ACTA ARITHMETICA
178.1 (2017)

Sur les occurrences des mots dans les nombres premiers

par

Gautier Hanna (Nancy)

1. Introduction. Mauduit et Rivat [14] ont démontré une conjecture vieille de 40 ans due à Gelfond [7]. Elle stipulait en particulier que la moitié des nombres premiers avaient un nombre de 1 pair dans l'écriture en base 2. Cette question est reliée à l'étude des fonctions définies sur les chiffres en base q (ici la fonction $s_2(n)$, la somme des chiffres en base 2) et des sous-suites de suites automatiques [2] (la suite de Thue–Morse). La recherche d'un théorème des nombres premiers pour des fonctions définies sur les chiffres, voire l'étude des sous-suites de suites automatiques, est un problème ardu. La méthode développée dans [14] a permis ces dernières années des progrès significatifs dans ce domaine [5, 6, 13, 15].

Parallèlement, Kalai [11] s'est intéressé au problème suivant. Étant donné S un sous-ensemble de $\{1,\dots,n\}$, $\mu(n)$ la fonction de Möbius, et Ω_n l'espace de tous les $x=(x_1,\dots,x_n)$ de $\{0,1\}^n$, a-t-on pour tout $A>0$,

$$\hat{\mu}(S) := \frac{1}{2^n}\sum_{x\in\Omega_n}\mu(x_1+2x_2+\cdots+2^{n-1}x_n)(-1)^{\sum_{i\in S}x_i} = O(n^{-A}) \ ?$$

Bourgain [3] a répondu positivement, montrant notamment un principe d'aléa de Möbius pour toutes les fonctions linéaires sur $\mathbb{Z}/2\mathbb{Z}$. Suite à ce travail, Kalai [12] a demandé d'étudier le cas des polynômes de plus haut degré, notamment le cas de la suite de Rudin–Shapiro [18, 19]. Étudier la suite de Rudin–Shapiro est naturel puisqu'il s'agit du cas le plus simple de polynôme de degré plus grand que 1. Si

$$n=\sum_{i\geq 0}\epsilon_i(n)q^i \tag{1}$$

2010 *Mathematics Subject Classification*: Primary 11A63; Secondary 11B85, 11N05, 11L20.
Key words and phrases: prime numbers, sums of exponential, digits.
Received 24 October 2015; revised 14 August 2016.
Published online 5 January 2017.

DOI: 10.4064/aa8337-8-2016

est l'écriture de n en base q, en utilisant (1) avec $q = 2$, on pose

$$a(n) = \sum_{i\geq 0} \epsilon_i(n)\epsilon_{i+1}(n)\,;$$

alors $(a(n) \bmod 2)_{n\geq 0}$ désigne la suite de Rudin–Shapiro. Tao (voir [12]) a esquissé une preuve d'un principe d'aléa de Möbius dans ce cas particulier, et Mauduit et Rivat [15] ont donné une formule asymptotique avec un terme d'erreur explicite et ont également obtenu un théorème des nombres premiers dans ce cas. Ils ont formulé deux conditions suffisantes sur une suite $(f(n))_{n\in\mathbb{N}}$ de module 1 pour estimer de manière non triviale la somme $\sum_{n<N} \Lambda(n)f(n)$, où Λ désigne la fonction de von Mangoldt. Pour notre part, nous allons altérer légèrement une de ces conditions.

Notons $\mathbb{U}$ le cercle unité, $f^{(\lambda)}$ une troncation de la fonction f (nous donnerons la définition précise dans la partie 3) et $e(x) = \exp(2\mathrm{i}\pi x)$.

Définition 1.1 (Faible propriété de petite propagation). On dit qu'une application $f : \mathbb{N} \to \mathbb{U}$ a la *faible propriété de petite propagation* si, uniformément pour $(\lambda, \kappa, \rho) \in \mathbb{N}^3$ avec $\rho < \lambda$, le nombre d'entiers l satisfaisant $0 \leq l < q^\lambda$ tels qu'il existe $(k_1, k_2) \in \{0, \ldots, q^\kappa - 1\}^2$ avec

$$f(lq^\kappa + k_1 + k_2)\overline{f(lq^\kappa + k_1)} \neq f^{(\kappa+\rho)}(lq^\kappa + k_1 + k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa + k_1)} \tag{2}$$

est $O(q^{\lambda-\rho+\log\rho})$, la constante ne dépendant que de q et f.

