sqrt{b}, \qquad y = y_0 + y_1\sqrt{b}.$$

At the same time, $C_2$ is isomorphic to the torus $T_2$ (Theorem 7.9).

For $p = 2$ we can take elements $b \in \mathbb{F}_q$, $a \in \mathbb{F}_{q^2}$ such that $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(b) = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(a) = 1$. As is well known, the equation $x^2 + x + b$ (resp. $x^2 + x + a$) has no roots over $\mathbb{F}_q$ (resp. $\mathbb{F}_{q^2}$). Thus there are not any problems to write out the equations of $C_2$ and $S_4$ in even characteristic.

For $i \in \mathbb{Z}/4$ we enumerate the lines $\widehat{L}_i$ of $S_4 \cap \{z = 0\}$ such that $\widehat{P}_i := \widehat{L}_{i+1} \cap \widehat{L}_{i+2}$ is a point. Also, let

$$L_i := pr(\widehat{L}_i), \quad P_i := pr(\widehat{P}_i) = L_{i+1} \cap L_{i+2}, \quad \text{where} \quad pr \colon S_4 \to \mathcal{E} \ \subset \ \mathbb{P}^3_{(x_0:x_1:y_0:y_1)}$$

is the well-defined projection of degree 2 onto the *elliptic quadratic surface* $\mathcal{E}$ (from Table 8.1). Finally, let

$$\widehat{\mathbf{L}}_4 := \sum_{i=0}^{3} \widehat{L}_i \qquad \text{and} \qquad \mathbf{P}_4 := \{P_i\}_{i=0}^3.$$

**Remark 8.17.** *The surface $S_4$ is toric with respect to the torus $T_4 \simeq U$ (see Theorem* 7.10*) and the lines $\widehat{L}_i$ (resp. $\widehat{P}_i$) are the unique $T_4$-invariant curves (resp. points) on $S_4$. Moreover, they are $\mathbb{F}_q$-conjugate.*

Recall that the surface $\mathcal{E}$ is also toric for $T_4$.

**Lemma 8.18** ([175, Table 6]). *We have:*

1. *The points $\widehat{P}_i$ are the unique singularities on $S_4$ (of type $\mathrm{A}_1$);*
2. *$\varphi_{min}\colon S'_4 \to S_4$ is the simultaneous blowing up at them;*
3. *$\widehat{L}_i$ are the unique lines on $S_4$.*

The following theorem is an analogue of Theorem 8.8, hence its statements are proved in a similar way. Unfortunately, we did not find quite exact references.

**Theorem 8.19.** *We have:*

1. *$S_4$ is the unique (up to an $\mathbb{F}_q$-isomorphism) toric del Pezzo surface of degree 4 with respect to the torus $T_4$;*
2. *$S_4$ is the non-split toric surface associated with the pair $(Pol_4, \Phi_4^t)$;*
3. *$S_4$ is the quotient $\mathcal{E}/\sigma$ under an automorphism $\sigma$ of $\mathcal{E}$ $\big($in particular, $\sigma \in \mathrm{PGL}(4,\mathbb{F}_q)\big)$, whose fixed point set is $\mathbf{P}_4$;*
4. *$S'_4$ is the blowing up of $\mathcal{E}$ at the set $\mathbf{P}_4$ of all (i.e., four $\mathbb{F}_q$-conjugate) $T_4$-invariant points.*

From Theorem 7.16 or one of Statements 3, 4 of Theorem 8.19 it follows that the Picard $\mathbb{F}_q$-number of $S_4$ is equal to 1. Since the Fano index of $S_4$ is also 1, we obtain

**Lemma 8.20.** *The Picard $\mathbb{F}_q$-group of the surface $S_4$ is equal to*

$$\mathrm{Pic}(S_4) = \langle -K_{S_4} \rangle \simeq \mathbb{Z}.$$

It is well known that besides $T_4$ the surface $\mathcal{E}$ is toric for the torus $T_{2.c}$ (from Theorem 7.10). Let $M_i$ be the lines outside $T_{2.c}$ and $R_i$ be their intersection points. The blowing up of $\mathcal{E}$ at the $\mathbb{F}_q$-point $R_0$ (or $R_2$) gives the nonsingular del Pezzo surface $\mathcal{D}_7$ of degree 7, which is also the blowing up of $\mathbb{P}^2$ at a pair $\mathbf{Q}_2 = \{Q_1, Q_2\}$ of $\mathbb{F}_q$-conjugate points. Thus we have the diagram

$$S_4 \overset{\varphi_{min}}{\longleftarrow} S'_4 \overset{bl_{\mathbf{P}_4}}{\longrightarrow} \mathcal{E} \overset{bl_{R_0}}{\longleftarrow} \mathcal{D}_7 \overset{bl_{\mathbf{Q}_2}}{\longrightarrow} \mathbb{P}^2,$$

where $bl_{\mathbf{P}_4}$, $bl_{R_0}$, $bl_{\mathbf{Q}_2}$ are the corresponding blowing up maps. Besides, let

$$\chi := bl_{\mathbf{P}_4} \circ \varphi_{min}^{-1} \qquad \chi\colon S_4 \dashrightarrow \mathcal{E}, \qquad\qquad \psi := bl_{\mathbf{Q}_2} \circ bl_{R_0}^{-1} \qquad \psi\colon \mathcal{E} \dashrightarrow \mathbb{P}^2,$$

$$\varphi := \psi \circ \chi \qquad \varphi\colon S_4 \dashrightarrow \mathbb{P}^2.$$

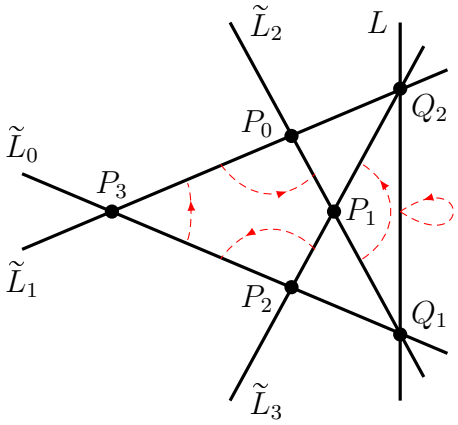


Figure 8.4: The lines $\widetilde{L}_i, L \subset \mathbb{P}^2$

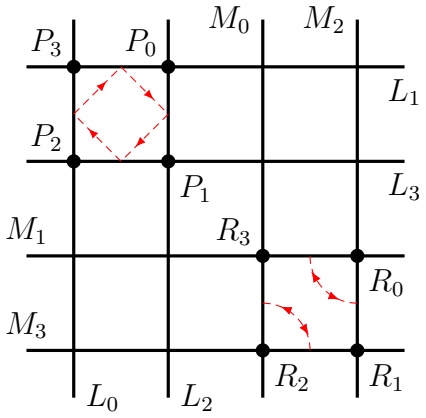


Figure 8.5: The lines $L_i, M_i \subset \mathcal{E}$

Further,

$$\widehat{M}_i := \chi^*(M_i), \qquad \widehat{\mathbf{M}}_2 := \widehat{M}_1 + \widehat{M}_2, \qquad \widetilde{L}_i := \psi_*(L_i), \qquad \widetilde{\mathbf{L}}_4 := \sum_{i=0}^{3} \widetilde{L}_i.$$

Finally, $L$ is the line through the points $Q_j = \psi(M_j)$ and also we identify $P_i$ with $\psi(P_i)$. For more clarity on what is going on, see Figures 8.4, 8.5, where arrows denote the Frobenius action.

