Rapport de Magistère

Louis Granboulan

Table des matières

Chapitre 1

Curriculum vitae

Louis Granboulan
né le 11 novembre 1971

École Normale Supérieure	
45 rue d'Ulm	22 rue de Tocqueville
75005 Paris	75017 Paris
(1) 46.33.82.39	*(1) 47.63.54.22*
`granboul@ens.fr`	

1990-1991 : première année ENS et MMFAI

Cours suivis :

Logique	(J. Stern)
Combinatoire énumérative I	(X.G. Viennot)
Intégration	(J.M. Coron)
Analyse complexe	(P. Gérard)
Analyse fonctionnelle	(Y. Brenier)
Probabilités I	(J.F. Le Gall)
Algèbre I	(D. Bertrand)
Algèbre II	(D. Perrin)
Groupes de Coxeter et algèbres de Hecke	(M. Cabanes)
Courbes et surfaces	(H. Rosenberg)
Géométrie différentielle	(J.P. Labesse)
Surfaces de Riemann	(D. Bennequin)
Programmation	(G. Cousineau)
Types abstraits de données et modularité	(G. Bernot & M. Bidoit)
Parallélisme et Synchronisation	(G. Vidal-Naquet)
Système UNIX	(R. Ehrlich)

Projet de programmation : *Circle Limit III et Kolams* (fait en commun avec A. Chambert-Loir et C. Lemaire ; sujet proposé par G. Cousineau.)

Exposé : *Jeux stochastiques à deux joueurs et à somme nulle* (fait en commun avec C. Lemaire ; sujet proposé par S. Sorin.)

Diplômes obtenus : licence et maîtrise de mathématiques pures à Paris VII.

1991-1992 : deuxième année ENS et MMFAI

DEA IMA.
Cours suivis :

Théorie des automates	(D. Perrin)
Algorithmique et complexité concrète	(C. Puech)
Planification de trajectoires en robotique	(J.P. Laumond)
Génie Logiciel	(M.C. Gaudel & G. Bernot)
Théorie algébrique des codes correcteurs	(P. Charpin)
Théorie algorithmique des nombres	(F. Morain)
Complexité	(C. Kenyon & M. Santha)
Fondements de la cryptographie moderne	(J. Stern & A. Shamir)
Procédés cryptographiques	(J.J. Quisquater)
Protocoles cryptographiques	(C. Crépeau)

Stage de DEA : *Étude d'algorithmes parallèles d'arithmétique sur machines parallèles. Implémentation sur Transputers* (sous la direction de M. Guillot, Thomson CSF)

Diplôme obtenu : DEA Informatique mathématique et Applications.

1992-1993 : troisième année ENS et MMFAI

Première année de thèse à Paris VII sous la direction de J. Stern (LIENS).

Participation aux Rencontres du troisième cycle de mathématiques, à Bordeaux. (14-15 décembre 1992).

Participation au séminaire et au groupe de travail hebdomadaires du GRECC. Exposés sur les articles suivants:

- *PP is closed under intersection*, Beigel, Reingold, Spielman, 1991.
- *Approximating clique is almost NP-complete*, Feige, Goldwasser, Lovász, Safra, Szegedy, 1991.
- *MAX 3DM is MAX-SNP complete*, Kann, 1991.
- *On the Hardness of Approximating Minimisation Problems*, Lund, Yannakakis, 1992.
- *A Well-Characterized Approximation Problem*, Håstad, Phillips, Safra, 1993.

Participation au congrès EUROCRYPT en Norvège. (23-27 mai 1993).

Agrégation de mathématiques.

1993-1994 : quatrième année ENS

Deuxième année de thèse.

Participation aux 18$^{\text{èmes}}$ journées arithmétiques à Bordeaux. (13-17 septembre 1993).

Rencontres sur la Complexité, Codage et Cryptographie de Cargèse. (11-15 octobre 1993).

Chapitre 2

Présentation de mes activités

1 Du coté des mathématiques

Puisque j'ai toujours préféré les mathématiques à la physique et que le rythme de vie du M.I.P. était trop scolaire et régulier, je n'ai pas beaucoup hésité à m'inscrire au M.M.F.A.I. à mon arrivée à l'École.

Pour ne pas oublier qu'il existe aussi d'autres domaines que mathématique ou informatique, je suivais en dilettante le cours de Mécanique Quantique d'É. Brézin, jusqu'à ce que la théorie sous-jacente me paraisse trop loin de ce qui me semblait être des mathématiques un minimum rigoureuses. J'ai donc restreint mes études à ce qui me semblait beau, c'est à dire surtout l'algèbre et la géométrie.

Puisqu'on nous proposait pendant la première année de Magistère de choisir parmi une multitude de cours, j'en profitai pour assister à la première séance de chacun des cours, afin de déterminer lesquels m'inspiraient. C'est comme ça que j'ai été amené à suivre certains cours d'analyse dont le titre m'aurait dégoûté.

Deux cours m'ont suffisamment marqué pour qu'aujourd'hui encore je travaille sur des problèmes assez proches : le cours de D. Perrin sur la théorie de Galois et le cours de D. Bennequin sur les Surfaces de Riemann. La théorie de Galois est une de ces théories mathématiques permettant d'adapter certains concepts généraux à plusieurs familles d'objets ; ce sont à mon avis les plus belles théories. La théorie des surfaces de Riemann et des courbes elliptiques en particulier est une autre de ces théories à cheval sur plusieurs domaines. Mais si j'appréciais le cours de Bennequin, j'avais l'impression d'en comprendre très peu. On voit donc que je considère les Mathématiques un peu comme un art et que me sentant capable d'admirer ces œuvres mais pas de les créer, j'ai préféré orienter mon travail vers l'informatique.

2 Du coté de l'informatique

Comme beaucoup de passionnés de mathématiques, j'aime jouer ou concevoir des jeux. C'est ainsi que j'ai pris contact avec le monde des ordinateurs.

De même, j'aimais le principe des codes secrets, avec le jeu du concepteur du code et de l'attaquant cherchant à résoudre le problème posé par un code.

C'est pour ça que je me suis tout naturellement tourné vers la filière Algorithmique, Complexité, Cryptographie du DEA Informatique Mathématique et Applications. La cryptographie est une discipline présentant de nombreux visages. Il y a l'aspect bricolage, où le but est de proposer des astuces ou des algorithmes pour résoudre divers problèmes, ou à montrer que les algorithmes proposés par d'autres ne résistent pas à une attaque bien organisée. Il y a aussi l'aspect fondamental, les preuves que certains problèmes ne peuvent être résolus, ou que d'autres problèmes peuvent être calculés en utilisant certaines ressources informatiques. De plus, la cryptographie moderne est dans sa majorité fondée sur des principes liés à la théorie des nombres.

ce qui me permettait de ne pas renier l'algèbre.

Puisque le DEA IMA laissait le choix de deux cours hors cursus, j'ai choisi de suivre le cours de J.P. Laumond sur la robotique, pour ne pas oublier le peu que j'avais appris en géométrie, et le cours de M.C. Gaudel et G. Bernot sur le génie logiciel, puisque je savais que j'aurais à faire des programmes efficaces, à ne pas me contenter du peu d'informatique que j'avais appris sur le tas.

Quant au stage de DEA, je désirais qu'il soit dans une entreprise, ce qui est possible pour un informaticien et qui permet de découvrir un univers assez différent de celui de la rue d'Ulm. Thomson proposait un stage d'étude d'algorithmes d'arithmétique sur machine parallèle. Les machines parallèles m'intéressaient et j'avais suivi le cours de parallélisme de G. Vidal-Naquet. Comme l'arithmétique m'a toujours plu, j'ai donc apprécié ce stage.

3 Mélange de mathématique et informatique

Après un DEA, il est courant d'envisager de préparer un doctorat et ce que j'avais vu l'année précédente du milieu de la recherche m'a motivé pour demander à Jacques Stern de m'accepter comme thésard.

J'ai donc commencé, dans le cadre du GRECC, à travailler sur quelques problèmes issus de la théorie de la complexité, en continuant à étendre ma culture mathématique. J'ai fait connaissance avec les "anciens" du groupe de recherche et je me suis intéressé à leurs travaux : j'ai donc regardé les applications des algorithmes de réduction de réseau avec Antoine Joux, en particulier les attaques des problèmes construits sur les sacs à dos (Ch. 7). J'ai aussi cherché avec Jean-Marc Couveignes à calculer explicitement des dessins d'enfants (Ch. 8) et à résoudre certaines instances du problème de Galois inverse. On trouve aussi dans ce rapport un début d'étude que j'avais faite, pour essayer de construire des protocoles cryptographies fondés sur la difficulté de résoudre un problème d'énoncé simple (Ch. 6).

Cette première année de thèse a donc été l'occasion de travailler sur divers sujets, afin de cerner mes compétences et mes préférences. Il s'est avéré que ma formation batarde, à cheval entre les mathématiques les plus abstraites et l'informatique du "hacker", me permet d'aborder certains problèmes sous un jour peut-être nouveau.

Chapitre 3

Projet : Une œuvre d'Escher en CAML

Antoine Chambert-Loir
Louis Granboulan
Clotilde Lemaire

Avril 1991

Sujet proposé par G. Cousineau

L'objet de cet article est d'expliquer comment la gravure *Circle Limit III* du peintre néerlandais Escher a été reproduite par ordinateur. Ce travail a été réalisé dans le cadre du cours de programmation de première année du Magistère de Mathématiques et Informatique à l'École Normale Supérieure. La programmation a été faite à l'ENS sur un ordinateur Sun 4/490 avec stations de travail Sparc 1 et 1+, dans le langage CAML, qui est un langage fonctionnel conçu à l'INRIA.

Cette œuvre trouve une explication mathématique dans la géométrie hyperbolique et la théorie des groupes de pavages.

1 Éléments de géométrie hyperbolique

Présentons tout d'abord le plan hyperbolique.

Il possède plusieurs modèles mathématiques, mais celui qui nous intéresse est le disque unité ouvert D de $\mathbf{C}$ muni de la métrique $\mu(x) = \frac{1}{1 - x\bar{x}}$. Cela signifie que, si z et z' sont deux points de D, la distance de z à z' est donnée par

$$d_\mu(z, z') = \inf_\gamma \int_0^1 \mu(\gamma(t))\, |\gamma'(t)|\, dt,$$

où la borne inférieure est prise sur tous les chemins $\gamma\ : [0,1] \to D$, de classe au moins $\mathcal{C}^1$ tels que $\gamma(0) = z$ et $\gamma(1) = z'$.

Muni de cette métrique, D est une variété riemannienne dont les isométries directes sont exactement les bijections holomorphes $D \to D$. Un théorème d'analyse complexe permet alors d'expliciter ces isométries : ce sont les *homographies* de la forme

$$h_{a,\lambda} : z \mapsto \lambda \frac{z + a}{1 + \bar{a} z},$$

a et λ étant des nombres complexes vérifiant $|a| < 1$ et $|\lambda| = 1$.

Les géodésiques de D sont les intersections avec D des droites passant par l'origine 0 et les cercles orthogonaux au disque unité $U = \partial D$.

Si les distances sont modifiées par rapport à le géométrie euclidienne, il est important de remarquer que les angles sont les mêmes car une application biholomorphe est *conforme* c'est à dire conserve les angles. Comme au voisinage de 0, la géométrie de D et de $\mathbf{C}$ coïncident, puisque $\mu(0) = 1$, les angles sont correctement transportés par les isométries de D.

On définit la rotation hyperbolique $r_{a,\theta}$ de centre a et d'angle θ comme la transportée de la rotation euclidienne de centre 0 et d'angle θ par l'isométrie $h_{a,1}$:

$$r_{a,\theta} = h_{a,1} \circ r_{0,\theta} \circ h_{a,1}^{-1}.$$

La particularité du plan hyperbolique par rapport au plan euclidien usuel est d'être un espace à *courbure négative*. Cela implique que la somme des angles d'un triangle géodésique est strictement inférieure à π. Réciproquement, étant donnés trois réels α, β et γ strictement positifs et de somme strictement inférieure à π, il existe un triangle géodésique dont les angles soient α, β et γ.

2 Un pavage du plan hyperbolique

Un groupe de pavage de D est la donnée d'un groupe G d'isométries du plan hyperbolique et d'une partie fermée P de D appelée *domaine fondamental* de D pour G vérifiant les propriétés suivantes

π–1. La famille $\{g(P) \mid g \in G\}$ est localement finie, c'est à dire que seul un nombre fini de ses éléments intersectent un compact donné de D.

π–2. Les $g(P)$ sont deux à deux d'intérieur disjoints.

π–3. La réunion des $g(P)$ est égale à D.

Soient alors n, p et q trois entiers strictement positifs tels que la somme $1/n + 1/p + 1/q$ est strictement inférieure à 1. Il existe un triangle géodésique $T = abc$ dont les angles sont π/n, π/p et π/q. Considérons les rotations hyperboliques A, B et C de centres a, b et c et d'angles $2\pi/n$, $2\pi/p$ et $2\pi/q$. Désignons par G le sous-groupe des isométries de D engendré par A, B et C. Une présentation de G est

$$A^n = B^p = C^q = ABC = 1.$$

Alors le fait fondamental est que la réunion du triangle T et du symétrique par rapport à de ses côtés est un domaine fondamental pour le groupe G ce qui procure des pavages du plan hyperbolique à volonté !

On remarque qu'on peut, étant donné un tel pavage par un quadrilatère, en obtenir une infinité d'autres en déformant partiellement les côtés du quadrilatère de sorte que le nouveau domaine P soit encore un domaine fondamental pour le groupe G.

Dans le cas qui nous concerne, $(n, p, q) = (3, 3, 4)$. La présentation du groupe s'écrit

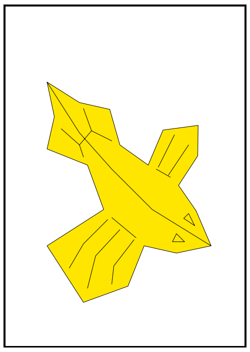
$$A^3 = B^3 = C^4 = ABC = 1 \tag{3.1}$$

Le triangle T est donné par

$$a = \left(1 + \sqrt{2}\right)^{-1/2} e^{i\pi/8} \qquad b = \bar{a} \qquad c = 0. \tag{3.2}$$

Le motif P choisi par Escher est un poisson.

