Contribution à la génération de vecteurs aléatoires et à la cryptographie

Abalo Baya

THESE

présentée par

BAYA Abalo

pour obtenir le titre de DOCTEUR

DE L'UNIVERSITÉ JOSEPH FOURIER - GRENOBLE I

«Mathématiques appliquées»

CONTRIBUTION A LA GÉNÉRATION DE VECTEURS ALÉATOIRES ET A LA CRYPTOGRAPHIE

Date de soutenance : 27 Février 1990

Composition du jury

Jean Paul Bertrandias Président

Alain Berlinet
Claude Moser
Bernard Van Cutsem } Examinateurs

Thèse préparée au sein du LABORATOIRE TIM3

UNIVERSITE Joseph FOURIER (GRENOBLE I)

Président de l'Université :
M. NEMOZ Alain

Année Universitaire 1988 - 1989

MEMBRES DU CORPS ENSEIGNANT DE SCIENCES ET DE GEOGRAPHIE

PROFESSEURS DE 1ère Classe

ADIBA Michel	Informatique
ANTOINE Pierre	Géologie I.R.I.G.M.
ARNAUD Paul	Chimie Organique
ARVIEU Robert	Physique Nucléaire I.S.N.
AUBERT Guy	Physique C.N.R.S
AURIAULT Jean-Louis	Mécanique
AYANT Yves	Physique Approfondie
BARBIER Marie-Jeanne	Electrochimie
BARJON Robert	Physique Nucléaire ISN
BARNOUD Fernand	Biochimie Macromoléculaire Végétale
BARRA Jean-René	Statistiques-Mathématiques Appliquées
BECKER Pierre	Physique
BEGUIN Claude	Chimie Organique
BELORISKY Elie	Physique
BENZAKEN Claude	Mathématiques Pures
BERARD Pierre	Mathématiques Pures
BERNARD Alain	Mathématiques Pures
BERTRANDIAS Françoise	Mathématiques Pures
BERTRANDIAS Jean-Paul	Mathématiques Pures
BILLET Jean	Géographie
BOELHER Jean-Paul	Mécanique
BRAVARD Yves	Géographie
CARLIER Georges	Biologie Végétale
CASTAING Bernard	Physique
CAUQUIS Georges	Chimie Organique
CHARDON Michel	Géographie
CHIBON Pierre	Biologie Animale
COHEN ADDAD Jean-Pierre	Physique
COLIN DE VERDIERE Yves	Mathématiques Pures
CYROT Michel	Physique du Solide
DEBELMAS Jacques	Géologie Générale
DEGRANGE Charles	Zoologie
DEMAILLY Jean-Pierre	Mathématiques Pures
DENEUVILLE Alain	Physique
DEPORTES Charles	Chimie Minérale
DOLIQUE Jean-Michel	Physique des Plasmas
DOUCE Roland	Physiologie Végétale
DUCROS Pierre	Cristallographie
FINKE Gerde	Informatique
GAGNAIRE Didier	Chimie Physique
GAUTRON René	Chimie
GENIES Eugène	Chimie
GERMAIN Jean-Pierre	Mécanique,
GIDON Maurice	Géologie
GUITTON Jacques	Chimie
HICTER Pierre	Chimie
IDELMAN Simon	Physiologie Animale
JANIN Bernard	Géographie
JOLY Jean René	Mathématiques Pures

JOSELEAU Jean Paul	Biochimie
KAHANE André, détaché	Physique
KAHANE Josette	Physique
KRAKOWIAK Sacha	Mathématiques Appliquées
LAJZEROWICZ Jeanine	Physique
LAJZEROWICZ Joseph	Physique
LAURENT Pierre-Jean	Mathématiques Appliquées
LEBRETON Alain	Mathématiques Appliquées
DE LEIRIS Joël	Biologie
LHOMME Jean	Chimie
LLIBOUTRY Louis	Géophysique
LOISEAUX Jean-Marie	Sciences Nucléaires I.S.N.
LONGEQUEUE Nicole	Physique
LUNA Domingo	Mathématiques Pures
MACHE Régis	Physiologie Végétale
MASCLE Georges	Géologie
MAYNARD Roger	Physique du Solide
OMONT Alain	Astrophysique
OZENDA Paul	Botanique (Biologie Végétale)
PANNETIER Jean	Chimie
PAYAN Jean-Jacques	Mathématiques Pures
PEBAY-PEYROULA Jean-Claude	Physique
PERRIER Guy	Géophysique
PIERRE Jean Louis	Chimie Organique
RENARD Michel	Thermodynamique
RIEDTMANN Christine	Mathématiques
RINAUDO Marguerite	Chimie CERMAV
ROSSI André	Biologie
SAXOD Raymond	Biologie Animale
SENGEL Philippe	Biologie Animale
SERGERAERT Francis	Mathématiques Pures
SOUCHIER Bernard	Biologie
SOUTIF Michel	Physique
STUTZ Pierre	Mécanique
TRILLING Laurent	Mathématiques Appliquées
VAN CUTSEM Bernard	Mathématiques Appliquées
VIALON Pierre	Géologie

PROFESSEURS de 2ème Classe

ARMAND Gilbert	Géographie
ATTANE Pierre	Mécanique
BARET Paul	Chimie
BERTIN José	Mathématiques
BLANCHI J.Pierre	STAPS
BLOCK Marc	Biologie
BLUM Jacques	Mathématiques Appliquées
BOITET Christian	Mathématiques Appliquées
BORNAREL Jean	Physique
BORRIONE Dominique	Automatique informatique
BOUVET Jean	Biologie
BROSSARD Jean	Mathématiques
BRUANDET J.François	Physique
BRUGAL Gérard	Biologie
BRUN Gilbert	Biologie
CASTAING Bernard	Physique
CERFF Rudiger	Biologie
CHIARAMELLA Yves	Mathématiques Appliquées
CHOLLET Jean Pierre	Mécanique
COLOMBEAU Jean François	Mathématiques (ENSL)
COURT Jean	Chimie
CUNIN Pierre Yves	Informatique
DAVID Jean	Géographie

DHOUAILLY Danielle	Biologie
DUFRESNOY Alain	Mathématiques Pures
GASPARD François	Physique
GIDON Maurice	Géologie
GIGNOUX Claude	Sciences Nucléaires
GILLARD Roland	Mathématiques Pures
GIORNI Alain	Sciences Nucléaires
GONZALEZ SPRINBERG Gérardo	Mathématiques Pures
GUIGO Maryse	Géographie
GUMUCHAIN Hervé	Géographie
HACQUES Gérard	Mathématiques Appliquées
HERBIN Jacky	Géographie
HERAULT Jeanny	Physique
HERINO Roland	Physique
JARDON Pierre	Chimie
KERCKHOVE Claude	Géologie
MANDARON Paul	Biologie
MARTINEZ Francis	Mathématiques Appliquées
MOREL Alain	Géographie
NEMOZ Alain	Thermodymamique CNRS - CRTBT
NGUYEN HUY Xuong	Informatique
OUDET Bruno	Mathématiques Appliquées
PAUTOU Guy	Biologie
PECHER Arnaud	Géologie
PELMONT Jean	Biochimie
PELLETIER Guy	Astrophysique
PERRIN Claude	Sciences Nucléaires I.S.N.
PIBOULE Michel	Géologie
RAYNAUD Hervé	Mathématiques Appliquées
REGNARD Jean René	Physique
RICHARD Jean-Marc	Physique
RIEDTMANN Christine	Mathématiques Pures
ROBERT Danielle	Chimie
ROBERT Gilles	Mathématiques Pures
ROBERT Jean-Bernard	Chimie Physique
SARROT-REYNAULD Jean	Géologie
SAYETAT Françoise	Physique
SERVE Denis	Chimie
STOECKEL Frédéric	Physique
SCHOLL Pierre-Claude	Mathématiques Appliquées
SUBRA Robert	Chimie
VALLADE Marcel	Physique
VIDAL Michel	Chimie Organique
VINCENT Gilbert	Physique
VIVIAN Robert	Géographie
VOTTERO Philippe	Chimie

MEMBRES DU CORPS ENSEIGNANT DE L' IUT 1

PROFESSEURS de 1ère Classe

BUISSON Roger	Physique IUT 1
CHEHIKIAN Alain	E.E.A. I.U.T.1
DODU Jacques	Mécanique Appliquée IUT 1
NEGRE Robert	Génie Civil IUT 1
NOUGARET Marcel	Automatique IUT 1
PERARD Jacques	EEA. IUT 1

PROFESSEURS de 2ème classe

BEE Marc	Physique IUT 1
BOUTHINON Michel	EEA. IUT 1
CHAMBON René	Génie Mécanique IUT 1
CHENAVAS Jean	Physique IUT 1

CHILO Jean	Physique IUT 1
CHOUTEAU Gérard	Physique IUT 1
CONTE René	Physique IUT 1
FOSTER Panayotis	Chimie IUT 1
GOSSE Jean-Pierre	EEA.IUT 1
GROS Yves	Physique IUT 1
HAMAR Roger	Chimie IUT 1
KUHN Gérard, (Détaché)	Physique IUT 1
LEVIEL Jean Louis	Physique IUT 1
MAZUER Jean	Physique IUT 1
MICHOULIER Jean	Physique IUT 1
MONLLOR Christian	EEA.IUT 1
PERRAUD Robert	Chimie IUT 1
PIERRE Gérard	Chimie IUT 1
TERRIEZ Jean-Michel	Génie Mécanique IUT 1
TOUZAIN Philippe	Chimie IUT 1
TURGEMAN Sylvain	Génie civil
VINCENDON Marc	Chimie IUT 1
ZIGONE Michel	Physique IUT 1

PROFESSEURS DE PHARMACIE

AGNIUS-DELORD Claudine	Physique	Faculté La Tronche
ALARY Josette	Chimie Analytique	Faculté La Tronche
BERIEL Hélène	Physiologie et Pharmacologie	Faculté La Tronche
CUSSAC Max	Chimie Therapeutique	Faculté La Tronche
DEMENGE Pierre	Pharmacodynamie	Faculté La Tronche
FAVIER Alain	Biochimie	C.H.R.G.
JEANNIN Charles	Pharmacie Galénique	Faculté Meylan
LATURAZE Jean	Biochimie	Faculté La Tronche
LUU DUC Cuong	Chimie Générale	Faculté La Tronche
MARIOTTE Anne-Marie	Pharmacognosie	Faculté La Tronche
MARZIN Daniel	Toxicologie	Faculté Meylan
RENAUDET Jacqueline	Bactériologie	Faculté La Tronche
ROCHAT Jacques	Hygiéne et Hydrologie	Faculté La Tronche
SEIGLE-MURANDI Françoise	Botanique et Cryptogamie	Faculté Meylan
VERAIN Alice	Pharmacie Galénique	Faculté Meylan

MEMBRES DU CORPS ENSEIGNANT DE MEDECINE

PROFESSEURS CLASSE EXEPTIONNELLE ET 1ère CLASSE

AMBLARD Pierre	Dermatologie	C.H.R.G.
AMBROISE-THOMAS Pierre	Parasitologie	C.H.R.G.
BEAUDOING André	Pédiatrie-Puericulture	C.H.R.G.
BEZEZ Henri	Orthopédie-Traumatologie	Hopital SUD
BONNET Jean-Louis	Ophtalmologie	C.H.R.G.
BOUCHET Yves	Anatomie	Faculté La Merci
	Chirurgie Générale et Digestive	C.H.R.G.
BUTEL Jean	Orthopédie-Traumatologie	C.H.R.G.
CHAMBAZ Edmond	Biochimie	C.H.R.G.
CHAMPETIER Jean	Anatomie-Topographique et Appliquée	C.H.R.G.
CHARACHON Robert	O.R.L.	C.H.R.G.
COLOMB Maurice	Immunologie	Hopital sud
COUDERC Pierre	Anatomie-Pathologique	C.H.R.G.
DELORMAS Pierre	Pneumophtisiologie	C.H.R.G.
DENIS Bernard	Cardiologie	C.H.R.G.
GAVEND Michel	Pharmacologie	Faculté La Merci

HOLLARD Daniel	Hématologie	C.H.R.G.
LATREILLE René	Chirurgie Thoracique et Cardiovasculaire	C.H.R.G.
LE NOC Pierre	Bactériologie-Virologie	C.H.R.G.
MALINAS Yves	Gynécologie et Obstétrique	C.H.R.G.
MALLION Jean-Michel	Médecine du Travail	C.H.R.G.
MICOUD Max	Clinique Médicale et Maladies Infectieuses	C.H.R.G.
MOURIQUAND Claude	Histologie	Faculté La Merci
PARAMELLE Bernard	Pneumologie	C.H.R.G.
PERRET Jean	Neurologie	C.H.R.G.
RACHAIL Michel	Hépato-Gastro-Entérologie	C.H.R.G.
DE ROUGEMONT Jacques	Neurochirurgie	C.H.R.G.
SARRAZIN Roger	Clinique Chirurgicale	C.H.R.G.
STIEGLITZ Paul	Anestésiologie	C.H.R.G.
TANCHE Maurice	Physiologie	Faculté La Merci
VIGNAIS Pierre	Biochimie	Faculté La Merci

PROFESSEURS 2ème CLASSE

BACHELOT Yvan	Endocrinologie	C.H.R.G.
BARGE Michel	Neurochirurgie	C.H.R.G.
BENABID Alim Louis	Biophysique	Faculté La Merci
BENSA Jean-Claude	Immunologie	Hopital Sud
BERNARD Pierre	Gynécologie-Obstétrique	C.H.R.G.
BESSARD Germain	Pharmacologie	ABIDJAN
BOLLA Michel	Radiothérapie	C.H.R.G.
BOST Michel	Pédiatrie	C.H.R.G.
BOUCHARLAT Jacques	Psychiatrie Adultes	Hopital Sud
BRAMBILLA Christian	Pneumologie	C.H.R.G.
CHIROSSEL Jean-Paul	Anatomie-Neurochirurgie	C.H.R.G.
COMET Michel	Biophysique	Faculté La Merci
CONTAMIN Charles	Chirurgie Thoracique et Cardiovasculaire	C.H.R.G.
CORDONNIER Daniel	Néphrologie	C.H.R.G.
COULOMB Max	Radiologie	C.H.R.G.
CROUZET Guy	Radiologie	C.H.R.G.
DEBRU Jean-Luc	Médecine Interne et Toxicologie	C.H.R.G.
DEMONGEOT Jacques	Biostatistiques et Informatique Médicale	Faculté La Merci
DUPRE Alain	Chirurgie Générale	C.H.R.G.
DYON Jean-François	Chirurgie Infantile	C.H.R.G.
ETERRADOSSI Jacqueline	Physiologie	Faculté La Merci
FAURE Claude	Anatomie et Organogénèse	C.H.R.G.
FAURE Gilbert	Urologie	C.H.R.G.
FOURNET Jacques	Hépato-Gastro-Entérologie	C.H.R.G.
FRANCO Alain	Médecine Interne	C.H.R.G.
GIRARDET Pierre	Anesthésiologie	C.H.R.G.
GUIDICELLI Henri	Chirurgie Générale et Vasculaire	C.H.R.G.
GUIGNIER Michel	Thérapeutique et Réanimation Médicale	C.H.R.G.
HADJIAN Arthur	Biochimie	Faculté La Merci
HALIMI Serge	Endocrinologie et Maladies Métaboliques	C.H.R.G.
HOSTEIN Jean	Hépato-Gastro-Entérologie	C.H.R.G.
HUGONOT Robert	Médecine Interne	C.H.R.G.
JALBERT Pierre	Histologie-Cytogénétique	C.H.R.G.
JUNIEN-LAVILLAUROY Claude	O.R.L.	C.H.R.G.
KOLODIE Lucien	Hématologie Biologique	C.H.R.G.
LETOUBLON Christian	Chirurgie Générale	C.H.R.G.
MACHECOURT Jacques	Cardiologie et Maladies Vasculaires	C.H.R.G.
MAGNIN Robert	Hygiène	C.H.R.G.
MASSOT Christian	Médecine Interne	C.H.R.G.

MOUILLON Michel	Ophtalmologie	C.H.R.G.
PELLAT Jacques	Neurologie	C.H.R.G.
PHELIP Xavier	Rhumatologie	C.H.R.G.
RACINET Claude	Gynécologie-Obstétrique	Hopital Sud
RAMBAUD Pierre	Pédiatrie	C.H.R.G.
RAPHAEL Bernard	Stomatologie	C.H.R.G.
SCHAERER René	Cancérologie	C.H.R.G.
SEIGNEURIN Jean-Marie	Bactériologie-Virologie	Faculté La Merci
SELE Bernard	Cytogénétique	Faculté La Merci
SOTTO Jean-Jacques	Hématologie	C.H.R.G.
STOEBNER Pierre	Anatomie Pathologique	C.H.R.G.
VROUSOS Constantin	Radiothérapie	C.H.R.G.

Je remercie vivement Messieurs Alain le Breton pour m'avoir accueilli au sein de l'Equipe de Statistique et Bernard Van Cutsem pour avoir proposé et dirigé cette thèse.

Je suis sensible à l'honneur que me fait Monsieur Jean Paul Bertrandias en acceptant de présider le jury de cette thèse.

Je tiens à exprimer ma profonde reconnaissance à Monsieur Jean Della Dora et au Groupe de Calcul Formel dont il est responsable pour leur soutien moral et pour leurs conseils concernant les langages de calcul formel adaptés à mon travail.

Je dois un grand merci au Laboratoire TIM3 pour son soutien financier et pour son environnement scientifique et technique dont j'ai bénéficié.

Monsieur Harald Niederreiter m'a guidé par ses conseils et sa grande connaissance sur la bibliographie concernant la génération de nombres aléatoires. Qu'il me soit permis de le remercier ici.

Je remercie vivement :

Monsieur Alain Berlinet, membre du jury, d'avoir dirigé la partie cryptographie de ce travail ;

Monsieur Claude Moser pour avoir critiqué la rédaction de cette thèse et pour avoir accepté de participer au jury ;

Les membres du service de reprographie qui ont effectué le tirage de la thèse.

à mon père

TABLE DES MATIERES

INTRODUCTION

L'une des étapes essentielles dans les méthodes de Monte - Carlo est l'échantillonnage aléatoire de points appartenant à un ensemble I donné. Pour fixer les idées on prend pour I l' intervalle [0, 1]. Alors une *procédure d'échantillonnage sans biais* produirait une suite de " nombres aléatoires " de loi uniforme sur I. Mais aussi longtemps qu'on n'aura pas défini de façon concrète l'expression "sans biais" et qu'aucune méthode de régulation de l'équiprobabilité des nombres n'est adoptée, le concept de "suite de nombres aléatoires " restera tout simplement une idéalisation. On voit le paradoxe, c'est-à-dire, essayer de caractériser le *hasard* à l'aide d'un ensemble de *règles connues à l'avance.*

Par ce début d'introduction quelque peu philosophique, nous avons voulu illustrer la difficulté qu'on a lorsqu'on cherche à définir concrètement ce que s'est une suite de nombres aléatoires(N. A). Ceci étant précisé intéressons nous maintenant à l'historique sur la génération d'une telle suite, historique permettant d'avoir une idée sur les différentes méthodes de réalisation d'une suite de N. A.

Les premiers générateurs de nombres aléatoires étaient basés sur des phénomènes physiques (bruits blancs, émissions radio-actives de particules etc.) dont les propriétés stochastiques avaient été démontrées. Cependant une telle méthode présentait deux inconvénients majeurs :

- Elle nécessitait la connection au calculateur d'une unité spéciale produisant le phénomène utilisé pour la génération des nombres, unité dont la maintenance était, dans la pratique, presque impossible à assurer car la seule manière de détecter un mauvais fonctionnement était de tester en permanence les nombres générés.

- Les séquences de nombres engendrés *n'étaient pas reproductibles* et il était donc difficile de tester ou de mettre au point une simulation.

L'étape suivante fut l'utilisation des *tables de nombres au hasard* (construites d'ailleurs à partir de phénomènes physiques et de machines spéciales) qui permettaient toute la reproductibilité désirée. Mais ces tables étaient peu utilisables dans

les systèmes informatiques à cause de l'encombrement mémoire et de la lenteur d'accès qu'elles entraînent. Aussi chercha-t-on assez tôt à trouver des algorithmes permettant de générer des nombres mimant le hasard.

Il peut sembler paradoxal de vouloir générer des suites de nombres aléatoires au moyen d'un algorithme s'exécutant sur un ordinateur, puisque chaque nombre va dépendre d'une manière déterministe (par l'intermédiaire de l'algorithme) du ou des nombres qui le précèdent. Aussi devons nous nous entendre dès maintenant sur le hasard que nous souhaitons avoir lors de la génération des nombres par le procédé algorithmique : une suite de nombre sera jugée satisfaisante, si l'application d'un certain nombre de tests statistiques assez fiables sur elle *ne met pas en défaut les propriétés du caractère aléatoire essentielles pour la simulation que nous désirons réaliser.* Nous dirons alors que nous avons une suite de *nombres pseudo-aléatoires* (en abrégé N.P. A.) et par abus de langage nous utiliserons souvent la terminologie " nombres aléatoires ".

Depuis la première génération d'ordinateurs, de nombreux algorithmes ont été proposés pour générer des suites de nombres aléatoires uniformément distribués. Les tout premiers algorithmes tels que prendre le carré du "milieu " d'un nombre (Von Neumann 1948) avaient non seulement le désavantage de ne pas donner de très bons résultats du point de vue de la qualité statistique des nombres générés, mais aussi celui de ne permettre une étude théorique assez approfondie. En 1951, Lehmer proposa une méthode congruentielle qui est encore bien utilisée maintenant bien qu'elle soit concurrencée par une autre méthode basée sur les régistres à décalage.

Dans le premier chapitre nous présentons les congruences linéaires simples et les tests de qualité des nombres pseudo-aléatoires congruentiels. L'accent est mis sur le test des treillis (ou réseaux), le test spectral et le test sériel. Les deux premiers tests faisant intervenir une phase de réduction de base de réseau, nous nous sommes intéressés aux algorithmes de réduction de U. Dieter, D.E. Knuth et de A. K. Lenstra, H.W. Lenstra et L . Lovasz (LLL) . Nous profitons alors de la mise en oeuvre de ces tests pour comparer les temps d'exécution de ces trois méthodes de réduction. L'étude du test

sériel est faite sur la base de l'estimation de la discrépance des vecteurs de N.P.A. congruentiels. Partant de cette estimation on introduit une quantité appelée *figure de mérite*. Celle-ci nous permet de rechercher, pour deux entiers m et b fixés, des multiplicateurs a tels que deux termes successifs de la suite $(u) = \{x_i/m\}$, avec

$$x_{i+1} \equiv ax_i + b \bmod m, \quad \forall\ i \geq 0$$

et x_0 fixé, soient statistiquement indépendants.

Nous débutons le second chapitre par l'étude des longueurs de cycle et du transitoire des suites engendrées par une congruence linéaire multidimensionnelle. Ensuite nous décrivons quelques méthodes de transformation de ces suites en suites de N.P.A. de loi uniforme sur [0, 1]. Nous terminons le chapitre par une discussion sur le choix des paramètres d'une congruence linéaire multidimensionnelle à partir de l'estimation de la discrépance des vecteurs de N.P.A. .

Dans le troisième chapitre nous étudions la période d'un générateur vectoriel basé sur le modèle de D.E. Daykin (1963) et une congruence linéaire multidimensionnelle de période maximale, puis nous faisons un aperçu sur les principaux *générateurs non linéaires de N.P.A* qu'on rencontre dans la littérature.

Le dernier chapitre, réservé à la cryptographie, traite du problème du décryptage de l'ordre et du modulo d'une congruence linéaire simple ou multidimensionnelle.

CONVENTION

Une lettre soulignée (par exemple $\underline{a}$) désignera toujours un vecteur et le transposé de $\underline{a}$ sera noté ${}^t\underline{a}$.

Le produit scalaire de $\underline{a}$ et de $\underline{b}$ est représenté par $\underline{a} \,.\, \underline{b}$. Pour un entier m, $m > 1$, $\mathbb{Z}_m$ est l'anneau des entiers modulo m et pour un entier naturel k strictement supérieur à 1 et un nombre premier p, on désigne par $\mathbb{Z}_m^k$, le produit cartésien $\mathbb{Z}_m \times \ldots \times \mathbb{Z}_m$ (le produit étant effectué k fois), par $\mathbb{Z}_m^{k\,*}$ l'ensemble $\mathbb{Z}_m^k$ privé du k- uplet nul, par $\mathbb{F}_p$ un corps fini à p éléments ($\mathbb{Z}_p$ en est un exemple) et par $\mathbb{F}_{p^k}$ une extension de $\mathbb{F}_p$ ayant p^k éléments.

D'autre part si A est un anneau, alors A[x] est l'ensemble des polynômes sur A à une indéterminée x et pour deux éléments F(x) et G(x) de A[x], RES (F(x), G(x)) est la résultante de F(x) et de G(x). Enfin GL(k, $\mathbb{F}_p$) est le groupe des matrices carrées inversibles d'ordre k à coefficients dans $\mathbb{F}_p$ et det (C) est le déterminant d'une matrice C à coefficients dans un sous -ensemble de $\mathbb{R}$.

CHAPITRE 1

CONGRUENCES LINEAIRES SIMPLES ET NOMBRES PSEUDO-ALEATOIRES

I. CONGRUENCES LINEAIRES SIMPLES

I.1. NOTATIONS ET DEFINITIONS

Soient m un entier strictement supérieur à 1, $\mathbb{Z}_m$ l'anneau des entiers modulo m et a et b deux entiers vérifiant $0 < a < m$ et $0 \leq b < m$. Alors l'application T de $\mathbb{Z}_m$ dans $\mathbb{Z}_m$ définie par

$$T(x) \equiv ax + b \mod m$$

permet d'engendrer une suite $(x) = \{x_n\}$ dont les termes, appelés *les itérés de* x_0 *par* T, sont donnés par

$$(1) \quad \begin{cases} x_{n+1} = T(x_n), \ \forall\, n \geq 0 \\ x_0 \in \mathbb{Z}_m \text{ fixé}. \end{cases}$$

Pour un choix convenable des entiers a, b et m la suite normalisée $(u) = \{u_n\}$, $u_n = x_n/m$ pour tout entier naturel n, est considérée comme une suite de *nombres pseudo-aléatoires* (en abrégé N.P.A.) de loi uniforme sur [0, 1].

La congruence linéaire T est appelée *générateur congruentiel* de N.P.A. et on la notera (a, b, m). Si b est nul, alors l'application T est dite *homogène ou multiplicative*, sinon elle est dite *mixte*. La suite $(x) = \{x_n\}$ ainsi engendrée sera notée (a, b, m, x_0).

Puisque l'anneau $\mathbb{Z}_m$ est un ensemble fini, les itérés de x_0 par T ne prennent qu'un nombre fini de valeurs et il existe deux entiers t et τ tels que

* si $x_1 \neq x_0$, alors

1) $t \geq 0$, $\tau > 0$

2) $x_0, x_1, \ldots, x_{t+\tau-1}$ sont deux à deux distincts

3) $x_{t+\tau} = x_t$

* et si $x_1 = x_0$, alors $t = 0$ et $\tau = 1$.

Dans le cas $t > 0$, la séquence $(x_0, x_1, \ldots, x_{t-1})$ est appelée partie transitoire ou tout simplement *transitoire* de la suite $(x) = \{x_n\}$.

La séquence $(x_t, x_{t+1}, \ldots, x_{t+\tau-1})$ est appelée *cycle limite ou cycle* de (x). L'entier t est la *longueur du transitoire* et τ est la *longueur du cycle ou période* de (x).

Remarquons que, si a est premier avec m, alors le transitoire de la suite (a, b, m, x_o) est vide et pour tout point fixe x_o de T le cycle de cette suite est de longueur 1. Ainsi on cherchera, en pratique, à construire des suites sans transitoire et de cycle le plus long possible en espérant que lors de l'utilisation de la suite $(u) = \{u_n\}$, le nombre de tirages de N.P.A. effectués sera au plus égal à la période de $(x) = \{x_n\}$. Il est clair que, lorsqu'on parcourt deux ou plusieurs fois un cycle, les nombres tirés ne sont plus indépendants. Il est donc nécessaire de faire l'étude des transitoires et des cycles des suites engendrées par T.

I.2. ETUDE DES TRANSITOIRES ET DES CYCLES DES SUITES ENGENDREES PAR UNE CONGRUENCE LINEAIRE SIMPLE

Dans la littérature concernant les congruences linéaires simples, différents auteurs, comme E.A. Galperin (1978), B.Jansson (1966), D.E. Knuth (1981), G. Marsaglia(1972) et B. Van Cutsem (1980, 1985a et 1985b), se sont intéressés à l'étude des transitoires et des cycles des suites des générateurs du type (a, b, m). Ainsi nous nous limiterons ici à

l'énoncé de quelques résultats relatifs à la période et à la structure de cycle des suites de certains cas particuliers importants de ces générateurs.

I.2.1. THEOREME

Soient $(x) = \{x_n\}$ une suite définie par (1) et τ sa période. On considère alors les cas suivants :

i) $b \neq 0$.

La valeur maximale de τ est m et elle est atteinte si et seulement si on a les trois conditions ci-après :

1. PGCD (a, m) = 1 et PGCD (b, m) = 1.
2. Si un nombre premier p divise m alors il divise a - 1.
3. Si 4 divise m alors 4 divise a - 1.

ii) $b = 0$.

La valeur maximale de τ est m-1 et $\tau = m - 1$ si et seulement si

1. m est un nombre premier et x_0 est non nul.
2. a est une racine primitive modulo m.

iii) $b = 0$ et $m = 2^e$ pour un entier $e > 2$.

La valeur maximale de τ est 2^{e-2} et elle est atteinte pour $a \equiv 3, 5 \bmod 8$ et x_0 impair. Supposons donc que la suite (a, b, m, x_0) soit de période 2^{e-2} et considérons sa structure de cycle :

1. Si $a \equiv 3 \bmod 8$ et $x_0 \equiv 1, 3 \bmod 8$, alors le cycle de la suite $(x) = \{x_n\}$ est une permutation des nombres $8k + 1$ et $8k + 3$ $(k = 0, 1, \ldots, 2^{e-3} - 1)$.

2. Si $a \equiv 3 \bmod 8$ et $x_o \equiv 5, 7 \bmod 8$, alors le cycle de (a, b, m, x_0) est une permutation des entiers $8k + 5$ et $8k + 7$ $(k = 0, 1, \ldots, 2^{e-3} - 1)$.

3. Pour $a \equiv 5 \bmod 8$ et $x_o \equiv 1 \bmod 4$, la séquence $(x_0, x_1, \ldots, x_{\tau-1})$ est une permutation des nombres $4k + 1$ $(k = 0, 1, \ldots, 2^{e-2} - 1)$.

4. Enfin si $a \equiv 5 \bmod 8$ et $x_o \equiv 3 \bmod 4$, alors la séquence $(x_0, x_1, \ldots, x_{\tau-1})$ est une permutation des entiers $4k + 3$ $(k = 0, 1, \ldots, 2^{e-2} - 1)$.

Au vu du théorème précédent on peut, pour un choix convenable des paramètres a, b et m, obtenir un générateur T engendrant une suite (a, b, m, x_0) de cycle suffisamment long. Cependant, avant d'utiliser les nombres pseudo-aléatoires provenant d'une telle suite, il est important de les soumettre à des tests de qualité pour s'assurer de leur adéquation ou de leur inadéquation à la simulation qu'on désire réaliser.

II. TESTS DE QUALITE DES NOMBRES PSEUDO-ALEATOIRES CONGRUENTIELS

Les propriétés statistiques les plus importantes pour une suite de nombres pseudo-aléatoires congruentiels sont l'équidistribution et l'indépendance statistique des termes successifs. On rencontre dans la littérature une liste impressionnante de tests statistiques permettant de s'assurer de ces propriétés (cf. U. Dieter (1971 et 1972), B. Jansson (1966), D.E. Knuth (1981), J. Leroudier (1980), G. Marsaglia(1972) et B. Van Cutsem (1985b)).

Nous nous intéressons ici à trois des tests les plus fiables : le test des treillis, le test spectral et le test sériel. Les deux premiers tests étudient respectivement l'équidistribution et la structure d'hyperplan (ou la "régularité cristalline") des vecteurs

de N.P.A. dans un espace de dimension s strictement supérieur à 1, tandis que le troisième est un test d'indépendance.

Dans le premier paragraphe consacré au test des treillis (ou réseaux) et au test spectral, nous présentons d'abord la structure des grilles engendrées par les vecteurs de N.P.A., puis certaines méthodes de réduction d'une base d'un treillis et de calcul d'un vecteur de norme minimum dans un réseau. Nous précisons ensuite comment on peut utiliser d'une part, une base réduite de chacune de ces grilles pour réaliser le test des treillis et d'autre part, la norme de ce vecteur pour faire le test spectral. Nous terminons le paragraphe par la mise en oeuvre de ces différentes méthodes de réduction d'une base d'un réseau et de calcul d'un vecteur de norme minimum dans un treillis. Aussi profitons nous de cette mise en oeuvre pour comparer d'une part les temps d'exécution des différents algorithmes de réduction d'une base d'un treillis et d'autre part les quotients de Beyer des bases réduites : le quotient de Beyer d'une base est le rapport des normes euclidiennes du vecteur le plus long et du vecteur le plus court de cette base. Quant à la mise en oeuvre du calcul d'un vecteur de norme minimum dans un treillis, nous l'appliquons au test spectral d'un générateur congruentiel d'une table de "Nombres au Hasard".

Le second paragraphe commence par une comparaison entre le test spectral et le test sériel. Partant ensuite de l'estimation de la discrépance d'une suite de vecteurs de N.P.A., on introduit une quantité appelée *figure de mérite*. Celle-ci nous permet de rechercher, pour m et b fixés, des multiplicateurs a tels que deux termes successifs de la suite engendrée par (a, b, m) soient statistiquement indépendants : ces multiplicateurs sont dits optimaux. Enfin nous mettons en oeuvre une méthode de recherche des multiplicateurs optimaux a pour certaines valeurs de m choisies entre les nombres premiers.

II.1. TEST DES TREILLIS et TEST SPECTRAL

A. ETUDE DE LA STRUCTURE DES GRILLES ENGENDREES PAR LES VECTEURS DE NOMBRES PSEUDO-ALEATOIRES CONGRUENTIELS

A.1. Introduction sur la géométrie des grilles et des treillis

a) Rappels sur la notion de norme d'un espace euclidien sur $\mathbb{R}$

Soit B un sous-ensemble d'un espace euclidien E^n de dimension n sur $\mathbb{R}$. On suppose que B est convexe, compact, symétrique et de mesure strictement positive. Alors la *norme* $||\underline{x}||$ d'un vecteur $\underline{x}$ de E^n est définie par

$$||\underline{x}|| = \min \{\lambda \in \mathbb{R}_+ : \underline{x} \in \lambda B\}$$

où, pour tout réel r, l'ensemble rB est donné par

$$rB = \{r\underline{b} : \underline{b} \in B\}.$$

I.1.1. Exemples

On pose $E^n = \mathbb{R}^n$ et $\underline{x} = (x_1, \ldots, x_n)$.

1. Norme L_p

$$||\underline{x}||_p = (|x_1|^p + \cdots + |x_n|^p)^{1/p}, \quad p > 0 \text{ et } p \in \mathbb{N}.$$

Si $p = 2$ alors on a la norme euclidienne. Le sous-ensemble B utilisé est B_p avec

$$B_p = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : |x_1|^p + \cdots + |x_n|^p \leq 1\}.$$

2 . Norme du maximum

$$\|\underline{x}\|_\infty = \max\{|x_i| : i = 1, 2, \cdots, n\}.$$

Le sous-ensemble B utilisé est

$$B_\infty = \{(x_1, \cdots, x_n) \in \mathbb{R}^n : |x_i| \leq 1, \forall i, 1 \leq i \leq n\}.$$

b) concept de grille dans un espace euclidien

Soit $\underline{e}_o$ (resp $(\underline{e}_i, 1 \leq i \leq n)$) un vecteur (resp.une base) de E^n. Alors l'ensemble

$$G_n = \left\{\underline{y} = \underline{e}_o + \sum_{i=1}^{n} y_i \underline{e}_i : (y_1, \ldots, y_n) \in \mathbb{Z}^n\right\}$$

est appelé *grille de vecteur de translation* $\underline{e}_o$ et de base $(\underline{e}_i, 1 \leq i \leq n)$.

II.1.2. LEMME (cf. W.A. Beyer (1972))

Soit $A \subset E^n$ un ensemble de points dont les coordonnées sont des entiers. On suppose que A contient (n + 1) vecteurs $(\underline{e}_i, 0 \leq i \leq n)$ tels que le système $(\underline{e}_i - \underline{e}_o, 1 \leq i \leq n)$ soit linéairement indépendant. Si, pour tout n-uplet d'entiers $(k_1, \ldots, k_n)$ et pour tout (n + 1)-uplet de points $(\underline{a}_o, \underline{a}_1, \ldots, \underline{a}_n)$ de A, on a $(\underline{a}_o + \sum_{i=1}^{n} k_i(\underline{a}_i - \underline{a}_o)) \in A$, alors A est une grille.

c) Notion de treillis et de treillis dual

Une grille de vecteur de translation nul est appelée *treillis ou réseau.*

Soit T_n le treillis

$$T_n = \left\{ \underline{z} = \sum_{i=1}^{n} z_i \underline{e}_i \ : \ (z_1, \ldots, z_n) \in \mathbb{Z}^n \right\}$$

où, rappelons - le, $(\underline{e}_i,\ 1 \leq i \leq n)$ constitue une base de T_n.

On considère ensuite la famille de vecteurs $(\underline{e}_i^*,\ 1 \leq i \leq n)$ définis par

$$\underline{e}_i^* . \underline{e}_k = \delta_{ik} = \begin{cases} 1 & \text{si } i = k \\ 0 & \text{si } i \neq k. \end{cases}$$

Alors l'espace $E^{n\,*}$ engendré par les $(\underline{e}_k^*,\ 1 \leq k \leq n)$ est dit *espace dual* de E^n et l'ensemble T_n^* donné par

$$T_n^* = \left\{ \underline{z} = \sum_{i=1}^{n} z_i \underline{e}_i^* \ : \ (z_1, \ldots, z_n) \in \mathbb{Z}^n \right\}$$

est appelé *treillis dual* de T_n. De plus la famille de vecteurs $(\underline{e}_i^*,\ 1 \leq i \leq n)$ est une base de T_n^* appelée *base duale* de $(\underline{e}_i,\ 1 \leq i \leq n)$.

Le dual B^* de B, B étant le sous-ensemble de E^n ayant servi à définir la norme sur E^n, est

$$B^* = \left\{ \underline{b}^* \in E^{n*} : \ |\underline{b}.\underline{b}^*| \leq 1, \forall\ \underline{b} \in E^n \right\}$$

et la norme de tout élément $\underline{x}^*$ de T_n^* est donnée par

$$\|\underline{x}^*\|^* = \min \left\{ \lambda^* \in \mathbb{R}_+ \ : \ \underline{x}^* \in \lambda^* B^* \right\}.$$

II.1.3. PROPRIETES

1. Pour $p > 1$ la norme L_p sur E^n correspond à la norme L_q sur E^{n*}, où $1/p + 1/q = 1$.

2. La norme du maximum sur E^n correspond à la norme L_1 sur E^{n*} et réciproquement.

3. Pour tout élément $\underline{x}$ de E^n et tout élément $\underline{x}^*$ de E^{n*}, on a

$$|\underline{x}^* . \underline{x}| \leq \|\underline{x}^*\|^* \|\underline{x}\|.$$

II.1.4. REMARQUE

Si $(\underline{e}_i,\ 1 \leq i \leq n)$ est une base d'un treillis, alors celle-ci n'est pas unique car si on prend une matrice unimodulaire $A = (A_{ij},\ 1 \leq i, j \leq n)$, c'est - à-dire, une matrice à coefficients dans $\mathbb{Z}$ et dont la valeur absolue du déterminant est égale à 1 alors le système $(\underline{e}_i',\ 1 \leq i \leq n)$ défini par

$$\underline{e}_i' = \sum_{j=1}^{n} A_{ij}\, \underline{e}_j, \quad 1 \leq i \leq n$$

est une autre base de ce treillis.

Dans toute la suite, si le contraire n'est pas spécifié, E^n est égal à $\mathbb{R}^n$.

A.2. Nombres pseudo- aléatoires et grilles

a) Généralités

Dans la plupart des applications numériques on a besoin de n-uplets de N.P.A. pour n strictement supérieur à 1. Ainsi, pour un décalage k de $\mathbb{N}^*$ fixé, certains auteurs, comme L. Afflerbach (1986), W. A. Beyer(1972) et W.A. Beyer, R.B. Roof et D. Williamson (1971), se sont intéressés à l'étude de la structure de grille de l'ensemble

$$G_n = \{ \underline{g} = \underline{x} + m\underline{z} \ : \ \underline{x} \in V_n, \ \underline{z} \in \mathbb{Z}^n \}$$

où

$$V_n = \{ (x_\ell, \ldots, x_{\ell+n-1}) \ : \ \ell = jk \, , j \in \mathbb{N} \}$$

et où $(x) = \{x_i\}$ est une suite (a, b, m, x_0).

Nous présentons ici cette étude en faisant remarquer que l'emploi d'une sous-suite de $(x) = \{x_i\}$ au lieu d'une sous-suite de la suite de N.P.A. $(u) = \{x_i/m\}$ pour la construction de V_n n'a pas d'influence significative sur les conclusions de cette étude.

II.1.5. DEFINITION

Soient a' et b' deux éléments de $\mathbb{Z}$ et F un ensemble d'entiers consécutifs. Alors l'ensemble des nombres de la forme a'f + b' pour f parcourant F est appelé progression arithmétique (en abrégé P.A.).

II.1.6. THEOREME (cf. W. A. Beyer(1972))

Si pour un décalage k strictement positif, l'ensemble des termes de la sous-suite $(x_k) = \{x_{tk}\}$ de la suite $(x) = \{x_i\}$ donnée par (1) est l'union de r progressions arithmétiques, alors G_n est une union de r grilles.

DEMONTRATION

Soit W_n l'ensemble de toutes les premières composantes de V_n. Par hypothèse W_n est une union de r progressions arithmétiques que nous notons par Q_n^s, $1 \leq s \leq r$. A chacun des Q_n^s, on fait correspondre l'ensemble V_n^s défini par

$$V_n^s = \{(x_i, \ldots, x_{i+n-1}) : x_i \in Q_n^s\}.$$

Ensuite à tout V_n^s associons G_n^s de la même manière qu'à V_n on a associé G_n. On va montrer que G_n^s, $1 \leq s \leq r$, est une grille en vérifiant les deux hypothèses du lemme II.1.2.

Soient $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_n$ n vecteurs unitaires de $\mathbb{R}^n$ ($\underline{u}_i = (u_{i1}, \ldots, u_{in})$ avec $u_{ij} = \delta_{ij}$ pour $1 \leq i, j \leq n$) et $\underline{v}$ un élément de G_n^s. Alors $\underline{v}$ et $((\underline{v} + m\underline{u}_i), 1 \leq i \leq n)$ sont des points de G_n^s tels que le système $(((\underline{v} + m\,\underline{u}_i) - \underline{v}), 1 \leq i \leq n)$ soit linéairement indépendant. Ainsi la première hypothèse du lemme est vérifiée.

Soient $\underline{z}_{i(j)}$, $0 \leq j \leq n$, (n+1) points de G_n^s non nécessairement distincts. La première composante $z_{i(j)}$ de $\underline{z}_{i(j)}$ est de la forme $x_{i(j)} + h_o m$ où $x_{i(j)}$, appartenant à la sième P.A., est le terme d'indice i(j) de la suite (a, b, m, x_o) et où h_o est un entier. Désignons toujours par (a, b, m) le générateur T et donnons nous n entiers quelconques k_i, $1 \leq i \leq n$. On sait que

$$\underline{z}_{i(j)} = (x_{i(j)} + h_o m, T(x_{i(j)}) + h_1 m, \ldots, T^{n-1}(x_{i(j)}) + h_{n-1} m)$$

où $h_0, h_1, \ldots, h_{n-1}$ sont des entiers relatifs et où T^k, $1 \leq k \leq n-1$, est k fois la composée de l'application T. Soit $\underline{x}$ le vecteur défini par

$$\underline{x} = \underline{z}_{i(o)} + \sum_{j=1}^{n} k_j (\underline{z}_{i(j)} - \underline{z}_{i(o)}).$$

Alors on a

$$\underline{x} = (x_{i(o)} + \sum_{j=1}^{n} k_j (x_{i(j)} - x_{i(o)}) + h_o'm,\ T(x_{i(o)} + \sum_{j=1}^{n} k_j (x_{i(j)} - x_{i(o)})) + h_1'm, \ldots,$$

$$T^{n-1}(x_{i(o)} + \sum_{j=1}^{n} k_j (x_{i(j)} - x_{i(o)})) + h_{n-1}'m)$$

où $h_o', \ldots, h_{n-1}'$ sont des entiers relatifs. Comme $x_{i(j)}$ appatient à la sième P.A. il en est de même pour $(x_{i(o)} + \sum_{j=1}^{n} k_j (x_{i(j)} - x_{i(o)}))$ et on en déduit que $\underline{x} \in G_n^s$.

C.Q.F.D.

b) Structure de grille d'un générateur mixte de période m

Dans ce paragraphe, on suppose que la suite (a, b, m, x_o) est de période m et on note par d le PGCD de n et de m. Alors pour k = 1, les ensembles V_n et G_n deviennent respectivement

$$V_n^1 = \{(x_i, \ldots, x_{i+n-1}) \ : \ x_j \equiv ax_{j-1} + b \bmod m, i < j < i+n, 0 \leq i < m\}$$

et

$$G_n^1 = \{\underline{v} = \underline{x} + m\underline{z} \ : \ \underline{x} \in V_n^1 , \ \underline{z} \in \mathbb{Z}^n\}.$$

D'après le théorème II.1.6. G_n^1 forme une grille puisque le cycle de la suite (a, b, m, x_o) est une permutation des termes de la progression arithmétique $(r + 1)$, $-1 \leq r \leq m - 2$. Mais dans les applications on s'intéresse assez souvent au cas $k = n$. Les ensembles V_n et G_n sont alors donnés respectivement par

$$V_n^2 = \{\underline{x}_i \in V_n^1 : \underline{x}_i = (x_{in}, \cdots , x_{in+n+1}), 0 \leq i < m/d\}$$

et

$$G_n^2 = \{\underline{v} = \underline{x} + m\underline{z} \ : \ \underline{x} \in V_n^2, \ \underline{z} \in \mathbb{Z}^n\}.$$

Il s'agit maintenant de montrer que G_n^2 est une grille et donc une sous grille de G_n^1.