Repeating the arguments used for the proof of Corollary 8.10, we obtain the following result. Let us not write out its proof, because it is also very technical and does not contain new ideas.

**Corollary 8.21.** *The anticanonical linear system of $S_4$ is equal to*

$$|-K_{S_4}| = \varphi^*(\mathcal{L}) - \hat{\mathbf{L}}_4 - 2\widehat{\mathbf{M}}_2, \qquad \textit{where} \qquad \mathcal{L} := |\widetilde{\mathbf{L}}_4 - \mathbf{P}_4 - 2\mathbf{Q}_2|$$

*is the (incomplete) linear system of all (possibly reducible or singular) quartics $C \subset \mathbb{P}^2$ passing through $\mathbf{P}_4$ and through $\mathbf{Q}_2$ with multiplicity at least 2.*

One can easily check that

**Remark 8.22.** *Any $C \in \mathcal{L}$ contains at most one absolutely irreducible $\mathbb{F}_q$-curve (of geometric genus $g \leqslant 1$) different from $L$.*

**Remark 8.23.** *Given $C \in \mathcal{L}$, the divisor $D := \varphi^*(C) - \hat{\mathbf{L}}_4 - 2\widehat{\mathbf{M}}_2$ is an elliptic curve if and only if $C$ is one of the following quartics:*

1. *$E \cup L$, where $E \subset \mathbb{P}^2$ is an elliptic curve passing through $\mathbf{P}_4, \mathbf{Q}_2$;*

2. *An irreducible quartic for which $Q_1, Q_2$ are the unique singularities (namely nodes).*

*Moreover, in the first case $\varphi\colon D \to E$ is an isomorphism and in the second one $\varphi\colon D \to C$ is the blowing up at $\mathbf{Q}_2$ such that $|\varphi^{-1}(Q_j)| = 2$.*

**Lemma 8.24.** *Let $E \subset \mathbb{P}^2$ be an elliptic $\mathbb{F}_q$-curve passing through $\mathbf{P}_4, \mathbf{Q}_2$ and $\mathcal{O} \in E(\mathbb{F}_q)$. Then*

$$P_0 - P_2 = P_1 - P_3 = Q_1 - Q_2$$

*is an $\mathbb{F}_q$-point of order 2 (with respect to $\mathcal{O}$ as the neutral element of the chord-tangent group law on $E$).*

*Proof.* By definition,

$$P_0 + P_1 + Q_1 \;=\; P_1 + P_2 + Q_2 \;=\; P_2 + P_3 + Q_1 \;=\; P_3 + P_0 + Q_2.$$

Therefore

$$P_0 + P_1 = P_2 + P_3, \qquad P_1 + P_2 = P_3 + P_0, \qquad P_0 + Q_2 = P_2 + Q_1$$

and hence

$$P_0 - P_2 \;=\; P_3 - P_1 \;=\; P_2 - P_0 \;=\; Q_2 - Q_1.$$

This is an $\mathbb{F}_q$-point, because $Q_1, Q_2$ are $\mathbb{F}_q$-conjugate. □

A quartic $C \in \mathcal{L}$ from Remark 8.23.2 gives a geometric interpretation of the group law on the elliptic curve $D$. Note that $C$ is similar to a (*twisted*) *Edwards quartic* [178], because both curves have two nodes. The group law on the latter is represented in [179, §4]. An analog for $C$ is defined in the following way.

For points $R_1, R_2 \in C \backslash \mathbf{Q}_2$ let $R_1 \cdot R_2$ be the eighth intersection point of $C$ with the unique conic passing through $R_1, R_2, P_1, Q_1, Q_2$. If $R_1 = R_2$ (resp. $R_1 = P_1$ or $R_2 = P_1$), then this conic intersects $C$ at $R_1$ (resp. $P_1$) with the intersection number at least 2 (3 if $R_1 = R_2 = P_1$). Besides, let $\overline{R_1}$ be the third intersection point of $C$ with the unique line passing through $R_1, Q_2$. The points $R_1 \cdot R_2$ and $\overline{R_1}$ are correctly defined by [47, §3.3, §5.3]. Then the addition and subtraction (with $P_0$ as the neutral point) have the form

$$R_1 + R_2 := \overline{R_1 \cdot R_2}, \qquad -R_1 := R_1 \cdot P_3$$

respectively. This can be proved in the same way as [179, Theorem 2]. Note that sometimes $R_1 + R_2$ or $-R_1$ falls into $\mathbf{Q}_2$. Finally, $P_2$ is obviously a point of order 2.

**Theorem 8.25.** *For any elliptic $\mathbb{F}_q$-curve $E \in |-K_{S_4}|$ the order $|E(\mathbb{F}_q)|$ is even.*

*Proof.* The result is proved by exhibiting an $\mathbb{F}_q$-point of order 2 on $E$.

By Lemma 8.24 it remains to only consider the case with a quartic $C \in \mathcal{L}$ from Remark 8.23.2. The corresponding elliptic curve $D$ has the group structure with respect to any point $\mathcal{O} \in D(\mathbb{F}_q) \neq \varnothing$ $\big($instead of $\varphi^{-1}(P_0)\big)$ as the neutral element. It is well known that there is the group $\mathbb{F}_{q^4}$-isomorphism $\tau(P) := P + \mathcal{O}$, $\tau\colon D \xrightarrow{\sim} D$. At the same time, $D$ has a Weierstrass form $W\colon y^2 + h(x)y = f(x)$ defined over $\mathbb{F}_q$, where $\deg(h) \leqslant 1$, $\deg(f) = 3$. Let $\sigma\colon D \xrightarrow{\sim} W$ be the corresponding $\mathbb{F}_q$-isomorphism such that $\sigma(\mathcal{O})$ is the point at infinity.

Consider the $\mathbb{F}_{q^4}$-point $(x_0, y_0) := (\sigma \circ \tau \circ \varphi^{-1})(P_2)$ of order 2 on $W$. For $p = 2$ it is the only such point, hence it is defined over $\mathbb{F}_q$. For $p > 3$, as is known, $y_0 = f(x_0) = 0$. If $x_0 \in \mathbb{F}_q$, then all is proved. Otherwise $f(x)$ has exactly two $\mathbb{F}_q$-irreducible factors, namely the $\mathbb{F}_q$-minimal (quadratic) polynomial of $x_0$ and $x - x_1$ for some $x_1 \in \mathbb{F}_q$. Thus $(x_1, 0) \in W(\mathbb{F}_q)[2]$. □

**Corollary 8.26.** *For $p = 2$ supersingular elliptic curves (i.e., of $j$-invariant 0) [5, §2.4.3] do not belong to $|-K_{S_4}|$.*

Finally, carefully analyzing small values $q$, we get the following result.

