OUTILS POUR L'ÉTUDE DES PROPRIÉTÉS ASYMPTOTIQUES DES ENSEMBLES DE FONCTIONS BOOLÉENNES

par

Robert Rolland

Résumé. — Nous donnons ici les notions de base qui permettent d'aborder les propriétés statistiques de certains ensembles de fonctions booléennes quand le nombre de variables tend vers l'infini. Ces notions ont été précisées et utilisées par François Rodier pour démontrer un certain nombre de propriétés asymptotiques intéressantes.

Table des matières

1. Introduction

Le but de cette note est d'exposer les outils de base pour l'étude des propriétés asymptotiques des fonctions booléennes. On utilisera les

***Classification mathématique par sujets* (2000).** — 11T71.
Mots clefs. — compact de Cantor, fonctions booléennes, transformation de Fourier, mesure de Haar, dualité de Pontryagin.

résultats exposés dans [**4**] concernant le compact de Cantor. Ces outils ont permis à F. Rodier dans [**1**], [**2**] et [**3**], d'obtenir des résultats intéressants sur le comportement asymptotique de la non-linéarité des fonctions booléennes quand le nombre de variables tend vers l'infini.

2. Le compact de Cantor

On trouvera une étude détaillée du compact de Cantor dans [**4**].

2.1. Notations. — Soit $\mathbb{N}^*$ l'ensemble des entiers ≥ 1. Notons :

$$\Omega = \{0,1\}^{\mathbb{N}^*}$$

l'ensemble produit dénombrable d'ensembles à deux éléments.

2.2. La topologie. — Sur Ω on met la topologie produit des espaces topologiques discrets $\{0,1\}$. Ainsi Ω devient un espace compact comme produit d'espaces compacts (théorème de Tichonov). Nous renvoyons à [**4**] pour les détails sur ce compact.

Rappelons rapidement que ce compact est métrisable grâce à la distance :

$$d(x,y) = \begin{cases} 0 & \text{si } x = y \\ 1/\inf\{i \mid x_i \neq y_i\} & \text{sinon} \end{cases},$$

et que c'est un compact totalement discontinu (les composantes connexes sont les parties réduites à un point). La boule ouverte de centre $w = (w_i)_{i\geq 1}$ et de rayon $1/n$ est :

$$B(w,1/n) = \{w_1\} \times \cdots \times \{w_n\} \times \{0,1\} \times \{0,1\} \times \cdots .$$

Rappelons aussi l'importance de l'criture des boules prcdentes sous la forme $\Omega_{j,\nu}$ où $\nu \geq 0$ et où $1 \leq j \leq 2^\nu$ définis par :

$$\Omega_{j,\nu} = \{w_1\} \times \cdots \times \{w_\nu\} \times \{0,1\} \times \{0,1\} \times \cdots ,$$

les w_i constituant les digits du développement binaire de $j-1$, plus prcisment :

$$j - 1 = \sum_{i=1}^{\nu} w_{\nu-i+1} 2^{i-1},$$

ou encore :

$$\frac{j-1}{2^\nu} = \sum_{i=1}^{\nu} \frac{w_i}{2^i}.$$

Pour ν fixé, les $\Omega_{j,\nu}$ sont 2^ν boules ouvertes qui constituent une partition de Ω.

La topologie sur Ω peut aussi être vue comme une limite projective. Soit en effet T_n l'application de $\{0,1\}^{n+1}$ dans $\{0,1\}^n$ qui à $(u_1, u_2, \cdots u_{n+1})$ fait correspondre $(u_1, u_2, \cdots u_n)$. Chaque $\{0,1\}^n$ est muni de la topologie discrète. Grâce à ces transitions, on a une limite projective Ω ainsi que des applications P_n de Ω sur $\{0,1\}^n$ telles que :

$$P_n\left((u_i)_{i\geq 1}\right) = (u_1, u_2, \cdots u_n).$$

La topologie de Ω est la topologie la moins fine rendant continues toutes les applications P_i.