Le domaine fondamental.



3 Un peu de réécriture

Pour représenter tous les poissons, on a choisi de générer les éléments du groupe G correspondant au pavage $(3,3,4)$. Formellement, il faut construire des mots de taille croissante formés à partir des générateurs A, B, C de notre groupe. Cependant, il existe des relations entre ces générateurs et créer simplement des mots entraîne immédiatement des redondances. Par exemple, une génération naïve ne distingue pas AAA et 1 qui sont pourtant égaux en vertu de la présentation 3.1. Il nous a paru nécessaire d'éviter ce fait pour plusieurs raisons, un principe esthétique déjà qui nous à poussés à améliorer cette solution; mais un souci d'efficacité surtout car la solution naïve implique une explosion combinatoire et, les objets informatiques que l'on manipulera étant assez lourds, la mémoire risque de faire rapidement défaut. Le même principe vaut aussi pour le fichier PostScript produit par notre programme: les imprimantes Laser Writer supportant assez mal les “gros” fichiers.

La première phase du programme consiste ainsi en un calcul formel. On cherche des règles de réécriture qui donnent aux éléments du groupe $(3,3,4)$ une forme normale unique. Après plusieurs essais infructueux qui donnaient des paires critiques en cascade, nous avons tiré profit de la thèse de P. Le Chenadec ([1]) dans laquelle ce genre de problème est étudié. La solution de notre problème s'y trouvait explicitement, page 151, dans le catalogue de règles de réécriture que ses méthodes ont engendrées.

Un élément du groupe est considéré comme une `elt list`, le type `elt` étant défini comme

```
type elt = 'A | 'B | 'C | 'a | 'b | 'c;;
```

où les minuscules représentent les inverses des générateurs correspondants, qu'il est utile d'introduire. L'algorithme de réduction en forme normale a été programmé, mais en fait n'est pas utilisé. Seule est utilisée une fonction qui décide si son argument est irréductible ou non, ce qui est un peu plus simple. Enfin la fonction `genere` crée, étant donné un entier n, une `elt list list` qui correspond à la liste des éléments du groupe qui s'écrivent à l'aide de moins de n symboles du type `elt`.

4 Graphisme

Les graphismes sont réalisés à l'aide de la librairie graphique CAML-Graphics réalisée par G. Cousineau et E. Chailloux. On gère des objets CAML assez complexes de type `picture` et `sketch`. Ensuite, ils sont traduits en PostScript par la librairie. Le fichier PostScript créé est, ou bien imprimé, ou bien visualisé sur l'écran à l'aide des programmes PAGEVIEW ou GHOSTSCRIPT.

Le poisson fondamental est codé comme une suite de points. Pour tracer l'image d'un poisson,nous avons jugé préférable de ne tracer que des segments de droite entre les points images. C'est un compromis convenable entre l'effet visuel et la taille dess objets informatiques manipulés...

Certains points du poisson sont arbitraires et leur choix n'a qu'une importance esthétique.

	A	B	C
Jaune	Rouge	Rouge	Vert
Vert	Jaune	Vert	Jaune
Rouge	Vert	Bleu	Bleu
Bleu	Bleu	Jaune	Rouge

Action des générateurs sur les couleurs

En revanche beaucoup d'autres sont uniquement déterminés par les précédents, si l'on veut obtenir un pavage du plan hyperbolique. Précisément, 20 points déterminent le contour du poisson; les quatre points `p0`, `p5`, `p10` et `p15` sont des sommets de triangles du pavage $(3, 3, 4)$; les huit points `p1`, `p2`, `p3`, `p4`, `p11`, `p12`, `p13` et `p14` définissent une forme de poisson qu'on espère harmonieuse; enfin, les huit autres points se déduisent des précédents par des rotations hyperboliques connues.

Les points `q1` à `q17` et `r1` à `r15` décrivent les entrailles du poisson : dos, nageoires, queue et yeux.

Mais la gravure d'Escher est en couleur, l'ensemble réalisant même un coloriage parfait, c'est-à-dire que deux poissons adjacents ne sont pas de la même couleur. Mathématiquement, les éléments du groupe de pavage $(3, 3, 4)$ agissent sur les quatre couleurs Jaune, Vert, Rouge et Bleu comme des permutations. On a même un morphisme de G dans le groupe $\mathfrak{S}_4$ des permutations des quatre couleurs de base.

Il suffit donc de regarder comment agissent les générateurs A, B et C sur le groupe grâce au tableau de la figure 2.

5 Artifices

Les couleurs originales n'ont pas été respectées pour permettre aux quatre couleurs de ressortir après impression N&B sur la Laser Writer.

On pourra remarquer que le poisson fondamental n'est pas au centre de la figure. Cela a pour conséquence que, sans artifice supplémentaire, les images produites sont dissymétriques. Pour éviter ceci, la fonction `esc` qui calcule l'image est dotée de deux arguments :

• `d` agit comme un filtre, car seuls les poissons situés à l'intérieur du disque de centre 0 et de rayon d sont affichés.

• `n` est la longueur maximale des éléments du groupe que l'on a à considérer.

Remerciements. Nous tenons à remercier Emmanuel Chailloux pour ses multiples conseils et encouragements, Catherine Delor et François Fages pour l'aide qu'ils nous ont apportée dans la recherche d'algorithmes de réduction et Guy Cousineau pour nous avoir proposé ce sujet intéressant, situé aux frontières de l'informatique, des mathématiques et de l'art.

Bibliographie

[1] Philippe Le Chenadec, *Formes canoniques dans les algèbres finiment présentées. Thèse de troisième cycle.*

[2] R. et A. Douady, Algèbre et théories galoisiennes, tome 2. Cedic/Fernand Nathan.

[3] H. S. M. Coxeter, The non euclidean symmetry of Escher's picture 'Circle Limit III'. Leonardo, Vol. 12, pp. 19-25, (1979).

[4] M.C. Escher : Art and Science. Edited by H.S.M. Coxeter, M. Emmer, R. Penrose and M.L. Teuber. North Holland.

Chapitre 4

Exposé : Jeux stochastiques à deux joueurs et à somme nulle

Louis Granboulan
Clotilde Lemaire

1991

Sujet proposé par S. Sorin

La théorie des jeux, imaginée par Borel, fondée par Von Neumann et Morgenstern, doit son importance au fait qu'elle permet de traiter certaines situations de conflits militaires ou économiques. Toutefois, c'est dans les situations de jeu proprement dit qu'on trouve les exemples à la fois les plus simples et les plus purs du point de vue de la concordance entre la théorie et la réalité (cette dernière restant à définir). Le jeu est dit stochastique car le temps et différents états vont intervenir. Un jeu statique pouvant toujours être interprété comme un jeu stochastique à un seul état, joué en une seule étape.

1 Jeux matriciels

Définition 1.1 *On appelle "jeu à deux joueurs à somme nulle, sous forme normale", un triplet:*

$$(X, Y, g)$$

où X et Y sont des ensembles et $g : X \times Y \to \mathbb{R}$.

X et Y sont les **ensembles de stratégie**, g est le **paiement** qu'on interprétera comme le gain (algébrique) du joueur dont l'ensemble des stratégies est X (qu'on appellera joueur I) ou comme la perte (algébrique) du joueur II.
Une **partie** s'effectue de la façon suivante : les deux joueurs choisissent simultanément des stratégies $x \in X$, $y \in Y$ de façon à maximiser leurs gains.

1.1 Stratégie optimale

Considérons un jeu (X, Y, g). I veut maximiser $g(x, y)$ mais il a le choix seulement de x. Il cherchera donc à maximiser $g(x, y)$ le mieux possible **indépendamment** de y. Pour cela, I considère, pour chaque x son gain minimum, i.e.

$$\inf_{y \in Y} g(x, y)$$

Cet inf ne dépend que de x, donc I en dispose. I peut alors jouer une stratégie optimale $\overline{x}$ qui maximise cet inf, à ε près i.e.

$$\inf_{y\in Y} g(\overline{x},y) \geqslant \sup_{x\in X}\inf_{y\in Y} g(x,y) - \varepsilon \stackrel{def}{=} \underline{v} - \varepsilon$$

Une telle stratégie $\overline{x}$ est dite ε-optimale pour I car cette façon de jouer lui garantit un gain minimal égal à $\underline{v}-\varepsilon$. $\underline{v}$ est appelée valeur inférieure du jeu.
Car

$$\forall y \in Y \quad \underline{v} - \varepsilon \leqslant g(\overline{x},y)$$

D'une manière symétrique, on définit pour II une stratégie ε-optimale, ainsi que la valeur supérieure du jeu $\overline{v}$. On a:

$$\forall x \in X \quad g(x,\overline{y}) \leqslant \overline{v} + \varepsilon$$

Bien sûr,

$$\underline{v} \leqslant \overline{v}$$

1.2 Equilibre ou point-selle

Si $\underline{v} = \overline{v} = v$, on dit que v est la **valeur** du jeu.
Dans le cas où le jeu a une valeur, et où il existe des stratégies optimales $\overline{x}$ et $\overline{y}$, on a:

$$\forall x \in X \;\; \forall y \in Y \quad g(x,\overline{y}) \leqslant v \leqslant g(\overline{x},y)$$

et donc:

$$\forall x \in X \;\; \forall y \in Y \quad g(x,\overline{y}) \leqslant g(\overline{x},\overline{y}) \leqslant g(\overline{x},y)$$

Un couple de stratégies $(\overline{x},\overline{y})$ vérifiant cette dernière inégalité est appelé **point-selle** de g.

Théorème 1.1 – *Si un jeu a une valeur, tout couple de stratégies optimales est un point selle de g et la valeur de g en un point selle est la valeur du jeu.*

– *Reciproquement si $(\overline{x},\overline{y})$ est un point-selle de g alors, le jeu a une valeur $v = g(\overline{x},\overline{y})$, $\overline{x}$ et $\overline{y}$) sont des stratégie optimales.*

Définition 1.2 *On appelle jeu matriciel (ou jeu fini), un jeu à deux joueurs à somme nulle et sous forme normale où X et Y sont des ensembles* ***finis****.*

Un tel jeu est entièrement défini par la matrice des gains $A = (a_{ij})$ avec $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant m$ et où $a_{ij} = g(x_i, x_j)$ si $X = \{x_1,\ldots,x_n\}$ et $Y = \{y_1,\ldots,y_m\}$. a_{ij} représente donc le gain de I (ou la perte de II) si I adopte sa $i^{ème}$ stratégie et II sa $j^{ème}$ stratégie.

Remarque :
Si $\underline{v} < \overline{v}$, pour tout couple de stratégies optimales $(\overline{x},\overline{y})$ on peut seulement écrire $\underline{v} \leqslant g(\overline{x},\overline{y}) \leqslant \overline{v}$ avec au moins une des deux inégalités strictes. Si par exemple $\underline{v} = \inf_{y\in Y} g(\overline{x},y) \leqslant g(\overline{x},\overline{y}) < \overline{v}$ alors I peut améliorer son gain en choisissant convenablement une autre stratégie que $\overline{x}$ et ainsi ruser son adversaire.
Pour éliminer le rôle de la ruse et de l'espionnage dans le cas des jeux sans valeur, E. Borel a introduit la notion de **stratégie mixte**.

1.3 Stratégie mixte (cas des jeux matriciels)

Considérons l'ensemble (fini) des stratégies de I: $X = \{x_1,\ldots,x_n\}$.
Soit p une distribution de probabilité sur X: $p = \{p_1,\ldots,p_n\}$ avec $p_i \geqslant 0, i = 1,\ldots,n$ et $\sum_{i=1}^{n} p_i = 1$.
Soit P l'ensemble de toutes les probabilités sur X. Par définition, le vecteur $p \in P$ est une stratégie mixte du joueur I. Par opposition, une stratégie $x_i \in X$ sera aussi appelée stratégie

pure. Evidemment $X \subset P$.
On définit de la même façon l'ensemble Q des stratégies mixtes de II et $Y \subset Q$.
On dit que le joueur I adopte la stratégie mixte p s'il adopte une stratégie pure au hasard dans X en assignant à x_i la probabilité p_i. Cette façon d'opérer rend inefficace la perspicacité de l'adversaire, car le meilleur moyen de le déjouer, c'est d'ignorer soi-même ce que l'on va faire jusqu'au moment de la décision.

1.4 Théorème de Von-Neumann

Théorème 1.2 *Un jeu matriciel en stratégies mixtes a toujours une valeur et des stratégies optimales, i.e.*

$$\exists v \quad \exists p \in P \quad \exists q \in Q$$

$$\forall j \in \{1, \dots, m\} \quad \sum_{i=1}^{n} p_i a_{ij} \geqslant v$$

$$\forall i \in \{1, \dots, n\} \quad \sum_{j=1}^{m} a_{ij} q_j \leqslant v$$

$$p_i \geqslant 0, \quad q_j \geqslant 0, \quad \sum_{i=1}^{n} p_i = 1, \quad \sum_{j=1}^{m} q_j = 1$$

Preuve : [Owen(1967)]
Soit $a = \max_{ij} |a_{ij}|$, $u(p) = \min_j \ p^t A^j$, $w(q) = \max_i \ A_i q$, où A^j (resp. A_i) désigne la $j^{ème}$ colonne (resp. $i^{ème}$ ligne de A).
Posons:

$$\underline{v} = \max_{p \in P} \ u(p)$$

$$\overline{v} = \min_{q \in Q} \ w(q)$$

Par compacité, on a l'existence de $\underline{v}$ et $\overline{v}$. Clairement $\underline{v} \leqslant \overline{v}$.
La démonstration du théorème se fait par récurrence sur la taille de A.

- Le théorème est trivial pour $n = 1$ et $m = 1$.