**Corollary 8.27.** *For any $\mathbb{F}_q$-divisor $D \in |-K_{S_4}|$ we have*

$$|\mathrm{Supp}(D)(\mathbb{F}_q)| \leqslant 2\lfloor N_q(1)/2 \rfloor,$$

*where the number $N_q(1)$ is given in Theorem 8.32.*

## 8.2 BCH codes

Let us recall some notions of *BCH codes* over an arbitrary finite field $\mathbb{F}_q$. Let $n, d^*, b \in \mathbb{N}$, where $d^*$ is so-called *designed distance*. Also, let $\alpha$ be a primitive $n$-th root of unity and $e := [\mathbb{F}_q(\alpha) : \mathbb{F}_q]$. $\mathrm{BCH}_q(n, d^*, b)$ is a cyclic code given by the generator polynomial

$$g := \mathrm{LCM}(m_{\alpha^b}, m_{\alpha^{b+1}}, \cdots, m_{\alpha^{b+d^*-2}}),$$

where $m_{\alpha^i}$ is the $\mathbb{F}_q$-minimal polynomial of $\alpha^i$. A BCH code is said to be *primitive* (resp. *narrow-sense*) if $n = q^e - 1$ (resp. $b = 1$). The theory of BCH codes is well represented, for example, in [3, §9].

**Theorem 8.28** ([13, Theorem 9.1.a])**.** *For a $\mathrm{BCH}_q(n, d^*, b)$ code we have*

$$k \geqslant n - e(d^* - 1), \qquad d \geqslant d^*.$$

The second inequality is called the *BCH bound*.

**Theorem 8.29** ([13, Proposition 2.3.9]). *Let*

$$r := b - 1, \qquad s := n + 1 - d^* - b, \qquad P_0 := (0:1), \qquad P_\infty := (1:0).$$

*A* $\mathrm{BCH}_q(n, d^*, b)$ *code is obtained by the successive puncturing of the split toric code* $\mathcal{C}_{q^e}(\mathbb{P}^1, \mathbb{G}_m, rP_0 + sP_\infty)$ *(see the notation in* §7.2.1*) at the coordinate set* $\sqrt[n]{1} = \langle\alpha\rangle$ *and the restriction to* $\mathbb{F}_q$*. As a result, BCH codes are independent (up to an equivalence) of choosing* $\alpha$*.*

**Corollary 8.30.** *A primitive narrow-sense* $\mathrm{BCH}_q(q^e - 1, d^*, 1)$ *code is the restriction to* $\mathbb{F}_q$ *of the Reed–Solomon* $\mathbb{F}_{q^e}$*-code of length* $q^e - 1$ *and dimension* $q^e - d^*$*.*

## 8.3 Codes associated with the "symmetric" polygons

Next we will need the following facts.

**Theorem 8.31** (Griesmer bound [5, Theorem 1.1.43]). *For any linear* $[n, k, d]_q$ *code we have*

$$\delta := n - \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil \geqslant 0.$$

**Theorem 8.32** ([5, Theorem 3.4.49]). *The maximal possible number of* $\mathbb{F}_q$*-points on an elliptic* $\mathbb{F}_q$*-curve is equal to*

$$N_q(1) = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor & \text{if } \sqrt{q} \notin \mathbb{N},\ p < q,\ \text{and } \ p \mid \lfloor 2\sqrt{q} \rfloor, \\ q + \lfloor 2\sqrt{q} \rfloor + 1 & \text{otherwise.} \end{cases}$$

For small $q$ Table 8.2 (the original source is [180]) contains Weierstrass forms of $\mathbb{F}_q$-optimal elliptic curves, i.e., having $N_q(1)$ points over $\mathbb{F}_q$. According to [181, Theorem 4.6, Table I] these curves are unique (up to $\mathbb{F}_q$-isomorphism) among $\mathbb{F}_q$-optimal. The last column of the table is filled by [181, Proposition 3.6.iv].

For $i \in \{3, 4, 6, 8, 9\}$ by $\mathcal{C}_i$ we will denote the non-split toric $\mathbb{F}_q$-code associated with the polygon $Pol_i$ from Figure 8.1. In other words, $\mathcal{C}_i$ are anticanonical codes on the non-split toric del Pezzo $\mathbb{F}_q$-surfaces from Table 8.1. In particular, $\mathcal{C}_9$ is equivalent to the so-called *projective Reed–Muller code*. The code parameters are represented in Table 8.3 (for a value $q$ satisfying the restriction). The bound on $d$ for the new codes $\mathcal{C}_3$, $\mathcal{C}_4$ follows from Corollaries 8.16, 8.27. Be careful that for very small $q$ (even if the restriction is satisfied) values of the column $\delta$ may be incorrect.

| $q$ | $N_q(1)$ | elliptic $\mathbb{F}_q$-curve | $j$-invariant | is supersingular |
|---|---|---|---|---|
| 2 | 5 | $y^2+y=x^3+x$ | 0 | yes |
| 3 | 7 | $y^2=x^3+2x+1$ | 0 | yes |
| 4 | 9 | $y^2+y=x^3$ | 0 | yes |
| 5 | 10 | $y^2=x^3+3x$ | 1728 | no |
| 7 | 13 | $y^2=x^3+3$ | 0 | no |
| 8 | 14 | $y^2+xy+y=x^3+1$ | 1 | no |
| 9 | 16 | $y^2=x^3+x$ | 0 | yes |

Table 8.2: $\mathbb{F}_q$-optimal elliptic curves for small $q$

| code | $n$ | $k$ | $d$ | restriction | $\delta$ | reference |
|---|---|---|---|---|---|---|
| $\mathcal{C}_3$ | $q^2+q+1$ | 4 | $\geqslant n-3\lfloor N_q(1)/3\rfloor$ | $3\leqslant q$ | $\leqslant 3\lfloor N_q(1)/3\rfloor-q-2$ | new codes |
| $\mathcal{C}_4$ | $q^2+1$ | 5 | $\geqslant n-2\lfloor N_q(1)/2\rfloor$ | | $\leqslant 2\lfloor N_q(1)/2\rfloor-q-2$ | |
| $\mathcal{C}_6$ | $q^2-q+1$ | 7 | $n-N_q(1)$ | $5\leqslant q$ | $N_q(1)-q-3$ | Cor. 7.47 |
| $\mathcal{C}_8$ | $q^2+1$ | 9 | $n-2(q+1)$ | $3\leqslant q$ | $q-3$ | [102, Prop. 4.7] |
| $\mathcal{C}_9$ | $q^2+q+1$ | 10 | $n-(3q+1)$ | $5\leqslant q$ | $2q-5$ | [100, §2] |

Table 8.3: The non-split toric codes on the polygons of Figure 8.1

For $n,i\in\mathbb{N}$ let $\alpha\in\overline{\mathbb{F}_q}$ be an element of order $n$ and $m_{\alpha^i}$ be the $\mathbb{F}_q$-minimal polynomial of $\alpha^i$. In Table 8.4 by means of Theorem 7.39 it is written the parity-check polynomials $h(x)$ of the codes from Table 8.3. It is immediately checked that these codes are $\mathrm{BCH}_q(n,d^*,b)$ ones. Finally, the column LCD answers whether a cyclic code is a *linear code with complementary dual* (or, equivalently, *reversible*) or not (details see in [167]). It is filled, looking at $h(x)$, but "yes" also follows from Corollary 7.40 or [3, Problem 7.27]. As a result, the dual codes to $\mathcal{C}_4$, $\mathcal{C}_6$ are $\mathrm{BCH}_q(n,4,n-1)$ codes.