2.3. La mesure. — L'ensemble $\{0,1\}$ est muni d'une structure d'espace mesuré en prenant comme tribu la tribu de toutes les parties de $\{0,1\}$ et comme mesure la probabilité équirépartie :

$$p(\emptyset) = 0, p(\{0\}) = p(\{1\}) = 1/2, p(\{0,1\}) = 1.$$

Nous mettrons sur Ω la probabilité produit et nous la noterons dx. La mesure d'une boule $\Omega_{j,\nu}$ est donnée par :

$$|\Omega_{j,\nu}| = dx(\Omega_{j,\nu}) = \frac{1}{2^\nu}.$$

2.4. Les caractères. — L'espace Ω possède en outre une structure de groupe comme produit de groupes (on considère que $\{0,1\}$ est muni de sa structure de groupe additif à deux éléments habituelle). L'espace Ω est donc un groupe compact, dont la mesure de Haar est la mesure dx que nous avons définie précédemment. Les caractères sont les fonctions de Walsh définies de la façon suivante. On considère pour toute suite u à support fini :

$$u = (u_1, u_2, \cdots u_n, 0, 0, \cdots),$$

le caractère χ_u défini par :

$$\chi_u(v) = (-1)^{\langle u,v\rangle},$$

où :

$$\langle u, v\rangle = \sum_{i\in Support(u)} u_i v_i.$$

Nous renvoyons à [**4**] pour les détails et les démonstrations concernant les caractères du groupe Ω.

2.5. Conclusions et remarques. — Ainsi on a défini Ω comme groupe compact, avec sa mesure de Haar. Il est clair que tout espace qui s'écrit comme produit G^A, où G est le groupe à deux éléments et où A est un ensemble infini dénombrable est un modèle du groupe compact de Cantor. En particulier, $\{-1,1\}^A$ où $\{-1,1\}$ est considéré comme sous-groupe multiplicatif des nombres complexes de module 1 et où A est dénombrable, a la même structure de groupe compact que Ω.

L'ensemble des caractères a été mis en bijection avec l'ensemble des suites ayant un support fini (appelées aussi presque nulles).

3. L'espace V_∞ (ou $\widehat{\Omega}$) des suites presque nulles

3.1. Notations. — Notons pour tout entier $n \geq 1$:

$$E_n = \{0,1\}^n,$$

$$V_n = E_n \times \{0\} \times \{0\} \times \cdots .$$

On définit alors l'espace des suites booléennes presque nulles ou appelées encore suites à support fini par :

$$V_\infty = \bigcup_{n\geq 1} V_n.$$

Nous avons vu qu'en fait V_∞ peut être interprété comme $\widehat{\Omega}$ l'ensemble des caractères de Ω. Par la suite nous noterons indifféremment cet ensemble V_∞ ou $\widehat{\Omega}$.

3.2. La topologie. — Nous mettons sur $\widehat{\Omega}$ la tologie discrète. Ceci peut être compris de deux points de vue différents :

– **topologie limite inductive.** Cette topologie est naturelle puisque on a vu que la topologie sur Ω pouvait être interprétée comme une limite projective. Par dualité on peut donc considérer

la limite inductive des espaces $E_n = \{0,1\}^n$ où les fonctions de transition t_n de E_n dans E_{n+1} sont définies par :

$$t_n\left((u_1, u_2, \cdots u_n)\right) = \left((u_1, u_2, \cdots u_n, 0)\right).$$

La limite inductive est donc $\widehat{\Omega}$ muni de la topologie la plus fine pour laquelle les applications p_n de E_n dans $\widehat{\Omega}$ définies par :

$$p_n\left((u_1, u_2, \cdots u_n)\right) = (u_1, u_2, \cdots u_n, 0, 0, \cdots),$$

sont continues. Cette topologie est la topologie discrète.

– **topologie de la convergence uniforme sur tout compact.** La topologie discrète sur $\widehat{\Omega}$ est aussi la topologie de la convergence uniforme sur tout compact de Ω (et comme ici Ω est compact, c'est la topologie de la convergence uniforme sur Ω).

Ces deux façons de voir conduisent à la même topologie qui fait de $\widehat{\Omega}$ un espace localement compact.

Il faut remarquer que même si $\widehat{\Omega}$ est inclus dans Ω, il n'est pas bon de mettre en avant cette identification de l'ensemble des caractères à une partie de Ω. En particulier, la topologie induite par Ω sur son sous-ensemble $\widehat{\Omega}$ n'est pas la topologie que nous avons définie, et ne correspond pas aux bonnes propriétés de dualité attendues.

3.3. La mesure. — Sur $\widehat{\Omega}$ on prend la tribu de toutes les parties et on définit la mesure par :

$$\mu(A) = \begin{cases} \#A & \text{si } A \text{ est fini} \\ +\infty & \text{sinon} \end{cases}.$$

Cette mesure μ est $\sigma-$finie.

3.4. Les caractères. — Les caractères (continus) de $\widehat{\Omega}$ sont les éléments de Ω.

4. Conclusion sur la dualité de Pontryagin $\langle \Omega, \widehat{\Omega} \rangle$

On a ainsi construit deux groupes topologiques Ω et $\widehat{\Omega}$ tels que :

– Ces groupes sont localement compacts (et même l'un d'entre eux est compact).

