ACTA ARITHMETICA
LXXVI.2 (1996)

Minoration de discrépance en dimension deux

par

Henri Faure et Henri Chaix (Marseille)

I. Introduction. Rappelons tout d'abord la définition de la discrépance pour une suite infinie $X = (x_n)_{n\geq 1}$ à valeurs dans le cube unité de dimension s, $I^s = [0,1[^s$.

Un *pavé* P de I^s est le produit de s intervalles $[a_k, b_k[$ de I.

Etant donné un ensemble d'entiers T, positifs ou nuls, on note $A(P;T;X)$ le nombre de points de la suite X d'indices n appartenant à T tels que x_n soit élément de P et on appelle *écart* $E(P;T;X)$ la différence $A(P;T;X) - |T|\cdot|P|$, où $|T|$ est le cardinal de T et $|P|$ le volume de P. Alors la *discrépance* $D(N,X)$ de la suite X est définie par

$$D(N,X) = \sup_{P\in\mathcal{P}_s} |E(P;]0,N];X)|,$$

où $\mathcal{P}_s$ est l'ensemble des pavés de I^s.

Si on se limite à la famille $\mathcal{P}_s^*$ des pavés P où les a_k sont nuls, on obtient la *discrépance à l'origine* D^*. Compte tenu de l'imprécision des connaissances actuelles en dimension $s \geq 2$, on peut se limiter à l'étude de D^*.

En dimension quelconque, la seule minoration connue est celle de K. F. Roth [8], obtenue en 1954 : il existe une constante $C_s > 0$ telle que, pour toute suite infinie X, on ait $\limsup_{N\to\infty}(D^*(N,X)/(\log N)^{s/2}) \geq C_s$.

Les deux seules améliorations apportées à ce théorème sont de W. M. Schmidt [9] en 1972 et G. Halász [4] en 1981 qui, par des méthodes différentes, ont obtenu l'ordre $\log N$ au lieu de $\sqrt{\log N}$ en dimension un, puis de J. Beck [1] en 1989 qui est passé de $\log N$ à $(\log N)(\log\log N)^{1/8-\varepsilon}$ en dimension deux.

Un certain nombre de suites ayant de très faibles irrégularités ont été construites en vue de leur utilisation dans les méthodes d'intégration de Monte Carlo; l'ordre de croissance pour leur discrépance est majoré par $(\log N)^s$ en dimension s; compte tenu de la méthode de Roth qui donne en fait une minoration de la discrépance quadratique, on conjecture que $(\log N)^s$ est l'ordre exact.

Chronologiquement, on peut citer les constructions de J. H. Halton [5] en 1960, I. M. Sobol' [10] en 1967, S. Srinivasan [11] en 1978, H. Faure [2] en 1982 et H. Niederreiter [6], [7] en 1987–1988. Il faut noter que même pour ces suites particulières on ne dispose que de la minoration de Roth (ou de Beck en dimension deux).

Dans cet article, nous obtenons, pour la première fois, l'ordre exact $(\log N)^2$ pour la discrépance d'une suite particulière en dimension deux, désignée par S, construite indépendamment par Sobol' et Srinivasan. Ce résultat a été annonçé dans la note [3].

En fait, cette suite S est la suite en dimension deux ayant la plus faible discrépance actuellement connue; si on pose

$$d_s(X) = \limsup_{N\to\infty}(D^*(N,X)/(\log N)^s),$$

on a la majoration $d_2(S) \le 1/(8(\log 2)^2) = 0{,}26\ldots$, obtenue par Niederreiter [6] en améliorant les bornes précédemment calculées par Sobol', Srinivasan et Faure; pour la meilleure suite H de Halton on a seulement $d_2(H) \le 1/(2\log 2\log 3) = 0{,}65\ldots$ [2].

Avec la notation ci-dessus, notre résultat s'énonce :

$$d_2(S) \ge \frac{1}{24(\log 2)^2} = 0{,}08\ldots$$

L'approche numérique et l'analogie avec les suites du même type en dimension un nous conduisent à conjecturer que la borne inférieure ci-dessus est la valeur exacte de $d_2(S)$.

Dans les paragraphes suivants, il ne sera plus question que de cette suite S en dimension deux.

II. Définition de la suite S et théorème

Suite de van der Corput en base b. Etant donnés des entiers $b \ge 2$ et $n \ge 1$, soit $n-1 = \sum_{r=0}^{\infty} a_r(n)b^r$ le développement de $n-1$ en base b; par définition, la *suite de van der Corput en base b* est la suite ϕ_b à valeurs dans I définie par $\phi_b(n) = \sum_{r=0}^{\infty} a_r(n)b^{-r-1}$.

Matrice de Pascal et suite associée. Soit $C = \left(\binom{h}{l}\right)$, où $\binom{h}{l} = 0$ si $l > h$; il est facile de voir que $C^k = \left(\binom{h}{l}k^{h-l}\right)$.

En posant $x_n^k = C^{k-1}\phi_b(n) \bmod b$, c'est-à-dire

$$x_n^k = \sum_{j=0}^{\infty} y_j^k(n)b^{-j-1}$$

avec

$$y_j^k(n) = \sum_{r\ge j}\binom{r}{j}(k-1)^{r-j}a_r(n) \bmod b,$$

on construit une suite de terme général $x_n = (x_n^1, \ldots, x_n^s)$, à valeurs dans I^s, de coordonnées distinctes dès que $b \geq s$.

Le cas particulier $b = s = 2$ donne la suite S, objet de notre étude.

Remarques. 1. Les suites de Halton s'obtiennent en prenant des $\phi_b(n)$ avec des bases premières entre elles deux à deux sur chaque coordonnée. En dimension deux, la plus simple est $(\phi_2(n), \phi_3(n))$.

2. Sobol' et Srinivasan ont construit chacun des familles de suites, Sobol' en faisant agir sur ϕ_2 des polynômes primitifs de $\mathbb{F}_2[X]$ et Srinivasan par un algorithme pas à pas où on a deux choix possibles à chaque étape; dans les deux cas, la suite S correspond aux situations les plus simples (polynômes du premier degré pour Sobol', toujours le même choix pour Srinivasan).

