Available online at www.sciencedirect.com

ScienceDirect

Journal of Number Theory 128 (2008) 2282–2317

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Sur la répartition des entiers premiers à un entier sans petit facteur premier

On the distribution of integers coprime to an integer free of small prime factors

Arnaud Chadozeau *

Université Bordeaux I, IMB, UMR 5251, 351 cours de la Libération, F-33 405 Talence cedex, France

Reçu le 2 juillet 2007

Disponible sur Internet le 18 avril 2008

Communiqué par R.C. Vaughan

Résumé

Soit $M_k(q;h)$ le moment d'ordre k du nombre d'entiers premiers à q dans un intervalle de longueur h centré sur sa moyenne $h\frac{\varphi(q)}{q}$. Par comparaison au moment centré d'ordre k de la loi binomiale de paramètre h et P, pour lequel nous montrons

$$\mu_k(h,P) \ll (ck)^{k/2}\big(k+hP(1-P)\big)^{k/2},$$

uniformément en k, h et P pour une certaine constante absolue $c>0$, nous donnons la majoration

$$M_k(q;h) \ll (c'k)^{k/2} q\left(k+h\frac{\varphi(q)}{q}\right)^{k/2},$$

uniforme en k, h et q pour une certaine constante absolue $c'>0$, sous la condition que tous les facteurs premiers de q soient plus grands que h.

* Fax : +33 0 5 4000 21 23.

Adresse e-mail : arnaud.chadozeau@math.u-bordeaux1.fr.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.12.008

Abstract

Let $M_k(q;h)$ be the kth moment of the number of integers coprime to q in an interval of length h centered on its mean $h\frac{\varphi(q)}{q}$. By comparison with the kth centered moment of the binomial distribution with parameters h and P, for which we show

$$\mu_k(h,P) \ll (ck)^{k/2}\big(k+hP(1-P)\big)^{k/2},$$

uniformly in k, h and P and where $c>0$ is an absolute constant, we prove the following upper bound

$$M_k(q;h) \ll (c'k)^{k/2} q\left(k+h\frac{\varphi(q)}{q}\right)^{k/2},$$

where $c'>0$ is an absolute constant, uniformly in k, h and q provided that every prime factor of q is greater than or equal to h.

Mots-clés : Nombres premiers entre eux ; Répartition dans les intervalles ; Moments centrés ; Loi binomiale ; Corrélation d'ordre supérieur

Keywords: Coprime integers; Distribution in intervals; Centered moments; Binomial distribution; Higher level correlation

Table des matières

Notations. Dans ce travail, la notation $[\![a,b]\!]$ désigne $\mathbb{Z}\cap[a,b]$ et on parle d'intervalle entier de longueur $b-a+1$. Les notations $P^-(q)$ et $P^+(q)$ pour le plus petit et le plus grand diviseur premier d'un entier $q>1$ sont aussi employées, avec la convention $P^-(1)=\infty$ et $P^+(1)=1$. Les nombres de Stirling de seconde espèce, à savoir le nombre de façons de partitionner l'ensemble $[\![1,a]\!]$ en b parties non-vides, seront notés $\left\{{a \atop b}\right\}$. (On trouvera dans [2] et [8] les propriétés

des nombres de Stirling utilisées dans cet article.) Nous utiliserons aussi la fonction δ, nulle en tous les entiers sauf en 0, où elle vaut 1. Enfin, nous définissons le symbole $[n \perp q]$, qui vaut 1 si n et q sont premiers entre eux, et 0 sinon.

1. Introduction

Soit $q > 1$ un entier naturel, et posons $1 = a_1 < a_2 < \cdots < a_i < \cdots$ la suite croissante exhaustive des entiers positifs premiers à q. Dès 1940, Erdős [5,7] proposa d'étudier la répartition de cette suite au travers de la question suivante : est-il vrai que pour tout réel positif γ fixé, on a la relation

$$\sum_{i=1}^{\varphi(q)} (a_{i+1} - a_i)^\gamma \ll_\gamma \varphi(q) \left(\frac{q}{\varphi(q)} \right)^\gamma \ ? \tag{1}$$

Pour $0 \leqslant \gamma \leqslant 1$, cela provient d'un simple argument de convexité. Pour traiter le cas $\gamma > 1$, il est généralement nécessaire d'établir une majoration du moment centré d'ordre $k \in \mathbb{N}$ du nombre d'entiers premiers à q contenus dans une fenêtre coulissante de longueur h

$$M_k(q;h) := \sum_{n=1}^{q} \left(\sum_{i=1}^{h} [n+i \perp q] - h\frac{\varphi(q)}{q} \right)^k. \tag{2}$$

Par exemple, Hooley [12] donne une réponse affirmative à la question (1) pour $\gamma < 2$ grâce à la majoration $M_2(q;h) \leqslant (1+o(1))h\varphi(q)$ (voir [11]). Dans leur article de 1986, Montgomery et Vaughan [18] généralisent ce résultat en prouvant

$$M_k(q;h) \ll_k q \left(h\frac{\varphi(q)}{q} \right)^{k/2} \tag{3}$$

pour k fixé et $h\varphi(q)/q \geqslant 1$, relation précisée en

$$M_{2k}(q;h) \sim \frac{(2k)!}{2^k k!} q \left(h\frac{\varphi(q)}{q} \right)^{k/2} \tag{4}$$

pour k fixé et pour $h(\varphi(q)/q)^{7k2^k} \to +\infty$ par Montgomery et Soundararajan [17]. La majoration (3) permet d'établir l'estimation (1) pour tout $\gamma \geqslant 0$ fixé.

L'objectif de cet article est de préciser la relation (3) en essayant de la rendre uniforme en k. Nous obtenons une majoration satisfaisante sous la condition que q ne possède pas de petit facteur premier.

Théorème A. *Pour une constante absolue $c > 0$, on a*

$$M_k(q;h) \ll q(ck)^{k/2} \left(k + h\frac{\varphi(q)}{q} \right)^{k/2}$$

uniformément en $k \geqslant 0$, $h \geqslant 0$ et q vérifiant $P^-(q) \geqslant h$.

1.1. Historique et motivations

À la suite de la question (1) dans [7], Erdős, repris pas Montgomery [16, p. 201], soumet la question de l'existence d'un réel $x > 0$ tel qu'uniformément en $q > 1$

$$\sum_{i=1}^{\varphi(q)} \exp\left(\frac{q}{\varphi(q)}(a_{i+1} - a_i)x\right) \ll \varphi(q). \tag{5}$$

Le terme de gauche est la série génératrice exponentielle des sommes majorées en (1) ; la majoration (5) est donc équivalente à la majoration suivante, uniforme en $q > 1$ et en $\gamma \geqslant 0$

$$\sum_{i=1}^{\varphi(q)} (a_{i+1} - a_i)^{\gamma} \ll (c\gamma)^{\gamma} \varphi(q) \left(\frac{q}{\varphi(q)}\right)^{\gamma}$$

où c est une constante absolue. Il s'agit d'une version uniforme de (1) qui se déduirait d'une majoration uniforme en k de $M_k(q; h)$.

Dans ce contexte, le théorème A permet de donner du crédit à une hypothétique majoration uniforme en k, h et q de la forme

$$M_k(q; h) \ll q(ck)^{k/2} \left(k + h\frac{\varphi(q)}{q}\right)^{k/2} \tag{6}$$

pour une constante absolue $c > 0$. À la valeur de la constante c près, la majoration précédente est, à k fixé, en accord avec l'estimation asymptotique (4) de Montgomery et Soundararajan.

L'estimation conjecturale (6) permettrait de répondre par l'affirmative à la question (5) d'Erdős. Elle impliquerait ainsi une majoration nouvelle de la fonction de Jacobsthal $g(q)$ définie par Jacobsthal [14] comme la différence maximale entre deux entiers consécutifs parmi les entiers relativement premiers à q, c'est-à-dire par $g(q) := \max(a_{i+1} - a_i)$.

Cette fonction fut en particulier étudiée par Erdős [6] qui montra que la quantité

$$\big(1 + o(1)\big)\omega(q)\frac{q}{\varphi(q)}$$

était à la fois un ordre normal et un minorant de $g(q)$. La meilleure majoration de $g(q)$ aujourd'hui connue est dûe à Iwaniec [13] qui utilise les minorations du crible linéaire pour montrer

$$g(q) \ll \frac{q}{\varphi(q)}\omega(q)^2 \log 2\omega(q).$$

Comme l'analyse Vaughan [21], la présence du carré de $\omega(q)$ est consubstancielle à la méthode employée ($1/2$ est la limite du crible linéaire) et toute amélioration de cette puissance aurait de fortes conséquences arithmétiques (voir les travaux de Kanold [15]).

L'estimation conjecturale (6) permettrait de montrer

$$g(q) \ll \frac{q}{\varphi(q)} \log q, \tag{7}$$

qui est la plus forte majoration conjecturale de $g(q)$ généralement admise. Les travaux de Rankin [19] montrent que pour q_r, produit des r plus petits nombres premiers, on a

$$g(q_r) \gg r(\log r)^2 \frac{\log_3 r}{(\log_2 r)^2} \gg \left(\frac{q_r}{\varphi(q_r)}\right)^{1-o(1)} \log q_r. \tag{8}$$

Parmi les conséquences arithmétiques de la majoration (7), on peut citer la majoration des différences entre entiers premiers consécutifs $p_{n+1} - p_n \ll \sqrt{p_n} \log p_n$, démontrée par Cramér [3,4] sous hypothèse de Riemann, ou bien la majoration par $d^{2+\varepsilon}$ du plus petit entier premier dans une progression arithmétique de raison d, établie sous hypothèse de Riemann généralisée par Chowla [1]. (Plus précisément, on pourrait montrer que cet entier premier est $\ll d^2(\log d)^2$.)

La majoration uniforme (6) des moments $M_k(q;h)$ permettrait donc de se passer de l'hypothèse de Riemann dans deux problèmes classiques de répartition des nombres premiers, problèmes pour lesquels les conjecture sont bien au delà des résultats fournis par l'hypothèse de Riemann. Cela peut conduire à des réserves quand à la véracité de la majoration (6). Dans cette direction, Granville et Soundararajan [9] ont montré qu'on ne peut pas attendre de trop bonnes majorations uniformes de $M_k(q;h)$.

Il est également à remarquer que le cas le plus intéressant du point de vue arithmétique est précisément le cas où q est le produit des plus petits nombres premiers, la suite des a_i se comportant plus comme la suite des nombres premiers. À l'inverse, lorsque l'entier q ne comporte que des grands facteurs premiers, la répartition des a_i est presque aléatoire et ne présente pas de phénomènes arithmétiques. Le sens du corollaire B suivant est que l'étude des cas « arithmétiques » (lorsque $P^+(q) < h$) peut se faire indépendamment des cas « probabilistes » (lorsque $P^-(q) \geqslant h$) traités dans cet article. En effet, par un processus de séparation des moments $M_k(q;h)$ légèrement adapté par rapport à celui présenté dans [18], l'étude de la majoration (5) peut se réduire au cas des entiers q sans grand facteur premier.

Corollaire B. *Pour une constante absolue $c > 0$, on a*

$$M_k(q;h) \ll q_\flat \left(2\frac{\varphi(q_\flat)}{q_\flat}\right)^k M_k(q_\sharp;h) + q(ck)^{k/2}\left(k + h\frac{\varphi(q)}{q}\right)^{k/2}$$

uniformément en $k \geqslant 0$ entier pair, $h \geqslant 0$ et $q \geqslant 1$, où les entiers $q_\sharp$ et $q_\flat$ sont définis par les relations $q = q_\sharp q_\flat$ et $P^+(q_\sharp) < h \leqslant P^-(q_\flat)$.

1.2. Interprétation probabiliste

Le moment $M_k(q;h)$ mesure la variation du nombre d'entiers premiers à q dans un intervalle de longueur h par rapport au nombre moyen ; en ce sens, on peut voir $1/q\, M_k(q;h)$ comme l'espérance de cette variation élevée à la puissance k calculée à partir des q observations dont nous disposons, à savoir le contenu

$$\mathcal{S}_n := \big\{i \in [\![1,h]\!];\ (n+i,q) = 1\big\},$$

des q intervalles de longueur h, distincts modulo q.

On modélise le contenu d'un intervalle de longueur h grâce à h variables aléatoires de Bernoulli $Y_1, \dots, Y_h$ d'espérance commune $P = \varphi(q)/q$. Les $\mathcal{S}_n$ constituent donc q observations de l'ensemble aléatoire

$$\mathcal{S} := \big\{ i \in [\![1, h]\!];\ Y_i = 1 \big\}.$$

Dans ce modèle, sous l'hypothèse que les variables Y_i sont deux à deux indépendantes, l'équivalent probabiliste du moment moyenné $1/q\, M_k(q; h)$ est le moment centré d'ordre k de la loi binomiale de paramètres (h, P)

$$\mu_k(h, P) := \mathbb{E}\big(|\mathcal{S}| - hP\big)^k = \mathbb{E}\left(\sum_{i=1}^{h} Y_i - hP \right)^k.$$

Nous réalisons dans cet article une étude de ces moments en recherchant l'uniformité en chacune des trois variables k, h et P. On obtient le résultat suivant qui justifie heuristiquement la forme de la majoration du théorème A.

Théorème C. *Pour une constante absolue $c > 0$, on a*

$$\mu_k(h, P) \ll (ck)^{k/2} \big(k + hP(1 - P) \big)^{k/2}$$

uniformément en $k \geqslant 0$, $h \geqslant 0$ et $P \in [0, 1]$.

Nous complétons cette étude au chapitre 3 en montrant que cette majoration est optimale en un certain sens, et notamment que l'on ne peut pas se passer de ce changement de comportement autour du point où la variance $\mu_2(h, P) = hP(1 - P)$ est du même ordre de grandeur que k.