II.1.7 THEOREME(cf. L. Afferbach(1986))

Si la période de la suite (a, b, m, x_0) est m, alors l'ensemble G_n^2 forme une grille de vecteur de translation

$$\underline{b}_o(x_o) = x_o(1, a, \ldots , a^{n-1}) + b\,(0, 1, 1 + a, \ldots , 1 + a + \ldots + a^{n-2})$$

et de base

$$\underline{b}_1 = d(1, a , \ldots , a^{n-1})$$

$$\underline{b}_2 = (0, m , \ldots ,0)$$

$$\vdots$$

$$\underline{b}_n = (0, \ldots , m)$$

DEMONSTRATION

On a

$$x_j \equiv a^j x_o + b(1 + a + \ldots + a^{j-1}) \bmod m, \quad \forall\ j \geq 1.$$

A cause de l'opération "mod m", le vecteur $(x_0, x_1, \ldots, x_{n-1})$ de V_n^2 peut se mettre sous la forme

$$(x_o, x_1, \ldots, x_{n-1}) = (x_o, ax_o + b, \ldots, a^{n-1}x_o + b(1 + a + \ldots + a^{n-2}))$$

$$= x_o(1, a, \ldots, a^{n-1}) + b(0, 1, 1 + a, 1 + a + \ldots + a^{n-2})$$

$$= \underline{b}_o(x_o).$$

Ainsi les éléments $\underline{x}_i$ de V_n^2 s'écrivent :

$$\underline{x}_i = (x_o, x_1, \ldots, x_{n-1}) + (x_{in} - x_o, \ldots, x_{in+n-1} - x_{n-1}).$$

Mais

$$x_{in+k} - x_k \equiv a^k(x_{in} - x_o) \bmod m$$

Donc

$$\underline{x}_i \equiv \underline{b}_o(x_o) + (x_{in} - x_o)(1, a, \ldots, a^{n-1}) \bmod m$$

On va montrer maintenant que $(x_{in} - x_o) \bmod m$ est de la forme μd, $0 \leq \mu < m/d$.

On a

$$(x_{in} - x_o) \equiv (a^{in} - 1)x_o + b(1 + a + \ldots + a^{in-1}) \mod m$$

$$\equiv (1 + a^d + \ldots + a^{in-d})((a^d - 1)x_o + b(1 + a + \ldots + a^{d-1})) \mod m$$

$$\equiv (1 + a^d + \ldots + a^{in-d})(x_d - x_o) \mod m.$$

Si on considère la suite $x_i \equiv ax_{i-1} + b \mod d$, elle est de période d puisque d divise m et donc $x_d \equiv x_o \mod d$; cela implique que $(x_{in} - x_o) \mod m$ est de la forme μd avec $0 \leq \mu < m/d$. Comme toutes les expressions $(x_{in} - x_o) \mod m$ sont distinctes pour les différentes valeurs de i avec $0 \leq i < m/d$, μ parcourt toutes les valeurs entières de $[0, m/d[$. Donc pour tout i, il existe μ $(0 \leq \mu < m/d)$ tel que

$$x_i \equiv \underline{b}_o(x_o) + \mu d\,(1, a, \ldots, a^{n-1}) \mod m.$$

Pour obtenir l'ensemble G_n^2 tout entier il faut ajouter aux éléments de V_n^2 les multiples entiers des vecteurs $(m, 0, \ldots, 0)$, $(0, m, 0, \ldots, 0)$, $\ldots$, $(0, \ldots, m)$. On a alors

$$G_n^2 = \left\{ \begin{array}{c} \underline{b}_o(x_o) + \mu \underline{b}_1 + z_1(m, 0, \ldots, 0) + z_2 \underline{b}_2 + \ldots + z_n \underline{b}_n : \\ (z_1, \ldots, z_n) \in \mathbb{Z}^n, \mu \in \mathbb{N}, 0 \leq \mu < m/d \end{array} \right\}.$$

Mais

$$(m, 0, \ldots, 0) = m\,(1, a, \ldots, a^{n-1}) - a\,(0, m, \ldots, 0) - \ldots - a^{n-1}(0, \ldots, m)$$

$$= (m/d)\,\underline{b}_1 - a\,\underline{b}_2 - \ldots - a^{n-1}\,\underline{b}_n$$

et donc

$$G_n^2 = \{\underline{b}_o(x_o) + z_1 \underline{b}_1 + z_2 \underline{b}_2 + \ldots + z_n \underline{b}_n : (z_1, \ldots, z_n) \in \mathbb{Z}^n\}.$$

C.Q.F.D.

II.1.8. REMARQUES

1. Pour d choix différents de x_o, avec $d > 1$, on a d sous grilles distinctes dont l'union donne la grille G_n^1.

2. Si $d = 1$ alors on a $G_n^1 = G_n^2$.

Mais, en pratique, au lieu d'utiliser les points de V_n^1 on se sert plutôt de ceux de V_n' avec

$$V_n' = V_n^1 / m = \{\underline{x} / m : \underline{x} \in V_n^1\}.$$

Ainsi l'extension G_n' correspondant, c'est - à- dire,

$$G_n' = \{\underline{x} / m + \underline{z} : \underline{x} \in V_n', \underline{z} \in \mathbb{Z}^n\}$$

est une grille de vecteur de translation

$$\underline{b}_o(x_o) = x_o(1, a, \ldots, a^{n-1}) / m + b\,(0, 1, 1 + a, \ldots, 1 + a + \ldots + a^{n-2}) / m$$

et de base

$$\underline{b}_1 = (1, a, \ldots, a^{n-1}) / m, \quad \underline{b}_2 = (0, 1, 0, \ldots, 0), \quad \ldots, \quad \underline{b}_n = (0, \ldots, 0, 1).$$

Comme V_n^1 est indépendant du choix de x_o, on peut prendre $x_o = 0$ et on a

$\underline{b}_o(0) = \underline{b}_o = b(0, 1, 1 + a, \ldots, 1 + a + \ldots + a^{n-2}) / m.$

Cette dernière remarque sera utile dans l'étude du test spectral.

c) Structure de grille d' un générateur multiplicatif

On suppose dans ce paragraphe que b est nul et on ne s'intéresse qu'aux cas couramment rencontrés dans les applications, c'est-à-dire, ceux pour lesquels la suite (a, b, m, x_o) est de période (m-1) ou m / 4 (cf. théorème I.2.1).

c.1 m est un nombre premier et a est une racine primitive modulo m

La période de la suite (a, b, m, x_o) est alors égale à m-1 pour tout x_o non nul et pour $k = 1$ les ensembles V_n et G_n sont respectivement

$$V_n^3 = \left\{ \underline{x} = (x_i, \cdots, x_{i+n-1}) \ : \ x_j \equiv a x_{j-1} \bmod m, \ i < j < i + n \ , 0 \le i < m-1 \right\}$$

et

$$G_n^3 = \left\{ \underline{v} = \underline{x} + m\underline{z} \ : \ \underline{x} \in V_n^3, \ \underline{z} \in \mathbb{Z}^n \right\}.$$

Comme les termes du cycle de $(x) = \{x_i\}$ constituent une permutation de la progression arithmétique $f + 1$ $(f = 0, 1, \ldots, m - 2)$, G_n^3 est d'après le théorème II.1.6 une grille de l'espace $[0, m[^n$ privé de l'origine.

On pose

$$d = \text{PGCD}\ (n, \ m - 1)$$

et on suppose que $k = n$. Alors les ensembles V_n et G_n deviennent respectivement

$$V_n^4(x_o) = \left\{ \underline{x}_i \in V_n^3 \ : \ \underline{x}_i = (x_{in}, \ldots, x_{in+n-1}) \right\}$$

et

$$G_n^4(x_o) = \{\underline{y} = \underline{x} + m\underline{z} \ : \ \underline{x} \in V_n^4(x_0), \ \underline{z} \in \mathbb{Z}^n\}.$$

Si $d \neq 1$ alors V_n^3 est l'union disjointe des d sous-ensembles $V_n^4(x_o)$ correspondant aux d choix distincts du terme initial x_o, mais en général $G_n^4(x_o)$ n'a pas une structure de grille.

c.2 m est une puissance de 2 et la période de la suite est m/4

Soit $(x) = \{x_i\}$ une suite (a, b, m, x_0) avec $m = 2^e$, $e > 2$, $b \equiv 5 \mod 8$ et x_o impair. On pose $d = \text{PGCD}(n, 2^{e-2})$.

D'après le théorème I.2.1. on a les trois résultats suivants :

1. La période τ de (x) est 2^{e-2}.

2. Si $a \equiv 1 \mod 4$ alors le cycle $(x_o, x_1, \ldots, x_{\tau-1})$ est une permutation des termes de la progression arithmétique $4\mu + 1$ $(\mu = 0, 1, \ldots, 2^{e-2} - 1)$.

3. Pour $x_0 \equiv 3 \mod 4$, la séquence $(x_o, \ldots, x_{\tau-1})$ est une permutation des termes de la progression arithmétique $4\mu + 3$ $(\mu = 0, 1, 2, \ldots, 2^{e-2} - 1)$.

Pour $k = 1$, les ensembles V_n et G_n sont respectivement

$$V_n^5(x_o) = \{\underline{x} = (x_i, \cdots, x_{i+n-1}) \ : x_j \equiv a x_{j-1} \mod 2^e, \ i < j < i + n, 0 \leq i < 2^{e-2}\}$$

et

$$G_n^5(x_o) = \{\underline{y} = \underline{x} + m\underline{z} \ : \ \underline{x} \in V_n^5(x_o), \ \underline{z} \in \mathbb{Z}^n\}.$$

Des trois résultats précédents et du théorème II.1.6. il est immédiat que $G_n^5(x_o)$ est une grille.

Considérons maintenant les ensembles V_n et G_n pour $k = n$. On a respectivement

$$V_n^6(x_o) = \left\{ \underline{x}_i \in V_n^5(x_o) : \underline{x}_i = (x_{in}, \ldots, x_{in+n-1}),\ 0 \le i < 2^{e-2}/d \right\}$$

et

$$G_n^6(x_o) = \left\{ \underline{v} = \underline{x} + m\underline{z} : \underline{x} \in V_n^6(x_o),\ \underline{z} \in \mathbb{Z}^n \right\}.$$

II .1. 9. THEOREME(cf. L. Afferbach(1986))

Pour tout x_o impair, l'ensemble $G_n^6(x_o)$ est une grille de vecteur de translation

$$\underline{b}_o(x_o) = x_o\,(1, a, \ldots, a^{n-1})$$

et de vecteurs de base

$$\underline{b}_1 = 4d\,(1, a, \ldots, a^{n-1}),\quad \underline{b}_2 = (0,\ 2^e,\ 0, \ldots, 0),\ \ldots,\ \underline{b}_n = (0, \ldots, 2^e).$$

DEMONSTRATION

De la relation

$$x_{i+1} \equiv a^{\ell} x_i \bmod 2^e$$

où i et ℓ sont deux entiers naturels, on déduit que

$$\begin{aligned} x_i &= (x_{in}, x_{in+1}, \ldots, x_{in+n-1}) \\ &= (x_o, x_1, \ldots, x_{n-1}) + (x_{in} - x_o, \ldots, x_{in+n-1} - x_o) \\ &= x_o(1, a, \ldots, a^{n-1}) + (x_{in} - x_o)\,(1, a, \ldots, a^{n-1}). \end{aligned}$$

On va montrer que $(x_{in} - x_o) \equiv (a^{in} - 1)\, x_o \bmod 2^c$ est de la forme $4\mu d$, μ étant un entier avec $0 \leq \mu < 2^c/4d$. Pour cela, on montre d'abord que $a^{2^\ell} \equiv 1 \bmod 2^{2+\ell}$, pour tout élément ℓ de $\mathbb{N}^*$.

Puisque $a \equiv 5 \bmod 8$, on a $a^2 \equiv 1 \bmod 8$. Ce qui implique que

$$a^2 \equiv 1 \bmod 16 \quad \text{ou} \quad a^2 \equiv 8 + 1 \bmod 16.$$

Dans chacune des deux possibilités, on a $a^4 \equiv 1 \bmod 16$. Plus généralement

$a^{2^{\ell-1}} \equiv 1 \bmod 2^{2+\ell-1}$ signifie que $a^{2^{\ell-1}} \equiv 1$ ou $(2^{2+\ell-1} + 1) \bmod 2^{2+\ell}$.

Ce qui entraîne que

$$a^{2^\ell} \equiv 1 \text{ ou } (2^{2+\ell-1})^2 + 2^{2+\ell} + 1 \bmod 2^{2+\ell}.$$

En définitive on a

$$a^{2^\ell} \equiv 1 \bmod 2^{2+\ell}, \quad \forall\ \ell \in \mathbb{N}^*.$$

D'autre part, d et n sont de la forme $d = 2^s$ et $n = h\,2^s$ pour deux entiers s et h convenables. Par conséquent

$$a^{in} \equiv a^{ih2^s} \equiv (a^{2^s})^{ih} \equiv 1 \bmod 2^{2+s}$$

et on en déduit que $(x_{in} - x_o) \bmod 2^c$ est de la forme $4\mu d$, pour un entier μ avec $0 \leq \mu < 2^c/4d$. Comme les $2^c/4d$ expressions $(x_{in} - x_o)$ sont deux à deux distinctes

pour les différents entiers i, $0 \leq i \leq 2^e/4d$, μ prend tous les entiers appartenant à l'intervalle $[0, 2^e/4d[$. Donc pour tout i il existe un entier μ tel que

$$\underline{x}_i \equiv x_0 (1, a, \ldots, a^{n-1}) + 4\mu d (1, a, \ldots, a^{n-1}) \bmod 2^e$$

On procède ensuite de façon analogue à la démonstration de la fin du théorème II.1.7 pour obtenir le résultat.

C.Q.F.D.

II.1.10 REMARQUES

1. Si $d = 1$ alors $G_n^6 = G_n^5$ et le théorème II.1.9 nous donne une base pour G_n^5.

2. On considère une suite $(a, 0, 2^e, x_o)$ avec $e > 2$, x_o impair et $a \equiv 3 \bmod 8$. Alors sa période τ est égale à 2^{e-2}.

Pour $k = 1$, les ensembles V_n et G_n sont donnés respectivement par

$$V_n^7(x_o) = \left\{ \underline{x} = (x_i, \cdots, x_{i+n-1}) : x_j \equiv a x_{j-1} \bmod 2^e,\ i < j < i + n,\ 0 \leq i < 2^{e-2} \right\}$$

et

$$G_n^7(x_o) = \left\{ \underline{y} = \underline{x} + 2^e \underline{z} : \underline{x} \in V_n^7(x_o),\ \underline{z} \in \mathbb{Z}^n \right\}.$$

et, pour $k = n$, on a respectivement

$$V_n^8(x_o) = \left\{ \underline{x}_i \in V_n^7(x_o) : \underline{x}_i = (x_{in}, \ldots, x_{in+n-1}),\ 0 \leq i < 2^{e-2}/d,\ d = \mathrm{PGCD}(n, 2^{e-2}) \right\}$$

et

$$G_n^8(x_o) = \left\{ \underline{y} = \underline{x} + 2^e \underline{z} : \underline{x} \in V_n^8(x_o),\ \underline{z} \in \mathbb{Z}^n \right\}.$$

On pose $d = PGCD(n, 2^{c-2})$. Alors pour tout entier d strictement supérieur à 1, un procédé analogue à celui de la démonstration du théorème II.1.9. permet de conclure que $G_n^8(x_o)$ est une grille. Mais d'après le théorème I.2.1. et le lemme II.1.6. $G_n^7(x_o)$ est une union de deux grilles et cette union n'est pas une grille. C'est l'une des raisons pour lesquelles le cas $a \equiv 3 \bmod 8$ et x_o impair est moins intéressant dans les applications.

B . PRESENTATION DE QUELQUES ALGORITHMES DE REDUCTION D'UNE BASE D'UN TREILLIS ET DE QUELQUES METHODES DE CALCUL D'UN VECTEUR DE NORME MINIMUM DANS UN RESEAU

Soit $(x) = \{x_n\}$ une suite (a, b, m, x_o) provenant de l'un des générateurs (a, b, m) considérés dans le théorème I.2.1. Nous avons vu au paragraphe précédent que pour deux entiers naturels $k > 0$ et $n > 1$ fixés, l'ensemble

$$G_n = \left\{ \underline{v} = \underline{x} + m\underline{z} \ : \ \underline{x} \in V_n, \ \underline{z} \in \mathbb{Z}^n \right\}$$

où

$$V_n = \left\{ (x_\ell, \ldots, x_{\ell+n-1}) \ : \ \ell = jk, j \in \mathbb{N} \right\}$$

est une grille ou une union de deux ou plusieurs grilles . Cette structure de grille a une certaine importance lors de l'étude de la distribution des points de V_n/m (resp V_n) dans l'espace $[0, 1[^n$ (resp $[0,m[^n$). Avant de faire un aperçu sur l'historique de cette étude, nous considérons un exemple sur la répartition des points de V_n dans l'espace $\mathbb{R}^n$.

Exemple

On pose

$a = 1 \quad b = 1 \quad m = 2 \quad x_0 = 0.$

Alors la suite $(x) = \{x_n\}$ est donnée par

0 1 0 1 0 1 0 1 0 1 . . .

Pour $k = 1$ et $n = 2$ on a

$V_2 = \{(0, 1), (1, 0)\}$

$= \{ \underline{v}_2, \underline{v}_1 \}$

et

$$G_2 = \left\{\underline{v}_1 + 2\underline{z} : \underline{z} \in \mathbb{Z}^2\right\} \cup \left\{\underline{v}_2 + 2\underline{z} : \underline{z} \in \mathbb{Z}^2\right\}$$

$$= G_2' \cup G_2''$$

Sur le schéma ci-dessous (Fig. 1), on voit que les points de G_2 et donc ceux de V_2 sont situés sur 3 familles de droites parallèles de $\mathbb{R}^2$. On pourra remarquer que les points de G_2' sont représentés par "■" et ceux de G_2'' par "◘". Dans une famille donnée, si h_1 est la distance entre deux droites adjacentes et h_2 la distance entre deux autres droites adjacentes, alors h_1 est identique à h_2. Sur le schéma, les distances entre deux droites adjacentes pour les trois familles sont respectivement d20, d21, d22.

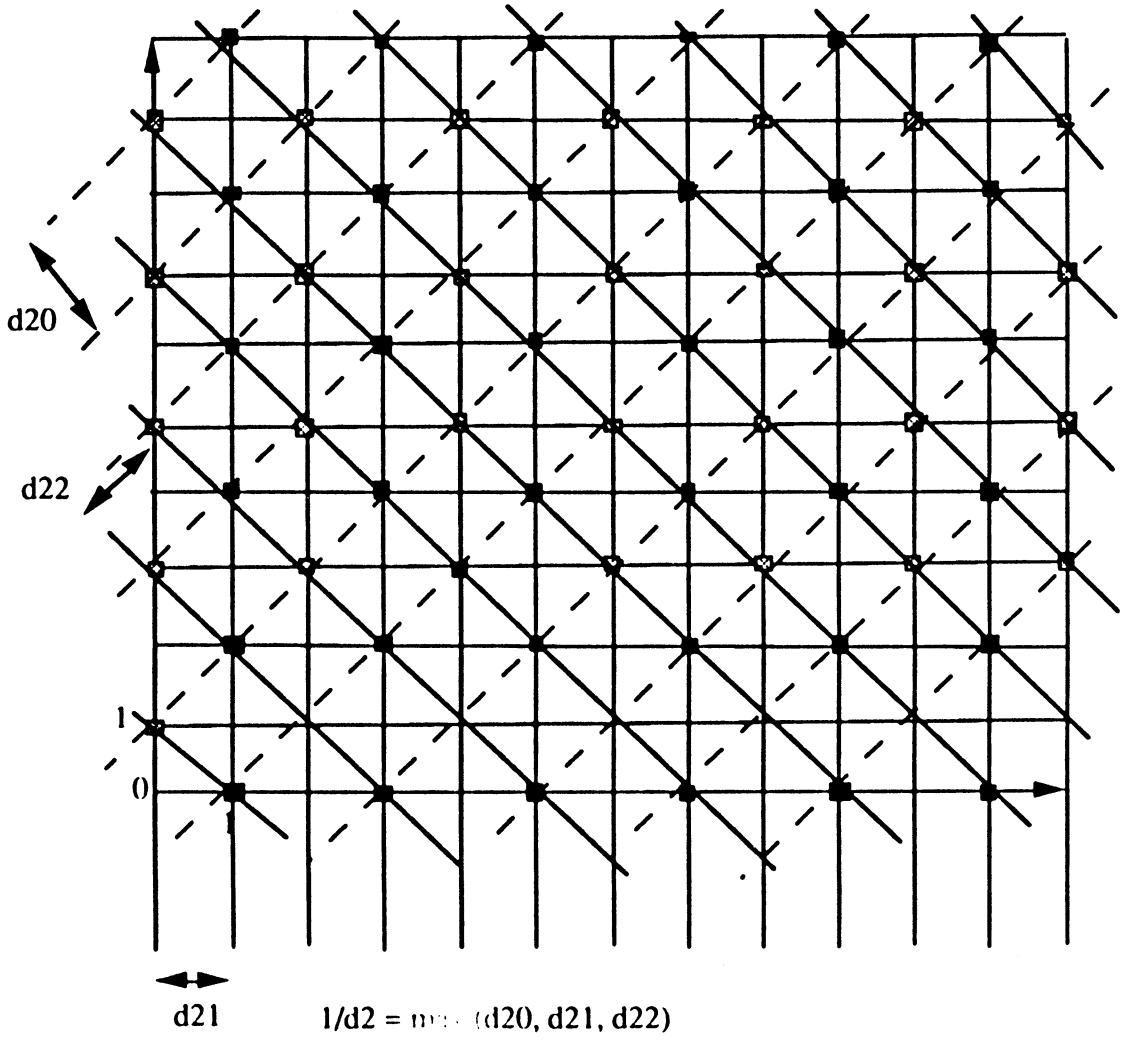


Fig. 1

L'exemple de répartition des points de V_n que nous venons de voir est en fait une illustration de certains résultats généraux établis par G. Marsaglia.

En effet, G. Marsaglia (cf. G. Marsaglia (1968)) a montré que les points de V_n/m (resp V_n) sont situés sur des familles d'hyperplans parallèles de l'espace $[0, 1[^n$ (resp $[0, m[^n$). Il a également établi que les hyperplans d'une même famille contiennent tous les points de V_n/m si l'espace de travail est $[0, 1[^n$ ou tous les points de V_n si cet espace est $[0, m[^n$. De plus si h_1 est la distance entre deux hyperplans adjacents d'une

famille donnée et h_2 la distance entre deux autres hyperplans adjacents de cette même famille, alors h_1 est identique à h_2.

Mais R.R. Coveyou et R.D. Mackpherson (1967) avaient considéré une année auparavant, sous l'angle analytique, le problème de distribution de ces points. Ainsi ils développèrent un algoritme de calcul d'une quantité $1/d_n$ qui, vue sous l'approche géométrique envisagé par G. Marsaglia, est le maximum des distances entre les hyperplans adjacents dans les familles d'hyperplans parallèles contenant tous les points de V_n/m (ou V_n).

Cet algoritme fut sensiblement amélioré par D.E. Knuth (1969) . Précisons que l'algorithme de R. R. Coveyou et R. D. Mackpherson et celui de D. E. Knuth sont basés sur la transformée de Fourier d'une fonction définie sur un ensemble fini de points.

U. Dieter (1975) utilisant le concept de treillis apporta une simplification à l'algorithme de D.E. Knuth : La procédure développée calcule un vecteur de norme minimum du dual T_n^* du treillis T_n, où T_n est le treillis engendré par la base de G_n. Si on considère la norme euclidienne alors la longueur du vecteur calculé est d_n. En revanche si on prend la norme L_1, alors la longueur du vecteur correspondant est le nombre minimum d'hyperplans parallèles de l'espace $[0, m[^n$ contenant tous les points de V_n. Se servant à son tour de ce concept, D. E. Knuth(1981) améliora son propre algorithme.

On remarque que dans les algorithmes de U. Dieter et de D.E. Knuth(1981), le calcul d'un vecteur de norme minimum dans un treillis comporte deux phases : dans la première on réduit une base donnée du treillis considéré et dans la seconde on se sert de la base réduite pour déterminer un sous-ensemble strict du treillis contenant un vecteur de norme minimum, puis on calcule le vecteur désiré par recherche exhaustive sur ce sous-ensemble. Cette seconde phase est dite phase de recherche exhaustive.

Nous allons d'abord présenter les algorithmes de réduction de U. Dieter, D.E. Knuth et aussi l'algorithme de réduction de A.K. Lenstra, H.W. Lenstra et L. Lovasz (cf. LLL(1982)) qui a été à l'origine construit pour une tout autre motivation,

c'est-à-dire, la factorisation des polynômes à coefficients entiers. Ensuite nous considérons les phases de recherche exhaustive relatives à chacune de ces techniques de réduction. A côté de ces méthodes standard de calcul d'un vecteur de norme minimum, on a l'algoritme de U. Fincke et M. Pohst n'ayant pas de phase de réduction, mais basé sur la décomposition de Cholesky d'une forme quadratique définie positive. Nous combinons cet algorithme et chacune des méthodes de réduction pour obtenir un autre procédé de calcul d'un vecteur de norme minimum dans un treillis.

B.1. FORMULATION DU PROBLEME DE CALCUL D'UN VECTEUR DE NORME MINIMUM DANS UN TREILLIS

Soient G un treillis de l'espace euclidien $\mathbb{R}^n$ et W le réel défini par

$$W = \min \left\{ \|\underline{y}\| : \underline{y} \in G , \underline{y} \neq \underline{0} \right\} .$$

Il s'agit de trouver un vecteur non nul $\underline{x}$ de G tel que $\|\underline{x}\| = W$.

Le réel W étant inconnu, on remplace le problème ci-dessus par celui qui consiste à chercher un vecteur $\underline{x}$ non nul de G et de norme minimum dans l'ensemble des $\underline{y}$ de G tels que

$$(2) \qquad \|\underline{y}\| \leq v$$

où v est la norme d'un vecteur $\underline{V}$ non nul de G. Mais il est plus avantageux de choisir $\underline{V}$ de norme suffisamment petite pour qu'on puisse faire pratiquement une recherche exhaustive sur les $\underline{y}$ vérifiant (2). C'est pourquoi on s'intéresse aux vecteurs d'une base réduite de G : pour simplifier on dira qu'une base est réduite si les vecteurs qui la composent sont "assez courts" et "assez orthogonaux "

B.2 METHODES ET ALGORITHMES DE REDUCTION D'UNE FORME QUADRATIQUE OU D'UNE BASE DE TREILLIS

a) Méthode et algorithme de réduction de base de U. Dieter

a.1 présentation de la méthode

Soient $(\underline{e}_i,\ 1 \le i \le n)$ une base d'un treillis G et $(\underline{e}_i^*,\ 1 \le i \le n)$ la base duale. Si $\underline{x} = z_1 \underline{e}_1 + \cdots + z_n \underline{e}_n$ est un élément non nul de G de norme minimum alors on a

$$|z_i| = |\underline{e}_i^* . \underline{x}| \le \|\underline{e}_i^*\|^* \|\underline{x}\| \le c_i$$

où

$$c_i = [\,\|\underline{e}_i^*\|^* \min\{\|\underline{e}_k\|,\ 1 \le k \le n\}\,],\ i = 1, \ldots, n$$

et où pour tout réel r, [r] est la partie entière de r. On pose

$$P = \prod_{i=1}^{n} (2c_i + 1).$$

On va maintenant faire des transformations simultanées des bases $(\underline{e}_i,\ 1 \le i \le n)$ et $(\underline{e}_i^*,\ 1 \le i \le n)$ jusqu'à ce qu'il soit impossible de diminuer la quantité P : à ce moment là on dira que les deux bases sont réduites. Pour cela on se propose de trouver une transformation vérifiant l'une au moins des deux propriétés suivantes :

i) La norme de la transformée de $\underline{e}_i$, $1 \le i \le n$, est inférieure ou égale à $\|\underline{e}_i\|$.

ii) La norme de la tranformée de $\underline{e}_i^*$, $1 \le i \le n$, est inférieure ou égale à $\|\underline{e}_i^*\|^*$.

On considère alors les deux types de transformations unimodulaires T_i et T_i^*, pour i fixé ($i = 1, 2, \ldots, n$), définies respectivement par

$$T_i : \quad \underline{e}_i \leftarrow \underline{e}_i, \quad \underline{e}_i^* \leftarrow \underline{e}_i^* + \sum_{\substack{j=1 \\ j \neq i}}^{n} m_j \underline{e}_j^*, \quad \underline{e}_k \leftarrow \underline{e}_k - m_k \underline{e}_i, \quad \underline{e}_k^* \leftarrow \underline{e}_k^*, \quad k \neq i \text{ et } 1 \leq k \leq n$$

et

$$T_i^* : \quad \underline{e}_i^* \leftarrow \underline{e}_i^*, \quad \underline{e}_i \leftarrow \underline{e}_i + \sum_{\substack{j=1 \\ j \neq i}}^{n} m_j^* \underline{e}_j, \quad \underline{e}_k^* \leftarrow \underline{e}_k^* - m_k^* \underline{e}_i^*, \quad \underline{e}_k \leftarrow \underline{e}_k, \quad k \neq i \text{ et } 1 \leq k \leq n.$$

où la notation algorithmique $\underline{x} \leftarrow \underline{z}$ signifie qu'on affecte au vecteur $\underline{x}$ la valeur du vecteur $\underline{z}$.

Les entiers m_k sont choisis de telle sorte que les nouveaux vecteurs $\underline{e}_i$, $1 \leq i \leq n$, soient de norme minimum. Ainsi m_k est déterminé par

$$(\underline{e}_k - m_k \underline{e}_i)^2 \leq (\underline{e}_k - (m_k + 1)\underline{e}_i)^2$$

et

$$(\underline{e}_k - m_k \underline{e}_i)^2 \leq (\underline{e}_k - (m_k - 1)\underline{e}_i)^2.$$

Soit

$$-0.5 + \underline{e}_k.\underline{e}_i/\underline{e}_i^2 \leq m_k \leq 0.5 + \underline{e}_k.\underline{e}_i/\underline{e}_i^2, \quad 1 \leq k \leq n \text{ et } k \neq i.$$

Pour déterminer m_k de façon unique, on remplace le second signe d'inégalité $\leq$ par $<$. Ce qui suggère

$$(3) \qquad m_k = [\, 0.5 + \underline{e}_i.\underline{e}_k/\underline{e}_i^2].$$

Un choix analogue des quantités m_k^* conduit à

$$(4) \qquad m_k^* = [0.5 + \underline{e}_i^* . \underline{e}_k^* / \underline{e}_i^{*2}].$$

Il est clair que les transformées par T_i (resp T_i^*) vérifient la propriété i) (resp ii)). Il serait sympatique si T_i satisfaisait ii). On montre cependant que ce n'est pas toujours le cas (cf. U. Dieter (1975)) . On pourra remarquer que les vecteurs $(\underline{e}_i,\ 1 \leq i \leq n)$ et $(\underline{e}_i^*,\ 1 \leq i \leq n)$ résultant de l'une ou l'autre des applications T_i et T_i^* vérifient $\underline{e}_i . \underline{e}_j^* = \delta_{ij},\ 1 \leq i, j \leq n$, où δ_{ij} est le symbole de Kronecker.

a.2 Description de l' algorithme de réduction

a.2.1 Préparation de l'algorithme

Pour une base $(\underline{e}_i,\ 1 \leq i \leq n)$ d'un treillis G donné, on calcule le dual $(\underline{e}_i^*,\ 1 \leq i \leq n)$, les bornes c_i et l'entier P. On cherche ensuite à appliquer la transformation T_i^* aux bases $(\underline{e}_i,\ 1 \leq i \leq n)$ et $(\underline{e}_i^*,\ 1 \leq i \leq n)$. Pour cela on calcule d'abord les entiers m_k^* en utilisant (4), puis on applique T_i^* si les m_k^* ne sont pas tous nuls. On itère ce processus jusqu'à ce que n calculs successifs des m_k^* aient donné lieu à n transformations T_i^* sans succès : on dira que la transformation T_i^* (resp T_i) est sans succès lorsque tous les entiers m_k^* (resp m_k) sont nuls ou lorsque l'application de T_i^* (resp T_i) aux bases $(\underline{e}_i,\ 1 \leq i \leq n)$ et $(\underline{e}_i^*,\ 1 \leq i \leq n)$ a donné lieu à une valeur de P supérieure ou égale à la précédente. On considère alors la transformation T_i et on itère le processus analogue à celui qu'on vient de présenter. L'algorithme de réduction s'arrête lorsqu'on a n transformations consécutives sans succès de l'un des T_i et T_i^* suivies de n autres transformations consécutives sans succès de l'autre transformation.

Dans l'algorithme ci - après nous avons adopté les notations suivantes :

- Tout vecteur $\underline{v}_j$ de dimension n est assimilé à la matrice ligne $(v_{j1}, \ldots, v_{jn})$ où v_{js}, $1 \leq j \leq s$, est la sième composante de $\underline{v}_j$ par rapport à une certaine base.
- La variable D contient les différents majorants de W, norme d'un vecteur de norme minimum dans le treillis G considéré.
- C contient les différentes valeurs de P.
- q vaut 1 si la transformation en cours est T_i et -1 si c'est T_i^*.
- t^* vaut 0 si on a eu n transformations consécutives sans succès pour T_i^* et $t = 0$ si c'est le cas pour T_i.

a. 2. 2 Algorithme de réduction de U. Dieter

ALGORITHME RBSD

Données

- $(\underline{e}_i,\ 1 \le i \le n)$, une base d'un treillis G de dimension n.
- $(\underline{e}_i^*,\ 1 \le i \le n)$, la base duale de $(\underline{e}_i,\ 1 \le i \le n)$.

Résultats Réduites des deux bases suivant la méthode de U. Dieter.

Début

[initialisation]

$D \leftarrow \min\{\|\underline{e}_i\|,\ 1 \le i \le n\}$, $C \leftarrow \prod_{j=1}^{n} (2\,[D\|\underline{e}_j^*\|^*]+1)$, $q \leftarrow -1$, $i \leftarrow n+1$, $t \leftarrow t^* \leftarrow n$.

Tant que $(t+t^* \neq 0)$ faire

Début

Pour $k=1$ jusqu'à n faire

Début

$r_k \leftarrow \|\underline{e}_k\|$, $r_k^* \leftarrow \|\underline{e}_k^*\|^*$, si $r_k < D$ alors faire $D \leftarrow r_k$ fsi.

fdébut

fpour

Pour $k = 1$ jusqu'à n faire $c_k \leftarrow [D r_k^*]$ fpour.

$P \leftarrow \sum_{j=1}^{n} (2c_j + 1)$

Si $P < C$ alors début $t \leftarrow t^* \leftarrow n$, $C \leftarrow P$, $E \leftarrow 3$ fdébut

Sinon

Début

Si $(q = -1)$ faire $t^* \leftarrow t^* - 1$ Sinon $t \leftarrow t-1$ fsi

Si $t^* = 0$ alors $E \leftarrow 4$ sinon $E \leftarrow 3$ fsi

fdébut

fsi

Tant que $((E = 3)$ ou $(E = 4))$ et $(t + t^* \neq 0)$ faire

début

Si $(E=3)$ alors faire

[calcul et application eventuelle de T^*]

Tant que $(E = 3)$ et $(t+t^* \neq 0)$ faire

début

$i \leftarrow i-1$, si $(i=0)$ alors $i \leftarrow n$ fsi, $cc1 \leftarrow 0$

Pour (k = 1) jusqu' à n faire

Si (k ≠ i) alors

début

$m_k^* \leftarrow [0.5 + \sum_{j=1}^{n} e_{kj}^* e_{ij}^* / \sum_{j=1}^{n} e_{ij}^{*2}]$, si ($m_k^* \neq 0$) alors cc1 ← 1 fsi

fdébut

fsi

fpour

si (cc1 = 0) alors début $t^* \leftarrow t^* - 1$, si ($t^* = 0$) alors E ← 4 fsi fdébut

sinon

début

pour (j=1) jusqu' à n faire $e_{ij} \leftarrow e_{ij} + \sum_{\substack{k=1 \\ k \neq i}}^{n} m_k^* e_{kj}$ fpour

pour (k=1) jusqu' à n faire

si (k≠i) alors pour (j=1) jusqu' à n faire $e_{kj}^* \leftarrow e_{kj}^* - m_k^* e_{ij}^*$ fpour fsi

fpour

q ← -1, E ← 2

fdébut

fsi

fdébut

ftant que

fsi

si (E = 4) alors

[calcul et application éventuelle de T]

Tant que ($t+t^* \neq 0$) et (E = 4) faire

début

i ← i-1, si (i = 0) alors i ← n fsi cc2 ← 0

Pour (k=1) jusqu 'à n faire

si (k≠i) alors début $m_k \leftarrow [0.5 + \sum_{j=1}^{n} e_{kj} e_{ij} / \sum_{j=1}^{n} e_{ij}^2]$, si $m_k \neq 0$ alors cc2 ← 1 fsi fdébu

fpour

si (cc2 =0) alors début t ← t-1, si (t =0) alors E ← 3 fsi fdébut

sinon

début

Pour j = 1 jusqu' à n faire $e_{ij}^* \leftarrow e_{ij}^* + \sum_{\substack{k=1 \\ k \neq i}}^{n} m_k e_{kj}^*$ fpour

Pour k = 1 jusqu' à n faire

si (k≠ i) alors pour (j = 1) jusqu' à n faire $e_{kj} \leftarrow e_{kj} - m_k e_{ij}$ fpour fsi

fpour

q ← 1, E ← 2

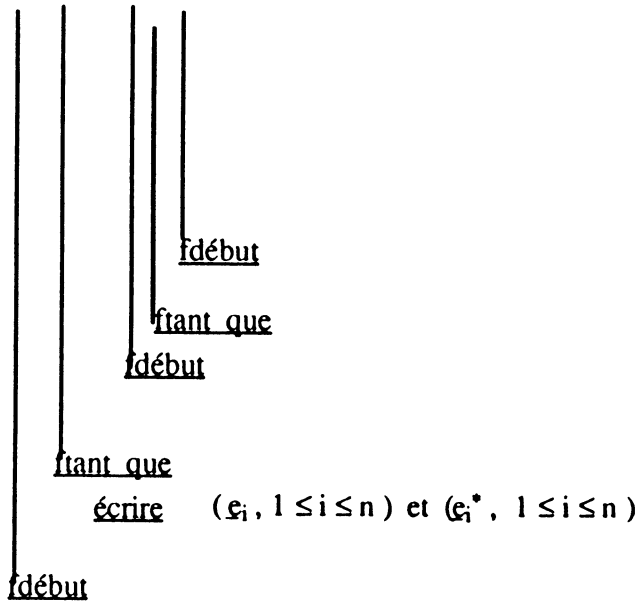
fdébut

fsi

fdébut

ftantque

fsi



b) Méthode et algorithme de réduction de A.K. Lenstra, H.W. Lenstra et L. Lovasz

b.1 Méthode de réduction

b.1.1 Préliminaire

Soient $(\underline{b}_i,\ 1 \le i \le n)$ une base d'un treillis G de $\mathbb{R}^n$ et $(\underline{b}_i^{\perp},\ 1 \le i \le n)$ la base orthogonale obtenue à partir de $\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_n$ par la méthode d'orthogonalisation de Gram-Schmidt, c'est - à - dire,

$$(5)\quad \begin{cases} \underline{b}_i^{\perp} = \underline{b}_i - \sum_{j=1}^{i-1} d_{ij}\underline{b}_j^{\perp}, & 1 \le i \le n \\ d_{ij} = \underline{b}_i.\underline{b}_j^{\perp}/\underline{b}_j^{\perp 2}, & 1 \le j < i \le n \end{cases}$$

où $\underline{a}.\underline{b}$ désigne le produit scalaire de deux vecteurs $\underline{a}$ et $\underline{b}$ et où par convention une somme vide est égale à 0.

II.1.11 DEFINITION

Une base $(\underline{b}_i,\ 1 \le i \le n)$ d'un treillis G est réduite suivant LLL si on a

$$(6)\quad |d_{ij}| \le 1/2, \qquad 1 \le j < i \le n$$

et

$$(7)\quad \left\|\underline{b}_i^{\perp} + d_{ii-1}\underline{b}_{i-1}^{\perp}\right\|^2 \ge 3\left\|\underline{b}_{i-1}^{\perp}\right\|^2/4, \quad 1 < i \le n.$$

b.1.2 description de la méthode

On commence par calculer les vecteurs $\underline{b}_i^{\perp}$, $(1 \le i \le n)$ et les nombres d_{ij} $(1 \le j < i)$ à partir de (5). La variable k sera réservée à un indice courant appartenant à l'ensemble $\{1, 2, \ldots, n-1\}$: initialement k vaut 2. A chacune des étapes de la méthode, l'un au moins des vecteurs $\underline{b}_1, \ldots, \underline{b}_n$ subira un changement de manière à ce que ces vecteurs restent une base de G. Après chaque modification de $\underline{b}_i$, on réactualise $\underline{b}_i^{\perp}$ et d_{ij} de telle sorte que (6) et (7) soient vérifiées.

On considère ensuite les relations

$$(8)\quad |d_{ij}| \le 1/2, \qquad 1 \le j < i < k$$

et

$$(9)\quad \left\|\underline{b}_i^{\perp} + d_{ii-1}\underline{b}_{i-1}^{\perp}\right\|^2 \ge 3\left\|\underline{b}_{i-1}^{\perp}\right\|^2/4, \quad 1 < i < k.$$

Partant alors de (8) et de (9) on répète l'exécution des deux étapes ci - après jusqu'à ce qu'on ait une base réduite.

Première étape.

On s'assure que l'inégalité $|d_{kk-1}| \leq 1/2$ est réalisée. Si ce n'est pas le cas on pose

$$r = [d_{kk-1} + 0.5]$$

et on affecte à $\underline{b}_k$ la valeur de $\underline{b}_k - r\underline{b}_{k-1}$. Les nombres d_{kj}, $1 \leq j < k$, et d_{kk-1} sont alors respectivement remplacés par $d_{kj} - rd_{k-1j}$ et $d_{kk-1} - r$; tous les $\underline{b}_i^{\perp}$ et les autres d_{ij} sont inchangés.

Deuxième étape

* Si on a la condition

$$(k>1) \quad \text{et} \quad \|\underline{b}_k^{\perp} + d_{kk-1}\underline{b}_{k-1}^{\perp}\|^2 < 3\|\underline{b}_{k-1}^{\perp}\|^2/4$$

alors

i) on échange les valeurs de $\underline{b}_k$ et de $\underline{b}_{k-1}$. Si les vecteurs et les nombres $\underline{c}_i$, $\underline{c}_i^{\perp}$ et v_{ij} désignent les remplaçants respectifs de $\underline{b}_i$, $\underline{b}_i^{\perp}$ et d_{ij}, alors on a :

$$\underline{c}_{k-1} = \underline{b}_k, \quad \underline{c}_k = \underline{b}_{k-1}, \quad \underline{c}_j = \underline{b}_j, \quad j = 1, \ldots, n \quad \text{et} \quad j \neq k, k-1.$$

$$\underline{c}_{k-1}^{\perp} = \underline{b}_k^{\perp} + d_{kk-1}\,\underline{b}_{k-1}^{\perp}, \quad \underline{c}_k^{\perp} = \underline{b}_{k-1}^{\perp} - v_{kk-1}\,\underline{c}_{k-1}^{\perp}, \quad \underline{c}_j^{\perp} = \underline{b}_j^{\perp}, \quad j = 1, \ldots, n \text{ et } j \neq k, k-1$$

avec

$$v_{kk-1} = d_{kk-1}\|\underline{b}_{k-1}^{\perp}\|^2/\|\underline{c}_{k-1}^{\perp}\|^2.$$

$$v_{ij} = d_{ij}, \quad 1 \le j < i \le n \quad \text{et} \quad \{i, j\} \cap \{k-1, k\} = \emptyset$$

et pour $i > k$ on a

$$v_{ik-1} = d_{ik-1}\, v_{kk-1} + d_{ik} \|\underline{b}_k^{\perp}\|^2 / \|\underline{c}_{k-1}^{\perp}\|^2, \qquad v_{ik} = d_{ik-1} - d_{ik} d_{kk-1}.$$

ii) On remplace k par k-1.

* En revanche si on a la condition

$$(k = 1) \quad \text{ou} \quad \|\underline{b}_k^{\perp} + d_{kk-1}\, \underline{b}_{k-1}^{\perp}\|^2 \ge 3 \|\underline{b}_{k-1}^{\perp}\|^2 / 4$$

alors

i) On s'assure qu'on a l'inégalité

$$(0) \quad |d_{kj}| \le 1/2, \qquad 1 \le j \le k-1.$$

Si ce n'est pas le cas (d'après la première étape l'inégalité (0) est vérifiée pour $j = k-1$) on répète l'opération ci-dessous jusqu'à ce qu'on ait cette inégalité pour tous les j, avec $1 \le j \le k-1$:

soient ℓ le plus grand indice inférieur à k tel que $|d_{k\ell}| > 1/2$ et r l'entier le plus proche de $d_{k\ell}$. On remplace $\underline{b}_k$ par $\underline{b}_k - r\underline{b}_\ell$. Les nombres d_{kj} $(j < \ell)$ et $d_{k\ell}$ sont alors remplacés respectivement par $d_{kj} - r\, d_{\ell j}$ et $d_{k\ell} - r$, tandis que les autres d_{ij} et tous les $\underline{b}_i$ sont inchangés.

ii) On remplace k par k+1.

ALGORITHME RBSLLL

Données $\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_n$ une base d'un treillis G avec $\|\underline{b}_1\| \leq \|\underline{b}_2\| \leq \ldots \leq \|\underline{b}_n\|$.
Résultat : réduite de cette base suivant la méthode de LLL.

début

[calcul de $\underline{b}_i^{\perp}$ et d_{ij}, $1 \leq i \leq n$, $1 \leq j < i$]

$\underline{b}_1^{\perp} \leftarrow \underline{b}_1$, $B_1 \leftarrow \underline{b}_1^{\perp}.\underline{b}_1^{\perp}$

pour i = 2 jusqu'à n faire
début
$\underline{b}_i^{\perp} \leftarrow \underline{b}_i$
pour (j = 1) jusqu'à (i-1) faire début $d_{ij} \leftarrow \underline{b}_i.\underline{b}_j^{\perp}/B_j$, $\underline{b}_i^{\perp} \leftarrow \underline{b}_i^{\perp} - d_{ij}\underline{b}_j^{\perp}$ fdébut fpour
$B_i \leftarrow \underline{b}_i^{\perp}.\underline{b}_i^{\perp}$
fdébut
fpour

$k \leftarrow 2$, $s \leftarrow 1$

[itération des deux étapes de la méthode]

Tant que (k < n) ou ((k = n) et (s = 1)) faire
début
$l \leftarrow k-1$
si ($|d_{kl}| > 1/2$) alors faire
début
$r \leftarrow [d_{kl} + 0.5]$, $\underline{b}_k \leftarrow \underline{b}_k - r\underline{b}_l$, $d_{kl} \leftarrow d_{kl} - r$
pour (j = 1) jusqu'à (l-1) faire $d_{kj} \leftarrow d_{kj} - r\, d_{lj}$ fpour
fdébut
fsi

si ($B_k < (3/4 - d_{kk-1}^2)B_{k-1}$) alors
début
$d \leftarrow d_{kk-1}$, $B \leftarrow B_k + d^2 B_{k-1}$, $d_{kk-1} \leftarrow dB_{k-1}/B$, $B_k \leftarrow B_{k-1}B_k/B$, $B_{k-1} \leftarrow B$

$\begin{pmatrix} b_{k-1} \\ b_k \end{pmatrix} \leftarrow \begin{pmatrix} b_k \\ b_{k-1} \end{pmatrix}$, pour (j = 1) jusqu'à (k-2) faire $\begin{pmatrix} d_{k-1j} \\ d_{kj} \end{pmatrix} \leftarrow \begin{pmatrix} d_{kj} \\ d_{k-1j} \end{pmatrix}$ fpour

pour (i= k+1) jusqu'à n faire $\begin{pmatrix} d_{ik-1} \\ d_{ik} \end{pmatrix} \leftarrow \begin{pmatrix} 1 & d_{kk-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -d \end{pmatrix} \begin{pmatrix} d_{ik-1} \\ d_{ik} \end{pmatrix}$ fpour

si (k> 2) alors k ← k-1 fsi
fdébut
sinon
début
l ← k-2
tant que (l >0) faire
début
si ($|d_{kl}|$ >1/2) alors
début
r ← [d_{kl} + 0.5], $\underline{b}_k$ - r$\underline{b}_l$

```
                    pour (j =1) jusqu'à (l-1) faire d_kj ← d_kj - r*d_lj fpour
                        d_kl ← d_kl - r
                fdébut
            fsi
            l ← l-1
        fdébut
    ftant que
        si (k<n) alors début k ← k+1, s ← 1 fdébut sinon s ← 0 fsi
    fdébut
  fsi
 fdébut
ftant que
  écrire (b_i, 1 ≤ i ≤ n )

fdébut

falgorithme
```

c) Méthode et algorithme de réduction d'une forme quadratique suivant D.E. Knuth

c.1 Préliminaire

La méthode de réduction que nous allons présenter a été à l'origine développée pour étudier la distribution d'une suite $(x) = \{x_i\}$ provenant d'un générateur congruentiel T noté (a, b, m). On choisit les entiers a, b et m de telle sorte que la suite $(x) = \{x_i\}$ définie par

$$\begin{cases} x_{i+1} = T(x_i), & i \in \mathbb{N} \\ x_o \text{ fixé}, \ 0 \leq x_o < m \end{cases}$$

soit de période maximale m. On considère alors, pour un entier n strictement supérieur à 1, le sous-ensemble V_n' de $[0, 1[^n$ donné par

$$V_n' = \left\{(x, T(x), \ldots, T^{n-1}(x)) / m \ : \ 0 \leq x < m\right\}$$

et l'extension G_n' de V_n' définie par

$$G_n' = \left\{\left(\frac{x}{m} + k_1, \frac{T(x)}{m} + k_2, \ldots, \frac{T^{n-1}(x)}{m} + k_n\right) \ : \ (x, k_1, \ldots, k_n) \in \mathbb{Z}^{n+1}\right\}.$$

D'après la remarque II.1.8, G_n' est une grille de vecteur de translation $\underline{b}_o$ et de base $(\underline{b}_i, \ 1 \leq i \leq n)$, où

$$\underline{b}_o = \frac{b}{m}(0, 1, 1 + a, \ldots, 1 + a + \ldots + a^{n-1}), \qquad \underline{b}_1 = \frac{1}{m}(1, a, \ldots, a^{n-1})$$

$$\underline{b}_2 = (0, 1, 0, \ldots, 0), \ldots, \qquad \underline{b}_n = (0, 0, \ldots, 1).$$

Soit

$$G_n' = \{\underline{b}_o + z_1 \underline{b}_1 + \ldots + z_n \underline{b}_n : (z_1, \ldots, z_n) \in \mathbb{Z}^n\}.$$

Partant de ces notations et définitions, on introduit la quantité $1/d_n$ qui est le maximum des distances entre les hyperplans adjacents dans les familles d'hyperplans parallèles et équidistants contenant G_n'.