Définition 1.2 (Propriété de Fourier). On dit qu'une application $f : \mathbb{N} \to \mathbb{U}$ a la *propriété de Fourier* s'il existe une fonction γ croissante avec $\lim_{\lambda\to\infty} \gamma(\lambda) = \infty$ et une constante absolue $c > 0$ telles que pour tous entiers positifs λ, κ avec $\kappa \leq c\lambda$ et tout réel t, on ait

$$\Big|\frac{1}{q^\lambda} \sum_{0\leq n<q^\lambda} f(q^\kappa n)e(-nt)\Big| \leq q^{-\gamma(\lambda)}.$$

Nous avons alors le

Théorème 1.3. *Soit f une application vérifiant les définitions* 1.1 *et* 1.2. *Alors f vérifie, uniformément en $\vartheta \in \mathbb{R}$,*

$$\begin{aligned}(3)\qquad &\Big|\sum_{n\leq x} \Lambda(n)f(n)e(\vartheta n)\Big| \\ &\ll c_1(q)(\log x)^{c_2(q)} x q^{-\gamma(2\lfloor(\log x)/(80\log q)\rfloor)/20+\log(\gamma(2\lfloor(\log x)/(80\log q)\rfloor)/20)}\end{aligned}$$

avec

$$\begin{aligned} c_1(q) &= \max(\tau(q)\log q, \log^{10} q)^{1/4}(\log q)^{2-2c_2(q)}, \\ c_2(q) &= 4 + \frac{\log q}{4} + \frac{1}{4}\max(\omega(q), 2). \end{aligned}$$

Ces énoncés diffèrent de [15] par une altération dans définition 1.1 de $O(q^{\lambda-\rho})$ en $O(q^{\lambda-\rho+\log\rho})$ et par l'altération des constantes $c_1(q)$ et $c_2(q)$.

Remarque 1.4. La démonstration du théorème 1.3 repose sur l'estimation de sommes de type I et de type II et en l'application du [14, lemme 1]. En particulier les techniques utilisées permettent d'avoir l'estimation (3) avec μ la fonction de Möbius à la place de Λ en utilisant [10, (13.40)].

Dans [15], Mauduit et Rivat utilisent leur théorème avec $f(n) = e(\alpha a(n))$ et $(a(n))_{n\in\mathbb{N}}$ une suite de Rudin–Shapiro généralisée ; ils traitent les deux cas suivants :

$$\beta_\delta(n) = \sum_{l\geq 0} \epsilon_l(n)\epsilon_{l+\delta}(n), \tag{4}$$

$$b_d(n) = \sum_{l\geq 0} \epsilon_l(n)\epsilon_{l+1}(n)\cdot\ldots\cdot\epsilon_{l+d}(n). \tag{5}$$

Notons que la suite $\beta_\delta(n)$ a été introduite par Allouche et Liardet [1]. Le théorème 1.3 implique que ces suites sont uniformément distribuées et ont un théorème des nombres premiers (pour les énoncés exacts, voir les corollaires 3.2–3.4).

Dans cet article nous généralisons les résultats de [15] à

$$a(n) = a(\lfloor n/q^{T_q(n)-\beta}\rfloor) + \sum_{0\leq l\leq T_q(n)-\beta} h(\epsilon_l(n), \epsilon_{l+1}(n), \ldots, \epsilon_{l+\beta-1}(n)),$$

où h est une fonction à β variables, β est un entier ≥ 2 et

$$T_q(n) = \lfloor \log n/\log q\rfloor$$

est la taille de n en base q. La forme de ces suites, que nous nommons *β-récursives*, généralise (4) et (5), mais également le cas des suites digitales, parfois nommées *bloc-additives*, qu'on peut trouver dans [4]. La recherche d'un principe d'aléa de Möbius pour les suites bloc-additives a été traitée par Müllner [16]. Du fait de leur forme, les suites β-récursives permettent de mieux répondre que les fonctions digitales à la question de Kalai (théorème 3.5).

Le lecteur trouvera dans la partie 2 une introduction aux suites β-récursives et aux différentes notations qui seront utilisées dans l'article. Dans la partie 3 nous développons plus précisément les conséquences du théorème principal (théorème 1.3). La condition de faible propagation obtenue et l'explication de l'altération de la condition initiale sont situées dans la partie 4. Comme nous altérons les définitions de [15], nous sommes obligés de reprendre partiellement cet article. C'est ce qui est fait dans la partie 6. Pour terminer l'étude des suites β-récursives, la condition de Fourier est vérifiée dans la partie 5. Pour ce faire, nous sommes amenés à contrôler la norme infinie d'une matrice reliée à la suite β-récursive. Nous donnons la formule exacte de la norme infinie de cette matrice (proposition 5.6) en exhibant un graphe. La partie 7 est dévolue à la collecte de résultats.