Théorème. *Soient le pavé* $Q = [0, 2/3[^2$ *et la suite* $(N_\lambda)_{\lambda \geq 1}$ *définie par* $N_\lambda = (16^{\lambda+1} - 1)/15$. *Alors*

$$E(Q;]0, N_{2^\tau - 1}]; S) = \frac{2}{3} 4^\tau + \frac{17}{9} 2^\tau - 3^\tau - 1,$$

où τ *est un entier supérieur ou égal à* 1.

En fait, nous obtenons des formules exactes pour tout entier λ, mais elles ne fournissent pas un résultat final explicite; de toute façon, l'approche numérique effectuée montre que la minoration n'en serait pas améliorée pour autant.

Corollaire. *On a la minoration*

$$d_2(S) \geq \frac{2}{3} \cdot \frac{1}{(\log 16)^2} = \frac{1}{24(\log 2)^2}.$$

Problèmes. Cette minoration est un premier pas dans l'étude du problème général des minorations de discrépance pour les suites usuelles :

Qu'en est-il pour les familles voisines de Sobol' et Srinivasan?

Que peut-on dire pour les bases b autres que 2 et pour les suites de Halton en dimension deux?

Que dire pour les dimensions supérieures?

Les questions les plus abordables semblent concerner les bases $b > 2$ et les suites de Halton en dimension 2.

III. Propriétés de la matrice de Pascal modulo deux

Notations. Etant donnée une matrice infinie M, on désigne par $M^l_{c',c}$ la sous-matrice de M obtenue en conservant les l premières lignes et les colonnes de rang compris entre c' et c inclus; pour simplifier, on convient de noter $M^l_c = M^l_{1,c}$.

Premières propriétés. La relation classique entre les coefficients du binôme s'écrit modulo 2 de trois manières différentes :

P1. $\binom{h}{l} = \binom{h-1}{l} + \binom{h-1}{l-1}$,

P2. $\binom{h-1}{l} = \binom{h}{l} + \binom{h-1}{l-1}$,

P3. $\binom{h-1}{l-1} = \binom{h}{l} + \binom{h-1}{l}$.

On en déduit les propriétés suivantes qu'on utilisera au cours de la démonstration :

P4. *Pour tout j entier et pour tout p entier vérifiant* $0 \leq p \leq j-1$, *on a*

$$\binom{2j}{2p+1} = 0.$$

P5. *Pour tout j entier et pour tout p entier vérifiant* $0 \leq p \leq j$, *on a*

$$\binom{2j}{2p} = \binom{j}{p}.$$

P6. *Pour tout j entier et pour tout p entier vérifiant* $0 \leq p \leq j$, *on a*

$$\binom{2j+1}{2p+1} = \binom{j}{p}.$$

P7. *Pour tout j entier et pour tout p entier vérifiant* $0 \leq p \leq j$, *on a*

$$\binom{2j+1}{2p} = \binom{j}{p}.$$

Construction automatique de la matrice de Pascal modulo deux

P8. *Pour tout entier* $\tau \geq 0$ *et pour tous entiers l et h vérifiant* $0 \leq l \leq 2^\tau - 1$ *et* $0 \leq h \leq 2^\tau - 1$, *on a*

$$\binom{h}{l} = \binom{h+2^\tau}{l} = \binom{h+2^\tau}{l+2^\tau}.$$

Grâce à cette propriété la matrice de Pascal se reproduit par blocs de la façon suivante :

$$C_{2^\tau}^{2^\tau} = \begin{pmatrix} C_{2^{\tau-1}}^{2^{\tau-1}} & C_{2^{\tau-1}}^{2^{\tau-1}} \\ 0 & C_{2^{\tau-1}}^{2^{\tau-1}} \end{pmatrix}.$$

En particulier, on a les deux propriétés qui serviront ultérieurement :

P9. *Pour l entier vérifiant* $1 \leq l \leq 2^\tau - 1$, *on a* $\binom{2^\tau}{l} = 0$.

P10. *Pour l entier vérifiant* $0 \leq l \leq 2^\tau - 1$, *on a* $\binom{2^\tau+l}{l} = 1$.

R e m a r q u e. Notons que les propriétés P4 à P10 résultent aussi immédiatement de la congruence de Lucas pour les coefficients binomiaux modulo 2 :

$$\binom{h}{l} = \prod_{r=0}^{\infty} \binom{h_r}{l_r} \quad \text{avec} \quad h = \sum_{r=0}^{\infty} h_r 2^r \text{ et } l = \sum_{r=0}^{\infty} l_r 2^r$$

développements binaires de h et l.

Autres propriétés utiles

P11. *Pour tout entier* $\tau \ge 1$, *pour tout entier* ν *vérifiant* $2^{\tau-1} \le \nu \le 2^\tau - 1$ *et pour tout entier* l *vérifiant* $0 \le l \le 2^\tau - 2$, *on a*

$$\sum_{j=\nu}^{2^\tau - 1} \binom{j}{l} = \binom{\nu}{l+1}.$$

Preuve. On procède par récurrence descendante sur ν. La propriété est vraie pour $\nu = 2^\tau - 1$ et pour $0 \le l \le 2^\tau - 2$ puisqu'on a $\binom{2^\tau - 1}{l} = \binom{2^\tau - 1}{l+1} = 1$, d'après la construction automatique de la matrice de Pascal. Supposons-la vraie pour $\nu + 1$; d'après P2 on a

$$\sum_{j=\nu}^{2^\tau - 1} \binom{j}{l} = \binom{\nu}{l} + \sum_{j=\nu+1}^{2^\tau - 1} \binom{j}{l} = \binom{\nu}{l} + \binom{\nu+1}{l+1} = \binom{\nu}{l+1},$$

d'où la propriété pour ν. ∎

P12. *Pour* l *compris entre* 0 *et* $2^{\tau-1} - 2$ *inclus*, *on a*

$$\sum_{j=2^{\tau-1}}^{2^\tau - 1} \binom{j}{l} = 0.$$

La propriété s'obtient en utilisant P11 et P9.