II.1.12 THEOREME (D. E. Knuth(1981))

L'entier d_n étant défini comme ci- dessus on a :

$$d_n^2 = \min\{u_1^2 + u_2^2 + \ldots + u_n^2 : (u_1, \ldots, u_n) \in \mathbb{Z}^{n*} \text{ et } u_1 + a\,u_2 + \ldots + a^{n-1} u_n \equiv 0 \bmod m\}$$

$$= \min\{(x_1 m - a\,x_2 - \ldots - a^{n-1} x_n)^2 + x_2^2 + \ldots + x_n^2 : (x_1, \ldots, x_n) \in \mathbb{Z}^{n*}\}.$$

DEMONSTRATION

Posons

$$G_n' = G_o + \underline{b}_o$$

où G_o est le treillis dont une base est $(\underline{b}_i,\ 1 \le i \le n)$.

On remarque que le terme b intervient uniquement dans l'expression du vecteur $\underline{b}_o$ et que G_n' est le translaté de G_o par le vecteur $\underline{b}_o$. Mais si on considère la distance entre deux points quelconques de G_o, celle- ci reste inchangée après l'opération de translation. Donc b n'affecte pas le calcul de $1/d_n$ et par conséquent on peut, sans perte de généralité, supposer que $\underline{b}_o$ est nul. Cette hypothèse étant faite, on est ramené au

calcul du maximum des distances entre les hyperplans adjacents dans les familles d'hyperplans parallèles et équidistants contenant le treillis G_0.

Considérons d'abord l'une quelconque de ces familles et évaluons la distance entre deux hyperplans adjacents. Cette famille est définie par un vecteur non nul $\underline{u} = (u_1, u_2, \ldots, u_n)$ perpendiculaire à tous les hyperplans qu' elle contient. D'autre part un hyperplan H est caractérisé par un entier q tel que

$$H = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_1 u_1 + \ldots + x_n u_n = q\}.$$

On choisit $\underline{u}$ de telle sorte que l'ensemble de tous les entiers q nous donne tous les hyperplans de la famille. Comme l'un de ceux-ci contient le vecteur nul la distance d entre deux hyperplans adjacents est la distance minimum entre le vecteur nul et l'hyperplan caractérisé par $q = 1$. Soit

$$d = \min \{(x_1^2 + \ldots + x_n^2)^{1/2} : (x_1, \ldots, x_n) \in \mathbb{R}^n \text{ et } x_1 u_1 + \ldots + x_n u_n = 1\}.$$

D'après l'inégalité de Cauchy on a

$$1 = (x_1 u_1 + \ldots + x_n u_n)^2 \leq (x_1^2 + x_2^2 + \ldots + x_n^2)(u_1^2 + u_2^2 + \ldots + u_n^2)$$

et le minimum est atteint au point $(x_1, x_2, \ldots, x_n)$ avec

$$x_j = u_j / (u_1^2 + u_2^2 + \ldots + u_n^2), \quad 1 \leq j \leq n.$$

La distance entre deux hyperplans adjacents est donc $1/\|\underline{u}\|$, où $\|\underline{u}\|$ désigne la norme euclidienne du vecteur $\underline{u}$.

Il vient alors que la valeur d_n cherchée est la longueur du vecteur $\underline{u}$ non nul et de norme euclidienne minimum dans l'ensemble des vecteurs définissant les familles

d'hyperplans contenant G_0. Un tel vecteur $\underline{u} = (u_1, u_2, \ldots, u_n)$ doit vérifier $\underline{v}.\underline{u} \equiv 0 \bmod 1$, pour tout élément $\underline{v}$ de G_0. Comme les vecteurs $(1, 0, \ldots, 0)$, $(0, 1, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, 1)$ et $\underline{b}_1$ sont dans G_0 les u_j, $1 \leq j \leq n$, sont des entiers vérifiant

$$u_1 + a\,u_2 + \ldots + a^{n-1}\,u_n \equiv 0 \bmod m.$$

Réciproquent tout vecteur $\underline{u} = (u_1, u_2, \ldots, u_n)$ de $\mathbb{Z}^{n*}$ vérifiant la congruence précédente définit une famille d'hyperplans parallèles contenant G_0, puisque $(z_1 \underline{b}_1 + \ldots + z_n \underline{b}_n) . \underline{u}$ est un entier pour tout n-uplet $(z_1, \ldots, z_n)$ de $\mathbb{Z}^n$. On vient donc de montrer que

$$d_n^2 = \min \left\{ u_1^2 + u_2^2 + \ldots + u_n^2 : (u_1, \ldots, u_n) \in \mathbb{Z}^{n*} \quad \text{et} \quad u_1 + au_2 + \ldots + a^{n-1}u_n \equiv 0 \bmod m \right\}$$

Soit

$$d_n^2 = \min \left\{ (x_1\, m - a\, x_2 - \ldots - a^{n-1}\, x_n)^2 + x_2^2 + \ldots + x_n^2 : (x_1, \ldots, x_n) \in \mathbb{Z}^{n*} \right\}.$$

C.Q.F.D.

c.2 Méthode de réduction d'une forme quadratique

c.2.1 Préparation de la méthode

Soient $(\underline{v}_i,\ 1 \leq i \leq n)$ une base d'un treillis G de dimension n strictement supérieur à 1, V la matrice dont les vecteurs lignes sont respectivement $\underline{v}_1$, $\underline{v}_2$, $\ldots$, $\underline{v}_n$ et enfin U la matrice dont les vecteurs lignes sont ceux de la base duale $(\underline{u}_i,\ 1 \leq i \leq n)$. On considère alors la forme quadratique définie positive F donnée par

$$F(z_1, z_2, \ldots, z_n) = (z_1 \underline{u}_1 + \ldots + z_n \underline{u}_n)^2, \qquad \forall\ (z_1, \ldots, z_n) \in \mathbb{Z}^n.$$

On s'intéresse ici au problème de minimisation de F sur $\mathbb{Z}^{n^*}$, ce qui revient à chercher un n - uplet non nul de $\mathbb{Z}^{n^*}$ réalisant le minimum de F.

II.1.13 REMARQUES

1. Si $\underline{v}_1 = \frac{1}{m}(1, a, \ldots, a^{n-1})$, $\underline{v}_2 = (0, 1, \ldots, 0), \ldots,$ $\underline{v}_n = (0, 0, \ldots, 1)$

alors

$$\underline{u}_1 = (m, 0, \ldots, 0), \quad \underline{u}_2 = (-a, 1, 0, \ldots, 0), \ldots, \quad \underline{u}_n = (-a^{n-1}, 0, \ldots, 1)$$

et le minimum de F est d_n^2.

2. Dans le cas général où $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n$ est une base d'un treillis quelconque G_o, on montre (cf. D.E. Knuth (1981)) que le maximum des distances entre les hyperplans adjacents dans les familles d'hyperplans parallèles et équidistants contenant G_o est $1/d_n$, où d_n^2 est la valeur minimum de F sur $\mathbb{Z}^{n^*}$, ce qui revient à dire que d_n est la longueur du vecteur de norme minimum dans le treillis engendré par la base duale $(\underline{u}_i,\ 1 \leq i \leq n)$.

Pour résoudre le problème de minimisation de F, on commence par réduire le domaine de minimisation infini $\mathbb{Z}^{n^*}$ en un domaine fini D.

II.1.14 LEMME(cf. D. E. Knuth(1981))

Si un élément $(x_1, x_2, \ldots, x_n)$ de $\mathbb{Z}^{n^*}$ réalise le minimum de F alors pour tout n-uplet $\underline{y} = (y_1, y_2, \ldots, y_n)$ de $\mathbb{Z}^{n^*}$ on a

(12) $\qquad x_k^2 \leq F(y_1, \ldots, y_n)\,(\underline{v}_k.\underline{v}_k), \qquad 1 \leq k \leq n\,.$

DEMONSTRATION

D'après l'inégalité de Cauchy on a

$$x_k^2 = ((x_1\,\underline{u}_1 + \ldots + x_n\,\underline{u}_n).\underline{v}_k)^2 \leq (\underline{v}_k.\underline{v}_k)\,F(x_1, \ldots, x_n) \qquad 1 \leq k \leq n.$$

Donc

$$x_k^2 \leq (\underline{v}_k.\underline{v}_k)\,F(y_1, \ldots, y_n), \quad \forall\,(y_1, \ldots, y_n) \in \mathbb{Z}^{n*}, \quad \forall\,k = 1, 2, \ldots, n.$$

C.Q.F.D.

Si le domaine D défini par le lemme précédent est suffisamment restreint on peut y faire une recherche exhaustive d'un n-uplet non nul réalisant le minimum de F sur $\mathbb{Z}^{n*}$. Si ce n'est pas le cas on cherche une forme quadratique F' équivalente à F de manière à réduire D.

Ainsi pour un indice j fixé, $1 \leq j \leq n$, on considère la transformation unimodulaire T_j définie par

$$T_j(\underline{v}_i) = \underline{v}_i' = \underline{v}_i - q_i\,\underline{v}_j, \qquad T_j(\underline{u}_i) = \underline{u}_i' = \underline{u}_i, \qquad i \neq j,\ i = 1, 2, \ldots, n$$

$$T_j(\underline{v}_j) = \underline{v}_j' = \underline{v}_j, \quad T_j(\underline{u}_j) = \underline{u}_j + \sum_{\substack{i=1 \\ i \neq j}}^{n} q_i\,\underline{u}_i$$

et si $\underline{x} \in \mathbb{Z}^{n*}$ et $\underline{x} = (x_1, \ldots, x_n)$ alors

$$T_j(\underline{x}) = \underline{x}' = (x_1', \ldots, x_n') \quad \text{avec} \quad x_i' = x_i - q_i x_j \qquad \text{pour } i \neq j \text{ et } x_j' = x_j.$$

La forme équivalente F' définie par $\underline{u}_1', \ldots, \underline{u}_n'$ vérifie

$$F'(T_j(x_1, \ldots, x_n)) = F(x_1, \ldots, x_n).$$

De plus on a $\underline{u}_i' \cdot \underline{u}_j' = \delta_{ij}$, $1 \leq i, j \leq n$. Enfin si les vecteurs $(x_1, x_2, \ldots, x_n)$ parcourent $\mathbb{Z}^{n*}$ il en est de même pour leurs transformées $(x_1', \ldots, x_n')$. Donc F et F' ont la même valeur minimum. On choisit les entiers q_i, $1 \leq i \leq n$ et $i \neq j$, de telle sorte que les transformées $\underline{v}_i'$ de $\underline{v}_i$ soient de norme minimum. Pour un tel critère de choix on trouve

$$q_i = \left[\frac{\underline{v}_i \cdot \underline{v}_j}{\underline{v}_j \cdot \underline{v}_j} + 0.5\right], \quad i = 1, 2, \ldots, n, \quad i \neq j.$$

c.2.2 Description de la méthode

On démarre avec la matrice V dont les vecteurs lignes sont les vecteurs $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_n$ d'une base du treillis G considéré. On calcule ensuite la base duale $(\underline{u}_i, 1 \leq i \leq n)$. On cherche alors à minimiser le second membre de (12) afin qu'on puisse calculer d_n par recherche exhaustive d'un vecteur de norme minimum sur un sous-ensemble strict du treillis dual de G. Pour ce faire, on fait intervenir la forme équivalente F'. Initialement on prend pour majorant s de d_n^2, c'est-à-dire, pour valeur de $F(y_1, \ldots, y_n)$ le minimum de $||\underline{u}_1||^2, \ldots, ||\underline{u}_n||^2$, où $||\underline{x}||$ désigne la norme euclidienne de $\underline{x}$. La variable j, $1 \leq j \leq n$, est l'indice intervenant dans la transformation unimodulaire T_j et k la variable contenant les indices j pour lesquels T_j est un succès : on dira que T_j est un succès si l'une au moins des transformées $\underline{v}_i'$ de $\underline{v}_i$ (i = 1, 2, ... , n) est de norme euclidienne strictement inférieure à celle de $\underline{v}_i$.

Partant de $j = 1$ et de $k = n$, on itère les opérations ci-après jusqu' à ce qu'on ait $j = k$.

i) On calcule T_j

ii) Si T_j est un succès alors $k \leftarrow j$.

iii)

1. Si $j < n$ alors $j \leftarrow j + 1$, sinon $j \leftarrow 1$.
2. $s \leftarrow \min(s, \underline{u}_j \cdot \underline{u}_j)$, $\underline{u}_j \leftarrow \underline{u}_j$.
3. $\underline{v}_i \leftarrow \underline{v}_i$, $1 \leq i \leq n$ et $i \neq j$.

Pour faciliter la compréhension de l'algorithme qu'on va présenter il est nécessaire de préciser les données, les résultats et certaines notations.

Données 3 entiers a, m et n avec

1. $n > 1$.
2. $0 < a < m$, $(a, m) = 1$.
3. Si un nombre premier divise m, alors il divise $a - 1$.
4. Si 4 divise m alors 4 divise $a - 1$.

Résultats On sort un majorant de F et la forme quadratique réduite F' de F où les lignes de la matrice U associée à F sont $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_n$ avec

$\underline{u}_1 = (m, 0, \ldots, 0)$, $\underline{u}_2 = (-a, 1, 0, \ldots, 0)$, $\underline{u}_3 = (-a^2, 0, 1, 0, \ldots, 0)$, $\ldots$, $\underline{u}_n = (-a^{n-1}, 0, \ldots, 1)$.

Notations

1. On utilisera la matrice V dont les lignes $\underline{v}_1, \ldots, \underline{v}_n$ vérifient $\underline{u}_i \cdot \underline{v}_j = \delta_{ij} m$, où δ_{ij} est le symbole de Kronecker.
2. r est la variable contenant $a^{t-1} \bmod m$ $(t = 2, 3, \ldots, n)$.
3. s est la variable contenant les majorants de F.

4 . $U^{(1)}$ et $V^{(1)}$ sont respectivement des sous-matrices carrées réduites ou non de U et de V telles que $\underline{U}_i^{(1)}.\underline{V}_j^{(1)} = \delta_{ij}\, m$, où $\underline{U}_i^{(1)}$ et $\underline{V}_j^{(1)}$ désignent respectivement les ième et jème lignes de $U^{(1)}$ et de $V^{(1)}$.

II.1.15 REMARQUES

- La réduction de F dans le cas $n = 2$ se fait à l'aide d'une méthode particulière qu'on peut assimiler à l'algorithme d'Euclide (cf. D.E. Knuth (1981)).

- La partie initialisation de l'algorithme correspond à :

$h \leftarrow a,\ h' \leftarrow m,\ p \leftarrow 1,\ p' \leftarrow 0,\ r \leftarrow a,\ s \leftarrow 1+a^2$.

ALGORITHME

début

(initialisation)

(Application de l'algorithme d' Euclide à la réduction de $\begin{pmatrix} 1 & a \\ 0 & m \end{pmatrix}$)

W← s-1

Tant que (W<s) faire

début

q← [h'/h], u← h' - qh, v← p' -qp, w← u^2+v^2

si (w <s) alors début s← $u^2+ v^2$, h'← h, h← u, p'← p, p←v, w← w-1 fdébut fsi.

fdébut

ftque

u← u-h, v← v-p

si ($u^2+ v^2$<s) alors début s←$u^2+ v^2$, h'← u, p'← v fdébut fsi

si p'> 0, alors E← -1 sinon E← 1 fsi

$$U^{(1)} \leftarrow \begin{pmatrix} -h & p \\ -h' & p' \end{pmatrix}, \quad V^{(1)} \leftarrow E^* \begin{pmatrix} p' & h' \\ -p & -h \end{pmatrix}$$

(réduction de $U^{(1)}$ de dimension successivement égale à 3,4,..., n)

tant que (t< n) faire

début

(on va incrémenter t d'une unité. Mais comme $U^{(1)}$ et $V^{(1)}$ sont des matrices t x t , on aura à les agrandir en ajoutant à chacune d'elles une ligne et une colonne convenables)

t← t+1, r← ar mod m, $\underline{U}_t^{(1)}$← (-r,0,..., 0,1). ($\underline{U}_t^{(1)}$ a t colonnes)

pour (i =1) jusqu'à (t-1) faire $U_{it}^{(1)}$← 0 fpour

$\underline{V}_t^{(1)}$← (0, ..., 0, m). ($\underline{V}_t^{(1)}$ a t colonnes)

pour (i=1) jusqu'à (t-1) faire

début $q \leftarrow \left[\frac{rV_{il}^{(1)}}{m} + 0.5\right]$, $V_{it}^{(1)} \leftarrow V_{il}^{(1)} - qm$, $\underline{U}_t^{(1)} \leftarrow \underline{U}_t^{(1)} + q\underline{U}_i^{(1)}$ fdébut

fpour

(Dans la boucle précédente on a affecté à $V_{it}^{(1)}$, la valeur $rV_{il}^{(1)}$,

puis on a appliqué la tranformation T_t)

s← min (s, $\underline{U}_t^{(1)}.\underline{U}_t^{(1)}$), k← t, j←1, i←1.

(l'étape suivante conceme la réduction de $U^{(1)}$ et de $V^{(1)}$)

```
        tant que (j≠k) faire
          début
            tant que (i≤t) faire
              si (i ≠ j) et (2|V_i^(1).V_j^(1)|>V_j^(1).V_j^(1)) alors faire
                début
                  q←[V_i^(1).V_j^(1) / V_j^(1).V_j^(1) +0.5], V_i^(1)←V_i^(1) - qV_j^(1), U_j^(1)←U_j^(1) +qU_i^(1), k←j, i← i+1.
                fdébut
              fsi
            ftque
            si (k=j) alors s← min (s, U_j^(1).U_j^(1)) fsi
              si (j=t) alors j← 1 sinon j← j+1 fsi i← 1.
          fdébut
        ftque
      fdébut
    ftque
      écrire (U_j^(1), 1 ≤ j ≤ n), écrire (s).
  fdébut
falgorithme
```

B.3 Algorithmes de réduction et calcul d'un vecteur de norme minimum dans un treillis

On va utiliser les algorithmes précédents pour calculer de deux façons différentes un vecteur non nul $\underline{x}$ de norme euclidienne minimum dans un treillis G.

Soient $(\underline{e}_i,\ 1 \le i \le n)$ une base réduite d'un treillis G, $(\underline{e}_i^*,\ 1 \le i \le n)$ la base duale et $\underline{x}$ l'un des vecteurs qu'on cherche à calculer. On pose

$$\underline{x} = z_1\underline{e}_1 + \cdots + z_n\underline{e}_n$$

où $z_1, z_2, \ldots, z_n$ sont des entiers convenables.

a) Première méthode de calcul d'un vecteur de norme minimum

Si la base est réduite au sens de U. Dieter ou de LLL, alors les coordonnées de $\underline{x}$ vérifient

$$|z_i| = |(z_1 \underline{e}_1 + \ldots + z_n \underline{e}_n).\underline{e}_i^*| \leq [\,||\underline{e}_i^*||\, D] = c_i$$

où

$$D = \min\ \{||\underline{e}_j||,\ 1 \leq j \leq n\}.$$

Dans le cas de réduction au sens de D.E. Knuth, précisons à nouveau les données et les résultats :

1. On se donne une base $\underline{v}_1, \ldots, \underline{v}_n$ d'un treillis G et on cherche à réduire la forme quadratique F définie sur $\mathbb{Z}^{n^*}$ par

$$F(y_1, \ldots, y_n) = (y_1 \underline{u}_1 + \ldots + y_n \underline{u}_n).(y_1 \underline{u}_1 + \ldots + y_n \underline{u}_n), \qquad \forall\ (y_1, \ldots, y_n) \in \mathbb{Z}^{n^*}$$

où $(\underline{u}_i,\ 1 \leq i \leq n)$ est la base duale de $(\underline{v}_i, 1 \leq i \leq n)$.

2. L'algorithme de réduction nous donne un majorant s de F, une base réduite $(\underline{v}_i', 1 \leq i \leq n)$ de $(\underline{v}_i, 1 \leq i \leq n)$ et une forme quadratique réduite F' définie sur $\mathbb{Z}^{n*}$ par

$$F'(y_1', \ldots, y_n') = (y_n' \underline{u}_n' + \ldots + y_n' \underline{u}_1').(y_1' \underline{u}_1' + \ldots + y_n' \underline{u}_n'), \qquad \forall (y_1', \ldots, y_n') \in \mathbb{Z}^{n*}$$

où $(\underline{u}_i', 1 \leq i \leq n)$ est la base duale de $(\underline{v}_i', 1 \leq i \leq n)$.

3. Un vecteur $\underline{x}^* = (z_1^*, \ldots, z_n^*)$ minimisant F sur $\mathbb{Z}^{n*}$ vérifie alors

$$|z_i| \leq [\sqrt{[(\underline{v}_i'. \underline{v}_i') s]}\,] = n_i, \qquad 1 \leq i \leq n.$$

Il vient alors que quelque soit la méthode de réduction utilisée pour la recherche d'un vecteur de norme minimum dans un treillis, les composantes $(t_1, \ldots, t_n)$ de ce vecteur s'obtiennent par recherche exhaustive sur l'ensemble des n-uplets d'entiers $(z_1, \ldots, z_n)$ non nuls tels que

$$|z_i| \leq \ell_i, \quad 1 \leq i \leq n$$

où ℓ_i, $1 \leq i \leq n$, est un entier convenable.

II.1.16 REMARQUE

La méthode qu'on vient de présenter permet de calculer dans les deux premiers cas un vecteur non nul de norme minimum dans un treillis G et dans le cas où on utilise la méthode de réduction de D.E. Knuth, on trouve les coordonnées dans la base $(\underline{u}_i', 1 \leq i \leq n)$, d'un vecteur non nul de norme minimum dans le treillis dual G*. Par conséquent si l'on veut utiliser l'algorithme de réduction de D.E. Knuth pour calculer

un vecteur de norme minimum dans G dont une base est $(\underline{v}_i,\ 1 \le i \le n)$, alors on cherchera à minimiser la forme quadratique

$$F(y_1, \ldots, y_n) = (y_1 \underline{v}_1 + \ldots + y_n \underline{v}_n).(y_1 \underline{v}_1 + \ldots + y_n \underline{v}_n), \qquad \forall\ (y_1, \ldots, y_n) \in \mathbb{Z}^{n^*}$$

au lieu de

$$F(y_1, \ldots, y_n) = (y_1 \underline{u}_1 + \ldots + y_n \underline{u}_n).(y_1 \underline{u}_1 + \ldots + y_n \underline{u}_n), \qquad \forall\ (y_1, \ldots, y_n) \in \mathbb{Z}^{n^*}$$

où $(\underline{u}_i,\ 1 \le i \le n)$ est la base duale de $(\underline{v}_i,\ 1 \le i \le n)$.

Dans l'application au test spectral on n'aura pas besoin de la valeur même du vecteur de norme minimum d'un treillis G, mais de sa norme. Ainsi on décrit maintenant un algorithme qui, partant d'une base réduite $(\underline{e}_i,\ 1 \le i \le n)$ d'un treillis G, sort la longueur du vecteur de norme minimum après une recherche exhaustive sur l'ensemble des vecteurs $\underline{x}$ de G tels que

$$\underline{x} = z_1 \underline{e}_1 + z_2 \underline{e}_2 + \ldots + z_n \underline{e}_n, \qquad |z_i| \le c_i,\ \ 1 \le i \le n$$

et

$$\|\underline{x}\|^2 \le r$$

où $(c_i,\ 1 \le i \le n)$ et r sont des entiers convenables.

ALGORITHME

- Données : $\underline{e}_1, \underline{e}_2, ..., \underline{e}_n$ une base réduite de G, c_i, $1 \le i \le n$ et r.

- Résultat : on sort un réel $t>0 : t = \min\{||\underline{v}|| : \underline{v} \in G, \underline{v} \neq 0, \underline{v} = v_1\underline{e}_1 + ... + v_n\underline{e}_n, |v_i| \le c_i, ||\underline{v}||^2 \le r\}$

- Variables utilisées : Y contient les vecteurs de la forme $v_1\underline{e}_1 + ... + v_1\underline{e}_1$,

s est un majorant de Y.Y et X est la matrice ${}^t(v_1, ..., v_n)$.

```
début
  ( initialisation )   k← n,  X← Y← (0, ..., 0), s← r.
  Tant que (k >0) faire
     si (v_k = c_k) alors k← k-1
      sinon
          début
                v_k ← v_k + 1, Y← Y + e_k, k← k+1
           si (k < n+1) alors
            tant que (k < n+1) faire début v_k ← -c_k, Y← Y -2c_k e_k, k← k+1, fdébut ftant que
           fsi
                s← min (s,  Y.Y), k← k-1
          fdébut
     fsi
  ftant que
  écrire (√s).
fdébut
falgorithme
```

b) Deuxième méthode de recherche d'un vecteur de norme minimum dans un treillis

On considère d'abord les algorithmes de réduction de LLL et de U. Dieter et on rappelle qu'il s'agit de trouver un vecteur non nul $\underline{x}$ d'un treillis G tel que

$$||\underline{x}||^2 = \min \{||\underline{v}||^2, \underline{v} \in G, \underline{v} \neq \underline{0} \text{ et } ||\underline{v}||^2 \le v\}$$

où $v = \min \{\|\underline{e}_i\|^2,\ 1 \le i \le n\}$ et où $(\underline{e}_i,\ 1 \le i \le n)$ est une base réduite de G.

Pour $\underline{z}$ dans G on pose

$$\underline{z} = z_1\underline{e}_1 + \ldots + z_n\underline{e}_n.$$

D'autre part on note par B_i, la matrice colonne formée des composantes du vecteur $\underline{e}_i$, $1 \le i \le n$, dans la base canonique et par B la matrice dont les vecteurs colonnes sont $B_1, B_2, \ldots, B_n$. La matrice de Gramm A' de la base $(\underline{e}_i,\ 1 \le i \le n)$ est alors donnée par

$$A' = {}^tBB$$

et on a

$$\|z\|^2 = {}^t\underline{Z}A'\underline{Z}$$

où $\underline{Z} = {}^t(z_1, z_2, \ldots, z_n)$.

Le vecteur $\underline{x}$ cherché est donc un vecteur non nul de norme minimum dans l'ensemble des vecteurs $\underline{z}$ de G tels que

$$\underline{z} = z_1\underline{e}_1 + z_2\underline{e}_2 + \ldots + z_n\underline{e}_n$$

et

$${}^t\underline{Z}A'\underline{Z} \le v, \quad \underline{Z} = {}^t(z_1, z_2, \ldots, z_n).$$

On considère maintenant la réduction au sens de D.E. Knuth. Partant des notations du paragraphe a) on désigne par A'^* la matrice de Gramm associée à la base $(\underline{u}_i',\ 1 \le i \le n)$. Il s'agit de trouver $\underline{X}^* = (x_1^*, x_2^*, \ldots, x_n^*)$ de $\mathbb{Z}^{n^*}$ tel que

$$^t\underline{X}^*A^{'*}\underline{X}^* = \min\left\{^t\underline{Z}^*A^{'*}\underline{Z}^* \ : \ \underline{Z}^* \in \mathbb{Z}^{n^*}, \qquad ^t\underline{Z}^*A^{'*}\underline{Z}^* \leq s\right\}.$$

Des considérations ci-dessus, on voit que quelque soit la méthode de réduction utilisée pour calculer un vecteur de norme minimum dans un treillis, on est ramené à chercher l'ensemble des points $T = (t_1, t_2, \ldots, t_n)$ de $\mathbb{Z}^{n^*}$ tels que

$$^tTAT \leq c$$

où $c \in \mathbb{R}_+^*$ et où A est une matrice carrée d'ordre n définie positive.

Nous nous intéressons maintenant à l'algorithme de U. Fincke et M. Pohst pour résoudre l 'inéquation ci- dessus. Cet algorithme, basé sur la décomposition de Cholesky d'une matrice carrée A définie positive, transforme une forme quadratique elle aussi définie positive en une somme de carrés.

Plus precisément si $A = (a_{ij},\ 1 \leq i, j \leq n)$ et

$$^tTAT = \sum_{i=1}^{n} a_{ij}\, t_i\, t_j$$

alors

$$Q(T) = {}^tTAT = \sum_{i=1}^{n} q_{ii}\,(t_i + \sum_{j=i+1}^{n} q_{ij}\, t_j)^2$$

où les quantités q_{ij} sont donnés par l'algorithme suivant :

```
ALGORITHME
   Données   A = ( a_ij , 1 ≤ i , j ≤ n).
   Résultat : Q = ( q_ij).
   début
    pour (j=1) jusqu ' à n faire pour (i=1) jusqu ' à j faire q_ij ← a_ij fpour fpour
    pour (i=1) jusqu ' à n-1 faire
      début
        pour (j = i+1) jusqu'à n faire début q_ji ← q_ij, q_ij ← q_ij/q_ii fdébut fpour
        pour (k = i+1) jusqu'à n faire
            pour (l = k) jusqu'à n faire q_kl ← q_kl - q_ki*q_il fpour
        fpour
      fdébut
    fpour
    écrire (Q = (q_ij)).
   fdébut
falgorithme
```

II.1.17. REMARQUE

Si ${}^tRR$ est la décomposition de Cholesky de la matrice A, alors les coefficients (r_{ij}) de R sont donnés par

$$r_{ij} = 0, \quad 1 \le j < i \le n$$

$$r_{ii} = q_{ii}^{1/2}, \quad 1 \le i \le n$$

$$r_{ij} = r_{ii}\, q_{ij}, \quad 1 \le i < j \le n.$$

On calcule maintenant l'ensemble des points $T = (t_1, \ldots, t_n)$ de $\mathbb{Z}^{n\,*}$ tels que

$$\sum_{i=1}^{n} q_{ii}(t_i + \sum_{j=i+1}^{n} q_{ij}\, t_j)^2 \leq c.$$

On a :

i) $q_{nn}\, t_n^2 \leq c = T_n$.

Par conséquent

$$BI(t_n) \leq t_n \leq BS(t_n)$$

où

$$BI(t_n) = \lceil -(\frac{T_n}{q_{nn}})^{1/2} \rceil, \qquad BS(t_n) = \lfloor (\frac{T_n}{q_{nn}})^{1/2} \rfloor$$

avec

$$\lceil x \rceil = \min \{n \in \mathbb{Z}, n \geq x\} \quad \text{et} \quad \lfloor x \rfloor = \max \{n \in \mathbb{Z}, n \leq x\}.$$

ii) $q_{n-1\,n-1}(t_{n-1} + q_{n-1\,n}\, t_n)^2 + q_{nn}\, t_n^2 \leq c.$

Par conséquent

$$BI(t_{n-1}) \leq t_{n-1} \leq BS(t_{n-1})$$

où

$$BI(t_n) = \lceil -(\frac{T_{n-1}}{q_{n-1\,n-1}})^{1/2} - q_{n-1\,n}\, t_n \rceil \quad \text{et} \quad BS(t_n) = \lfloor (\frac{T_{n-1}}{q_{n-1\,n-1}})^{1/2} - q_{n-1\,n}\, t_n \rfloor$$

avec

$$T_{n-1} = T_n - q_{nn} t_n^2.$$

Plus généralement pour $t_n, t_{n-1}, \ldots, t_{k+1}$ fixés, on obtient les bornes de t_k, $t_{k-1}, \ldots, t_1$ en utilisant la relation

$$\sum_{i=1}^{k} q_{ii} \left(t_i + \sum_{j=i+1}^{n} q_{ij} t_j\right)^2 \leq T_k$$

avec

$$T_k = T_{k+1} - q_{k+1\,k+1} \left(t_{k+1} + \sum_{j=k+2}^{n} q_{k+1\,j}\, t_j\right)^2, \quad k = n-1, n-2, \ldots, 1$$

et

$$T_n = c.$$

On est maintenant en mesure de donner l'algorithme de U. Fincke et M. Pohst.

ALGORITHME

Données $(q_{ij},\ 1 \le i \le j \le n)$ et un réel $c > 0$.

Résultats

Tous les $\underline{x}$ à n composantes entières avec $Q(\underline{x}) \le c$. On sort aussi le $Q(\underline{x})$ non nul et minimal.

début

[Initialisation]

$i \leftarrow n,\ T_i \leftarrow c,\ U_i \leftarrow 0,\ Q \leftarrow c,\ Z \leftarrow (T_i/q_{ii})^{1/2},\ BS(x_i) \leftarrow \lfloor Z - U_i \rfloor,\ x_i \leftarrow \lceil -Z - U_i \rceil,\ r \leftarrow 1.$

Tant que $(r = 1)$ faire

si $(x_i > BS(x_i))$ alors début $i \leftarrow i+1,\ x_i \leftarrow x_i + 1$ fdébut fsi

si $(x_i \le BS(x_i))$ alors

si $(i=1)$ alors

début

$\underline{x} \leftarrow (x_n, x_{n-1}, \ldots, x_1)$, écrire $(\underline{x})$,

si $(\underline{x} = 0)$ alors $(r = 0)$

sinon

début $Q(\underline{x}) \leftarrow -T_1 + c + q_{11}(x_1 + U_1)^2$, si $Q(\underline{x}) < Q$ alors $Q \leftarrow Q(\underline{x})$ fsi $x_i \leftarrow x_i + 1$ fdébut

fsi

fdébut

sinon

début

$i \leftarrow i-1,\ U_i \leftarrow \sum_{j=i+1}^{n} q_{ij} x_j,\ T_i \leftarrow T_{i+1} - q_{i+1\,i+1}(x_{i+1} + U_{i+1})^2,\ Z \leftarrow \left(\frac{T_i}{q_{ii}}\right)^{1/2},$

$BS(x_i) \leftarrow \lfloor Z - U_i \rfloor,\ x_i \leftarrow \lceil -Z - U_i \rceil$

fdébut

fsi

fsi

ftanque

écrire (Q)

fdébut

falgorithme

C . Application de la réduction d'une base d'un treillis et du calcul d'un vecteur de norme minimum dans un réseau au test des treillis et au test spectral des vecteurs de nombres pseudo-aléatoires

Au paragraphe A, nous avons fait la description des grilles engendrées par des vecteurs provenant d'une congruence linéaire simple. Nous utilisons ici les treillis associés à ces grilles pour tester les qualités de distribution d'une suite de N.P.A. congruentielle.

Soit $(x) = \{x_i\}$ une suite (a, b, m, x_0) obtenue par l'un des générateurs (a, b, m) du théorème I.2.1. Pour $n > 1$, on considère les deux suites de vecteurs suivantes

$$(13) \qquad \underline{x}_i = (x_i, x_{i+1}, \ldots, x_{i+n-1}), \qquad i = 0, 1, \ldots$$

$$(14) \qquad \underline{x}_i' = (x_{in}, x_{in+1}, \ldots, x_{in+n-1}), \qquad i = 0, 1, \ldots$$

On se propose maintenant d'étudier la distribution des suites de vecteurs pseudo-aléatoires $\underline{u} = \{\underline{x}_i / m\}$ et $\underline{u}' = \{\underline{x}_i' / m\}$ dans l'espace $[0, 1[^n$. Les conclusions de cette étude étant les mêmes que celles qu'on a lorsqu'on considère la répartition de $(\underline{x}) = \{\underline{x}_i\}$ et de $(\underline{x}') = \{\underline{x}_i'\}$ dans $[0, m[^n$, on s'intéressera suivant les cas à $(\underline{x})$ et à $(\underline{x}')$ ou à $(\underline{u})$ et à $(\underline{u}')$.

Pour simplifier la tâche, on suppose de plus que les paramètres a, b, m et x_0 sont choisis de telle sorte que chacune des suites (13) et (14) engendre une seule grille G_n. Soient alors R_n le réseau déduit de G_n par annulation du vecteur de translation et $(\underline{e}_i,\ 1 \le i \le n)$ une base de ce réseau. L'application de l'un des algorithmes de réduction à cette base nous permet de calculer le quotient q_n de Beyer en dimension n : q_n est le quotient de la norme euclidienne du vecteur le plus long de la base réduite par celle

du vecteur le plus court . Si q_n est voisin de 1, alors on dit que la suite (a, b, m, x_o) ou le générateur (a, b, m) a un bon treillis en dimension n. Partant d'une base réduite du treillis dual R_n^* de R_n, on calcule d'abord la longueur d_n d'un vecteur non nul de norme minimum dans R_n^*, puis la quantité μ_n définie par

$$\mu_n = \frac{\pi^{n/2} d_n^n}{\left(\frac{n}{2}\right) ! \; m}$$

avec

$$\left(\frac{n}{2}\right) ! = \left(\frac{n}{2}\right)\left(\frac{n}{2} - 1\right) \ldots \left(\frac{1}{2}\right)\sqrt{\pi}, \quad \text{pour n impair.}$$

Si $\mu_n \geq 0.1$, alors on dit que les suites (x) et (x') passe le test spectral en dimension n et si $\mu_n \geq 0.1$ pour $2 \leq n \leq 6$, alors on dit tout simplement que ces suites passent le test spectral.

D. Résultats de la mise en oeuvre des algorithmes de réduction d'une base d'un treillis et du calcul d'un vecteur de norme minimum dans un réseau : application au test des treillis et au test spectral d'un générateur d'une table de "Nombres au Hasard"

Dans cette partie, nous nous sommes intéressés aux treillis engendrés par le générateur congruentiel $(3125, 1, 2^{35})$ utilisé pour la table de "Nombres au Hasard " du livre " Tables Statistiques et Financières " de J. Laborde (Dunod 1971) (cf. B. Van Cutsem (1980)).

D.1 Caractéristiques du Générateur (3125, 1, 2^{35})

Pour construire cette table on s'est servi de la suite (3125, 1, 2^{35}, 71). Avant de préciser les caractéristiques de cette suite (période et période effective), nous donnons quelques définitions et certains résultats généraux portant sur la longueur de cycle et la période effective d'une suite (a, b, m, x_0).

D.1.1 Quelques aspects généraux sur les caractéristiques d'une suite (a, b, m, x_0)

II.1.18 Définition

1) Soient a et m deux entiers strictement positifs tels que PGCD(a, m) = 1. On appelle *ordre multiplicatif de* a *modulo* m le plus petit entier δ strictement positif tel que $a^{\delta} \equiv 1 \bmod m$.

2) Soient a et m deux entiers strictement positifs. Alors le plus petit entier r strictement positif tel que $ar \equiv 0 \bmod m$ est dit *ordre additif de* a *modulo* m.

II. 1. 19. Définition

Soit (x) = { x_n }, une suite (a, b, m, x_0) avec PGCD(a,m) = 1.

1) L'ordre multiplicatif δ de a modulo m est appelé *période effective* de la suite (x) ou du générateur (a, b, m).

2) Si de plus b est égal à 1 et x_0 est nul , alors la suite (x) est dite *suite fondamentale* et le générateur (a, 1, m) est appelé *générateur fondamental.*

Le théorème suivant montre qu'on peut d'une part, ramener le calcul de la période d'une suite (a, b, m, x_0) à celui de la suite fondamentale (a, 1, m_1, 0) pour un entier m_1

convenablement choisi et d'autre part, retrouver la suite (a, b, m, x_0) par transformation affine de la suite fondamentale $(a, 1, m, 0)$.

II. 1. 20 Théorème (cf. B. van Cutsem(1980)).

Soit T le générateur (a, b, m) tel que $PGCD(a, m) = 1$. On choisit ensuite un entier x_0 quelconque appartenant à l'intervalle $[0, m[$ et on pose

$$d = PGCD(x_0(a-1) + b, m).$$

Enfin, si $(x) = \{x_n\}$ est la suite (a, b, m, x_0) et $(d) = \{d_n\}$ la suite $(a, 1, m, 0)$, alors la période de (a, b, m, x_0) est égale à celle de $(a, 1, m/d, 0)$ et on a

$$x_n \equiv d_n (x_0(a-1) + b) + x_0 \mod m.$$

Nous terminons ces considérations d'ordre général par l'énoncé d'un résultat établissant une relation entre la longueur de cycle et la période effective d'une suite fondamentale et faisant ressortir l'influence de la valeur de la période effective sur la structure de cycle de cette suite.

II. 1. 21 Théorème (cf G. Marsaglia (1972))

Soient a et m deux entiers tels que $PGCD(a, m) = 1$ et $1 < a < m$. On note par δ l'ordre multiplicatif de a modulo m. Alors la suite fondamentale $(d) = \{d_n\}$, égale à la suite $(a, 1, m, 0)$, est constituée du bloc $\{B\} = \{d_0, d_1, \ldots, d_{\delta-1}\}$ suivi des translatés de ce bloc. Soit

$$\{B\}, \{B + c\}, \{B + 2c\}, \ldots$$

où la constante c est donnée par

$$c \equiv 1 + a + a^2 + \ldots + a^{\delta-1} \mod m$$

et où, pour tout entier naturel non nul j, $\{B + jc\}$ est défini par

$$\{B + jc\} = \{b + jc \mod m : b \in \{B\}\}.$$

La période de (a, 1, m, 0) est δr, où r est l'ordre additif de c modulo m, c'est - à - dire, r = m / PGCD(c,m).

II. 1. 22 REMARQUES

1) Dans le théorème ci - dessus, les δ éléments du bloc {B} sont deux à deux distincts.

2) Nous avons déjà souligné au paragraphe I.1 qu'un bon générateur congruentiel doit avoir une longueur de cycle suffisamment grande et au vu des théorèmes II. 1. 20 et II. 1. 21, il est souhaitable qu' il ait également une période effective assez élévée de telle sorte que la suite engendrée n'ait pas une structure trop régulière.

D.1.2 Calcul de la longueur de cycle et de la période effective de (3125, 1, 2^{35}, 71)

Puisque les paramètres (a, b, m) = (3125, 1, 2^{35}) du générateur de la suite (3215, 1, 2^{35}, 71) vérifient les conditions du théorème I. 2. 1 i), la longueur de cycle de cette suite est égale à 2^{35}. D'après G. Marsaglia (1972), Théorème 3, la période effective δ de cette suite est donnée par

$$\delta = 2^{35} / \text{PGCD}(3125-1, 2^{35}).$$

Soit

$$\delta = 2^{33}.$$

Ainsi le générateur de la table de "Nombres au Hasard" vérifie les critères de qualité cités dans la remarque II. 1. 22 2) : les période et période effective sont suffisamment grandes.

D.2 Test des Treillis

Soit $(x) = \{ x_i \}$ une suite (a, b, m, x_0) de période maximale m. Nous avons montré au paragraphe II. 1 que, pour un entier n, n > 1, l'ensemble

$$G_n^1 = \{\underline{y} = \underline{x} + m\underline{z} \ : \underline{x} \in V_n^1, \underline{z} \in \mathbb{Z}^n\}$$

avec

$$V_n^1 = \{(x_i, \ldots, x_{i+n-1}) : x_j \equiv ax_{j-1} + b \mod m, i < j < i + n, 0 \leq i < m\}$$

est une grille de vecteur de translation

$$\underline{b}_0(x_0) = x_o(1, a, \ldots, a^{n-1}) + b(0,1, 1 + a, \ldots, 1 + a + \ldots + a^{n-2})$$

et de base

$$\underline{b}_1 = (1, a, \ldots, a^{n-1})$$

$$\underline{b}_2 = (0, m, \ldots, 0)$$

$$\vdots$$

$$\underline{b}_n = (0, 0, \ldots, m).$$

Mais pour faciliter l'étude de la distribution de la suite $(x) = \{x_i\}$ en dimension n, on fait l'étude du treillis R_n engendré par les vecteurs $\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_n$, c'est - à - dire,

$$R_n = \{z_1\underline{b}_1 + \ldots + z_n\underline{b}_n : (z_1, \ldots, z_n) \in \mathbb{Z}^n\}.$$

D'un point de vue géométrique, les vecteurs $\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_n$ engendrant le treillis R_n déterminent un parallélépipède P_n donné par

$$P_n = \{c_1\underline{b}_1 + \ldots + c_n\underline{b}_n : 0 \leq c_i \leq 1, i = 1, \ldots, n\}$$

et le volume de P_n est la valeur absolue du déterminant de la matrice carrée d'ordre n dont les lignes sont les vecteurs $\underline{b}_1, \underline{b}_2, \ldots, \underline{b}_n$. Si la suite (a, b, m, x_0) est équidistribuée en dimension n, alors le treillis R_n est identique au treillis idéal, c'est - à - dire, le treillis engendré par $(1, 0, \ldots, 0)$, $(0, 1, 0, \ldots, 0), \ldots, (0, 0, 0, \ldots, 1)$. Cela veut dire que le volume du parallélépipède obtenu à partir des vecteurs de la base de R_n est égal à 1. Dans ce cas on dit que le générateur (a, b, m) passe le test des treillis.