2. Notations et définitions. Soit q un entier supérieur ou égal à 2. On note $\mathcal{A}$ l'alphabet $\mathcal{A} := \{0, \dots, q-1\}$. On note Σ l'ensemble des mots sur $\mathcal{A}$, Σ^* l'ensemble des mots finis, Σ_k l'ensemble des mots de taille k, Σ_k^* l'ensemble des mots de taille au plus k, et ϵ le mot de taille 0. Ainsi $\Sigma_0 = \{\epsilon\}$, $\Sigma_1 = \{0, \dots, q-1\}$, $\Sigma_1^* = \{\epsilon, 0, \dots, q-1\}$, etc. Soient $\omega, \omega' \in \Sigma$. On note $\omega \cdot \omega'$ leur concaténation et $|\omega|$ la taille de ω (on omettra parfois le symbole $\cdot$, toutefois sans risque de confusion). Pour un entier $k \geq 0$, on note $\overline{\omega}^k$ le préfixe de ω de taille k, et $\underline{\omega}_k$ son suffixe de taille k. On a par convention $\overline{\omega}^0 = \underline{\omega}_0 = \epsilon$. Ainsi, pour tout entier k entre 0 et $|\omega|$, on a la décomposition $\omega = \overline{\omega}^{|\omega|-k} \cdot \underline{\omega}_k$. On note $\epsilon_i(\omega)$ la i-ième lettre de ω, lu de droite à gauche, donc $\omega = \epsilon_{|\omega|-1}(\omega) \cdot \ldots \cdot \epsilon_0(\omega)$.

On définit l'application $\varphi : \Sigma^* \to \mathbb{N}$ par

$$\varphi(\omega) = \sum_{i=0}^{|\omega|-1} \epsilon_i(\omega) q^i.$$

Pour $r \in \mathcal{A}$, on utilisera la notation $\hat{r}$ pour l'entier $\varphi(r)$. Pour un entier x compris entre 0 et $q-1$, on note $\dot{x} = \varphi^{-1}(x)$ la lettre correspondante. Par exemple, pour $\omega = 280163$, on a $|\omega| = 6$, $\overline{\omega}^2 = 28$, $\underline{\omega}_3 = 163$, et pour la base $q = 11$,

$$\varphi(\omega) = 2 * 11^5 + 8 * 11^4 + 0 * 11^3 + 1 * 11^2 + 6 * 11^1 + 3 * 11^0 = 439420.$$

Enfin, pour $\omega' \in \Sigma^*$, nous notons $\mathbb{1}_{\omega'} : \Sigma^* \to \{0, 1\}$ la fonction

$$\mathbb{1}_{\omega'}(\omega) = \begin{cases} 1 & \text{si } \omega = \omega', \\ 0 & \text{sinon.} \end{cases}$$

Nous introduisons maintenant l'objet central de l'étude de cet article.

DÉFINITION 2.1. Soient $(a(n))_{n\in\mathbb{N}}$ une suite à valeurs dans $\mathbb{Z}$ et β un entier supérieur ou égal à 2. On dit que $(a(n))_{n\in\mathbb{N}}$ est *β-récursive* s'il existe une application $g : \Sigma_\beta \to \mathbb{N}$ telle que pour tout $n \geq 1$ et pour tout ω dans Σ_β, on ait

$$a(q^\beta n + \varphi(\omega)) = a(q^{\beta-1} n + \varphi(\overline{\omega}^{|\omega|-1})) + g(\omega), \tag{6}$$

et telle que si $\overline{\omega}^1 \neq 0$,

$$a(\varphi(\omega)) = a(\varphi(\overline{\omega}^{|\omega|-1})) + g(\omega). \tag{7}$$

Nous dirons que g est la *fonction de propagation* de a.

Comme ω est un élément de Σ_β, si $\overline{\omega}^1 = 0$ il existe $\tilde{\omega}$ dans $\Sigma^*_{\beta-1}$ tel que

$$\varphi(\omega) = \varphi(\tilde{\omega}) = \sum_{i=0}^{\beta-2} \epsilon_i(\omega) q^i < q^{\beta-1}.$$

Ainsi la notion de β-récursivité n'impose de contrainte que pour les entiers au moins égaux à $q^{\beta-1}$.