P13 (Convolution de Vandermonde). *Etant donnés les entiers* n, m, l *vérifiant* $0 \le l \le \min(n, m)$, *on a*

$$\binom{n+m}{l} = \sum_{j=0}^{l} \binom{n}{l-j} \binom{m}{j}.$$

Matrices carrées suspendues dans la matrice de Pascal

P14. *Pour tous entiers* c *et* l *strictement positifs*, *la matrice suspendue* $C^l_{c,c+l-1}$ *est régulière.*

Preuve. En utilisant la propriété P1, on constate que la somme de la ligne k et de la ligne $k-1$ de la matrice $C^l_{c,c+l-1}$ est égale à la ligne k de la matrice $C^l_{c+1,c+l}$; en itérant l'opération de $k = l$ à 2, on obtient $\det(C^l_{c,c+l-1}) = \det(C^l_{c+1,c+l})$; la propriété en résulte par récurrence en remarquant que $\det(C^l_{1,l}) = 1$. ∎

IV. Démonstration du théorème. Nous noterons $E(N_\lambda) = E(Q;]0, N_\lambda]; S)$ et $E(S(T)) = E(Q; T; S)$.

Pavés élémentaires et réseaux

• Un *pavé élémentaire en base* 2 *de* I^2 est un pavé de la forme $[u/2^p,(u+1)/2^p[\times[v/2^q,(v+1)/2^q[$, avec u,v,p,q entiers tels que $0\le u<2^p$ et $0\le v<2^q$;

• un $(0,m,2)$-*réseau en base* 2 est un ensemble fini de 2^m points de I^2 tel que tout pavé élémentaire de volume 2^{-m} contienne exactement un point du réseau;

• une $(0,2)$-*suite en base* 2 est une suite infinie à valeurs dans I^2 telle que, pour tous les entiers m et l, $X_m^l=\{x_{l2^m+1},\dots,x_{(l+1)2^m}\}$ est un $(0,m,2)$-réseau en base 2.

LEMME 0 [10]. *La suite* S *est une* $(0,2)$-*suite en base* 2.

Preuve. Nous en donnons la démonstration pour faciliter la compréhension du lemme 3 et faire en sorte que l'article se suffise à lui-même.

D'après la définition d'une $(0,2)$-suite en base 2, étant donnés deux entiers naturels m et l et un pavé élémentaire $P=[u/2^p,(u+1)/2^p[\times[v/2^q,(v+1)/2^q[$ de volume 2^{-m}, il faut montrer que $P\cap S_m^l$ est réduit à un seul élément.

Soit $n\ge 1$ et $n-1=\sum_{r=0}^{\infty}a_r(n)2^r$ le développement de $n-1$ en base 2.

La condition $x_n\in S_m^l$ se traduit par $l2^m<n\le(l+1)2^m$, donc les entiers $a_r(n)$ sont déterminés avec unicité pour $r\ge m$ par la donnée de m et l.

La condition $x_n\in P$, c'est-à-dire $u\le 2^px_n^1<u+1$ et $v\le 2^qx_n^2<v+1$ avec $p+q=m$, s'écrit (en désignant par ${}^tM$ la matrice transposée de M)

$$\begin{pmatrix} I_m^p \\ C_m^q \end{pmatrix} {}^t(a_0(n)\ \dots\ a_{m-1}(n)) = {}^t(u_1\ \dots\ u_p\ v_1\ \dots\ v_q)$$

avec

$$\frac{u}{2^p}=\sum_{k=1}^{p}\frac{u_k}{2^k}\qquad\text{et}\qquad\frac{v}{2^q}=\sum_{k=1}^{q}\frac{v_k}{2^k},$$

compte tenu de la construction de la suite S; ce système linéaire est de Cramer d'après la propriété P14 de la matrice binomiale, d'où l'existence et l'unicité de la solution $a_0(n),\dots,a_{m-1}(n)$. On en déduit l'existence d'un unique point de S_m^l appartenant à P. ■

LEMME 1 (Expression de $E(N_\lambda)$). *La suite* (l_μ) *étant définie par* $l_0=0$ *et* $l_\mu=\sum_{i=1}^{\mu}2^{4i}$ *pour* $\mu\ge 1$, *on a*

$$E(N_\lambda)=\sum_{\nu=0}^{\lambda}E(S_{4\nu}^{l_{\lambda-\nu}}).$$

Preuve. D'après la définition de N_λ, on a $N_\lambda=\sum_{i=0}^{\lambda}2^{4i}$; on en déduit la décomposition de l'intervalle $]0,N_\lambda]$ en réunion d'intervalles disjoints

$$]0, N_\lambda] = \bigcup_{\nu=0}^{\lambda}]l_{\lambda-\nu}2^{4\nu}, (l_{\lambda-\nu}+1)2^{4\nu}];$$

par additivité de l'écart, on obtient la formule annoncée. ■

Lemme 2 (Expression de $E(S_{4\nu}^{l_{\lambda-\nu}})$ pour $\nu \geq 1$). *Posons successivement* :

$$\alpha_k = \sum_{i=0}^{2\nu-k} 2^{-2i-1}, \quad \alpha'_k = \alpha_k + 2^{-4\nu+2k-1} \quad \textit{pour } 1 \leq k \leq 2\nu$$

et

$$\alpha_{2\nu+1} = 0, \quad \alpha'_{2\nu+1} = 1;$$

$$\beta_1 = 0, \quad \beta_k = \sum_{i=0}^{k-2} 2^{-2i-1} \quad \textit{pour } 2 \leq k \leq 2\nu+1,$$

$$\beta'_k = \beta_k + 2^{-2k+1} \quad \textit{pour } 1 \leq k \leq 2\nu, \quad \beta'_{2\nu+1} = \beta_{2\nu+1} + 2^{-4\nu}.$$

Puis posons

$$\pi_k = [\alpha_k, \alpha'_k[\times [\beta_k, \beta'_k[\quad \textit{pour } 1 \leq k \leq 2\nu+1$$

et

$$D_\nu = Q \cap \Big(\bigcup_{k=1}^{2\nu+1} \pi_k\Big).$$

Alors

$$E(S_{4\nu}^{l_{\lambda-\nu}}) = A(D_\nu; S_{4\nu}^{l_{\lambda-\nu}}) - \frac{2}{3}\left(\nu + \frac{2}{3}\right).$$

Preuve. Le pavé Q est réunion disjointe de pavés élémentaires inclus dans Q et des pavés $\pi_k \cap Q$ (pour $1 \leq k \leq 2\nu+1$). Les pavés élémentaires inclus dans Q ont un écart nul sur l'intervalle d'entiers concerné en vertu de la propriété des pavés élémentaires. D'après l'additivité de l'écart, le calcul de l'écart sur Q se réduit donc au calcul de $A(D_\nu; S_{4\nu}^{l_{\lambda-\nu}}) - |D_\nu|2^{4\nu}$.