- Supposons le résultat acquis pour toute sous-matrice A' de A et raisonnons par l'absurde.
  On suppose donc que $\underline{v} < \overline{v}$. Prenons p et q tel que $u(p) = \underline{v}$ et $w(q) = \overline{v}$.
  On a $\underline{v} \leqslant p^t A q \leqslant \overline{v}$ avec une des deux inégalités qui est **stricte**.
  Supposons que: $p^t A q < \overline{v}$.
  Il existe alors un k tel que $A_k q = \overline{v} - \rho$ où $\rho > 0$.
  Considérons A' la matrice obtenue en supprimant la $k^{ème}$ ligne de A, l'hypothèse de récurrence donne l'existence de $v, p' \in P$, avec $p'_k = 0, q' \in Q$, tels que $\min_j \ {p'}^t A^j = \max_{i \neq k} \ A_i q' = v \leqslant a$.
  Posons maintenant $p'' = (1 - \alpha)p + \alpha p'$, $q'' = (1 - \alpha)q + \alpha q'$, où $0 < \alpha < \frac{\rho}{a - v + \rho}$.
  Évidemment, $p'' \in P$ et $q'' \in Q$.
  Et nous avons:

$$\min_j \ p''^t A^j \geqslant (1 - \alpha)\underline{v} + \alpha v$$

$$\max_{i \neq k} \ A_i q'' \leqslant (1 - \alpha)\overline{v} + \alpha v$$

  tandis que:

$$A_k q'' \leqslant (1 - \alpha)(\overline{v} - \rho) + \alpha a < (1 - \alpha)\overline{v} + \alpha v$$

  Ainsi:

$$u(p'') \geqslant (1 - \alpha)\underline{v} + \alpha v$$

$$w(q'') \leqslant (1-\alpha)\overline{v} + \alpha v$$

Par suite:

$$\overline{v} - \underline{v} \leqslant w(q'') - u(p'') \leqslant (1-\alpha)(\overline{v} - \underline{v}) < \overline{v} - \underline{v}$$

Contradiction avec la définition de $\overline{v}$ ou $\underline{v}$. De la même manière, on obtient une contradiction si on suppose que $\underline{v} < pA^t q$. D'où:

$$\underline{v} = \overline{v}$$

Exemple : La valeur du jeu suivant est 1

$$\begin{pmatrix} 1 & 2 \\ 0 & 0,5 \end{pmatrix}$$

Car I peut obtenir au moins 1 en jouant en haut et II peut donner au plus 1 en jouant à gauche. La valeur du jeu

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

est $v = \frac{ad-bc}{(a+d)-(b+c)}$. (En effet $v = ax + (1-x)c = xb + (1-x)d$)

2 Jeux sur le carré et Théorème de Ville

Une classe importante de jeu infini est celle où l'ensemble des stratégies pures de chacun des deux joueurs a la puissance du continu et peut être représenté par l'intervalle [0;1].
Le paiement est une fonction définie sur [0;1] $\times$ [0;1] à valeurs réelles notée $A(x,y)$ et habituellement continue.
Comme pour les jeux finis, une stratégie mixte est une distribution de probabilité sur l'ensemble des stratégies pures. Elle peut alors être représentée comme une fonction de répartition i.e. comme une fonction F, définie sur [0;1] vérifiant

1. $F(0^-) = 0$
2. $F(1) = 1$
3. F croissante
4. F continue à gauche

Si le joueur I utilise la stratégie pure x, alors que II utilise la stratégie mixte G, l'espérance du paiement est l'intégrale de Stieltjes

$$E(x,G) = \int_0^1 A(x,y)dG(y)$$

Mais si II utilise la stratégie pure y et si I utilise la stratégie mixte F, le paiement attendu est

$$E(F,y) = \int_0^1 A(x,y)dF(x)$$

Sous l'hypothèse d'existence des intégrales et de la validité de Fubini, si I utilise F et si II utilise G

$$E(F,G) = \int_0^1 \int_0^1 A(x,y)dF(x)dG(y)$$

et évidemment

$$E(F,G) = \int_0^1 E(F,y)\ dG(y) = \int_0^1 E(x,g)\ dF(x)$$

Comme pour les jeux finis, nous pouvons définir

$$\underline{v} = \sup_F \ \inf_y E(F,y) \qquad \overline{v} = \inf_G \ \sup_x E(x,G)$$

- Deux questions se posent
  - $\underline{v} = \overline{v}$?
  - Peut-on remplacer sup inf (resp. inf sup) par max min (resp. min max)?
- Dans l'affirmative, des stratégies mixtes optimales existent. Si elles peuvent être trouvées, le jeu sera aussi bien déterminé qu'un jeu fini.
  (Si on a seulement $\underline{v} = \overline{v}$, le jeu a une valeur et des stratégies ε-optimales.

Théorème 2.1 *Si la fonction de paiement $A(x,y)$ est globalement continue,* sup inf *(resp.* inf sup*) peut être remplacé par* max min *(resp.* min max*).*

Preuve : $A(x,y)$ est continue, donc pour tout F, la fonction

$$E(F,y) = \int_0^1 A(x,y)dF(x) \text{ est continue en } y$$

[0;1] est compact, donc $E(F,y)$ y atteint son minimum.
sup inf peut donc être remplacé par sup min.
Par définition de $\underline{v}$, pour n donné, il existe une distribution de probabilité F_n telle que

$$\min_y E(F_n,y) > \overline{v} - \frac{1}{n}$$

De plus, l'ensemble des fonctions de [0;1] sur [0;1] est un espace relativement séquentiellement compact pour la convergence simple (utiliser l'extraction diagonale). La suite $(F_n)_{n\in N}$ admet une sous suite convergente de limite notée F_0. Il est clair que $F_0(0^-) = 0$, $F_0(1) = 1$, F_0 croissante. En revanche, F_0 n'est pas nécessairement continue à gauche (car ce n'est pas le type de propriété préservée à la limite). Définissons donc $\tilde{F}_0$ par

$$\tilde{F}_0 = \begin{cases} 0 & \text{si } x = 0 \\ F_0(x^+) & \text{si } 0 < x < 1 \\ 1 & \text{si } x = 1 \end{cases}$$

Il est clair que $\tilde{F}_0$est bien une stratégie. F_0 et $\tilde{F}_0$ ne diffèrent que par leurs points de discontinuité. Comme ces fonctions sont monotones, ces points de discontinuité forment un ensemble dénombrable. Ainsi, pour tout y

$$\int_0^1 A(x,y)d\tilde{F}_0(x) = \int_0^1 A(x,y)dF_0(x)$$

La fonction $A(x,y)$ est uniformément continue, F_0 est limite d'une sous-suite de $(F_n)_n$. Par suite

$$\int_0^1 A(x,y)dF_0(x) = \lim_{n\to\infty} \int_0^1 A(x,y)dF_n(x)$$

d'où

$$E(\tilde{F}_0,y) = \lim_{n\to\infty} E(F_n,y)$$

Par suite

$$\min_y E(\tilde{F}_0,y) \geqslant \underline{v}$$

Ainsi $\tilde{F}_0$ donne le maximum désiré.

De la même façon, on montre que inf sup peut être remplacé par min max.

Théorème 2.2 *Si la fonction de paiement $A(x,y)$ est continue, alors $\underline{v} = \overline{v}$ et le jeu sur le carré a une valeur.*

PREUVE : Par discrétisation.
Soit n un entier donné. Considérons la matrice $(n+1) \times (n+1)$ A_n de terme général (a_{ij}^n) où

$$(a_{ij}^n) = A(\frac{i}{n}, \frac{j}{n}) \quad i, j = 0, \ldots, n$$

Pour chaque $n^{ème}$ jeu défini par la matrice A_n, le théorème de Von Neumann donne l'existence de sa valeur v_n et l'existence de stratégies optimales $r_n = (r_0^n, \ldots, r_n^n)$ (resp. $s_n = (s_0^n, \ldots, s_n^n)$) pour I (resp. II).
La fonction $A(x, y)$ est uniformément continue sur $[0;1]^2$. Soit $\varepsilon > 0$, il existe $\delta > 0$ tel que

$$\sqrt{(x-x')^2 + (y-y')^2} < \delta \Rightarrow |A(x,y) - A(x', y')| < \varepsilon$$

Prenons n suffisamment grand pour que $\frac{1}{n} < \delta$
Considérons la stratégie F_n définie par

$$F_n(x) = \sum_{i=0}^{\lfloor nx \rfloor} r_i^n$$

(on a bien $F_n(0^-) = 0, F_n(1) = 1, \ldots$)
Soit y dans $[0;1]$, prenons $j = \lfloor ny \rfloor$. Alors

$$E(F_n, \frac{j}{n}) = \sum_{i=0}^{n} a_{ij}^n r_i^n > v_n \qquad (\star)$$

Or $\left|y - \frac{j}{n}\right| < \delta$, donc

$$\left|A(x,y) - A(x, \frac{j}{n})\right| < \varepsilon$$

et donc

$$\left|E(F_n, y) - E(F_n, \frac{j}{n})\right| < \varepsilon$$

soit $E(F_n, y) > v_n - \varepsilon$
Ceci est vrai pour tout y de $[0;1]$. Par suite

$$\underline{v} > v_n - \varepsilon$$

De la même manière on montre que

$$\overline{v} < v_n + \varepsilon$$

De ces deux inégalités, on déduit que $\underline{v} > \overline{v} - 2\varepsilon$.
Or, comme $\underline{v} \leqslant \overline{v}$ et que ε est arbitraire, on en déduit que $\underline{v} = \overline{v}$.
De $(\star)$, on déduit

$$v = \underline{v} \geqslant \limsup_{n \to \infty} v_n$$

et comme on a aussi

$$v = \overline{v} \leqslant \liminf_{n \to \infty} v_n$$

on en déduit

$$v = \lim_{n \to \infty} v_n$$

Remarquons, que les stratégies F_n peuvent approcher la stratégie optimale d'aussi près qu'on peut le désirer.
Si la fonction de paiement est très lisse ou aplatie, une petite valeur de n sera suffisante pour une bonne approximation. En revanche, si elle est très irrégulière une bonne approximation demandera une grande valeur de n.

Autre preuve Formons des grilles de pas $\frac{1}{2^n}$.
Pour chacun de ces jeux, le théorème de Von Neumann donne l'existence de sa valeur v_n et de stratégies optimales, distributions de probabilité sur les 2^n+1 points. Soit $(F_n)_{n\in\mathbb{N}}$ la suite de fonctions de répartition ainsi obtenue. L'ensemble des fonctions de [0;1] sur [0;1] étant relativement séquentiellement compact pour la convergence simple, la suite $(F_n)_{n\in\mathbb{N}}$ admet une sous suite convergente de limite F_0. Quitte à redéfinir $\tilde{F}_0$ comme ci-dessus, on a une fonction croissante. à valeur dans [0;1], continue à gauche, définie sur les rationnels, donc définie et continue partout.
La fonction de paiement est uniformément continue, soit δ son module de continuité; sur un pas carré, l'erreur est au plus δ, donc en intégrant sur le carré, on fait une erreur de l'ordre de ε.

3 Jeux stochastiques finis à deux joueurs et à somme nulle

Un tel jeu Γ est défini par la donnée de

- un ensemble non vide fini K (espace des états).
- un ensemble non vide fini X, resp. Y (espace des actions du joueur I, resp. II).
- une fonction de paiement g, à valeurs réelles, définie sur $K\times X\times Y$ et bornée.
- une probabilité de transition Q (qui associe à chaque triplet (k,x,y) une probabilité $Q(.|k,x,y)$ sur K.
- une probabilité initiale P sur K.

3.1 Définitions

Règle du jeu

Une partie se déroule en plusieurs étapes.
Un état initial $k\in K$ est choisi selon la probabilité P. Les deux joueurs choisissent simultanément et indépendamment une action. Le joueur I reçoit $g(k,x,y)$ et le jeu passe à l'état suivant l selon la probabilité $Q(l|k,x,y)$ et l'on passe à l'étape suivante...

Définition 3.1 *Une histoire (resp. une partie) est une suite finie (resp. infinie) d'éléments de $K\times X\times Y$ et l'ensemble correspondant sera noté H (resp.H_∞)*
H_n est le sous ensemble de H des histoires "en n étapes".

Définition 3.2 *Une stratégie pure pour le joueur I est une fonction de H dans X spécifiant après chaque histoire l'action à sélectionner.*

L'ensemble des stratégies pures noté S (resp. T) de I (resp. II) — produit d'ensembles finis — est un espace compact pour la topologie produit lorsque chaque facteur est muni de la topologie discrète.

Définition 3.3 *Une stratégie pure est dite stationnaire si l'action qu'elle détermine ne dépend que de l'état courant.*

Définition 3.4 *Une stratégie mixte est une probabilité sur l'ensemble des stratégies pures.*

L'ensemble des stratégies mixtes du joueur I (resp. II) sera noté Σ (resp. $\mathcal{T}$). $\Sigma=\mathcal{M}_+^1(S)$, ensemble des probabilités de Radon sur S est un compact du dual de $\mathcal{C}(S)$ (espace de Banach des fonctions continues) sur S pour la topologie faible-$\star$.

3.2 Trois classes de jeux stochastiques

jeu fini Γ_n Le paiement du jeu est l'espérance mathématique de la moyenne arithmétique des paiements des n premières étapes et est noté

$$\overline{\gamma}_n(\sigma,\tau) = E_{\sigma,\tau}(\overline{g}_n) \text{ où } \overline{g}_n = \frac{1}{n}\sum_{p=1}^{n} g_p$$

jeu escompté Γ_λ Le paiement du jeu est l'espérance mathématique de la moyenne géométrique de la suite infinie et est noté

$$\overline{\gamma}_\lambda(\sigma,\tau) = E_{\sigma,\tau}(\overline{g}_\lambda) \text{ où } \overline{g}_\lambda = \sum_{p=1}^{\infty} \lambda(1-\lambda)^{p-1} g_p \quad \lambda \in]0;1]$$

où $g_p = g(k_p, x_p, y_p)$. $\overline{g}_\lambda$ est bien définie. En effet les fonctions de paiement g_n sont uniformément bornées en x et y et $(1-\lambda)^{p-1}$ tend vers 0 lorsque p tend vers ∞. Interprétation : À chaque état deux possibilités se présentent : la première, avec une probabilité λ, est d'entrer dans un état absorbant donc de garder le même état et de ne plus recevoir de paiement jusqu'à la fin du jeu et la seconde, avec une probabilité $(1-\lambda)$, et de continuer le jeu.