Partant de de cette définition du test des treillis, on déduit de l'étude de la structure de grille des nombres pseudo - aléatoires congruentiels que toutes les congruences linéaires simples échouent à ce test. En particulier pour une congruence linéaire (a, b, m) de période m, le volume du parallélépipède P_n est égal à m^{n-1}. L'échec des générateurs congruentiels à ce test est dû à leur structure d'hyperplans dont l'exposé a été fait au début du paragraphe B. Il existe cependant des méthodes permettant de brasser un générateur congruentiel afin de détruire sa " régularité cristalline" (cf. D . E . Knuth (1969), p. 30 et M. D. Maclaren et G. Marsaglia(1965)). Dans la recherche des congruences linéaires candidats à ce brassage, on choisit celles dont le treillis (en dimension 2, 3, 4 et 5 par exemple) n'est pas "trop éloigné" du treillis idéal. Un treillis en dimension n n'est pas "trop éloigné" du treillis idéal lorsque le quotient de Beyer de sa base réduite est proche de 1. Si pour un entier n, $n > 1$, une congruence linéaire donne lieu à un treillis dont le quotient de Beyer de sa base réduite est proche de 1, alors on dit alors que cette congruence linéaire a un bon treillis en dimension n.

Le tableau ci - dessous comporte entre autres les quotients de Beyer en dimension 2, 3, 4, 5 et 6 des treillis provenant du générateur $(3125, 1, 2^{35})$.

dim n	2	3	4	5	6
Q. B. KNUTH	10995116.0	1.20768	5.52222	1.69948	2.13537
Q. B. LLL	3518.44	1.20768	5.52222	1.7301	2.22773
T. KNUTH	2.173	9.783	20.005	38.816	65.749
T. LLL	2.458	3.973	11.592	32.066	60.855

Q. B. KNUTH : Quotient de Beyer obtenu après la réduction d'une base au sens de KNUTH.

Q. B. LLL : Quotient de Beyer obtenu après la réduction de la même base, mais cette fois-ci au sens de LLL.

T. KNUTH : Temps mis pour réduire une base donnée suivant la méthode de KNUTH.

T. LLL : Temps mis pour réduire la même base suivant l'algorithme de LLL.

La première ligne du tableau ci-dessus contient les différentes dimensions des treillis provenant du générateur $(3125, 1, 2^{35})$. Les lignes 2 et 3 nous permettent de faire l'étude comparée des quotients de Beyer suivant les réductions au sens de Knuth et de LLL. Pour les dimensions 3 et 4 les Q. B sont identiques.Quant aux dimensions 5 et 6 les Q. B obtenus après réduction suivant la méthode de Knuth sont légèrement inférieurs à ceux résultant de l'algorithme de réduction de LLL. Au vu de ces résultats le générateur $(3125, 1, 2^{35})$ n'a pas un bon treillis pour les dimensions 2, 4 et 6.

Dans les lignes 4 et 5 apparaissent les temps de réduction en secondes C. P. U. : l'algorithme de réduction de LLL est plus rapide pour les dimensions n strictement supérieurs à 2.

Nous avons omis ici l'algorithme de réduction suivant U. DIETER, car dès la dimension 2 on a dépassé les 70 secondes C. P. U.

D. 3 TEST SPECTRAL

L'analyse du test spectral du générateur $(3125, 1, 2^{35})$ nous a donné les résultats résumés dans le tableau suivant.

n	2	3	4	5	6
d_n^2	9765626	9765626	56550	10126	1852
μ_n	0.000893254	3.72189	0.459658	1.58195	0.956524

Le générateur $(3125, 1, 2^{35})$ passe de façon remarquable le test spectral en dimension 3, 4, 5 et 6. En revanche il échoue au test spectral en dimension 2 : cela est probablement dû au fait que le multiplicateur 3125 est trop petit.

En conclusion le générateur $(3125, 1, 2^{35})$ peut être utilisé dans les simulations en dimension 3, 4, 5 et 6.

REMARQUE

Etant limités par les ressources, nous n'avons pas pû comparer les temps d'exécution des phases de recherche exhaustives des méthodes standard et de la méthode résultant de la combinaison de ces méthodes et de la méthode basée sur la décomposition de Cholesky.

II.2 Test sériel, test spectral et construction des multiplicateurs optimaux

A . Discrépance, test sériel et comparaison des tests sériel et spectral

Soient $N > 1$ et $n \geq 1$ deux entiers et $t_0, t_1, \ldots, t_{N-1}$ une suite d'éléments de $[0, 1[^n$. Désignons alors par SI l'ensemble des sous - intervalles de $[0, 1[^n$ donné par

$$SI = \{[a_1,b_1[\times \ldots \times [a_n, b_n[\ : \ 0 \leq a_i < b_i < 1, \ 1 \leq i \leq n\},$$

puis par $A_N^{(n)}(J)$ le nombre de points t_i, $0 \leq i < N$, appartenant à un intervalle J de SI, c'est - à -dire

$$A_N^{(n)}(J) = \#\{t_i \in J, 0 \leq i < N\}$$

où pour tout ensemble dénombrable E, #E est le cardinal de E.

Si Vol (J) dénote le volume de J alors la quantité $D_N^{(n)}(\underline{t}_0, \ldots, \underline{t}_{N-1})$, déterminée par

$$D_N^{(n)}(\underline{t}_0, \ldots, \underline{t}_{N-1}) = \max \left\{ \left| \frac{A_N^{(n)}(J)}{N} - \mathrm{Vol}(J) \right| : J \in SI \right\},$$

est appelée *discrépance* des points $\underline{t}_0, \underline{t}_1, \ldots, \underline{t}_{N-1}$.

Nous considérons ici la discrépance $D_N^{(n)}(\underline{u}_0, \ldots, \underline{u}_{N-1})$ des points

$$\underline{u}_i = \underline{x}_i / m = (x_i / m, \ldots, x_{i+n-1} / m), \quad 0 \le i < N$$

où $(x) = \{x_i\}$ est une suite (a, b, m, x_0) et nous la notons $D_N^{(n)}$.

Pour $n = 1$, $D_N^{(n)}$ évalue l'écart entre la distribution empirique des N premiers N.P.A. de la suite $(u) = \{x_i/m\}$ et l'équirépartition sur $[0, 1[$: si la valeur de $D_N^{(n)}$ est suffisamment petite alors on dit que la suite $(u) = \{x_i/m\}$ est uniformément répartie sur $[0, 1[$. Des estimations de $D_N^{(n)}$ effectuées dans Niederreiter (1976b) montrent que pour N suffisamment grand, la suite $(u) = \{x_i/m\}$, où $(x) = \{x_i\}$ provient de l'un des générateurs spécifiés dans le théorème I.2.1, est une bonne approximation de l'équidistribution sur $[0, 1[$.

D'autre part le test basé sur $D_N^{(n)}$, pour $n > 1$, est appelé *test sériel en dimension* n : Si la valeur de $D_N^{(n)}$ est voisine de zéro pour N grand, alors on dit que la suite de N.P.A. $(u) = \{x_i/m\}$ passe le test sériel d'ordre n, c'est-à-dire; n termes consécutifs du cycle de cette suite sont considérés comme étant statistiquement indépendants.

On va établir maintenant une relation entre le test sériel et le test spectral.

II.2.1. THEOREME (cf. D.E. Knuth (1981))

Soient $(x) = \{x_i\}$ une suite (a, b, m, x_0) de période m et s le plus petit entier naturel non nul tel que $a^s \equiv 1 \bmod m$. Si pour $n > 1$, la quantité d_n déterminée dans le théorème II.1.12 n'est pas trop petite alors la discrépance $D_N^{(n)}$ des N premiers termes du cycle de la suite $u = \{x_i/m\}$ vérifie

$$(15) \quad \begin{cases} D_N^{(n)} = O\left(\dfrac{\sqrt{s}\ (\log m)^n \log s}{N}\right) + \dfrac{m\,(\log m)^n}{N\sqrt{s}} + O\left(\dfrac{(\log m)^n}{d_n}\right), & 1 \le N < m \\ D_m^{(n)} = O\left(\dfrac{(\log m)^n}{d_n}\right) \end{cases}$$

où O(v) désigne le produit de v par une constante.

Pour N = m, l'estimateur (15) de la discrépance nous donne une relation entre le test sériel et le test spectral. En effet si d_n est assez grand, c'est-à-dire, si la suite $(x) = \{x_i / m\}$ passe le test spectral en dimension n, alors $D_m^{(n)}$ est voisin de zéro et par conséquent cette suite passe le test sériel en dimension n. Notons cependant qu'il existe (cf. D.E. Knuth (1981)) des suites de discrépance négligeable pour certaines dimensions n et ne passant pas le test spectral pour ces dimensions.

Nous allons nous intéresser, pour b et m fixés, au calcul des multiplicateurs a dits optimaux en ce sens que chacun des générateurs (a, b, m) donne lieu à une suite de N.P.A. passant le test sériel d'ordre 2 . Ainsi pour obtenir des suites passant le test spectral, on pourra faire une recherche sur les suites (a, b, m, x_0) où a est un multiplicateur optimal.

B. Présentation de quelques résultats Théoriques sur la discrépance des vecteurs de nombres pseudo-aléatoires et la figure de mérite d'une congruence linéaire simple

Soit $(x) = \{x_i\}$ une suite (a, b, m, x_0) de période τ avec

1. $m > 2$
2. $2 \leq a < m$ et $(a, m) = 1$
3. $0 \leq b < m$, $0 \leq x_0 < m$.

Pour $n \geq 2$, l'indépendance statistique entre n termes consécutifs de $(x) = \{x_i\}$ peut être mesurée à l'aide de la quantité $\rho^{(n)}(a, m)$ appelée *figure de mérite de* a *en dimension* n et définie comme suit :

Pour tout élément $\underline{h} = (h_1, h_2, \ldots, h_n)$ de $\mathbb{Z}^n$ on pose

$$r(\underline{h}) = \prod_{i=1}^{n} \max(1, |h_i|).$$

Alors $\rho^{(n)}(a, m)$ est donnée par

$$\rho^{(n)}(a, m) = \min \{r(2\underline{h})\}$$

où le minimum est étendu à tous les éléments $\underline{h} = (h_1, \ldots, h_n)$ de $\mathbb{Z}^{n*}$ tels que

$$h_1 + h_2 a + \ldots + h_n a^{n-1} \equiv 0 \bmod m, \qquad -\frac{m}{2} < h_j \leq \frac{m}{2}, \qquad 1 \leq j \leq n.$$

Nous allons considérer maintenant l'estimation de $D_\tau^{(n)}$ en fonction de $\rho^{(n)}(a, m)$. Pour cela on pose les trois conditions ci - après :

i) m est un nombre premier et a est une racine primitive modulo m.

ii) $m = 2^{\alpha}, \alpha \geq 3$, $a \equiv 5 \mod m$ et b impair.

iii) $m = 2^{\alpha}, \alpha \geq 3$, $a \equiv 5 \mod m$ et $b = 0$.

Alors les relations suivantes entre $D_{\tau}^{(n)}$ et $\rho^{(n)}(a, m)$ ont été établies dans H. Niederreiter (1985).

Dans le cas où les paramètres a, b et m vérifient l'une ou l'autre des conditions i) et ii) on a :

$$\frac{c_n}{\rho^{(n)}(a, m)} \leq D_{\tau}^{(n)} \leq \frac{c'_n (\log m)^n}{\rho^{(n)}(a, m)}$$

et si ces paramètres satisfont iii), alors on obtient

$$\frac{c_n}{\rho^{(n)}(a, m/4)} \leq D_{\tau}^{(n)} \leq \frac{c'_n (\log m)^n}{\rho^{(n)}(a, m/4)}$$

où les quantités c_n et c_n' sont des constantes strictement positives ne dépendant que de n. On en déduit que pour m et n fixés, les bons multiplicateurs a relativement au test sériel en dimension n sont obtenus en maximisant la figure de mérite appropriée. Dans le cas $n = 2$, cela est facilité par l'existence d'une relation entre la figure de mérite et les fractions continues. Plus précisément si $[a_1, \ldots, a_q]$ est le développement en fraction continue simple de a / m, alors (cf. S. K. Zaremba(1966)) on a

$$\frac{m}{4(K + 1)} \leq \rho^{(2)}(a, m) \leq \frac{m}{4K}$$

avec

$$K = K(a/m) = \max (a_1, \ldots, a_q).$$

Ainsi la valeur de $\rho^{(2)}(a, m)$ est assez grande si les quotients partiels du développement en fraction continue simple de a/m sont suffisamment petits. D'autre part une formule établie dans I. Borosh et H.Niederreiter (1983) permet de calculer en temps raisonnable $\rho^{(2)}(a, m)$:

$$(16) \quad \rho^{(2)}(a, m) = \min \{|q_k| q_k a - p_k m|\}$$

où le minimum est étendu à toutes les réduites p_k / q_k de a/m avec $q_k < m$.

Mais si pour a et m donnés on peut calculer aisément $K = K(a/m)$, est - il possible pour m fixé de trouver un majorant ou mieux une borne supérieure de K_m avec

$$K_m = \min \{K(a/m)\}$$

où le minimum est étendu à tous les entiers a vérifiant $1 \leq a < m$ et $(a, m) = 1$.

Une conjecture de Zaremba (cf . Zaremba (1972), pp. 69 et 76) affirme que $K_m \leq 5$ pour tout m et cette conjecture a été démontrée par H. Niederreiter (1986d) dans le cas où m est une puissance de 2 : plus précisément il a établi de façon constructive que pour tout m de la forme 2^n, $n \geq 1$, il existe un entier impair a tel que $1 \leq a < m$ et $K(a / m) \leq 3$, le majorant 3 étant en fait une borne supérieure .

Nous considérons ici le cas où m est un nombre premier et nous mettons en oeuvre une méthode de recherche des multiplicateurs optimaux relatifs à n = 2, méthode due à I. Borosh et H. Niederreiter (1983).

C. Description d'une méthode de recherche des multiplicateurs optimaux en dimension 2

D'après le paragraphe précédent les bons multiplicateurs a pour m fixé sont ceux pour lesquels K(a / m) est le plus petit possible. Nous présentons maintenant une méthode de recherche qui consiste à trouver des racines primitives a modulo m telles que $K(a / m) \leq 5$.

Pour $\ell \in \mathbb{N}^*$ et $(a_1, \ldots, a_\ell) \in \mathbb{N}^\ell$, on considère l'ensemble $I_{a_1, \ldots, a_\ell}$ des réels de l'intervalle]0,1] dont le développement en fraction continue simple est de la forme $[a_1, a_2, \ldots, a_\ell, \ldots]$. $I_{a_1, \ldots, a_\ell}$ est un intervalle dont les extrémités sont $[a_1, a_2, \ldots, a_\ell]$ et $[a_1, \ldots, a_{\ell-1}, a_\ell + 1]$ et dont la longueur est $1 / q_\ell (q_\ell + q_{\ell-1})$ avec $p_\ell / q_\ell = [a_1, a_2, \ldots, a_\ell]$. Pour $\ell_1 \in \mathbb{N}^*$, on considère l'ensemble

$$F_{\ell_1} = \left\{ I_{a_1, \ldots, a_{\ell_1}} : a_i \in \{1,2\},\ 1 \leq i \leq \ell_1 \right\}.$$

Chaque intervalle I de F_{ℓ_1} nous donne deux intervalles de F_{ℓ_1+1} contenus dans I ; ensuite chaque intervalle I' de F_{ℓ_1+1} nous donne deux intervalles de F_{ℓ_1+2} contenus dans I' et ainsi de suite. Une telle construction conduit à la limite à un ensemble de Cantor. On arrête cependant la subdivision d'un intervalle lorsque sa longueur est strictement inférieure à un réel $\varepsilon > 0$ fixé à l'avance. L'ensemble $F(\varepsilon)$ de tous les intervalles ainsi obtenus est appelé *ensemble de Cantor tronqué* donné par

$$F(\varepsilon) = \left\{ I_{a_1, \ldots, a_t} : t \in \mathbb{N}^*,\ a_i \in \{1,2\},\ 1 \leq i \leq t,\ |I_{a_1, \ldots, a_t}| < \varepsilon \text{ et } |I_{a_1, \ldots, a_{t-1}}| \geq \varepsilon \right\}.$$

Pour tout élément l de $F(\varepsilon)$ et pour tout a appartenant à l'intervalle ml, on calcule $K(a / m)$. Si $K(a / m) \leq 5$ et si a est un élément primitif modulo m alors on calcule la figure de mérite $\rho^{(2)}(a, m)$ suivant la formule (16).

D. Résultats de la mise en oeuvre de l'algorithme de calcul des multiplicateurs optimaux en dimension 2

Un programme a été écrit dans le système réduce installé sur le Cyber 990 du Centre de Calcul Universitaire de Grenoble. Ce système de calcul formel, adapté entre autres à la manipulation des grands entiers et au calcul exact en arithmétique, nous a permis de tester la primalité des entiers de l'ordre de 11 chiffres (c'est une taille raisonnable pour les entiers utilisés comme modulo dans les congruences linéaires simples considérés comme générateurs de nombres pseudo-aléatoires), de calculer $F(\varepsilon)$ et de faire la recherche des coefficients optimaux sur un intervalle donné.

a) TEST DE PRIMALITE

Pour tester la primalité d'un entier n, nous avons choisi un algorithme nécessitant la factorisation complète de n-1(cf. D. E. Knuth (1981)). Il y a bien sûr des tests de primalité plus rapides utilisant la factorisation partielle de n-1(cf. H. Cohen (1980-1981)), mais notre choix a été motivé par le fait que nous aurons à utiliser les diviseurs premiers de p-1, où p est un nombre premier résultant du test de primalité, pour tester la primitivité modulo p de certains entiers lors de la recherche des coefficients optimaux.

Exemples de nombres premiers p de 11 chiffres

p	FACTEURS PREMIERS DE p-1
$2^{35}-31 = 34\ 359\ 738\ 337$	2, 3, 7, 11, 31, 151, 331
$2^{35} - 141 = 34\ 359\ 738\ 227$	2, 11, 23, 67 904 621
$2^{36} - 5 = 68\ 719\ 476\ 731$	2, 5, 6 871 947 673

b) CALCUL DE F(ε)

Afin de faire une comparaison avec les résultats obtenus par I. Borosh et H. Niederreiter (1983), nous nous sommes proposés de choisir les mêmes valeurs de ε que ces deux auteurs. La valeur maximum de ε utilisée par ceux-ci étant 1/100 et le coût du calcul de F(ε) étant une fonction décroissante de ε, nous nous sommes limités à ε = 1/00. Aussi avons nous trouvé

F(1/100) = {[5/12, 7/17], [7/12, 10/17], [8/11, 11/15], [7/10, 12/17], [12/17, 17/24], [3/8, 5/13], [5/13, 7/18], [4/11, 7/19], [7/19, 10/27], [5/12, 8/19], [8/19,11/26], [5/8, 8/13], [8/13, 11/18], [7/11, 12/19], [12/19, 17/27], [7/12, 11/19], [11/19, 15/26], [8/11, 13/18], [13/18, 18/25] }.

Nous constatons que le cardinal de F(1/100) est de 19 alors que pour I. Borosh et H. Niederreiter ce cardinal n'est que 13. L'unique explication que avons pu donner à cette différence entre les deux résultats est la suivante : Les deux auteurs ont travaillé avec des réels en double précison alors que nous avons fait un calcul exact.

c) Recherche des coefficients optimaux

Il est clair que pour les nombres premiers p assez petits (p = 2, 3, 5, ...), on a peu de chance de trouver des coefficients optimaux(mêmes lorsqu'ils existent) à l'aide de $F(\varepsilon)$ pour de faibles valeurs de ε(ε = 1/100 par exemple). Mais pour de tels nombres premiers, on peut faire une recherche à la main ou utiliser $F(\varepsilon)$ avec ε suffisamment grand.

Pour les nombres premiers p assez modestes (nombres de quatre chiffres par exemple) les intervalles pI, où I est un élément de F(1/100), sont suffisamment grands pour qu'on puisse y faire pratiquement une recherche exhaustive des coefficients optimaux.

Exemples de coefficients optimaux pour deux nombres premiers p de 4 chiffres

p	coefficient optimal a	K(a/p)	$\rho^{(2)}(a, p)$
1999	826	3	484
2909	1707	2	960
2909	1205	3	770
2909	1704	3	770
2909	2129	3	779

Nous remarquons que pour p = 2909, K(1704/p) = K(2129/p). Ainsi pour discriminer les multiplicateurs optimaux 1704 et 2129, on fait intervenir leur figure de mérite respective et on choisit 2129 qui a une figure de mérite plus élévée. Notons cependant que le critère de figure de mérite est quelquefois insuffisant pour discriminer deux coefficients optimaux : c'est le cas pour les multiplicateurs 1205 et 1704.

Pour les nombres premiers p assez grands ($p = 2^{35} - 31$ par exemple) les intervalles pI, où I est un élément de F(1/100), sont en général trop grands pour qu'on puisse y faire rapidement une recherche exhaustive des coefficients optimaux. Aussi avons nous fait une recherche par tranche de 50 entiers et on a arrêté la recherche dès qu'on avait trouvé un coefficient optimal ou dès qu'on a fait des recherches sans succès sur un certain nombre de tranches fixées. Dans ce dernier cas on a recommencé la recherche sur un autre intervalle pI.

_ Pour $p = 2^{35}-31$, une recherche sans succès a été faite sur les 1850 premiers entiers de chacun des intervalles [14 148 127 452, 14 316 557 067], [20 043 179 895, 20 211 610 644] et [24 998 900 359, 25 197 141 195]. Notons que ces trois intervalles correspondent respectivement aux éléments [5/12,7/17], [7/12, 10/17] et [8/11, 11/15] de F(1/100).

_Quant à $p = 2^{36}-5$, une recherche, elle aussi sans succès, a été réalisée sur seulement les 500 premiers entiers de chacun des trois intervalles [25 769 803 775, 26 430 567 656], [40 086 359 823, 40 423 221 323] et [49 977 800 760, 50 394 282 432], intervalles correspondant respectivement à [3/8, 5/13], [7/12, 10/17], et [8/11, 11/15].

Etant limités par les ressources, les recherches ont été faites sur une proportion peu significative pour qu'on puisse faire l'hypothèse qu'il n'existe pas de coefficients optimaux pour les modulo p assez grands : sur la première série de trois intervalles cette proportion est de $1/10^4$, alors que sur la seconde elle n'est que de $7/10^7$.

D'après ces résultats on serait peut - être tenté de dire qu'il aurait été plus avantageux de concentrer, pour chacun des deux nombres p utilisés, les recherches sur

un seul intervalle. Cette réflexion nous amène naturellement aux deux questions suivantes. Pour un nombre premier p donné et pour un intervalle I inclus dans [1, p[fixé, peut-on donner une estimation ou mieux la valeur exacte de la proportion des nombres primitifs modulo p appartenant à I. Plus généralement, étant donné un nombre premier p, quelle est la distribution des nombres primitifs modulo p dans l'intervalle [1, p-1]. Une réponse à l'une ou à l'autre de ces questions est une information importante pouvant nous permettre d'adopter une meilleure stratégie dans la recherche des coefficients optimaux.

REMARQUE Une recherche sans succès sur une tranche de 100 chiffres a coûté environ 12 s c.p.u.

CHAPITRE 2

CONGRUENCES LINEAIRES MUTLIDIMENSIONNELLES

ET NOMBRES PSEUDO-ALEATOIRES

I. ETUDE DES SUITES ENGENDREES PAR UNE CONGRUENCE LINEAIRE MULTIDIMENSIONNELLE

I.1 CARACTERISTIQUES D'UNE SUITE ENGENDREE PAR UNE CONGRUENCE LINEAIRE MULTIDIMENSIONNELLE

Soient $k, m, a_0, a_1, \dots, a_{k-1}$ des entiers vérifiant

$$m > 1, \quad k > 1$$
$$0 \le a_i < m, \quad i = 0, 1, \dots, k-1$$
$$0 \le b < m.$$

On considère alors la suite $(s) = \{s_n\}$ sur $\mathbb{Z}_m$ définie par la donnée des termes initiaux $s_0, \dots, s_{k-1}$ et la congruence linéaire

$$(0) \qquad s_{n+k} \equiv a_{k-1}s_{n+k-1} + \dots + a_0 s_n + b \bmod m, \quad \forall\, n \ge 0.$$

L'identité (0) est appelée **congruence linéaire multidimensionnelle** (en abrégé C.L.M.) ou récurrence linéaire d'ordre k sur $\mathbb{Z}_m$. Si b est non nul alors elle est dite **non homogène** sinon elle est dite **homogène**. Comme on peut toujours se ramener à ce dernier cas (cf. R. Lidl and H. Niederreiter (1983)) on supposera dans la suite que b est nul.

La suite $(s) = \{s_n\}$ engendrée par (0) est dite **suite congruentielle linéaire multidimensionnelle** (en abrégé S.C.L.M.) ou **suite récurrente linéaire homogène** (en abrégé S.R.L.H.) d'ordre k sur $\mathbb{Z}_m$. Les termes de la suite $(s) = \{s_n\}$ appartenant à l'ensemble fini $\mathbb{Z}_m$ il existe, comme dans le cas d'une congruence linéaire simple, deux entiers $c > 0$ et $t \ge 0$ tels que

$$(**) \qquad s_{n+c} = s_n, \quad \forall\, n \ge t.$$

On dit alors que la suite (s) est **fondamentalement périodique.** Soit $c_0 > 0$ le plus petit entier c vérifiant (**). Alors c_0 est appelé **longueur de cycle** ou **période** de la suite $(s) = \{s_n\}$, tandis que la **longueur du transitoire** t_0 de cette suite est définie comme étant le minimum des entiers naturels t tels que

$$s_{n+c_0} = s_n, \quad \forall\, n \ge t.$$

La séquence $(s_{t_o}, s_{t_o+1}, \cdots, s_{t_o+c_o-1})$ est appelée cycle de (s) et dans le cas $t_0 > 0$, $(s_o, s_1, \cdots, s_{t_o-1})$ est le transitoire de (s).

REMARQUE

Si pour un entier strictement positif c on a

$$s_{n+c} = s_n , \quad \forall \ n \geq t_o$$

alors c_o divise c.

I.2. GENERALITES SUR LE CALCUL DES LONGUEURS DU TRANSITOIRE ET DE CYCLE

Nous présentons ici les principaux résultats établis par M. Ward(1933).

Etant donné un entier $k > 1$, on considère la récurrence

$$(1) \qquad d_{n+k} = c_1 d_{n+k-1} + \cdots + c_{k-1} d_{n+1} + c_k d_n, \quad \forall \ n \geq 0$$

et le polynôme associé F(x)

$$(2) \qquad F(x) = x^k - c_1 x^{k-1} - \ldots - c_{k-1} x - c_k$$

où les coefficients $c_1, c_2, \ldots, c_k$ sont dans $\mathbb{N}$.

Soient $m > 1$ un entier et $(u) = \{u_n\}$ une suite d'éléments de $\mathbb{N}$ vérifiant (1). On se propose d'étudier ici les longueurs de cycle et du transitoire de (u) mod m :

$$(u) \bmod m = \{u_n \bmod m\}.$$

Pour cela, il est nécessaire de préciser certaines notations et définitions.

La suite (u) mod m est dite **purement périodique** si sa longueur du transitoire est nulle et **elle est dite nulle** lorsque son cycle est réduit à l'entier 0. Il convient de remarquer qu'une suite nulle peut être différente d'une suite identiquement nulle dans laquelle tous les termes sont égaux à 0.

U_1 désignera l'ensemble des suites (u) sur $\mathbb{N}$ vérifiant (1) et U_2 l'ensemble des résidus modulo m des éléments de U_1. Afin de faire ressortir la dépendance d'un

élément (t) de U_2 par rapport à F(x), on notera quelquefois (t) modd (m, F(x)) au lieu de (t) mod m. Enfin (u) = (a) mod m signifie

$$(a) = \{u_n \bmod m\}.$$

a) THEOREMES FONDAMENTAUX SUR LES SUITES NULLES ET PUREMENT PERIODIQUES

Nous commençons par définir les opérations d'addition sur U_1 et U_2. Pour tout (u) et (v) de U_1, la somme (u) + (v) est définie par

$$(u) + (v) = (u + v) = \{u_n + v_n\}$$

et quels que soient les éléments (a) et (b) de U_2 on pose

$$(a) + (b) = (a + b) = \{(a_n + b_n) \bmod m\}.$$

On vérifie immédiatement que U_1 et U_2 sont des groupes pour ces opérations d'addition.

I.2.1. LEMME

Toute suite (u) de U_1 peut se mettre sous la forme

$$(u) = (v) + (w)$$

où (v) mod m est une suite purement périodique de même période que (u) mod m et où (w) mod m est une suite nulle de même longueur du transitoire que (u) mod m. De plus cette décomposition est unique modulo m, c'est-à-dire, s'il existe une seconde décomposition

$$(u) = (v') + (w')$$

où (v') mod m est une suite purement périodique et (w') mod m est une suite nulle alors

$$(v') \bmod m = (v) \bmod m \quad \text{et} \quad (w) \bmod m = (w') \bmod m.$$

DEMONSTRATION

Désignons respectivement par t et c les longueurs du transitoire et de cycle de (u) mod m. Si on suppose que

$$t = -r \bmod c, \text{ pour } 0 \leq r < c$$

alors $t + r = qc$ pour un entier q convenable.
On pose

$$v_n = u_{t+r+n}, \quad w_n = u_n - v_n, \qquad n \geq 0.$$

Alors on vérifie immédiatement que

$$(u) = (v) + (w)$$

est une décomposition de (u), où (w) mod m est une suite nulle de longueur du transitoire t et où (v) mod m est une suite purement périodique de période c. Cette décomposition est unique modulo m. En effet s'il existait une seconde décomposition

$$(u) = (v') + (w')$$

alors on aurait $(v - v') = (w - w')$ et donc $(w - w')$ mod m serait une suite identiquement nulle. Ce qui conduirait à

$$(w) \bmod m = (w') \bmod m \text{ et } (v) \bmod m = (v') \bmod m .$$

C . Q . F . D.

Nous sommes maintenant en mesure d'énoncer et de démontrer les deux théorèmes fondamentaux suivants :

I.2.2. THEOREME

Si $(u) = \{u_n\}$ est une solution de (1), alors une condition nécessaire et suffisante pour que (u) mod m soit purement périodique de période divisant d est que

$$(3) \qquad x^{d-1}U(x) \equiv 0 \text{ modd } (m, F(x))$$

où

$$(4) \qquad U(x) = u_0x^{k-1} + (u_1 - c_1u_0)x^{k-2} + \ldots + (u_{k-1} - c_1u_{k-2} - \ldots - c_{k-1}u_0)$$

est un polynôme dont les coefficients sont entièrement déterminés par les k valeurs initiales de (u) et les coefficients de (1), tandis que F(x) est le polynôme associé à (1).

I.2.3. DEFINITION

Le polynôme U(x) défini dans le théorème I.2.2. est appelé générateur de (u).

I.2.4. THEOREME

Si U(x) est le générateur de (u) solution de (1), alors une condition nécessaire et suffisante pour que (u) mod m soit une suite nulle de longueur du transitoire inférieure ou égale à d est que

$$(5) \qquad x^d U(x) \equiv 0 \text{ modd } (m, F(x)).$$

DEMONSTRATION DU THEOREME I.2.2.

Soit $U_d(x)$ le polynôme défini à partir des d premiers termes de (u) par

$$U_d(x) = u_ox^{d-1} + u_1x^{d-2} + \ldots + u_{d-2}x + u_{d-1}.$$

Alors, compte tenu de (1), on a

$$F(x)U_d(x) = x^d\{u_ox^{k-1} + (u_1 - c_1u_o)x^{k-2} + \cdots + (u_{k-1} - c_1u_{k-2} - \cdots - c_{k-1}u_o)\}$$

$$- \{u_dx^{k-1} + (u_{d+1} - c_1u_d)x^{k-2} + \ldots + (u_{d+k-1} - c_1u_{d+k-2} - \ldots - c_{k-1}u_d)\}.$$

Notons respectivement par U(x) et $U^{(d)}(x)$ les deux polynômes entre accolades et considérons l'identité ci-dessus modulo m, puis modulo F(x). Alors on obtient la congruence à double modulo

$$(6) \qquad x^d U(x) - U^{(d)} \equiv 0 \text{ modd } (m, F(x)).$$

Supposons maintenant que (u) mod m soit purement périodique et que d soit un multiple de sa période. Alors

$$U^{(d)}(x) \equiv U(x) \text{ modd } (m, F(x))$$

et (6) devient

$$(x^d-1)U(x) \equiv 0 \text{ modd } (m, F(x)).$$

Réciproquement si d vérifie cette dernière congruence alors (u) mod m est purement périodique de période divisant d.

C. Q. F. D.

DEMONSTRATION DU THEOREME I.2.4.

D'après (6) on a :

$$x^d U(x) - U^{(d)}(x) \equiv 0 \text{ modd } (m, F(x)).$$

Supposons que (u) mod m est une suite nulle de longueur du transitoire inférieure ou égale à d. Alors

$$U^{(d)}(x) \equiv 0 \text{ modd } (m, F(x))$$

et la congruence ci-dessus devient

$$x^d U(x) \equiv 0 \text{ modd } (m, F(x)).$$

Réciproquement si pour un entier d cette dernière congruence est vérifiée alors (u) mod m est une suite nulle de longueur du transitoire inférieure ou égale à d .

C.Q.F.D.

Des théorèmes I.2.2. et I.2.4. on déduit les deux corollaires suivants :

I.2.5. COROLLAIRE

Si (u) est une suite solution de (1) et si (u) mod m est purement périodique, alors sa période est le plus petit entier d tel que la relation (3) soit satisfaite.

I.2.6. COROLLAIRE

Soit (u) une suite vérifiant (1). Si (u) mod m est une suite nulle, alors sa longueur du transitoire est le plus petit entier d pour lequel on a (5).

Nous constatons que les théorèmes I.2.2. et I.2.4., permettant de calculer les longueurs du transitoire et de cycle d'une suite (u) mod m pour (u) vérifiant (1), font intervenir des congruences à double modulo m et F(x). Il est donc intéressant de déterminer un anneau U_3 associé à ce double modulos, anneau isomorphe à U_2 (qu'on munira d'une structure d'anneau) et dans lequel on peut utiliser la théorie des congruences à double modulo. Pour cela on prend pour U_3 l'ensemble des m^k polynômes

$$L(x) = \ell_o x^{k-1} + \ell_1 x^{k-2} + \ldots + \ell_{k-2} x + \ell_{k-1}, \quad \text{pour} \quad 0 \le \ell_i < m \quad \text{et} \quad i = 0, 1, \ldots, k-1.$$

Avant d'énoncer un résultat qui établit un isomorphisme entre U_2 et U_3, on munit U_2 d'une structure d'anneau.
Pour un polynôme L(x) de U_3 avec

$$L(x) = \ell_o x^{k-1} + \ldots + \ell_{k-2} x + \ell_{k-1}$$

on considère le problème de recherche d'une suite $(a) = \{a_n\}$ de U_2 tel qu'il existe une solution $(u) = \{u_n\}$ de (1) satisfaisant

$$(7) \quad \begin{cases} a_i = u_i \mod m, & i = 0, 1, \cdots, k-1 \\ (u_r - c_1 u_{r-1} - \ldots - c_r u_o) \mod m = \ell_r, & r = 0, 1, \ldots, k-1. \end{cases}$$

Puisque le système (7) admet une solution unique (u) mod m on prend pour (a) l'élément de U_2 dont les k termes initiaux $a_o, \ldots, a_{k-1}$ satisfont

$$a_i = u_i \mod m, \quad i = 0, 1, \ldots, k-1.$$

Il est alors naturel d'associer à L(x) la suite (a) = $\{a_n\}$.
Réciproquement le système (7) admet pour un élément (a) de U_2 donné une solution en l_r, donc L(x) est déterminé de façon unique . On a ainsi une bijection entre U_2 et U_3 et nous notons

$$(a) \sim L(x)$$

si l'élément (a) de U_2 correspond à l'élément L(x) de U_3.
Supposons

$$(b) \sim M(x) .$$

Il est alors clair que

$$(a + b) \sim L(x) + M(x).$$

De plus si

$$L(x).M(x) \equiv N(x) \text{ modd } (m, F(x))$$

alors le produit (a). (b) est défini comme étant la suite (c) associée à N(x) et on note

$$(a).(b) \sim L(x).M(x).$$

Enfin le théorème suivant découle de ces considérations.

I.2.7. THEOREME

L'ensemble U_2 muni des opérations d'addition et de multiplication définies ci-dessus est un anneau isomorphe à l'anneau U_3. Le polynôme L(x) de U_3 associé à un élément (a) de U_2 par cet isomorphisme est

$$L(x) = \ell_0 x^{k-1} + \ell_1 x^{k-2} + \ldots + \ell_{k-2} x + \ell_{k-1}$$

où

$$\ell_r = (a_r - c_1 a_{r-1} - \ldots - c_r a_0) \bmod m, \quad r = 0, 1, \ldots, k-1.$$

b) SIMPLIFICATION DE LA FORME DE m ET DE F(x)

b.1. simplification de la forme de m

Soit

$$m = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$

la décomposition de m en un produit de facteurs premiers. Alors l'anneau des polynômes U_3 associé à m et à F(x) est la somme directe des anneaux associés à $p_i^{n_i}$ et F(x) pour i = 1, 2, ... , r . On obtient également une décomposition similaire de U_2 en somme directe d'anneaux plus simples.

I.2.8. THEOREME

Si $m = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$

est la factorisation en nombres premiers de m et si $(u) = \{u_n\}$ est une solution de (1), alors la période de (u) mod m est le PPCM des périodes de (u) mod $p_i^{n_i}$, tandis que sa longueur du transitoire est le maximum des longueurs du transitoire de (u) mod $p_i^{n_i}$ pour i = 1, 2, ... , r .

DEMONSTRATION

Il suffit de démontrer le théorème dans le cas m = ab, pour deux entiers a et b premiers entre eux, et le résultat général s'obtiendra par simple induction sur r.
Soit (u) = (v) + (w), la décomposition de $(u) = \{u_n\}$ telle que (v) mod m soit une suite purement périodique et (w) mod m une suite nulle. Comme a et b divisent m, (v) mod a et (v) mod b sont deux suites purement périodiques et d'autre part, (w) mod a et (w) mod b sont deux suites nulles.
D'après le lemme I.2.1., il suffit de démontrer le théorème pour la période de (v) mod m et pour la longueur du transitoire de (w) mod m.
Considérons d'abord la suite (w) et notons par t_m, t_a et t_b ses longueurs du transitoire respectivement pour les modulos m, a et b, par V(x) son générateur et enfin par d le maximum de t_a et de t_b. D'après le corollaire I.2.6. on a :

$x^{t_m} V(x) \equiv 0$ modd (m, F(x)), $x^{t_a} V(x) \equiv 0$ modd (a, F(x)) et $x^{t_b} V(x) \equiv 0$ modd (b, F(x)).

Par conséquent

$$x^{t_m}V(x) \equiv 0 \text{ modd } (a, F(x)) \quad \text{et} \quad x^{t_m}V(x) \equiv 0 \text{ modd } (b, F(x)).$$

Donc

$$t_m \geq d.$$

Puisque a et b sont premiers entre eux , on a

$$x^dV(x) \equiv 0 \text{ modd } (ab, F(x)).$$

Ce qui nous donne

$$d \geq t_m$$

et en définitive, on a

$$d = t_m.$$

En ce qui concerne la suite (v) nous posons

$$x_n \equiv v_n \text{ mod } m, \quad y_n \equiv v_n \text{ mod } m \quad \text{et} \quad z_n \equiv v_n \text{ mod } m, \qquad \forall\ n \geq 0.$$

Il s'agit maintenant de montrer que si c_o est la période de

$(X) = \{x_n\}$, c_1 celle de $(Y) = \{y_n\}$ et c_2 celle de $(Z) = \{z_n\}$ alors c_o est identique à c, avec

$$c = \text{PPCM } (c_1, c_2).$$

Mais

(8) $x_n = x_k$ si seulement si $y_n = y_k$ et $z_n = z_k$; $\forall\ n, k \geq 0.$

Et comme

$$x_{n+c_o} = x_n, \quad \forall \quad n \geq 0$$

on a

$$y_{n+c_o} = y_n \quad \text{et} \quad z_{n+c_o} = z_n, \quad \forall \quad n \geq 0.$$

Donc

$$c_o \geq c.$$

Mais d'après (8) on peut écrire

$$x_{n+c} = x_n, \quad \forall \quad n \geq 0.$$

Donc $c_o \leq c$. Soit $c_o = c$.

C.Q.F.D.

On suppose dans la suite que m est de la forme p^N, p étant un nombre premier et N un entier strictement positif.

b.2. simplification de la forme de F(x)

Soit

$$F(x) \equiv \{\phi_1(x)\}^{t_1} \{\phi_2(x)\}^{t_2} \ldots \{\phi_s(x)\}^{t_s} \bmod p$$

la décomposition de F(x) modulo p en un produit de puissance de polynômes unitaires et irréductibles sur $\mathbb{Z}_p$. Alors la décomposition de Schönemann de F(x) modulo p^N est donnée par

$$(9) \qquad F(x) \equiv F_1(x) \cdots F_s(x) \mod p^N.$$

A cette décomposition on fait correspondre celle de l'anneau U_3 des polynômes associés au double modulo p^N et F(x) en une somme directe des anneaux associés à p^N et $F_i(x)$ pour i = 1, 2, ... , s.

I.2.9. THEOREME

Soit U(x) le générateur de $(u) = \{u_n\}$ vérifiant (1). On considère ensuite la décomposition de Schönemann (9) de F(x) modulo p^N et on pose

$$U^{(i)}(x) \equiv U(x) \quad \text{modd } (p^N, F_i(x))$$

où le polynôme $U^{(i)}(x)$, de degré strictement inférieur à celui de $F_i(x)$, est considéré comme le générateur d'une suite $(u^{(i)}) = \{u_n^{(i)}\}$ solution de l'équation de récurrence (1) dont le polynôme associé est $F_i(x)$.
Alors la période de (u) modd $(p^N, F(x))$ est le PPCM des périodes de $(u^{(i)})$ modd $(p^N, F_i(x))$, i = 1, ... , s, tandis que sa longueur du transitoire est le maximum des longueurs du transitoire de $(u^{(i)})$ modd $(p^N, F_i(x))$ pour i = 1, 2, ... , s.

DEMONSTRATION

Soient

$$(u) = (v) + (w)$$

la décompositon de (u), où (v) mod p^N est une suite purement périodique et où (w) mod p^N est une suite nulle et

$$U(x) \equiv V(x) + W(x) \quad \text{modd } (p^N, F(x))$$

la décomposition correspondante du générateur U(x) de $(u) = \{u_n\}$.
On considère les identités

$$\begin{cases} U^{(i)}(x) \equiv U(x) \ \text{modd } (p^N, F_i(x)) \\ V^{(i)}(x) \equiv V(x) \ \text{modd } (p^N, F_i(x)) \\ W^{(i)}(x) \equiv W(x) \ \text{modd}(p^N, F_i(x)) \end{cases}$$

où les polynômes $U^{(i)}(x)$, $V^{(i)}(x)$ et $W^{(i)}(x)$, de degré strictement inférieur à celui de

$F_i(x)$, sont respectivement considérés comme étant les générateurs des suites $(u^{(i)})$, $(v^{(i)})$ et $(w^{(i)})$ solutions de l'équation (1) à laquelle on a associé le polynôme $F_i(x)$. Alors on a :

$$(10) \quad \begin{cases} (u^{(i)}) \equiv (v^{(i)}) + (w^{(i)}) \bmod p^N \\ U^{(i)}(x) \equiv V^{(i)}(x) + W^{(i)}(x) \bmod (p^N, F_i(x)). \end{cases}$$

Nous allons montrer que $(v^{(i)}) \bmod p^N$ est une suite purement périodique et $(w^{(i)}) \bmod p^N$ est une suite nulle.
Soient t et c les longueurs de cycle et du transitoire de (u) mod p^N. Alors d'après le lemme I.2.1., les corollaires I.2.5. et I.2.6. on a

$$x^t W(x) \equiv 0 \text{ modd } (p^N, F(x)) \quad \text{et} \quad (x^c-1)V(x) \equiv 0 \text{ modd}(p^N, F(x)).$$

Par conséquent

$$(11) \quad x^t W^{(i)}(x) \equiv 0 \text{ modd } (p^N, F_i(x)) \quad \text{et} \quad (x^c-1)V^{(i)}(x) \equiv 0 \text{ modd } (p^N, F_i(x))$$

et d'après les théorèmes I.2.2 et I.2.4., $(v^{(i)}) \bmod p^N$ est une suite purement périodique et $(w^{(i)}) \bmod p^N$ est une suite nulle.
Soient t_i la longueur du transitoire de $(w^{(i)}) \bmod p^N$ et c_i la période de $(v^{(i)}) \bmod p^N$ pour $i = 1, 2, ..., s$.
Nous allons montrer que c est égal à c' avec

$$c' = \text{PPCM } (c_1, \dots, c_s).$$

D'après la seconde congruence de (11), c_i divise c pour tout $i = 1, 2, \dots, s$. Par conséquent c' divise c.
D'autre part, on a

$$(x^{c'}-1)V^{(i)}(x) \equiv 0 \text{ modd } (p^N, F_i(x)), \qquad i = 1, 2, \dots, s.$$

Donc

$$(x^{c'}-1)V(x) \equiv 0 \text{ modd } (p^N, F_i(x)) \qquad i=1, 2, \dots, s.$$

Comme RES $\{F_i(x), F_j(x)\}$ est premier avec p pour $i \neq j$, on déduit des s dernières congruences l'équation

$$(x^c-1)V(x) \equiv 0 \text{ modd } (p^N, F(x)).$$

Et le théorème I.2.2. entraîne que c divise c'.

D'où

$$c = c'.$$

En ce qui concerne la longueur du transitoire t de (u) mod p^N, un raisonnement analogue à celui qu'on vient de faire nous permet de montrer que t est le maximum de $t_1, \ldots, t_s$.

C. Q. F. D.

c) DETERMINATION DES COMPOSANTES NULLE ET PUREMENT PERIODIQUE D'UNE SUITE MODULO p^N

On suppose ici que $m = p^N$ et que le coefficient c_k de (1) est divisible par p.

I.2.10. REMARQUE

Si c_k est premier avec m et si $(u) = \{u_n\}$ est une solution de (1) alors (u) mod m est une suite purement périodique.

I.2.11. THEOREME

Soient F(x) le polynôme associé à (1) et

$$F(x) \equiv F_1(x) \cdots F_s(x) \mod p^N$$

la décomposition de Schönemann (9) de F(x) mod p^N. On suppose que

$$F(x) = x^{t_1} + pV(x).$$

Si $(u) = \{u_n\}$ est une solution de (1) alors une condition nécessaire et suffisante pour que (u) mod p^N soit une suite nulle est que son générateur U(x) vérifie

$$U(x) \equiv 0 \mod d(p^N, F_2(x) \cdots F_s(x)).$$

Dans ce cas, la longueur du transitoire de (u) modulo p^N est le plus petit entier d tel que

$$(12) \qquad x^d U(x) \equiv 0 \mod d\ (p^N, F_1(x)).$$

DEMONSTRATION

Soient $(u) = \{u_n\}$ une solution de (1) et

$$F'(x) = F_2(x) \ \ldots \ F_s(x).$$

Alors RES $\{F_1(x), F'(x)\}$ est premier avec p. D'après le théorème I.2.4., la suite (u) mod p^N est une suite nulle si et seulement s'il existe un entier d tel que

$$x^d U(x) \equiv 0 \mod d(p^N, F(x))$$

où U(x) est le générateur de $(u) = \{u_n\}$. Mais cette congruence admet une solution d si et seulement si les deux congruences

$$\begin{cases} x^d U(x) \equiv 0 \mod d\ (p^N, F_1(x)) \\ x^d U(x) \equiv 0 \mod d\ (p^N, F'(x)) \end{cases}$$

en admettent une. La première de ces congruences a toujours une solution, car il suffit de prendre $d = Nt_1$ et la seconde admet une solution si et seulement si

$$U(x) \equiv 0 \mod d\ (p^N, F'(x))$$

puisque RES $\{x, F'(x)\}$ est premier avec p

C.Q.F.D.