The output of the code [182] written in the language of the CAS Magma motivates us to formulate

**Conjecture 8.33.** *The lower bounds from Table* 8.3 *for the minimum distance $d$ of the codes $\mathcal{C}_3$, $\mathcal{C}_4$ are exact.*

The codes $\mathcal{C}_3$, $\mathcal{C}_4$ for small $q$ are represented in Tables 8.5, 8.6. The column $\mathrm{LB}(d)$ (lower bound on $d$ for fixed $q$, $n$, $k$) is rewritten from the Brouwer–Grassl tables

| code | $h(x)$ | $d^*$ | $b$ | $d - d^*$ | LCD |
|---|---|---|---|---|---|
| $\mathcal{C}_3$ | $(x-1)\cdot m_\alpha$ | $q^2-q$ | $q+1$ | $\geqslant 2q+1-3\lfloor N_q(1)/3\rfloor$ | no |
| $\mathcal{C}_4$ | | $q^2-2q+1$ | | $\geqslant 2q-2\lfloor N_q(1)/2\rfloor$ | yes |
| $\mathcal{C}_6$ | | $q^2-3q+1$ | | $2q-N_q(1)$ | yes |
| $\mathcal{C}_8$ | $(x-1)\cdot m_\alpha \cdot m_{\alpha^{q+1}}$ | $q^2-2q-1$ | $q+2$ | 0 | yes |
| $\mathcal{C}_9$ | $(x-1)\cdot m_\alpha \cdot m_{\alpha^{q+1}} \cdot m_{\alpha^{q+2}}$ | $q^2-2q-2$ | $q+3$ | 2 | no |

Table 8.4: The parity-check polynomials (the restrictions as in Table 8.3)

[174]. Note that $\mathcal{C}_3$ for $q=3$ and $\mathcal{C}_4$ for $q=7$ (cf. [183]) have parameters that are the best known at the moment.

| $q$ | $n$ | $k$ | $d$ | LB($d$) |
|---|---|---|---|---|
| 3 | 13 | 4 | 7 | 7 |
| 4 | 21 | | 12 | 14 |
| 5 | 31 | | 22 | 23 |
| 7 | 57 | | 45 | 47 |
| 8 | 73 | | 61 | 62 |
| 9 | 91 | | 76 | 79 |

Table 8.5: The code $\mathcal{C}_3$ for small $q$

| $q$ | $n$ | $k$ | $d$ | LB($d$) |
|---|---|---|---|---|
| 3 | 10 | 5 | 4 | 5 |
| 4 | 17 | | 9 | 10 |
| 5 | 26 | | 16 | 17 |
| 7 | 50 | | 38 | 38 |
| 8 | 65 | | 51 | 52 |
| 9 | 82 | | 66 | 67 |

Table 8.6: The code $\mathcal{C}_4$ for small $q$

**Remark 8.34.** *The codes $\mathcal{C}_3$, $\mathcal{C}_4$ can be naturally generalized, using for any $r \in \mathbb{N}$ the multiple polygons $rPol_3$, $rPol_4$ as well as it is done for $\mathcal{C}_6$ in Theorem 7.46. However, in this case it seems that there are no elegant ways to quite exactly estimate the minimum distance $d$.*

# Bibliography


[1] Hartshorne R. *Algebraic geometry.* — Berlin.: Springer, 1977.

[2] Galbraith S. *Mathematics of public key cryptography.* — New York.: Cambridge University Press, 2012.

[3] MacWilliams F., Sloane N. *The theory of error-correction codes.* — Amsterdam.: North Holland, 1977.

[4] Cohen H. et al. *Handbook of elliptic and hyperelliptic curve cryptography.* — Boca Raton.: Chapman & Hall, 2006.

[5] Tsfasman M., Vlăduţ S., Nogin D. *Algebraic geometric codes: Basic notions.* — Providence.: American Mathematical Society, 2007.

[6] Silverman J. *The arithmetic of elliptic curves.* — New York.: Springer, 2009.

[7] El Mrabet N., Joye M. *Guide to pairing-based cryptography.* — New York.: Chapman & Hall, 2016.

[8] Koblitz N., Menezes A. *Cryptocash, cryptocurrencies, and cryptocontracts.* // Designs, Codes and Cryptography, 2016. Vol. 78(1). P. 87–102.

[9] De Feo L. *Mathematics of isogeny based cryptography.* // arXiv preprint 1711.04062, 2017.

[10] Bernstein D., Buchmann J., Dahmen E. *Post-quantum cryptography.* — Berlin.: Springer, 2009.

[11] Tsfasman M., Vlăduţ S., Nogin D. *Algebraic geometry codes: Advanced chapters.* — Providence.: American Mathematical Society, 2019.

[12] Martinez-Moro E., Munuera C., Ruano D. *Advances in algebraic geometry codes.* — Singapore.: World Scientific, 2008.

[13] Stichtenoth H. *Algebraic function fields and codes.* — Berlin.: Springer, 2008.

[14] Koshelev D. *Non-split toric codes.* // Problems of Information Transmission, 2019. Vol. 55(2). P. 124–144.

[15] Koshelev D. *Hashing to elliptic curves of $j = 0$ and Mordell–Weil groups.* // Mathematical Notes, 2020. Vol. 108(5). P. 748–751.

[16] Koshelev D. *Non-split toric BCH codes on singular del Pezzo surfaces.* // IEEE Transactions on Information Theory, 2020. Vol. 66(12). P. 7341–7347.

[17] Koshelev D. *New point compression method for elliptic $\mathbb{F}_{q^2}$-curves of $j$-invariant* 0. // Finite Fields and Their Applications, 2021.

[18] Bos J. et al. *Elliptic curve cryptography in practice.* // International Conference on Financial Cryptography and Data Security, 2014. P. 157–175.

[19] Dudeanu A., Oancea G.-R., Iftene S. *An x-coordinate point compression method for elliptic curves over $\mathbb{F}_p$.* // SYNASC, 2010. P. 65–71.

[20] Eagle P., Galbraith S., Ong J. *Point compression for Koblitz elliptic curves.* // Advances in Mathematics of Communications, 2011. Vol. 5(1). P. 1–10.

[21] Seroussi G. *Compact representation of elliptic curve points over $\mathbb{F}_{2^n}$.* // HP Labs Technical Reports, 1998.

[22] Duursma I., Gaudry P., Morain F. *Speeding up the discrete log computation on curves with automorphisms.* // Asiacrypt, 1999. P. 103–121.

[23] Open Mobile Alliance, *Wireless Application Protocol Wireless Transport Layer Security (WAP WTLS) Specification*, 2001.

[24] SECG, *SEC* 2: *Recommended elliptic curve domain parameters. Version 2.0.* // Standards for Efficient Cryptography, 2010.

[25] *Secp256k1.* // BitcoinWiki, https://en.bitcoin.it/wiki/Secp256k1.

[26] Gallant R., Lambert R., Vanstone S. *Faster point multiplication on elliptic curves with efficient endomorphisms.* // Annual International Crypto. Conference, 2001. P. 190–200.

[27] Hu Z., Longa P., Xu M. *Implementing 4-dimensional GLV method on GLS elliptic curves with j-invariant 0.* // Designs, Codes and Cryptography, 2012. Vol. 63(3). P. 331–343.

[28] Galbraith S., Lin X., Scott M. *Endomorphisms for faster elliptic curve cryptography on a large class of curves.* // Journal of Cryptology, 2011. Vol. 24(3). P. 446–469.