Le théorème A est donc en accord avec l'heuristique suivante : lorsque q ne possède pas de facteur premier plus petit que l, les événements « n est premier à q » et « $n + l$ est premier à q » sont indépendants. Cela peut se vérifier en calculant la corrélation de ces événements

$$\begin{aligned} &\frac{1}{q} \sum_{n=1}^{q} \big([n \perp q] - P \big) \big([n + l \perp q] - P \big) \\ &\quad = \frac{1}{q} \sum_{n=1}^{q} [n \perp q][n + l \perp q] - P^2 \\ &\quad = P^2 \left(\prod_{\substack{p \mid q \\ p \mid l}} \left(1 + \frac{1}{p - 1} \right) \prod_{\substack{p \mid q \\ p \nmid l}} \left(1 - \frac{1}{(p-1)^2} \right) - 1 \right). \end{aligned} \tag{9}$$

Lorsque $l < P^-(q)$, cette corrélation est très faible et ne dépend pas de l :

$$\frac{1}{q} \sum_{n=1}^{q} \big([n \perp q] - P \big) \big([n + l \perp q] - P \big) \ll \frac{P^2}{P^-(q) \log P^-(q)}. \tag{10}$$

La modélisation de ces événements par deux variables aléatoires indépendantes est donc justifiée. Pour que les hypothèses d'indépendance sur les Y_i soient justifiées, ce calcul doit être valable pour tout $l \leqslant h-1$; la condition $h \leqslant P^-(q)$ du théorème A est donc justifiée et se présente comme la limite naturelle de ce raisonnement. En outre, si q possède un facteur premier $p < h$, les événements « n est premier à q » et « $n+p$ est premier à q » ne sont manifestement plus indépendants ; et la valeur (9) de la corrélation est de l'ordre de $1/p$, alors que l'on obtient $o(1/h)$ dans le cas $h \leqslant P^-(q)$.

Cet argument des corrélations faibles jouent un rôle clef dans la démonstration du théorème A puisqu'il s'agit de valider les hypothèses d'indépendance des variables Y_i ; on définit pour cela les corrélations d'ordre supérieur. Pour $I \subset [\![1,h]\!]$ de cardinal t, on définit de la corrélation d'ordre t par

$$\frac{1}{q}\sum_{n=1}^{q}\prod_{i\in I}\big([n+i\perp q]-P\big).$$

Dans le cas d'événements indépendants, cette valeur est nulle. Nous montrons que dans le cas de la suite des a_i, ces corrélations sont très petites.

Proposition D. *Pour une constante absolue $c>0$, on a*

$$\frac{1}{q}\sum_{n=1}^{q}\prod_{i\in I}\big([n+i\perp q]-P\big) \ll P^t\left(c\frac{t}{P^-(q)\log P^-(q)}\right)^{t/2}$$

uniformément pour $t,h\geqslant 1$, pour $I\subset[\![1,h]\!]$ de cardinal t et pour q vérifiant $P^-(q)\geqslant h$.

Cette estimation permet d'exploiter les estimations menant au théorème probabiliste C et d'obtenir au chapitre 5 la majoration du théorème A.

1.3. Estimations combinatoires

La majoration de la proposition D, essentielle pour obtenir le théorème A, est une spécialisation du théorème général suivant, objet du chapitre 4.

Théorème E. *Soient $\varepsilon\in\,]0,1/2[$ et $K,K'>0$ trois réels. Uniformément pour tout vecteur complexe $\mathbf{x}=(x_1,\dots,x_m)\in\mathbb{C}^m$ vérifiant $|1-x_i|\geqslant\varepsilon$ pour tout i et pour tout entier naturel t vérifiant $t\|\mathbf{x}\|_\infty\leqslant K$ et $t\|\mathbf{x}\|_2^2\leqslant K'$, on a*

$$\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}\frac{1-sx_i}{(1-x_i)^s} \ll_{K,K',\varepsilon}\left(ct\|\mathbf{x}\|_2^2\right)^{t/2}$$

pour une constante c dépendant au plus de K, de K' et de ε.

Ce résultat est rendu possible par l'étude de certains coefficients

$$\omega(\mathbf{r},t):=\frac{\prod_{j=1}^{k}r_j!}{t!}\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{j=1}^{k}\binom{s}{r_j}, \tag{11}$$

où $\mathbf{r} = (r_1, \ldots, r_k)$ est un k-uplet d'entiers, coefficients qui interviennent dans l'étude des quantités

$$\sum_{s=0}^{t} (-1)^{t-s} \binom{t}{s} \prod_{i=1}^{m} \frac{1 - s x_i}{(1 - x_i)^s}. \tag{12}$$

Pour cela, nous interprétons $\omega(\mathbf{r}, t)$ comme la solution d'un problème d'énumération de partitions d'ensemble. Nous en déduisons l'encadrement $0 \leqslant \omega(\mathbf{r}; t) \leqslant \left\{ {r_1 + \cdots + r_k \atop t} \right\}$, et donc la nullité des coefficients $\omega(\mathbf{r}; t)$ lorsque $\sum_1^k r_j < t$.

La partie 2 de cet article est consacrée à l'étude d'une suite de polynômes, qui sont utilisées dans les parties 3 et 5. Le théorème C ainsi que son optimalité, est le sujet de la troisième partie. La partie 4 est entièrement indépendante et mène au théorème E. Enfin, en utilisant les résultats des parties 2 et 4, et en s'inspirant du travail effectué dans la partie 3, nous prouvons dans la partie 5 le théorème principal A ainsi que son corollaire B.

2. Étude d'une suite récurrente de polynômes

Nous consacrons cette section à l'étude d'une suite de polynômes qui interviennent dans l'expression polynomiale en les variables h et P de $\mu_k(h, P)$, le moment centré d'ordre k de la loi binomiale de paramètre (h, P). L'estimation de ces polynômes est rendue simple par la relation de récurrence (13) qu'ils vérifient, et sera un ingrédient important dans la majoration des moments $\mu_k(h, P)$ et $M_k(q; h)$.

On définit les polynômes $R_{k,j} \in \mathbb{Z}[X]$ par les valeurs initiales

$$R_{0,j} = \delta(j), \quad R_{1,j} = 0 \quad \text{et} \quad R_{k,0} = \delta(k), \quad \text{pour tous les } j \text{ et } k \in \mathbb{N}$$

et par la formule de récurrence valable pour $j \geqslant 1$ et $k \geqslant 1$

$$R_{k+1,j}(X) = k R_{k-1,j-1}(X) + j(1 - 2X) R_{k,j}(X) + X(1 - X) R'_{k,j}(X). \tag{13}$$

Remarque 1. On utilisera par la suite la notation classique de la double factorielle, définie sur les entiers naturels positifs par la relation de récurrence $(2n + 2)!! = (2n + 1) \cdot (2n)!!$ et par les valeurs initiales $0!! = 1$ et $1!! = 0$. La double factorielle possède une interprétation probabiliste puisqu'il s'agit des moments de la loi normale centrée réduite

$$n!! := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} t^n e^{-t^2/2} \, \mathrm{d}t = \begin{cases} \frac{n!}{2^{n/2}(n/2)!} & \text{si } n \text{ est pair ;} \\ 0 & \text{si } n \text{ est impair.} \end{cases}$$

Il sera donc naturel de retrouver ce facteur dans l'estimation de moments centrés. Il nous sera utile de disposer d'une interpolation régulière des valeurs non nulles de ces moments, on définit donc

$$\mathbb{\Gamma}(n + 1) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} |t|^n e^{-t^2/2} \, \mathrm{d}t = \Gamma\left(\frac{n+1}{2}\right) \frac{2^{n/2}}{\sqrt{\pi}} = \frac{\Gamma(n+1)}{2^{n/2}\Gamma(n/2+1)}.$$

Tableau 1
Valeurs des premiers polynômes $R_{k,j}$

$k \setminus j$	0	1	2	3
0	1	0	0	0
1	0	0	0	0
2	0	1	0	0
3	0	$1-2X$	0	0
4	0	$1-6X(1-X)$	3	0
5	0	$(1-2X)(1-12X(1-X))$	$10(1-2X)$	0
6	0	$1-30X(1-X)+120X^2(1-X)^2$	$25-130X(1-X)$	15

Cette fonction $\mathbb{\Gamma}$ est donc définie pour tout réel sauf aux entiers impairs négatifs et vérifie $\mathbb{\Gamma}(n+1)=n!!$ pour tout entier pair positif. Par la formule de Stirling, on a $\mathbb{\Gamma}(t+1)\sim\sqrt{2}\,(t/e)^{t/2}$ pour t réel tendant vers $+\infty$.

Un simple raisonnement par récurrence grâce à la formule (13) définissant les $R_{k,j}$ permet de prouver les propriétés simples qui apparaissent sur les premières valeurs, que nous réunissons dans une table pour le confort du lecteur.

Lemme 2. *Soient j et k deux entiers naturels.*

(a) $R_{k,j}(1-X)=(-1)^k R_{k,j}(X)$.
(b) *Si k est pair, on a $R_{k,j}\in\mathbb{Z}[X(1-X)]$, et si k est impair, on a $R_{k,j}\in(1-2X)\cdot\mathbb{Z}[X(1-X)]$.*
(c) *Si $1\leqslant j\leqslant k/2$, on a* $\deg R_{k,j}=k-2j$.
(d) *Si $j>k/2$, on a $R_{k,j}(X)=0$.*

2.1. Majoration en norme

Nous allons estimer la norme $\|\cdot\|_1$ de ces polynômes. On rappelle que cette norme est définie par $\|\sum_i c_i X^i\|_1=\sum_i|c_i|$, que c'est une norme d'algèbre de $\mathbb{R}[X]$ (i.e. on a $\|P\cdot Q\|_1\leqslant\|P\|_1\cdot\|Q\|_1$) et qu'elle vérifie l'inégalité $\|P'\|_1\leqslant\deg P\|P\|_1$.

Lemme 3. *Pour tous les entiers $j\geqslant 1$ et $k\geqslant 1$, on a*

$$\|R_{k+1,j}\|_1\leqslant k\|R_{k-1,j-1}\|_1+(2k-j)\|R_{k,j}\|_1.$$

Démonstration. On utilise la relation de récurrence (13) pour majorer $\|R_{k,j}\|_1$:

$$\begin{aligned}\|R_{k+1,j}\|_1&=\big\|kR_{k-1,j-1}(X)+j(1-2X)R_{k,j}(X)+X(1-X)R'_{k,j}(X)\big\|_1\\&\leqslant k\|R_{k-1,j-1}\|_1+j\|1-2X\|_1\|R_{k,j}\|_1+\big\|X-X^2\big\|_1\big\|R'_{k,j}\big\|_1\\&\leqslant k\|R_{k-1,j-1}\|_1+\big(3j+2(k-2j)\big)\|R_{k,j}\|_1\\&\leqslant k\|R_{k-1,j-1}\|_1+(2k-j)\|R_{k,j}\|_1.\qquad\square\end{aligned}$$

Pour tous les entiers naturels j et k, on pose

$$T_{k,j}:=\mathbb{\Gamma}(2k-2j+1)\binom{k-j-1}{j-1}.\tag{14}$$

Tableau 2
Premières valeurs de $\|R_{k,j}\|_1$ et de $T_{k,j}$

$k \diagdown j$	0	1	2	3
0	1	0	0	0
1	0	0	0	0
2	0	1	0	0
3	0	3	0	0
4	0	13	3	0
5	0	75	30	0
6	0	541	285	15

$k \diagdown j$	0	1	2	3
0	1	0	0	0
1	0	0	0	0
2	0	1	0	0
3	0	3	0	0
4	0	15	3	0
5	0	105	30	0
6	0	945	315	15

En particulier, on a $T_{k,j} = (2k-2j)!!\binom{k-j-1}{j-1}$ si $k \geqslant j$ et $T_{k,j} = 0$ sinon. On rappelle

$$\binom{n}{k} = \begin{cases} \frac{n!}{k!(n-k)!} & \text{si } 0 \leqslant k \leqslant n, \\ (-1)^{n-k}\frac{(-k-1)!}{(-n-1)!(n-k)!} & \text{si } k \leqslant n < 0, \\ 0 & \text{sinon,} \end{cases}$$

si bien que les relations $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ et $\binom{n}{k} = (-1)^{n-k}\binom{-k-1}{-n-1}$ sont vérifiées pour tous les n et k dans $\mathbb{Z}$. On sait que $\binom{n}{k} \leqslant 2^n$ si $n \in \mathbb{N}$ et, en utilisant les approximations de Stirling, que $(2n)!! \leqslant \sqrt{2}(2n/e)^n$ pour tout $n \in \mathbb{N}$; on a donc

$$T_{k,j} \leqslant \frac{1}{\sqrt{2}}\left(\frac{4(k-j)}{e}\right)^{k-j}, \quad \text{pour } k \geqslant j \geqslant 1. \tag{15}$$

Lemme 4. *On a $T_{k,0} = \delta(k)$ pour $k \in \mathbb{N}$ et $T_{k,j} = 0$ si $j > k/2$. Pour $k \geqslant 1$ et $j \geqslant 1$, on a*

$$T_{k+1,j} = kT_{k-1,j-1} + (2k-j)T_{k,j}.$$

Démonstration. Pour $j = 0$, on a bien $T_{k,0} = (2k)!!\binom{k-1}{-1} = (2k)!!\delta(k) = \delta(k)$.

Pour $j > k/2$, on a $k - j - 1 < j - 1$, donc $\binom{k-j-1}{j-1}$ est nul, et $T_{k,j}$ aussi.