Pour Γ_n et Γ_λ, la fonction de gain est continue pour la topologie produit donc $\overline{\gamma}_\lambda(\sigma,\tau)$ et $\overline{\gamma}_n(\sigma,\tau)$ sont continues par rapport à σ et à τ pour la topologie faible-$\star$.

jeu infini Γ_∞ Le paiement est pris comme la limite des $\overline{g}_n$ et différentes définitions sont possibles. En effet, cette limite peut ne pas exister, et dans ce cas on peut prendre la limite inf ou la limite sup ou toute autre limite. Dans ce cas, on s'intéresse à des propriétés uniformes (stratégies optimales, par exemple).

3.3 Étude de Γ_n et Γ_λ

Théorème 3.1 *Les jeux Γ_n (resp. Γ_λ) ont une valeur v_n (resp. v_λ) et des stratégies optimales.*

PREUVE :

1. Pour Γ_n, les ensembles K, X, Y sont finis donc le jeu Γ_n peut s'écrire comme un jeu matriciel sous forme normale à une étape dont l'ensemble des stratégies possibles du joueur I (resp. II) est X^{H^n} (resp. Y^{H^n}). Le théorème de Von-Neumann donne alors l'existence de v_n et de stratégies mixtes optimales pour les deux joueurs.

2. Pour Γ_λ,
$$\overline{g}_\lambda(s,t) = \sum_{p=1}^{\infty} \lambda(1-\lambda)^{p-1} g_p(s,t) \quad \lambda \in]0;1]$$
Chaque $g_p(s,t) = g(k_p, x_p, y_p)$ est continue sur $S \times T$. Par convergence uniforme de la série (les fonctions de paiement étant uniformément bornées) $\overline{g}_\lambda$ est continue sur $S \times T$. Ainsi $\overline{\gamma}_\lambda(\sigma,\tau) = E_{\sigma,\tau}(\overline{g}_\lambda) = \int_{S\times T} \overline{\gamma}_{s,t}(\sigma \otimes \tau)$ est continue pour la topologie faible-$\star$ sur le produit $\Sigma \times \mathcal{T}$
Un analogue du théorème de Ville avec des compacts métrisables donne le résultat.

Formule de récurrence

NB : Il existe des stratégies optimales stationnaires, on se limitera à celles-ci.

Γ_λ Considérons le jeu avec escompte débutant à l'état k, Γ_λ^k, il a une valeur v_λ^k. Après une première étape où I joue x et II joue y, on arrive dans l'état l, selon la probabilité

$Q(l|k,x,y)$. Écrivons que le paiement total de Γ_λ^k est la somme du paiement de la première étape et du paiement du jeu Γ_λ^l où les deux joueurs jouent de manière optimale

$$\overline{g}_\lambda^k = \lambda g_1^k(x,y) + (1-\lambda)\sum_{l\in K} Q(l|x,y,k)v_\lambda^l$$

I va jouer optimal pour recevoir un paiement v_λ^k d'où

$$v_\lambda^k = \max_x \ \min_y \left[\lambda g_1^k(x,y) + (1-\lambda)\sum_{l\in K} Q(l|x,y,k)v_\lambda^l\right]$$

Γ_n De la même manière pour le jeu Γ_n^k débutant à l'état k, on décompose le paiement :

$$n\,\overline{g}_n^k = g_1^k(x,y) + (n-1)\sum_{l\in K} Q(l|x,y,k)v_{n-1}^l$$

D'où

$$n\,v_n^k = \max_x \ \min_y \left[g_1^k(x,y) + \sum_{l\in K} Q(l|x,y,k)(n-1)\,v_{n-1}^l\right]$$

Définition 3.5 *On définit l'opérateur Ψ de $\mathbb{R}^K$ dans $\mathbb{R}^K$ par*

$$\Psi^k\,\omega = \max_x \ \min_y \left[g_1^k(x,y) + \sum_{l\in K} Q(l|x,y,k)\omega^l\right]$$

Ainsi

$$n\,v_n = \Psi\left[(n-1)\,v_{n-1}\right]$$
$$\frac{v_\lambda}{\lambda} = \Psi\left[(1-\lambda)\frac{v_\lambda}{\lambda}\right]$$

Posons $V_n = nv_n$ et $V_\lambda = \frac{v_\lambda}{\lambda}$.

Théorème 3.2

$$V_n = \Psi\left[V_{n-1}\right]$$
$$V_\lambda = \Psi\left[(1-\lambda)V_\lambda\right]$$

V_n et V_λ sont déterminés de façon unique par les formules précédentes.

Lemme 1 *Pour tout ω dans $\mathbb{R}^K$ et tout vecteur constant c, on a*

$$\Psi(\omega + c) = \Psi(\omega) + c$$

Ψ est monotone.

Lemme 2 *Ψ est une application non dilatante (lorsqu'on munit $\mathbb{R}^K$ de la norme du sup).*

PREUVE : Soient u et v dans $\mathbb{R}^K$.

$$\forall k\in K \quad \left|u^k - v^k\right| \leqslant \|u-v\|$$

donc

$$\forall x \ \ \forall y \quad \sum_{l\in K} Q(l|x,y,k)u^l \leqslant \sum_{l\in K} Q(l|x,y,k)v^k + \|u-v\|$$

d'où

$$\max_x \ \min_y \left[g_1^k(x,y) + \sum_{l\in K} Q(l|x,y,k)u^l\right] \leqslant$$

$$\max_x \min_y \left[g_1^k(x,y) + \sum_{l \in K} Q(l|x,y,k) u^l \right] + ||u - v||$$

soit

$$\Psi^k u \leqslant \Psi^k v + ||u - v||$$

On permute les rôles de u et v, d'où

$$\left|\Psi^k u - \Psi^k v\right| \leqslant ||u - v||$$

Ceci étant valable pour tout k. On a

$$||\Psi u - \Psi v|| \leqslant ||u - v||$$

Ainsi $\omega \mapsto \Psi[(1-\lambda)\omega]$ est une contraction ($\lambda \in]0;1]$) donc (théorème de Picard) elle admet un unique point fixe de V_λ dans $\mathbb{R}^K$.
Remarquons encore que V_1 est bien défini et que V_n est déterminé de manière unique à partir de V_{n-1}.

3.4 Analyse asymptotique. Aspect algébrique

V_λ est solution de $f = \Psi[(1-\lambda)f]$ Puisque les ensembles d'états et d'actions sont finis, l'égalité précédente s'écrit comme un système d'égalités et d' inégalités polynômiales utilisant un nombre fini de variables.
Le système est aussi polynômial en λ.
Nous montrons ainsi

Proposition 3.1 *L'ensemble $E = \{(\lambda, v_\lambda, \sigma_\lambda, \tau_\lambda) \mid 0 < \lambda \leqslant 1,\ \sigma_\lambda$ et τ_λ étant des stratégies optimales stationnaires et v_λ la valeur de $\Gamma_\lambda\}$ est, pour chaque λ fixé, compact, non vide et semi-algébrique (i.e. un ensemble de solutions d'un système d'égalités et d'inégalités polynômiales)*

Théorème 3.3 *Il existe $\lambda_0 > 0$, un entier $M > 0$ et des développements en série de Puiseux tels que*

$$v_\lambda^k(\lambda) = \sum_{p \geqslant 0} h_p^k \ \lambda^{\frac{p}{M}}$$

$$\sigma_\lambda^k(\lambda) = \sum_{p \geqslant 0} \alpha_p^k \ \lambda^{\frac{p}{M}}$$

$$\tau_\lambda^k(\lambda) = \sum_{p \geqslant 0} \beta_p^k \ \lambda^{\frac{p}{M}}$$

tels que pour tout $\lambda \in]0;\lambda_0]$, σ_λ et τ_λ soient des stratégies optimales stationnaires pour les deux joueurs avec paiement v_λ.

Preuve : $(v_\lambda, \sigma_\lambda, \tau_\lambda)$ est une fonction semi-algébrique du graphe E, chaque coordonnée $f(\lambda)$ (en tant que projection d'une fonction semi-algébrique) est alors une fonction semi-algébrique à valeurs réelles sur $]0;1]$. Elle admet donc un développement en série de Puiseux [Ahlfors 1966] au voisinage de 0.

$$\exists \lambda_0 \in]0;1] \quad \exists k_0 \in \mathbb{Z} \quad \exists M \in \mathbb{N}^\star \quad f(\lambda) = \sum_{p \geqslant k_0} \phi_p \, \lambda^{\frac{p}{M}}$$

La série convergeant absolument vers $f(\lambda)$ sur l'intervalle $]0;\lambda_0]$.
Chacune des coordonnées $f(\lambda)$ est bornée, donc $k_0 \geqslant 0$ et — quitte à prendre $\phi_k = 0$ pour $0 \leqslant k \leqslant k_0$ — on choisit $k_0 = 0$.
Il suffit de remplacer les différents M par leur plus petit commun multiple, de remplacer les différents λ_0 par le plus petit pour obtenir le résultat.

Théorème 3.4 *v_λ admet une limite lorsque λ tend vers 0 appelée v_∞.*

PREUVE : v_∞ est le premier coefficient du développement de Puiseux de v_λ. On a $v_\lambda - v_\infty = O(\lambda^{\frac{1}{M}}$

Théorème 3.5 *v_n admet une limite lorsque $n \to \infty$ qui est la limite de v_λ lorsque $\lambda \to 0$.*

PREUVE : Comme on l'a vu précédemment, il existe des vecteurs a_i dans $\mathbb{R}^K$, $M > 0$, $\lambda_0 \in]0;1]$ tels que pour $\lambda \leqslant \lambda_0$

$$v_\lambda = v_\infty + \sum_{i=1}^{\infty} a_i \lambda^{\frac{i}{M}}$$

$$V_\lambda = \lambda^{-1} v_\infty + \lambda^{-1} \sum_{i=1}^{M} a_i \lambda^{\frac{i}{M}} + \mathcal{O}(\lambda^{\frac{1}{M}})$$

Comme $V_\lambda = \Psi((1-\lambda)V_\lambda)$ et que $\Psi[\omega + c] = \Psi[\omega] + c$, on a

$$\Psi\left[v_\infty(\lambda^{-1} - 1) + \lambda^{-1} \sum_{i=1}^{M} a_i \lambda^{\frac{i}{M}} + \mathcal{O}(\lambda^{\frac{1}{M}})\right] = V_\lambda$$

Prenons $n \geqslant n_0 = \frac{1}{\lambda_0}$, en posant $n = \frac{1}{\lambda}$, on a

$$\Psi\left[v_\infty(n-1) + \sum_{i=1}^{M} a_i n^{1-\frac{i}{M}} + \mathcal{O}(\lambda^{\frac{1}{M}})\right] = n v_\infty + \sum_{i=1}^{M} a_i n^{1-\frac{i}{M}} + \mathcal{O}(n^{-\frac{1}{M}})$$

De plus, comme $V_n = \Psi(V_{n-1})$ et que Ψ est non dilatante, on a

$$\left| V_n - n v_\infty - \sum_{i=1}^{M} a_i n^{1-\frac{i}{M}} \right| \leqslant \left| V_{n-1} - (n-1) v_\infty - \sum_{i=1}^{M} a_i n^{1-\frac{i}{M}}) \right| + \mathcal{O}(n^{-\frac{1}{M}})$$

D'où, si on pose

$$u_n = v_\infty + \sum_{i=1}^{M} a_i n^{-\frac{i}{M}}$$

l'inégalité ci-dessus devient :

$$|n v_n - n u_n| \leqslant |(n-1) v_{n-1} - (n-1) u_{n-1}| + \varphi(n) \qquad \text{où } \varphi(n) = \mathcal{O}(n^{-\frac{1}{M}})$$

On a donc $|N v_N - N u_N| \leqslant \sum\limits_{n=1}^{N} \varphi(n)$,

or $\varphi(n) \to 0 \Rightarrow \frac{1}{N} \sum\limits_{n=1}^{N} \varphi(n) \to 0$ (Césaro), d'où $|v_n - u_n| \to 0$

En outre $|u_n - v_\infty| \to 0$ et $|v_n - v_\infty| \leqslant |v_n - u_n| + |u_n - v_\infty|$ d'où $v_n \to v_\infty$.

Remarques : le jeu infini Comme on le verra sur un exemple par la suite, les joueurs n'ont pas nécessairement des stratégies optimales dans le jeu infini.
Meme sans avoir défini de manière exacte la notion de paiement pour le jeu infini, on a :

Proposition 3.2 *Si Γ_∞ a une valeur v_∞, alors la suite (v_n) des valeurs des suites Γ_n tend ω_∞ lorsque n tend vers l'∞.*

PREUVE : On note σ_ε (resp. τ_ε une stratégie ε-optimale pour le joueur I (resp. II) dans Γ_∞. Γ_∞ a une valeur ω_∞ donc

$$\forall \varepsilon > 0 \quad \exists \tau_\varepsilon \in \mathcal{T} \quad \exists \sigma_\varepsilon \in \Sigma \quad \exists N \quad \forall n \geqslant N$$

$$\forall \tau \in \mathcal{T} \quad \omega_\infty - \varepsilon \leqslant E_{\sigma_\varepsilon, \tau}(\overline{g}_n)$$

$$\forall \sigma \in \Sigma \quad E_{\sigma,\tau_\varepsilon}(\overline{g}_n) \leqslant \omega_\infty + \varepsilon$$

Or pour tout n, il existe $\sigma_n \in \Sigma_n$ et $\tau_n \in \mathcal{T}_n$ tels que

$$\forall \sigma \in \Sigma_n \quad \forall \tau \in \mathcal{T}_n \quad E_{\sigma,\tau_n}(\overline{g}_n) \leqslant v_n \leqslant E_{\sigma_n,\tau}(\overline{g}_n)$$

Donc en particulier

$$E_{\sigma^n_\varepsilon,\tau_n}(\overline{g}_n) \leqslant v_n \leqslant E_{\sigma_n,\tau^n_\varepsilon}(\overline{g}_n)$$

où σ^n_ε désigne la projection de σ_ε sur Σ_n. Comme

$$E_{\sigma^n_\varepsilon,\tau_n}(\overline{g}_n) = E_{\sigma_\varepsilon,\tau_n}(\overline{g}_n)$$

On obtient

$$\forall \varepsilon > 0 \quad \exists N \quad \forall n \geqslant N \quad \omega_\infty - \varepsilon \leqslant v_n \leqslant \omega_\infty + \varepsilon$$

En faisant tendre ε vers 0, on a le résultat voulu.