[29] Costello C., Longa P. *Four$\mathbb{Q}$: Four-dimensional decompositions on a $\mathbb{Q}$-curve over the Mersenne prime.* // Asiacrypt, 2015. P. 214–235.

[30] Longa P., Sica F. *Four-dimensional Gallant–Lambert–Vanstone scalar multiplication.* // Journal of Cryptology, 2014. Vol. 27(2). P. 248–283.

[31] Shamir A. *Identity-based cryptosystems and signature schemes.* // Workshop on the Theory and Application of Cryptographic Techniques, 1985. P. 47–53.

[32] Costello C. *Fast formulas for computing cryptographic pairings,* https:// eprints.qut.edu.au/61037/1/Craig_Costello_Thesis.pdf, 2012.

[33] IEEE Computer Society, *Standard (Std 1363.3) for identity based cryptographic techniques using pairings.* // IEEE Standard Specifications for Public-Key Cryptography, 2013.

[34] ISO/IEC, *Cryptographic techniques based on elliptic curves (ISO/IEC 15946)*, 2017.

[35] ISO/IEC, *Key management — Part 3: Mechanisms using asymmetric techniques (ISO/IEC 11770-3)*, 2015.

[36] Lindemann R. et al. *FIDO ECDAA algorithm*, 2018.

[37] W3C, *Web Authentication: An API for accessing public key credentials*, 2019.

[38] Bowe S. *BLS12-381: New zk-SNARK elliptic curve construction.* // Zcash Company blog, https://z.cash/blog/new-snark-curve/.

[39] Brickell E., Li J. *Enhanced privacy ID from bilinear pairing for hardware authentication and attestation.* // IEEE Second Inter. Conference on Social Computing, 2010. P. 768–775.

[40] Ethereum Foundation, *Program code*, https://github.com/ethereum/.

[41] Freeman D., Scott M., Teske E. *A taxonomy of pairing-friendly elliptic curves.* // Journal of Cryptology, 2010. Vol. 23(2). P. 224–280.

[42] Barreto P., Naehrig M. *Pairing-friendly elliptic curves of prime order.* // International Workshop on Selected Areas in Cryptography, 2006. P. 319–331.

[43] Naehrig M. *Constructive and computational aspects of cryptographic pairings*, https://research.tue.nl/en/publications/constructive-and-computational-aspects-of-cryptographic-pairings, 2009.

[44] Barreto P., Lynn B., Scott M. *Constructing elliptic curves with prescribed embedding degrees.* // Inter. Conference on Security in Communication Networks, 2002. P. 257–267.

[45] Adj G., Rodríguez-Henríquez F. *Square root computation over even extension fields.* // IEEE Transactions on Computers, 2013. Vol. 63(11). P. 2829–2841.

[46] Cho G. et al. *New cube root algorithm based on the third order linear recurrence relations in finite fields.* // Designs, Codes and Cryptography, 2015. Vol. 75(3). P. 483–495.

[47] Fulton W. *Algebraic curves: An introduction to algebraic geometry.* — Boston.: Addison-Wesley, 1969.

[48] Frey G. *Applications of arithmetical geometry to cryptographic constructions.* // International Conference on Finite Fields and Applications, 2001. P. 128–161.

[49] Iskovskih V. *Rational surfaces with a pencil of rational curves.* // Mathematics of the USSR-Sbornik, 1967. Vol. 3(4). P. 563–587.

[50] Iskovskih V. *Rational surfaces with a pencil of rational curves and with positive square of the canonical class.* // Mathematics of the USSR-Sbornik, 1970. Vol. 12(1). P. 91–117.

[51] Groth J. *On the size of pairing-based non-interactive arguments.* // Eurocrypt, 2016. P. 305–326.

[52] Khabbazian M., Gulliver T., Bhargava V. *Double point compression with applications to speeding up random point multiplication.* // IEEE Transactions on Computers, 2007. Vol. 56(3). P. 305–313.

[53] Liedtke C. *Algebraic surfaces in positive characteristic.* // Birational Geometry, Rational Curves, and Arithmetic. — Springer, New York, 2013. P. 229–292.

[54] Koshelev D. *On rationality of Kummer surfaces over the field of two elements in the context of the discrete logarithm problem* (in russian), https://www.hse.ru/en/edu/vkr/206737687, 2017.

[55] Aranha D., Beuchat J., Detrey J., Estibals N. *Optimal Eta pairing on supersingular genus-2 binary hyperelliptic curves.* // Crypto. Track at the RSA Conference, 2012. P. 98–115.

[56] Sakemi Y., Kobayashi T., Saito T., Wahby R. *Pairing-friendly curves.* // IETF Secretariat, 2020.

[57] Faz-Hernandez A. et al. *Hashing to elliptic curves.* // IETF Secretariat, 2020.

[58] Boneh D., Franklin M. *Identity-based encryption from the Weil pairing.* // SIAM Journal on Computing, 2003. Vol. 32(3). P. 586–615.

[59] Icart T. *How to hash into elliptic curves.* // Annual International Cryptology Conference, 2009. P. 303–316.

[60] Bernstein D., Hamburg M., Krasnova A., Lange T. *Elligator: Elliptic-curve points indistinguishable from uniform random strings.* // ACM CCS, 2013. P. 967–980.

[61] Skałba M. *Points on elliptic curves over finite fields.* // Acta Arithmetica, 2005. Vol. 117. P. 293–301.

[62] Mordell L. *Diophantine equations.* — London.: Academic Press, 1969.

[63] Shallue A., van de Woestijne C. *Construction of rational points on elliptic curves over finite fields.* // International Algorithmic Number Theory Symposium, 2006. P. 510–524.

[64] Sendra J., Winkler F., Pérez-Díaz S. *Rational algebraic curves: A computer algebra approach.* — Berlin.: Springer, 2008.

[65] van der Geer G., Katsura T. *On the height of Calabi–Yau varieties in positive characteristic.* // Documenta Mathematica, 2003. Vol. 8(1). P. 97–113.

[66] Andreatta M., Wiśniewski J. *On the Kummer construction.* // Revista Matemática Complutense, 2010. Vol. 23(1). P. 191–215.

[67] Cynk S., Schütt M. *Generalised Kummer constructions and Weil restrictions.* // Journal of Number Theory, 2009. Vol. 129(8). P. 1965–1975.

[68] Donten M. *On Kummer 3-folds.* // Revista Matemática Complutense, 2011. Vol. 24(2). P. 465–492.

[69] Kollár J., Larsen M. *Quotients of Calabi–Yau varieties.* // Algebra, Arithmetic, and Geometry. — Birkhäuser, Boston, 2009. P. 179–211.

[70] Debarre O. *Higher-dimensional algebraic geometry.* — Berlin.: Springer, 2001.

[71] Voisin C. *Miroir set involutions sur les surfaces K3.* // Astérisque, 1993. Vol. 218. P. 273–323.

[72] Bogomolov F., Tschinkel Y. *Rational curves and points on K3 surfaces.* // American Journal of Mathematics, 2005. Vol. 127(4). P. 825–835.

[73] Brier E. et al. *Efficient indifferentiable hashing into ordinary elliptic curves.* // Annual Cryptology Conference, 2010. P. 237–254.

[74] Mestre J.-F. *Rang de courbes elliptiques d'invariant donné.* // Comptes Rendus de l'Académie des Sciences - Series I - Mathematics, 1992. Vol. 314(12). P. 919–922.