Soient $k \geqslant 1$ et $j \geqslant 1$. Si $k < j$, les trois termes de la relation sont nuls. Si $k \geqslant j$, on pose $m = k - j \geqslant 0$. On a

$$\binom{m-1}{j-1} = \frac{1}{(2m)!!}T_{j+m,j}.$$

La relation d'absorption $(j-1)\binom{m-1}{j-1} = (m-j+1)\binom{m-1}{j-2}$ se traduit par

$$(j-1)T_{k,j} = (k-2j+1)T_{k-1,j-1}, \tag{16}$$

et la relation de récurrence $\binom{m}{j-1} = \binom{m-1}{j-2} + \binom{m-1}{j-1}$ par

$$\frac{1}{(2m+2)!!}T_{j+m+1,j} = \frac{1}{(2m)!!}T_{j+m-1,j-1} + \frac{1}{(2m)!!}T_{j+m,j}.$$

En utilisant dans cette dernière identité la relation $(n+2)!! = (n+1)\cdot n!!$ et en revenant sur le changement de variable, on obtient

$$\begin{aligned} T_{k+1,j} &= (2k-2j+1)(T_{k-1,j-1}+T_{k,j}) \\ &= kT_{k-1,j-1}+(2k-j)T_{k,j}+\big((k-2j+1)T_{k-1,j-1}-(j-1)T_{k,j}\big), \end{aligned}$$

où le terme entre parenthèses est effectivement nul par la relation (16). □

Proposition 5. *Pour tous les entiers naturels j et k, on a*

$$\|R_{k,j}\|_1 \leqslant T_{k,j},$$

où $T_{k,j}$ est la valeur définie en (14).

Démonstration. Par récurrence, on déduit des lemmes 3 et 4 la majoration $\|R_{k,j}\|_1 \leqslant T_{k,j}$ valable pour tous les entiers naturels j et k. □

2.2. Minoration des termes constants

La relation de récurrence (13) se simplifie pour les termes constants en

$$R_{k+1,j}(0) = kR_{k-1,j-1}(0) + jR_{k,j}(0).$$

On en rappelle les premières valeurs : $R_{0,j}(0) = \delta(j)$, $R_{1,j}(0) = 0$ et $R_{k,0}(0) = \delta(k)$ pour tous les entiers naturels j et k. On peut en tirer les premières conséquences.

Lemme 6. *Soient j et k deux entiers naturels.*

(a) *On a $R_{k,j}(0) \geqslant 0$.*
(b) *Si $j > k/2$, on a $R_{k,j}(0) = 0$.*
(c) *On a $R_{2k,k}(X) = R_{2k,k}(0) = (2k)!!$.*
(d) *Si $k \geqslant 2$, on a $R_{k,1}(0) = 1$.*

Pour simplifier la forme des calculs, on pose pour l et j entiers naturels

$$r_{l,j} := \frac{1}{\mathbb{\Gamma}(2j+l+1)} R_{2j+l,j}(0). \tag{17}$$

Le facteur $1/\sqrt{2\pi}$ de la table 3 provient du fait que $\mathbb{\Gamma}(2) = \sqrt{2/\pi}$. Cette normalisation nécessite de modifier la relation de récurrence.

Tableau 3
Premières valeurs de $R_{k,j}(0)$ et de leur normalisation $r_{l,j}$

$k \diagdown j$	0	1	2	3
0	1	0	0	0
1	0	0	0	0
2	0	1	0	0
3	0	1	0	0
4	0	1	3	0
5	0	1	10	0
6	0	1	25	15

$l \diagdown j$	0	1	2	3
0	1	1	1	1
1	0	$1/\sqrt{2\pi}$	$5/2\sqrt{2\pi}$	…
2	0	1/3	5/3	…
3	0	$1/4\sqrt{2\pi}$	…	…
4	0	1/15	…	…
5	0	…	…	…
6	0	…	…	…

Lemme 7. *Soient l et j deux entiers naturels. On a $r_{0,j} = 1$ et $r_{l,0} = \delta(l)$. Si $l \geqslant 1$ et $j \geqslant 1$, on a*

$$r_{l,j} = r_{l,j-1} + j\frac{\mathbb{\Gamma}(2j+l)}{\mathbb{\Gamma}(2j+l+1)} r_{l-1,j}.$$

Démonstration. Par le lemme 6, on a $r_{0,j} = \frac{1}{(2j)!!} R_{2j,j}(0) = 1$ et par définition des valeurs initiales des polynômes $R_{k,j}$, on a $r_{l,0} = \frac{1}{\mathbb{\Gamma}(l+1)} R_{l,0}(0) = \frac{1}{\mathbb{\Gamma}(l+1)}\delta(l) = \delta(l)$. En outre, pour l, $j \geqslant 1$ on a

$$\begin{aligned}
r_{l,j} &= \frac{1}{\mathbb{\Gamma}(2j+l+1)} R_{2j+l,j}(0) \\
&= \frac{1}{\mathbb{\Gamma}(2j+l+1)}\big((2j+l-1)R_{2j+l-2,j-1}(0) + jR_{2j+l-1,j}(0)\big) \\
&= \frac{1}{\mathbb{\Gamma}(2j+l-1)} R_{2j+l-2,j}(0) + j\frac{\mathbb{\Gamma}(2j+l)}{\mathbb{\Gamma}(2j+l+1)}\frac{1}{\mathbb{\Gamma}(2j+l)} R_{2j+l-1,j}(0) \\
&= r_{l,j-1} + j\frac{\mathbb{\Gamma}(2j+l)}{\mathbb{\Gamma}(2j+l+1)} r_{l-1,j}. \qquad \square
\end{aligned}$$

Proposition 8. *Pour une constante absolue $c > 0$, on a pour tout $\alpha \in]0,1]$ et pour $j \geqslant \alpha l \geqslant 0$*

$$r_{l,j} \geqslant c^l \alpha^{l/2} \frac{j^{3l/2}}{l!}.$$

Démonstration. En itérant la relation du lemme 7, on a pour $l \geqslant 1$

$$r_{l,j} = \sum_{i \leqslant j} i\frac{\mathbb{\Gamma}(2i+l)}{\mathbb{\Gamma}(2i+l+1)} r_{l-1,i}.$$

Nous avons par la formule de Stirling que pour $t \to +\infty$, on a $\mathbb{\Gamma}(t+1)/\mathbb{\Gamma}(t) \sim \sqrt{t/e}$. Posons K le maximum de $\sqrt{t/3}\,\mathbb{\Gamma}(t)/\mathbb{\Gamma}(t+1)$ pour $t \geqslant 0$. On obtient donc

$$r_{l,j} \geqslant \sum_{i \leqslant j} i\frac{K\sqrt{3}}{\sqrt{2i+l}} r_{l-1,i}.$$

En oubliant les premiers termes de la somme, on a pour tout $\alpha \in]0,1]$

$$\begin{aligned}
r_{l,j} &\geqslant \sum_{\alpha l \leqslant i \leqslant j} i\frac{K\sqrt{3}}{\sqrt{2i+l}} r_{l-1,i} \geqslant \sum_{\alpha l \leqslant i \leqslant j} K\sqrt{\alpha i}\sqrt{\frac{3}{2\alpha+1}} r_{l-1,i} \\
&\geqslant K\sqrt{\alpha} \sum_{\alpha l \leqslant i \leqslant j} \sqrt{i}\, r_{l-1,i}. \qquad (18)
\end{aligned}$$

Nous allons prouver par récurrence sur l que pour tout réel $\alpha \in]0,1]$ et pour tout $j \geqslant \alpha l$ on a

$$r_{l,j} \geqslant \left(K\frac{1-e^{-3/2}}{3/2}\right)^l \alpha^{l/2}\frac{j^{3l/2}}{l!}.$$

Pour $l = 0$, on a par le lemme 7 l'inégalité (et même l'égalité) pour tout $j \geqslant 0$, puisque $r_{0,j} = 1$.

Soit à présent $l \geqslant 1$. Soit $\alpha \in]0, 1]$ un réel. Si pour $i \geqslant \alpha(l-1)$ il est vrai que

$$r_{l-1,i} \geqslant \left(K\frac{1-e^{-3/2}}{3/2}\right)^{l-1} \alpha^{(l-1)/2} \frac{i^{3(l-1)/2}}{(l-1)!},$$

et en utilisant la minoration (18), on a pour $j \geqslant \alpha l$

$$r_{l,j} \geqslant K\left(K\frac{1-e^{-3/2}}{3/2}\right)^{l-1} \alpha^{l/2} \sum_{\alpha l \leqslant i \leqslant j} \frac{i^{3l/2-1}}{(l-1)!}.$$

On a $\lceil \alpha l \rceil \geqslant 1$, donc

$$\begin{aligned} r_{l,j} &\geqslant K\left(K\frac{1-e^{-3/2}}{3/2}\right)^{l-1} \alpha^{l/2} \int_{\lceil \alpha l \rceil - 1}^{j} \frac{x^{3l/2-1}}{(l-1)!}\,\mathrm{d}x \\ &= K\left(K\frac{1-e^{-3/2}}{3/2}\right)^{l-1} \alpha^{l/2} \frac{j^{3l/2}}{\frac{3}{2}l!}\left(1-\left(\frac{\lceil \alpha l \rceil - 1}{j}\right)^{3l/2}\right) \end{aligned}$$

or $j \geqslant \lceil \alpha l \rceil$ et $l \geqslant \lceil \alpha l \rceil$, ce qui donne $((\lceil \alpha l \rceil - 1)/j)^l \leqslant (1 - 1/\lceil \alpha l \rceil)^l \leqslant e^{-l/\lceil \alpha l \rceil} \leqslant e^{-1}$, donc en replaçant cela dans notre expression

$$\geqslant \left(K\frac{1-e^{-3/2}}{3/2}\right)^{l} \alpha^{l/2} \frac{j^{3l/2}}{l!}.$$

Ainsi on a bien uniformément pour tout réel $\alpha \in]0, 1]$ et pour tout $j \geqslant \alpha l \geqslant 0$

$$r_{l,j} \geqslant c^l \alpha^{l/2} \frac{j^{3l/2}}{l!},$$

où l'on peut choisir $c = K\frac{1-e^{-3/2}}{3/2}$ comme constante. □

En choisissant $\alpha = \min(1/2, j/l) \geqslant j/(2j+l)$ dans la proposition 8, on obtient une estimation de $R_{k,j}(0)$ sans faire apparaître de paramètre α.

Corollaire 9. *Pour une constante absolue $c > 0$, on a pour tout $j \geqslant 1$ et pour tout $k \geqslant 2j$*

$$R_{k,j}(0) \geqslant c^k k^j \frac{j^{2(k-2j)}}{(k-2j)!}.$$

Toutefois, ce résultat n'est intéressant que si k et j sont du même ordre de grandeur (c'est-à-dire pour α assez grand). Par exemple, si l'on choisit $j = 1$, le corollaire 9 ne nous donne que $R_{k,1}(0) \gg c^k/k!$ alors que $R_{k,1}(0) = 1$.

3. Moments centrés d'une loi binomiale

On rappelle qu'une variable aléatoire X suit la loi binomiale de paramètre (h, P) si l'on a pour tout entier j la probabilité

$$\mathbb{P}(X = j) = \binom{h}{j} P^j (1-P)^{h-j}.$$

Dans cette partie, nous étudions le comportement asymptotique du moment centré d'ordre k d'une loi binomiale de paramètre (h, P), noté $\mu_k(h, P)$, de façon uniforme en les trois variables k, h et P. Bien que ce moment soit un sujet d'étude courant, les résultats obtenus semblent être inédits. Nous réalisons donc une étude détaillée de ce moment, plus détaillée que ce qui est nécessaire pour établir le théorème A.

On commence par rappeler certaines propriétés de $\mu_k(h, P)$.

Proposition 10. *(Voir Romanovsky [20].) Pour tout $k \geqslant 1$, on a*

$$\mu_{k+1}(h, P) = khP(1-P)\mu_{k-1}(h, P) + P(1-P)\frac{\partial \mu_k}{\partial P}(h, P).$$

On en connaît également certaines expressions

$$\begin{aligned}\mu_k(h, P) &= \mathbb{E}\big(X - \mathbb{E}(X)\big)^k \\ &= \sum_{j=0}^{h} (j - hP)^k \binom{h}{j} P^j (1-P)^{h-j} \\ &= \sum_{a} \binom{k}{a} (-hP)^{k-a} \sum_{b} b! \binom{h}{b} \left\{ {a \atop b} \right\} P^b. \end{aligned} \tag{19}$$

On note également que $\mu_2(h, P) = hP(1-P)$. La dernière identité (19) provient du lemme suivant.

Lemme 11. *Pour tous les entiers naturels h et k, on a l'identité polynomiale suivante*

$$\sum_{j=0}^{h} (j - hX)^k \binom{h}{j} Y^j (1-Y)^{h-j} = \sum_{a} \binom{k}{a} (-hX)^{k-a} \sum_{b} b! \binom{h}{b} \left\{ {a \atop b} \right\} Y^b.$$

Démonstration. On transforme notre expression en utilisant la formule de Newton

$$\begin{aligned}&\sum_{j=0}^{h} (j - hX)^k \binom{h}{j} Y^j (1-Y)^{h-j} \\ &\quad = \sum_{j=0}^{h} (j - hX)^k \binom{h}{j} \sum_{b=0}^{h-j} (-1)^b \binom{h-j}{b} Y^{b+j}\end{aligned}$$

puis en translatant de j la variable b

$$= \sum_{j=0}^{h} \sum_{b=j}^{h} (j - hX)^k (-1)^b (-1)^j \binom{h}{j} \binom{h-j}{b-j} Y^b$$

enfin en interpolant les binomiales $\binom{h}{b}\binom{b}{j} = \binom{h}{j}\binom{h-j}{b-j}$ et en permutant les sommes

$$= \sum_{b=0}^{h} (-1)^b \binom{h}{b} \left(\sum_{j=0}^{b} (-1)^j \binom{b}{j} (j - hX)^k \right) Y^b. \tag{20}$$

On examine la somme intérieure en utilisant de nouveau la formule de Newton

$$\sum_{j=0}^{b} (-1)^j \binom{b}{j} (j - hX)^k = \sum_{j=0}^{b} \sum_{a=0}^{k} (-1)^j \binom{b}{j} \binom{k}{a} j^a (-hX)^{k-a}$$

puis on traite la somme sur j grâce à l'identité $k! \left\{ {n \atop k} \right\} = \sum_{b=0}^{k} (-1)^{k-b} \binom{k}{b} b^n$

$$= \sum_{a=0}^{k} \binom{k}{a} (-hX)^{k-a} (-1)^b b! \left\{ {a \atop b} \right\}. \tag{21}$$

En replaçant (21) dans l'expression (20), on obtient bien l'identité attendue. □

La forme (19) de $\mu_k(h, P)$ est particulièrement importante : elle permet de considérer ce moment comme un polynôme en les variables h et P. Elle permet également de démontrer la proposition suivante.