– Chacun est le dual de l'autre (avec continuité des caractères bien entendu).
– La topologie de chacun est la topologie de la convergence uniforme sur tout compact de l'autre.

5. Les fonctions booléennes

Nous étudierons les fonctions booléennes sous leur *version exponentielle*, c'est-à-dire comme espaces des fonctions de $\widehat{\Omega}$ dans $\{-1, 1\}$. En effet lorsqu'on a une fonction f de $\widehat{\Omega}$ dans le groupe additif $\{0, 1\}$, il est facile de la transformer en une fonction F de $\widehat{\Omega}$ dans le groupe multiplicatif $\{-1, 1\}$ en prenant :

$$F(x) = (-1)^{f(x)}.$$

5.1. Notations. — On notera $\mathcal{B}_n$ l'espace des fonctions de V_n dans $\{-1, 1\}$ et $\mathcal{B}_\infty$ l'espace des fonctions de $\widehat{\Omega}$ dans $\{-1, 1\}$.

Remarquons que toutes ces fonctions sont continues (puisque sur $\widehat{\Omega}$ on a la topologie discrète.

5.2. La topologie. — Compte tenu des définitions précédentes on a :

$$\mathcal{B}_n = \{-1, 1\}^{V_n},$$

et

$$\mathcal{B}_\infty = \{-1, 1\}^{\widehat{\Omega}}.$$

Comme $\widehat{\Omega}$ est dénombrable, $\mathcal{B}_\infty$ peut être muni de la structure de groupe compact de Cantor. C'est la topologie de cette structure qui sera donnée à $\mathcal{B}_\infty$.

5.3. La mesure. — Pour la mesure, on fait la même démarche. On met sur $\mathcal{B}_\infty$ la mesure habituelle sur un compact de Cantor qui est une probabilité. Ceci va nous permettre de déterminer la probabilité de tel ou tel ensemble de fonctions booléennes ayant telles ou telles propriétés. Nous noterons P cette probabilité.

5.4. Transformation de Fourier. — Nous avons étudié dans [**4**] la transformation de Fourier des fonctions définies sur Ω. Nous regardons maintenant la transformation de Fourier des fonctions définies sur $\widehat{\Omega}$.

Soit $f \in \mathcal{B}_\infty$ une fonction définie sur $\widehat{\Omega}$. Si $u \in \Omega$ on définit, pourvu que l'intégrale existe :

$$\widehat{f}(u) = \int_{\widehat{\Omega}} f(x)(-1)^{\langle x,u\rangle} d\mu(x).$$

Remarquons que l'espace des fonctions intégrables pour la mesure μ n'est rien d'autre que l^1 puisque $\widehat{\Omega}$ est dénombrable. Cette transformation ne sera donc pas applicable à des fonctions booléennes dont les images sont -1 et 1 et qui en aucun cas ne seront dans l^1.

5.5. Les distributions sur Ω. — Une fonction g définie sur Ω est dite localement constante s'il existe un entier $\nu \geq 0$ telle que g soit constante sur chacune des 2^ν composantes $\Omega_{j,\nu}$. Une telle fonction est intégrable et si on note λ_j la valeur de g sur $\Omega_{j,\nu}$ on a alors :

$$\int_\Omega g(x)dx = \frac{1}{2^\nu} \sum_{j=1} 2^\nu \lambda_j.$$

Si on considère la transformation de Fourier d'une telle fonction, on obtient une fonction $\widehat{g}$ définie sur $\widehat{\Omega}$ à support fini.

En effet :

$$\widehat{g}(u) = \int_\Omega g(x)(-1)^{\langle x,u\rangle} dx.$$

Si u a une composante non nulle de rang $> \nu$ alors la fonction de Walsh $(-1)^{\langle x,u\rangle}$ oscille sur chacun des morceaux $\Omega_{j,\nu}$ où g est constante et donc l'intégrale est nulle.

Soit maintenant $f \in \mathcal{B}_\infty$ une fonction définie sur $\widehat{\Omega}$. Définissons $\widehat{f}$ comme la forme linéaire sur l'espace des fonctions localement constantes sur Ω :

$$\widehat{f}(g) = \int_{\widehat{\Omega}} \widehat{g}(x) f(x) d\mu(x) = \sum_{x \in Support(\widehat{g})} \widehat{g}(x) f(x).$$

6. Les résultats de F. Rodier

François Rodier a utilisé dans plusieurs articles cet outillage pour obtenir des résultats sur la non-linéarité des fonctions booléennes. En particulier on pourra se reporter à [**2**] et à [**3**].