[75] Satgé P. *Une construction de courbes k-rationnelles sur les surfaces de Kummer d'un produit de courbes de genre* 1. // Rational Points on Algebraic Varieties. — Birkhäuser, Basel, 2001. P. 313–334.

[76] Ulas M. *Rational points on certain hyperelliptic curves over finite fields.* // Bulletin of the Polish Academy of Sciences. Mathematics, 2007. Vol. 55(2). P. 97–104.

[77] Kuwata M., Wang L. *Topology of rational points on isotrivial elliptic surfaces.* // International Mathematics Research Notices, 1993. Vol. 1993(4). P. 113–123.

[78] Wahby R., Boneh D. *Fast and simple constant-time hashing to the BLS12-381 elliptic curve.* // IACR Trans. on Crypto. Hardware and Embedded Systems, 2019. P. 154–179.

[79] Kachisa E., Schaefer E., Scott M. *Constructing Brezing–Weng pairing-friendly elliptic curves using elements in the cyclotomic field.* // Pairing, 2008. P. 126–135.

[80] Barbulescu R., El Mrabet N., Ghammam L. *A taxonomy of pairings, their security, their complexity.* // IACR Cryptology ePrint Archive 2019/485.

[81] Barbulescu R., Duquesne S. *Updating key size estimations for pairings.* // Journal of Cryptology, 2019. Vol. 32(4). P. 1298–1336.

[82] Ghammam L., Fouotsa E. *Adequate elliptic curves for computing the product of n pairings.* // International Workshop on the Arithmetic of Finite Fields, 2016. P. 36–53.

[83] Gorchinskiy S., Shramov C. *Unramified Brauer group and its applications.* — Providence.: American Mathematical Society, 2018.

[84] Inose H. *Defining equations of singular $K3$ surfaces and a notion of isogeny.* // Proceedings of the International Symposium on Algebraic Geometry. — Books Kinokuniya, Kyoto, 1977. P. 495–502.

[85] Kuwata M. *Elliptic $K3$ surfaces with given Mordell–Weil rank.* // Rikkyo Daigaku Sugaku Zasshi, 2000. Vol. 49(1). P. 91–100.

[86] Kloosterman R. *Explicit sections on Kuwata's elliptic surfaces.* // Commentarii Mathematici Universitatis Sancti Pauli, 2005. Vol. 54(1). P. 69–86.

[87] Kumar A., Kuwata M. *Elliptic $K3$ surfaces associated with the product of two elliptic curves: Mordell–Weil lattices and their fields of definition.* // Nagoya Mathematical Journal, 2017. Vol. 228. P. 124–185.

[88] Shioda T. *A note on $K3$ surfaces and sphere packings.* // Proceedings of the Japan Academy, 2000. Vol. 76(5). P. 68–72.

[89] Shioda T. *$K3$ surfaces and sphere packings.* // Journal of the Mathematical Society of Japan, 2008. Vol. 60(4). P. 1083–1105.

[90] Shioda T., Schütt M. *Elliptic surfaces.* // Mordell–Weil Lattices. — Springer, Singapore, 2019. P. 79–114.

[91] Shioda T., Inose H. *On singular $K3$ surfaces.* // Complex Analysis and Algebraic Geometry. — Cambridge University Press, Cambridge, 1977. P. 119–136.

[92] Cox D., Little J., Schenck H. *Toric varieties.* — Providence.: American Mathematical Society, 2011.

[93] Hansen J. *Toric surfaces and error-correcting codes.* // Coding Theory, Cryptography and Related Areas. — Springer, Berlin, 2000. P. 132–142.

[94] Hansen J. *Toric varieties, Hirzebruch surfaces and error-correcting codes.* // Applicable Algebra in Engineering, Communication and Computing, 2002. Vol. 13. P. 289–300.

[95] Berman S. *On the theory of group codes.* // Kibernetika, 1967. Vol. 3. P. 31–39.

[96] Berman S. *Semisimple cyclic and abelian codes. II.* // Kibernetika, 1967. Vol. 3. P. 21–30.

[97] Joyner D. *Toric codes over finite fields.* // Applicable Algebra in Engineering, Communication and Computing, 2004. Vol. 15. P. 63–79.

[98] Voskresenskii V. *Algebraic groups and their birational invariants.* — Providence.: American Mathematical Society, 1998.

[99] Massey J. *Reversible codes.* // Information and Control, 1964. Vol. 7. P. 369–380.

[100] Lachaud G. *The parameters of projective Reed–Müller codes.* // Discrete Mathematics, 1990. Vol. 81. P. 217–221.

[101] Coray D., Tsfasman M. *Arithmetic on singular del Pezzo surfaces.* // Proceedings of the London Mathematical Society, 1988. Vol. 3(1). P. 25–87.

[102] Couvreur A., Duursma I. *Evaluation codes from smooth quadric surfaces and twisted Segre varieties.* // Designs, Codes and Cryptography, 2013. Vol. 66. P. 291–303.

[103] Blache R. et al. *Anticanonical codes from del Pezzo surfaces with Picard rank one.* // Transactions of the American Mathematical Society, 2020. Vol. 373. P. 5371–5393.

[104] Boguslavsky M. *Sections of the del Pezzo surfaces and generalized weights.* // Problems of Information Transmission, 1998. Vol. 34. P. 14–24.

[105] Little J., Schenck H. *Codes from surfaces with small Picard number.* // SIAM Journal on Applied Algebra and Geometry, 2018. Vol. 2(2). P. 242–258.

[106] Zarzar M. *Error-correcting codes on low rank surfaces.* // Finite Fields and Their Applications, 2007. Vol. 13(4). P. 727–737.

[107] Janson S. *Roots of polynomials of degrees* 3 *and* 4. // arXiv preprint 1009.2373, 2010.

[108] Shoup V. *A computational introduction to number theory and algebra.* — Cambridge.: Cambridge University Press, 2009.

[109] Manin Yu. *Cubic forms: algebra, geometry, arithmetic.* — Amsterdam.: North Holland, 2012.

[110] Hess F., Smart N., Vercauteren F. *The eta pairing revisited.* // IEEE Transactions on Information Theory, 2006. Vol. 52(10). P. 4595–4602.

[111] Popov V., Vinberg E. *Invariant theory.* // Algebraic Geometry IV. — Springer, Berlin, 1994. P. 123–278.

[112] Katsura T. *On Kummer surfaces in characteristic* 2. // Proceedings of the International Symposium on Algebraic Geometry. — Books Kinokuniya, Kyoto, 1977. P. 525–542.

[113] Katsura T., Schütt M. *Zariski K3 surfaces.* // Revista Matemática Iberoamericana, 2020. Vol. 36(3). P. 869–894.

[114] Zariski O. *On Castelnuovo's criterion of rationality* $p_a = P_2 = 0$ *of an algebraic surface.* // Illinois Journal of Mathematics, 1958. Vol. 2. P. 303–315.

[115] Fujiki A. *Finite automorphism groups of complex tori of dimension two.* // Publications of the Research Institute for Math. Sciences, Kyoto University, 1988. Vol. 24(1). P. 1–97.

[116] Yoshihara H. *Quotients of abelian surfaces.* // Publications of the Research Institute for Mathematical Sciences, Kyoto University, 1995. Vol. 31(1). P. 135–143.