4 Un exemple: le Big Match

4.1 Définition du jeu

Le Big Match est défini par sa matrice du gain du joueur I:

$$\begin{pmatrix} 1^\star & 0^\star \\ 0 & 1 \end{pmatrix}$$

Le joueur I choisit la ligne, et le joueur II choisit la colonne. On en déduit une case de la matrice, qui est ce que le joueur II paie au joueur I. Si cette case était marquée d'une étoile, il s'agit d'un état absorbant: à chacun des coups suivant, le jeu restera dans cette case, et I recevra le paiement correspondant à chaque fois. Sinon, c'est à dire si l'état n'est pas absorbant, le jeu recommence exactement identique.
Ceci se décrit à l'aide d'un jeu stochastique fini à trois états. L'ensemble des stratégies pures du joueur I est $\{H$ (noté aussi 1), B (noté aussi 0)$\}$, celui du joueur II est $\{G$ (noté aussi 1), D (noté aussi 0)$\}$.

- État 1: Les fonctions g (paiement) et Q (état suivant) sont représentées par les deux tableaux:
$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}$$
- État 2: Paiement de 1 à tous les coups, et on reste dans le même état. g et Q sont représentés par les tableaux:
$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} 2 & 2 \\ 2 & 2 \end{bmatrix}$$
- État 3: Paiement de 0 à tous les coups, et on reste dans le même état. g et Q sont représentés par les tableaux:
$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad \begin{bmatrix} 3 & 3 \\ 3 & 3 \end{bmatrix}$$

On voit facilement que si II choisit la stratégie stationnaire $({}^1\!/_2; {}^1\!/_2)$, quels que soient le choix de I, il s'assure de ne pas payer (en espérance) plus de ${}^1\!/_2$. La valeur supérieure du jeu est donc inférieure à ${}^1\!/_2$.

4.2 Valeur et stratégies optimales de Γ_n et Γ_λ

Nous allons calculer l'opérateur Ψ, dans le cas particulier qui nous intéresse.
On se doute que si le Big Match a une valeur, c'est le triplet $v_0 = (^1/_2; 1; 0)$. En effet, si le jeu commence dans l'état 2 ou 3, le gain est constant, c'est donc sa valeur. Si le jeu commence dans l'état 1 et a une valeur $^1/_2$ parait être vraisemblable, car $^1/_2$ est celle du jeu en un coup.

Lemme 3 $\forall\theta \in \mathbb{R} \quad \Psi[\theta v_0] = (\theta + 1)v_0$

Preuve : Soient les stratégies pour un coup $\sigma = (\varepsilon; 1-\varepsilon)$ et $\tau = (\eta; 1-\eta)$. Le gain de ce coup est:

$$g_{\sigma\tau} = (\varepsilon\eta + (1-\varepsilon)(1-\eta); 1; 0)$$

L'espérance de paiement, dans un jeu ou les coups suivants entraînent un gain ω:

$$\mathcal{E}_{\sigma\tau}(\omega) = ((1-\varepsilon)\,\omega^1 + \varepsilon\eta\,\omega^2 + \varepsilon(1-\eta)\,\omega^3; \omega^2; \omega^3)$$

$$\text{et} \qquad \Psi\omega = \max_\sigma \min_\tau [\mathcal{E}_{\sigma\tau}(\omega)]$$

On a alors, pour $\omega = \theta v_0$:

$$(\Psi\omega)^1 = \max_\varepsilon \min_\eta \; f(\varepsilon, \eta)$$

$$\text{où} \qquad f(\varepsilon, \eta) = \Big(1 + \tfrac{\theta}{2}\Big)\Big(1 - \varepsilon + 2\varepsilon\eta\Big) - \eta$$

Ceci est atteint pour $\varepsilon = \frac{1}{2+\theta}$ et $(\Psi\omega)^1 = \frac{1+\theta}{2}$ d'où

$$\Psi[\theta v_0] = \Psi[(\tfrac{\theta}{2}; \theta; 0)] = (\tfrac{1+\theta}{2}; 1+\theta; 0) = (1+\theta)v_0$$

Théorème 4.1 *Pour tout n, la valeur de Γ_n est v_0, et pour tout λ, la valeur de Γ_λ est v_0*

Preuve :

- Γ_n
  Montrons par récurrence $v_n = v_0$. On a $v_1 = v_0$ (jeu en un coup) et si on suppose $v_n = v_0$, on a $(n+1)v_{n+1} = \Psi[nv_n]$ or $\Psi[nv_0] = (n+1)v_0$, d'où $(n+1)v_{n+1} = (n+1)v_0$
- Γ_λ
  On sait que v_λ est l'unique point fixe de $\omega \mapsto \Psi[(1-\lambda)\omega]$, or $\frac{v_0}{\lambda}$ est un tel point fixe (en effet, $\Psi[(1-\lambda)\frac{v_0}{\lambda}] = \Psi[(\frac{1}{\lambda}-1)v_0] = \frac{1}{\lambda}v_0$)

4.3 Analyse de trois stratégies simples de I

On définit le paiement du jeu infini comme $\lim \frac{1}{n}(g_1 + \ldots g_n)$. Cette limite existe.
Il s'agit de montrer que, si les stratégies de I vérifient certaines propriétés (de simplicité), alors I ne s'assure pas un gain supérieur à 0. On peut donc trouver des stratégies pour II qui annulent l'espérance de paiement à ε près.

1. **stratégies stationnaires**
   Si le joueur I choisit la stratégie stationnaire $(\eta; 1-\eta)$, avec $\eta \in [0, 1]$, on a

$$\lim_{n\to\infty} \sum_{k=0}^{n} \eta(1-\eta)^k = 1 \qquad \text{d'où} \qquad \forall\varepsilon > 0 \;\; \exists n_\varepsilon \quad \sum_{k \geqslant n_\varepsilon} \eta(1-\eta)^k < \varepsilon$$

   Prenons pour le joueur II la stratégie suivante: droite pour les n_ε premiers coups, gauche ensuite. Le paiement total moyen après n coups ($n \geqslant n_\varepsilon$) est

$$n\,\overline{\gamma}_n = \sum_{k=0}^{n_\varepsilon - 1} (1-\eta)^{k+1} + \sum_{k=n_\varepsilon}^{n} (n-k)\eta(1-\eta)^k$$

d'où $\overline{\gamma}_n < \frac{constante}{n} + \sum_{n_\varepsilon \leqslant k \leqslant n} \eta(1-\eta)^k < \frac{constante}{n} + \sum_{n_\varepsilon \leqslant k} \eta(1-\eta)^k < \frac{constant}{n} + \varepsilon$, inférieur à 2ε pour n grand.
Le joueur I ne peut donc pas s'assurer un gain de 2ε, il ne peut donc pas s'assurer mieux que 0.

2. **stratégies déterminées à l'avance**
Si le joueur I choisit la stratégie $(\eta_k; 1-\eta_k)$ au au $k^{ème}$ coup, la probabilité que le jeu ne soit pas arrêté au $k^{ème}$ coup est: $\prod\limits_{i<k}(1-\eta_i)$.

$$\lim_{n\to\infty} \sum_{k=0}^{n} \eta_k \prod_{i<k}(1-\eta_i) \leqslant 1 \qquad \text{d'où} \qquad \forall \varepsilon > 0 \ \exists n_\varepsilon \quad \sum_{k \geqslant n_\varepsilon} \eta_k \prod_{i<k}(1-\eta_i) < \varepsilon$$

Prenons pour le joueur II la stratégie suivante: droite pour les n_ε premiers coups, gauche ensuite. Le paiement total moyen après n coups ($n \geqslant n_\varepsilon$) est

$$n\,\overline{\gamma}_n = constant + \sum_{k=n_\varepsilon}^{n} (n-k)\eta_k \prod_{i<k}(1-\eta_i)^k$$

d'où $\overline{\gamma}_n < \frac{constant}{n} + \sum\limits_{k \geqslant n_\varepsilon} \lambda_\eta \prod\limits_{i<k}(1-\eta_i)$, qui est inférieur à 2ε pour n grand.
Le joueur I ne peut donc pas s'assurer un gain de 2ε, il ne peut donc pas s'assurer mieux que 0.

3. **stratégies à mémoire finie**
On définit la mémoire du joueur I comme un ensemble de cases $\mathcal{M}$ de cardinal $M < \infty$. La stratégie du joueur est déterminée par deux fonctions:

   - $f : \mathcal{M} \to \{H, B\}$ (haut ou bas)
     Le coup que joue I selon la case où il est.
   - $g : \mathcal{M} \times \{G, D\} \to \mathcal{P}_M$ (probabilités sur $\mathcal{M}$).
     La nouvelle case,selon le coup joué par II.

On choisit d'appeler la case $0 \in \mathcal{M}$ l'unique case telle que $f(0) = H$; en effet, si une autre case fait aussi jouer I en haut, elle est équivalente à la première, car le jeu est alors terminé...
On fait alors jouer au joueur II la stratégie constante $(\varepsilon, 1-\varepsilon)$. Ceci induit (à l'aide de g) une chaîne de Markov sur $\mathcal{M}$. Il existe donc un nombre N tel qu'à partir du $N^{ème}$ coup de la partie, la probabilité d'être arrivé dans un état récurrent soit supérieure à $1-\eta$
Au temps N, le joueur II change sa stratégie en $(1-\varepsilon, \varepsilon)$. La nouvelle chaîne a la même décomposition ergodique.
Le joueur I se retrouve avec une espérance de gain de:

   - ε s'il a joué haut avant le temps N
   - inférieure à $\eta(1-\varepsilon) + \varepsilon$ sinon.

Le joueur I n'a pas non plus de stratégie assurant mieux que 0.

4.4 Exemple de "bonne" stratégie pour le joueur I

On définit le paiement du jeu infini comme $\limsup \frac{1}{n}(g_1 + \dots g_n)$, car dans le cas général, la limite n'existe pas toujours.

Théorème 4.2 *Le joueur I peut, pour tout entier N strictement positif, obtenir au moins*

$$V(N) = \frac{1}{2} - \frac{1}{2(N+1)}$$

en utilisant la stratégie σ_N suivante:
Il note les n premières actions du joueur II, $(y_1, \cdots, y_n)$, il calcule la différence k_n entre le nombre de 0 et le nombre de 1 (appelée excès dans la suite), et il annonce 1 avec la probabilité $p((k_n + N + 1)^{-2})$.

Corollaire 4.2.1 *La valeur du Big Match est $^1/_2$.*

Preuve : On a vu que la valeur du Big Match est inférieure à $^1/_2$. Or il existe des stratégies asurant un paiement de $^1/_2 - \varepsilon$, La valeur est donc bien $^1/_2$.

Preuve : théorème: Évidemment, la stratégie σ_N prévoit 1 avec probabilité 1 chaque fois que l'excès des actions du joueur II atteint $-N$.
Supposons que nous ayons vérifié que la stratégie σ_N produise une espérance de gain d'au moins $V(N)$ contre chaque suite d'actions du joueur II qui réalise un excès égal à $-N$ presque sûrement.
Considérons alors une suite quelconque $\omega = (y_1, y_2, \cdots)$ d'actions du joueur II et σ une stratégie quelconque du joueur I.
Soit t le nombre d'étapes tel que le joueur I annonce 1 à l'étape $t + 1$. ($t = \infty$ s'il n'annonce jamais 1) Posons, pour $m \in N$,

$$\lambda_\sigma(m) = P_\sigma\{t < m \text{ et } y_{t+1} = 0\}$$

$$\mu_\sigma(m) = P_\sigma\{t < m \text{ et } y_{t+1} = 1\}$$

$$\lambda_\sigma = \lim_{m \to \infty} \lambda_\sigma(m)$$

$$\mu_\sigma = \lim_{m \to \infty} \mu_\sigma(m)$$

Si $t < \infty$, le gain moyen du du joueur I à l'étape n est

$$\frac{t - \sum_{i=1}^{t} y_i + (n-t) y_{t+1}}{n}$$

donc le gain g_∞ est nul si $y_{t+1} = 0$ est égal à 1 si $y_{t+1} = 1$. Supposons maintenant que l'excès de ω soit toujours supérieur à $-N$. ω vérifie alors

$$(y_1 + \cdots + y_n)/n < \frac{1}{2} + \frac{N}{2n} \quad \forall n$$

si bien que, lorsque $t = \infty$ le gain du joueur I vérifie

$$g_\infty = \limsup_{n \to \infty} \frac{(1 - y_1) + \cdots + (1 - y_n)}{n} \geqslant \frac{1}{2}$$

L'espérance de gain du joueur I est donc au moins

$$\mu_\sigma + \frac{1}{2}(1 - \lambda_\sigma - \mu_\sigma)$$

puisque

$$\mu_\sigma = P_\sigma\{t < \infty \text{ et } y_{t+1} = 1\} \text{ et } (1 - \lambda_\sigma - \mu_\sigma) = P_\sigma\{t = \infty\}$$

Montrons alors que

$$\mu_{\sigma_N} + \frac{1}{2}(1 - \lambda_{\sigma_N} - \mu_{\sigma_N}) \geqslant V(N)$$

Considérons, pour $m \in N$, la stratégie suivante τ_m du joueur II: choisir $(y_1, \cdots, y_m)$ quelconques, puis tirer à pile ou face. Avec une probabilité 1 l'excès d'une telle suite atteint $-N$.