Proposition 12. *Pour tout $k \geqslant 0$, on a*

$$\mu_{2k}(h, P) = \delta(k) + \sum_{i=1}^{k} \big(hP(1-P)\big)^i Q_{2k,i}\big(P(1-P)\big),$$

$$\mu_{2k+1}(h, P) = (1-2P) \sum_{i=1}^{k} \big(hP(1-P)\big)^i Q_{2k+1,i}\big(P(1-P)\big),$$

où les $Q_{k,i}$ sont des polynômes de degré $\lfloor k/2 \rfloor - i$.

On préférera aux propositions 10 et 12 le corollaire suivant, qui justifie l'introduction au chapitre précédent des polynômes $R_{k,j}$.

Corollaire 13. *Pour tout $k \geqslant 0$, on a*

$$\mu_k(h, P) = \sum_{j \geqslant 0} \big(hP(1-P)\big)^j R_{k,j}(P),$$

où les polynômes $R_{k,j}$ sont les polynômes définis par les conditions initiales $R_{k,0} = R_{0,k} = \delta(k)$ et par la relation de récurrence (13).

Démonstration. On a $\mu_k(h, P) \in \mathbb{Z}[P][hP(1-P)]$ grâce à la proposition 12 : on note $\tilde{R}_{k,j} \in \mathbb{Z}[P]$ le coefficient de $(hP(1-P))^j$ dans $\mu_k(h, P)$. Il reste à montrer que ces polynômes sont bien les polynômes $R_{k,j}$ étudiés au chapitre précédent. Puisque $\mu_0 = 1$, on constate que les polynômes $\tilde{R}_{0,j}$ sont bien égaux aux polynômes $R_{0,j}$. La formule de Romanovsky de la proposition 10 permet de montrer par récurrence que pour $k \geqslant 1$, le polynôme $\mu_k(h, P)$ est un multiple de $hP(1-P)$, donc le polynôme $\tilde{R}_{k,0}$ est nul, tout comme l'est le polynôme $R_{k,0}$. On a donc $\tilde{R}_{k,j} = R_{k,j}$ si $j = 0$ ou si $k = 0$. De plus, la relation de la proposition 10 traduite en terme des polynômes $\tilde{R}_{k,j}$ montre que les polynômes $\tilde{R}_{k,j}$ vérifie la même formule de récurrence (13) que les polynômes $R_{k,j}$. On a donc bien $\tilde{R}_{k,j} = R_{k,j}$ pour tous les entiers j et k. □

On peut à présent utiliser nos connaissances sur les polynômes $R_{k,j}$ pour estimer $\mu_k(h, P)$, et établir un résultat légèrement plus précis que le théorème C.

Proposition 14. *Pour tout $k \geqslant 0$, on a*

$$\mu_k(h, P) \ll c^k k^{k/2} hP(1-P)\big(k + hP(1-P)\big)^{\lfloor k/2 \rfloor - 1},$$

où c est une constante absolue strictement supérieure à $\frac{4}{e}$.

Démonstration. Puisque P est une probabilité, on a $P \in [0, 1]$ et donc

$$\big|R_{k,j}(P)\big| \leqslant \|R_{k,j}\|_1 \leqslant T_j^k \leqslant \left(\frac{4}{e}(k-j)\right)^{k-j} \leqslant \left(\frac{4}{e}\right)^k k^{k-j}, \tag{22}$$

grâce à la proposition 5 et à la majoration (15). On peut donc écrire grâce à la proposition 12

$$\begin{aligned}\big|\mu_k(h, P)\big| &\leqslant \sum_{j=1}^{\lfloor k/2 \rfloor} \big(hP(1-P)\big)^j \big|R_{k,j}(P)\big| \\ &\leqslant \left(\frac{4}{e}\right)^k k^k \sum_{j=1}^{\lfloor k/2 \rfloor} \big(hP(1-P)/k\big)^j\end{aligned}$$

et puisque $\sum_{i=0}^{m} x^i \leqslant (1+x)^m$ pour $x \geqslant 0$,

$$\leqslant \left(\frac{4}{e}\right)^k k^{k-\lfloor k/2 \rfloor} hP(1-P)\big(k + hP(1-P)\big)^{\lfloor k/2 \rfloor - 1}. \qquad \square$$

On peut être étonné de ce changement de comportement asymptotique qui a lieu pour $hP(1-P) \approx k$. On peut cependant obtenir des minorations qui font état de cette déviation.

Proposition 15. *On a uniformément pour $hP(1-P)/k^3 \to +\infty$*

$$\mu_{2k}(h,P) \sim \frac{(2k)!}{2^k k!}\big(hP(1-P)\big)^k.$$

Démonstration. On a égalité si $k=0$, on suppose donc $k \geqslant 1$. En utilisant la propriété (c) du lemme 6 et l'identité du corollaire 13, on a

$$\frac{\mu_{2k}(h,P)}{(2k)!!(hP(1-P))^k} - 1 = \frac{1}{(2k)!!}\sum_{j=1}^{k-1}\frac{R_{2k,j}(P)}{(hP(1-P))^{k-j}}. \tag{23}$$

Or la formule de Stirling permet d'établir $(2k)!! = \frac{(2k)!}{2^k k!} \sim \sqrt{2}\frac{(2k)^k}{e^k}$. Ainsi, on obtient grâce à cette remarque et à la proposition 5

$$\begin{aligned}\frac{\mu_{2k}(h,P)}{(2k)!!(hP(1-P))^k} - 1 &\ll \frac{e^k}{(2k)^k}\sum_{j=1}^{k-1}\frac{(4k-2j)^{2k-j}}{e^{2k-j}(hP(1-P))^{k-j}}\binom{2k-j-1}{j-1}\\ &= \sum_{j=1}^{k-1}\left(1+\frac{k-j}{k}\right)^k\left(\frac{4k-2j}{e\,hP(1-P)}\right)^{k-j}\binom{2k-j-1}{j-1}\end{aligned}$$

or $1+\frac{k-j}{k} \leqslant e^{(k-j)/k}$, donc

$$\leqslant \sum_{j=1}^{k-1}\left(\frac{4k-2j}{hP(1-P)}\right)^{k-j}\binom{2k-j-1}{j-1}$$

en changeant de variable

$$= \sum_{j=1}^{k-1}\left(\frac{2k+2j}{hP(1-P)}\right)^{j}\binom{k+j-1}{k-j-1}$$

or $\binom{k+j-1}{k-j-1} = \binom{k+j-1}{2j} \leqslant \frac{(2k)^{2j}}{(2j)!}$

$$\leqslant \sum_{j=1}^{k-1}\frac{1}{(2j)!}\left(\frac{16k^3}{hP(1-P)}\right)^{j},$$

ce qui est bien $= o(1)$ si $hP(1-P)/k^3 \to +\infty$. □

Ainsi la majoration de la proposition 14 ne peut pas être améliorée (à la valeur de la constante de magnitude près) pour $hP(1-P) \gg k^3$, puisque cela contredirait le résultat de la proposition 15 précédente.

Remarque 16. Il serait intéressant de pouvoir affaiblir cette condition jusqu'à $hP(1-P) \gg k$, qui serait la limite naturelle. Cependant, cette imprécision ne provient pas d'une connaissance imparfaite des polynômes $R_{k,j}$. En effet, dans la somme à estimer de la formule (23), le terme $R_{2k,k-1}(P)/((2k)!!hP(1-P))$—correspondant au choix $j = k-1$—semble être dominant. Et grâce à la formule de récurrence (13), on peut montrer

$$R_{2k,k-1}(P) = \frac{k(k-1)(2k-1)(2k)!!}{18}\left((1-2P)^2 - \frac{6}{2k+1}P(1-P)\right),$$

qui est $o((2k)!!hP(1-P))$ uniformément en P, uniquement lorsque $hP(1-P)/k^3$ tend vers $+\infty$.

Nous prouvons de plus qu'à variance $\bar{\mu}_2$ fixée

$$\sup_{hP(1-P)=\bar{\mu}_2} \mu_k(h,P) \gg_\varepsilon (ck)^{k/2}\left(k^{1-\varepsilon} + hP(1-P)\right)^{k/2}, \tag{24}$$

pour une certaine constante $c > 0$ dépendant au plus de ε. Cela plaide pour l'optimalité de la majoration de la proposition 14.

Nous fixons donc un réel $\bar{\mu}_2 \geqslant 0$, et l'on considère l'ensemble des couples $(h,P) \in \mathbb{R}_+ \times [0,1]$ qui vérifient la condition $hP(1-P) = \bar{\mu}_2$. On note alors $\bar{\mu}_k$ la limite de $\mu_k(h,P)$ pour P tendant vers 0 et pour (h,P) dans l'ensemble sus-cité. Les valeurs de $\bar{\mu}_k$ dépendent donc implicitement de $\bar{\mu}_2$, et les deux définitions de $\bar{\mu}_2$ sont cohérentes entre elles. On a en passant à la limite dans l'expression du corollaire 13 la formule suivante

$$\bar{\mu}_k = \sum_j R_{k,j}(0)\bar{\mu}_2^j = \Gamma(k+1)\sum_j \bar{\mu}_2^j r_{k-2j,j}, \tag{25}$$

puisque les termes $r_{l,j}$ sont définies par (17). La minoration (24) se déduira des deux propositions suivantes.

Proposition 17. *On a uniformément pour $k \geqslant 2$*

$$\bar{\mu}_k \gg c^k k^{k/2}\bar{\mu}_2^{\lfloor k/2 \rfloor},$$

où la constante c est absolue.

Démonstration. Par la proposition 8 avec $\alpha = \min(1/2, j/l) \geqslant j/(2j+l)$, on a

$$\bar{\mu}_k \geqslant c^k \Gamma(k+1) \sum_{2j+l=k} \bar{\mu}_2^j \frac{j^{2l}}{k^{l/2} l!}.$$

On minore la somme par un seul de ses termes que l'on choisit par $j_0 = \lfloor k/2 \rfloor \geqslant 1$ et $l_0 = 2\{k/2\} \leqslant 1$. Ainsi on a $l_0! = 1$ et ${j_0}^2/\sqrt{k} \gg k^{3/2}$, donc

$$\bar{\mu}_k \gg k^{3/2} c^k \Gamma(k+1)\bar{\mu}_2^{\lfloor k/2 \rfloor}. \qquad \square$$

Proposition 18. *On a uniformément pour $k \geqslant 0$, pour $\bar{\mu}_2 > 0$ et pour $\varepsilon \in]0, 1/3]$*

$$\bar{\mu}_k \gg c^k \varepsilon^{2k} k^k (\bar{\mu}_2/k)^{\varepsilon k},$$

où la constante c est absolue.

Démonstration. On pose $\alpha = \varepsilon/(1-2\varepsilon) \in]0, 1]$. On rappelle que l'on note $r_{l,j} = R_{2j+l,j}(0)/\mathbb{\Gamma}(2j+l+1)$, si bien que

$$\bar{\mu}_k = \mathbb{\Gamma}(k+1) \sum_j \bar{\mu}_2^j r_{k-2j,j}.$$

On a par la proposition 8 la minoration valable pour $j \geqslant \alpha l \geqslant 0$

$$r_{l,j} \geqslant C^l \alpha^{l/2} \frac{j^{3l/2}}{l!},$$

où $C > 0$ est une constante absolue. Ainsi, on a

$$\bar{\mu}_k \geqslant \mathbb{\Gamma}(k+1) \sum_{\substack{2j+l=k \\ j \geqslant \alpha l}} C^l \alpha^{l/2} \bar{\mu}_2^j \frac{j^{3l/2}}{l!}.$$

Les conditions de sommation imposent $j \geqslant \frac{\alpha}{1+2\alpha} k = \varepsilon k$. On minore la somme par un seul de ses termes que l'on choisit par $j_0 = \lceil \varepsilon k \rceil \geqslant \varepsilon k$ et $l_0 = k - 2j_0$. On a l'encadrement

$$\frac{\varepsilon}{\alpha} k - 2 = k - 2(\varepsilon k + 1) \leqslant l_0 \leqslant k - 2(\varepsilon k) = \frac{\varepsilon}{\alpha} k.$$

On en déduit $l_0! \leqslant (\frac{\varepsilon}{\alpha} k)^{k\varepsilon/\alpha}$, $j_0^{3l_0/2} \geqslant k^{-3}((\varepsilon k)^{k\varepsilon/\alpha})^{3/2}$, $\bar{\mu}_2^{j_0} \geqslant \bar{\mu}_2^{\varepsilon k}$ et $\alpha^{l_0/2} \geqslant (\alpha^{\varepsilon/\alpha})^{k/2}$. On obtient

$$\begin{aligned} \bar{\mu}_k &\geqslant \mathbb{\Gamma}(k+1) C^{k\varepsilon/\alpha} k^{-3} \left(\varepsilon^{1/2} \alpha^{3/2}\right)^{k\varepsilon/\alpha} \bar{\mu}_2^{\varepsilon k} \left(k^{k\varepsilon/\alpha}\right)^{1/2} \\ &\gg c^k \left(\varepsilon^{1/2} \alpha^{3/2}\right)^{k\varepsilon/\alpha} k^k (\bar{\mu}_2/k)^{\varepsilon k}, \end{aligned}$$

puisque $\varepsilon/\alpha = 1 - 2\varepsilon$ et $\mathbb{\Gamma}(k+1) \gg (k/e)^{k/2}$, et pour une constante absolue $c < C/\sqrt{e}$. Enfin, en remarquant les minorations suivantes $\varepsilon^{1-2\varepsilon} \geqslant \varepsilon$ et $\alpha^{\varepsilon/\alpha} \geqslant \varepsilon$, on obtient la relation souhaitée. □

En choisissant $\varepsilon = \frac{\log 2}{3\log(k/\bar{\mu}_2)}$ dans la proposition 18, on obtient le corollaire suivant.