On démontre de façon analogue le résultat suivant :

I.2.12. THEOREME

Sous les hypothèses du théorème I.2.11., une condition nécessaire et suffisante pour que (u) mod p^N soit purement périodique est que le générateur U(x) de (u) vérifie

$$U(x) \equiv 0 \ \text{modd}\ (p^N,\ F_1(x)).$$

On détermine maintenant les composantes nulle et purement périodique de (u) mod p^N où (u) est une solution de (1).
Puisque RES $\{F_1(x), F'(x)\}$ est premier avec p, on peut calculer deux polynômes $S_1(x)$ et $S_2(x)$ tels que

$$S_1(x)F_1(x) + S_2(x)F'(x) \equiv U(x) \ \text{modd}\ (p^N, F(x)).$$

Posons

$$V(x) \equiv S_1(x)F_1(x) \ \text{modd}\ (p^N, F(x)) \quad \text{et} \quad W(x) \equiv S_2(x)F'(x) \ \text{modd}\ (p^N, F(x))$$

où V(x) et W(x) sont des polynômes de degré strictement inférieur à celui de F(x).
Si $(v) = \{v_n\}$ et $(w) = \{w_n\}$ sont deux solutions de (1) engendrées respectivement par V(x) et W(x) alors

$$\begin{cases} U(x) \equiv V(x) + W(x) \ \text{modd}\ (p^N, F(x)) \\ (u) \equiv (v) + (w) \ \text{mod}\ p^N \end{cases}$$

où (v) mod p^N est une suite purement périodique et (w) mod p^N une suite nulle.

Pour le calcul effectif de la longueur du transitoire d'une suite nulle (w) mod m et d'une suite purement périodique (v) mod m nous renvoyons le lecteur à M. WARD (1933) et à D.E. KNUTH (1981) dans les cas suivants :

i) $m = p^N$

où p est un nombre premier et où $N > 1$ est un entier.

ii) (w) est une solution de l'équation (1) dont le polynôme associé F(x) est de la forme

$$F(x) = (G(x))^{n_1}$$

où G(x) est un polynôme unitaire irréductible sur $\mathbb{Z}_p$ et où $n_1 > 0$ est un entier.

iii) (v) est une solution de l'équation (1) dont le polynôme associé F(x) est de la forme

$$F(x) = (G'(x))^{n_2}$$

où G'(x) est un polynôme unitaire et irréductible sur $\mathbb{Z}_p$ et où n_2 est un entier strictement positif.

Nous nous proposons de présenter ici le calcul de la période d'une suite purement périodique dans le cas particulier où m est un nombre premier et où F(x) est un polynôme quelconque sur $\mathbb{Z}_p$.

I.3 CALCUL DE LA PERIODE D'UNE SUITE RECURRENTE LINEAIRE HOMOGENE SUR UN CORPS FINI

Dans ce paragraphe p désignera toujours un nombre premier. D'autre part les théorèmes et les lemmes sont dus à R. Lidl et H. Niederreiter(1983).

a) PRELIMINAIRE SUR L'ORDRE D'UN POLYNOME A COEFFICIENTS DANS UN CORPS FINI

En ce qui concerne l'ordre d'un polynôme, nous donnons quelques résultats qui seront utiles lors de la détermination de la période d'une suite récurrente linéaire. La définition de l'ordre d'un polynôme est basée sur le lemme suivant :

I.3.1. LEMME

Soit g(x) un élément de $\mathbb{Z}_p[x]$ de degré $d \geq 1$ avec $g(0) \neq 0$. Alors il existe un entier naturel non nul e avec $e < p^d$ et x^e-1 divisible par g(x) dans $\mathbb{Z}_p[x]$.

I.3.2. DEFINITION

On considère un polynôme non nul g de $\mathbb{Z}_p[x]$. Si $g(0) \neq 0$ alors le plus petit entier $e > 0$ tel que g(x) divise x^e-1 est appelé l'ordre de g qu'on notera par Ord(g). Si $g(0) = 0$ alors on écrit g(x) sous la forme

$$g(x) = x^h g'(x)$$

où h est un entier strictement positif et où le polynôme g'(x) appartenant à $\mathbb{Z}_p[x]$ vérifie $g'(0) \neq 0$. Dans ce cas l'ordre de g est par définition celui de g'.

Puisqu'on sait calculer l'ordre d'un polynôme irréductible sur un corps fini (cf. R. Lidl and H. Niederreiter(1983)) le théorème suivant nous permet de déterminer celui d'un polynôme quelconque sur un corps fini.

I.3.3. THEOREME

Soient g un polynôme sur $\mathbb{Z}_p$ de degré strictement positif et de terme constant non nul. On note par

$$g = a g_1^{n_1} \cdots g_r^{n_r}$$

la factorisation canonique de g dans $\mathbb{Z}_p[x]$ où a est un élément de $\mathbb{Z}_p$, $n_1, \ldots, n_r$ des entiers naturels non nuls et $g_1, \ldots, g_r$ k polynômes unitaires distincts deux à deux et irréductibles sur $\mathbb{Z}_p$. Alors $Ord(g) = ep^t$, où $e = PPCM(Ord(g_1), \ldots, Ord(g_r))$ et où t est le plus petit entier n non nul tel que $p^n \geq \max(n_1, \ldots, n_r)$.

b) CALCUL DE LA PERIODE D'UNE SUITE RECURRENTE LINEAIRE HOMOGENE SUR UN CORPS FINI

CONVENTION Les opérations d'addition et de multiplication sont ceux du corps fini $\mathbb{Z}_p$.

Soient k un entier strictement supérieur à 1 et $(s) = \{s_n\}$ une S.R.L.H. d'ordre k sur $\mathbb{Z}_p$ définie par la donnée des termes initiaux $s_0, s_1, \ldots, s_{k-1}$ et la relation de récurrence linéaire (en abrégé R.D.R.L)

$$(13) \qquad s_{n+k} = a_{k-1}s_{n+k-1} + \cdots + a_1 s_{n+1} + a_o s_n, \quad \forall\, n \geq 0$$

où les coefficients $a_o, a_1, \ldots, a_{k-1}$ sont dans $\mathbb{Z}_p$, avec $a_o \neq 0$. Le polynôme

$$F(x) = x^k - a_{k-1}x^{k-1} - \ldots - a_1x - a_o$$

considéré comme un polynôme sur $\mathbb{Z}_p$ est appelé **polynôme caractéristique** de la récurrence (13) ou de la S.R.L.H. $(s) = \{s_n\}$. La matrice

$$A = \begin{bmatrix} 0 & 1 & . & . & . & 0 & 0 \\ 0 & 0 & . & . & . & 0 & . \\ . & 0 & . & . & . & 0 & . \\ . & 0 & . & . & . & 0 & . \\ . & 0 & . & . & . & 1 & 0 \\ 0 & 0 & . & . & . & 0 & 1 \\ a_0 & a_1 & . & . & . & a_{k-2} & a_{k-1} \end{bmatrix}$$

est appelée **matrice compagnon** de F(x), tandis que le vecteur colonne

$$\underline{s}_n = {}^t(s_n, \cdots, s_{n+k-1}), \qquad \forall\, n \geq 0$$

est dit **nième vecteur d'état** de $(s) = \{s_n\}$.

Remarquons que $(s) = \{s_n\}$ vérifie des relations de récurrence linéaire autres que celle donnée par (13). Ainsi le théorème suivant permet d'établir une relation entre les différentes R.D.R.L. satisfaites par une S.R.L.H. fixée.

I.3.4. THEOREME

La suite $(s) = \{s_n\}$ étant définie par (13) il existe un polynôme unitaire unique m (x) de $\mathbb{Z}_p[x]$ ayant la propriété suivante :
Un polynôme unitaire $f_o(x)$ de $\mathbb{Z}_p[x]$ est un polynôme caractéristique de (s) si et seulement si m(x) divise $f_o(x)$.

I.3.5. DEFINITION

Le polynôme m(x) du théorème I.3.4. est appelé polynôme minimal de (s).

I.3.6. REMARQUE

Si (s) est une suite identiquement nulle alors m(x) est le polynôme constant 1 et, dans le reste des cas, le polynôme minimal est de degré strictement positif.

Avant d'énoncer un théorème permettant de calculer la période d'une suite (s), il est nécessaire de donner le résultat ci-après.

I.3.7. LEMME

i) Soit

$$h(x) = x^t - b_{t-1}x^{t-1} - \ldots - b_1x - b_o$$

un polynôme de degré t strictement positif sur $\mathbb{Z}_p$ tel que $b_o \neq 0$. Alors l'ordre de h(x) est égal à celui de sa matrice compagnon dans le groupe linéaire GL(t, $\mathbb{Z}_p$).

ii) On désigne par (d) = $\{d_n\}$ une S.R.L.H. sur $\mathbb{Z}_p$ de polynôme caractéristique g(x) sur $\mathbb{Z}_p$ avec

$$g(x) = x^s - c_{s-1}x^{s-1} - c_1x - c_o, \qquad c_o \neq 0 \text{ et } s > 0.$$

Alors la période de (d) divise l'ordre de la matrice compagnon de g(x) dans le groupe linéaire GL(s, $\mathbb{Z}_p$).

DEMONSTRATION

i) Notons par B la matrice compagnon de h(x) et par I la matrice identité d'ordre t sur $\mathbb{Z}_p$. Alors $B^e = I$ pour un entier $e > 1$ si et seulement si h(x) divise $x^e - 1$. D'après les définitions de h(x) et de B on a immédiatement le résultat.

ii) Si c désigne la matrice compagnon de g(x), alors on a

$$\det(c) = (-1)^{s-1}c_o \neq 0.$$

Par conséquent c est un élément de GL(s, $\mathbb{Z}_p$). Soit r son ordre. D'autre part il est facile de vérifier par induction sur n que le nième vecteur d'état de la suite (d) vérifie

$$\underline{d}_n = c^n\underline{d}_o \qquad \forall\ n \geq 0.$$

Par suite

$$\underline{d}_{n+r} = c^{n+r}\underline{d}_0$$

$$= c^n\underline{d}_0$$

$$= \underline{d}_n$$

pour tout $n \geq 0$. Donc la période de la suite (d) divise l'ordre de c.

C.Q.F.D.

I.3.8. THEOREME

La période de la suite (s) définie par (13) est égale à l'ordre de son polynôme minimal m(x). En particulier, si F(x) est irréductible sur $\mathbb{Z}_p$, cette période est égale à l'ordre de F(x).

DEMONSTRATION

Si r est la période de (s) alors on a

$$s_{n+r} = s_n, \qquad \forall\ n \geq 0.$$

Du théorème I.3.4. on déduit que m(x) divise x^r-1 et par conséquent

$$\mathrm{Ord}(m(x)) \leq r$$

Mais d'après le lemme I.3.7. r divise Ord(m(x)).
Donc

$$r = \mathrm{Ord}(m(x)).$$

Si F(x) est irréductible sur $\mathbb{Z}_p$, alors $m(x) = F(x)$ et donc $r = \mathrm{Ord}(f(x))$.

C.Q.F.D.

Comme on peut calculer l'ordre d'un polynôme sur un corps fini (cf. théorème I.3.3.), le théorème I.3.8. nous permet de déterminer la période d'une S.R.L.H. lorsqu'on connaît le polynôme minimal de celle-ci. Voici une méthode de calcul de ce polynôme. Si

$$F(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1x - a_o$$

est un polynôme caractéristique de la suite $(s) = \{s_i\}$ non nulle dont on cherche à calculer la période alors on pose

$$H(x) = \sum_{j=0}^{k-1} \sum_{i=0}^{k-1-j} (a_{i+j+1} s_i) x^j$$

avec $a_k = -1$.

Les polyômes F(x) et H(x) étant considérés comme des polynômes sur $\mathbb{Z}_p$, on note par d(x) leur PGCD. Alors le polynôme minimal m(x) est donné par

$$m(x) = F(x)/d(x).$$

Remarquons que dans les applications on préfère souvent, pour k fixé, engendrer une S.R.L.H. d'ordre k sur $\mathbb{Z}_p$ de période maximale $p^k - 1$. Pour cela on prend pour polynôme caractéristique de cette suite un polynôme primitif sur $\mathbb{Z}_p$ de degré k.
Un tel polynôme peut être obtenu soit par la mise en oeuvre d'une méthode constructive (cf. par exemple M. Ribowicz (1987)), soit par lecture sur une table (cf. par exemple R. Lidl et H. Niederreiter (1983)).

I.4. ETUDE DE LA SOMME ET DU PRODUIT DES SUITES RECURRENTES LINEAIRES HOMOGENES SUR UN CORPS FINI

Soient p un nombre premier et F(x) un polynôme sur $\mathbb{Z}_p$ de degré k strictement positif. On désigne alors par S(F(x)) l'ensemble des S.R.L.H. sur $\mathbb{Z}_p$ de polynôme caractéristique F(x).

Afin d'étudier la somme de S.R.L.H. sur $\mathbb{Z}_p$, on munit S(F(x)) d'une structure d'espace vectoriel sur $\mathbb{Z}_p$ en définissant les deux opérations suivantes : si $(t) = \{t_n\}$ et $(s) = \{s_n\}$ sont deux suites de S(F(x)) et, si c est dans $\mathbb{Z}_p$, alors on pose

$$((t) + (s)) = \{t_n + s_n\} \quad \text{et} \quad (c(s)) = \{cs_n\}.$$

Il est clair que les axiomes d'espace vectoriel sont vérifiés et, comme S(F(x)) a q^k éléments, c'est un espace vectoriel de dimension k sur $\mathbb{Z}_p$. De plus si $(s) = \{s_n\}$ est une suite de S(F(x)) alors, pour tout entier naturel b, la suite translatée $(s') = \{s_{n+b}\}$ appartient à S(F(x)). On dit que la translation de suite est une opération interne sur S(F(x)).

I.4.1.LEMME(cf. R. Lidl et H. Niederreiter(1983))

i) Soient F(x) et G(x) deux polynômes unitaires non constants sur $\mathbb{Z}_p$. Alors S(F(x)) est un sous ensemble de S(G(x)) si et seulement si F(x) divise G(x).

ii) On considère h polynômes $F_1(x), F_2(x), \ldots, F_h(x)$ unitaires et non constants sur $\mathbb{Z}_p$.

S'ils sont premiers entre eux alors

$$S(F_1(x)) \cap \cdots \cap S(F_h(x)) = \{(0)\}$$

sinon

$$S(F_1(x)) \cap \cdots \cap S(F_h(x)) = S(d(x))$$

où (0) est la suite identiquement nulle et où d(x) est le PGCD de $F_1(x), \ldots, F_h(x)$.

DEMONSTRATION

i) On suppose

$$S(F(x)) \subset S(G(x)).$$

Si k est le degré de F(x), on note par $(d) = \{d_n\}$ la suite de S(F(x)) telle que

$$d_o = d_1 = \ldots = d_{k-2} = 0 \quad \text{et} \quad d_{k-1} = 1.$$

Alors, d'après R. Lidl and H. Niederreiter(1983), chapitre 8, corollaire 8.52, F(x) est le polynôme minimal de (d). Comme (d) appartient à S(G(x)), son polynôme minimal F(x) divise G(x). Réciproquement, si F(x) divise G(x) et si (s) est un élément de S(F(x)), alors le polynôme minimal m(x) de cette suite divise F(x).Par conséquent m(x) divise G(x) et une application du théorème I.3.4. montre que (s) appartient à S(G(x)). Donc S(F(x)) est un sous ensemble de S(G(x)).

ii) Le polynôme minimal m(x) d'un élément de l'intersection des $S(F_i(x))$, (i = 1, 2, ..., h), divise chacun des polynômes $F_1(x), \ldots, F_h(x)$. Si ces polynômes sont premiers entre eux, alors m(x) est égal au polynôme constant 1, si bien que l'intersection des $S(F_i(x))$, (i = 1, 2, ... , h), est réduite à (0). En revanche, s'il ne sont pas premiers entre eux alors m(x) divise d(x) et une nouvelle application du théorème I.3.4. montre que l'intersection des $S(F_i(x))$, (i = 1, 2, ... , h), est incluse dans S(d(x)). Mais d'après i) S(d(x)) est un sous ensemble de cette intersection. Donc

$$S(F_1(x)) \cap \cdots \cap S(F_h(x)) = S(d(x)).$$

C.Q.F.D.

On désigne par S(F(x)) + S(G(x)) l'ensemble des suites de la forme ((s) + (t)) où (s) et (t) appartiennent respectivement à S(F(x)) et à S(G(x)). Cette définition pouvant être étendue de façon naturelle à h ensembles $S(F_i(x))$, i = 1, 2,..., h, on a le théorème suivant.

I.4.2. THEOREME(cf. R. Lidl et H. Niederreiter(1983))

Soient $F_1(x)$, ... , $F_h(x)$ des polynômes unitaires et non constants sur $\mathbb{Z}_p$. Alors

$$S(F_1(x)) + \cdots + S(F_h(x)) = S(C(x))$$

où

$$C(x) = \text{PPCM } (F_1(x), F_2(x), \cdots, F_h(x)).$$

DEMONSTRATION

Il suffit de faire la démonstration pour $h = 2$, puisque le cas général s'obtient aisément par induction sur h. Notons d'abord que, d'après le lemme I.4.1. i), tout élément de $S(F_1(x))$ ou de $S(F_2(x))$ appartient à $S(c(x))$ et comme l'ensemble $S(c(x))$ est un espace vectoriel, il contient $S(F_1(x)) + S(F_2(x))$. Comparons maintenant les dimensions sur $\mathbb{Z}_p$ des espaces vectoriels $S(F_1(x)) + S(F_2(x))$ et $S(c(x))$. Si on pose

$$V_1 = S(F_1(x)), \quad V_2 = S(F_2(x)) \quad \text{et} \quad d(x) = \text{PGCD } (F_1(x), F_2(x))$$

alors

$$\dim (V_1 + V_2) = \dim(V_1) + \dim(V_2) - \dim(V_1 \cap V_2)$$

$$= \deg(F_1(x)) + \deg(F_2(x)) - \deg d(x)).$$

Mais

$$c(x) = F_1(x)\, F_2(x) / d(x).$$

Donc

$$\dim (V_1 + V_2) = \deg(c(x)) = \dim(S(c(x))).$$

Finalement

$$S(F_1(x)) + S(F_2(x)) = S(c(x)).$$

C.Q.F.D.

Le théorème I.4.2. assure non seulement que la somme de deux ou plusieurs S.R.L.H. est une S.R.L.H., mais nous donne aussi le polynôme caractéristique de la suite résultante. Dans certains cas particuliers, il est possible de calculer directement le polynôme minimal et la période de la somme de suites à partir des informations correspondantes sur celles-ci.

I.4.3. THEOREME(cf. R. Lidl et H. Niederreiter(1983))

Pour un entier $h > 1$ et pour $i = 1, 2, \ldots, h$, on désigne par (t_i) une S.R.L.H. sur $\mathbb{Z}_p$ de polynôme minimal $m_i(x)$ sur $\mathbb{Z}_p$ et de période r_i. On suppose que les polynômes $m_i(x)$, $1 \leq i \leq h$, sont deux à deux premiers entre eux. Alors le polynôme minimal et la période de la somme $((t_1) + (t_2) + \ldots + (t_h))$ sont respectivement égaux à $m_1(x) \ldots m_h(x)$ et à PPCM $(r_1, r_2, \ldots, r_h)$.

DEMONSTRATION

Il suffit de faire la démonstration pour $h = 2$ et le cas général se déduira par simple induction sur h.Soient donc $(t) = \{t_n\}$ et $(s) = \{s_n\}$ deux S.R.L.H. sur $\mathbb{Z}_p$.
On commence par montrer que le polynôme minimal de la somme $((t) + (s))$ vaut $m_1(x)m_2(x)$.
Si $m_1(x)$ ou $m_2(x)$ est le polynôme constant 1 alors le résultat est trivial. De même si le polynôme minimal $m(x)$ sur $\mathbb{Z}_p$ de $((t) + (s))$ est égal à 1 alors le théorème est trivial.
On suppose donc que les polynômes $m_1(x)$, $m_2(x)$ et $m(x)$ sont de degré strictement positif. D'après le théorème I.4.2. on a

$$S(m_1(x) + m_2(x)) = S(m_1(x)\, m_2(x)).$$

Par conséquent, $((t) + (s))$ est un élément de $S(m_1(x)\, m_2(x))$. Ce qui entraîne que $m(x)$ divise $m_1(x)\, m_2(x)$. Si

$$m(x) = x^k - a_{k-1}x^{k-1} - a_1x - a_o$$

alors

$$s_{n+k} + t_{n+k} = a_{k-1}(s_{n+k-1} + t_{n+k-1}) + \cdots + a_o(s_{n+k} + t_{n+k}), \qquad \forall\, n \geq 0.$$

Soit $(u) = \{u_n\}$ la suite définie par

$$u_n = s_{n+k} - a_{k-1}s_{n+k-1} - \cdots - a_o s_n$$

$$= -t_{n+k} + a_{k-1}t_{n+k-1} + \cdots + a_o t_n$$

pour tout $n \geq 0$.
Puisque $S(m_1(x))$ et $S(m_2(x))$ sont des espaces vectoriels sur $\mathbb{Z}_p$ invariants par l'opération de translation de leurs éléments, la suite $(u) = \{u_n\}$ appartient à l'intersection de $S(m_1(x))$ et de $S(m_2(x))$ et d'après le lemme I.4.1. ii), (u) est une suite identiquement nulle. Il vient alors que $m_1(x)$ et $m_2(x)$ divisent $m(x)$ et par suite $m_1(x)\, m_2(x)$ divise $m(x)$. D'où $m(x) = m_1(x)\, m_2(x)$.

Il nous reste à montrer que la période r de $((t) + (s))$ est égale à $PPCM(r_1, r_2)$.
Mais d'après i) et le théorème I.3.8., on a

$$r = Ord(m_1(x)m_2(x))$$

et une application du théorème I.3.3. donne

$$r = PPCM\,(Ord(m_1(x)), Ord(m_2(x))).$$

Soit $r = PPCM(r_1, r_2)$.

C.Q.F.D.

Nous nous intéressons maintenant au produit de S.R.L.H. sur $\mathbb{Z}_p$.
Soient $(s) = \{s_n\}$ et $(t) = \{t_n\}$ deux suites sur $\mathbb{Z}_p$. Le produit de (s) par (t) est défini par

$$((s)\,(t)) = \{s_n t_n\}.$$

On définit de façon analogue le produit d'un nombre fini de suites sur $\mathbb{Z}_p$.

D'autre part, si S dénote l'espace vectoriel de toutes les suites sur $\mathbb{Z}_p$ muni de l'addition usuelle et de la multiplication par un scalaire, alors pour h polynômes $F_1(x)$, $F_2(x)$, ..., $F_h(x)$ sur $\mathbb{Z}_p$, unitaires et non constants, on désigne par $S(F_1(x)) \dots S(F_h(x))$ le sous espace de S engendré par tous les produits $(v_1) \dots (v_h)$ avec (v_i) appartenant à $S(F_i(x))$, $1 \leq i \leq h$, et par $F_1(x) \nabla \cdots \nabla F_h(x)$ le polynôme unitaire dont les racines sont les différents éléments de la forme $a_1 \dots a_h$ où a_i, $1 \leq i \leq h$, est une racine de $F_i(x)$ dans le corps de décomposition de $F_1(x) \dots F_h(x)$ sur $\mathbb{Z}_p$. Comme les conjugués sur $\mathbb{Z}_p$ des produits $a_1 \dots a_h$ sont des éléments de cette forme, $F_1(x) \nabla \cdots \nabla F_h(x)$ est un polynôme sur $\mathbb{Z}_p$.

I.4.4. THEOREME (cf. par exemple R. Lidl et H.Niederreiter (1983))

Pour un entier $h > 1$ et pour $i = 1, 2, \dots, h$, on se donne un polynôme $F_i(x)$, unitaire et non constant sur $\mathbb{Z}_p$. De plus, on suppose que, pour tout i, $1 \leq i \leq h$, toutes les racines de $F_i(x)$ dans le corps de décomposition de $F_i(x)$ sont simples. Alors

$$S(F_1(x)) \dots S(F_h(x)) = S(F_1(x) \nabla \cdots \nabla F_h(x))$$

Du théorème I.4.4. on déduit, comme on l'avait fait pour la somme de S.R.L.H., que le produit de S.R.L.H. sur $\mathbb{Z}_p$ est également une S.R.L.H. sur $\mathbb{Z}_p$. Concernant la période du produit de suites sur $\mathbb{Z}_p$ on a le résultat classique suivant :

I.4.5. THEOREME

Pour un entier $h > 1$ et pour tout $i = 1, 2, \dots, h$, soit (t_i) une suite non identiquement nulle sur $\mathbb{Z}_p$, fondamentalement périodique et de période r_i. Si $r_1, \dots, r_h$ sont premiers entre eux alors le produit $((t_1) \dots (t_h))$ est de période $r_1 \dots r_h$.

II. ETUDE STATISTIQUE DES N.P.A. ENGENDRES PAR UNE CONGRUENCE LINEAIRE MULTIDIMENSIONNELLE ET CHOIX DES PARAMETRES DE CELLE-CI

II.1. PRESENTATION DE QUELQUES METHODES DE TRANSFORMATION D'UNE SUITE ENGENDREE PAR UNE CONGRUENCE LINEAIRE MULTIDIMENSIONNELLE EN UNE SUITE DE NOMBRES PSEUDO-ALEATOIRES

Dans cette partie nous présentons deux méthodes de transformation d'une suite congruentielle linéaire en une suite de N.P.A. de distribution uniforme sur [0, 1] . Il est utile de préciser que le fait de se limiter à la génération de N.P.A. équidistribués sur [0, 1] n'est pas une perte de généralité, puisque des transformations convenables de N.P.A. équirépartis sur [0, 1] permettent d'obtenir les approximations des autres lois de probabilité.

Soient p un nombre premier, k un entier strictement supérieur à 1 et $(s) = \{s_n\}$ une suite sur $\mathbb{Z}_p$ déterminée par la donnée des termes initiaux $s_o, s_1, \ldots, s_{k-1}$ supposés non tous nuls et la congruence linéaire

$$(14) \qquad s_{i+k} \equiv a_{k-1}s_{i+k-1} + \cdots + a_1 s_{i+1} + a_o s_i \bmod p, \quad \forall\, i \geq 0$$

où le polynôme caractéristique associé

$$F(x) = x^k - a_{k-1}x^{k-1} - \cdots - a_1 x - a_o$$

est un polynôme primitif sur $\mathbb{Z}_p$.

Il y a deux types de méthodes couramment utilisées pour la construction d'une suite de N.P.A. à partir de $(s) = \{s_n\}$: la méthode de normalisation et les méthodes digitales.

a) METHODE DE NORMALISATION

On prend pour valeur de p, un nombre premier assez grand (par exemple $p = 2^{31}-1$) et la suite désirée $(u) = \{u_i\}$ est définie par

$$(15) \qquad u_i = s_i / p, \qquad i \geq 0.$$

b) METHODES DIGITALES

Soient p, un petit nombre premier (p = 2 dans le cas usuel) et L un entier vérifiant $2 \leq L \leq k$.
Dans la méthode digitale due à R.C. Tausworthe (1965), la suite $(s) = \{s_i\}$ est découpée en blocs disjoints de longueur L et les éléments de chacun d'eux sont interprétés comme étant les digits du développement dans la base p d'un réel appartenant à [0, 1]. En d'autres termes, la suite $(u) = \{u_i\}$ obtenue en posant

$$(16) \qquad u_i = \sum_{j=1}^{L} s_{Li+j-1} p^{-j}, \quad \forall\ i \geq 0$$

est une approximation de la loi uniforme sur [0, 1].
Une deuxième méthode digitale, proposée par T.G. Lewis et W.H. Payne (1973) et appelée régistre à décalage généralisé (en abrégé R.D.G.) est en un certain sens plus performante que la première : L entiers naturels distincts $K_1, \ldots, K_L$ étant choisis, la suite de N.P.A. $(u) = \{u_i\}$ est alors définie par

$$(17) \qquad u_i = \sum_{j=1}^{L} s_{i+K_j} p^{-j}, \quad \forall\ i \geq 0.$$

La période τ de la suite $(u) = \{u_i\}$ obtenue par la méthode de normalisation ou par la méthode de T.G. Lewis et W.H. Payne est $p^k - 1$, tandis que celle de la suite (u) provenant de la méthode de R.C. Tausworthe est $(p^k - 1) / PGCD(L, p^k - 1)$.

II.2. ETUDE STATISTIQUE DES N.P.A. ET CHOIX DES PARAMETRES D'UNE CONGRUENCE LINEAIRE MULTIDIMENSIONNELLE

Soient s et N deux entiers tels que $s > 0$ et $1 \leq N \leq \tau$. Notons alors par $D_N^{(s)}$ la discrépance (on pourra se reporter au paragraphe II.2. du chapitre I pour la définition de la discrépance) des vecteurs

$$(18) \qquad \underline{u}_i = (u_i, \ldots, u_{i+s-1}), \qquad 0 \leq i < \tau$$

où la suite $(u) = \{u_i\}$ est donnée par l'une des relations (15), (16) et (17).

L'étude détaillée des estimations de $D_N^{(s)}$ a été faite par H. Niederreiter (1982, 1986a, 1986b, 1987a, 1988c). On déduit de ces estimations des critères de choix

des paramètres $a_o, a_1, \ldots, a_{k-1}$ pour que la suite de nombres pseudo-aléatoires $(u) = \{u_i\}$ passe le test d'uniformité et le test sériel. Après avoir énoncé celles-ci nous présentons ces critères en considérant séparément les méthodes de normalisation, de R.C. Tausworthe et de T.G. Lewis et W.H. Payne.

a) DISCREPANCE, TEST DES TREILLIS ET CHOIX DE PARAMETRES POUR LA METHODE DE NORMALISATION

Soit $c_p^{(s)}$ l'ensemble des points non nuls $\underline{h}$ de $\mathbb{Z}^s$ tels que

$$\underline{h} = (h_1, \ldots, h_s), \quad -p/2 < h_j \leq p/2 \qquad \text{pour } j = 1, 2, \ldots, s.$$

Pour tout $\underline{h} = (h_1, \cdots, h_s)$ de $c_p^{(s)}$ on pose

$$r(\underline{h}) = \prod_{i=1}^{s} \max(1, |h_i|)$$

et

$$g(\underline{h}) = h_1 + h_2 x + \cdots + h_s x^{s-1}, \quad \forall\, s > 0$$

où $g(\underline{h})$ est considéré comme un polynôme sur $\mathbb{Z}_p$.

Alors pour $s > k$ la quantité $\rho^{(s)}(F, p, 1)$, appelée **figure de mérite** en dimension s, est définie par

$$\rho^{(s)}(F, p, 1) = \min r(2\underline{h})$$

où le minimum est étendu à tous les points $\underline{h}$ de $c_p^{(s)}$ tels que F divise $g(\underline{h})$.

Ces notations et définitions étant ainsi précisées, nous considérons le choix de $a_o, a_1, \ldots, a_{k-1}$ respectivement pour $s \leq k$ et $s > k$.
Pour $s \leq k$ on a (cf. H. Niederreiter (1982))

$$(19) \qquad D_N^{(s)} < s/p + cp^{k/2}(\log p)^s \log\tau/N, \quad 1 \leq N < \tau$$

et

$$(20) \qquad D_\tau^{(s)} \leq s/p + c(\log p)^s/\tau$$

où c est une constante strictement positive.

Il vient alors que, pour N suffisamment grand (par exemple $N > p^{k/2+e}$ pour tout $e > 0$), la séquence $(u_i,\ 0 \leq i < N)$ est une approximation satisfaisante de la loi uniforme sur [0, 1] et pour $s \geq 2$, s termes successifs de $(u_i,\ 0 \leq i < N + s-2)$ peuvent être considérés comme étant statistiquement indépendants. On remarquera que l'estimation de $D_N^{(s)}$, $1 \leq N \leq \tau$, donnée par (19) et (20) ne fait pas intervenir la spécificité du polynôme primitif F utilisé, ce qui n'est pas le cas pour s strictement supérieur à k.

En effet pour $s > k$ on a (cf. H. Niederreiter(1982))

$$(21) \qquad D_N^{(s)} \leq s/p + cp^{k/2}(\log p)^s \log\tau/N + c_s(\log p)^s/\rho^{(s)}(F,p,1)\ ,\quad 1 \leq N < \tau$$

et

$$(22) \qquad D_\tau^{(s)} \leq s/p + c(\log p)^s/\tau + c_s(\log p)^s/\rho^{(s)}(F,p,1)$$

où $c > 0$ est une constante absolue et où $c_s > 0$ est une constante ne dépendant que de s.

Cette fois-ci, pour que la suite (u) passe le test sériel en dimension s pour N raisonnablement grand, on doit choisir F de telle sorte que la valeur de la figure de mérite soit suffisamment élevée. Théoriquement un tel polynôme existe (cf. H.Niederreiter (1982)). De plus si on considère l' indépendance statistique de s termes successifs de la suite (u), il est possible de choisir, entre deux polynômes primitifs F_1 et F_2, celui qui nous donne le plus de satisfaction, c'est-à-dire, celui dont la figure de mérite est la plus grande. Mais à notre connaissance, il n'y a pas d' algorithme permettant d' évaluer la figure de mérite et un calcul direct risque d' être très coûteux même pour de petites valeurs de s.

Aussi pour avoir plus d' informations sur les qualités de la suite (u), introduit-on le test des treillis. Comme nous le soulignions lors de l'étude des congruences linéaires simples, ce test conduit aux mêmes conclusions lorsqu'il est appliqué à (s) au lieu de la suite de N.P.A. (u), où (s) est la suite donnée par la relation (14).

Soient $n \geq 2$ un entier et $\underline{y}_i$, $1 \leq i \leq \tau$, les vecteurs colonnes définis par

$$(23) \qquad \underline{y}_i = {}^t(\underline{s}_i,\ \underline{s}_{i+1}, \cdots, \underline{s}_{i+n-1}),\quad \underline{s}_i = (s_i, \cdots, s_{i+k-1})\ ,\qquad 1 \leq i \leq \tau.$$

Le test des treillis concerne l'étude la distribution des vecteurs (23) dans un espace de dimension kn, ce qui revient à étudier l'indépendance statistique de n termes successifs de la suite $(\underline{s}) = \{\underline{s}_i\}$.

II.2.1. THEOREME (cf. L. Afferbach et H. Grothe (1988))

En adoptant les mêmes notations que ci-dessus on pose :

$$V_{kn} = \{\underline{y}_i : i = 1, 2, ..., p^k - 1\} \cup \{\underline{0}\}.$$

où $\underline{0}$ est le vecteur nul de $\mathbb{Z}_p^{kn}$.
Alors l'ensemble

$$G_{kn} = V_{kn} + p\mathbb{Z}^{kn} = \{\underline{y} = \underline{v} + p\underline{z} : \underline{v} \in V_{kn},\ \underline{z} \in \mathbb{Z}^{kn}\}$$

est un treillis (cf. chapitre I paragraphe II.1. pour la définition de treillis).

Pour réaliser ce test, on cherche d'abord une base du treillis G_{kn}, puis on la réduit. Rappelons qu'il y a plusieurs conceptions de base réduite (cf. L. Afflerbach et H. Grothe (1985), B. Vallée (1986) et le chapitre I) et qu'en un sens large, réduire une base B d'un treillis G consiste à la transformer en une autre base B' de G de telle sorte que les vecteurs qui composent B' soient "assez courts" et "assez orthogonaux". Une fois la base réduite trouvée, on calcule le quotient q_{kn} de Beyer, c'est-à-dire, le quotient de la norme euclidienne du vecteur le plus long de la base réduite par celle du vecteur le plus court de cette même base. La suite (23) a un bon treillis en dimension kn si q_{kn} est proche de 1.

Comme choix d'une base de G_{kn}, on peut prendre les kn vecteurs colonnes de la matrice

$$C = \begin{bmatrix} I & 0 & 0 & . & . & . & 0 & 0 \\ A & pI & 0 & 0 & 0 & 0 & 0 & 0 \\ . & 0 & . & 0 & 0 & 0 & 0 & 0 \\ . & 0 & . & . & 0 & 0 & 0 & 0 \\ . & 0 & . & . & . & 0 & 0 & 0 \\ A^{n-3} & 0 & . & . & . & pI & 0 & 0 \\ A^{n-2} & 0 & . & . & . & 0 & pI & 0 \\ A^{n-1} & 0 & . & . & . & 0 & 0 & pI \end{bmatrix}$$

composée de n^2 sous matrices carrées où I est la matrice identité d'ordre k, pI la matrice diagonale d'ordre k dont les éléments diagonaux sont égaux à p et où A est la matrice compagnon du polynôme F associé à la congruence (14).

Ainsi la structure de treillis de G_{kn} décrite par la matrice C nous donne des renseignements aussi bien sur la distribution des vecteurs (23) que sur l'indépendance statistique de n termes consécutifs de la suite $(\underline{s}) = \{\underline{s}_i\}$.

D'autre part, si au lieu de considérer la distribution des vecteurs $\underline{y}$ à kn composantes, on s' intéressait à celle des vecteurs dont les t composantes ($t < kn$, $n \geq 1$) sont les termes successifs de la suite $(s) = \{s_i\}$, alors il suffit de supprimer les kn - t dernières composantes de chacun des vecteurs $\underline{y}_i$ et de prendre pour base du nouveau treillis les vecteurs colonnes de la matrice C' obtenue en éliminant les kn -t dernières lignes et kn - t dernières colonnes de la matrice C.

On va utiliser maintenant le test des treillis pour choisir les coefficients $a_o, \ldots, a_{k-1}$ du polynôme primitif F associé à (14).

D'après L. Afflerbach et H. Grothe (1988), la suite $(\underline{s})$ n'a pas en général un bon treillis pour les dimensions $t > k$ si les coefficients $a_o, a_1, \ldots, a_{k-1}$ de F ne sont pas à la fois distincts deux à deux et différents de 0 et de 1. Notons cependant qu'on peut utiliser un tel polynôme pour construire une suite de vecteurs Pseudo-aléatoires ayant un bon treillis.

Plus précisément pour un polynôme primitif F de degré $k > 1$ sur $\mathbb{Z}_p$ et pour un choix convenable d'une matrice T carrée d'ordre k sur $\mathbb{Z}_p$ et dont le déterminant est premier avec p, on génère la suite de vecteurs sur $\mathbb{Z}_p$

$$(24) \qquad \underline{w}_i \equiv D\underline{w}_{i-1} \mod p, \quad \forall\, i \geq 1$$

où $\underline{w}_0$ est un vecteur colonne non nul de $\mathbb{Z}_p^k$ donné, D la matrice

$$D = T\,A\,T^{-1}$$

et A la matrice compagnon de F. Dans la congruence (24), l'opération " mod p " signifie que les calculs sont faits composante par composante sur le corps fini $\mathbb{Z}_p$. Il est clair que la suite de vecteurs donnée par (24) est de période p^k-1. Pour un entier n strictement positif, on pose

$$(25) \qquad \underline{y}_i = ({}^t\underline{w}_i, {}^t\underline{w}_{i+1}, \cdots, {}^t\underline{w}_{i+n-1}), \qquad \forall\ i \geq 1.$$

Alors on peut étudier comme précédemment la structure du treillis G'_t (t = 2, 3, ... , kn - 1, kn, (n + 1)k, ...) correspondant à la suite donnée par (25).

L' exemple suivant, emprunté à L . Afferbach et H.Grothe (1988), illustre les deux affirmations suivantes :

i) Une récurrence linéaire sur un corps fini, d'ordre k > 1 et de période maximale, n'a pas en général un bon treillis en dimension t > k si ses coefficients ne sont pas à la fois distincts deux à deux et différents de 0 et de 1.

ii) Partant d'une récurrence linéaire vérifiant i), on peut construire un générateur matriciel de la forme (24) ayant de meilleurs treillis en dimension t > k.

II.2.2. EXEMPLE

$$k = 3, \quad p = 2^{29} - 3 = 536\,870\,909, \qquad F(x) = x^3 - x^2 - x - 532\,130\,240.$$

$$T = \begin{bmatrix} 235\,510\,801 & 429\,634\,356 & 238\,525\,549 \\ 281\,043\,327 & 398\,307\,193 & 492\,485\,298 \\ 291\,922\,635 & 190\,076\,583 & 473\,675\,892 \end{bmatrix}$$

ce qui donne

$$D = \begin{bmatrix} 32\,009\,361 & 506\,208\,029 & 281\,476\,751 \\ 97\,715\,140 & 195\,637\,636 & 201\,812\,864 \\ 101\,381\,044 & 9\,996\,681 & 309\,223\,913 \end{bmatrix}$$

TABLEAU DES QUOTIENTS DE BEYER q_t (t = 4, ... , 12) *respectivement pour la congruence linéaire multidimensionnel (C.L.M .) de polynôme caractéristique* F(x) *et pour le générateur matriciel (G. M.) donné par* (24).

t	q_t (C.L.M.)	q_t (G.M.)
4	0.00007877662	0.80625067302
5	0.00012007194	0.79937518567
6	0.81716409968	0.66288265589
7	0.02069423220	0.59003430569
8	0.04492271680	0.32444075067
9	0.26940729225	0.15555969981
10	0.32089716206	0.57714708974
11	0.47053245267	0.62415024982
12	0.73707340274	0.69937487241

Pour $t \leq 3$, on a $q_t = 1$ quel que soit le générateur utilisé. Dans le cas d'une C.L.M., la suite n'a pas un bon treillis pour t = 4, 5, 7 et 8. Tous les quotients de Beyer du générateur matriciel sont supérieurs à 0.5 sauf pour t = 8 et 9.

La procédure de génération des N.P.A. à l'aide d'une congruence linéaire simple est plus rapide que la méthode de normalisation. Mais pour un choix convenable des coefficients $a_0, a_1, ..., a_{k-1}$ du polynôme primitif, cette dernière a l'avantage de produire des vecteurs de N.P.A. répartis de façon satisfaisante dans les espaces de dimension t, avec $2 \leq t \leq k$ et même pour certaines valeurs de t strictement supérieures à k. D'autre part, ces deux méthodes utilisent comme modulo un grand nombre premier p et ceci pose un problème lors de leur implantation sur des micro-ordinateurs pour lesquels la longueur du mot mémoire est très modeste. C'est l'une des raisons pour lesquelles on s'est intéressé aux méthodes digitales qui n'emploient que de petits nombres premiers.

b) DISCREPANCE ET CHOIX DES PARAMETRES POUR LES METHODES DIGITALES

b.1. méthode de R.C. TAUSWORTHE

Soient β une racine du polynôme primitif F dans l'extension $\mathbb{F}_{p^k}$ de $\mathbb{F}_p$ et s un entier naturel non nul. Pour $s > k/L$, on désigne par E l'ensemble des s-uplets d'entiers $(d_1, ..., d_s)$ de composantes non toutes nulles vérifiant les deux conditions suivantes :

i) $0 \leq d_i \leq L$, pour $1 \leq i \leq s$
ii) Le système $\{ \beta^{L(i-1)+j-1} : 1 \leq j \leq d_i, \ 1 \leq i \leq s \}$ est linéairement dépendant sur $\mathbb{F}_p$.

Alors la quantité $\rho_1^{(s)}(F, p, L)$, appelée *figure de mérite de* F *en dimension* s pour la méthode de R. C. Tausworthe, est définie par

$$\rho_1 = \rho_1^{(s)}(F, p, L) = \min\left\{ \sum_{i=1}^{s} d_i : (d_1, ..., d_s) \in E \right\}$$

si E est non vide et par

$$\rho_1 = \rho_1^{(s)}(F, p, L) = k+1$$

si le système décrit en ii) est linéairement indépendant sur $\mathbb{F}_p$.

Notons enfin par B_N la quantité

$$B_N = \frac{p^{k/2}}{N} - \frac{1}{1 + p^{k/2}}, \quad \text{si } N = \tau$$

et

$$B_N = \frac{p^{k/2}(\frac{2\log\tau}{p} + \frac{2}{5})}{N} + \frac{p^{k/2}}{\tau} - \frac{1}{1 + p^{k/2}}, \quad \text{si } 1 \le N < \tau.$$

Nous considérons à présent le choix des paramètres $a_o, \ldots, a_{k-1}$ à partir de l'estimation de la discrépance $D_N^{(s)}$ respectivement pour $s \le k/L$ et $s > k/L$.

Pour $s \le k/L$ on a (cf. H. Niederreiter(1982-1983))

$$D_N^{(s)} < s/p^L + c_s B_N L^s (\log p)^s \qquad 1 \le N \le \tau$$

où c_s est une constante strictement positive ne dépendant que de s.

Ce résultat montre que pour N suffisamment grand, la méthode de R.C. Tausworthe produit une suite de N.P.A. passant le test sériel en dimension s, avec $2 \le s \le k/L$. Nous constatons, comme dans le cas de la méthode de normalisation, que l'estimation de $D_N^{(s)}$ en petite dimension ne fait pas apparaître la spécificité du polynôme primitif F.

Pour $s > k/L$ on a (cf. H. Niederreiter((1982-1983), 1986b, 1987a))

$$D_N^{(s)} < s/p^L + c_s B_N L^s (\log p)^s + c_{p,s} L^s p^{-\rho_1} \qquad 1 \le N \le \tau$$

où la constante $c_s > 0$ ne dépend que de s et où $c_{p,s} > 0$ est une constante qui dépend à la fois de p et de s.

Il vient alors que si l'on cherche à générer des N.P.A. statistiquement indépendants, il est préférable d'utiliser un polynôme primitif F qui nous donne une figure de mérite ρ_1 suffisamment grande. Mais est - il - possible de calculer $\rho_1(F, p, L)$ pour un polynôme F fixé ? Ou bien peut - on construire un polynôme primitif F avec une valeur satisfaisante de $\rho_1(F, p, L)$?

Avant d'essayer de répondre à ces questions, il convient de noter que dans le cas où $\mathrm{PGCD}(\tau, L) = 1$ et $s \le k/L$, il a été établi dans H. Niederreiter (1986b) que

$$(26) \qquad D_\tau^{(s)} = 1 - (1 - p^{-L})^s.$$

Par conséquent l'ordre de grandeur de $D_\tau^{(s)}$ est, à un facteur multiplicatif près, égal à p^{-L}. Précisons que p^{-L} est interprété comme étant l'erreur de discrétisation due au fait que tous les N.P.A., obtenus par la méthode de R.C. Tausworthe, sont des fractions rationnelles de dénominateur p^L. Pour minimiser cette erreur, on prend la plus grande valeur possible de L, soit $L = k$.

Dans le cas $L = k$, $s = 2$ est la plus petite valeur de s pour laquelle la formule (26) n'est pas satisfaite et on a (cf. H. Niederreiter(1986b et 1987a))

$$(1/2 - 1/2p)p^{-r} \leq D_\tau^{(s)} \leq 1/\tau + ((p-1)r/2 + 3/2)p^{k-r}/\tau$$

où

$$r = \rho_1^{(2)}(F, p, L) - 1.$$

Ainsi pour savoir si la suite de N.P.A. passe le test sériel en dimension 2, on est amené à donner une solution à l'un des problèmes posés précédemment dans le cas particulier $s = 2$

Pour cela on considère le développement en fraction continue simple de $F(x) / x^k$

$$F(x) / x^k = [1, A_2, ..., A_h]$$

où A_i est un polynôme sur $\mathbb{F}_p$ avec $\deg(A_i) \geq 1$ pour $1 \leq i \leq h$. Si la quantité L(F) est définie par

$$L(F) = \max \{ \deg (A_i), \quad 1 \leq i \leq h\},$$

alors la formule

$$\rho_1^{(2)}(F, p, k) = k + 2 - L(F)$$

démontrée dans H. Niederreiter (1986b) suggère de choisir F avec L(F) petit si l'on désire avoir de grandes valeurs pour $\rho_1^{(2)}$ (F, p, k).