Donc l'espérance de gain du joueur I est au moins $V(N)$ s'il adopte la stratégie σ_N. D'autre part, pour une stratégie σ quelconque du joueur I, son espérance de gain contre τ_m est exactement

$$\mu_\sigma(m) + \frac{1}{2}(1 - \lambda_\sigma(m) - \mu_\sigma(m))$$

D'où le résultat par passage à la limite lorsque $m \to \infty$ et $\sigma = \sigma_N$.
Il suffit donc de montrer la propriété pour les suites d'actions du joueur II dont l'excès atteint $-N$ avec probabilité 1. Soit ω une telle suite. Le joueur I utilise la stratégie σ_N. Soit t le nombre d'étapes après lesquelles il prédit 1. Soit

$$E(m) = \{\, t \geqslant m, \text{ ou } t < m \text{ et } y_{t+1} = 1\}, \quad m = 1, 2, \ldots$$

Montrons par récurrence sur m que

$$\forall N \quad P_{\sigma_N}(E(m)) \;\geqslant\; V(N)$$

1. $m = 1$.
   Si $y_1 = 1$, $P_{\sigma_N}(E(1)) = 1 > V(N) = N/2(N+1)$.
   Si $y_1 = 0$, $P_{\sigma_N}(E(1)) = P_{\sigma_N}\{t \geqslant 1\} = 1 - p(N) = \frac{N(N+2)}{N+1^2} \geqslant V(N) = N/2(N+1)$.
2. Supposons que $\forall N \quad P_{\sigma_N}(E(m)) \geqslant V(N)$.
   Si $y_1 = 1$, $P_{\sigma_N}(E(m+1)) = p(N) + [1-p(N)]P_{\sigma_{N-1}}(E(m)) \;\geqslant\; p(N) + [1-p(N)]V(N-1) = V(N)$ puisque utiliser la stratégie σ_N contre ω est équivalent á prédire 1 initialement avec une probabilité $p(N)$ et á prédire 0 initialement avec une probabilité $1 - p(N)$ et donc ensuite utiliser la stratégie σ_{N-1} contre $\omega' = (y_2, y_3, \ldots)$.
   Si $y_1 = 0$ De la même manière, si $y_1 = 0$,

   $$P_{\sigma_N}(E(m+1)) = [1 - p(N)]P_{\sigma_{N+1}}(E(m)) \geqslant [1 - p(N)]V(N+1) = V(N)$$

   Ainsi, l'inégalité

   $$\forall N \quad P_{\sigma_N}(E(m)) \geqslant V(N)$$

   est démontrée. Puisque $t < \infty$ avec une probabilité 1, lorsque m tend vers l'infini cette inégalité donne

   $$\forall N \quad P_{\sigma_N}\{y_{t+1} = 1\} \geqslant V(N)$$

   Ainsi la stratégie σ_N garantit au moins $V(N)$ contre toute suite d'actions du joueur II et la valeur du jeu est $1/2$.

4.5 Non existence de stratégies optimales pour le joueur I

Théorème 4.3 *I n'a pas de stratégie optimale.*

Soit σ une stratégie de I. Si σ ne prévoit jamais 1 avec une probabilité positive, il gagne 0 contre $\omega = (1, 1, 1, \cdots)$ et σ n'est donc pas optimale. Sinon, soit $m \geqslant 0$ le plus petit nombre d'étapes après lesquelles σ prédit 1 avec une probabilité positive ε. Le joueur II peut contrer σ en choisissant m fois 1, puis 0 et en jouant à pile ou face ensuite. L'espérance de gain du joueur I est alors (cf. plus haut)

$$\mu_\sigma(m+1) + \frac{1}{2}(1 - \lambda_\sigma(m+1) - \mu_\sigma(m+1))$$

Or

$$\lambda_\sigma(m+1) = P_\sigma\{t = m \text{ et } y_{t+1} = 0\} = \varepsilon$$
$$\mu_\sigma(m+1) = P_\sigma\{t = m \text{ et } y_{t+1} = 1\} = 0$$

ce qui donne une espérance de gain égale à $\frac{1}{2}(1 - \varepsilon)$. σ n'est donc pas optimale.

Remerciements

Nous tenons à remercier, monsieur Sorin de nous avoir proposé un sujet aussi intéressant, pour ses conseils et pour le temps qu'il a nous a consacré.

Bibliographie

[BF] **D.Blackwell, T.S. Ferguson** (1968) The big match, The Annals of Mathematical Statistics, Vol 39, num. 1, 159-163.

[MSZ] **J.F. Mertens, S.Sorin, S.Zamir** Repeated games (Ch. iv, vii).

[O] **G. Owen** (1989) An elementary proof of the Minimax Theorem, Management Science, vol. 13, num. 9.

Chapitre 5

Rapport de stage de DEA

Chapitre 6

Étude d'un problème NP-Complet

1 Énoncé du problème

Ce problème apparaît lors de l'étude des perceptrons d'Ising. C'est un bon candidat à une utilisation en cryptographie, car son énoncé est simple, la vérification d'une solution est rapide, mais il est difficile à résoudre.

On appellera un ε-vecteur de taille n un vecteur dont les composantes sont $+1$ ou -1.

Soient m, n deux entiers. Soient $X^1, ..., X^m$ des ε-vecteurs de taille n.

Problème de décision

Existe-t-il un ε-vecteur Y de taille n tel que pour tout j, $X^j.Y \geqslant 0$.

Problème de recherche

Trouver un ε-vecteur Y de taille n tel que pour tout j, $X^j.Y \geqslant 0$.

2 Le problème est NP-complet

Pour prouver que le problème ci-dessus est NP-complet, on réduit polynomialement une instance de 3-SAT à une instance de ce problème.

Soit donc une instance de 3-SAT : des clauses à 3 variables $c_1, ..., c_q$ sur les variables $x_1, ..., x_k$.

On construit pour chaque clause un ε-vecteur de taille $2k$: à une clause c on associe C tel que :

- si $x_i \in c$, alors $C_i = -1$ et $C_{i+k} = -1$
- si $\bar{x}_i \in c$, alors $C_i = +1$ et $C_{i+k} = +1$
- sinon alors $C_i = +1$ et $C_{i+k} = -1$

On construit pour une distribution de vérité un ε-vecteur de taille $2k$: à une distribution de vérité v on associe V tel que :

- si $x_i \in v$, alors $V_i = -1$ et $V_{i+k} = -1$
- si $\bar{x}_i \in v$, alors $V_i = +1$ et $V_{i+k} = +1$

On remarque que c vrai sous $v \Leftrightarrow C.V$ vaut -2, $+2$ ou $+6$

et que c faux sous $v \Leftrightarrow C.V$ vaut -6

Donc c vrai sous $v \Leftrightarrow C.V \geqslant -2$ et V correspond à une distribution de vérité.

V correspond à une distribution de vérité si pour tout i, $V_i = V_{i+k}$. On construit donc des ε-vecteurs $Z^1, ...Z^k$ tels que :

pour tout i, $V_i = V_{i+k} \Leftrightarrow$ pour tout j, $Z^j.V = 0$.

Par exemple les Z^j définis comme suit :

- si $i = j$, $Z_i^j = +1$ et $Z_{i+k}^j = -1$

- si $i \neq j$, $Z_i^j = -1$ et $Z_{i+k}^j = +1$
Donc c vrai sous $v \Leftrightarrow C.V \geqslant -2$ et pour tout j, $Z^j.V = 0$.

On définit des ε-vecteurs de taille $n+2$: $\tilde{V} = (V, +1, +1)$ $\tilde{C} = (C, +1, +1)$ $\tilde{Z} = (Z, +1, -1)$ $\tilde{Z'} = (Z, -1, +1)$

Et alors c vrai sous $v \Leftrightarrow \tilde{C}.\tilde{V} \geqslant 0$ et pour tout j, $\tilde{Z^j}.\tilde{V} = 0$ et $\tilde{Z^j}'.\tilde{V} = 0$.
Ce qui devient c vrai sous $v \Leftrightarrow \tilde{C}.\tilde{V} \geqslant 0$ et pour tout j, $\tilde{Y^j}.\tilde{V} \geqslant 0$, avec $\tilde{Y^j}$ prenant les valeurs $\tilde{Z^j}$, $\tilde{Z'^j}$, $-\tilde{Z^j}$ et $-\tilde{Z'^j}$.

On transforme donc le problème 3-SAT à q clauses sur k variables en un problème à $m = q + 4k$ ε-vecteurs de taille $n = 2k + 2$.

3 Équivalence avec le problème dans le cas impair

Nous allons réduire le problème dans le cas où n est pair à un problème où $\tilde{n} = n + 1$ est impair.
On pose $\tilde{X} = (X, +1)$,
alors $X.Y \geqslant 0 \Rightarrow \tilde{X}.(Y, +1) \geqslant 0$
et $\tilde{X}.(Y, +1) \geqslant 0 \Rightarrow X.Y \geqslant 0$ et $\tilde{X}.(Y, -1) \geqslant 0 \Rightarrow X.Y \geqslant 2 \geqslant 0$.

On transforme donc le problème à m vecteurs de taille n (pair) en un problème à m vecteurs de taille $n + 1$.

4 Approximation

On s'intéresse à la résolution du problème de recherche d'un vecteur V solution, sachant qu'il existe une solution. Ce problème est NP-complet, mais il est peut-être possible d'obtenir une valeur approchée de V.
Le seul vecteur candidat est le vecteur *majorité* obtenu en prenant sur chaque ligne la valeur majoritaire. On note $W(C^j)$ ou simplement W ce vecteur définit par : $W_i = signe(\sum_j C_i^j)$. (NB: si m est impair, cette somme n'est jamais nulle).

On va étudier le cas où m est impair et $n = m$. En effet, si m est impair W est défini sans ambiguité. En outre, si $n = m$, le nombre moyen de solutions du problème est 1. Donc si on construit un tel problème à partir d'une solution V, il suffit de calculer la distance de V à W. On trouve que V et W diffèrent de environ $n(\frac{1}{2} - \frac{2}{\pi})$ (distance de Hamming).

Si on tire $V, C^1, ...C^m$ au hasard parmi les ε-vecteurs de taille n et que si on remplace C^j par $-C^j$ lorsque $C^j.V \leqslant O$, on obtient un énoncé du problème ayant au moins une solution.
Alors en moyenne le nombre de valeurs communes à V et W est $nG_{n,m}$ où

$$G_{n,m} = \sum_{2s>m} \binom{m}{s} (1 - F_n)^{m-s} {F_n}^s \text{ , où } F_n = 2^{-(n-1)} \sum_{2r>k} \binom{n-1}{r-1}.$$

on calcule si $n = 2x + 1$, $F_n = \frac{1}{2} + 2^{-n} \binom{2x}{x}$, ce qui donne à peu près $F_n \simeq \frac{1}{2} + \frac{1}{\sqrt{2\pi n}}$.
d'où $G_{n,m} \simeq \frac{1}{2} + \frac{1}{\pi}\sqrt{\frac{m}{n}}$ (l'approximation est assez grossière lorsque m et n ont même ordre de grandeur, mais néanmoins utile).

On obtient les formules pour F_n et $G_{n,m}$ comme suit :
Si on tire V et C de taille n au hasard, la probabilité que r éléments correspondent est $p\{C \cap V = l\} = 2^{-n} \binom{n}{r}$, donc après remplacement éventuel de C par $-C$, cette probabilité est $p = 2^{-(n-1)} \binom{n}{r}$.
Le nombre moyen d'éléments correspondants est donc $2^{-(n-1)} \sum_{2r>n} r \binom{n}{r}$.

La probabilité qu'un élément fixé corresponde est donc

$$F_n = \frac{1}{n} 2^{-(n-1)} \sum_{2r>n} r \binom{n}{r} = 2^{-(n-1)} \sum_{2r>n} \frac{r}{n} \binom{n}{r} = 2^{-(n-1)} \sum_{2r>n} \binom{n-1}{r-1}$$

La probabilité que pour un élément fixé, plus de la moitié des C^j corresponde à V est donc $G_{n,m}$.

Chapitre 7

Algorithmes cryptographiques utilisant le problème des sac à dos

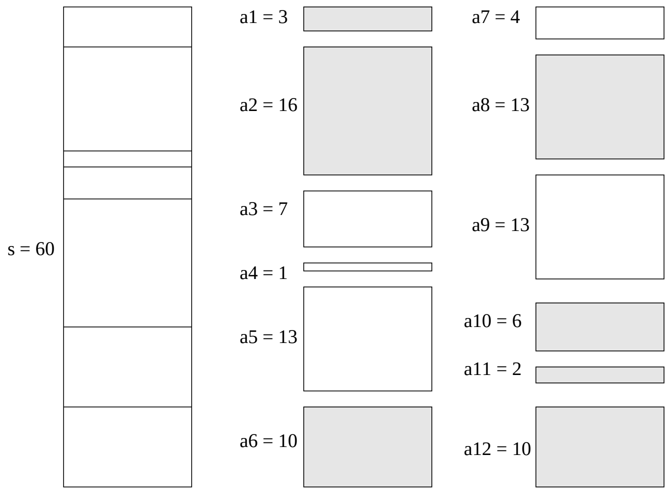
1 Attaque générale des problèmes de sac à dos

1.1 Le problème du sac-à-dos

Le problème du sac-à-dos consiste, étant donnés des entiers positifs $a_1, ..., a_n$ et s à trouver un sous-ensemble de a dont la somme soit s. Ceci est équivalent à résoudre l'équation:

$$s = \sum_{i=1}^{n} e_i a_i \text{ avec } e_i \in \{0, 1\}$$

De façon imagée, on se donne un grand sac de taille s qu'on veut remplir avec des boites de taille a_i.



Ce problème est connu pour être NP-complet, il est donc considéré comme difficile dans le cas général.

1.2 Attaques basse densité

Des algorithmes dits *basse densité* ont été proposés pour résoudre ce problème dans certains cas particuliers, l'un par Brickell [1] et l'autre Lagarias et Odlyzko [6]. Ces algorithmes prouvent que presque tous les sac-à-dos de densité assez basse peuvent être résolus en temps polynômial.

Définition 1.1 *La densité d'un sac-à-dos $a_1, ..., a_n$ est le nombre*

$$d = \frac{n}{\log_2 \max_{1 \leqslant i \leqslant n} a_i}$$

Le cas intéressant est $d \leqslant 1$, car pour $d > 1$ il y a en général plusieurs solutions au même problème de sac-à-dos, il est donc difficile de coder ainsi une information utile. Les algorithmes de Brickell et Lagarias-Odlyzko permettent de résoudre presque tous les sac-à-dos pour d assez petit. Ces deux algorithmes ramènent le problème du sac-à-dos à un problème de recherche de vecteur court dans un réseau, puis utilisent LLL pour trouver ce vecteur. Associée à LLL, la méthode de Lagarias-Odlyzko permet de résoudre presque tous les sacs-à-dos de densité d inférieure à c/n, lorsque n est assez grand; la constante c est liée à l'utilisation de LLL. Elle peut être améliorée en utilisant à la place de LLL, l'un des algorithmes de réduction par blocs de Schnorr, cela augmente bien sûr le degré du polynôme déterminant le temps de calcul.