[117] Katsura T. *Generalized Kummer surfaces and their unirationality in characteristic p.* // Journal of the Faculty of Science, the University of Tokyo, 1987. Vol. 34. P. 1–41.

[118] Hwang W. *On a classification of the automorphism groups of polarized abelian surfaces over finite fields.* // arXiv preprint 1809.06251, 2018.

[119] Ueno K. *Classification of algebraic varieties, I.* // Compositio Mathematica, 1973. Vol. 27(3). P. 277–342.

[120] Schicho J. *The parameterization problem for algebraic surfaces.* // ACM SIGSAM Bulletin, 1999. Vol. 33(3). P. 13.

[121] van Hoeij M., Cremona J. *Solving conics over function fields.* // Journal de Théorie des Nombres de Bordeaux, 2006. Vol. 18(3). P. 595–606.

[122] Koshelev D. *Magma code*, https://github.com/dishport/New-point-compression-method-for-elliptic-Fq2-curves-of-j-invariant-0, 2019.

[123] Azarderakhsh R. et al. *Key compression for isogeny-based cryptosystems.* // ACM International Workshop on ASIA Public-Key Cryptography, 2016. P. 1–10.

[124] De Feo L., Jao D., Plût J. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies.* // Journal of Math. Cryptology, 2014. Vol. 8(3). P. 209–247.

[125] Fan X., Otemissov A., Sica F., Sidorenko A. *Multiple point compression on elliptic curves.* // Designs, Codes and Cryptography, 2017. Vol. 83(3). P. 565–588.

[126] Diem C. *The GHS attack in odd characteristic.* // Journal of the Ramanujan Mathematical Society, 2003. Vol. 18(1). P. 1–32.

[127] Oguiso K., Truong T. *Explicit examples of rational and Calabi–Yau threefolds with primitive automorphisms of positive entropy.* // Journal of Mathematical Sciences, the University of Tokyo, 2015. Vol. 22. P. 361–385.

[128] Catanese F., Oguiso K., Verra A. *On the unirationality of higher dimensional Ueno-type manifolds.* // Revue Roumaine de Math. Pures et Appliquées, 2015. Vol. 60(3). P. 337–353.

[129] Milne J. *Abelian varieties.* // Arithmetic Geometry. — Springer, New York, 1986. P. 103–150.

[130] Hunt B. *The geometry of some special arithmetic quotients.* — Berlin.: Springer, 1996.

[131] Huybrechts D. *Lectures on K3 surfaces.* — Cambridge.: Cambridge University Press, 2016.

[132] Ulmer D. *Elliptic curves over function fields.* // Arithmetic of $L$-functions. — American Mathematical Society, Providence, 2011. P. 211–280.

[133] Shioda T. *Supersingular K3 surfaces.* // Algebraic Geometry, 1979. P. 564–591.

[134] Hirschfeld J., Korchmáros G., Torres F. *Algebraic curves over a finite field.* — Princeton.: Princeton University Press, 2008.

[135] Gaudry P., Schost É. *On the invariants of the quotients of the Jacobian of a curve of genus* 2. // AAECC, 2001. P. 373–386.

[136] Koshelev D. *Magma code,* https://github.com/dishport/Hashing-to-elliptic-curves-of-j-invariant-1728, 2019.

[137] Aubry Y., Perret M. *A Weil theorem for singular curves.* // Arithmetic, Geometry and Coding Theory, 1993. P. 1–7.

[138] Ireland K., Rosen M. *A classical introduction to modern number theory.* — New York.: Springer, 1990.

[139] Fouque P.-A., Tibouchi M. *Estimating the size of the image of deterministic hash functions to elliptic curves.* // Latincrypt, 2010. P. 81–91.

[140] Koshelev D. *Magma code*, https://github.com/dishport/Hashing-to-elliptic-curves-of-j-0-and-Mordell-Weil-groups, 2020.

[141] Chahal J., Meijer M., Top J. *Sections on certain $j = 0$ elliptic surfaces.* // Commentarii Mathematici Universitatis Sancti Pauli, 2000. Vol. 49(1). P. 79–89.

[142] Oguiso K., Shioda T. *The Mordell–Weil lattice of a rational elliptic surface.* // Rikkyo Daigaku Sugaku Zasshi, 1991. Vol. 40(1). P. 83–99.

[143] Shimada I., Zhang D. *Classification of extremal elliptic $K3$ surfaces and fundamental groups of open $K3$ surfaces.* // Nagoya Mathematical Journal, 2001. Vol. 161. P. 23–54.

[144] Shioda T. *On the Mordell–Weil lattices.* // Rikkyo Daigaku Sugaku Zasshi, 1990. Vol. 39(2). P. 211–240.

[145] Nishiyama K. *The Jacobian fibrations on some $K3$ surfaces and their Mordell–Weil groups.* // Japanese Journal of Mathematics, 1996. Vol. 22(2). P. 293–347.

[146] Ma S. *On K3 surfaces which dominate Kummer surfaces.* // Proceedings of the American Mathematical Society, 2013. Vol. 141(1). P. 131–137.

[147] Bilu Y., Luca F., Pizarro-Madariaga A. *Rational products of singular moduli.* // Journal of Number Theory, 2016. Vol. 158. P. 397–410.

[148] Naehrig M., Niederhagen R., Schwabe P. *New software speed records for cryptographic pairings.* // Latincrypt, 2010. P. 109–123.

[149] Silverman J. *Advanced topics in the arithmetic of elliptic curves.* — New York.: Springer, 1994.

[150] Jones J., Cremona J. *Global minimal model*, https://www.lmfdb.org/knowledge/show/ec.global_minimal_model, 2018.

[151] Koshelev D. *Magma code*, https://github.com/dishport/Hashing-to-elliptic-curves-of-j-0-and-quadratic-imaginary-orders-of-class-number-2, 2020.

[152] Voskresenskii V. *Projective invariant Demazure models.* // Mathematics of the USSR-Izvestiya, 1983. Vol. 20. P. 189–202.

[153] Platonov V., Rapinchuk A. *Algebraic groups and number theory.* — Boston.: Academic Press, 1993.

[154] Rubin K., Silverberg A. *Compression in finite fields and torus-based cryptography.* // SIAM Journal on Computing, 2008. Vol. 37. P. 1401–1428.

[155] Voskresenskii V. *On two-dimensional algebraic tori.* // Fourteen Papers on Algebra, Topology, Algebraic and Differential Geometry. — AMS, Providence, 1968. P. 190–195.

[156] Voskresenskii V. *On two-dimensional algebraic tori. II.* // Mathematics of the USSR-Izvestiya, 1967. Vol. 1. P. 691–696.

[157] Graber T., Harris J., Mazur B., Starr J. *Arithmetic questions related to rationally connected varieties.* // The Legacy of Niels Henrik Abel. — Springer, Berlin, 2004. P. 531–542.

[158] Voskresenskii V., Klyachko A. *Toroidal Fano varieties and root systems.* // Mathematics of the USSR-Izvestiya, 1985. Vol. 24. P. 221–244.

[159] Batyrev V., Tschinkel Y. *Rational points of bounded height on compactifications of anisotropic tori.* // International Math. Research Notices, 1995. Vol. 1995. P. 591–635.

[160] Ballard M., Duncan A., McFaddin P. *On derived categories of arithmetic toric varieties.* // Annals of $K$-Theory, 2019. Vol. 4(2). P. 211–242.