Corollaire 19. *On a uniformément pour $0 < \bar{\mu}_2 \leqslant k/2$*

$$\bar{\mu}_k \gg \left(\frac{c}{\log(k/\bar{\mu}_2)}\right)^{2k} k^k,$$

où la constante c est absolue.

Lorsque $\bar{\mu}_2$ est vraiment très petit, la minoration obtenue par le corollaire 19 est moins bonne que la minoration triviale $\bar{\mu}_k \geqslant \bar{\mu}_2$ obtenue en ne considérant que le premier terme de la somme de l'identité (25), c'est-à-dire $R_{k,1}(0)\bar{\mu}_2$ et en remarquant que $R_{k,1}(0) = 1$ (cf. lemme 6(d)).

4. Estimation des corrélations sous une forme générale

Cette section est entièrement dédiée à la démonstration du théorème E. Ce résultat représente notre principal apport à la preuve de Montgomery et Vaughan. Avant d'en présenter la preuve, nous souhaitons également en souligner l'enjeu.

L'objectif est de comparer les valeurs

$$\prod_{i=1}^{m}(1-tx_i) \quad \text{et} \quad \left(\prod_{i=1}^{m}(1-x_i)\right)^t,$$

pour une famille de réels $(x_i)_{1\leqslant i\leqslant m}$. Pour établir le théorème E, cette famille sera celle des $1/p$, pour p diviseur premier de q. Pour estimer le moment $M_k(q;h)$ à partir des moments centrés de loi binomiale $\mu_k(h,P)$, Montgomery et Vaughan utilisent la proximité de ces deux produits sous la forme suivante.

Lemme 20. *Soient $\mathbf{x} = (x_1,\dots,x_m) \in \mathbb{R}^m$ un vecteur et $t \geqslant 1$ un entier. Si $\|\mathbf{x}\|_\infty \leqslant 1/t$, on a*

$$\prod_{i=1}^{m}(1-tx_i) - \left(\prod_{i=1}^{m}(1-x_i)\right)^t \ll t^2\|\mathbf{x}\|_2^2\prod_{i=1}^{m}(1-x_i)^t.$$

En mesurant cette proximité grâce à la proposition 21 au travers des quantités (12), nous pouvons étendre le domaine de validité de leur estimation asymptotique de $M_k(q;h)$, et surtout, nous pouvons rendre ces estimations uniformes en k.

Par souci de consision, nous noterons par la suite x_∞ la norme absolue du vecteur $\mathbf{x}$ et $\|\mathbf{x}\|$ sa norme euclidienne.

Proposition 21. *Soient $K, K' > 0$ deux réels, t un entier naturel et $\mathbf{x} \in (\mathbb{C}\smallsetminus\{1\})^m$ un vecteur complexe. On définit le vecteur complexe associé $\mathbf{X} = (\frac{x_1}{1-x_1},\dots,\frac{x_m}{1-x_m})$. Sous les conditions $tX_\infty \leqslant K$ et $t\|\mathbf{X}\|^2 \leqslant K'$, on a*

$$\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}\frac{1-sx_i}{(1-x_i)^s} \leqslant 2{C_1}^t\big(t\|\mathbf{X}\|^2\big)^{t/2} + C_2{C_3}^t\big(t\|\mathbf{X}\|^2\big)^{(t+1)/2},$$

avec

$$C_1 = 2\big(e^{K/\sqrt{2}}-1\big)/K, \quad C_2 = 2\frac{e^K-1}{K}\max(1,\sqrt{K'}) \quad \text{et} \quad C_3 = e^{\frac{K'}{K}(e^K-1)}\sqrt{2e\frac{e^K-1}{K}}.$$

Cet énoncé précise le théorème E. En effet, on peut donner une version compacte (mais moins précise) de la majoration de la proposition sous la forme

$$\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}\frac{1-sx_i}{(1-x_i)^s} \ll_{K,K'} \left(ct\|\mathbf{X}\|^2\right)^{t/2}$$

pour une constante $c>0$ dépendant au plus des paramètres K et K'.

4.1. Égalités polynomiales

Nous transformons la quantité (12) afin d'obtenir une expression polynomiale en les $x_i/(1-x_i)$, plus simple à évaluer.

Lemme 22. *Soit $x\in\mathbb{C}\smallsetminus\{1\}$. En posant $X=x/(1-x)$, on a pour tout entier $t\in\mathbb{N}$*

$$\frac{1-sx}{(1-x)^s}=1-X^2\sum_{r=0}^{s-2}(r+1)\binom{s}{r+2}X^r.$$

Démonstration. On a

$$\frac{1-sx}{(1-x)^s}=\frac{(1-x+x)^{s-1}(1-x-(s-1)x)}{(1-x)^s}=(1+X)^{s-1}\big(1-(s-1)X\big)$$

ce qui vaut en développant

$$=\sum_r\binom{s-1}{r}X^r\big(1-(s-1)X\big)=\sum_r\left(\binom{s-1}{r}-(s-1)\binom{s-1}{r-1}\right)X^r.$$

En retranchant à l'identité d'absorption $r\binom{s}{r}=s\binom{s-1}{r}$ la formule d'addition $\binom{s}{r}=\binom{s-1}{r}+\binom{s-1}{r-1}$, on obtient $(r-1)\binom{s}{r}=(s-1)\binom{s-1}{r-1}-\binom{s-1}{r}$, ce qui permet enfin d'écrire

$$=-\sum_r(r-1)\binom{s}{r}X^r=1-X^2\sum_{r\geqslant 0}(r+1)\binom{s}{r+2}X^r. \qquad \square$$

Lemme 23. *Soit $\mathbf{x}=(x_1,\dots,x_m)\in(\mathbb{C}\smallsetminus\{1\})^m$. En posant $X_i=x_i/(1-x_i)$, on a pour tout entier $s\in\mathbb{N}$*

$$\prod_{i=1}^{m}\frac{1-sx_i}{(1-x_i)^s}=\sum_{J\subset[\![1,m]\!]}(-1)^{|J|}\left(\prod_{j\in J}X_j\right)^2\sum_{\substack{r_j\geqslant 0\\(j\in J)}}\prod_{j\in J}(r_j+1)\binom{s}{r_j+2}{X_j}^{r_j}.$$

Démonstration. Il s'agit de développer le produit obtenu en utilisant le lemme 22 pour chacune des m variables x_i. $\square$

Proposition 24. *Soit* $\mathbf{x} = (x_1, \dots, x_m) \in (\mathbb{C} \setminus \{1\})^m$. *En posant* $X_i = x_i/(1-x_i)$, *on a pour tout entier* $t \in \mathbb{N}$

$$\sum_{s=0}^{t} (-1)^{t-s} \binom{t}{s} \prod_{i=1}^{m} \frac{1 - s x_i}{(1-x_i)^s} = \sum_{J \subset [\![1,m]\!]} (-1)^{|J|} \left(\prod_{j \in J} X_j \right)^2 t! \sum_{\substack{r_j \geqslant 0 \\ (j \in J)}} \omega(\mathbf{r} + \mathbf{2}, t) \prod_{j \in J} \frac{r_j + 1}{(r_j+2)!} {X_j}^{r_j}.$$

Ici, pour un vecteur d'entiers $\mathbf{r} = (r_j)_{j \in J}$, le vecteur $\mathbf{r} + \mathbf{2}$ désigne le vecteur d'entiers $(r_j + 2)_{j \in J}$.

Démonstration. On a par le lemme 23

$$\sum_{s=0}^{t} (-1)^{t-s} \binom{t}{s} \prod_{i=1}^{m} \frac{1 - s x_i}{(1-x_i)^s} = \sum_{J \subset [\![1,m]\!]} (-1)^{|J|} \left(\prod_{j \in J} X_j \right)^2 \sum_{\substack{r_j \geqslant 0 \\ (j \in J)}} \prod_{j \in J} (r_j + 1) {X_j}^{r_j} \sum_{s=0}^{t} (-1)^{t-s} \binom{t}{s} \prod_{j \in J} \binom{s}{r_j + 2},$$

ce qui fournit le résultat souhaité en utilisant la définition (11) de $\omega(\mathbf{r}, t)$. □

4.2. Étude du coefficient $\omega(\mathbf{r}, t)$

Nous allons majorer le coefficient $\omega(\mathbf{r}, t)$ en l'interprétant comme solution d'un problème énumératif.

Lemme 25. *Soient* t *un entier naturel et* $\mathbf{r} = (r_1, \dots, r_k)$ *un* k*-uplet d'entiers naturels. Il existe exactement*

$$\frac{t!}{\prod_{j=1}^{k} r_j!} \omega(\mathbf{r}, t)$$

façons de choisir k *sous-ensembles* $A_1, \dots, A_k$ *de* $[\![1, t]\!]$ *vérifiant les conditions suivantes* :

- $\forall j$, $\operatorname{card} A_j = r_j$;
- $\bigcup_{j=1}^{k} A_j = [\![1, t]\!]$.

Démonstration. Soit un sous-ensemble $E \subset [\![1, t]\!]$ de cardinal s. Le nombre de k-uplets $(A_1, \dots, A_k)$ de sous-ensembles de E vérifiant $\operatorname{card} A_j = r_j$ pour tout j est exactement $\prod_{j=1}^{k} \binom{s}{r_j}$. Par principe d'inclusion-exclusion, le nombre recherché est donc

$$\sum_{s=0}^{t} (-1)^{t-s} \binom{t}{s} \prod_{j=1}^{k} \binom{s}{r_j}$$

qui vaut bien $\frac{t!}{\prod_{j=1}^{k} r_j!} \omega(\mathbf{r}, t)$ par la définition (11). □

Cela nous apporte déjà une quantité d'informations sur les coefficients $\omega(\mathbf{r}, t)$:

(a) Si $\sum_{j=1}^{k} r_j < t$, on a $\omega(\mathbf{r}, t) = 0$. En effet, l'existence de k-uplets comptés dans le lemme 25 implique l'inégalité

$$t = \operatorname{card} \bigcup_{j=1}^{k} A_j \leqslant \sum_{j=1}^{k} \operatorname{card} A_j = \sum_{j=1}^{k} r_j.$$

(b) On a $0 \leqslant \omega(\mathbf{r}, t) \leqslant t^{r_1+\cdots+r_k}/t!$. En effet, le nombre de k-ulpets vérifiant les deux conditions du lemme 25 sont moins nombreux que les k-uplets qui ne vérifient que la première des conditions, et qui sont au nombre de $\prod_{j=1}^{k} \binom{t}{r_j}$. Ainsi, on a

$$\omega(\mathbf{r}, t) \leqslant \frac{\prod_{j=1}^{k} r_j!}{t!} \prod_{j=1}^{k} \binom{t}{r_j} = \frac{1}{t!} \prod_{j=1}^{k} r_j! \binom{t}{r_j} \leqslant \frac{1}{t!} \prod_{j=1}^{k} t^{r_j}.$$

La positivité est évidente.

Ces deux remarques suffisent à établir le théorème E, même avec une constante explicite. Mais pour obtenir la qualité des constantes C_1, C_2 et C_3 de la proposition 21, nous allons donner une nouvelle interprétation énumérative de $\omega(\mathbf{r}, t)$ menant à des estimations plus précises.

On pose pour la suite de ce paragraphe $r := \sum_{j=1}^{k} r_j$.

Lemme 26. *Soient t un entier et $\{R_j\}_{1 \leqslant j \leqslant k}$ une partition de l'ensemble $[\![1, r]\!]$. Posons $\mathbf{r} = (\operatorname{card} R_1, \ldots, \operatorname{card} R_k)$. Il existe exactement $\omega(\mathbf{r}; t)$ partitions $\{B_i\}_{1 \leqslant i \leqslant t}$ en t parties de l'ensemble $[\![1, r]\!]$ vérifiant $\operatorname{card}(R_j \cap B_i) \leqslant 1$ pour tout $1 \leqslant j \leqslant k$ et tout $1 \leqslant i \leqslant t$.*

Démonstration. La partition $\{R_1, \ldots, R_k\}$ étant donnée, on pose $r_j = \operatorname{card} R_j$ pour tout j. On souhaite compter le nombre de surjections $\tau : [\![1, r]\!] \twoheadrightarrow [\![1, t]\!]$ telles les k applications restreintes $\tau_j : R_j \to [\![1, t]\!]$ soient toutes des injections.

Premier calcul. Toute application $\tau : [\![1, r]\!] \to [\![1, t]\!]$ se décompose de la façon suivante : pour chaque j, on pose A_j comme l'image de l'application τ_j et $\tilde{\tau}_j : R_j \twoheadrightarrow A_j$ comme la surjection issue de τ_j. La donnée de k sous-ensembles $A_j \subset [\![1, t]\!]$ et de k surjections $\tilde{\tau}_j : R_j \twoheadrightarrow A_j$ permet de définir uniquement chaque application $\tau : [\![1, r]\!] \to [\![1, t]\!]$. On souhaite compter les applications τ qui vérifient que :

- les τ_j sont des injections pour tout $1 \leqslant j \leqslant k$;
- τ est une surjection.

La première condition se traduit par le fait que les k applications $\tilde{\tau}_j$ sont bijectives, et donc que l'ensemble A_j est de cardinal r_j. Ainsi pour chaque choix de k sous-ensembles $A_j \subset [\![1, t]\!]$ de cardinaux respectifs r_j, il y a exactement $\prod r_j!$ choix possibles pour le k-uplets de bijections $\tilde{\tau}_j$.