Citons ici trois exemples de suites β-récursives :

(E1) *Suites de Rudin–Shapiro généralisées.* Les suites de type Rudin–Shapiro, constituées des généralisations proposées par Queffélec [17], Grant, Shallit et Stoll [8], ou encore Allouche et Liardet [1], sont β-récursives.

(E2) *Suites bloc-additives.* Les suites digitales, parfois nommées bloc-additives [2, 4], définies par

$$a(n) = \sum_{i \geq 0} g\big(\epsilon_{i+\beta-1}(n) \cdot \ldots \cdot \epsilon_i(n)\big)$$

avec $g(0 \cdot \ldots \cdot 0) = 0$ et satisfaisant (1), sont β-récursives.

(E3) *Suites bloc-additives finies.* On peut se passer de la condition $g(0 \cdot \ldots \cdot 0) = 0$ et prendre la suite

$$a(n) = \sum_{i=0}^{T_q(n)-r} g\big(\epsilon_{i+\beta-1}(n) \cdot \ldots \cdot \epsilon_i(n)\big),$$

ce qui est fondamental si on veut compter les blocs de chiffres en écriture finie (par exemple la suite bloc-additive qui compte le nombre de 01 vaudra 2 pour 101, ce qui est contraire à l'intuition). Cette suite est également β-récursive.

L'objet de la proposition suivante est de faire le lien entre la définition 2.1 et les trois exemples précités :

Proposition 2.2. *Soient $\beta \geq 2$ un entier et $(a(n))_{n\in\mathbb{N}}$ une suite β-récursive. Soit n un entier ; nous considérons sa décomposition en base q,*

$$n = \sum_{i=0}^{N} \epsilon_i(n) q^i = \varphi\big(\epsilon_N(n) \cdot \ldots \cdot \epsilon_1(n) \cdot \epsilon_0(n)\big),$$

où $N = T_q(n)$. Alors, si $n \geq q^{\beta-1}$, on a $N \geq \beta - 1$ et

$$a(n) = a\Big(\varphi\big(\epsilon_N(n) \cdot \epsilon_{N-1}(n) \cdot \ldots \cdot \epsilon_{N-\beta+2}(n)\big)\Big) + \sum_{l=0}^{N-\beta+1} g\big(\epsilon_{l+\beta-1}(n) \cdot \ldots \cdot \epsilon_{l+1}(n) \cdot \epsilon_l(n)\big).$$

Remarquons que $|\epsilon_N(n) \cdot \epsilon_{N-1}(n) \cdot \ldots \cdot \epsilon_{N-\beta+2}(n)| = \beta - 1$ et $\epsilon_N(n) \neq 0$.

Démonstration. Le cas $N = \beta - 1$ étant immédiat, nous pouvons désormais supposer $N > \beta - 1$. Nous allons montrer par récurrence sur r que pour tout entier r compris entre 0 et $N - \beta$,

$$\begin{aligned} a\Big(\sum_{i=0}^{N} \epsilon_i(n) q^i\Big) &= a\Big(q^{\beta-1} \sum_{i=\beta+r}^{N} \epsilon_i(n) q^{i-\beta-r} + \varphi\big(\epsilon_{\beta-1+r}(n) \cdot \ldots \cdot \epsilon_{r+1}(n)\big)\Big) \\ &\quad + \sum_{l=0}^{r} g\big(\epsilon_{l+\beta-1}(n) \cdot \ldots \cdot \epsilon_l(n)\big). \end{aligned} \tag{8}$$

Pour $r = 0$, par (6) on a

$$\begin{aligned} a\Big(\sum_{i=0}^{N} \epsilon_i(n) q^i\Big) &= a\Big(q^{\beta} \sum_{i=\beta}^{N} \epsilon_i(n) q^{i-\beta} + \varphi\big(\epsilon_{\beta-1}(n) \cdot \ldots \cdot \epsilon_1(n) \cdot \epsilon_0(n)\big)\Big) \\ &= a\Big(q^{\beta-1} \sum_{i=\beta}^{N} \epsilon_i(n) q^{i-\beta} + \varphi\big(\epsilon_{\beta-1}(n) \cdot \ldots \cdot \epsilon_1(n)\big)\Big) \\ &\quad + g\big(\epsilon_{\beta-1}(n) \cdot \ldots \cdot \epsilon_0(n)\big). \end{aligned}$$