Joux et Stern [5] et [4] et Coster, LaMacchia, Odlyzko et Schnorr [3] ont proposé des modifications de l'algorithme de Lagarias-Odlyzko.

Bien que la recherche de vecteurs courts dans un réseau puisse être très difficile dans le cas général, les algorithmes connus s'avèrent en pratique bien plus performants que ne l'affirment leurs analyses théoriques. Il est donc fort possible qu'en moyenne la recherche de vecteurs courts soit facile, même si dans le cas général elle est difficile. Il est donc parfaitement raisonnable de séparer l'efficacité de la recherche du vecteur court et la qualité de la transformation du sac-à-dos en recherche d'un vecteur court. Pour cela nous allons imaginer un oracle qui, étant donnée une base d'un réseau entier, calcule un vecteur réalisant le premier minimum de ce réseau. Dans les applications, cet oracle sera remplacé par un algorithme de réduction de réseau bien choisi. A partir d'un tel oracle, l'algorithme de Lagarias-Odlyzko est capable de résoudre presque tous les sac-à-dos de densité inférieure à une densité critique égale à $0.6463\cdots$; les améliorations de Joux et al. permettent de monter la densité critique à $0.9408\cdots$.

1.3 Construction des réseaux à partir du sac à dos

Pour le problème du sac à dos, comme pour d'autres problèmes qu'on résoud avec l'algorithme LLL, il faut transormer l'énoncé en un problème de minimisation de certaines valeurs.

Une première idée (attaque de Lagarias et Odlyzko) est de chercher des nombres e_i les plus petits possibles tels que $\sum_{i=1}^{n} e_i a_i - s = 0$. On cherche donc un vecteur court dans le réseau engendré par $a_1, ...a_n, -s$. On réduit donc la matrice suivante, où K est un facteur d'échelle, en espérant trouver une solution de la forme $0, e_1, ...e_n, 1$ avec e_i petit, c'est à dire $e_i \in \{-1, 0, 1\}$

Lagarias, Odlyzko

$$\begin{pmatrix} K.a_1 & K.a_2 & ... & K.a_n & -K.S \\ 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & ... & 1 & 0 \\ 0 & 0 & ... & 0 & 1 \end{pmatrix}$$

Les améliorations proposées pour augmenter la densité critique cherche en fait à éviter que e_i puisse valoir -1. On cherche donc non plus un vecteur court au sens de la norme usuelle, c'est à dire dans une boule centrée en 0 et de rayon minimal, mais un vecteur dans une boule décalée ou dans une famille de boules décalées pour éviter d'inclure la coordonnée -1. Cela revient à travailler dans une métrique différente et on obtient les matrices ci dessous :

Joux, Stern

$$\begin{pmatrix} K.a_1 & K.a_2 & \ldots & K.a_n & -K.S \\ n+1 & -1 & \ldots & -1 & -1 \\ -1 & n+1 & \ldots & -1 & -1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -1 & -1 & \ldots & n+1 & -1 \\ -1 & -1 & \ldots & -1 & n+1 \end{pmatrix}$$

Coster, LaMacchia, Odlyzko, Schnorr

$$\begin{pmatrix} K.a_1 & K.a_2 & \ldots & K.a_n & -K.S \\ 1 & 0 & \ldots & 0 & 1/2 \\ 0 & 1 & \ldots & 0 & 1/2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 1/2 \\ 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

2 Utilisation et attaque des sac à dos en cryptographie

2.1 Merkle-Hellman

Merkle et Hellman [7] ont décrit un système de cryptage basé sur le masquage de sacs supercroissants par multiplication modulaire. Ce système a une densité faible et il ne résiste pas aux attaques basse densité décrites ci-dessus.

Ce cryptosystème est construit suivant un schéma commun à de nombreux cryptosystèmes : un problème difficile dans le cas général sert de point de départ. On cherche alors une famille d'instances de ce problème qu'on sait résoudre et une façon de les transformer en instances apparemment quelconques.

Dans le cas du système de Merkle et Hellman, les problèmes qu'on sait résoudre sont ceux où le sac à dos est supercroissant. Cela signifie que tout élément a_i est supérieur à la somme des éléments d'avant ($\sum_{j<i} a_j$). Un tel sac à dos se résoud en temps linéaire.

On masque la famille des a_i en calculant $b_i = a_i c \bmod d$. Cette famille apparemment quelconque hérite suffisamment de la structure des a_i pour qu'il existe plusieurs méthodes pour casser ce cryptosystème. De plus, la densité du sac à dos obtenu est faible, donc les attaques basse densité marchent.

2.2 Chor-Rivest

Chor et Rivest [2] ont conçu un système qui résiste encore, masquant la solution à l'aide de méthodes algébriques.

2.3 Hachage

Damgard a décrit une fonction de hachage basée sur des sac à dos.

On peut généraliser l'attaque des problèmes de type hachage en cherchant des collisions dans un sac à dos, c'est à dire deux ensembles disjoints de boites de même somme, donc à résoudre une équation de la forme :

$$s = \sum_{i=1}^{n} e_i a_i \text{ avec } e_i \in \{-1, 0, 1\}$$

on utilise donc une matrice de type Lagarias-Odlyzko :

$$\begin{pmatrix} K.a_1 & K.a_2 & \dots & K.a_n \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

3 Résultats après implémentation

Les tableaux ci-dessous donnent la dimension de coupure (dimension où le taux de réussite est 1/2) et le temps de calcul pour cette dimension en fonction de l'algorithme de réduction utilisé et de la densité du sac à dos. Pour ces tests, on a créé des sac à dos aléatoires de densité donnée.

Le premier tableau correspons à l'attaque des sac à dos de hachage, les autres tableaux correspondent à l'attaques des sac à dos de cryptage.

Attaque du hachage

	LLL		BKZ10		BKZ20	
1.0	45	20.0s	67	498.2s	85	3774.8s
1.1	50	20.9s	>70	454.6s	100	6417.3s
1.2	55	21.9s	>70	400.3s	100	4802.9s
1.3	60	26.9s	>70	315.7s	>110	6304.8s
1.4	65	30.6s	>70	370.4s	>110	5076.1s
1.5	70	41.9s	>70	318.7s	>110	4547.5s

Attaque par matrices de Lagarias et Odlysko

	LLL		BKZ10		BKZ20	
0.6	22	2.0s	30	15.8s	38	84.8s
0.7	14	0.0s	17	0.7s	21	2.1s
0.8	7	0.0s	–	–	–	–
0.9	6	0.0s	–	–	–	–
1.0	–	–	–	–	–	–

Attaque par matrices de Joux et Stern

	LLL		BKZ10		BKZ20	
0.6	50	64.2s	>70	1231.5s	>70	4343.6s
0.7	40	22.4s	63	735.4s	>65	2893.6s
0.8	32	8.2s	51	258.7s	65	2391.0s
0.9	30	5.4s	45	133.8s	60	1463.9s
1.0	28	3.8s	38	53.7s	50	548.0s

Attaque par matrices de Coster, LaMacchia, Odlysko et Schnorr

	LLL		BKZ10		BKZ20	
0.6	49	49.4s	>70	1270.1s	>70	3621.6s
0.7	44	26.1s	58	475.0s	>65	2581.7s
0.8	31	6.2s	51	270.7s	65	2469.2s
0.9	27	3.3s	43	107.8s	60	1273.0s
1.0	24	2.0s	39	64.2s	49	408.7s

Bibliographie

[1] E. F. Brickell. Solving low density knapsacks. In *Advances in Cryptology, Proceedings of Crypto'83*, pages 25–37, New York, 1984. Plenum Press.

[2] B. Chor and R. Rivest. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE trans. Information Theory*, IT-34:901–909, 1988.

[3] M. J. Coster, B. A. LaMacchia, A. M. Odlyzko, and C.-P. Schnorr. An improved low-density subset sum algorithm. In D. W. Davies, editor, *Advances in Cryptology, Proceedings of Eurocrypt'91*, volume 547 of *Lecture Notes in Computer Science*, pages 54–67, New York, 1991. Springer-Verlag.

[4] A. Joux. La réduction des Réseaux en Cryptographie. Thèse. 1993.

[5] A. Joux and J. Stern. Improving the critical density of the lagarias-odlyzko attack against subset sum problems. In L. Budach, editor, *Proceedings of Fundamentals of Computation Theory 91*, volume 529 of *Lecture Notes in Computer Science*, pages 258–264, New York, 1991. Springer-Verlag.

[6] J. C. Lagarias and A. M. Odlyzko. Solving low-density subset sum problems. *J. Assoc. Comp. Mach.*, 32(1):229–246, 1985.

[7] R. C. Merkle and M. E. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Trans. Inform. Theory*, IT–30:594–601, 1984.

Chapitre 8

Dessins d'enfant et théorie de Galois

1 Définitions générales

On définit brièvement ici les objets que nous allons manipuler.

1.1 Les dessins d'enfant

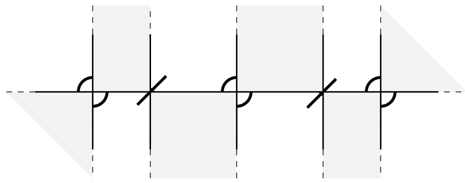
Je ne vais pas rappeler ce qu'est un revêtement ou une ramification, c'est très bien expliqué par exemple dans [4].

Définition 1.1 *Un dessin d'enfant est un revêtement fini irréductible de la sphère de Riemann ramifié au dessus de trois points, traditionnellement* 0, 1 *et* ∞.

C'est un couple $(\mathcal{C}, \phi)$ défini à isomorphisme près où $\mathcal{C}$ est une courbe projective non singulière et ϕ est une application rationnelle de $\mathcal{C}$ dans $\mathbf{P}_1(\mathbf{C})$ appelée fonction de Belyi.

De façon concrète, on peut voir le dessin comme un pavage en triangles de $\mathcal{C}$: on trace $\phi^{-1}(\mathbf{R})$ pour obtenir cette triangulation.

Exemple : soit le revêtement $\phi : \mathbf{P}_1(\mathbf{C}) \to \mathbf{P}_1(\mathbf{C})$ tel que $\phi(x) = x^2(x^2 - 2)$.

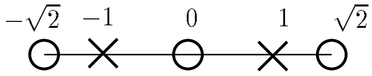


On remarque qu'un revêtement étant topologiquement déterminé par les degrés de ses ramifications et la monodromie (relations entre ces ramifications), il suffit de numéroter les éléments de ce pavage (ou drapeaux) et de répertorier leur position autour des points de ramification (en tournant dans le sens positif).

Définition 1.2 *Si l'indice de ramification en chaque point au dessus de* 1 *est exactement* 2*, le dessin est dit* propre.

Dans le cas d'un dessin propre, on aime dessiner l'image réciproque du segment réel $[0, 1] \in \mathbf{P}_1(\mathbf{C})$. On trace donc un graphe sur $\mathcal{C}$ d'où le terme *dessin d'enfant.*

Exemple : soit le revêtement tel que $\phi(x) = x^2(x^2 - 2)$.



On remarque que dans ce graphe, les ramifications au dessus de 0 correspondent aux sommets, les ramifications au dessus de 1 aux cotés et les ramifications au dessus de ∞ aux faces.

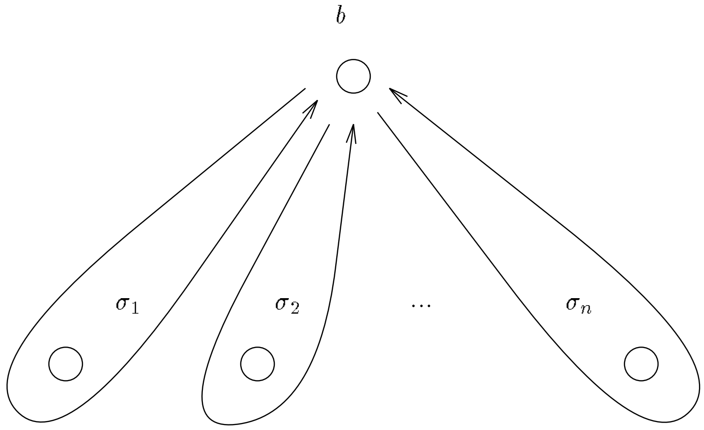
1.2 Dessins et monodromie

Soit un revêtement $(\mathcal{C}, \phi)$ de $\mathcal{S}$. On choisit un point base non ramifié $b \in \mathcal{S}$ et on étudie l'action du $\pi_1(\mathcal{S})$ sur la fibre au dessus de b.

Cela signifie qu'on étudie la façon dont on change de feuillet au dessus de b lorsqu'on tourne autour des ramifications du revêtement.

Le stabilisateur $\mathfrak{m} \subset \pi_1$ d'un point b_0 dans la fibre caractérise le revêtement (voir 1.3).

On choisit un sytème $(\sigma_1, ..., \sigma_n)$ de générateurs du π_1 tel que $\sigma_1 ... \sigma_n = 1$, la monodromie est l'action de $\mathfrak{m}$ sur $(\sigma_1, ..., \sigma_n)$.



Dans le cas des dessins d'enfants, $n = 3$.

1.3 Dessins et théorie de Galois

Un automorphisme du revêtement permute les points situés au dessus de b, on dit qu'un revêtement est galoisien si son groupe d'automorphismes (de Galois) agit transitivement sur les fibres (i.e. si tout point de la fibre s'envoie sur tout point de la fibre).

Une condition équivalente est que $\mathfrak{m}$ soit distingué dans π_1, le groupe de Galois est alors le quotient. Plus précisément, les chemins $\sigma_0, \sigma_1, \sigma_\infty$ se relèvent sur $\mathcal{C}$ et induisent des permutations de $\phi^{-1}(b)$, le groupe de Galois est le sous-groupe de $\mathfrak{S}_d$ engendré par ces permutations. d est le degré du revêtement, c'est le cardinal de $\phi^{-1}(b)$ et aussi le cardinal du groupe de Galois.