6.1. Fonctions affines, code de Reed-Muller d'ordre 1. — On considère l'ensemble $\mathcal{A}_m$ des fonctions booléennes affines à m variables booléennes : une telle fonction f de $\{0,1\}^m$ dans $\{0,1\}$ est de la forme :

$$f(x_1, x_2, \cdots, x_m) = a_1x_1 + a_2x_2 + \cdots a_mx_m + b = \langle a, x\rangle + b,$$

où $a \in \{0,1\}^m$ et $b \in \{0,1\}$.

Le code de Reed-Muller $RM(1,m)$ d'ordre 1 et de longueur 2^m est l'espace des mots :

$$(f(x))_{x\in\{0,1\}^m},$$

où $f \in \mathcal{A}_m$.

Rappelons que si f est une fonction booléenne de $\{0,1\}^m$ dans $\{0,1\}$ on introduit la distance de Hamming de la fonction f au code de Reed-Muller d'ordre 1,qu'on appelle la non-linéarité de f :

$$D_m(f) = \inf_{g\in RM(1,m)} d(f,g),$$

où $d(f,g)$ est la distance de Hamming entre f et g, c'est-à-dire :

$$d(f,g) = \#\{x \in \{0,1\}^m \mid f(x) \neq g(x)\}.$$

Le rayon de recouvrement du code de Reed-Muller d'ordre 1 est alors donné par :

$$\rho_m = \max_f D_m(f).$$

Ce rayon constitue la distance entre le code de Reed-Muller d'ordre 1 et le mot le plus éloigné de ce code au sens de la distance de Hamming.

Il est bien connu que :

$$D_m(f) = 2^{m-1} - \frac{1}{2}S_m(f),$$

où

$$S_m(f) = \max_{v\in\{0,1\}^m} \left| \sum_{x\in\{0,1\}^m} (-1)^{f(x)+\langle v,x\rangle} \right|.$$

En conséquence si on associe à chaque fonction f la fonction $F \in \mathcal{B}_m$ de $\{0,1\}^m$ dans $\{-1,1\}$ définie par $F(x) = (-1)^{f(x)}$ alors :

$$S_m(f) = ||\widehat{F}||_\infty^{(m)} = \max_{v\in\{0,1\}^m} \left|\widehat{F}(v)\right|$$

et

$$D_m(f) = 2^{m-1} - \frac{1}{2}||\widehat{F}||_\infty^{(m)}.$$

Pour m pair, on connaît exactement le rayon de recouvrement :

$$\rho_m = 2^{m-1} - 2^{\frac{m}{2}-1},$$

et cette borne est atteinte par les fonctions courbes, dont la classe n'est pas très bien connue.

Pour m impair, on ne connaît pas (sauf cas particuliers) la valeur exacte du rayon de recouvrement, la notion de fonction courbe n'a plus de sens. Cependant la notion de fonction maximalement non-linéaire a bien entendu un sens. Les fonctions maximalement non-linéaires sont celles pour lesquelles :

$$S_m(f) = ||\widehat{F}||_\infty^{(m)} = \max_{v\in\{0,1\}^m} \left|\widehat{F}(v)\right|$$

est minimum et donc qui rendent la non-linéarité $D_m(f)$ maximum.

Si $F \in \mathcal{B}_\infty$, notons F_m la fonction de $\mathcal{B}_m$ obtenu par restriction de F à V_m. Avec ces notations, on peut énoncer le très beau résultat obtenu par F. Rodier dans [**3**] :

Théorème 6.1 **(F. Rodier)**. — *Pour P-presque toute fonction $F \in \mathcal{B}_\infty$ on a :*

$$\lim_{m\to+\infty} \frac{||\widehat{F_m}||_\infty^{(m)}}{\sqrt{2^{m+1}m\ln 2}} = 1.$$

Références

[1] F. Rodier – « On the nonlinearity of boolean functions », in *Proceedings of WCC2003, workshop on coding and cryptography*, INRIA, 2003, p. 397–405.

[2] ———, « Sur la non-linéarité des fonctions booléennes », *Acta Arithmetica* **115** (2004), p. 1–22.

[3] ———, « Asymptotic nonlinearity of boolean functions », *Designs Codes and Cryptography* **40** (2006), p. 59–70.

[4] R. Rolland – « Rappels : Analyse de fourier sur le compact de cantor », *Dossiers Acrypta* (2004 Rév. 2007).

---

10 décembre 2008

R. Rolland, Association ACrypTA, 50 Rue Edmond Rostand 13006 Marseille,
E-mail : robert.rolland@acrypta.fr