Nous présentons maintenant une méthode de G.L. Mullen et H. Niederreiter (1987) permettant de rechercher des polynômes primitifs F qui, utilisée dans le procédé de génération de R.C.Tausworthe, nous permettent d'engendrer une suite de N.P.A. $(u) = \{u_n\}$ telle que u_n et u_{n+1} $(n = 0, 1, 2, ...)$ soient statistiquement indépendants.

b.1.1. Généralités sur le calcul des polynômes caractéristiques optimaux

L'algorithme qu'on va décrire sort à chacune de ses exécutions un polynôme primitif M sur $\mathbb{F}_2$ dont le degré d et la figure de mérite $\rho_1^{(2)}(M, 2, d)$ sont fixés à l'avance. Un tel polynôme est dit optimal si $\rho_1^{(2)}(M, 2, d)$ est assez grand, ce qui correspond à une petite valeur de L(M). Rappelons que ces polynômes optimaux ne sont appropriés à la méthode de génération de R.C. Tausworthe que dans le cas L = d et p = 2.

On montre (cf. Niederreiter (1987b)) que, pour tout entier strictement positif d il existe un polynôme unique M_d sur $\mathbb{F}_2$ tel que $M_d(0) \neq 0$ et $L(M_d) = 1$. Ce polynôme, appelé polynôme de Fibonacci, est donné par

$$M_d(x) = \sum_{j=0}^{c+1} x^{d - \lfloor (d/2^j) \rfloor}$$

où c est l'entier déterminé par $2^c \leq d \leq 2^{c+1}$ et où $\lfloor t \rfloor$ désigne le plus grand entier inférieur ou égal au réel t.

Ainsi, pour chercher un polynôme primitif (en abrégé P.P.) M sur $\mathbb{F}_2$ de degré d et avec L(M) = 1, il suffit de tester la primitivité de M_d. Voici deux P.P. de Fibonacci sur $\mathbb{F}_2$ de degrés respectifs 42 et 54.

$$F_{42}(x) = x^{42} + x^{41} + x^{40} + x^{37} + x^{32} + x^{21} + 1$$

$$F_{54}(x) = x^{54} + x^{53} + x^{51} + x^{48} + x^{41} + x^{27} + 1$$

Les P.P. de Fibonacci étant rares, ceci découle des calculs effectués dans G. L. Mullen and H. Niederreiter (1987) d'où on a tiré les deux exemples précédents, il est naturel de s'intéresser aux P.P. M avec L(M)>1.

La méthode de construction que nous allons présenter est basée sur les résultats particuliers suivants, résultats dont la généralisation est exposée dans H. Niederreiter(1987b).

II.2.3. LEMME

Soient $A_1, A_2, \ldots, A_h$, h polynômes sur $\mathbb{F}_2$ avec $\deg(A_i) \geq 1$, $1 \leq i \leq h$ et

$$[1, A_1, \ldots, A_h] = M(x) / x^d.$$

On pose

$$B_i = A_i \text{ pour } 1 \leq i < h,\ B_h = B_{h+1} = A_h + 1 \text{ et } B_{h+i} = A_{h+1-i},\ 1 \leq i \leq h.$$

Alors

$$[1, B_1, \ldots, B_{2h}] = (x^d M(x) + 1) / x^{2d}.$$

II.2.4. LEMME

On considère les polynômes $A_1, A_2, \ldots, A_h$ et B de $\mathbb{F}_2[x]$ avec $\deg(A_i) \geq 1$, $1 \leq i \leq h$, $\deg(B) \geq 1$ et

$$[1, A_1, \ldots, A_h] = M(x) / x^d$$

Si on pose

$$B_i = A_i,\ 1 \leq i \leq h,\ B_{h+1} = B \text{ et } B_{h+1+i} = A_{h+1-i},\ 1 \leq i \leq h$$

alors

$$[1, B_1, \ldots, B_{2h+1}] = (BM(x)x^d + 1) / Bx^{2d}.$$

Afin d'appliquer ces deux lemmes on se donne :

i) Un entier $d > 1$

ii) Un entier v avec $2 \leq v \leq d$

iii) Un polynôme M sur $\mathbb{F}_2$ tel que $\deg(M) = d$, $M(0) \neq 0$ et $L(M) = v$.

Ainsi, au vu du lemme II.2.3., le polynôme $G(x) = M(x)x^d + 1$ est de degré $2d$ et satisfait $G(0) \neq 0$ et $L(G) = v$. D'autre part, si dans le lemme II.2.4. le polynôme B est égal à x où à x^2, alors $G(x) = BM(x)x^d + 1$ est de degré $2d + 1$ ou $2d + 2$ et on a $G(0) \neq 0$ et $L(G) = v$. Il vient alors que pour la donnée d'un polynôme $M(x)$ sur $\mathbb{F}_2$ avec $\deg(M) = d$, $M(0) \neq 0$ et $L(M) = v$, on peut construire trois autres polynômes G_1, G_2 et G_3 sur $\mathbb{F}_2$ de degrés respectifs $2d$, $2d + 1$ et $2d + 2$ tels que $L(G_i) = v$ pour $i = 1, 2, 3$.

Avant de présenter la méthode proprement dite, on a besoin d'une définition et d'une remarque.

On désigne par chaîne de degrés de bout initial $d_1 > 0$ et de bout terminal d_n, la séquence de degrés $d_1 \rightarrow d_2 \rightarrow \cdots \rightarrow d_n$ où d_i est un élément de $\{ 2d_{i-1}, 2d_{i-1}+1, 2d_{i-1}+2\}$.

II.2.5 REMARQUE

Si on construit à partir des lemmes II.2.3. et II.2.4. une série de polynômes $G_1, \ldots, G_n$ de degrés respectifs $d_1, d_2, \ldots, d_n$ avec $M = G_1$ et $L(G_1) = v$ alors $L(G_i) = v$, $1 \leq i \leq n$.

b.1.2. description de l'algorithme de calcul d'un polynôme primitif Q de degré d tel que $L(Q) = v$

Données : deux entiers d et v, $2 \leq v \leq d$.

i) On applique l'algorithme d'Euclide aux polynômes de $\mathbb{F}_2[x]$ de bas degré afin d'obtenir les polynômes initiaux M tels que $M(0) \neq 0$ et $L(M) = v$. On sait que de tels polynômes existent (cf. H. Niederreiter (1987b)).

ii) On construit une chaîne de degrés $d_1 \rightarrow d_2 \rightarrow \cdots \rightarrow d_n = d$ telle que d_1 soit le dégré de l'un des polynômes initiaux calculés en i). Soit donc G_1 un polynôme initial de degré d_1. Partant de $M = G_1$, on met en oeuvre les lemmes II.2.3. et II.2.4. autant de fois qu'il est nécessaire pour trouver un polynôme G_n de degré d tel que $L(G_n) = v$. Si G_n est un polynôme primitif alors $Q = G_n$ et l'algorithme s'arrête. Si G_n n'est pas primitif , alors on teste les polynômes initiaux restants qui ont pour degré d_1 et, si aucun de ces polynômes ne donne un polynôme final G_n primitif, on utilise les polynômes initiaux de degré d_2. Si à nouveau on n'obtenait pas un polynôme final G_n primitif, on répète le processus avec les polynômes initiaux de degré $d_3, d_4, \ldots$.

II.2.6. REMARQUE.

Au lieu de continuer la recherche du polynôme primitif G_n à partir des polynômes initiaux de degré élevé, il est parfois plus efficace, dans le cas où il existe plusieurs chaînes de degrés se terminant par d, de changer de chaîne de degrés et de débuter la recherche de G_n avec des polynômes initiaux de degré bas.

Voici trois exemples de polynômes primitifs G_1, G_2, G_3 sur $\mathbb{F}_2$ de degrés respectifs 55, 59 et 64 avec $L(G_1) = L(G_2) = L(G_3) = 2$. Ils sont empruntés à G. L. Mullen and H. Niederreiter (1987).

$$G_1(x) = x^{55} + x^{53} + x^{50} + x^{49} + x^{42} + x^{28} + 1$$

$$G_2(x) = x^{59} + x^{58} + x^{57} + x^{53} + x^{45} + x^{30} + 1$$

$$G_3(x) = x^{64} + x^{63} + x^{60} + x^{59} + x^{58} + x^{54} + x^{49} + x^{32} + 1$$

c) DISCREPANCE ET CHOIX DE PARAMETRE POUR LA METHODE DE T.G. LEWIS ET W.H. PAYNE

Soient β une racine de l'extension $\mathbb{F}_{p^k}$ de $\mathbb{F}_p$, s un entier naturel non nul et $\underline{K}$ le vecteur $(K_1, K_2, \dots, K_L)$. Pour un entier s strictement supérieur à 1, on désigne par E l'ensemble des s-uplets $(d_1, d_2, \dots, d_s)$ de composantes non toutes nulles telles que

i) $0 \le d_i \le L$, $1 \le i \le s$

ii) Le système $\left\{\beta^{K_j + i - 1},\ 1 \le i \le s,\ 1 \le j \le d_i\right\}$ est linéairement dépendant sur $\mathbb{F}_p$.

Alors la quantité $\rho_2^{(s)}(F, p, \underline{K})$, appelé **figure de mérite en dimension s pour la méthode de T.G. Lewis et W.H. Payne**, est définie par

$$\rho_2 = \rho_2^{(s)}(F, p, \underline{K}) = \min\left\{\sum_{i=1}^{s} d_i :\ (d_1, \cdots, d_s) \in E\right\}$$

si E est non vide et par

$$\rho_2 = \rho_2^{(s)}(F, p, \underline{K}) = \infty$$

si le système décrit en ii) est linéairement indépendant sur $\mathbb{F}_p$.

Par ailleurs on pose

$$B_N = 1/\tau \quad \text{si } N = \tau$$

et

$$B_N = p^{k/2}((2\log\tau) + 2/5)/N + 1/\tau,\ 1 \le N < \tau$$

Partant de ces notations et définitions, nous nous intéressons maintenant au choix des paramètres $a_o, a_1, \dots, a_{k-1}$ sur la base de l'estimation de $D_N^{(s)}$, $1 \le N \le \tau$.

⊗ Pour $N = \tau$ et $\rho_2 = \infty$ on a

$$D_N^{(s)} = 1 - (1-p^{-L})^s$$

⊗ Pour $1 \leq N < \tau$ on a

$$D_N^{(s)} < s/p^L + c_s B_N L^s (\log p)^s + c_s' L^s p^{-\rho_2} \qquad \text{pour } s>1.$$

où les constantes $c_s > 0$ et $c_s' > 0$ ne dépendent que de s.

REMARQUE.
$\rho_2 = \infty$ n'est possible que dans le cas $s \leq k/L$.

Ainsi au vu de ces estimations , et pour N assez grand , s termes successifs de N.P.A. engendrés par un régistre à décalage généralisé sont considérés comme indépendants dès qu'on a choisi les paramètres $a_o, \ldots, a_{k-1}$ de telle sorte que la figure de mérite ρ_2 soit suffisamment élevée. Contrairement à la méthode de R.C. Tausworthe, il n'y a pas à notre connaissance un algorithme de calcul de ρ_2.

CHAPITRE 3

PERIODE D'UN GENERATEUR VECTORIEL BASE SUR LE MODELE DE D. E. DAYKIN ET UNE CONGRUENCE LINEAIRE MULTIDIMENSIONNELLE DE PERIODE MAXIMALE . APERCU SUR LES GENERATEURS NON LINEAIRES DE NOMBRES PSEUDO - ALEATOIRES

I. GENERATION DES VECTEURS PSEUDO-ALEATOIRES

I.1. INTRODUCTION.

Soient k un entier strictement supérieur à 1 et $(u) = \{u_i\}$ une suite de N.P.A. de loi uniforme sur [0, 1]. Une méthode standard de génération de vecteurs pseudo-aléatoires équirépartis sur $[0, 1]^k$ consiste à prendre les k-uplets

$$\underline{u}_i = (u_i, \ldots, u_{i+k-1}), \quad i \geq 0$$

dont les coordonnées sont constituées par les termes successifs de la suite $(u) = \{u_i\}$. Mais certains auteurs se sont intéressés à des méthodes directes de génération de points pseudo-aléatoires équidistribués sur $[0,1]^k$.

Ainsi Tahmi El Hadj (1982) a étudié, pour un entier $m \geq 2$, les longueurs du transitoire et de cycle de la suite $(\underline{x}) = \{\underline{x}_i\}$ dont les termes, appartenant à $\mathbb{Z}_m^k$, sont définis par la donnée du terme initial $\underline{x}_o$, d'une matrice carrée A d'ordre k sur $\mathbb{Z}_m$, d'un vecteur $\underline{b}$ de $\mathbb{Z}_m^k$ et de la congruence

$$\underline{x}_{i+1} \equiv A\underline{x}_i + \underline{b} \mod m, \quad \forall\ i \geq 0.$$

La suite normalisée $(\underline{u}) = \{\underline{x}_i / m\}$ est alors considérée comme une approximation de l'équidistribution sur $[0, 1]^k$.

H. Niederreiter (1986c), utilisant l'arithmétique sur les corps finis, a construit, pour un nombre premier p quelconque mais assez grand, une suite de vecteurs pseudo-aléatoires $(\underline{u}) = \{\underline{u}_i\}$ de période $p^k - 1$, de loi uniforme sur $[0, 1]^k$ et telle que

$$\underline{u}_i = \left(\frac{u_i^{(1)}}{p}, \cdots, \frac{u_i^{(k)}}{p}\right), \qquad i \geq 0$$

où les coordonnées $u_i^{(j)}$, $1 \leq j \leq k$, peuvent être calculées à l'aide d'une congruence linéaire multidimensionnelle.

Pour un nombre premier p et pour un entier s, $s > 1$, J. Eichenauer-Herrmann, H. Grothe et J. Lehn (1989) se sont intéressés au choix de la matrice carrée A d'ordre k sur $\mathbb{Z}_p$, telle que la suite $(\underline{x}) = \{\underline{x}_i\}$ sur $\mathbb{Z}_p^k$, définie par la donnée de $\underline{x}_o$ non nul et la relation

$$\underline{x}_{i+1} \equiv A\underline{x}_i \mod p^s, \quad i \geq 0,$$

soit de période $(p^k-1)p^{s-1}$. Comme dans le cas de Thami el Hadj on obtient une suite de vecteurs pseudo-aléatoires sur $[0, 1]^k$ par normalisation des termes de la suite $(\underline{x}) = \{\underline{x}_i\}$.

Nous considérons pour un nombre premier p quelconque, mais assez grand, le modèle de D.E. Daykin (1963) donné par

$$\underline{x}_{i+1} \equiv B\underline{x}_i + \underline{w}_i \mod p, \quad \forall\ i \geq 1$$

où B est une matrice carrée d'ordre k, $k > 1$, sur $\mathbb{Z}_p$, $\underline{x}_i$ un élément de $\mathbb{Z}_p^k$ et où $(\underline{w}) = \{\underline{w}_i, i \geq 1\}$ est une suite de vecteurs de $\mathbb{Z}_p^k$. Partant d'une congruence linéaire multidimensionnelle de période maximale, nous choisissons la suite $(\underline{w}) = \{\underline{w}_i, i \geq 1\}$ et la matrice B de telle sorte que la suite $(\underline{x}) = \{\underline{x}_i, i \geq 1\}$ soit purement périodique de période $p(p^k - 1)$, pour tout choix du vecteur initial $\underline{x}_1$.

Dans toute la suite de cette partie, p désignera un nombre premier et k un entier strictement supérieur à 1. Les opérations d'addition et de multiplication sur les éléments de $\mathbb{Z}_p^k$ se font composante par composante suivant celles de $\mathbb{Z}_p$.

I.2 . GENERALITES SUR LE CALCUL DE LA PERIODE D'UNE SUITE VECTORIELLE ENGENDREE PAR LE MODELE DE D.E. DAYKIN

Soient B une matrice carrée d'ordre k sur $\mathbb{Z}_p$ et $(\underline{w}) = \{\underline{w}_i, i \geq 1\}$ une suite de vecteurs colonnes sur $\mathbb{Z}_p^k$. On considère alors la suite $(\underline{x}) = \{\underline{x}_i, i \geq 1\}$ de vecteurs colonnes de $\mathbb{Z}_p^k$ définie par la donnée de $\underline{x}_1$ et la récurrence

$$(1) \qquad \underline{x}_{i+1} = B\underline{x}_i + \underline{w}_i, \qquad \forall\, i \geq 1.$$

On fait l'hypothèse que $(\underline{w})$ est une suite purement périodique de période w, soit

$$\underline{w}_{i+w} = \underline{w}_i, \quad \forall\ i \geq 1.$$

Il est alors clair que $(\underline{x})$ est une suite fondamentalement périodique, c'est-à-dire, qu' il existe deux entiers $c > 0$ et $t \geq 0$ tels que

$$(2) \qquad \underline{x}_{i+c} = \underline{x}_i\,, \quad \forall\, i > t.$$

Soit c_o le plus petit entier c vérifiant (2) . On dit que c_o est la *longueur de cycle* ou *période* de la suite $(\underline{x}) = \{\underline{x}_i, i \geq 1\}$, tandis que la *longueur du transitoire* t_o de cette suite est définie comme étant le minimum des entiers $t \geq 0$ pour lesquels on a

$$\underline{x}_{i+c_o} = \underline{x}_i\,, \quad \forall\, i > t.$$

On pose

$$(3) \qquad \underline{E}_r = \sum_{i=1}^{r} B^{r-i}\underline{w}_i.$$

Alors de l'équation (1) on déduit

$$(4) \qquad \underline{x}_{i+1} = B^i \underline{x}_1 + \underline{E}_i \ , \ \forall \ i \geq 1.$$

I.2.1. THEOREME(D. E. Daykin(1963))

La période de toute suite $(\underline{x}) = \{\underline{x}_i, i \geq 1\}$ vérifiant (1) est divisible par w.

DEMONSTRATION

Etant donné un vecteur $\underline{x}_1$ de dimension k sur $\mathbb{Z}_p$, on note respectivement par c_o et t_o les longueurs de cycle et du transitoire de $(\underline{x})$. Alors on a :

$$\underline{x}_{n+c_o+1} - \underline{x}_{n+1} = 0 \ , \quad \forall \ n > t_o.$$

Mais

$$\underline{x}_{n+c_o+1} - \underline{x}_{n+1} = B(\underline{x}_{n+c_o} - \underline{x}_n) + (\underline{w}_{n+c_o} - \underline{w}_n) , \qquad \forall \ n > t_o.$$

Donc

$$\underline{w}_{n+c_o} - \underline{w}_n = 0 , \qquad \forall \ n > t_o.$$

Par conséquent c_o est divisible par w.

C.Q. F. D.

I.2.2. THEOREME(cf. D. E. Daykin(1963))

i) Toute suite $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$ satisfaisant (1) est purement périodique si et seulement si B est inversible dans $GL(k, \mathbb{Z}_p)$ (B est inversible dans le groupe $GL(k, \mathbb{Z}_p)$ si son déterminant est premier avec p).

ii) Si B est inversible et si z désigne le PPCM de w et de l'ordre b de la matrice B dans le groupe linéaire GL (k, $\mathbb{Z}_p$), alors le PPCM d de toutes les longueurs de cycle des suites $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$ vérifiant (1) est égal à z ou à pz suivant que $\underline{E}_z$ est un vecteur nul ou non nul.

DEMONSTRATION

i)

Condition nécessaire

On suppose que toute suite $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$ solution de (1) est purement périodique. Alors

$$\underline{x}_{d+1} = B^d \underline{x}_1 + \underline{E}_d = \underline{x}_1, \quad \forall \ \underline{x}_1 \in \mathbb{Z}_p^k.$$

En particulier pour $\underline{x}_1 = \underline{0}$, on a

$$\underline{E}_d = \underline{0}.$$

Donc

$$B^d = I$$

où I est la matrice identité d'ordre k sur $\mathbb{Z}_p$. Par conséquent la matrice B est inversible et son ordre b dans le groupe linéaire GL (k, $\mathbb{Z}_p$) divise d.

Condition suffisante.

On fait l'hypothèse que B est inversible dans $GL(k, \mathbb{Z}_p)$. Puisque z est le PPCM de b et de w, on a

$$\underline{E}_{tz} = t\underline{E}_z$$

pour tout entier $t \geq 1$. Par conséquent

$$(5) \qquad \underline{x}_{tz+1} = \underline{x}_1 + t\underline{E}_z \ , \forall \ \underline{x}_1 \in \mathbb{Z}_p^k \text{ et } t \geq 1 .$$

En particulier, pour $t = p$, on a

$$p\underline{E}_z = \underline{0}$$

et

$$\underline{x}_{pz+1} = \underline{x}_1 \ , \forall \ \underline{x}_1 \in \mathbb{Z}_p^k \ .$$

Donc d divise pz et toute suite $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$ vérifiant (1) est purement périodique.

ii)

On suppose que B est inversible dans $GL(k, \mathbb{Z}_p)$. Alors d'après i) toute suite $(\underline{x})$ vérifiant (1) est purement périodique et d'après la démonstration de la condition nécessaire de i) b divise d. Mais, au vu du théorème I.2.1., w divise également d. Donc z divise d.

(*) Si $\underline{E}_z = \underline{0}$, alors (5) implique

$$\underline{x}_{z+1} = \underline{x}_1 \ , \ \forall \ \underline{x}_1 \in \mathbb{Z}_p^k .$$

Et on en déduit que d divise z et est donc égal à z.

(* *) Si en revanche on a $\underline{E}_z \neq 0$, alors $\underline{x}_{z+1} \neq \underline{x}_1$ et par conséquent d ne divise pas z. Mais d divise pz, donc $d = pz$.

C.Q.F.D.

On énonce maintenant un résultat pouvant servir de base au calcul de la période d'une suite purement périodique vérifiant (1).

I.2.3. THEOREME.(D. E. Daykin(1963))

Si la suite $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$, solution de (1), est purement périodique, alors sa période est le plus petit multiple μw de w tel que

$$(6) \qquad \sum_{i=0}^{\mu-1} B^{iw}\underline{v} = \underline{0}$$

où

$$(7) \qquad \underline{v} = (B^w - I)\,\underline{x}_1 + \underline{E}_w .$$

DEMONSTRATION

Comme w divise la période de $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$, celle- ci est le plus petit multiple μw de w tel que

$$\underline{x}_{\mu w+1} - \underline{x}_1 = \underline{0}.$$

Mais

$$\underline{x}_{\mu w+1} - \underline{x}_1 = (B^{\mu w} - I)\underline{x}_1 + \underline{E}_{\mu w}$$

$$= (B^{\mu w} - I)\underline{x}_1 + \sum_{j=0}^{\mu - 1} B^{jw}\underline{E}_w$$

$$= (\sum_{j=0}^{\mu - 1} B^{jw})((B^w - I)\underline{x}_1 + \underline{E}_w)$$

Donc

$$\sum_{j=0}^{\mu - 1} B^{jw}\underline{v} = \underline{0}$$

C.Q.F.D.

I.2.4. COROLLAIRE

Si B est une matrice inversible d'ordre b dans le groupe $GL(k, \mathbb{Z}_p)$ avec b divisant w, alors toute suite $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$ vérifiant (1) est purement périodique de période w ou pw suivant que $\underline{E}_w$ est un vecteur nul ou non nul.

DEMONSTRATION

Comme B est inversible, toute suite $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$ solution de (1) est purement périodique. Par hypothèse l'ordre b de B divise w. Donc le vecteur $\underline{v}$ du théorème

I.2.3. est indépendant du terme initial $\underline{x}_1$ et par conséquent toutes les suites satisfaisant (1) ont même période. D'après les théorèmes I.2.1. et I.2.2., on a le résultat.

C.Q.F.D.

I.3. PERIODE D'UN GENERATEUR VECTORIEL BASE SUR LE MODELE DE D. E. DAYKIN ET UNE CONGRUENCE LINEAIRE MULTIDIMENSIONNELLE DE PERIODE MAXIMALE

Soient $(s) = \{s_n\}$, la suite sur $\mathbb{Z}_p$ donnée par la relation (14) du chapitre II et $(\underline{s}) = \{\underline{s}_n\}$ la suite des nièmes vecteurs d'état de (s), c'est - à- dire,

$$\underline{s}_n = {}^t(s_n, \ldots, s_{n+k-1}), \qquad n = 0, 1, 2, \ldots$$

On sait alors que

$$\underline{s}_n = A^n \underline{s}_o, \qquad n = 0, 1, 2, \ldots$$

où A est la matrice compagnon du polynôme caractéristique F(x) associé à la relation (14) du chapitre II. On pose

$$(8) \qquad \underline{w}_n = \underline{s}_n, \qquad n = 1, 2, \ldots .$$

Comme la suite $(\underline{s}) = \{\underline{s}_n\}$ est purement périodique de période p^k-1, il en est de même pour la suite $(\underline{w}) = \{\underline{w}_i, i \geq 1\}$.

I.3.1. THEOREME

La suite $(\underline{w}) = \{\underline{w}_i, i \geq 1\}$ étant donnée par (8), nous considèrons la suite de vecteurs $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$ définie par (1), c'est -à -dire,

$$\underline{x}_{n+1} = B\underline{x}_n + \underline{w}_n, \quad n \geq 1$$

et nous supposons que $B = A$. Alors la suite $(\underline{x})$ est purement périodique de période $p(p^k-1)$, pour tout choix du vecteur initial $\underline{x}_1$.

DEMONSTRATION

On a bien sûr

$$\underline{w}_n = A^n \underline{s}_0, \quad n \geq 1.$$

L'ordre de la matrice A dans GL (k, $\mathbb{Z}_p$) est égal à l'ordre de son polynôme caractéristique F(x) (cf. chapitre II, lemme I.3.7.), c'est -à-dire, la quantité p^k-1 qui est aussi la période w de $(\underline{w}) = \{\underline{w}_n , n \geq 1\}$. D'après le corollaire I.2.4., il suffit de montrer que les composantes du vecteur $\underline{E}_w$ sont non toutes nulles dans $\mathbb{Z}_p$.

Mais

$$\underline{E}_w = \sum_{i=1}^{w} A^{w-i}\underline{w}_i = \sum_{i=1}^{w} A^{w-i}A^i\underline{s}_o = w\underline{s}_o.$$

On en déduit que $\underline{E}_w$ est non nul , puisque $\underline{s}_o$ est un vecteur non nul et p premier avec $p^k - 1$.

C.Q.F.D.

I.3.2. REMARQUES

i) Si le terme initial $\underline{x}_1$ de la suite $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$ définie par le théorème I.3.1. est $\underline{s}_o$, alors on a

$$\underline{x}_{n+1} = (n+1)\underline{w}_n, \quad \text{pour tout } n \geq 1.$$

ii) Le théorème I.3.1. reste vrai pour k = 1, si B est une racine primitive modulo p et si on pose

$$s_{n+1} \equiv Bs_n \bmod p, \quad \forall\, n \geq 0$$

où s_o est un élément non nul de $\mathbb{Z}_p$. De plus si le terme initial x_1 est égal à s_o, on a comme dans le cas particulier i)

$$x_{n+1} = (n+1)\, w_n, \quad n \geq 1.$$

Pour p assez grand, la suite normalisée $(\underline{u}) = \{\underline{x}_n/p, n \geq 1\}$, où $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$ est donnée par le théorème I.3.1., peut être considérée comme une suite de vecteurs pseudo-aléatoires sur $[0, 1]^k$ ayant pour période $p(p^k-1)$. Comme la suite $(\underline{x}) = \{\underline{x}_n, n \geq 1\}$ est basée sur la suite $(\underline{w}) = \{\underline{w}_i, i \geq 1\}$ qui a de bonnes propriétés statistiques (cela découle de l'étude réalisée au chapitre II, paragraphe II), on peut espérer qu'il en sera de même pour la suite de vecteurs pseudo-aléatoires $(\underline{u}) = \{\underline{x}_n/p, n \geq 1\}$.

II PRESENTATION DE QUELQUES GENERATEURS NON LINEAIRES DE NOMBRES PSEUDO-ALEATOIRES ET TESTS DE QUALITE

Au chapitre I nous avons vu que la suite de nombres pseudo-aléatoires $(u) = \{x_i/p\}$, où $(x) = \{x_i\}$ est définie par la donnée d'un élément x_o de $\mathbb{Z}_p$ et la relation

$$(10) \qquad x_{i+1} \equiv ax_i + b \bmod p, \qquad i \geq 0$$

a de bonnes propriétés statistiques si l'on choisit convenablement les paramètres a, b et p. Mais la linéarité de la récurrence (10) fait que pour $n \geq 2$, les vecteurs de nombres pseudo-aléatoires $\underline{u}_i$ $(i = 0, 1, 2, \ldots)$

$$\underline{u}_i = (x_i/p, x_{i+1}/p, \ldots, x_{i+n-1}/p), \qquad i \geq 0$$

ont certaines régularités de distribution dans l'espace $[0, 1]^n$, régularités indésirables pour la plupart des simulations de Monte - Carlo. En particulier, la suite $(\underline{u}) = \{\underline{u}_i\}$ ne passe pas le test des treillis de G. Marsaglia (cf. G. Marsaglia (1972)) et les termes de cette suite sont situés sur des hyperplans parallèles relativement nombreux appartenant au cube unité $[0, 1]^n$.

Ainsi dans cette partie, nous nous proposons de faire une présentation de quelques générateurs non linéaires de N.P.A. suivie du test de G. Marsaglia et du test sériel des suites produites par certains de ces générateurs.

II.1. DESCRIPTION DE QUELQUES GENERATEURS NON LINEAIRES DE NOMBRES PSEUDO-ALEATOIRES

a) Générateurs de la forme

$x_{n+1} \equiv f(x_n) \mod p.$

La suite $(x) = \{x_n\}$ sur $\mathbb{Z}_p$ provenant du générateur introduit par J. Eichenauer, H. Grothe et J. Lehn (1988) est définie par la donnée d'un élément x_o de $\mathbb{Z}_p$ et la récurrence

$$(11) \qquad x_{n+1} \equiv f(x_n) \mod p, \qquad \forall\, n \geq 0$$

où $p \geq 5$ est un nombre premier assez grand et où la fonction non linéaire f, définie sur $\mathbb{Z}_p$ et à valeurs dans $\mathbb{Z}$, est choisie de telle sorte que la suite $(x) = \{x_n\}$ soit purement périodique de période maximale p.

Voici un exemple d'un tel générateur dû à J. Eichenauer et J. Lehn(1986).
Pour un élément non nul c de $\mathbb{Z}_p$, on note par c^{-1} l'inverse de c pour l'opération de multiplication dans $\mathbb{Z}_p$ et par convention on pose $0^{-1} = 0$. Si deux éléments a et b de $\mathbb{Z}_p$, avec $ab \neq 0$, sont choisis de manière que $x^2 - bx - a$ soit un polynôme primitif sur $\mathbb{Z}_p$, alors la suite

$$(12) \qquad x_{n+1} \equiv a x_n^{-1} + b \mod p, \qquad n \geq 0$$

est purement périodique de période p.

b) Générateurs de la forme

$x_{n+1} \equiv f(x_n) \mod 2^t$.

Soient t , $t \geq 1$, un entier et $q = 2^t$. On note par G_q l'ensemble des entiers impairs c avec $1 \leq c < q$ et par c^{-1} l'inverse de l'élément c de G_q pour l'opération de multiplication modulo q sur G_q. Alors la suite non linéaire $(x) = \{x_n\}$ sur G_q est définie par

(13) $$x_{n+1} \equiv f(x_n) \mod q, \quad \forall\, n \geq 0$$

où x_o est un élément donné de G_q et où la fonction non linéaire f est choisie de telle sorte que la suite (x) soit purement périodique de période q/2. Comme exemple d'un générateur ayant la forme (13), on peut citer celui de J. Eichenauer, J. Lehn et A. Topuzoglu (1988) où la suite $(x) = \{x_n\}$ est donnée par

(14) $$x_{n+1} \equiv a x_n^{-1} + b \mod q, \quad \forall\, n \geq 0$$

avec $a \equiv 1 \mod 4$, $b \equiv 2 \mod 4$ et $x_0 \equiv 1 \mod 2$.

c) Générateur non linéaire basé sur une congruence linéaire multidimensionnelle

Nous nous intéressons maintenant à un générateur non linéaire introduit par J. Eichenauer, H. Grothe, J. Lehn et A. Topuzoglu (1987) et construit à partir d'une suite récurrente linéaire homogène d'ordre k sur $\mathbb{F}_p$, pour $k > 1$.

Soient p un nombre premier assez grand et $r \geq 1$ un entier. Si la suite $(y) = \{y_n\}$ définie par

$$(15) \qquad y_{n+1} \equiv a_0 y_n + a_1 y_{n-1} + \cdots + a_r y_{n-r} \mod p, \qquad n \geq r$$

où $y_o, \ldots, y_r$ et $a_o, \ldots, a_r$ sont des éléments de $\mathbb{F}_p$ donnés avec $a_r \neq 0$ et $(y_o, \ldots, y_r) \neq (0, \ldots, 0)$, alors le générateur non linéaire est défini par

$$(16) \qquad x_n \equiv y_{N(n)+1} y_{N(n)}^{-1} \mod p, \qquad \forall\, n \geq 0$$

où N est une fonction définie sur l'ensemble des entiers par

$$(17) \qquad \begin{cases} N(0) = \min \{k \geq 0 : y_k \geq 1\} \\ N(n) = \min \{k \geq N(n-1) : y_k \geq 1\}, \ \forall\, n \geq 1 \end{cases}$$

et où pour tout c dans $\mathbb{F}_p$, c^{-1} est l'inverse de c pour l'opération de multiplication sur $\mathbb{F}_p$.

Avant d'énoncer un théorème sur le calcul de la période de $(x) = \{x_n\}$, il est nécessaire de faire certaines hypothèses sur le polynôme caractéristique h(x) associé à (15) :

$$h(x) = x^{r+1} - a_o x^r - \ldots - a_{r-1} x - a_r.$$

On suppose donc qu'on a les deux conditions suivantes :

(18) h(x) est un polynôme irréductible sur $\mathbb{F}_p$.

(19) Toute racine β de h(x) dans $\mathbb{F}_{p^{r+1}}$ est telle que

$$\begin{cases} \beta^k \neq \mu, \ \forall\, \mu \in \mathbb{F}_p, \ 1 \leq k < s \\ \beta^s = \mu, \quad \text{pour un } \mu \in \mathbb{F}_p \end{cases}$$

où $s = p^r + p^{r-1} + \ldots + p + 1$.

Remarquons que pour r fixé, $r \geq 1$ il existe au moins $(p - 1)\phi(p^r + p^{r-1} + ... + 1)/r$ polynômes unitaires sur $\mathbb{F}_p$ vérifiant (18) et (19), étant entendu que ϕ désigne la fonction D'Euler.

II.1.1. THEOREME (cf. J. Eichenauer, H. Grothe, J. Lehn et A. Topuzoglu (1987))

On suppose que le polynôme caractéristique h(x) associé à (15) vérifie les conditions (18) et (19). Alors la suite non linéaire $(x) = \{x_n\}$ donnée par (16) est purement périodique de période p^r, pour tout choix du vecteur initial $(y_0, y_1, ..., y_r)$. De plus, chacun des $(p-1)^r$ r- uplets $(z_1, ..., z_r)$, $1 \leq z_1, ..., z_r < p$, apparaît une et une seule fois dans un cycle.

II.1.2. REMARQUE

Dans chacun des cas a), b) et c), on obtient une suite de nombres pseudo-aléatoires sur [0, 1] en posant $(u) = \{x_n/m\}$, où m est le modulo de la congruence utilisée pour la génération de la suite $(x) = \{x_n\}$.

II.2. TEST DES TREILLIS DE G. MARSAGLIA ET TEST SERIEL

a) Test des treillis

En ce qui concerne le test des treillis de G. Marsaglia, nous présentons un développement théorique effectué par J. Eichenauer, H. Grothe et J. Lehn (1988) et H. Niederreiter (1988a, 1988b).

a.1. Préliminaires.

Nous précisons ici un certain nombre de notations, définitions et propriétés nécessaires à cette présentation.

Soit $(y) = \{y_n\}$ une suite sur un corps K. On définit l'opérateur Δ^k sur cette suite par

$$\Delta^0 y_n = y_n, \quad \Delta^k y_n = \Delta^{k-1} y_{n+1} - \Delta^{k-1} y_n, \qquad \forall\, k \geq 1$$

et on vérifie par induction sur k qu'on a la propriété suivante.

II.2.1. PROPRIETE

$$(20) \qquad \Delta^k y_n = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} y_{n+j}.$$

$$(21) \qquad \Delta^k h(n) = 0, \quad \text{pour } h \in K[x] \text{ et } \deg(h) < k.$$

II.2.2 DEFINITION

Si les termes de la suite $(\Delta y) = \{\Delta^1 y_n\}$ sont égaux à une constante, alors la suite $(y) = \{y_n\}$ est dite additive.

Pour un nombre premier p et un entier d, $d \geq 2$, donnés, considérons une suite $(x) = \{x_n\}$ sur $\mathbb{F}_p$ purement périodique et de période p et posons

$$\underline{x}_i^{(d)} = (x_i, \ldots, x_{i+d-1}), \quad i \geq 0$$

et

$$\underline{w}_i^{(d)} \equiv {}^t\underline{x}_i^{(d)} - {}^t\underline{x}_o^{(d)} \mod p, \quad i \geq 0.$$

Alors l'ensemble

$$V^d = \left\{ \underline{v} \in \mathbb{F}_p^d : \underline{v} \equiv \sum_{i=1}^{p-1} z_i \underline{w}_i^{(d)} \mod p, \ (z_1, \cdots, z_{p-1}) \in \mathbb{F}_p^{p-1} \right\}$$

déterminé à partir des d-vecteurs $\underline{w}_i^{(d)}$ de $\mathbb{F}_p^d$, est appelé le **d-treillis du générateur G** de la suite $(x) = \{x_n\}$. D'autre part si la suite de vecteurs $\underline{u}_i$ est définie par

$$(22) \qquad \underline{u}_i = {}^t(0,\ x_{i+1} - x_i, \cdots, x_{i+p-1} - x_i) \mod p\,, \quad \forall\, i \geq 0$$

alors la d x p matrice

$$G^{(d)} = (\underline{w}_o^{(d)}, \cdots, \underline{w}_{p-1}^{(d)})$$

ayant pour vecteurs lignes ${}^t\underline{u}_0, \ldots, {}^t\underline{u}_{d-1}$ et pour vecteurs colonnes $\underline{w}_o^{(d)}, \cdots, \underline{w}_{p-1}^{(d)}$ est appelée la **d-matrice du générateur G** et son rang est noté $rg\,(G^{(d)})$.

II.2.2. DEFINITION

On dira que le générateur G passe le test des treillis de G. Marsaglia si V^d est identique à $\mathbb{F}_p^d$ et il ne le passe pas si V^d est un sous-treillis strict de $\mathbb{F}_p^d$.

Puisque les colonnes de $G^{(d)}$ engendrent le treillis V^d on a le lemme suivant.

II.2.3 LEMME(cf. J. Eichenauer, H. Grothe et J. Lehn(1988))

Le générateur G passe le test des treillis de G. Marsaglia pour une dimension d , $d \geq 2$, si et seulement si $rg\,(G^{(d)}) = d$.

a.2. *Aspect théorique du test des treillis des générateurs* (11) et (12)

Une suite $(x) = \{x_n\}$ déterminée par (11) étant purement périodique de période p on a

$$x_{n+p} = x_n, \quad n \geq 0.$$

Ainsi cette suite peut être considérée comme une suite récurrente linéaire sur $\mathbb{F}_p$ de polynôme caractéristique $x^p - 1 = (x - 1)^p$. Le polynôme minimal est donc de la forme $(x - 1)^t$ avec $1 \leq t \leq p$. Mais, d'après la formule générale des termes d'une suite récurrente linéaire (cf.R. Lidl et H. Niederreiter (1986), p. 210), on a

$$(23) \qquad x_n = \sum_{j=0}^{s} \binom{n+j}{j} a_j = g(n), \qquad n \geq 0$$

où $s = t-1$, a_j un élément de $\mathbb{F}_p$ et g un polynôme sur $\mathbb{F}_p$ avec $\deg(g) \leq s$. En fait, si on utilise les relations (20) et (21), on constate que $\deg(g) = s$.

Terminons l'introduction de ce paragraphe en remarquant que g est un polynôme de permutation sur $\mathbb{F}_p$, puisque $\{g(0), \ldots, g(p-1)\} = \mathbb{F}_p$, et donc l'entier s est non nul.

II.2.3. LEMME (cf. H. Niederreiter(1988a))

On a toujours $1 \leq s \leq p-2$ et si $s > 1$ alors s ne divise pas p-1. De plus, on a, dans le cas non additif, $s \geq 3$.

DEMONSTRATION

Il est clair que s vérifie $1 \leq s \leq p-1$. Mais pour $s > 1$, s ne divise pas (p-1) (cf. R. Lidl et H. Niederreiter (1983), corollaire 7.5). Dans le cas non additif, s ne peut pas être égal à 1, car sinon on aurait d'après (23)

$$x_n = a_o + (n+1)\, a_1$$

et

$$\Delta^1 x_n = a_1, \qquad \forall\, n \geq 0.$$

Ce qui contredirait le fait que s est non additif. Comme s ne divise pas p-1,

on a $s \geq 3$.

C.Q.F.D.

II.2.4. LEMME (cf. H. Niederreiter(1988a))

La suite de vecteurs $(\underline{u}) = \{\underline{u}_i\}$ étant donnée par la relation (22) on a

$$\sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} \underline{u}_{k+j} = \underline{0} \quad ,\forall\, k \geq 0.$$

DEMONSTRATION

Pour tout $h \geq 0$, on a d'après (20), (21) et (23)

$$\sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} (x_{k+j+h} - x_{k+j}) = \sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} \sum_{n=k}^{k+h-1} \Delta^1 x_{n+j}$$

$$= \sum_{n=k}^{k+h-1} \Delta^s \Delta^1 (x_n) = \sum_{n=k}^{k+h-1} \Delta^{s+1} (x_n) = 0$$

pour tout $k \geq 0$.

C.Q.F.D.

Le théorème suivant nous permet de faire le test des treillis de G. Marsaglia pour le générateur de la forme (11) et pour tout d, $d \geq 2$, dès que la valeur de s est connue.

II.2.5. THEOREME (cf. H. Niederreiter(1988a))

La matrice $G^{(d)}$, dont les lignes sont ${}^t\underline{u}_o, \ldots, {}^t\underline{u}_{d-1}$, est de rang d si d est inférieur ou égal à s et de rang s si d est strictement supérieur a s.

DEMONSTRATION

Si on applique le lemme II.2.4. à $k = 0$, on voit que ${}^t\underline{u}_s$ est une combinaison linéaire sur $\mathbb{F}_p$ de ${}^t\underline{u}_0, \ldots, {}^t\underline{u}_{s-1}$. Donc $rg(G^{(s+1)}) \leq s$. Les colonnes de $G^{(s+1)}$ étant les vecteurs $\underline{w}_i^{(s+1)}$, $0 \leq i \leq p-1$, et le polynôme minimal de $(x) = \{x_n\}$ étant de degré t, $t = s + 1$, les vecteurs $\underline{x}_o^{(s+1)}, \cdots, \underline{x}_s^{(s+1)}$ sont linéairement indépendants sur $\mathbb{F}_p$ (cf. R. Lidl and H. Niederreiter (1983), théorème 8.51) et donc il en est de même pour les vecteurs $\underline{w}_1^{(s+1)}, \cdots, \underline{w}_s^{(s+1)}$. Par suite le rang de $G^{(s+1)}$ est identique à s. On en déduit en particulier que les vecteurs ${}^t\underline{u}_0, \ldots, {}^t\underline{u}_{s-1}$ sont linéairement indépendants et donc le rang de $G^{(d)}$ est égal à d, pour tout d inférieur ou égal à s. Mais, d'après le lemme II.2.4., $\underline{u}_d$ est une combinaison linéaire de $\underline{u}_0, \ldots, \underline{u}_{s-1}$ et par conséquent on a, $rg(G^{(d)}) = s$ pour tout entier d strictement supérieur à s.

C.Q.F.Q.

II.2.6. REMARQUE .

La démonstration du théorème II.2.5. montre que s est le plus petit entier n strictement positif tel que $\underline{u}_n$ soit combinaison linéaire de $\underline{u}_0, \ldots, \underline{u}_{n-1}$. Ceci nous donne une méthode de calcul de s. Comme le degré du polynôme minimal de la suite $(x) = \{x_n\}$ vaut s+1, on peut également obtenir s en calculant le polynôme minimal de la suite $(x) = \{x_n\}$ suivant la méthode décrite au chapitre II, paragraphe I.3.

Nous considérons maintenant le cas particulier du générateur (11) donné par la relation (12).

II.2.7. THEOREME(cf. H. Niederreiter(1988a))

La suite $(x) = \{x_n\}$ passe le test des treillis en dimension d pour tout entier d vérifiant $d \leq (p+1)/2$.

DEMONSTRATION

Au vu du théorème II.2.5., il suffit de démontrer que $s \geq (p+1)/2$. Mais, d'après (23), z_n est représenté par un polynôme en n de degré 2s, où

$$z_n = x_n x_{n+1} - b x_n - a.$$

Puisque (p-1) termes de la suite $z_o, \ldots, z_{p-1}$ sont nuls on a $p-1 \leq 2s$. Mais d'après le lemme II.2.3., s est distinct de (p-1)/2, donc $s \geq (p+1)/2$.

C.Q.F.D.

II.3. TEST SERIEL.

Etant donnés deux entiers k et N strictement supérieurs à 1, on considère les vecteurs $\underline{u}_i$ définis par

$$\underline{u}_i = (x_i/m, \ldots, x_{i+k-1}/m), \qquad i = 0, 1, 2, \ldots$$

où la suite $(x) = \{x_n\}$ est donnée par l'une ou l'autre des relations (11) et (12) et où m est le modulo de la relation utilisée.

On s'intéresse ici à la distribution de ces vecteurs dans l'espace $[0, 1]^k$, ce qui revient à étudier l'indépendance statistique de k termes successifs de la suite $(u) = \{x_i/m\}$. Pour cela on estime la discrépance D_N^k, $1 \leq N \leq p$ et $2 \leq k \leq s$, des points $\underline{u}_o, \underline{u}_1, \ldots, \underline{u}_{N-1}$ en considérant séparément les cas suivant le générateur employé pour engendrer la suite $(x) = \{x_n\}$.

a) cas du générateur déterminé par (11)

II.3.1. THEOREME(cf. H. Niederreiter (1988b)).

Si l'entier s est défini comme au paragraphe II.2., alors on a

$$\text{i)} \quad D_p^{(k)} < 1 - (1-1/p)^k + (s-1)p^{-1/2}(2\log p/\pi + 7/5)^k$$

pour $k \leq s$.

$$\text{ii)} \quad D_N^{(k)} < 1 - (1 - 1/p)^k + (s-1)p^{1/2}/(4\log p/\pi^2 + 0.38 + (N+1)/p)(2\log p/\pi + 7/5)^k/N$$

pour $1 \leq N < p$ et pour tout $k \leq s-1$.

Faisons maintenant une comparaison entre les conclusions du test sériel des congruences linéaires simples et des générateurs non linéaires de la forme (11).
On sait (cf. H.Niederreiter (1977)) que pour une congruence linéaire modulo un nombre premier p et pour tout entier k, $k > 1$, il est possible de choisir des paramètres dépendant de k de telle sorte que cette congruence engendre une suite de période p-1, suite pour laquelle l'ordre de grandeur de la discrépance $D_{p-1}^{(k)}$ est de $p^{-1}(\log p)^k \log\log p$. Mais, d'après le théorème ci-dessus, l'ordre de grandeur de $D_p^{(k)}$ d'une congruence non linéaire de la forme (11) est de $p^{-1/2}(\log p)^k$ pour tout $k \leq s$. Ainsi, pour un choix convenable des paramètres, une congruence linéaire simple a un meilleur comportement sous le test sériel qu'une congruence non linéaire de la forme (11).