Le calcul de $A(D_\nu; S_{4\nu}^{l_{\lambda-\nu}})$ résultera des lemmes 3 à 7. D'autre part, par construction,

$$|D_\nu| = \sum_{k=1}^{2\nu} |[\alpha_k, 2/3[\times [\beta_k, \beta'_k[| + |[\alpha_{2\nu+1}, 2/3[\times [\beta_{2\nu+1}, 2/3[|;$$

d'après la définition des α_k, on trouve $\frac{2}{3} - \alpha_k = \frac{1}{3} \cdot 2^{-4\nu+2k-1}$ pour $1 \leq k \leq 2\nu+1$ et par ailleurs $\frac{2}{3} - \beta_{2\nu+1} = \frac{1}{3} \cdot 2^{-4\nu+1}$, ce qui donne

$$|D_\nu| = \frac{1}{3}\sum_{k=1}^{2\nu} 2^{-2k+1}2^{-4\nu+2k-1} + \frac{1}{9} \cdot 2^{-4\nu+2} = \frac{2}{3}\left(\nu + \frac{2}{3}\right)2^{-4\nu}. \ ■$$

Remarque. Pour $\nu = 0$, on obtient directement $E(S_0^{l_\lambda}) = 1 - \frac{4}{9}$. En effet, $x^1_{N_\lambda-1} = \sum_{h=1}^{\lambda} 2^{-4h-1} = \phi_2(N_\lambda - 1) < \frac{1}{16}$ et $x^2_{N_\lambda-1} = Cx^1_{N_\lambda-1}$ est inférieur à $\frac{1}{16}$ si λ est pair et compris entre $\frac{1}{2}$ et $\frac{1}{2}+\frac{1}{16}$ si λ est impair; d'où $A(Q;]N_\lambda-1,N_\lambda])=1$.

Lemme 3 (Condition pour que $\pi_k\cap Q\cap S_{4\nu}^{l_{\lambda-\nu}}\neq\emptyset$). *Pour* $1\le\nu<\lambda$ *et* $1<k\le 2\nu$, *soit* $\Delta(\lambda,\nu,k)$ *le déterminant d'ordre* $2\nu+1$:

$$\begin{vmatrix}
1 & \dots & 0 & \dots & 0 & 1\\
0 & & & & & \\
\vdots & \ddots & 0 & \vdots & \vdots & \vdots\\
0 & \dots & 1 & \dots & 0 & 1\\
\binom{0}{0} & \dots & \binom{2\nu-k}{0} & \dots & \binom{2\nu-1}{0} & 1+\sum_{j=\nu+1}^{\lambda}\binom{2j}{0}\\
\vdots & & \vdots & \vdots & \vdots & \vdots\\
\binom{0}{k-2} & \dots & \binom{2\nu-k}{k-2} & \dots & \binom{2\nu-1}{k-2} & 1+\sum_{j=\nu+1}^{\lambda}\binom{2j}{k-2}\\
\binom{0}{k-1} & \dots & \binom{2\nu-k}{k-1} & \dots & \binom{2\nu-1}{k-1} & \sum_{j=\nu+1}^{\lambda}\binom{2j}{k-1}
\end{vmatrix},$$

pour $k=1$, *le déterminant est le même en prenant en compte la dernière ligne et pour* $\nu=\lambda$, *il faut convenir que* $\sum_{j=\lambda+1}^{\lambda}\binom{2j}{k-1}=0$. *Alors*

$$A(\pi_k\cap Q;S_{4\nu}^{l_{\lambda-\nu}})=1 \quad \textit{si et seulement si} \quad \Delta(\lambda,\nu,k)=0 \bmod 2.$$

Preuve. Il s'agit de caractériser les points x_n de la suite appartenant à $\pi_k\cap Q$, d'indice n appartenant à $\{l_{\lambda-\nu}2^{4\nu}+1,\dots,(l_{\lambda-\nu}+1)2^{4\nu}\}$. Rappelons que l'ensemble $\pi_k\cap S_{4\nu}^{l_{\lambda-\nu}}$ contient un et un seul point d'après la propriété des pavés élémentaires puisque S est une $(0,2)$-suite (voir le lemme 0).

La condition sur n se traduit par $a_{4\nu+h}(n)=l_{\lambda-\nu,h}$, pour h compris entre 0 et $4(\lambda-\nu)$ où $n-1=\sum_{j=0}^{4\lambda}a_j(n)2^j$ et $l_{\lambda-\nu}=\sum_{h=0}^{4(\lambda-\nu)}l_{\lambda-\nu,h}2^h$ (rappelons que $l_{\lambda-\nu,h}=1$ si h est multiple de 4 et 0 sinon).

La condition $x_n\in\pi_k$, c'est-à-dire $\alpha_k\le x_n^1<\alpha'_k$ et $\beta_k\le x_n^2<\beta'_k$, s'écrit

$$\begin{pmatrix} I_{4\lambda+1}^{4\nu-2k+1}\\ C_{4\lambda+1}^{2k-1}\end{pmatrix}A=\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

où A est la colonne des composantes binaires de $n-1$ $(a_0(n),\dots,a_{4\lambda}(n))$, α la colonne des $(4\nu-2k+1)$ composantes binaires de α_k $(1,0,1,0,\dots,0,1)$ et β la colonne des $(2k-1)$ composantes binaires de β_k $(1,0,1,0,\dots,0,1,0,0)$.