[161] Poonen B. *Rational points on varieties.* — Providence.: American Mathematical Society, 2017.

[162] Hirschfeld J. *Finite projective spaces of three dimensions.* — Oxford.: Oxford University Press, 1986.

[163] Couvreur A. *Construction of rational surfaces yielding good codes.* // Finite Fields and Their Applications, 2011. Vol. 17. P. 424–441.

[164] Kollár J. *Looking for rational curves on cubic hypersurfaces.* // Higher-Dimensional Geometry over Finite Fields. — IOS Press, Amsterdam, 2008. P. 92–122.

[165] Hernando F., O'Sullivan M., Popovici E., Srivastava S. *Subfield-subcodes of generalized toric codes.* // IEEE International Symposium on Info. Theory, 2010. P. 1125–1129.

[166] Massey J. *Linear codes with complementary duals.* // Discrete Mathematics, 1992. Vol. 106–107. P. 337–342.

[167] Yang X., Massey J. *The condition for a cyclic code to have a complementary dual.* // Discrete Mathematics, 1994. Vol. 126. P. 391–393.

[168] Kasami T., Lin S., Peterson W. *New generalizations of the Reed–Muller codes. Part I Primitive Codes.* // IEEE Transactions on Information Theory, 1968. Vol. 14. P. 189–199.

[169] Ruano D. *On the parameters of r-dimensional toric codes.* // Finite Fields and Their Applications, 2007. Vol. 13. P. 962–976.

[170] Aubry Y., Berardini E., Herbaut F., Perret M. *Bounds on the minimum distance of algebraic geometry codes defined over some families of surfaces.* // arXiv preprint 1912.07450, 2020.

[171] Daskalov R., Hristov P. *New one-generator quasi-cyclic codes over $GF(7)$.* // Problems of Information Transmission, 2002. Vol. 38. P. 50–54.

[172] Daskalov R., Hristov P. *New quasi-cyclic degenerate linear codes over $GF(8)$.* // Problems of Information Transmission, 2003. Vol. 39. P. 184–190.

[173] Daskalov R., Metodieva E., Hristov P. *New minimum distance bounds for linear codes over $GF(9)$.* // Problems of Information Transmission, 2004. Vol. 40. P. 13–24.

[174] Grassl M. *Bounds on the minimum distance of linear codes and quantum codes*, http://www.codetables.de.

[175] Derenthal U. *Singular Del Pezzo surfaces whose universal torsors are hypersurfaces.* // Proceedings of the London Mathematical Society, 2014. Vol. 108(3). P. 638–681.

[176] Kasprzyk A. *Bounds on fake weighted projective space.* // Kodai Mathematical Journal, 2009. Vol. 32(2). P. 197–208.

[177] Hirschfeld J. *Projective geometries over finite fields.* — Oxford.: Clarendon Press, 1998.

[178] Bernstein D. et al. *Twisted Edwards curves.* // Africacrypt, 2008. P. 389–405.

[179] Arene C., Lange T., Naehrig M., Ritzenthaler C. *Faster computation of the Tate pairing.* // Journal of Number Theory, 2011. Vol. 131(5). P. 842–857.

[180] van der Geer G., Howe E., Lauter K., Ritzenthaler C. *Tables of curves with many points*, http://www.manypoints.org.

[181] Schoof R. *Nonsingular plane cubic curves over finite fields.* // Journal of Combinatorial Theory, Series A, 1987. Vol. 46(2). P. 183–211.

[182] Koshelev D. *Magma code*, https://github.com/dishport/Non-split-toric-BCH-codes-on-singular-del-Pezzo-surfaces, 2020.

[183] Daskalov R., Gulliver T. *Bounds in minimum distance for linear codes over $GF(7)$.* // The Journal of Combinatorial Math. and Combinatorial Comp., 2001. Vol. 36. P. 175–191.

**Titre:** Nouvelles applications des surfaces rationnelles et surfaces de Kummer généralisées sur des corps finis à la cryptographie à base de couplages et à la théorie des codes BCH

**Mots clés:** Corps finis, tores algébriques et variétés toriques non déployés, polygones réflexifs et surfaces de del Pezzo (singulières), surfaces de Kummer (généralisées), fibrations en coniques et fibrations elliptiques, groupes de Mordell–Weil, restriction de Weil, isogénies et couplages, compression de points et hachage pour courbes elliptique de $j$-invariants $0, 1728$, codes BCH et codes de géométrie algébrique

**Résumé:** Dans la thèse deux tâches se posant pour des courbes elliptiques de $j$-invariants $0, 1728$ sont considérées. Ces courbes sont connues pour être prioritaires en cryptographie à base de couplages. La première tâche est consacrée à la compression de points d'une courbe elliptique, et la seconde à la construction d'une application d'un corps fini dans le groupe des points d'une courbe elliptique sur lui. Pour dériver les formules explicites correspondantes, nous utilisons des méthodes peu banales de géométrie birationnelle sur des corps finis, ainsi que la théorie des surfaces de Kummer (généralisées). Contrairement aux approches déjà connues pour résoudre les tâches mentionnées, les nôtres nécessitent moins d'exponentiations dans le corps de base. C'est important, car en général, même une seule exponentiation est considérée comme une opération assez longue.

La thèse étudie également une large classe de codes (AG) de géométrie algébrique sur des surfaces toriques non déployées que nous appelons codes toriques non déployés. Beaucoup d'entre eux sont contenus dans une classe bien connue de codes BCH $q$-aires qui peuvent être décodés rapidement (par rapport à ceux AG). En revanche, la théorie des codes BCH (contrairement à ceux AG) n'est pas assez profonde pour estimer exactement leurs paramètres. Plus précisément, pour calculer la distance minimale de certains codes BCH toriques non déployés, nous utilisons la théorie des courbes elliptiques sur des corps finis.

**Title:** New applications of rational and generalized Kummer surfaces over finite fields in pairing-based cryptography and in the theory of BCH codes

**Keywords:** Finite fields, non-split algebraic tori and toric varieties, reflexive polygons and (singular) del Pezzo surfaces, (generalized) Kummer surfaces, conic bundles and elliptic fibrations, Mordell–Weil groups, Weil restriction, isogenies and pairings, point compression and hashing for elliptic curves of $j$-invariants $0, 1728$, BCH and algebraic geometry codes

**Abstract:** In the thesis two tasks arising for elliptic curves of $j$-invariants $0, 1728$ are considered. These curves are known to have priority in pairing-based cryptography. The first task is devoted to the point compression of an elliptic curve, and the second one to the construction of a mapping from a finite field to the point group of an elliptic curve over it. To derive the corresponding explicit formulas, we use rather non-trivial methods of birational geometry over finite fields, along with the theory of (generalized) Kummer surfaces. In contrast to the already known approaches to solving the mentioned tasks, ours require fewer exponentiations in the base field. This is significant, since in general even one exponentiation is considered a quite time-consuming operation.

The thesis also studies a wide class of algebraic geometry (AG) codes on non-split toric surfaces, which we call non-split toric codes. Many of them are contained in a well-known class of $q$-ary BCH codes that can be quickly decoded (compared with AG ones). On the other hand, the theory of BCH codes (in contrast to AG ones) is not deep enough to exactly estimate their parameters. More precisely, to calculate the minimum distance of some non-split toric BCH codes, we use the theory of elliptic curves over finite fields.