Notons cependant que les générateurs de la forme (11) passent de façon satisfaisante le test sériel en dimension k, $2 \leq k \leq s$, dès que la fonction f utilisée vérifie les conditions requises et que les congruences linéaires simples dont les paramètres ne sont pas choisis de manière judicieuse donnent de mauvais résultats comparativement à ces générateurs (cf. H. Niederreiter (1978)).

b) Générateurs de la forme (12)

II.3.2. THEOREME (cf. H. Niederreiter (1988b))

Pour $2 \leq k < p$ on a

$$D_p^{(k)} < 2p^{-1/2}(2\log p/\pi + 7/5)^{k-1}((2k-2)\log p/\pi + (2k-7)/5) + 2p^{-1/2} +$$

$$+ (2\log p/\pi + 7/5)^{k-1}((2k-2)\log p/\pi + (12k-7)/5)/p.$$

Remarquons d'abord que les générateurs de la forme (12) sont des cas particuliers de ceux de (11). D'autre part, si l'ordre de grandeur de $D_p^{(k)}$ est le même que dans le cas (11), il est valable pour tout k avec $2 \leq k < p$ au lieu de k vérifiant $2 \leq k \leq s$. Notons enfin que l'estimation de $D_p^{(k)}$ dans le théorème II.3.2. est indépendante de la spécificité des paramètres a et b de (12) auxquels on a imposé les deux seules conditions suivantes :

i) a et b sont des éléments de $\mathbb{F}_p$ tels que $ab \neq 0$.

ii) $x^2 - bx - a$ est un polynôme primitif sur $\mathbb{F}_p$.

CHAPITRE 4

CRYPTOGRAPHIE : CALCULS DES DETERMINANTS DE HANKEL ET CONJECTURE SUR LE DECRYPTAGE DE L'ORDRE ET DU MODULO D'UNE CONGRUENCE LINEAIRE SIMPLE OU MULTIDIMENSIONNELLE

INTRODUCTION SUR LA CRYPTOGRAPHIE

L 'essentiel du travail d'un cryptographe consiste à mettre en relation, par des canaux peu sûrs ou publics (ondes hertziennes, services postaux, réseaux télématiques ...), deux individus de manière à ce que leurs conversations soient confidentielles. Du point de vue mathématique, le problème peut être formalisé succinctement de la façon suivante :

Etant donné un espace M dit "de messages ", il s'agit de trouver une application C injective de M dans un certain espace M' telle que connaîssant l'image C(m) d'un élément m de M, on ne puisse pas retrouver m sans connaître C^{-1}, réciproque de C.

Un cryptosystème sera alors défini par la donnée de deux espaces M et M' et d'une collection de couples (C, C^{-1}). On appelle généralement clé d'encryptage ou de codage l'application C (ou une caractérisation de C) et clé de décryptage ou de décodage sa réciproque C^{-1} (ou une caractérisation de C^{-1}) .

Il y a deux grandes classes de cryptosystèmes : les systèmes conventionnels et les systèmes à clés publiques (ou P.K.C pour Public Key Cryptosystem).

Les systèmes conventionnels ou traditionnels .

Ces systèmes fonctionnent de la manière suivante :
Soient a et b deux individus souhaitant communiquer secrètement.
Chacun d'eux conserve secrètement un couple de clés (C_{ab}, C_{ab}^{-1}) .
Si a désire envoyer un message m à b il transmet en fait $C_{ab}(m)$.
L'individu b retrouve le message en clair m en appliquant à $C_{ab}(m)$, la clé C_{ab}^{-1}.

Un exemple type de tels systèmes est le système dit "one time pad " dans la littérature anglo-saxonne . Dans ce cryptosystème, un message m est une suite binaire . L'encryptage d'un tel message se fait en ajoutant terme à terme (addition modulo 2) à m une suite binaire aléatoire de même longueur que m, tandis que le décryptage se fait en ajoutant au message codé la même suite aléatoire .

Du point de vue de la sécurité une telle méthode est parfaite : il est impossible à partir du message codé de distinguer m parmi tous les messages m' de même longueur que m . Ce cryptosystème est qualifié "d'inconditionnellement sûr " par opposition aux cryptosystèmes "calculatoirement sûrs" où la sécurité repose sur l'impossibilité d'obtenir avec les algorithmes actuels et en un temps raisonnable des solutions effectives à des problèmes intrinsèques à ces cryptosystèmes.

Pour communiquer concrètement par le système "one time pad", deux individus doivent au préalable échanger par un canal privé une suite aléatoire de même longueur que le message à transmettre. On a ainsi un paradoxe caractéristique des cryptosystèmes

traditionnels : les utilisateurs doivent échanger des clés par un canal privé avant de pouvoir communiquer secrètement par voie publique. Ce paradoxe a conduit les cryptographes à définir un autre type de cryptosystème.

Les cryptosystèmes à clés publiques (P.K.C).

Dans ces systèmes, on affecte à chaque utilisateur a un couple de clés $(C_{K(a)}, C_{K(a)}^{-1})$, où K(a) est un paramètre caractéristique de l'utilisateur. La clé d'encryptage $C_{K(a)}$ est publiée dans un répertoire accessible au public, tandis que a conserve secrètement $C_{K(a)}^{-1}$ et K(a). L'orsqu'un individu b souhaite envoyer un message m à l'individu a il utilise la clé $C_{K(a)}$ du répertoire public et transmet $C_{K(a)}(m)$; l'individu a récupère ensuite le message m en appliquant $C_{K(a)}^{-1}$ au message codé $C_{K(a)}(m)$.

La confidentiabilité et l'effectivité d' une méthode basée sur ce schéma sont garanties par les deux points suivants :

i) Il est impossible de calculer $C_{K(a)}^{-1}$ en un temps raisonnable en connaîssant uniquement $C_{K(a)}$.

ii) Il est relativement facile de calculer $C_{K(a)}^{-1}$ à partir de K(a).

Les fonctions vérifiant i) sont dits " one - way ", tandis que celles qui satisfont i) et ii) sont appelées "fonctions trappes ".

Les systèmes à clés publiques offrent non seulement l'avantage de ne pas nécessiter d'échange préalable de clés secrètes avant toute communication confidentielle, mais permettent également de réduire le nombre de clés à calculer lorsque plusieurs individus doivent communiquer entre eux. Mais l'inconvénient est que les phases d'encryptage et de décryptage coûtent généralement plus chers que dans les systèmes conventionnels.

Comme exemple de P.K.C., on peut citer le système R.S.A. de Rivest-Shamir-Adlemann (cf. R. Lidl and H. Niederreiter (1986), chapitre 9) servant de référence en matière de P.K.C.

Remarquons qu'on combine souvent les cryptosystèmes conventionnels et à clés publiques pour réduire le coût de certaines transmissions de messages. Ainsi on choisit parfois de communiquer avec le système conventionnel après avoir transmis les clés secrètes au moyen d'un P.K.C. .

Dans l'exemple du système conventionnnel "one time pad ", la clé secrète peut être représentée par les paramètres du générateur ayant servi au codage du message et pour qu'un tel système résiste aux attaques des cryptanalystes (casseurs de codes), il est nécessaire d'utiliser un générateur cryptographiquement sûr.

Un générateur de nombres pseudo- aléatoires est dit cryptographiquement sûr si, étant donné un segment suffisamment long de la suite produite par ce générateur, un cryptanalyste est incapable de calculer en un temps raisonnable le terme suivant de ce segment de suite. En ce qui concerne les exemples de générateurs cryptographiquement sûrs, nous renvoyons le lecteur à ceux de A. Shamir (1980), M. Blum et S. Micali (1984) et L. Blum, M. Blum et M. Shub (1986). Mais ces générateurs sont lents. D'autre part les générateurs linéaires de nombres pseudo-aléatoires de la forme

$$s_{i+1} \equiv as_i + b \mod m \qquad \forall\ i \geq 0$$

sont rapides et d 'usage courant dans les méthodes de simulation de Monte - Carlo et dans les algorithmes probabilistes . En revanche ils ne sont pas cryptographiquement sûrs.

En effet J.B. Plumstead (1982) a montré que, étant donné un segment relativement court de la suite engendrée par une congruence linéaire, on peut retrouver en temps raisonnable le reste de la suite en supposant a, b et m inconnus.
Faisant l'hypothèse que l'ordre k est connu, A. Bauval (1986) et J. Boyar (1989) ont pû reconstruire également les suites engendrées par les congruences linéaires multidimensionnelles

$$s_{i+k} \equiv a_{k-1}s_{i+k-1} + \cdots + a_0 s_0 + b \mod m \qquad \forall\ i \geq 0$$

à partir d'un segment de $(s) = \{s_n\}$. La méthode de reconstruction utilisée par ces deux auteurs repose essentiellement sur des estimations successives des paramètres $a_0, a_1, \ldots, a_{k-1}$ et m. Notons cependant que dans certains cas, on retrouve la suite désirée bien qu'on ait

$$(\hat{a}_0, \hat{a}_1, \cdots, \hat{a}_{k-1}, \hat{m}) \neq (a_0, a_1, \cdots, a_{k-1}, m)$$

où $\hat{a}_0, \hat{a}_1, \cdots, \hat{a}_{k-1}$ et $\hat{m}$ sont respectivement les estimateurs de $a_0, a_1, \cdots, a_{k-1}$ et m.

Nous supposons dans ce chapitre que l'ordre k et les paramètres $a_0, a_1, \ldots, a_{k-1}$, b et m sont inconnus et nous faisons une conjecture sur le décryptage de k et de m. Pour cela nous mettons en oeuvre un algorithme de calcul des déterminants de Hankel basé sur les travaux de A. Draux (1981).

I. CALCUL DES DETERMINANTS DE HANKEL

I.1. IDENTITE DE SYLVESTER

Soient n un entier naturel non nul et $A = (a_{ij},\ 1 \leq i, j \leq n)$ une matrice carrée d'ordre n à coefficients réels. Alors le déterminant de A est noté D ou Det (A).

PROPRIETE (identité de Sylvester) .

Soit d le déterminant de la matrice obtenue en supprimant dans A, d'une part les première et dernière lignes et d'autre part les première et dernière colonnes. On désigne ensuite par A_{ij} le cofacteur de a_{ij} dans D pour $1 \leq i, j \leq n$. Alors

$$(1) \qquad Dd = A_{11}A_{nn} - A_{n1}A_{1n}.$$

DEMONSTRATION

On pose

$$B = \begin{bmatrix} A_{11} & 0 & 0 & 0 & 0 & 0 & A_{n1} \\ A_{12} & 1 & 0 & 0 & 0 & 0 & A_{n2} \\ . & 0 & . & 0 & 0 & 0 & . \\ . & 0 & 0 & . & 0 & 0 & . \\ . & 0 & 0 & 0 & . & 0 & . \\ A_{1n-1} & 0 & 0 & 0 & 0 & 1 & A_{nn-1} \\ A_{1n} & 0 & 0 & 0 & 0 & 0 & A_{nn} \end{bmatrix}$$

Alors

$$\text{Det } (AB) = D^2 d$$

D'autre part on a

$$\text{Det } (A) \text{ Det } (B) = D\,(A_{11}A_{nn} - A_{n1}A_{1n}).$$

Donc

$$D^2 d = D\,(A_{11}A_{nn} - A_{n1}A_{1n}\ ).$$

Si D est non nul alors on a immédiatement le résultat . Supposons donc D nul et posons $A^* = (A_{ij},\ 1 \leq i, j \leq n)$. Alors on a

$$AA^* = DI = 0 .$$

Nous distinguons maintenant deux cas suivant la valeur de rang (A) , où pour toute matrice M à coefficients réels, rang (M) désigne le rang de M.

i) Rang(A) < n-1.

Dans ce cas l'identité est trivialement vérifiée après avoir remarqué que tous les Aij, $1 \leq i, j \leq n$, sont nuls.

ii) Rang (A) = n-1.

Alors il est clair que Ker(A) est de dimension 1, où Ker (A) désigne le noyau de l'application linéaire définie sur $\mathbb{R}^n$ et dont la matrice associée est A. Comme AA^* est la matrice nulle les colonnes de A^* sont solutions du système d'équations linéaires

$$A\underline{X} = 0$$

avec $\underline{X} = {}^t(X_1, ..., X_n)$. On en déduit que ces colonnes appartiennent à une même droite vectorielle puisqu'elles sont dans Ker (A) qui est de dimension 1. Il s'ensuit que le rang de A^* est identique à 1 et par conséquent toutes les sous matrices carrées de A^* d'ordre supérieur ou égal à 2 sont de déterminant nul. Ce qui achève la démonstration de l'identité de Sylvester.

I.2. QUELQUES DEFINITIONS ET PROPRIETES SUR LES DETERMINANTS DE HANKEL

I.2.1. DEFINITIONS

Soit $(s) = \{s_i , i \in \mathbb{Z}\}$ une suite de réels . On appelle *matrice de Hankel d'ordre k*, la matrice $M_k^{(i)}(s)$ construite à partir de $s_i, s_{i+1}, \cdots, s_{i+k-1}$ et définie par

$$M_k^{(i)}(s) = \begin{bmatrix} s_i & s_{i+1} & \cdot & \cdot & \cdot & s_{i+k-1} \\ s_{i+1} & \cdot & \cdot & \cdot & \cdot & s_{i+k} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ s_{i+k-1} & s_{i+k} & \cdot & \cdot & \cdot & s_{i+2k-2} \end{bmatrix} , \quad \forall\ k>0, \text{ et } i \in \mathbb{Z} .$$

Le *déterminant de Hankel* $H_k^{(i)}(s)$ est le déterminant de la matrice $M_k^{(i)}(s)$. Soit

$$H_k^{(i)}(s) = \mathrm{Det}\,(M_k^{(i)}(s)),\ \forall\, k>0 \text{ et } i\in \mathbb{Z}$$

et (2)

$$H_0^{(i)}(s) = 1 \quad \text{et} \quad H_{-1}^{(i)}(s) = 0 \qquad \forall\, i\in \mathbb{Z}.$$

I.2.2 REMARQUE .

Pour simplifier, on écrira souvent $H_k^{(i)}$ au lieu de $H_k^{(i)}(s)$.

I.2.3. PROPRIETE .

Pour deux entiers quelconque i et $k>0$ on a

$$(3) \qquad H_k^{(i+1)}H_k^{(i-1)} - (H_k^{(i)})^2 = H_{k+1}^{(i-1)}H_{k-1}^{(i+1)}.$$

DEMONSTRATION

On pose

$$D = \mathrm{Det}\ (M_{k+1}^{(i-1)}).$$

Alors

$$d = H_{k-1}^{(i+1)}, \quad A_{11} = H_k^{(i+1)}, \ A_{ii} = H_k^{(i-1)} \text{ et } A_{i1} = A_{1i} = H_k^{(i)}$$

et l'application de (1) donne immédiatement le résultat.

I.2.4. DEFINITIONS.

i) On appelle *table H* le tableau triangulaire contenant les $H_k^{(i)}$. Soit

$H_0^{(0)}$

$H_0^{(1)}$ $H_1^{(0)}$

$H_0^{(2)}$ $H_1^{(1)}$ $H_2^{(0)}$

$H_0^{(3)}$ $H_1^{(2)}$ $H_2^{(1)}$ $H_3^{(0)}$

$H_0^{(4)}$ $H_1^{(3)}$ $H_2^{(2)}$ $H_3^{(1)}$

$H_0^{(5)}$ $H_1^{(4)}$ $H_2^{(3)}$

$H_0^{(6)}$ $H_1^{(5)}$

$H_0^{(7)}$

où les indices supérieurs et inférieurs correspondent respectivement aux indices des *diagonales principales* et des colonnes.

ii) La table H est dite *normale* si les $H_k^{(i)}$ sont tous non nuls, en revanche s'il y a au moins un déterminant nul alors elle est dite *non normale*.

iii) On appelle *bloc H* un bloc carré de la table H où tous les déterminants $H_k^{(i)}$ sont nuls alors que les éléments de la périphérie sont tous non nuls (cf. FIG. 1).

I.2.5. REMARQUE (cf. A. Draux (1981)).

Dans une table non normale les déterminants nuls sont toujours groupés en blocs H.

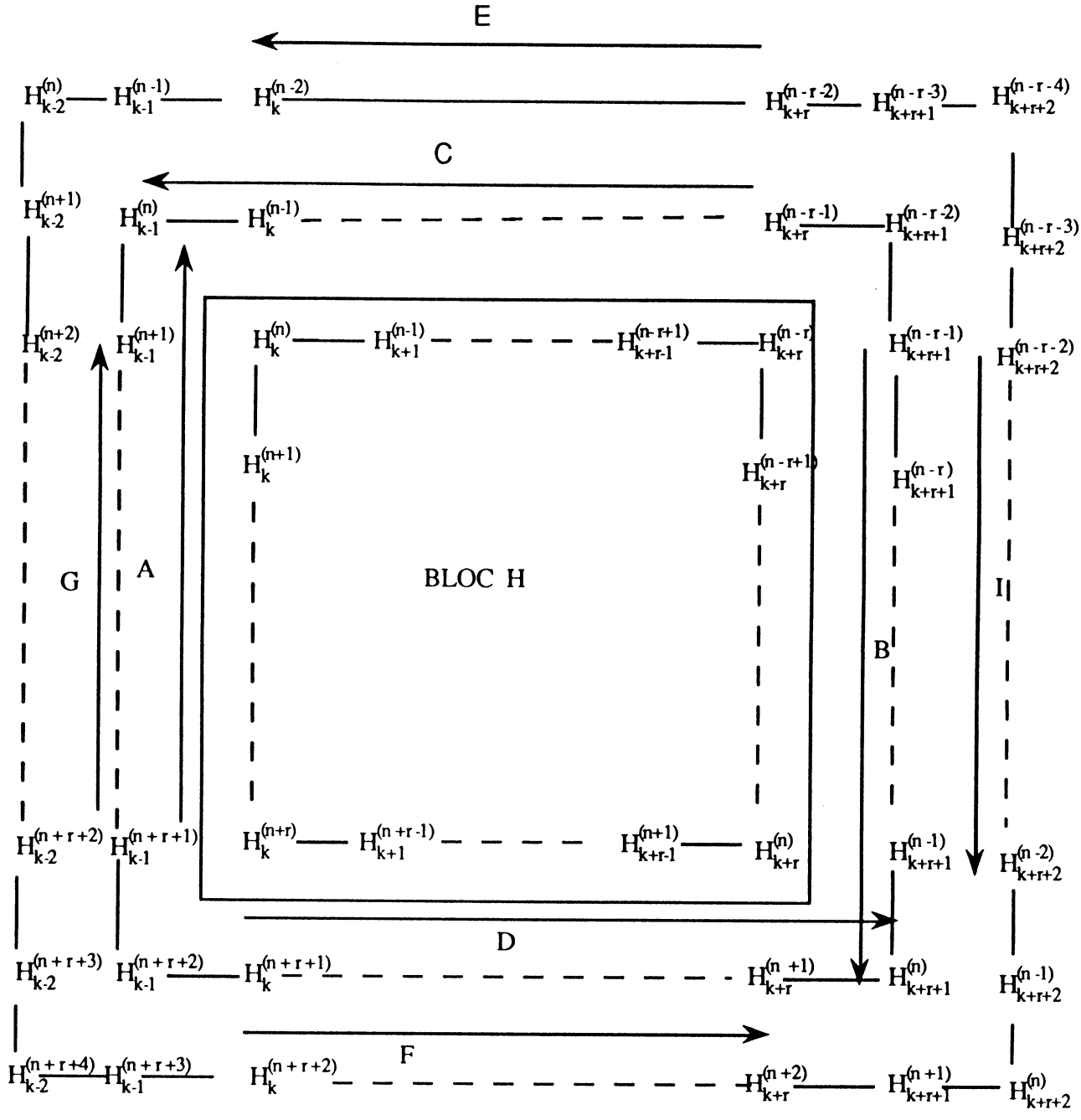


FIG. 1. SCHEMA D'UN BLOC H AVEC DEUX PERIPHERIES

Le carré ne contient que des zéros, les éléments de la périphérie étant tous non nuls, c'est - à - dire

$$H_j^{(i)} = 0 \text{ pour } i \in \mathbb{N},\ j \in \mathbb{N},\ k \le j \le k+r \text{ et } k+n \le i+j \le k+n+r .$$

et $H_j^{(i)} \neq 0$ pour

⊗ $j=k-1, i\in \mathbb{N},\ n \le i \le n+r+2$

⊗ $j = k+r+1, i\in \mathbb{N},\ n-r-2 \le i \le n$

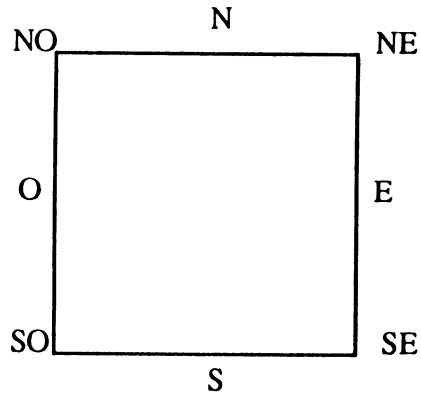
⊗ $i+j = k+n-1, i\in \mathbb{N},\ n-r-2 \le i \le n$

⊗ $i+j = k+n+r+1, i\in \mathbb{N},\ n \le i \le n+r+2$

Convention. Si pour $i \in]\, n, n-r\,]$ des indices i sont strictement négatifs on conviendra de limiter le carré par la diagonale principale correspondant à $H^{(0)}$.

I.2.6 REMARQUE

On définira les côtés et les coins de chacun des blocs par un repère géographique Nord, Sud, Est et Ouest pour les côtés, Nord- Ouest, Nord-Est, Sud- Est et Sud-Ouest pour les coins . On les note en abrégé N, S, E, O, NO, NE, SE et SO.



I.3. DESCRIPTION DES DIFFERENTS TYPES DE BLOC D'UNE TABLE DE DETERMINANTS DE HANKEL

Notation .

Un bloc sera caractérisé par ses coordonnées k, n et r définies par

k : Indice de la colonne sur laquelle débute le bloc .

n : Indice supérieur du déterminant de Hankel situé dans le coin N.O. intérieur du bloc

r + 1 : Largeur du bloc

Comme en pratique on ne peut travailler qu'avec une table H finie, on introduit IDC et NBE1C :

IDC : Indice de la dernière colonne de la table H

NBE1C : Nombre d'éléments de la colonne d'indice 1 de la table H.

On aura besoin, dans la présentation des types de bloc des quantités T1C et T2C :

T1C : Nombre d'éléments de la colonne (k+r+1) de la table H.

T2C : Nombre d'éléments de la colonne (k+r+2) de la table H.

Description des types de bloc .

1. La deuxième colonne à l'est du bloc H existe .

1.0. Bloc non tronqué

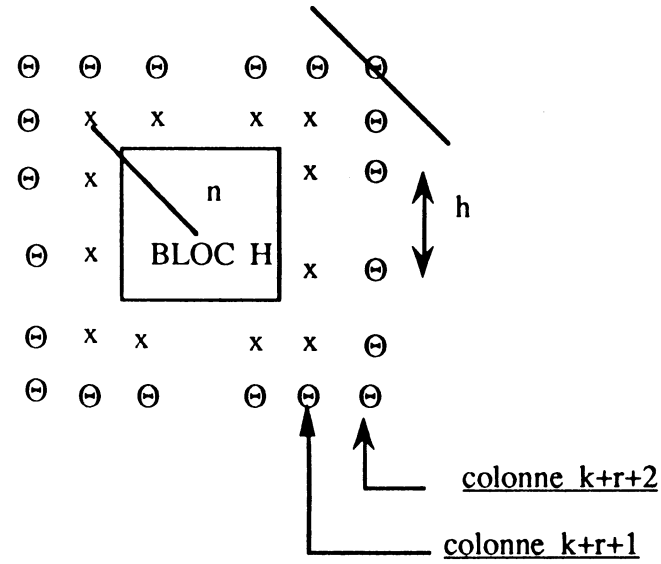


FIG. 2.

Soit :

$$k + r + 2 \leq IDC,\ 0 \leq n - r - 2 \text{ et } n - 2 \leq T2C - 1.$$

1.1. bloc tronqué uniquement au Nord- Est .

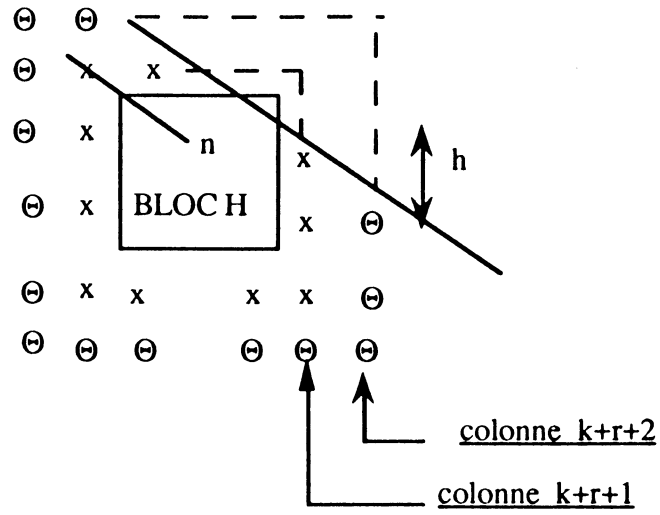


FIG . 3.

Soit :

$$k + r + 2 \leq IDC \quad \text{et} \quad n - r - 2 < 0 \leq n - 2 \leq T2C - 1.$$

1.2. bloc tronqué uniquement au Sud - Est .

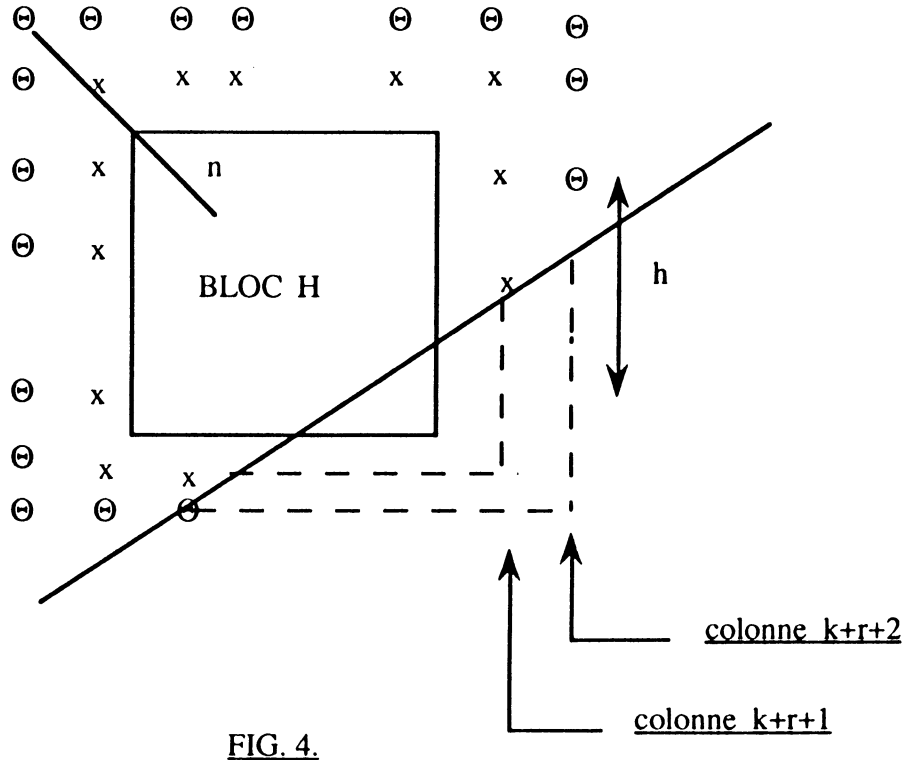


FIG. 4.

Soit : $k + r + 2 \leq IDC$ et $0 \leq n - r - 2 \leq T2C - 1 < n-2$.

1.3. bloc tronqué à la fois au Nord - Est et au Sud - Est.

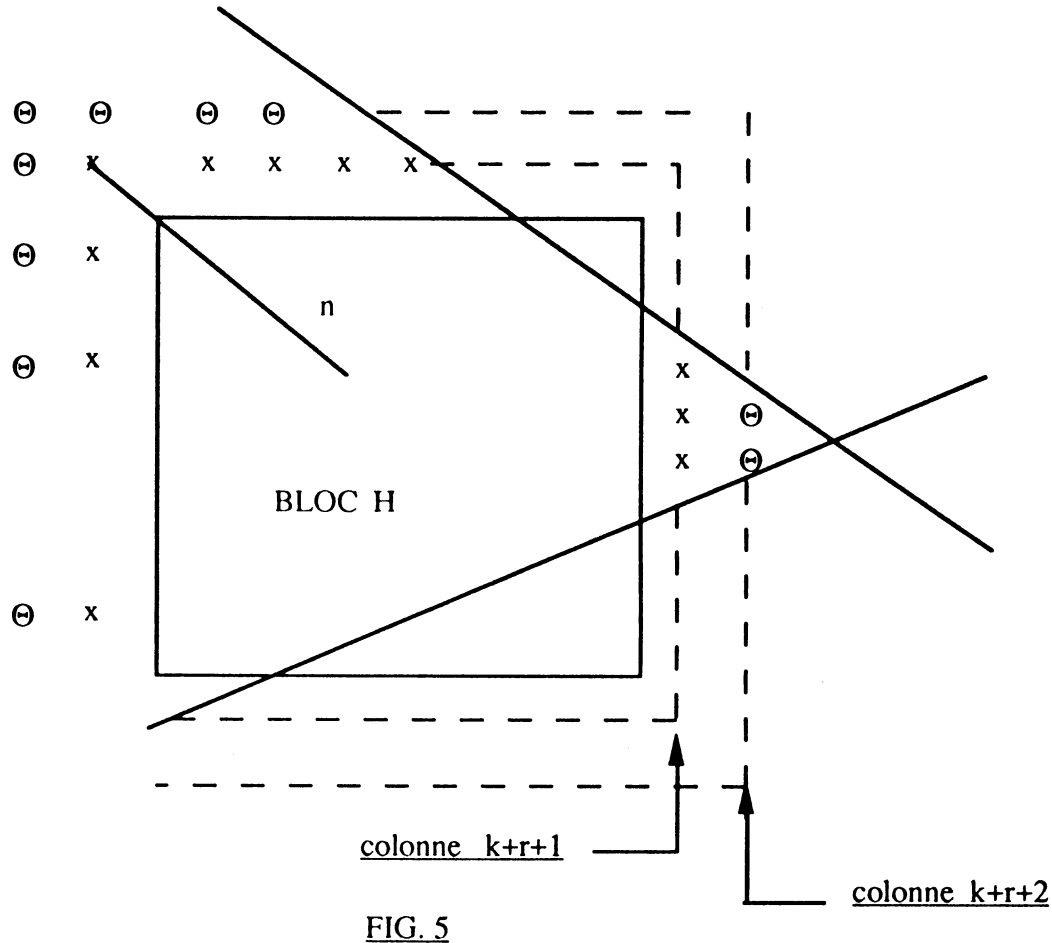


FIG. 5

Soit : $k + r + 2 \leq IDC$ et $n - r - 2 < 0 \leq T2C - 1 < n - 2$

2. Cas où, seule, la première colonne à l'est du bloc existe

2.0. la colonne (k + r + 1) n'est pas tronquée.

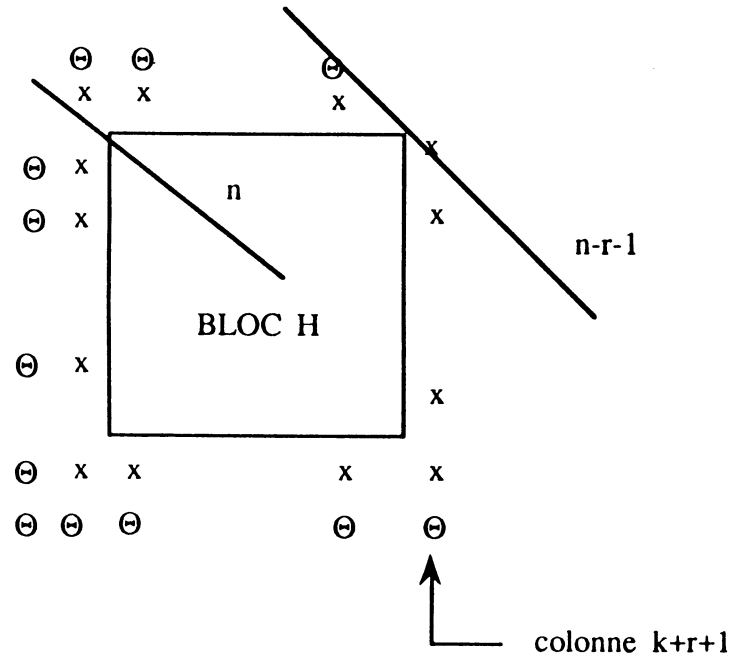


FIG. 6

Soit : k + r + 1 = IDC, $0 \leq n - r - 1$ et $n - 1 \leq T1C - 1$.

2.1. La colonne (k+r+1) est tronquée uniquement au Nord-Est .

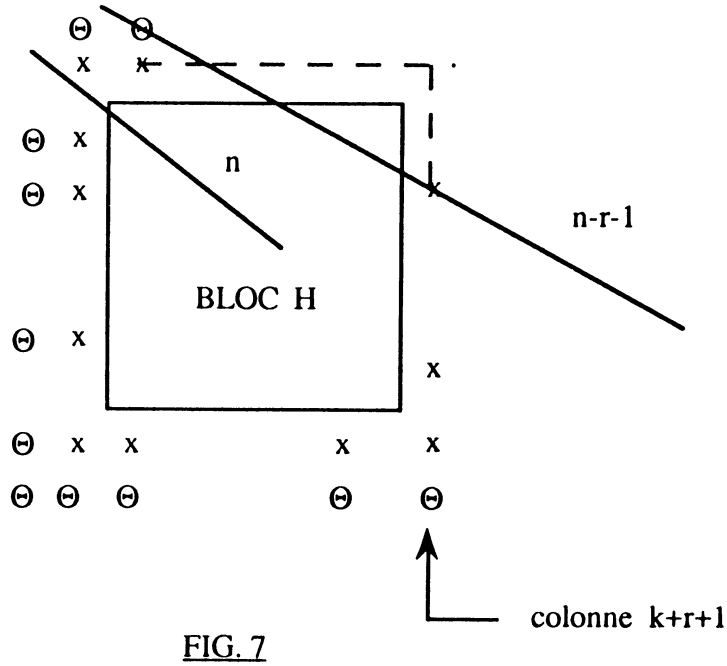


FIG. 7

Soit : k + r + 1 = IDC et $n - r - 1 < 0 \leq n - 1 \leq T1C - 1$.

2.2. La colonne (k + r + 1) est tronquée uniquement au Sud.

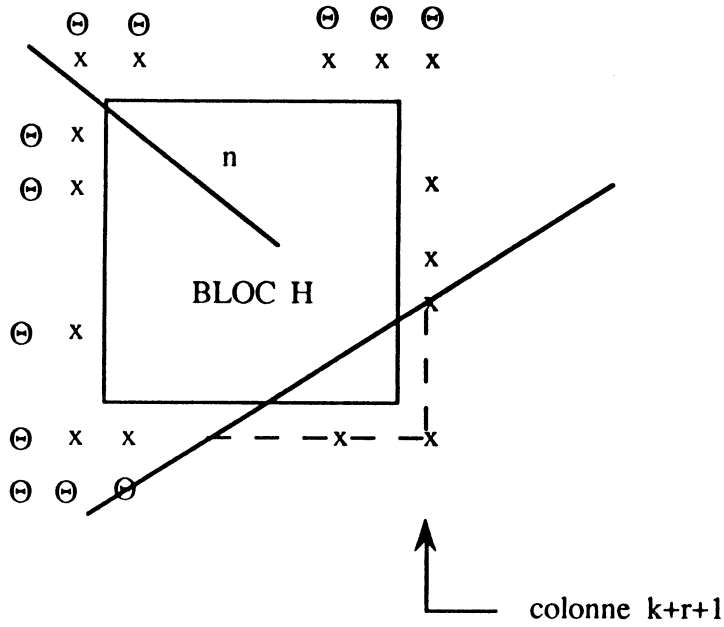


FIG. 8

Soit : $k + r + 1 = IDC$ et $0 \leq n - r - 1 < T1C - 1 < n - 1$.

2.3. La colonne (k+r+1) est tronquée à la fois au nord et au sud.

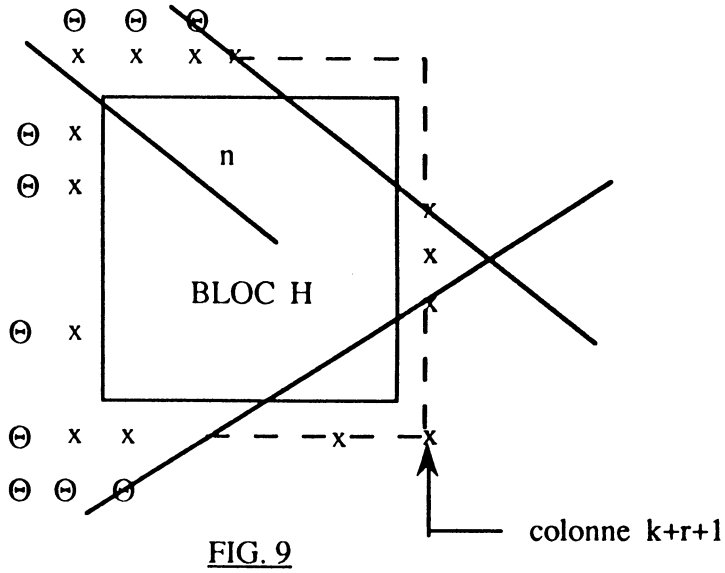
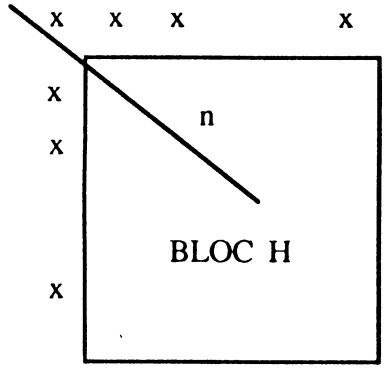


FIG. 9

Soit : $k + r + 1 = IDC$ et $n - r - 1 < 0 \leq T1C - 1 < n - 1$.

3. Cas où les 2 colonnes (k + r + 2) et (k + r + 1) n'existent pas.



I.4. ALGORITHME DE CALCUL DES DETERMINANTS DE HANKEL

Conduite générale du calcul de la table $\mathbb{H}$.

On calcule la table H colonne après colonne en utilisant (3) et les valeurs de départ

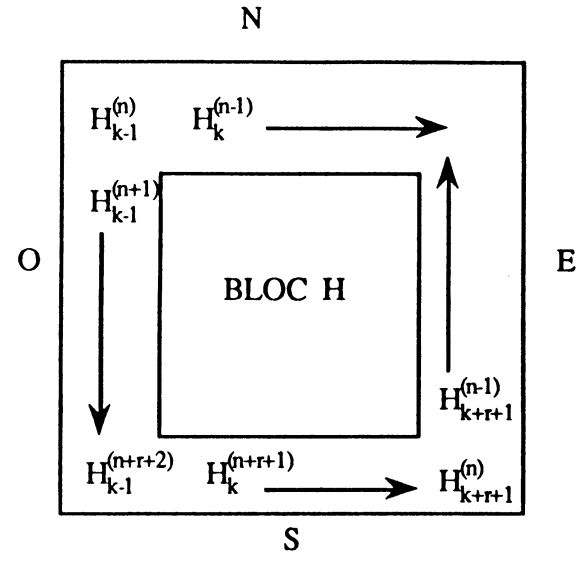
$$H_{-1}^{(n)} = 0, \quad H_0^{(n)} = 1 \text{ et } H_1^{(n)} = s_n , \ \forall\, n \in \mathbb{N} \ .$$

Mais, il y a des cas où l'identité (3) ne permet pas de calculer les éléments se trouvant sur les première et deuxième colonnes à l'est d'un bloc H. Aussi fait - on intervenir d'autres relations entre les déterminants de Hankel situés dans un voisinage du bloc H.

Calcul des déterminants de Hankel bordant un bloc H .

Considérons le schéma ci-dessous représentant pour l'essentiel le pourtour d'un bloc H de coordonnées k, n et r.

FIG. 10.



Une application de (3) montre qu'il y a une progression géométrique entre les déterminants bordant le bloc H . Plus précisément on détermine complètement le côté Nord du bloc à partir de $H_{k-1}^{(n)}$ et $H_k^{(n-1)}$, le côté Ouest au moyen de $H_{k-1}^{(n)}$ et $H_{k-1}^{(n+1)}$, le côté sud au moyen de $H_{k-1}^{(n+r+2)}$ et $H_k^{(n+r+1)}$ et enfin le côté Est à partir de $H_{k+r+1}^{(n)}$ et $H_{k+r+1}^{(n-1)}$. Sur la figure 10, les flèches indiquent le sens de la progression géométrique sur chacun des quatre côtés du pourtour du bloc.

La relation (3) nous donne les quantités $H_k^{(n-1)}$, $H_{k-1}^{(n)}$, $H_{k-1}^{(n+1)}$ et $H_k^{(n+r+1)}$. Pour évaluer $H_{k+r+1}^{(n-1)}$ on peut utiliser le lemme suivant :

I.4. 1 . LEMME (cf. A. DRAUX (1981)).

Soit un bloc H de coordonnées k, n et r (cf. FIG. 10.). Alors la relation

$$H_{k-1}^{(n+1)} H_{k+r+1}^{(n-1)} = H_k^{(n-1)} H_{k+r}^{(n+1)}$$

permet de calculer H_{k+r+1}^{n-1} .

Calcul des déterminants de Hankel sur la deuxième colonne à l'est d'un bloc H.

I.4.2. THEOREME (cf. A. DRAUX (1981))

On suppose qu'on a un bloc H de largeur r+1 et dont le coin Nord-Ouest intérieur est occupé par le déterminant $H_k^{(n)}$ (cf. FIG. 1.). Alors la relation suivante nous permet de calculer $H_{k+r+2}^{(n-r-1+i)}$, pour $i \in \mathbb{Z}$, $-1 \leq i \leq r-1$.

$$(4)\quad \frac{H_{k+r+2}^{(n-r-1+i)}\,H_{k+r-1-i}^{(n-r+i)}}{H_{k+r+1}^{(n-r+i)}\,H_{k+r-i}^{(n-r-1+i)}} + \frac{H_{k+r+1}^{(n-r+i)}\,H_{k+r-1-i}^{(n-r-1+i)}}{H_{k+r-1-i}^{(n-r+i)}\,H_{k+r+1}^{(n-r-1+i)}} = \frac{H_{k+i+1}^{(n+r-i)}\,H_{k-2}^{(n+r+1-i)}}{H_{k+i}^{(n+r+1-i)}\,H_{k-1}^{(n+r-i)}} + \frac{H_{k+i+1}^{(n+r+1-i)}}{H_{k+i+1}^{(n+r-i)}}\,\frac{H_{k-1}^{(n+r-i)}}{H_{k-1}^{(n+r+1-i)}}.$$

Détail du calcul de $H_{k+r+2}^{n-r-1+i}$ suivant le type de bloc rencontré.

Cas d'un bloc non tronqué (cf. FiG. 2).

On considère les listes suivantes (cf. FIG. 1.) :

$$A = \left[\, H_{k-1}^{(n+r+1)},\quad H_{k-1}^{(n+r)},\quad \cdots,\quad H_{k-1}^{(n+1)},\quad H_{k-1}^{(n)} \,\right]$$

$$B = \left[\, H_{k+r+1}^{(n-r-1)},\ H_{k+r+1}^{(n-r)},\quad \cdots,\quad H_{k+r+1}^{(n-1)},\ H_{k+r+1}^{(n)} \,\right]$$

$$C = \left[\, H_{k+r}^{(n-r-1)},\ H_{k+r-1}^{(n-r)},\quad \cdots,\quad H_{k}^{(n-1)},\quad H_{k-1}^{(n)} \,\right]$$

$$D = \left[\, H_{k}^{(n+r+1)},\quad H_{k+1}^{(n+r)},\quad \cdots,\quad H_{k+r}^{(n+1)},\quad H_{k+r+1}^{(n)} \,\right]$$

$$E = \left[\, H_{k+r}^{(n-r-2)},\ H_{k+r-1}^{(n-r-1)},\quad \cdots,\quad H_{k+1}^{(n-3)},\quad H_{k}^{(n-2)} \,\right]$$

$$F = \left[\, H_{k}^{(n+r+2)},\quad H_{k+1}^{(n+r+1)},\quad \cdots,\quad H_{k+r-1}^{(n+3)},\quad H_{k+r}^{(n+2)} \,\right]$$

$$G = \left[\, H_{k-2}^{(n+r+2)},\quad H_{k-2}^{(n+r+1)},\quad \cdots,\quad H_{k-2}^{(n+3)},\quad H_{k-2}^{(n+2)} \,\right]$$

$$I = \left[\, H_{k+r+2}^{(n-r-2)},\ H_{k+r+2}^{(n-r-1)},\quad \cdots,\quad H_{k+r+2}^{(n-3)},\ H_{k+r+2}^{(n-2)} \,\right]$$

Si L est une liste, on désigne par L[j] l'élément de L se trouvant dans la case d'indice j, (j = 1, 2, 3, ...), étant entendu que la numérotation se fait de gauche à droite. On fait l'hypothèse que les listes A, B, C, D, E, F et G sont connues et on cherche à calculer la liste I.

D'après (3), (4) et le lemme I.4.1. on a :

$$(5)\quad I[j] = \left(\frac{(D[j+1]\,G[j] - A[j+1]\,F[j])\,C[j]\,B[j]}{A[j]\,D[j]} + B[j+1]\,E[j]\right)/C[j+1]\ ,\quad j = 1, 2, \cdots, r+1.$$

Cas d'un bloc tronqué (cf. Fig. 3, 4, 5)

On suppose que la portion de la colonne (k+r+2) correspondant à la hauteur h (cf. FIG. 3, 4 et 5) est tronquée de t_1 éléments dans sa partie Nord et de t_2 éléments dans sa partie sud où

$$0 \leq t_1 < r+1,\ 0 \leq t_2 < r+1 \text{ et } 0 < t_1+t_2 < r+1 .$$

On en déduit alors les listes A', B', C', D', E', F', G' et I' en supprimant les t_1 premiers éléments et les t_2 derniers éléments des listes respectives A, B, C, D, E, F, G et I. On calcule ensuite la liste I' en appliquant (5) après avoir remplacé A, B, C, D, E, F, G, I et (r+1) respectivement par A', B', C', D', E', F', G', I' et $(r+1-t_1-t_2)$.

REMARQUE

Lors du calcul de la table H colonne après colonne, on peut déterminer les coordonnées d'un bloc H dès qu'on rencontre celui-ci pour la première fois. En effet si on considère la figure 1, la première rencontre du bloc H se fait après le calcul de $H_k^{(n)}$ dont la valeur est identique à 0. On note alors n et k. Ensuite le nombre de termes successifs nuls à partir de $H_k^{(n)}$ est égal à (r+1) qui est la largeur du bloc H.