Montrons que si $x_n\in\pi_k\cap S_{4\nu}^{l_{\lambda-\nu}}$ alors $x_n\in Q$ équivaut à $a_j=a_j(n)=0$ pour j allant de $4\nu-2k+1$ à $4\nu-1$. En effet, on sait que

$$\begin{aligned}
&a_1=a_3=\dots=a_{4\nu-2k-1}=0,\\
&a_{4\nu+1}=a_{4\nu+3}=\dots=a_{4\lambda-1}=0,\\
&a_0=a_2=\dots=a_{4\nu-2k}=1,
\end{aligned}$$

donc x_n dans Q implique $a_{4\nu-2k+1}=0$, d'où la propriété si $k=1$; si $k>1$, les $a_1, a_3, \dots, a_{4\lambda-1}$ vérifient le système $C_{2\lambda}^{k-1}\ {}^t(a_1\ a_3\ \dots\ a_{4\lambda-1}) = 0$; les seules décimales non nulles a priori sont $a_{4\nu-2k+3}, \dots, a_{4\nu-1}$ et elles vérifient le système homogène dont la matrice est une matrice carrée suspendue de la matrice de Pascal, donc régulière (d'après P14), d'où la nullité de ces décimales. La réciproque est évidente.

En conséquence, toujours d'après les propriétés de C, on a $x_n \in \pi_k \cap S_{4\nu}^{l_{\lambda-\nu}} \cap Q$ si et seulement si les inconnues $a_0, a_2, \dots, a_{4\lambda}$ de $n-1$ vérifient le système

$$\begin{pmatrix} I_{2\lambda+1}^{2\nu-k+1} \\ C_{2\lambda+1}^{k} \end{pmatrix} {}^t(a_0\ a_2\ \dots\ a_{4\lambda}) = {}^t(1\ \dots\ 1\ 0)$$

ou encore, en passant au second membre la partie déjà connue (correspondant à $a_{4\nu}, \dots, a_{4\lambda}$), si et seulement si les inconnues $a_0, a_2, \dots, a_{4\nu-2}$ vérifient le système de $2\nu+1$ équations à 2ν inconnues :

$$\begin{pmatrix} I_{2\nu}^{2\nu-k+1} \\ C_{2\nu}^{k} \end{pmatrix} {}^t(a_0\ a_2 \dots\ a_{4\nu-2}) = {}^t(b_1\ \dots\ b_{2\nu+1})$$

avec $b_h = 1$ pour h allant de 1 à $2\nu - k + 1$, et

$$b_{2\nu-k+2+h} = 1 + \sum_{j=\nu+1}^{\lambda} \binom{2j}{h} \qquad \text{pour } h \text{ allant de 0 à } k-2,$$

$$b_{2\nu+1} = \sum_{j=\nu+1}^{\lambda} \binom{2j}{k-1}.$$

Ce système privé de sa dernière équation est de Cramer; il a donc une solution unique si et seulement si le déterminant caractéristique $\Delta(\lambda, \nu, k)$ de la dernière équation est nul. ∎

R e m a r q u e. Le cardinal de $\pi_{2\nu+1} \cap Q \cap S_{4\nu}^{l_{\lambda-\nu}}$ est toujours égal à un. En effet, la condition $x_n \in \pi_{2\nu+1} \cap S_{4\nu}^{l_{\lambda-\nu}}$ s'écrit

$$C_{4\lambda+1}^{4\nu}\,{}^t(a_0\ a_1 \dots\ a_{4\lambda}) = {}^t(1\ 0\ 1\ \dots\ 1\ 0);$$

les décimales $a_{4\nu}, \dots, a_{4\lambda}$ étant connues, le système précédent est de Cramer en les inconnues $a_0, a_1, \dots, a_{4\nu-2}$; sa solution est donnée par $a_1 = a_3 = \dots = a_{4\lambda-1} = 0$ et par la solution de

$$C_{2\lambda+1}^{2\nu}\,{}^t(a_0\ a_2 \dots\ a_{4\lambda}) = {}^t(1\ 1\ \dots\ 1),$$

système de Cramer en les inconnues $a_0, a_2, \dots, a_{4\nu-2}$; le système initial admet donc toujours une seule solution dont les décimales impaires sont nulles, ce qui montre que x_n appartient à Q, d'où la remarque.

LEMME 4 (Opération de décalage). *Soit un k-uplet d'entiers $(l_1, \ldots, l_k)$; on appelle décalage l'opération qui lui associe le k-uplet*

$$(l_1, l_2 + l_1, \ldots, l_{k-1} + l_{k-2}, l_k + l_{k-1}).$$

Après d décalages, le dernier terme du k-uplet obtenu s'écrit

$$\sum_{h=0}^{\min(d,k-1)} \binom{d}{h} l_{k-h}.$$

Preuve. Notons $(l_1^d, \ldots, l_k^d)$ le k-uplet obtenu après d décalages et montrons par récurrence sur d que

$$l_{k'}^d = \sum_{h=0}^{\min(d,k'-1)} \binom{d}{h} l_{k'-h} \quad \text{pour } 2 \le k' \le k.$$

Par définition du décalage, les formules sont vraies pour $d = 1$ et pour $d \ge 2$ on a

$$l_{k'}^{d+1} = l_{k'}^d + l_{k'-1}^d.$$

Si $k' - 1 \le d$, on a

$$\min(d, k'-1) = k'-1, \quad \min(d, k'-2) = k'-2 \quad \text{et} \quad \min(d+1, k'-1) = k'-1;$$

si $k' - 1 > d$, on a

$$\min(d, k'-1) = d, \quad \min(d, k'-2) = d \quad \text{et} \quad \min(d+1, k'-1) = d+1;$$

le résultat est alors obtenu en utilisant la formule P1 : $\binom{d}{h} + \binom{d}{h-1} = \binom{d+1}{h}$; d'où le lemme en faisant $k' = k$. ∎