L'image de τ est l'union de celles des τ_j donc la surjectivité de τ est équivalente à $\bigcup A_j = [\![1, t]\!]$. Grâce au lemme 25, le nombre d'applications τ recherchées vaut

$$\prod_{j=1}^{k} r_j! \times \left(\frac{t!}{\prod_{j=1}^{k} r_j!} \omega(\mathbf{r}, t) \right) = t! \omega(\mathbf{r}, t).$$

Second calcul. Toute surjection $\tau : [\![1, r]\!] \to [\![1, t]\!]$ se décompose de la façon suivante : pour une partition $\{B_i\}_{1 \leqslant i \leqslant t}$ de $[\![1, r]\!]$ en t parties et une bijection σ de l'ensemble des parties de la partition dans $[\![1, t]\!]$, on peut définir la surjection qui à un élément x de $[\![1, r]\!]$ associe l'image par ρ de la partie B_i qui contient x. On cherche à compter les surjections τ telles que les restrictions τ_j soient des injections. Cette propriété ne dépend pas de la bijection σ, mais uniquement du fait que chaque partie R_j ne contienne pas deux pré-images par τ d'un même élément de $[\![1, t]\!]$, peu importe cet élément ; en d'autres termes, il faut et il suffit que $\operatorname{card} B_i \cap R_j < 2$ pour tout i et pour tout j. Le nombre de surjections τ recherchées est donc $t!$ fois le nombre de partitions $\{B_i\}_{1 \leqslant i \leqslant t}$ de $[\![1, r]\!]$ en t parties vérifiant $\operatorname{card} B_i \cap R_j \leqslant 1$ pour tout $1 \leqslant i \leqslant t$ et pour tout $1 \leqslant j \leqslant k$.

En comparant les résultats des deux précédents calculs, on établit le résultat annoncé. □

On déduit de ceci que $\omega(\mathbf{r}, t)$ est un entier, mais surtout une estimation de ω qui précise les propriétés (a) et (b) mentionnées plus haut.

Corollaire 27. *Soient t un entier naturel et $\mathbf{r} = (r_1, \ldots, r_k)$ un k-uplets d'entiers naturels. On pose $r = \sum_{j=1}^{k} r_j$. On a l'encadrement $0 \leqslant \omega(\mathbf{r}, t) \leqslant \left\{ {r \atop t} \right\}$.*

4.3. Quelques majorations combinatoires

La proposition 24 nous pousse donc à majorer le terme

$$\sum_{\substack{r_j \geqslant 0 \\ (j \in J)}} \omega(\mathbf{r} + \mathbf{2}, t) \prod_{j \in J} \frac{r_j + 1}{(r_j + 2)!} {X_j}^{r_j}.$$

Ces majorations se basent sur l'estimation de la quantité $\omega(\mathbf{r}, t)$ fournie par le corollaire 27. Nous en profitons pour rappeler la fonction génératrice exponentielle des nombres de Stirling de seconde espèce :

$$\sum_{s} \left\{ {s \atop t} \right\} \frac{Y^s}{s!} = \frac{(e^Y - 1)^t}{t!}. \tag{26}$$

Similairement au lemme 20, nous devons supposer que $\max |x_i| \ll 1/t$, ce qui équivaut *approximativement* à supposer $X_\infty \ll 1/t$, où l'on a posé $X_\infty := \max |X_i|$. Pour expliquer par la suite cet « approximativement » de façon rigoureuse, nous allons fixer un réel $K > 0$ et nous allons supposer que $t X_\infty \leqslant K$. On utilisera aussi la norme euclidienne que l'on notera $\| \cdot \|$.

Lemme 28. *Sous la condition $tX_\infty \leqslant K$, on a*

$$\left| \sum_{\substack{r_j \geqslant 0 \\ (j \in J)}} \omega(\mathbf{r}+\mathbf{2},t) \prod_{j\in J} \frac{r_j+1}{(r_j+2)!} {X_j}^{r_j} \right| \leqslant \frac{t^{2|J|}}{t!} \left(\frac{e^K-1}{K} \right)^{|J|}.$$

Démonstration. En utilisant le corollaire 27, en majorant les $|X_j|$ par X_∞ et en remarquant que $\frac{r_j+1}{(r_j+2)!} \leqslant \frac{1}{(r_j+1)!}$, on a

$$\sum_{\substack{r_j \geqslant 0 \\ (j \in J)}} \omega(\mathbf{r}+\mathbf{2},t) \prod_{j\in J} \frac{r_j+1}{(r_j+2)!} {X_j}^{r_j} \leqslant \sum_{\substack{r_j \geqslant 0 \\ (j \in J)}} \left\{ \begin{matrix} \sum_J r_j + 2|J| \\ t \end{matrix} \right\} \frac{{X_\infty}^{\sum_J r_j}}{\prod_{j\in J}(r_j+1)!}.$$

En posant $r = \sum_J r_j$ et en faisant apparaître un coefficient multinomial, on obtient une nouvelle expression du majorant en

$$\sum_{r\geqslant 0} \left\{ \begin{matrix} r+2|J| \\ t \end{matrix} \right\} \frac{{X_\infty}^r}{(r+|J|)!} \sum_{\substack{r_j \geqslant 0 \\ (j\in J) \\ \sum_j r_j = r}} \binom{r+|J|}{\mathbf{r}+\mathbf{1}},$$

et la somme intérieure vaut $|J|! \left\{ \begin{matrix} r+|J| \\ |J| \end{matrix} \right\}$: on obtient la majoration

$$\left| \sum_{\substack{r_j \geqslant 0 \\ (j \in J)}} \omega(\mathbf{r}+\mathbf{2},t) \prod_{j\in J} \frac{r_j+1}{(r_j+2)!} {X_j}^{r_j} \right| \leqslant \sum_{r\geqslant 0} \frac{|J|!}{(r+|J|)!} \left\{ \begin{matrix} r+2|J| \\ t \end{matrix} \right\} \left\{ \begin{matrix} r+|J| \\ |J| \end{matrix} \right\} {X_\infty}^r.$$

On utilise la majoration $\left\{ \begin{matrix} n \\ k \end{matrix} \right\} \leqslant k^n/k!$ pour faire disparaître le premier nombre de Stirling :

$$\begin{aligned} &\sum_{r\geqslant 0} \frac{|J|!}{(r+|J|)!} \left\{ \begin{matrix} r+2|J| \\ t \end{matrix} \right\} \left\{ \begin{matrix} r+|J| \\ |J| \end{matrix} \right\} {X_\infty}^r \\ &\quad \leqslant \frac{t^{2|J|}}{t!} \sum_{r\geqslant 0} \frac{|J|!}{(r+|J|)!} \left\{ \begin{matrix} r+|J| \\ |J| \end{matrix} \right\} (tX_\infty)^r = \frac{t^{2|J|}}{t!} \sum_{r\geqslant 0} \frac{|J|!}{r!} \left\{ \begin{matrix} r \\ |J| \end{matrix} \right\} (tX_\infty)^{r-|J|} \end{aligned}$$

où, malgré l'ajout de $|J|$ termes à la somme consécutivement au changement de variable, l'égalité est justifiée par la nullité des nombres de Stirling $\left\{ \begin{matrix} r \\ |J| \end{matrix} \right\}$ lorsque $r < |J|$. On utilise l'identité (26) pour transformer le majorant

$$\frac{t^{2|J|}}{t!} \sum_{r\geqslant 0} \frac{|J|!}{r!} \left\{ \begin{matrix} r \\ |J| \end{matrix} \right\} (tX_\infty)^{r-|J|} = \frac{t^{2|J|}}{t!} \left(\frac{e^{tX_\infty}-1}{tX_\infty} \right)^{|J|}.$$

Par convexité de la fonction exponentielle, la condition $tX_\infty \leqslant K$ fournit la majoration désirée. □

Cette estimation n'exploite pas le fait que $\omega(\mathbf{r};t)=0$ lorsque $r<t$, ce qui améliore l'estimation pour de petits ensembles J. Par $\mathbf{X}_J$, on désigne le vecteur $(X_j)_{j\in J}$

Lemme 29. *Sous les conditions $tX_\infty \leqslant K$ et $t \geqslant 2|J|$, on a*

$$\Big|\sum_{\substack{r_j\geqslant 0\\(j\in J)}} \omega(\mathbf{r}+\mathbf{2},t)\prod_{j\in J}\frac{r_j+1}{(r_j+2)!}{X_j}^{r_j}\Big| \leqslant \frac{\sqrt{(2|J|)!}|J|^{t/2}}{t!}\Big(2\frac{e^{K/\sqrt{2}}-1}{K}\Big)^t \|\mathbf{X}_J\|^{t-2|J|}.$$

Démonstration. En regroupant les termes selon la valeur de $|\mathbf{r}| := \sum_J r_j$ et en utilisant l'inégalité de Cauchy–Schwarz, on a

$$\sum_{\substack{r_j\geqslant 0\\(j\in J)}} \omega(\mathbf{r}+\mathbf{2},t)\prod_{j\in J}\frac{r_j+1}{(r_j+2)!}{X_j}^{r_j}$$
$$\leqslant \sum_{r\geqslant 0}\Big(\sum_{\substack{r_j\geqslant 0\\(j\in J)\\|\mathbf{r}|=r}} \frac{\omega(\mathbf{r}+\mathbf{2},t)^2}{\prod_{j\in J} r_j!(r_j+2)^2}\Big)^{1/2}\Big(\sum_{\substack{r_j\geqslant 0\\(j\in J)\\|\mathbf{r}|=r}}\prod_{j\in J}\frac{|X_j|^{2r_j}}{r_j!}\Big)^{1/2},$$

puis en utilisant la borne du corollaire 27 et en faisant apparaître des coefficients multinomiaux

$$\leqslant \sum_{r\geqslant 0}\frac{\left\{{r+2|J|\atop t}\right\}}{\sqrt{r!(r+2|J|)!}}\Big(\sum_{\substack{r_j\geqslant 0\\(j\in J)\\|\mathbf{r}|=r}}\binom{r+2|J|}{\mathbf{r}+\mathbf{2}}\Big)^{1/2}\Big(\sum_{\substack{r_j\geqslant 0\\(j\in J)\\|\mathbf{r}|=r}}\binom{r}{\mathbf{r}}\prod_{j\in J}|X_j|^{2r_j}\Big)^{1/2}.$$

En remarquant que $1/r! = (2|J|)!/(r+2|J|)!\binom{r+2|J|}{2|J|} \leqslant (2|J|)!/(r+2|J|)!\,2^{r+2|J|}$, que par formule de Newton le premier terme entre parenthèse est majoré par $|J|^{r+2|J|}$ et le second vaut $\|\mathbf{X}_J\|^{2r}$, on poursuit notre majoration par

$$\leqslant \sum_{r\geqslant 0}\frac{\sqrt{(2|J|)!}}{(r+2|J|)!}\left\{{r+2|J|\atop t}\right\}\sqrt{2|J|}^{r+2|J|}\|\mathbf{X}_J\|^r$$
$$= \sum_{r\geqslant 0}\frac{\sqrt{(2|J|)!}}{r!}\left\{{r\atop t}\right\}\sqrt{2|J|}^{r}\|\mathbf{X}_J\|^{r-2|J|},$$

après changement de variable. La dernière ligne est bien une égalité lorsque $t\geqslant 2|J|$, malgré l'ajout de $2|J|$ termes, grâce à la nullité des nombres de Stirling $\left\{{r\atop t}\right\}$. On utilise l'identité (26) pour obtenir le majorant

$$\sqrt{(2|J|)!}\|\mathbf{X}_J\|^{-2|J|}\sum_{r\geqslant 0}\frac{1}{r!}\left\{{r\atop t}\right\}\big(\sqrt{2|J|}\|\mathbf{X}_J\|\big)^r = \frac{\sqrt{(2|J|)!}}{t!}\frac{(e^{\sqrt{2|J|}\|\mathbf{X}_J\|}-1)^t}{\|\mathbf{X}_J\|^{2|J|}}.$$

Par convexité de la fonction exponentielle, la condition $\sqrt{2|J|}\|\mathbf{X}_J\| \leqslant \sqrt{2}|J|X_\infty \leqslant tX_\infty/\sqrt{2} \leqslant K/\sqrt{2}$ fournit la majoration désirée. □

4.4. Estimations finales

Nous débutons par trois lemmes généraux, dont le premier est généralement attribué à Erdős. On rappelle que la norme notée $\|\cdot\|$ est la norme euclidienne.