II. DETERMINANTS DE HANKEL ET DECRYPTAGE THEORIQUE DE L' ORDRE D' UNE RECURRENCE LINEAIRE SUR UN CORPS FINI.

Soient p un nombre premier et k >1 un entier.

REMARQUE .

Dans cette partie les opérations d'addition et de multiplication entre éléments du corps fini $\mathbb{F}_p$ sont celles de ce corps et l'addition entre vecteurs sur $\mathbb{F}_p$ se fait composante par composante suivant l'addition dans $\mathbb{F}_p$.

Pour une suite récurrente linéaire homogène non identiquement nulle $(s) = \{s_n\}$ sur $\mathbb{F}_p$ définie par

$$(6) \qquad s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \cdots + a_1 s_{n+1} + a_0 s_n , \quad \forall\, n \geq 0$$

où les coefficients $a_0, a_1, \ldots, a_{k-1}$ sont des éléments de $\mathbb{F}_p$ tels que $a_0 \neq 0$, on désigne par

$$\underline{s}_n = (s_n, s_{n+1}, \ldots, s_{n+k-1}),\ n = 0, 1, \ldots$$

le nième vecteur d'état de (s), par F(x) le polynôme caractéristique associé à (6) et par A

$$A = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 & 1 & & a_{k-2} \\ 0 & 0 & 0 & 0 & 1 & a_{k-1} \end{bmatrix}$$

la matrice compagnon de F(x).

On se propose maintenant de présenter quelques résultats préparatoires au décryptage de k supposé inconnu, à partir d'un segment de la suite (s).

II.1. RESULTATS PREPARATOIRES AU DECRYPTAGE DE k.

II.1.1. THEOREME

Soit $(s) = \{s_n\}$ une suite non identiquement nulle vérifiant (6) et dont l'un des polynômes caractéristiques est F(x) . Alors F(x) est le polynôme minimal de (s) si et seulement si les vecteurs d'état $\underline{s}_0, \underline{s}_1, \ldots, \underline{s}_{k-1}$ sont linéairement indépendants sur $\mathbb{F}_p$.

DEMONSTRATION

i) condition nécessaire

on suppose que F(x) est le polynôme minimal de la suite. Si les vecteurs $\underline{s}_0, \underline{s}_1, \ldots, \underline{s}_{k-1}$ étaient linéairement dépendants sur F_p alors on aurait

$$b_0\underline{s}_0 + b_1\underline{s}_1 + \ldots + b_{k-1}\underline{s}_{k-1} = 0$$

où les coefficients $b_0, b_1, \ldots, b_{k-1}$ sont des éléments de $\mathbb{F}_p$ non tous nuls. On en déduirait alors que

$$b_0\underline{s}_0A^n + b_1\underline{s}_1A^n + \ldots + b_{k-1}\underline{s}_{k-1}A^n = \underline{0},\quad n = 0, 1, \ldots$$

Soit

$$b_0\underline{s}_n + \ldots + b_{k-1}\underline{s}_{n+k-1} = \underline{0}, \qquad n = 0, 1, \ldots$$

et on aurait en particulier

$$b_0 s_n + \ldots + b_{k-1} s_{n+k-1} = 0, \qquad n = 0, 1, \ldots$$

Si $b_j = 0$ pour $1 \leq j < k$, alors $s_n = 0$ pour tout $n \geq 0$; ce qui contredit le fait que la suite (s) n'est pas identiquement nulle. Soit donc $j \geq 1$ le plus grand indice tel que $b_j \neq 0$. Il vient alors que la suite $(s) = \{s_n\}$ vérifie une récurrence linéaire homogène d'ordre j, avec $j < k$, ce qui contredit l'hypothèse selon laquelle F(x) est un polynôme minimal, si bien qu'en définitive les vecteurs $\underline{s}_0, \underline{s}_1, \ldots, \underline{s}_{k-1}$ sont linéairement indépendants sur $\mathbb{F}_p$.

condition suffisante

Supposons $s_0, s_1, \ldots, s_{k-1}$ linéairement indépendants sur $\mathbb{F}_p$. Comme $\underline{s}_0$ est un vecteur non nul, le polynôme minimal est de degré strictement positif . Si F(x) n'était pas le polynôme minimal, alors la suite $(s) = \{s_n\}$ vérifierait une suite récurrente linéaire homogène d'ordre m avec $1 \leq m < k$. Soit

$$s_{n+m} = a'_{m-1} s_{n+m-1} + \ldots + a'_1 s_{n+1} + a'_0 s_n, \quad n = 0, 1, \ldots$$

où $a'_0, a'_1, \ldots, a'_{m-1}$ sont des éléments de $\mathbb{F}_p$ non tous nuls . On aurait alors

$$s_m = a'_{m-1}\underline{s}_{m-1} + \ldots + a'_0\underline{s}_0 .$$

Ce qui est en contradiction avec l'indépendance linéaire des vecteurs $\underline{s}_0, \underline{s}_1, \ldots, \underline{s}_{k-1}$ sur $\mathbb{F}_p$. Donc F(x) est un polynôme minimal.

II.1.2. LEMME .

Soient $n \geq 0$ et $r > 0$ deux entiers et $(s) = \{s_n\}$ une suite sur $\mathbb{F}_p$. Alors

$$H_r^{(n)}(s) = H_{r+1}^{(n)}(s) = 0$$

implique $H_r^{(n+1)}(s) = 0$.

DEMONSTRATION . C'est une conséquence immédiate de la relation (3) .

II.1.3. THEOREME.

Une suite $(s) = \{s_n\}$ sur $\mathbb{F}_p$ est une suite récurrente linéaire homogène sur $\mathbb{F}_p$ si et seulement s' il existe un entier $r > 0$ tel que $H_r^{(n)} = 0$ pour tous les entiers naturels n sauf peut être pour un nombre fini d'entre eux.

DEMONSTRATION .

condition nécessaire.

On suppose que $(s) = \{s_n\}$ vérifie une relation de récurrence linéaire homogène d'ordre k sur $\mathbb{F}_p$. Alors pour tout entier $n \geq 0$, le déterminant $H_{k+1}^{(n)}(s)$ est nul, car les vecteurs d'état $\underline{s}_0, \underline{s}_1, \ldots, \underline{s}_{n+k-1}$ qui constituent les lignes de ce déterminant sont linéairement dépendants sur $\mathbb{F}_p$. On peut donc prendre pour valeur de r l'entier k+1.

condition suffisante .

Soit $t > 0$ le plus petit entier naturel tel que $H_t^{(n)} = 0$ pour tous les entiers naturels n sauf peut être pour un nombre fini d'entre eux . Si $t = 0$ alors la condition suffisante est trivialement vérifiée . On suppose donc $t > 0$. Alors il existe un entier naturel m tel que $H_t^{(n)} = 0$ pour tout $n \geq m$. Si on avait $H_{t-1}^{(n_0)} = 0$ pour un entier $n_0 \geq m$, alors d'après le lemme II.1.2., on aurait $H_{t-1}^{(n)} = 0$ pour tout $n \geq n_0$, ce qui est en contradiction avec la définition de t et par conséquent $H_{t-1}^{(n)} \neq 0$ pour tout entier $n \geq m$.
Pour $n \geq m$, on considère le système d'équations linéaires suivant :

$$\begin{cases} a_0 s_n + a_1 s_{n+1} + \cdots + a_{t-2} s_{n+t-2} = -s_{n+t-1} \\ a_0 s_{n+1} + a_1 s_{n+2} + \cdots + a_{t-2} s_{n+t-1} = -s_{n+t} \\ \qquad\qquad \vdots \\ a_0 s_{n+t-2} + a_1 s_{n+t-1} + \cdots + a_{t-2} s_{n+2t-4} = -s_{n+2t-3} \end{cases}$$

où les inconnues sont $a_0, a_1, \ldots, a_{k-1}$ et les coefficients $s_n, \ldots, s_{n+2t-4}$. Le déterminant des coefficients $H_{t-1}^{(n)}$ étant non nul, ce système possède une solution unique $(a_0, a_1, \ldots, a_{t-2})$ dans $\mathbb{F}_p^{t-1}$. Mais $H_t^{(n)} = 0$ pour tout $n \geq m$. Donc

$$a_0 s_{n+t-1} + a_1 s_{n+t} + a_{t-2} s_{n+2t-3} = -s_{n+2t-2}, \quad \forall\, n \geq m.$$

En définitive on a :

$$a_0 s_n + a_1 s_{n+1} + a_{t-2} s_{n+t-2} = -s_{n+t-1}, \quad \forall\, n \geq m.$$

ou encore

$$a_0 s_{n+m} + a_1 s_{n+m+1} + a_{t-2} s_{n+m+t-2} = -s_{n+m+t-1}, \quad \forall\, n \geq 0.$$

Ainsi la suite $(s) = \{s_n\}$ vérifie une relation de récurrence linéaire homogène d'ordre $m + t - 1$.

C.Q.F.D.

On maintenant en mesure d'énoncer un théorème qui, partant des N (N étant un entier assez grand) premiers termes d'une suite récurrente linéaire homogène sur $\mathbb{F}_p$, permet de retrouver théoriquement le degré du polynôme minimal de cette suite .

II.2. DECRYPTAGE THEORIQUE DE K

II.2.1 THEOREME

Soit $(s) = \{s_n\}$ une suite récurrente linéaire homogène sur $\mathbb{F}_p$ de polynôme minimal F(x) . Alors F(x) est de degré k si et seulement si

$$(7) \qquad H_r^{(0)} = 0 , \quad \forall\, r \geq k+1$$

et $(k + 1)$ est le plus petit entier naturel pour lequel on a (7) .

DEMONSTRATION.

condition nécessaire

Si tous les termes de la suite (s) sont nuls alors la condition nécessaire est trivialement vérifiée. On suppose donc k strictement positif. Alors la relation

$$H_r^{(0)} = 0 , \qquad \forall\, r \geq k+1$$

découle immédiatement du fait que la (k+1) ième ligne de $H_r^{(0)}$ est une combinaison linéaire sur $\mathbb{F}_p$ des k premières lignes . De plus d'après le théorème II.1.1., on a $H_k^{(0)} \neq 0$. Donc la condition nécessaire est démontrée dans tous les cas.

condition suffisante

On suppose que la condition sur les déterminants de Hankel est satisfaite. Alors en utilisant le lemme II.1.2. et en raisonnant par récurrence sur n, on établit que

$$H_r^{(n)} = 0, \quad \forall\, r \geq k+1 \quad \text{et } n \geq 0.$$

En particulier $H_{k+1}^{(n)} = 0$ pour tout $n \geq 0$ et on déduit du théorème II.1.3. que la suite (s) est une suite récurrente linéaire homogène. Soit d le degré du polynôme minimal de cette suite . D' après la démonstration de la condition nécessaire on a

$$H_{k+1}^{(0)} = 0, \forall\, r \geq d+1$$

où (d+1) est le plus petit entier naturel non nul pour lequel cette relation est vérifiée ; donc k = d .

C.Q.F.D.

III CALCUL DES DETERMINANTS DE HANKEL ET CONJECTURE SUR LE DECRYPTAGE PRATIQUE DE L'ORDRE ET DU MODULO D'UNE CONGRUENCE LINEAIRE

Comme pour la recherche des coefficients optimaux, un programme a été ecrit dans le système REDUCE pour calculer la table H des déterminants de Hankel. La souplesse de manipulation des grands entiers dans ce système revêt ici une importance particulière pour les deux raisons suivantes.

-- En général, on ne connaît pas à l'avance l'ordre de grandeur d'un déterminant de Hankel.

-- Lors du calcul des PGCD des déterminants de chacune des colonnes de la table H, nous avons trouvé un PGCD ayant 123 chiffres décimaux.

Des résultats de la mise en oeuvre de l'algorithme de calcul de H pour un certain nombre de suites récurrentes linéaires homogènes d'ordre k et de modulo M, pour différentes valeurs de k et de M premier, nous avons déduit la conjecture ci-après.

CONJECTURE

Soit $(s) = \{s_n\}$ une suite engendrée par une congruence linéaire homogène d'ordre k, $k \geq 1$, de modulo M premier et de période τ " suffisamment grande ". Si IDC désigne le nombre d'éléments de la dernière colonne de la table H et si le nombre d'éléments NBE1C de la colonne d'indice 1 est "assez grand", alors k est le plus petit entier tel que le PGCD de la colonne d'indice k+j soit M^j, pour tout $j \geq 1$ et ce jusqu'à la colonne d'indice IDC ou jusqu'à la colonne d'indice $k+j_1$, où $k + j_1 + 1$ est le plus petit indice de la colonne à partir de laquelle on a la dégénérescence de toutes les autres colonnes de la table H : nous disons qu'une colonne est dégénérée lorsque tous ses éléments sont nuls. De plus le nombre minimum Nombmin des déterminants visités sur chacune de ces colonnes pour avoir ce PGCD est en "moyenne" égal à 5.

REMARQUE

Dans l'énoncé de la conjecture nous avons mis les expressions "suffisamment grande " et "assez grand" entre griffes parce que nous n'étions pas en mesure de donner l'ordre de grandeur de τ et de NBE1C. L'analyse des exemples suivants nous permettra d'avoir une petite idée sur ces ordres de grandeurs.

ANALYSE DE QUELQUES EXEMPLES D'ILLUSTRATION DE LA CONJECTURE

La stratégie générale adoptée pour le choix des exemples consiste à se donner l'ordre k_1 et le modulo M de la congruence, à fixer ensuite les coefficients et à faire varier les termes initiaux.

Le message de la première ligne du premier exemple indique qu'on est dans le système REDUCE. Sur les trois lignes suivantes apparaissent les noms des 21 procédures constituant le programme du calcul de la table H. Dans les 9 autres exemples, nous avons supprimé ces 4 premières lignes et nous avons commencé par l'appel de la procedure principale "Chankel ".

Pour les quatre premiers exemples, k_1 est identique à 1 et M vaut 101. Dans les exemples 1 et 2 le coefficient est 2 et dans les deux exemples suivants il est égal à 15. Dans chacun des 4 cas la période est 100. D'autre part la valeur 50 attribuée à NBE1C a été suffisante pour obtenir les résultats annoncés dans la conjecture. Dans les exemples 5, 6, 7 et 8, k_1 vaut 3 et M est égal à 2^{35}-31. Nous remarquons que si les exemples 7 et 8, où les coefficients sont fixés à 13, 15 et 17, confirment la conjecture il n'en est pas de même pour les exemples 5 et 6 où les coefficients sont 2, 0, 1. Aussi avons nous repris les exemples 5 et 6 en modifiant la valeur de NBE1C : de 50 elle est passée à 90. Nous avons ainsi obtenu les exemples 9 et 10 avec les résultats escomptés. Cette anomalie est une illustration du problème du choix de la valeur de NBE1C : elle doit être "suffisamment grande". Par ailleurs on note dans les exemples 9 et 10 que la valeur de Nombmin s'écarte nettement de la valeur annoncée dans la conjecture. Cette anomalie sur la valeur de Nombmin et le problème rencontré dans les exemples 5 et 6 s'expliquent par l'apparition au début de la colonne d'indice 3 d'un bloc H de largeur r assez grande.

Quant au problème de l'ordre de grandeur de la période τ on peut l'illustrer par l'exemple extrême, où la suite $(s) = \{s_n\}$ est une suite constante. Dans ce cas il est clair que la colonne d'indice 2 est dégénérée et quelque soit le choix de NBE1C la conjecture est toujours fausse. Un autre exemple d'illustration de ce problème est donné par :

$k_1 = 4$, $M = 2$, $(a_0, a_1, a_2, a_3) = (s_0, s_1, s_2, s_3) = (1, 1, 0, 1)$.

Ainsi dans cet exemple la suite $(s) = \{s_n\}$, vérifiant la congruence

$$s_{n+4} = s_{n+3} + s_{n+1} + s_n \mod 2$$

est de période 3. La table H corresppondant à cette suite dégénère à partir de la colonne d'indice 4, pour toute valeur de NBE1C. En particulier pour NBE1C égal à 50 les colonnes 1, 2, 3 et 4 sont données par :

H_1 = (1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1).

H_2 = (-1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1, -1, -1, 1).

H_3 = (-2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2, -2).

H_4 = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0).

Au vu de nos expériences, il est possible d'entrevoir une conjecture à l'aide des PGCD des déterminants de Hankel de colonnes de H lorsque M est une puissance d'un nombre premier et même lorsque M est quelconque. Mais ces expériences sont insuffisantes pour poser une telle conjecture.

LISTE DES EXEMPLES

Exemple 1

```
REDUCE 3.3, 1-Aug-88 ...
CTCOL3 MISJMAT LIRE CHANKEL EXTRACT NOMBMINPGCD CTCOL2
COMPLET CA2 CTCOL1 DONNEE TNBLOC TRONL NBHC1 NBHC2 CA1
CTSUIV DETECT H12 H0123 RAISON
CHANKEL ( );
Entrer l'ordre k1 de la récurrence: k1=1,2,...
1
 Entrer le nombre d'écart(s) E3: E3=0,1,...
0
 Entrer le nombre de facteur(s) de M
1
 Entrer le facteur de M
101
 Entrer l'exposant du facteur de M
1
 La valeur de M  est 101
```

Entrer le nombre de facteur(s) du terme additif
1
Entrer le facteur du terme additif
0
Entrer l'exposant du facteur du terme additif
1
La valeur du terme additif est 0

Entrer l'indice IDC et le nombre d'éléments de la dernière colonne de

la table H

6 40
Entrer le coefficient A de la récurrence:A=1,2,... 100
2
Entrer la valeur initiale d'indice 0
2
Le PGCD des éléments de la colonne H1 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 7

Le PGCD des éléments de la colonne H2 est 101

Le nombre minimum des éléments visités pour avoir ce PGCD est 6

Le PGCD des éléments de la colonne H3 est 10201

Le nombre minimum des éléments visités pour avoir ce PGCD est 5

Le PGCD des éléments de la colonne H4 est 1030301

Le nombre minimum des éléments visités pour avoir ce PGCD est 4

Le PGCD des éléments de la colonne H5 est 104060401

Le nombre minimum des éléments visités pour avoir ce PGCD est 3

Le PGCD des éléments de la colonne H6 est 10510100501

Le nombre minimum des éléments visités pour avoir ce PGCD est 2

Voulez_vous continuer ?

Si oui entrer l'entier 1 suivi d'un point virgule

Sinon entrer l'entier 0 suivi d'un point virgule

0;

Time : 25.625

Exemple 2

```
CHANKEL ();

Entrer l'ordre k1 de la récurrence : k1 = 1, 2, ...
1
 Entrer le nombre d'écart(s)  E3 : E3 = 0, 1, ...
0
 Entrer le nombre de facteur(s) de M
1
 Entrer le facteur de M
101
 Entrer l'exposant du facteur de M
1
 La valeur de M  est 101

 Entrer le nombre de facteur(s) du terme additif
1
 Entrer le facteur du terme additif
0
 Entrer l'exposant du facteur du terme additif
1
 La valeur du terme additif  est 0

Entrer l'indice IDC et le nombre d'éléments de la dernière colonne de

la table H

6 40

 Entrer le coefficient A de la récurrence : A = 1, 2, ... 100
2
 Entrer la valeur initiale d'indice 0
13
Le PGCD des éléments de la colonne H1 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD  est 4

Le PGCD des éléments de la colonne H2 est 101

Le nombre minimum des éléments visités pour avoir ce PGCD  est 3

Le PGCD des éléments de la colonne H3 est 10201

Le nombre minimum des éléments visités pour avoir ce PGCD  est 2

Le PGCD des éléments de la colonne H4 est 1030301

Le nombre minimum des éléments visités pour avoir ce PGCD  est 7

Le PGCD des éléments de la colonne H5 est 104060401

Le nombre minimum des éléments visités pour avoir ce PGCD  est 6

Le PGCD des éléments de la colonne H6 est 10510100501

Le nombre minimum des éléments visités pour avoir ce PGCD  est 5
```

Voulez_vous continuer ?

Si oui entrer l'entier 1 suivi d'un point virgule

Sinon entrer l'entier 0 suivi d'un point virgule
0;

Time : 19.731

Exemple 3

CHANKEL ();

Entrer l'ordre k1 de la récurrence : k1 = 1, 2, ...
1
Entrer le nombre d'écart(s) E3 : E3 = 0, 1, ...
0
Entrer le nombre de facteur(s) de M
1
Entrer le facteur de M
101
Entrer l'exposant du facteur de M
1
La valeur de M est 101

Entrer le nombre de facteur(s) du terme additif
1
Entrer le facteur du terme additif
0
Entrer l'exposant du facteur du terme additif
1
La valeur du terme additif est 0

Entrer l'indice IDC et le nombre d'éléments de la dernière colonne de

la table H

6 40

Entrer le coefficient A de la récurrence : A = 1,2,... 100
15
Entrer la valeur initiale d'indice 0
2

Le PGCD des éléments de la colonne H1 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 6

Le PGCD des éléments de la colonne H2 est 101

Le nombre minimum des éléments visités pour avoir ce PGCD est 5

Le PGCD des éléments de la colonne H3 est 10201

Le nombre minimum des éléments visités pour avoir ce PGCD est 4

Le PGCD des éléments de la colonne H4 est 1030301

Le nombre minimum des éléments visités pour avoir ce PGCD est 6

Le PGCD des éléments de la colonne H5 est 104060401

Le nombre minimum des éléments visités pour avoir ce PGCD est 5

Le PGCD des éléments de la colonne H6 est 10510100501

Le nombre minimum des éléments visités pour avoir ce PGCD est 4

Voulez_vous continuer ?

Si oui entrer l'entier 1 suivi d'un point virgule

Sinon entrer l'entier 0 suivi d'un point virgule
0;

Time : 14.441

Exemple 4

chankel ();

Entrer l'ordre k1 de la récurrence : k1=1, 2, ...
1
entrer le nombre d'écart(s) E3 : E3 = 0, 1, ...
0
Entrer le nombre de facteur(s) de M
1
Entrer le facteur de M
101
Entrer l'exposant du facteur de M
1
La valeur de M est 101

Entrer le nombre de facteur(s) du terme additif
1
Entrer le facteur du terme additif
0
Entrer l'exposant du facteur du terme additif
1
La valeur du terme additif est 0

Entrer l'indice IDC et le nombre d'éléments de la dernière colonne de

la table H

6 40

Entrer le coefficient A de la récurrence : A = 1,2, ... 100
15
Entrer la valeur initiale d'indice 0
13
Le PGCD des éléments de la colonne H1 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 2

Le PGCD des éléments de la colonne H2 est 101

Le nombre minimum des éléments visités pour avoir ce PGCD est 3

Le PGCD des éléments de la colonne H3 est 10201

Le nombre minimum des éléments visités pour avoir ce PGCD est 2

Le PGCD des éléments de la colonne H4 est 1030301

Le nombre minimum des éléments visités pour avoir ce PGCD est 2

Le PGCD des éléments de la colonne H5 est 104060401

Le nombre minimum des éléments visités pour avoir ce PGCD est 4

Le PGCD des éléments de la colonne H6 est 10510100501

Le nombre minimum des éléments visités pour avoir ce PGCD est 3

Voulez_vous continuer ?

Si oui entrer l'entier 1 suivi d'un point virgule

Sinon entrer l'entier 0 suivi d'un point virgule
0;

Time : 14.537

Exemple 5

Chankel ();

Entrer l'ordre k1 de la récurrence : k1 = 1, 2, ...
3
Entrer le nombre d'écart(s) E3 : E3 = 0,1, ...
0
Entrer le nombre de facteur(s) de M
1
Entrer le facteur de M

34359738337

Entrer l'exposant du facteur de M
1
La valeur de M est 34359738337

Entrer le nombre de facteur(s) du terme additif
1
Entrer le facteur du terme additif
0
Entrer l'exposant du facteur du terme additif
1
La valeur du terme additif est 0

Entrer l'indice IDC et le nombre d'éléments de la dernière colonne de

la table H

```
6 40

Entrer les 3 coefficients Ai de la récurrence par

ordre d'indice croissant :  Ai = 0, 1, 2, ... 34359738336
 2 0 1

 Entrer la valeur initiale d'indice 0
1
 Entrer la valeur initiale d'indice 1
2
 Entrer la valeur initiale d'indice 2
1
Le PGCD des éléments de la colonne H1 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD  est 1

Le PGCD des éléments de la colonne H2 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD  est 2

Le PGCD des éléments de la colonne H3 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD  est 44

Le PGCD des éléments de la colonne H4 est 34359738337

Le nombre minimum des éléments visités pour avoir ce PGCD  est 44

Le PGCD des éléments de la colonne H5 est 1237940037051594860731039744

Le nombre minimum des éléments visités pour avoir ce PGCD  est 42

Le PGCD des éléments de la colonne H6 est

42371415762523327209500686974606998180043161 6

Le nombre minimum des éléments visités pour avoir ce PGCD  est 40

Voulez_vous continuer ?

Si oui entrer l'entier 1 suivi d'un point virgule

Sinon entrer l'entier 0 suivi d'un point virgule
0;

Time : 13.298

          Exemple 6

CHANKEL ();

Entrer l'ordre k1 de la récurrence :  k1=1, 2, ...
3
Entrer le nombre d'écart(s) E3 :  E3 = 0,1, ...
0
 Entrer le nombre de facteur(s) de M
1
```

```
 Entrer le facteur de M

34359738337

 Entrer l'exposant du facteur de M
1
 La valeur  De M  est 34359738337
 Entrer le nombre de facteur(s) du terme additif
1
 Entrer le facteur du terme additif
0
 Entrer l'exposant du facteur du terme additif
1
 La valeur  Du terme additif  est 0

Entrer l'indice IDC et le nombre d'éléments de la dernière colonne de

la table H

6 40

Entrer les 3 coefficients Ai de la récurrence par

ordre d'indice croissant : Ai = 0,1, 2, ... 34359738336
 2 0 1
 Entrer la valeur initiale d'indice 0
1
 Entrer la valeur initiale d'indice 1
3
 Entrer la valeur initiale d'indice 2
1
Le PGCD des éléments de la colonne H1 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD  est 1

Le PGCD des éléments de la colonne H2 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD  est 46

Le PGCD des éléments de la colonne H3 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD  est 45

Le PGCD des éléments de la colonne H4 est 34359738337

Le nombre minimum des éléments visités pour avoir ce PGCD  est 44

Le PGCD des éléments de la colonne H5 est 990352029641275888585848317952

Le nombre minimum des éléments visités pour avoir ce PGCD  est 42

Le PGCD des éléments de la colonne H6 est

1427247688842891021793707350723604149222506496

Le nombre minimum des éléments visités pour avoir ce PGCD  est 40

Voulez_vous continuer ?
```

Si oui entrer l'entier 1 suivi d'un point virgule

Sinon entrer l'entier 0 suivi d'un point virgule
0;

Time : 13.588

Exemple 7

CHANKEL ();

Entrer l'ordre k1 de la récurrence : k1 = 1,2, ...
3
Entrer le nombre d'écart(s) E3 : E3 = 0,1, ...
0
Entrer le nombre de facteur(s) de M
1
Entrer le facteur de M

34359738337

Entrer l'exposant du facteur de M
1
La valeur de M est 34359738337

Entrer le nombre de facteur(s) du terme additif
1
Entrer le facteur du terme additif
0
Entrer l'exposant du facteur du terme additif
1
La valeur du terme additif est 0

Entrer l'indice IDC et le nombre d'éléments de la dernière colonne de

la table H

6 40

Entrer les 3 coefficients Ai de la récurrence par

ordre d'indice croissant : Ai = 0,1, 2,... 34359738336

13 15 17

Entrer la valeur initiale d'indice 0
1
Entrer la valeur initiale d'indice 1
3
Entrer la valeur initiale d'indice 2
1

Le PGCD des éléments de la colonne H1 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 1

Le PGCD des éléments de la colonne H2 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 9

Le PGCD des éléments de la colonne H3 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 8

Le PGCD des éléments de la colonne H4 est 34359738337

Le nombre minimum des éléments visités pour avoir ce PGCD est 7

Le PGCD des éléments de la colonne H5 est 1180591618587107525569

Le nombre minimum des éléments visités pour avoir ce PGCD est 6

Le PGCD des éléments de la colonne H6 est

405648190975083202202343770387 53

Le nombre minimum des éléments visités pour avoir ce PGCD est 5

Voulez_vous continuer ?

Si oui entrer l'entier 1 suivi d'un point virgule

Sinon entrer l'entier 0 suivi d'un point virgule
0;

Time : 13.690

Exemple 8

chankel ();

Entrer l'ordre k1 de la récurrence: k1=1, 2, ...
3
Entrer le nombre d'écart(s) E3 : E3 = 0, 1, ...
0
Entrer le nombre de facteur(s) de M
1
Entrer le facteur de M

34359738337

Entrer l'exposant du facteur de M

1

La valeur de M est 34359738337

Entrer le nombre de facteur(s) du terme additif

1

Entrer le facteur du terme additif

0

Entrer l'exposant du facteur du terme additif

1

La valeur du terme additif est 0

Entrer l'indice IDC et le nombre d'éléments de la dernière colonne de

la table H

6 40

Entrer les 3 coefficients Ai de la récurrence par

ordre d'indice croissant : Ai = 0, 1, 2, ... 34359738336

13 15 17

Entrer la valeur initiale d'indice 0

7

Entrer la valeur initiale d'indice 1

5

Entrer la valeur initiale d'indice 2

3

Le PGCD des éléments de la colonne H1 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 2

Le PGCD des éléments de la colonne H2 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 9

Le PGCD des éléments de la colonne H3 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 8

Le PGCD des éléments de la colonne H4 est 34359738337

Le nombre minimum des éléments visités pour avoir ce PGCD est 7

Le PGCD des éléments de la colonne H5 est 1180591618587107525569

Le nombre minimum des éléments visités pour avoir ce PGCD est 6

Le PGCD des éléments de la colonne H6 est

405648190975083202202343770387 53

Le nombre minimum des éléments visités pour avoir ce PGCD est 5

Voulez_vous continuer ?

Si oui entrer l'entier 1 suivi d'un point virgule

Sinon entrer l'entier 0 suivi d'un point virgule

0 ;

Time : 13.716

Exemple 9

Chankel ();

Entrer l'ordre k1 de la récurrence: k1=1, 2, ...
3
Entrer le nombre d'écart(s) E3 : E3 = 0,1, ...
0
Entrer le nombre de facteur(s) de M
1
Entrer le facteur de M

34359738337

Entrer l'exposant du facteur de M
1
La valeur de M est 34359738337

Entrer le nombre de facteur(s) du terme additif
1
Entrer le facteur du terme additif
0
Entrer l'exposant du facteur du terme additif
1
La valeur du terme additif est 0

Entrer l'indice IDC et le nombre d'éléments de la dernière colonne de

la table H

6 80

Entrer les 3 coefficients Ai de la récurrence par

ordre d'indice croissant : Ai = 0,1,2, . .. 34359738336

2 0 1

Entrer la valeur initiale d'indice 0
1
Entrer la valeur initiale d'indice 1
2
Entrer la valeur initiale d'indice 2
1

Le PGCD des éléments de la colonne H1 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 1

Le PGCD des éléments de la colonne H2 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 2

Le PGCD des éléments de la colonne H3 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 44

Le PGCD des éléments de la colonne H4 est 34359738337

Le nombre minimum des éléments visités pour avoir ce PGCD est 44

Le PGCD des éléments de la colonne H5 est 1180591618587107525569

Le nombre minimum des éléments visités pour avoir ce PGCD est 43

Le PGCD des éléments de la colonne H6 est

405648190975083202202343770387 53

Le nombre minimum des éléments visités pour avoir ce PGCD est 42

Voulez_vous continuer ?

Si oui entrer l'entier 1 suivi d'un point virgule

Sinon entrer l'entier 0 suivi d'un point virgule

0;

Time : 24.055

Exemple 10

chankel ();

Entrer l'ordre k1 de la récurrence : k1=1,2, ...
3
Entrer le nombre d'écart(s) E3 : E3 = 0,1, ...
0
Entrer le nombre de facteur(s) de M
1
Entrer le facteur de M

34359738337

Entrer l'exposant du facteur de M
1
La valeur de M est 34359738337

Entrer le nombre de facteur(s) du terme additif
1
Entrer le facteur du terme additif

0
Entrer l'exposant du facteur du terme additif
1
La valeur du terme additif est 0

Entrer l'indice IDC et le nombre d'éléments de la dernière colonne de

la table H

6 80

Entrer les 3 coefficients Ai de la récurrence par

ordre d'indice croissant : Ai = 0,1,2,... 34359738336

2 0 1

Entrer la valeur initiale d'indice 0
1
Entrer la valeur initiale d'indice 1
3
Entrer la valeur initiale d'indice 2
1

Le PGCD des éléments de la colonne H1 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 1

Le PGCD des éléments de la colonne H2 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 46

Le PGCD des éléments de la colonne H3 est 1

Le nombre minimum des éléments visités pour avoir ce PGCD est 45

Le PGCD des éléments de la colonne H4 est 34359738337

Le nombre minimum des éléments visités pour avoir ce PGCD est 44

Le PGCD des éléments de la colonne H5 est 1180591618587107525569

Le nombre minimum des éléments visités pour avoir ce PGCD est 43

Le PGCD des éléments de la colonne H6 est

405648190975083202202343770387 53

Le nombre minimum des éléments visités pour avoir ce PGCD est 42

Voulez_vous continuer ?

Si oui entrer l'entier 1 suivi d'un point virgule

Sinon entrer l'entier 0 suivi d'un point virgule

0;

Time : 24.820

REMARQUE

On note que dans la conjecture, nous nous sommes intéressés uniquement aux suites récurrentes linéaires homogènes. Ceci n'est pas une perte de généralité , car on montre sans peine (cf. R. Lidl and H. Niederreiter (1983)) qu'une suite récurrente linéaire non homogène d'ordre k , vérifie une récurrence linéaire homogène d'ordre k+1.

Lors d'une tentative éventuelle de démonstration de notre conjecture, on pourra utiliser le théorème suivant.

THEOREME (cf. J. B. PLUMSTEAD(1982))

Soient a, b et c trois entiers quelconques. Alors on a

PGCD(ab, c) = PGCD(a, c) PGCD(b, c/PGCD(a,c)).

BIBLIOGRAPHIE

[1] AFFLERBACH L . (1986). The sub-lattice structure of linear congruential random number generators. Manuscripta Math. 55, pp. 455- 465.

[2] AFFLERBACH L . and GROTHE, H. (1985). Calculation of Minkowski -reduced lattice bases. Computing 35, pp. 269 -276.

[3] AFFLERBACH L . and GROTHE, H. (1988). The lattice structure of pseudo-random vectors generated by matrix generators . J. Computational and Applied Mathematics . 23, pp. 127-131.

[4] BAUVAL A . (1986). Cryptanalysis of pseudo-random number sequences generated by a linear congruential recurrence of given order. Centre Nationale d'Etude des Télécommunications , Paris.

[5] BERLINET A . (1985). Sequence transformations as statistical tools. Applied Numerical Mathematics. 1, pp. 531-544.

[6] BEYER, W . A . (1972). Lattice structure and reduced bases of random vectors generated by linear recurrences. In Applications of Number Theory to Numerical Analysis. Ed. Zaremba, S. K.

[7] BEYER W. A. , ROOF R. B. and WILLIAMSON D. (1971). The lattice structure of multiplicative congruential pseudo-random vectors. Mathematics of Computation. Vol. 25. n ° 114.

[8] BLUM L. , BLUM M. and SHUB M. (1986). A simple impredictible pseudo-random number generator. S.I.A.M. J. Comput. Vol. 15 n° 2.

[9] BLUM M . and MICALI S. (1984). How to generate cryptographically strong sequences of pseudo-random bits. S.I.A.M. J.Comp. Vol. 13. n°4 pp. 850-864.

[10] BOROSH I. and NIEDERREITER H. (1983). Optimal multipliers for pseudo-random number generation by the linear congruential method. BIT. 23, pp. 65-74.

[11] BOYAR J. (1989). Inferring sequences produced by pseudo-random number generators. J. A. C. M. vol. 36 n° 1, pp. 129-141.

[12] CASSELS J. W. S. (1959). An introduction to the geometry of numbers. Springer -verlag.

[13] CASSELS J. W. S. (1978). Rational quadratique forms. Academic Press.

[14] COHEN H. (1980-1981). Test de primalité d'après Adleman, Rumely, Pomerance et Lenstra. Séminaire de la théorie des nombres à l'Université de Grenoble.

[15] COVEYOU R.R. and MACPHERSON R. D. (1967). Fourier analysis of uniform random number generators . J. A. C. M. Vol. 14 n°1, pp. 100-119.

[16] DAYKIN D. E. (1963). On linear sequences over a finite field. American Mathematical Monthly 70, pp. 637 -642.

DIETER U.

[17] * (1971). Pseudo-random numbers : the exact distribution of pair. Mathematics of Computation 25, pp. 855-884.

[18] * (1972) Statistical Interdependance of Pseudo-Random Numbers generated by the Linear Congruential Method. In Application of Number Theory to Numerical Analysis. ed. S. K. Zaremba.

[19] * (1975). How to calculate shortest vectors in a lattice. Mathematics of Computation Vol. 29, N°131, pp. 827-833.

[20] * (1985). Calculating shortest vectors in a lattice bericht n° 244.

[21] DRAUX A. (1981). Polynômes orthogonaux formels. Applications. Thèse d' état de l' Université des sciences et techniques de Lille .

[22] EICHENAUER J., GROTHE H. and LEHN J. (1988). Marsaglia 's lattice test and non -linear congrential pseudo-random number generators. Metrika, vol. 35, pp. 241-250.

[23] EICHENAUER - HERRMAN J ., GROTHE H. and LEHN J. (1989). On the period length of pseudo-random vector sequences generated by matrix generators. Mathematics of Computation vol. 52, n°185, pp. 145 -148.

[24] EICHENAUER J., GROTHE H. and TOPUZOGLU A. (1987). A multiple recursive non-linear congruential pseudo-random number generator. Manuscripta Math. 59, pp. 331-346.

[25] EICHENAUER J., LEHN J. (1986). A non - Linear Congruential Pseudo - Random Number Generator. Statistische Hefte 27, p. 315 - 326.

[26] EICHENAUER J., LEHN J., TOPUZOGLU A. (1988). A Nonlinear Congruential Pseudorandom Number Generator With Power of Two Modulus. Mathematics of Computation Volume 51, Number 184 October 1988, pp. 757 - 759.

[27] FINCKE U. and POHST M . (1985). Improved methods for calculating vectors of short length in a lattice including a complexity analysis . Mathematics of Computation Vol. 44, n° 170, PP. 463-471.

[28] GALPERIN E. A. (1978). Loop properties and controllability of linear congruential sequences . I. E. E. E. Transactions on Computers, VOL . C-27, n°1.

[29] HARDY, G. H., WRIGHT E. M. (1960). An introduction to the theory of numbers. 4ième édition oxford . Clarendon Press.

[30] JANSSON B. (1966). Random number generators. Victor Petterson's Bokindustriab, stockolm.

[31] KNUTH D. K. (1969). The art of computer programming, vol. 2 Semi-numerical algorithms Reading, Ma, Addison-Wesley 1ère édition.

[32] KNUTH D. K. (1981). The art of computer programming, vol. 2 semi-numerical algoritms Reading, MA, Addison-Wesley 2ième édition .

[33] KUIPERS L . and NIEDERREITER H. (1974). Uniform distribution of sequences . New-York Wiley-Interscience.

[34] LENSTRA A. K., LENSTRA H. W. and LOVASZ L .(1982). Factoring polynomials with rational coefficients. Math. Ann. 261, pp. 515-534.

[35] LEROUDIER J. (1980). La simulation à événements discrets . Edition Hommes et Techniques.

[36] LEWIS T. G. and PAYNE W. H. (1973). Generalized feedback shift register pseudo-random number algorithm. J.A.C.M. vol. 20 n°3, pp. 456-468.

[37] LIDL R. and NIEDERREITER H. (1983). Finite fields . Encyclopedia of Mathematics and its Applications vol. 20, Addison -Wesley Reading, Ma.

[38] LIDL R. and NIEDERREITER H. (1986). Introduction to finite fields and their applications . Cambridge University Press.

[39] MACLAREN, M. D. and MARSAGLIA G. (1965). Uniform random number generators, J.A.C.M. vol. 12, n°1, pp. 83-89.

[40] MARSAGLIA G. (1968). Random numbers fall mainly on the plane Proc. Nat. Acad. Sci. 60, pp. 25-28.

[41] MARSAGLIA G. (1972). The structure of Linear Congruential Sequences. In Application of Number Theory to Numerical Analysis. Ed. by S. K. Zaremba. Acad. Press. p. 249-285.

[42] MOUKOKO D. (1978). Conception des logiciels sur l' algorithme QD général. Applications. Thèse de l'Université des Sciences et Techniques de Lille.

[43] MULLEN, G. L . and NIEDERREITER H. (1987) . Optimal characteristic polynomials for digital multistep pseudo-random numbers. Computing 39, pp. 155-163 .

NIEDERREITER H.

[44] * (1974). Some new exponential sums with applications to pseudo-random numbers Colloquia Mathematica Societatis Janos Bolyar 13. Topics in number theory. Debrecen (Hungary).

[45] * (1976a). On the cycle structure of linear recurring sequences.Math. Scand. 38, pp. 53 -77.

[46] * (1976b). On the distribution of pseudo-random numbers generated by the linear congruential method III . Mathematics of Computation . Vol. 30 n° 135, pp. 571-597.

[47] * (1977). Pseudo-random numbers and optimal coefficients. Advances in Mathematics 26, pp.99-181.

[48] * (1978). Quasi-Monte Carlo methods and pseudo -random numbers . American Mathematical Society 84, pp. 957-1041.

[49] * (1982). Statistical tests for Tausworthe pseudo-random numbers. Probability and Statistical Inference, pp. 265-274.

[50] *(1982-1983) . Application des corps finis aux nombres pseudo-aléatoires Séminaire de la théorie des nombres de Bordeau, exposé n° 38.

[51] *(1984a) . Number-theoretic problems in pseudo- random number generation. Proc.symp. on Applications of Number Theory to Numerical Analysis, Kyoto. Lecture notes n° 537. Research Institut of Math.Sciences, Kyoto Universitry, pp. 18-28.

[52] * (1984b). The performance of k-step pseudo-random generators under the uniformity test .Siam . J. Sci. Stat. Comput. vol.5 n°4, pp. 798-810.

[53] *(1985). The serial test for pseudo-random numbers generated by the linear cogruential method. Numer.Math. 46. pp. 51-68.

[54] * (1986a). A statistical analysis of generalized feedback shift register pseudo-random number generators, preprint

[55] * (1986b). Pseudozufallszahlen und die theorie der gleichverteilung Sitzungsber Oterr. Akad .WIss .math. Naturnwiss K1.195. pp. 109-138

[56] *(1986c). A pseudo-random vector generator based on finite field arithmetic Math. Japonica 31, n°5, pp. 759-774.

[57] * (1986d). Dyadic fraction with small partial quotients. Monatsh. Math.101, pp. 309-315.

[58] *(1987a) . Point sets and sequences with small discrepancy. Monatsh. Math . 104, pp.273-337.

[59] * (1987b). Rational functions with partial quotients of small degre in their continued fraction expansion. Monatsh. Math. 103, pp. 269-288.

[60] * (1988a). Remarks on non-linear congruential pseudo-random numbers. Metrika, vol. 35, pp. 321-328.

[61] * (1988b) . Statistical Independance of nonlinear congruential pseudo - random numbers. Monatsh. Math. 106, 149-159.

[62] * (1988c). The serial test for digital k-step pseudo-random numbers . Mathematical journal of Okayama University, 30, pp. 93-119.

[63] *(1989). The serial test for congruential pseudo-random numbers generated by inversion . Mathematics of Computation .Vol. 52, n°185 pp.135-144.

[64] PARENT D.P.(1978) Exercices de théorie des nombres. Edit. Gauthier _ Villars.

[65] PESKUN P.H. (1980). Theoretical tests for choosing the parameters of the general mixed linear congruential pseudo-random number generator. J. Statist.Comput. Simul. vol.11, pp. 281-305.

[66] PLUMSTEAD J.B. (1982). Inferring a sequence generated by a linear congruence. In proceeding of the 23 rd I.E.E.E. Symposium on Foundation of Computer Science I.E.E.E. New-York, pp. 153-159.

[67] RYBOWICZ M. (1987). Implantation en lisp du cryptosystème de Chor et de Rivest. Rapport de D.E.A. en mathématiques appliquées. Université de Grenoble.

[68] SHAMIR A. (1980). On the generation of cryptographycally strong pseudo-random sequences 8th . International Colloquium on Automata Languages and Programming .

[69] THAMI E.H. (1982). Contribution aux générateurs de vecteurs pseudo-aléatoires Thèse du troisième cycle de l' Université Houari Boumedienne. Alger.

[70] TAUSWORTHE R. C. (1965). Random numbers generated by linear recurrence modulo two. Mathematics of Computation vol. 19, pp. 201-209.

[71] VALLEE B. (1986). Une approche géométrique de la réduction des réseaux en petite dimension. Thèse de doctorat de l'Université de caen

VAN CUTSEM B.

[72] * (1980). Etude de la période d'une suite de nombres pseudo-aléatoires engendrés par une congruence linéaire. Bulletin de l'Association des Professeurs de Mathématiques de l' Enseignement Public n° 324 .

[73] *(1985a). Itération des congruences linéaires et génération des nombres pseudo-aléatoires. Rapport de Recherche n°568 Laboratoire Tim3 Université de Grenoble.

[74] * (1985b) . Simulation des lois de probabilité . Statistiques et Analyse des Données. vol. 10 n°2 pp. 63-87

[75] WARD M. (1933) . The arithmetical theory of linear recurring series Trans. Amer. Math. Soc. 35. pp. 600-628.

ZAREMBA S. K.

[76] * (1966). Good Lattice points, discrepancy and numerical integration. Annali Di Mathematica Pura ed Applicata IV, 73, pp. 293-317.

[77] * (1972). Méthode des " bons treillis " pour le calcul des intégrales multiples. In Application of Number Theory to Numerical Analysis. Ed. S. K. Zaremba New-York Academic Press, pp. 39-119.

Résumé Dans un premier temps, nous utilisons la géométrie des grilles d'un espace euclidien réel pour tester les qualités d'une suite de Nombres Pseudo-Aléatoires (NPA) engendrée par une congruence linéaire simple (CLS). Ensuite, pour m et b fixés, nous nous intéressons à la recherche des multiplicateurs a tels que deux termes successifs d'une suite engendrée la CLS de paramètres a, b et m soient statistiquement indépendants. Mais du point de vue de la génération des NPA, les congruences linéaires multidimensionnelles(CLM) constituent en un certain sens une amélioration des CLS. De plus les qualités statistiques d'une suite de NPA engendrée par une CLM sont étroitement liées au choix du polynôme caractéristique associé à cette CLM. Aussi nous sommes nous intéressés à la recherche des polynômes caractéristiques optimaux. Par ailleurs la construction des vecteurs de NPA à partir d'un générateur de NPA est une méthode indirecte de génération de vecteurs pseudo-aléatoires et il est parfois plus avantageux d'utiliser une méthode directe. Ainsi nous avons introduit un générateur vectoriel basé sur le modèle de Daykin et une CLM de période maximale, puis nous avons considéré le choix des paramètres de ce modèle de telle sorte que ce générateur soit de période maximale. La deuxième et dernière partie de la thèse est réservée à la cryptographie. Nous faisons une conjecture sur le décryptage de l'ordre et du modulo d'une CLM à partir du calcul exact des déterminants de Hankel.

Mots Clés Congruences Linéaires, Nombres Pseudo-Aléatoires, Vecteurs Pseudo-aléatoires, Figure de Mérite, Générateur non Linéaire, Déterminants de Hankel, Cryptographie, Décryptage.