LEMME 5 (Calcul de $\Delta(\lambda, \nu, k)$). *L'entier ν étant donné $(1 \le \nu \le \lambda)$, on définit l'entier μ par $2^{\mu-1} \le \nu < 2^\mu$. Alors, pour $2p$ et $2p+1$ compris entre 1 et 2ν inclus, on a les relations*

$$\Delta(\lambda, \nu, 2p) = \binom{2^\mu - \nu + p - 1}{p} + \binom{2^\mu - \nu + p + \lambda}{p} \bmod 2$$

et

$$\Delta(\lambda, \nu, 2p+1) = \binom{2^\mu - \nu + p - 1}{p} + \binom{2^\mu - \nu + p + \lambda + 1}{p+1} \bmod 2.$$

Preuve. 1. Traitons d'abord le cas $1 \le \nu < \lambda$. En premier lieu, dans le cas particulier $\Delta(\lambda, \nu, 1)$, en ajoutant les 2ν premières colonnes à la dernière, on obtient

$$\Delta(\lambda, \nu, 1) = \sum_{j=\nu+1}^{\lambda} \binom{2j}{0} = \binom{\lambda - \nu}{1} = \binom{\lambda - \nu}{0} + \binom{\lambda - \nu + 1}{1}$$
$$= 1 + \binom{2^\mu + \lambda - \nu + 1}{1}$$

d'après la reproduction par blocs de la matrice binomiale, d'où le résultat.

Pour le cas général, dans un premier temps on transforme le déterminant du lemme 3 pour aboutir à une formule qu'on réduira dans un second temps.

La première étape est d'arriver à écrire $\Delta(\lambda,\nu,k)$ sous la forme

$$\begin{vmatrix} I_{2\nu+1}^{2\nu-k+1} \\ C^k_{2^{\mu+1}-2\nu+k,2^{\mu+1}} C^k_{2^{\mu+1}+1,2^{\mu+1}+k-1} K^k \end{vmatrix}$$

où $(C^k_{2^{\mu+1}+1,2^{\mu+1}+k-1}K^k)$ est une matrice triangulaire supérieure dont tous les termes diagonaux sont égaux à un sauf le dernier qui vaut $\Delta(\lambda,\nu,k)$. Pour cela, on effectue $2^{\mu+1}-2\nu+k-1$ décalages sur les k dernières lignes de $\Delta(\lambda,\nu,k)$; d'une part, un décalage, comme son nom l'indique, décale d'une colonne à droite la matrice de Pascal sans changer la valeur du déterminant; d'autre part, d'après le lemme 4, le dernier terme de la dernière colonne du déterminant vaut

$$\sum_{h=1}^{k-1}\binom{2^{\mu+1}-2\nu+k-1}{h}\left(1+\sum_{j=\nu+1}^{\lambda}\binom{2j}{k-h-1}\right)+\sum_{j=\nu+1}^{\lambda}\binom{2j}{k-1};$$

alors en ajoutant les $2\nu-k+1$ premières colonnes à la dernière, on obtient le déterminant sous la forme précédemment annoncée, mais le dernier terme se trouve augmenté de la quantité $\sum_{j=2^{\mu+1}-2\nu+k-1}^{2^{\mu+1}-1}\binom{j}{k-1}$. La première étape est achevée et donne la formule

$$\begin{aligned}\Delta(\lambda,\nu,k) = {}&\sum_{h=1}^{k-1}\binom{2^{\mu+1}-2\nu+k-1}{h}+\sum_{j=2^{\mu+1}-2\nu+k-1}^{2^{\mu+1}-1}\binom{j}{k-1}\\ &+\sum_{h=0}^{k-1}\binom{2^{\mu+1}-2\nu+k-1}{h}\sum_{j=\nu+1}^{\lambda}\binom{2j}{k-h-1}.\end{aligned}$$

Dans la suite, nous noterons $\delta(\nu,k)$ la première ligne de l'expression ci-dessus et $\gamma(\lambda,\nu,k)$ la deuxième ligne.

La deuxième étape consiste à réduire la formule aux deux formules énoncées dans le lemme. A cet effet, on utilise les formules démontrées au paragraphe 3.

1.1. *Calcul de* $\delta(\nu,k)$. Si $k=2p$,

$$\begin{aligned}&\sum_{h=1}^{k-1}\binom{2^{\mu+1}-2\nu+k-1}{h}\\ &\qquad=\sum_{h=0}^{p-1}\binom{2^{\mu}-\nu+p-1}{h}+\sum_{h=1}^{p-1}\binom{2^{\mu}-\nu+p-1}{h}=1,\end{aligned}$$

d'après P6 et P7, et

$$\begin{aligned}\sum_{j=2^{\mu+1}-2\nu+k-1}^{2^{\mu+1}-1}\binom{j}{k-1} &= \sum_{j=0}^{2\nu-k}\binom{2^{\mu+1}-2\nu+k-1+j}{k-1}\\ &= \sum_{j=0}^{\nu-p}\binom{2^{\mu}-\nu+p-1+j}{p-1}\\ &= \sum_{j=0}^{\nu-p}\binom{2^{\mu}-\nu+p+j}{p}+\sum_{j=0}^{\nu-p}\binom{2^{\mu}-\nu+p-1+j}{p}\\ &= \binom{2^{\mu}-\nu+p-1}{p},\end{aligned}$$

d'après P6, P3 et P9.