Lemme 30. *Soit k un entier naturel. On a*

$$\sum_{\substack{J\subset[\![1,m]\!]\\|J|=k}} \left|\prod_{j\in J} X_j\right|^2 \leqslant \frac{\|\mathbf{X}\|^{2k}}{k!}.$$

Démonstration. On a

$$\left(\sum_{i=1}^{m}|X_i|^2\right)^k = \sum_{\substack{i_j\in[\![1,m]\!]\\(j\in[\![1,k]\!])}}\left|\prod_{j=1}^{k}X_{i_j}\right|^2 \geqslant \sum_{\substack{i_j\in[\![1,m]\!]\\(j\in[\![1,k]\!])\\\forall j\neq j',\, i_j\neq i_{j'}}}\left|\prod_{j=1}^{k}X_{i_j}\right|^2 = k!\sum_{\substack{i_j\in[\![1,m]\!]\\(j\in[\![1,k]\!])\\i_1<\cdots<i_k}}\left|\prod_{j=1}^{k}X_{i_j}\right|^2.$$

En posant $J=\{i_j;\ j\in[\![1,k]\!]\}$, on retrouve bien l'inégalité annoncée. □

Lemme 31. *Soit $\kappa>0$ un réel. On a*

$$\sum_{J\subset[\![1,m]\!]}\kappa^{|J|}\left|\prod_{j\in J}X_j\right|^2 \leqslant \exp\bigl(\kappa\|\mathbf{X}\|^2\bigr).$$

Démonstration. C'est un corollaire du lemme 30 précédent. On peut aussi remarquer que la somme à majorer est le produit

$$\prod_{i=1}^{m}\bigl(1+\kappa|X_i|^2\bigr) \leqslant \exp\left(\kappa\sum_{i=1}^{m}|X_i|^2\right). \qquad \square$$

Lemme 32. *Soient $\kappa>0$ un réel et k un entier naturel. On a*

$$\sum_{\substack{J\subset[\![1,m]\!]\\|J|\geqslant k}}\kappa^{|J|}\left|\prod_{j\in J}X_j\right|^2 \leqslant \kappa^k\exp\bigl(\kappa\|\mathbf{X}\|^2\bigr)\frac{\|\mathbf{X}\|^{2k}}{k!}.$$

Démonstration. Il s'agit d'un corollaire du lemme 30 précédent si l'on remarque que $\sum_{n\geqslant k}\frac{x^n}{n!}\leqslant\frac{x^k}{k!}e^x$. On peut aussi remarquer qu'un ensemble J à plus de k éléments peut s'écrire

plus d'une fois comme réunion disjointe d'un ensemble J_1 à k élément et d'un autre ensemble J_2, donc

$$\sum_{\substack{J\subset[\![1,m]\!]\\|J|\geqslant k}} \kappa^{|J|}\left|\prod_{j\in J} X_j\right|^2 \leqslant \left[\kappa^k \sum_{\substack{J_1\subset[\![1,m]\!]\\|J_1|=k}} \left|\prod_{j\in J_1} X_j\right|^2\right] \times \left[\sum_{J_2\subset[\![1,m]\!]} \kappa^{|J_2|}\left|\prod_{j\in J_2} X_j\right|^2\right].$$

Les lemmes 30 et 31 permettent de conclure. □

Démonstration de la proposition 21. On sépare la somme de la proposition 24 en deux, selon la valeur de $|J|$ par rapport à $t/2$, et l'on applique respectivement à l'une et à l'autre des sous-sommes obtenues, les majorations des lemmes 29 et 28 :

$$\begin{aligned}
&\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{i=1}^{m}\frac{1-sx_i}{(1-x_i)^s}\\
&\quad=\left\{\sum_{\substack{J\subset[\![1,m]\!]\\|J|\leqslant t/2}}+\sum_{\substack{J\subset[\![1,m]\!]\\|J|>t/2}}\right\}(-1)^{|J|}\left(\prod_{j\in J}X_j\right)^2 t!\sum_{\substack{r_j\geqslant 0\\(j\in J)}}\omega(\mathbf{r}+\mathbf{2},t)\prod_{j\in J}\frac{r_j+1}{(r_j+2)!}{X_j}^{r_j}\\
&\quad\leqslant\sum_{\substack{J\subset[\![1,m]\!]\\|J|\leqslant t/2}}\left|\prod_{j\in J}X_j\right|^2\sqrt{(2|J|)!}|J|^{t/2}\left(2\frac{e^{K/\sqrt{2}}-1}{K}\right)^t\|\mathbf{X}_J\|^{t-2|J|}\\
&\qquad+\sum_{\substack{J\subset[\![1,m]\!]\\|J|>t/2}}\left|\prod_{j\in J}X_j\right|^2 t^{2|J|}\left(\frac{e^K-1}{K}\right)^{|J|}.
\end{aligned}$$

On pose par commodité $k=|J|$, $c_1=2(e^{K/\sqrt{2}}-1)/K$ et $c_2=(e^K-1)/K$. On traite d'abord la première somme Σ_1 en majorant $\|\mathbf{X}_J\|\leqslant\|\mathbf{X}\|$, puis grâce au lemme 30

$$\begin{aligned}
\Sigma_1&\leqslant {c_1}^t\sum_{k=0}^{\lfloor t/2\rfloor}k^{t/2}\frac{\sqrt{(2k)!}}{k!}\|\mathbf{X}\|^{2k}\|\mathbf{X}\|^{t-2k}\\
&={c_1}^t\sum_{k=0}^{\lfloor t/2\rfloor}k^{t/2}\binom{2k}{k}^{1/2}\|\mathbf{X}\|^t\\
&\leqslant {c_1}^t\|\mathbf{X}\|^t(t/2)^{t/2}\sum_{k=0}^{\lfloor t/2\rfloor}2^k\leqslant 2{c_1}^t\big(t\|\mathbf{X}\|^2\big)^{t/2}.
\end{aligned}$$

Pour la seconde somme, on utilise le lemme 32

$$\Sigma_2\leqslant\big(c_2t^2\big)^{\lfloor t/2\rfloor+1}\exp\big(c_2t^2\|\mathbf{X}\|^2\big)\frac{\|\mathbf{X}\|^{2\lfloor t/2\rfloor+2}}{(\lfloor t/2\rfloor+1)!}$$

et grâce aux inégalités $n! \geqslant (n/e)^n e$

$$\leqslant e^{-1}\left(c_2 e \frac{t^2}{\lfloor t/2\rfloor + 1}\|\mathbf{X}\|^2\right)^{\lfloor t/2\rfloor+1} e^{c_2 t^2\|\mathbf{X}\|^2}$$
$$\leqslant 2c_2\left(2c_2 e^{2c_2 t\|\mathbf{X}\|^2+1}\right)^{t/2}\left(t\|\mathbf{X}\|^2\right)^{\lfloor t/2\rfloor+1}$$

et si $t\|\mathbf{X}\|^2 \leqslant K'$

$$= 2c_2 \max(1, \sqrt{K'})\left(2c_2 e^{2c_2 K'+1}\right)^{t/2}\left(t\|\mathbf{X}\|^2\right)^{(t+1)/2}. \qquad \square$$

5. Démonstration du théorème principal

Ce chapitre est entièrement consacré à la preuve du théorème A et de son corollaire B. Afin d'alléger certaines formules d'un facteur $\log 2$, nous supposerons q impair et donc que $\log P^-(q) \geqslant 1$.

On introduit pour $h, k \in \mathbb{N}$ la fonction $m_k(h, X, Y)$, polynomiale en X et en Y, définie par

$$m_k(h, X, Y) := \sum_j (j - hX)^k \binom{h}{j} Y^j (1 - Y)^{h-j}.$$

Le polynôme $m_k(h, X, Y)$ possède beaucoup de points communs avec le moment centré de la loi binomiale : en effet, il est immédiat que $m_k(h, P, P) = \mu_k(h, P)$. De même, il s'écrit aussi sous forme d'un polynôme de $\mathbb{Z}[h, X, Y]$ grâce au lemme 11

$$m_k(h, X, Y) = \sum_a \binom{k}{a}(-hX)^{k-a} \sum_b b! \binom{h}{b} \left\{ \begin{matrix} a \\ b \end{matrix} \right\} Y^b.$$

Lemme 33. *Soit k un entier naturel. On a l'identité polynomiale suivante*

$$m_k(h, X, Y) = \sum_t \binom{k}{t} \big(h(Y - X)\big)^t \mu_{k-t}(h, Y).$$

Démonstration. On a pour $h \in \mathbb{N}$

$$m_k(h, X, Y) = \sum_j (j - hX)^k \binom{h}{j} Y^j (1 - Y)^{h-j}$$
$$= \sum_j \sum_t \binom{k}{t} (j - hY)^{k-t} (hY - hX)^t \binom{h}{j} Y^j (1 - Y)^{h-j}$$
$$= \sum_t \binom{k}{t} \big(h(Y - X)\big)^t m_{k-t}(h, Y, Y).$$

Comme les deux termes de l'identité sont des éléments de $\mathbb{Z}[h, X, Y]$, l'identité a un sens en tant qu'identité polynomiale. $\square$

Sous la condition $P^-(q) \geqslant h$, l'espérance calculée à partir des observations des variables Y_i vaut

$$\mathbb{E}_{\text{obs}}\left(\prod_{i\in I} Y_i\right) = \frac{1}{q}\sum_{n=1}^{q}\prod_{i\in I}[n+i \perp q] = \prod_{p|q}\left(1-\frac{\operatorname{card} I}{p}\right)$$

pour un sous-ensemble $I \subset [\![1, P^-(q)]\!]$. Comme ces quantités dépendent de I uniquement par son cardinal, cela nous conduit à définir une forme linéaire $\mathbb{E}_{\text{obs}}$ (dépendant de q) sur l'espace des polynômes en une variable Y de degré au plus $P^-(q)$ par

$$\mathbb{E}_{\text{obs}}\big(Y^t\big) := \prod_{p|q}\left(1-\frac{t}{p}\right), \tag{27}$$

pour tout $t \leqslant P^-(q)$. On étend également la définition du moment $M_k(q;h)$ aux ensembles finis $I \subset \mathbb{N}$ de la façon suivante

$$M_k(q;I) := \sum_{n=1}^{q}\left(\sum_{i\in I}[n+i \perp q] - \frac{\varphi(q)}{q}\operatorname{card} I\right)^k,$$

si bien que $M_k(q;h) = M_k(q;[\![1,h]\!])$.

La démonstration du lemme 9 de [18] contient essentiellement le résultat suivant, qui nous sera utile lors de la démonstration du corollaire B.

Lemme 34. *Soient q un entier naturel et $I \subset [\![1, P^-(q)]\!]$. On pose $h = \operatorname{card} I$. On a*

$$M_k(q;I) = q\mathbb{E}_{\text{obs}}\big(m_k(h,P,Y)\big).$$

En particulier, on a $M_k(q;I) = M_k(q;h)$.

Des lemmes 33 et 34, on voit que la quantité à étudier est

$$q\sum_t \binom{k}{t} h^t \mathbb{E}_{\text{obs}}\big((Y-P)^t \mu_{k-t}(h,Y)\big),$$

pour laquelle on profite de la bonne connaissance des moments $\mu_k(h,P)$ acquise précédemment, notamment au travers des polynômes $R_{k,j}$, ainsi que de la bonne connaissance des corrélations $\mathbb{E}_{\text{obs}}((Y-P)^t)$ grâce aux calculs du chapitre précédent. L'évaluation de ces corrélations constitue le cœur de notre raisonnement ; il s'agit d'une reformulation de la proposition D de l'introduction.

Lemme 35. *Uniformément pour tout entier naturel t et pour tout entier q sans facteur carré vérifiant $t \leqslant P^-(q)$, on a*

$$\mathbb{E}_{\text{obs}}\big((Y/P-1)^t\big) \ll \left(c\frac{t}{P^-(q)\log P^-(q)}\right)^{t/2},$$

où la constante $c > 0$ est absolue.

Démonstration. Par la formule du binôme et par la définition (27), il est clair que l'expression à majorer est

$$\mathbb{E}_{\text{obs}}\big((Y/P-1)^t\big)=\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}P^{-s}\mathbb{E}_{\text{obs}}\big(Y^s\big)$$
$$=\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{p|q}\frac{1-s/p}{(1-1/p)^s}.$$

Cette expression est une spécialisation au vecteur $\mathbf{x}=(1/p_1,\dots,1/p_m)$ du moment considéré par le théorème E, où $p_1, p_2, \dots, p_m$ sont les facteurs premiers de q ordonnés de façon croissante, i.e. $q=p_1p_2\cdots p_m$ et $p_1<p_2<\cdots<p_m$. On a clairement $\|\mathbf{X}\|^2=\sum_i 1/(p_i-1)^2\ll 1/(p_1\log p_1)$. Par le théorème E, on a sous la condition $t\leqslant P^-(q)$

$$\sum_{s=0}^{t}(-1)^{t-s}\binom{t}{s}\prod_{p|q}\frac{1-s/p}{(1-1/p)^s}\ll\left(c\frac{t}{P^-(q)\log P^-(q)}\right)^{t/2},$$

pour une constante $c>0$ absolue, ce qui fournit bien la majoration désirée. □

Corollaire 36. *Uniformément pour tout couple d'entiers naturels (t,m) et pour tout entier q sans facteur carré vérifiant $t+m\leqslant P^-(q)$ on a*

$$\mathbb{E}_{\text{obs}}\big((Y-P)^tY^m\big)\ll(cP)^{t+m}\frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}},$$

pour une constante $c>0$ absolue.

Démonstration. Puisque $Y=(Y-P)+P$, on a

$$\mathbb{E}_{\text{obs}}\big((Y-P)^tY^m\big)=P^{t+m}\sum_{k=0}^{m}\binom{m}{k}\mathbb{E}_{\text{obs}}\big((Y/P-1)^{t+k}\big)$$

et grâce au lemme 35, on sait que pour une constante absolue C on a uniformément

$$\ll P^{t+m}\sum_{k=0}^{m}\binom{m}{k}C^{t+k}\frac{(t+k)^{(t+k)/2}}{(P^-(q)\log P^-(q))^{(t+k)/2}}$$
$$\ll P^{t+m}C^t\frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}}\sum_{k=0}^{m}\binom{m}{k}C^k\left(1+\frac{k}{t}\right)^{t/2}\left(\frac{t+k}{P^-(q)\log P^-(q)}\right)^{k/2}$$

or on a $t+k\leqslant t+m\leqslant P^-(q)$ et $(1+k/t)^t\leqslant e^k$, donc

$$\ll P^{t+m}C^t\big(Ce^{1/2}+1\big)^m\frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}}$$

$$\ll c^{t+m} P^{t+m} \frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}},$$

où l'on a posé $c = Ce^{1/2} + 1$. □

Corollaire 37. *Uniformément pour tout couple d'entiers naturels (t, m), tout polynôme R de $\mathbb{R}[X]$ de degré d et pour tout entier q sans facteur carré vérifiant $t + m + d \leqslant P^-(q)$ on a*

$$\mathbb{E}_{\mathrm{obs}}\big((Y-P)^t Y^m R(Y)\big) \ll c^{t+m+d} P^{t+m} \|R\|_1 \frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}},$$

pour une constante $c > 0$ absolue.