Voir [4] pour une présentation agréable de la théorie de Galois pour des surfaces de Riemann.

1.4 Construction explicite de revêtements ayant un groupe de Galois donné

Tout groupe fini peut être représenté comme un quotient d'un groupe libre à $n-1$ générateurs. Donc comme un quotient du groupe de monodromie de $\pi_1(\mathbf{P}_1(\mathbf{C}) - \{1, ..., n\})$.

Cette théorie permet, si on connait une définition d'un groupe par des générateurs dans $\mathfrak{S}_n$ de construire le dessin ayant la monodromie correspondante et d'en déduire une solution explicite du problème de Galois inverse sur $\mathbf{C}(t)$ pour ce groupe.

Il faut calculer la fonction de Belyi exactement pour déterminer le corps de définition du dessin. Il existe aussi des critères dits de rigidité permettant d'assurer que le corps de définition est $\mathbf{Q}$.

2 Calculs explicites

2.1 Cas des arbres

La famille la plus simple de dessins est la famille des dessins de genre 0 totalement ramifiés au dessus de l'infini : le graphe représentant ces dessins n'a qu'une face, c'est un arbre.

Pour la commodité des calculs, on place cette face à l'infini. La fonction de Belyi est donc un polynôme.

On va chercher des équations vérifiées par ϕ afin de calculer explicitement ce polynôme.

- **Sommets**

  Si les sommets sont α_i de multiplicité ν_i, on peut écrire $\phi = \frac{1}{\lambda}\prod_i (X-\alpha_i)^{\nu_i}$.

- **Cotés**

  Si les cotés sont β_i de multiplicité 2 (car le dessin est propre), on peut écrire $\phi - 1 = \frac{1}{\lambda}\left(\prod_i (X-\beta_i)\right)^2$.

Si on considère l'équation de polynômes :

$$\prod_i (X-\alpha_i)^{\nu_i} - \lambda = \left(\prod_i (X-\beta_i)\right)^2$$

les α_i, β_i et λ sont les inconnues, alors que les ν_i sont fixés.

On peut chercher à résoudre directement ce système, mais il est utile de le transformer légèrement.

En procédant comme dans [1], on aboutit a ce sytème linéaire :

$$\sum_i \bar{\nu}_i \alpha_i^k = 0 \qquad \text{pour} \qquad 0 \leqslant k \leqslant N-2$$

où N est le nombre de sommets et $\bar{\nu}_i$ vaut $\pm\nu_i$ selon une coloration des sommets en deux couleurs.

Cette coloration s'obtient en remarquant que l'équation $\phi = Q^2 + \lambda$ permet de décomposer $\phi = (Q + \sqrt{-\lambda}).(Q - \sqrt{-\lambda})$. Si α_i annule le premier facteur, $\bar{\nu}_i = \nu_i$, sinon $\bar{\nu}_i = -\nu_i$.

2.2 Résolution du système pour certaines familles d'arbres

La méthode algébrique de résolution d'un tel système utilise des bases de Grobner, mais au delà d'un certain nombre de points, il est nécessaire de résoudre ce système par approximations.

On part de deux constatations :

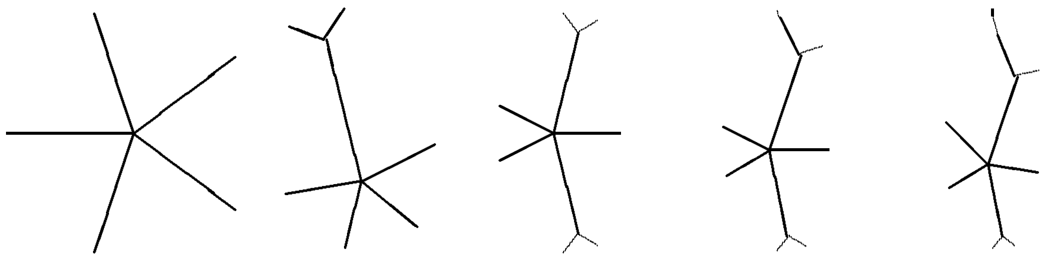
- Si on déforme légèrement le dessin en rajoutant des points, ça ne change pas grand chose. Plus précisément : si on a calculé un revêtement, le revêtement obtenu en scindant une ramification est assez proche.

- Si on calcule des valeurs approchées suffisamment précises, il est possible de revenir à des nombres algébriques.

Cela nous mène donc à une méthode utilisant l'algorithme de Newton pour résoudre un système d'équations à valeurs complexes puis à utiliser des méthodes de réduction de réseaux pour redescendre dans un corps de nombres.

On commence donc par calculer de façon algébrique une *graine* sur laquelle on va faire pousser des excroissances.

Voici par exemple une étoile à cinq branches, à laquelle on rajoute sur deux branches des petites fourches, puis on prolonge l'une des branches...



3 Les groupes de Matthieu M_{23} et M_{24}

3.1 Résumé des données initiales

On peut définir le groupe de Matthieu M_{24} comme étant le groupe agissant sur 24 éléments, engendré par les quatre éléments suivants :

- $(1,2,3,4,5,6,7,8,9,10,11,12)(13,14,15,16,17,18,19,20,21,22,23,24)$
- $(3,15)(4,14)(5,17)(6,9)(10,16)(18,19)(21,24)(22,23)$
- $(2,12)(3,14)(4,20)(5,16)(6,7)(11,15)(13,24)(17,19)$
- $(1,12)(2,11)(4,19)(5,9)(7,8)(10,15)(13,20)(21,23)$

Les quatre générateurs ci-dessus, signalés par Matzat dans [3] appartiennent à quatre classes rationnelles notées $12B$, $2A$, $2A$ et $2A$. Cependant ces quatre classes forment un vecteur qui n'est pas rigide. Il y a 144 quadruplets tels que celui donné ci-dessus, à conjugaison près. En revanche, l'action du groupe des tresses à quatre brins est transitive sur ces 144 quadruplets. Comme M_{24} n'a pas de centre, on en déduit, d'après des résultats de Fried ([2] page 22, Théorème 4.3 par exemple) l'existence d'une famille de revêtements (famille de Hurwitz):

$$\mathcal{F} : \mathcal{T} \to \mathcal{H} \times \mathbf{P}_1(\mathbf{C})$$

avec les définitions et propriétés suivantes:

- $\mathcal{F}$ est un morphisme fini de variétés quasi-projectives, définies sur Q.
- $\mathcal{H}$ est irréductible et la fibre générique $\mathcal{F}^{-1}(h \times \mathbf{P}_1(\mathbf{C}))$ est irréductible. La restriction de $\mathcal{F}$ à cette fibre est un revêtement galoisien de $\mathbf{P}_1(\mathbf{C})$ de groupe de Galois M_{24}. On note ce revêtement $\mathcal{R}_h$.
- Soit $\mathcal{S} = \mathbf{P}_1(\mathbf{C})^4 - \mathcal{D}$ où $\mathcal{D}$ est la classique variété discrimant. Il existe un morphisme Ψ de $\mathcal{H}$ dans $\mathcal{S}$, de degré 144 tel que pour $h \in \mathcal{H}$ un point de $\mathcal{H}$, le revêtement $\mathcal{R}_h$ est ramifié au dessus de $\Psi(h) = (h_1, h_2, h_3, h_4)$. La ramification en h_1 est dans la classe $12B$. Celles en h_2, h_3, h_4 sont dans la classe $2A$.
- La variété $\mathcal{H}$ est birationnellement équivalente à $\mathcal{C} \times \mathbf{P}_1(\mathbf{C}) \times \mathbf{P}_1(\mathbf{C}) \times \mathbf{P}_1(\mathbf{C})$, où $\mathcal{C}$ est obtenue par restriction du revêtement Ψ à la sous-variété de dimension 1 de $\mathcal{S}$ formée des points de la forme $(\lambda, 0, 1, \infty)$.

3.2 Calculs explicites

Dans le cas qui nous interesse, le genre de $\mathcal{C}$ est 1. On le calcule grace à la formule de Hurwitz en regardant l'action du groupe de tresses sur les 144 revêtements ramifiés au dessus de 4 points donnés.

Prouver l'existence de points rationnels sur une courbe de genre 1 n'est pas aisé. On a donc recours à l'artifice suivant. On remplace la courbe $\mathcal{C}$ par la courbe $\mathcal{C}'$ obtenue par restriction de

Ψ aux points de la forme $(\lambda, -1, 1, \infty)$. Pour $t \in \mathcal{C}'$, on a un revêtement φ_t de $\mathbf{P}_1(\mathbf{C})$ ramifié au dessus de $(\lambda(t), -1, 1, \infty)$ ou λ est une fonction de degré 144. On considère le revêtement défini par $\lambda(t)\varphi(t)$, qui est ramifié au dessus de $(\lambda^2, -\lambda, \lambda, \infty)$. On constate que l'ensemble des ramifications est invariant par $\lambda \rightarrow -\lambda$, il existe donc un automorphisme d'ordre 2 sur $\mathcal{C}'$, a, tel que $\lambda(a(t)) = -\lambda(t)$, et $\lambda(t)\varphi(t)$ soit isomorphe à $\lambda(a(t))\varphi(a(t))$. La courbe $\mathcal{C}'/a$ est appelée espace des modules symétrisé. Dans notre cas, cette courbe est de genre 0, munie d'un point rationnel (donc isomorphe à $\mathbf{P}_1$ sur $\mathbf{Q}$), ce que l'on déduit encore de l'action du groupe de tresses sur les revêtements. Cela prouve l'existence dans la famille de revêtements définis sur $\mathbf{Q}$. Remarque : le groupe de symétrie de $(12B, 2A, 2A, 2A)$ est $\mathfrak{S}_3$ (permutations des trois dernières classes), nous n'avons symétrisé que selon le sous groupe d'ordre 2 qui permute les deuxième et troisième classes.

Dans la pratique, on cherche une fonction rationnelle ramifiée au dessus de (∞, A_1, A_2, A_3) $\phi(X)/X^{12}$ où ϕ est un polynôme unitaire de degré 24, tel que

$$\phi = P_1(X)^2 Q_1(X) + A_1 X^{12} = P_2(X)^2 Q_2(X) + A_2 X^{12} = P_3(X)^2 Q_3(X) + A_3 X^{12}$$

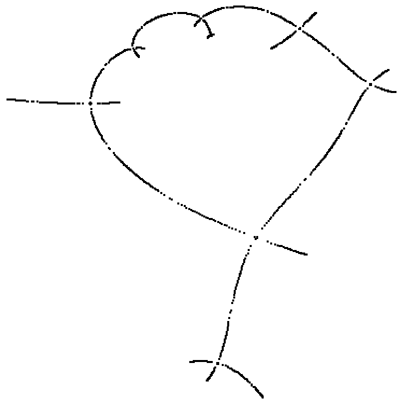
où les P_i et les Q_i sont des polynômes de degré 8.

Puisque la solution de ces équations est une famille à trois paramètres, on peut l'obtenir par déformation continue d'un élément de la famille.

Il suffit donc de calculer un revêtement aussi simple que possible dans cette famille. On choisit un revêtement correspondant à une fibre *singulière* de l'application $\mathcal{F}$. Ces revêtements dégénérés ramifiés au dessus de trois points seulement, correspondent aux points de ramification de Ψ. Ils sont obtenus en rapprochant deux valeurs singulières jusqu'à les confondre. Une fois obtenu ce revêtement singulier, on sépare les deux valeurs singulières (ce qui revient a étudier le système ci-dessus au voisinage d'une valeur critique). On obtient alors un revêtement "régulier" de la famille, que l'on peut perturber numériquement pour en obtenir d'autres, différents.

Une fois que l'on dispose de nombreux revêtements, correpondant à de nombreux points sur la variété $\mathcal{H}$, on recherche numériquement des relations de dépendance entre les coefficients des P_i et des Q_i.

Voici un exemple de revêtement calculé ainsi :



3.3 Résultats en vue

Le calcul ci-dessus doit conduire à la réalisation explicite de M_{24} comme groupe de Galois sur $\mathbf{Q}(T)$. Plus précisément, on doit obtenir une courbe de genre 0, $\mathcal{C}_t$ et un revêtement Galoisien de groupe de Galois M_{24}, $\phi_t : \mathcal{C}_t \rightarrow \mathbf{P}_1(\mathbf{C})$, définis sur $\mathbf{Q}$ et dépendant d'un paramètre rationnel t. Par application du théorème d'irréductibilité de Hilbert, on en déduit que M_{24} est groupe de Galois sur $\mathbf{Q}$.

En fait, on peut aller un peu plus loin. Soit $\mathcal{D}_t$ une courbe algébrique et $\psi_t : \mathcal{D}_t \to \mathcal{C}_t$ un revêtement définis sur $\mathbf{Q}$, tels que $\phi_t \circ \psi_t$ soit la clôture galoisienne de ϕ_t. Alors, ψ_t est un revêtement Galoisien de groupe de Galois le stabilisateur d'un élément dans M_{24}. Ce stabilisateur est appelé M_{23}. On obtient donc une extension de corps de fonctions de groupe de Galois M_{23}. Si pour une valeur de t, la courbe $\mathcal{C}_t$ a un point rationnel, alors son corps de fonctions est purement transcendant et on réalise M_{23} comme groupe de Galois sur $\mathbf{Q}(T)$. On est donc conduit à calculer une famille de coniques et à chercher un point rationnel dans cette famille.

Bibliographie

[1] J.-M. Couveignes, Calcul et rationalité de fonctions de Belyi en genre 0. *Annales de l'Institut Fourier*, to appear, jan. 1994.

[2] P. Debes, M. D. Fried, Nonrigid construction in Galois Theory. *Pacific Journal of Math.*, to appear.

[3] G. Malle, B. H. Matzat, Action of Braids. In *Inverse Galois Theory*, ch. 3, Preprint. University of Heidelberg 1993.

[4] É. Reyssat, Galois Theory for Covering and Riemann Surfaces. In *From Number Theory to Physics*, pages 394–412, 1992. Springer Verlag.

[5] J.-P. Serre, Topics in Galois Theory. Volume 001 of *Research Notes in Mathematics*, Boston, 1992. Jones and Bartlett.