Si $k = 2p + 1$,

$$\begin{aligned}\sum_{h=1}^{k-1}\binom{2^{\mu+1}-2\nu+k-1}{h} &= \sum_{h=1}^{p}\binom{2^{\mu}-\nu+p}{h}\\ &= \sum_{h=1}^{p}\binom{2^{\mu}-\nu+p-1}{h}+\sum_{h=1}^{p}\binom{2^{\mu}-\nu+p-1}{h-1}\\ &= 1+\binom{2^{\mu}-\nu+p-1}{p}\end{aligned}$$

d'après P4, P5, P1 et, d'après P5, P7,

$$\sum_{j=2^{\mu+1}-2\nu+k-1}^{2^{\mu+1}-1}\binom{j}{k-1} = 0.$$

D'où,

$$\delta(\nu, 2p) = \delta(\nu, 2p+1) = 1 + \binom{2^{\mu}-\nu+p-1}{p}.$$

1.2. *Calcul de* $\gamma(\lambda, \nu, k)$. Si $k = 2p$,

$$\begin{aligned}\gamma(\lambda,\nu,2p) &= \sum_{h=0}^{2p-1}\binom{2^{\mu+1}-2\nu+2p-1}{h}\sum_{j=\nu+1}^{\lambda}\binom{2j}{2p-h-1}\\ &= \sum_{h=0}^{p-1}\binom{2^{\mu}-\nu+p-1}{h}\sum_{j=\nu+1}^{\lambda}\binom{j}{p-h-1}\end{aligned}$$

d'après P4, P6 et P5.

Si $k = 2p + 1$,

$$\gamma(\lambda, \nu, 2p+1) = \sum_{h=0}^{2p} \binom{2^{\mu+1} - 2\nu + 2p}{h} \sum_{j=\nu+1}^{\lambda} \binom{2j}{2p-h}$$
$$= \sum_{h=0}^{p} \binom{2^{\mu} - \nu + p}{h} \sum_{j=\nu+1}^{\lambda} \binom{j}{p-h}$$

d'après P4 et P5. D'où

$$\gamma(\lambda, \nu, 2p+1) = \gamma(\lambda, \nu, 2p+2).$$

L'entier τ étant défini par $2^{\tau-1} \leq \lambda < 2^{\tau}$, on obtient la décomposition

$$\sum_{j=\nu+1}^{\lambda} \binom{j}{p-h} = \sum_{j=\nu+1}^{2^{\mu}-1} \binom{j}{p-h} + \sum_{j=2^{\tau-1}}^{\lambda} \binom{j}{p-h} \qquad \text{pour } 1 \leq \mu \leq \tau;$$

en effet, pour $\mu \leq \tau - 1$, la somme intermédiaire de $j = 2^{\mu}$ à $2^{\tau-1} - 1$ est nulle d'après la propriété P12 ou n'existe pas; et pour $\mu = \tau$,

$$\sum_{j=\nu+1}^{2^{\tau}-1} \binom{j}{p-h} + \sum_{j=2^{\tau-1}}^{\lambda} \binom{j}{p-h}$$
$$= \sum_{j=\nu+1}^{2^{\tau}-1} \binom{j}{p-h} + \sum_{j=2^{\tau-1}}^{\nu} \binom{j}{p-h} + \sum_{j=\nu+1}^{\lambda} \binom{j}{p-h}$$
$$= \sum_{j=\nu+1}^{\lambda} \binom{j}{p-h}$$

puisque $\sum_{j=2^{\tau-1}}^{2^{\tau}-1} \binom{j}{p-h} = 0$.

Par ailleurs, en utilisant la propriété P11, on obtient

$$\sum_{j=\nu+1}^{2^{\mu}-1} \binom{j}{p-h} = \binom{\nu+1}{p-h+1}$$

et

$$\sum_{j=2^{\tau-1}}^{\lambda} \binom{j}{p-h} = \sum_{j=\lambda}^{2^{\tau}-1} \binom{j}{p-h} = \binom{\lambda+1}{p-h+1};$$

d'où

$$\gamma(\lambda, \nu, 2p+1)$$
$$= \sum_{h=0}^{p} \binom{2^{\mu} - \nu + p}{h} \binom{\nu+1}{p-h+1} + \sum_{h=0}^{p} \binom{2^{\mu} - \nu + p}{h} \binom{\lambda+1}{p-h+1}.$$

La convolution de Vandermonde (P13) donne ici successivement :

$$\sum_{h=0}^{p+1} \binom{2^\mu - \nu + p}{h} \binom{\nu + 1}{p - h + 1} = \binom{2^\mu + p + 1}{p + 1}$$

et

$$\sum_{h=0}^{p+1} \binom{2^\mu - \nu + p}{h} \binom{\lambda + 1}{p - h + 1} = \binom{2^\mu - \nu + p + \lambda + 1}{p + 1}.$$

En remarquant que $\binom{\lambda+1}{0} = \binom{\nu+1}{0} = 1$ et en appliquant la propriété P10, on obtient

$$\begin{aligned} \gamma(\lambda, \nu, 2p + 1) &= \binom{2^\mu + p + 1}{p + 1} + \binom{2^\mu - \nu + p + \lambda + 1}{p + 1} \\ &= 1 + \binom{2^\mu - \nu + p + \lambda + 1}{p + 1}. \end{aligned}$$

En ajoutant les formules obtenues pour δ et γ, on arrive au résultat annoncé pour Δ dans le cas où $1 \le \nu < \lambda$.

2. Si $\nu = \lambda$, la quantité $\gamma(\nu, \nu, k)$ n'existe pas, donc Δ se réduit à δ, donc

$$\Delta(\nu, \nu, 2p) = \Delta(\nu, \nu, 2p + 1) = 1 + \binom{2^\mu - \nu + p - 1}{p};$$

d'où le résultat puisque $\binom{2^\mu+p+1}{p+1} = \binom{p+1}{p+1} = 1$. ∎

Lemme 6 (Cas particulier $\lambda = 2^\tau - 1$). *En notant* $\Delta(\nu, k) = \Delta(2^\tau - 1, \nu, k)$, *on a les formules*

$$\Delta(\nu, 2p) = 0 \quad \textit{pour } 1 \le p \le \nu$$

et

$$\Delta(\nu, 2p + 1) = \binom{2^\tau - \nu + p - 1}{p + 1} \bmod 2 \quad \textit{pour } 0 \le p \le \nu - 1.$$

Preuve. La première formule résulte de la propriété P8 et la deuxième des propriétés P8 et P2. ∎

Remarque. C'est grâce à ce lemme exprimant $\Delta(\nu, k)$ avec un seul coefficient binomial qu'il est possible de comptabiliser les points de $S_{4\nu}^{l_{\lambda-\nu}}$ appartenant à D_ν, dans le cas où $\lambda = 2^\tau - 1$.