Démonstration. En posant $R = \sum_{i=0}^{d} \alpha_i X^i$, on a

$$\mathbb{E}_{\mathrm{obs}}\big((Y-P)^t Y^m R(Y)\big) = \sum_{i=0}^{d} \alpha_i \mathbb{E}_{\mathrm{obs}}\big((Y-P)^t Y^{m+i}\big)$$

puisque $t + m + i \leqslant t + m + d \leqslant P^-(q)$, on sait par le corollaire 36 qu'il existe une constante absolue $C \geqslant 1$ telle qu'on a uniformément

$$\begin{aligned} &\ll \sum_{i=0}^{d} |\alpha_i| C^{t+m+i} P^{t+m+i} \frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}} \\ &\ll C^{t+m+d} P^{t+m} \left(\sum_{i=0}^{d} |\alpha_i|\right) \frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}}. \end{aligned}$$ □

Nous pouvons à présent établir le théorème A annoncé.

Démonstration du théorème A. Si $h \leqslant k$, on a *a fortiori* $hP \leqslant k$ et donc

$$M_k(q;h) = \sum_{n=1}^{q} \left(\sum_{n=1}^{h} [n+i \perp q] - hP\right)^k \leqslant q h^k \leqslant q k^k \leqslant q k^{k/2} (k + hP)^{k/2}.$$

On peut donc se placer dans le cas où $k \leqslant h \leqslant P^-(q)$. On replace l'expression du corollaire 13 dans le résultat du lemme 33 et donc

$$m_k(h, X, Y) = \sum_{t} \binom{k}{t} \big(h(Y-X)\big)^t \sum_{j} \big(hY(1-Y)\big)^j R_{k-t,j}(Y),$$

où le polynôme $R_{k-t,j}$ est de degré inférieur à $k - t - 2j$ (proposition 12). Puisque $h \leqslant P^-(q)$, on a par le lemme 34

$$M_k(q;h) = q\mathbb{E}_{\mathrm{obs}}\big(m_k(h,P,Y)\big)$$
$$= q\sum_t\sum_j \binom{k}{t} h^{j+t}\mathbb{E}_{\mathrm{obs}}\big((Y-P)^t Y^j (1-Y)^j R_{k-t,j}(Y)\big).$$

Puisque le degré en Y est inférieur à $t+2j+(k-t-2j)=k\leqslant P^-(q)$, on peut appliquer le corollaire 37 à notre situation. On note que similairement à la majoration (22)

$$\big\|(1-Y)^j R_{k-t,j}(Y)\big\|_1 \leqslant 2^j \|R_{k-t,j}\|_1 \leqslant 2^j\left(\frac{4}{e}(k-t-j)\right)^{k-t-j} \leqslant 2^k k^{k-t-j},$$

ainsi on a pour une constante absolue $C>0$

$$\mathbb{E}_{\mathrm{obs}}\big((Y-P)^t Y^j (1-Y)^j R_{k-t,j}(Y)\big) \ll C^k P^{t+j}\frac{t^{t/2}}{(P^-(q)\log P^-(q))^{t/2}}k^{k-t-j}.$$

On rappelle que les variables de sommation j et t vérifient $t+2j\leqslant k$. À présent, le moment peut être majoré

$$M_k(q;h) \ll C^k q\sum_{t+2j\leqslant k}\frac{(hP)^{t+j}}{(P^-(q)\log P^-(q))^{t/2}}t^{t/2}k^{k-t-j}$$

or $P^-(q)\log P^-(q)\geqslant P^-(q)\geqslant h\geqslant hP$ et $t\leqslant k$, donc

$$\ll C^k q\sum_{t+2j\leqslant k}(hP)^{t/2+j}k^{k-t/2-j}$$

et à $u\in[\![0,k]\!]$ fixé, il y a au plus $k\ll(1+1/C)^k$ couples (j,t) qui vérifient $t+2j=u$

$$\ll (C+1)^k q k^k\sum_{u\leqslant k}\left(\frac{hP}{k}\right)^{u/2}$$
$$\ll (C+1)^k q k^k\left(1+\sqrt{\frac{hP}{k}}\right)^k$$
$$\ll c^k q k^{k/2}(k+hP)^{k/2},$$

pour $c=\sqrt{2}(C+1)$. □

La démonstration du corollaire B se fait de façon tout à fait similaire au paragraphe 7 de [18], en décomposant $q=q_\sharp q_\flat$ selon la taille des facteurs premiers. Avant d'en donner une démonstration, il nous faut prouver que le moment dans le cas « arithmétique » n'est pas démesurément grand.

Lemme 38. *On a uniformément en $k \geqslant 0$, h et q vérifiant $P^+(q) \leqslant h$*

$$M_k(q;h) \ll q\left(ch\frac{\varphi(q)}{q}\right)^k,$$

où $c > 0$ est une constante absolue.

Démonstration. Par une application directe du crible de Brun (cf. [10, Theorem 2.2]), on a uniformément pour tout n, h et q vérifiant $P^+(q) \leqslant h$, la majoration

$$\sum_{i=1}^{h}[n+i \perp q] \leqslant ch\prod_{p|q}\left(1-\frac{1}{p}\right) \leqslant chP,$$

où $c \geqslant 1$ est une contante absolue. En replaçant cette inégalité dans (2), on obtient la majoration voulue. □

Démonstration du corollaire B. Par la multiplicativité en chacune des variables de la fonction $[\cdot \perp \cdot]$, on a pour tout n la relation $[n \perp q] = [n \perp q_\sharp][n \perp q_\flat]$. En notant $n_\sharp$ (resp. $n_\flat$) un entier congru à n modulo $q_\sharp$ (resp. $q_\flat$), on a pour tout entier i

$$[n+i \perp q] = [n_\sharp + i \perp q_\sharp][n_\flat + i \perp q_\flat].$$

On a donc $P = P_\sharp P_\flat$, mais également

$$\begin{aligned}\sum_{i=0}^{h-1}[n+i \perp q] - hP &= \sum_{i=0}^{h-1}[n_\sharp + i \perp q_\sharp][n_\flat + i \perp q_\flat] - hP \\ &= \left(P_\flat\sum_{i=0}^{h-1}[n_\sharp + i \perp q_\sharp] - hP\right) + \left(\sum_{i=0}^{h-1}[n_\sharp + i \perp q_\sharp][n_\flat + i \perp q_\flat] - P_\flat\sum_{i=0}^{h-1}[n_\sharp + i \perp q_\sharp]\right).\end{aligned}$$

Pour m entier, on pose $I_m := \{i \in [\![0, h-1]\!];\ (m+i, q_\sharp) = 1\}$ et on note h_m le cardinal de I_m. On obtient alors

$$\sum_{i=0}^{h-1}[n_\sharp + i \perp q_\sharp] - hP = P_\flat\left(\sum_{i=0}^{h-1}[n_\sharp + i \perp q_\sharp] - hP_\sharp\right) + \left(\sum_{i \in I_{n_\sharp}}[n_\flat + i \perp q_\flat] - h_{n_\sharp}P_\flat\right).$$

Puisque $(x+y)^k \leqslant 2^k(x^k + y^k)$ lorsque k est pair, on a en passant à la puissance k, et en sommant sur n

$$M_k(q;h) \leqslant 2^k\left(q_\flat {P_\flat}^k M_k(q_\sharp;h) + \sum_{n_\sharp=1}^{q_\sharp} M_k(q_\flat; I_{n_\sharp})\right). \tag{28}$$

Il s'agit à présent de majorer la somme $\sum_{m=1}^{q_\sharp} M_k(q_\flat; I_m)$. On a $h \leqslant P^-(q_\flat)$ et donc $I_m \subset [\![0, h-1]\!] \subset [\![0, P^-(q_\flat)-1]\!]$ pour tout m. On peut donc appliquer le lemme 34 :

$$\sum_{m=1}^{q_\sharp} M_k(q_\flat; I_m) = \sum_{m=1}^{q_\sharp} M_k(q_\flat; h_m), \tag{29}$$

où $h_m \leqslant h \leqslant P^-(q_\flat)$. On utilise à présent le théorème A, pour obtenir qu'il existe une constante absolue c telle que

$$M_k(q_\flat; h_m) \ll q_\flat (ck)^{k/2} (k + h_m P_\flat)^{k/2} \ll q_\flat (2ck)^{k/2} \big(k^{k/2} + (h_m P_\flat)^{k/2}\big)$$

uniformément pour m et pour $h \leqslant P^-(q_\flat)$. Le premier terme de la somme fournit $q(2ck)^{k/2}k^{k/2}$ dans (29). Pour le second terme, on a par l'inégalité $|x+y|^\kappa \leqslant 2^\kappa(|x|^\kappa + |y|^\kappa)$ pour $\kappa > 0$, puis par inégalité de Cauchy–Schwarz (k est pair)

$$\begin{aligned}\sum_{m=1}^{q_\sharp} {h_m}^{k/2} &\leqslant 2^{k/2} \left(\sum_{m=1}^{q_\sharp} |h_m - h P_\sharp|^{k/2} + q_\sharp (h P_\sharp)^{k/2} \right) \\ &\leqslant 2^{k/2} \big({q_\sharp}^{1/2} \big(M_k(q_\sharp; h) \big)^{1/2} + q_\sharp (h P_\sharp)^{k/2} \big).\end{aligned}$$

En utilisant la majoration du lemme 38 pour majorer $M_k(q_\sharp; h)$, on voit qu'il existe une constante c' telle que

$$\sum_{m=1}^{q_\sharp} (h_m P_\flat)^{k/2} \ll {c'}^{k/2} q_\sharp (hP)^{k/2}.$$

On regroupe ces deux termes pour obtenir une majoration de (29)

$$\begin{aligned}\sum_{m=1}^{q_\sharp} M_k(q_\flat; I_m) &\ll q(2ck)^{k/2}k^{k/2} + {c'}^{k/2} q (hP)^{k/2} \\ &\leqslant q(Ck)^{k/2}(k + hP)^{k/2},\end{aligned}$$

avec $C = \max(2c, c')$, ce qui fournit l'inégalité proposée en la replaçant dans la majoration (28). □

Remerciements

Je tiens à remercier Michel Balazard et Laurent Habsieger pour les différentes discussions tenues sur ce sujet, desquelles ce travail a largement profité.

Références

[1] S. Chowla, On the least prime in an arithmetical progression, J. Indian Math. Soc. (N.S.) 1 (1934) 1–3.
[2] L. Comtet, Analyse combinatoire, tome 2, Coll. Le Mathématicien, vol. 5, Presses Universitaires de France, Paris, 1970.
[3] H. Cramér, Some theorems concerning prime numbers, Ark. Mat. Astr. Fys. 15 (5) (1921) 1–32.
[4] H. Cramér, On the order of magnitude of the difference between consecutive prime numbers, Acta Arith. 2 (1936) 23–46.
[5] P. Erdős, The difference of consecutive primes, Duke Math. J. 6 (1940) 438–441.
[6] P. Erdős, On the integers relatively prime to n and on a number-theoretic function considered by Jacobsthal, Math. Scand. 10 (1962) 163–170.
[7] P. Erdős, Problems and results in number theory, in: H. Halberstam, C. Hooley (Eds.), Recent Progress in Analytic Number Theory, vol. 1, Symp. Durham, 1979, Academic Press, London, New York, 1981, pp. 1–13.
[8] R.L. Graham, D.E. Knuth, O. Patashnik, Concrete Mathematics, second ed., Addison–Wesley Publishing Company, Reading, MA, 1994. Trad. française : A. Denise, Mathématiques concrètes, International Thomson Publishing, Paris, 1998.
[9] A. Granville, K. Soundararajan, An uncertainty principle for arithmetic sequences, Ann. of Math. 165 (2007) 593–635.
[10] H. Halberstam, H.-E. Richert, Sieve Methods, London Math. Soc. Monogr., vol. 4, Academic Press, London, New York, 1974.
[11] M. Hausman, H.N. Shapiro, On the mean square distribution of primitive roots of unity, Comm. Pure Appl. Math. 26 (4) (1973) 539–547.
[12] C. Hooley, On the difference of consecutive numbers prime to n, Acta Arith. 8 (1963) 343–347.
[13] H. Iwaniec, On the problem of Jacobsthal, Demonstratio Math. 11 (1978) 225–231.
[14] E. Jacobsthal, Über Sequenzen ganzer Zahlen, von denen keine zu n teilerfremd ist, I–III, Norske Vid. Selsk. Forh., Trondheim 33 (1961) 117–124, 125–131, 132–139; IV–V, Norske Vid. Selsk. Forh., Trondheim 34 (1962) 1–7, 110–115.
[15] H.-J. Kanold, Über Primzahlen in arithmetischen Folgen, I, Math. Ann. 156 (1964) 393–395; II, Math. Ann. 157 (1965) 358–362.
[16] H.L. Montgomery, Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis, CBMS Reg. Conf. Ser. Math., vol. 84, Amer. Math. Soc., Providence, RI, 1994.
[17] H.L. Montgomery, K. Soundararajan, Primes in short intervals, Comm. Math. Phys. 252 (1–3) (2004) 589–617.
[18] H.L. Montgomery, R.C. Vaughan, On the distribution of reduced residues, Ann. of Math. 123 (1986) 311–333.
[19] R.A. Rankin, The difference between consecutive prime numbers, I, J. London Math. Soc. 13 (1938) 242–247; V, Proc. Edinb. Math. Soc. (2) 13 (1962/1963) 331–332.
[20] V. Romanovsky, Note on the moments ot a binomial $(p+q)^n$ about its mean, Biometrika 15 (1923) 410.
[21] R.C. Vaughan, On the order of magnitude of Jacobsthal's function, Proc. Edinb. Math. Soc. (2) 20 (1976/1977) 329–331.