Lemme 7 (Nombre de zéros dans la matrice de Pascal). *Le nombre de zéros dans la matrice* $C_{2^\tau}^{2^\tau}$ *(modulo 2) est égal à* $4^\tau - 3^\tau$.

Preuve. Notons K_τ le nombre de zéros cherché; on procède par récurrence : K_0 vaut 0 et d'après la propriété P8 de reproduction par blocs de la matrice, on a la relation $K_\tau = 3K_{\tau-1} + (2^{\tau-1})^2$, d'où le résultat. ∎

F i n d e l a d é m o n s t r a t i o n. D'après les lemmes 1 et 2, l'écart cherché est donné par

$$E(N_\lambda) = \sum_{\nu=0}^{\lambda}\left(A(D_\nu; S_{4\nu}^{l_{\lambda-\nu}}) - \frac{2}{3}\left(\nu + \frac{2}{3}\right)\right).$$

La remarque suivant le lemme 2 donne $A(D_0; S_0^{l_\lambda}) = 1$ et d'après la remarque suivant le lemme 3, on obtient

$$\sum_{\nu=1}^{\lambda} A(\pi_{2\nu+1} \cap Q; S_{4\nu}^{l_{\lambda-\nu}}) = \lambda.$$

D'où en appliquant le lemme 3, on déduit

$$\sum_{\nu=0}^{\lambda} A(D_\nu; S_{4\nu}^{l_{\lambda-\nu}}) \\ = \lambda + 1 + \operatorname{card}\{(\nu, k) : 1 \le \nu \le \lambda,\ 1 \le k \le 2\nu,\ \Delta(\lambda, \nu, k) = 0\}.$$

La forme obtenue pour les Δ au lemme 5 ne nous a pas permis de mener à terme le calcul pour λ quelconque, d'où le choix particulier fait pour λ au lemme 6; dans ces conditions la formule ci-dessus s'écrit

$$\sum_{\nu=0}^{\lambda} A(D_\nu; S_{4\nu}^{l_{\lambda-\nu}}) = 2^\tau + \operatorname{card}\{(\nu, p) : 1 \le \nu \le 2^\tau - 1,\ 1 \le p \le \nu\} \\ + \operatorname{card}\left\{(\nu, p) : 1 \le \nu \le 2^\tau - 1,\ 0 \le p \le \nu - 1, \binom{2^\tau - \nu + p - 1}{p+1} = 0\right\}.$$

Le premier cardinal s'interprète comme le cardinal de l'ensemble

$$\left\{(q, r) : 1 \le q \le 2^\tau - 1,\ 0 \le r \le q - 1,\ \binom{r}{q} = 0\right\}$$

d'après la définition de la matrice binomiale et le deuxième cardinal se décompose en la somme des cardinaux des deux ensembles suivants :

$$\left\{(\nu, p) : \nu = 2^\tau - 1, 0 \le p \le \nu - 1, \binom{p}{p+1} = 0\right\}$$

et

$$\left\{(q, r) : 1 \le q \le 2^\tau - 2, q \le r \le 2^\tau - 2,\ \binom{r}{q} = 0\right\}.$$

Sachant que $\binom{r}{0} = 1$ pour tout r et que $\binom{2^\tau-1}{q} = 1$ pour $q \le 2^\tau - 1$, on aboutit à la formule

$$\sum_{\nu=0}^{\lambda} A(D_\nu; S_{4\nu}^{l_{\lambda-\nu}})$$
$$= 2^{\tau+1} - 1 + \operatorname{card}\left\{(r,q) : 0 \le q \le 2^\tau - 1,\ 0 \le r \le 2^\tau - 1,\ \binom{r}{q} = 0\right\}.$$

Enfin, en appliquant le lemme 7, on obtient

$$E(N_{2^\tau-1}) = 4^\tau - 3^\tau + 2^{\tau+1} - 1 - \frac{2}{3}\sum_{\nu=0}^{2^\tau-1}\left(\nu + \frac{2}{3}\right),$$

d'où, en calculant cette dernière somme le résultat annoncé. ∎

Références

[1] J. Beck, *A two dimensional van Aardenne–Ehrenfest theorem in irregularities of distribution*, Compositio Math. 72 (1989), 269–339.

[2] H. Faure, *Discrépance de suites associées à un système de numération* (*en dimension s*), Acta Arith. 41 (1982), 337–351.

[3] H. Faure et H. Chaix, *Minoration de discrépance en dimension* 2, C. R. Acad. Sci. Paris Sér. I 319 (1994), 1–4.

[4] G. Halász, *On Roth's method in the theory of irregularities of point distribution*, in: Recent Progress in Analytic Number Theory, Vol. 2, Academic Press, 1981, 79–94.

[5] J. H. Halton, *On the efficiency of certain quasi-random points in evaluating multi-dimensional integrals*, Numer. Math. 2 (1960), 84–90.

[6] H. Niederreiter, *Point sets and sequences with small discrepancy*, Monatsh. Math. 104 (1987), 273–337.

[7] —, *Low discrepancy and low dispersion sequences*, J. Number Theory 30 (1988), 51–70.

[8] K. F. Roth, *On irregularities of distribution*, Mathematika 1 (1954), 73–79.

[9] W. M. Schmidt, *Irregularities of distribution, VII*, Acta Arith. 21 (1972), 45–50.

[10] I. M. Sobol', *On the distribution of points in a cube and the approximate evaluation of integrals*, U.S.S.R. Comput. Math. and Math. Phys. 7 (1967), 86–112.

[11] S. Srinivasan, *On two dimensional Hammersley sequences*, J. Number Theory 10 (1978), 421–429.

Laboratoire de Mathématiques Discrètes
U.P.R. 9016 du CNRS
163 avenue de Luminy
case 930
F-13288 Marseille Cedex 09, France

Centre de Mathématiques
et d'Informatique
Université de Provence
39 rue F. Joliot-Curie
F-13453 Marseille Cedex 13, France

Reçu le 21.4.1995 (2784)