Supposons l'hypothèse de récurrence (8) satisfaite pour un certain $r \leq N - \beta - 1$ et montrons (8) pour $r + 1$. Comme $\beta + r + 1 \leq N$,

$$\sum_{i=\beta+r+1}^{N} \epsilon_i(n) q^{i-\beta-r-1} \geq 1.$$

Alors, en utilisant (8) puis (6) pour $r > 0$ on obtient

$$\begin{aligned} a\Big(\sum_{i=0}^{N} \epsilon_i(n) q^i\Big) &= a\Big(q^{\beta-1} \sum_{i=\beta+r}^{N} \epsilon_i(n) q^{i-\beta-r} + \varphi\big(\epsilon_{\beta-1+r}(n) \cdot \ldots \cdot \epsilon_{r+1}(n)\big)\Big) \\ &\quad + \sum_{l=0}^{r} g\big(\epsilon_{l+\beta-1}(n) \cdot \ldots \cdot \epsilon_l(n)\big) \\ &= a\Big(q^{\beta-1} \sum_{i=\beta+r+1}^{N} \epsilon_i(n) q^{i-\beta-r-1} \\ &\qquad\qquad + \varphi\big(\epsilon_{\beta+r}(n) \cdot \epsilon_{\beta-1+r}(n) \cdot \ldots \cdot \epsilon_{r+2}(n)\big)\Big) \\ &\quad + \sum_{l=0}^{r+1} g\big(\epsilon_{l+\beta-1}(n) \cdot \ldots \cdot \epsilon_l(n)\big), \end{aligned}$$

ce qui conclut la récurrence.

En appliquant (8) à $r = N - \beta$, on obtient

$$\begin{aligned} a(n) &= a\big(q^{\beta-1}\epsilon_N(n) + \varphi\big(\epsilon_{N-1}(n)\cdot\ldots\cdot\epsilon_{N-\beta+1}(n)\big)\big) \\ &\quad + \sum_{l=0}^{N-\beta} g\big(\epsilon_{l+\beta-1}(n)\cdot\ldots\cdot\epsilon_l(n)\big) \\ &= a\big(\varphi\big(\epsilon_N(n)\cdot\epsilon_{N-1}(n)\cdot\ldots\cdot\epsilon_{N-\beta+1}(n)\big)\big) \\ &\quad + \sum_{l=0}^{N-\beta} g(\epsilon_{l+\beta-1}(n)\cdot\ldots\cdot\epsilon_l(n)), \end{aligned}$$

et on conclut par (7), parce que N désigne l'indice du dernier terme non nul dans la décomposition de n, ce qui veut dire $\epsilon_N(n) \neq 0$, et enfin

$$\epsilon_N(n)\cdot\epsilon_{N-1}(n)\cdot\ldots\cdot\epsilon_{N-\beta+1}(n) \in \Sigma_\beta. \ \blacksquare$$

Remarque 2.3. Avec l'écriture de la proposition précédente, il suffit pour avoir les exemples de (E1) de prendre la fonction g correspondante. Par exemple pour retrouver $a(n) = \sum_{i\ge 0}\epsilon_{i+\delta}(n)\epsilon_i(n) = \beta_\delta(n)$ (suite d'Allouche et Liardet), on pose

$$g(\omega) = \sum_{(i_1,\ldots,i_{\delta-1})\in\{0,\ldots,q-1\}^{\delta-1}} \widehat{\epsilon_\delta(\omega)}\mathbb{1}_{\widehat{\epsilon_{\delta-1}(\omega)}=i_{\delta-1}}\cdot\ldots\cdot\mathbb{1}_{\widehat{\epsilon_1(\omega)}=i_1}\widehat{\epsilon_0(\omega)}.$$

Quant à l'exemple (E2), il suffit de prendre

$$a(\varphi(\omega)) = \sum_{i=1}^{\beta-1} g(0^{\beta-i}\cdot\overline{\omega}^i) \tag{9}$$

si $\overline{\omega}^1 \neq 0$ et $a(\varphi(\omega)) = 0$ si $\overline{\omega}^1 = 0$.

3. Résultats principaux. Pour cette partie nous rappelons que $\tau(n)$ désigne le nombre de diviseurs de n, et $\omega(n)$ le nombre de facteurs premiers dans la décomposition de n (ainsi $\omega(2^2 * 3) = 2$). Les deux notations ω pour désigner un mot et la suite arithmétique $\omega(n)$ ne se recoupent pas dans l'article, et nous pouvons utiliser conjointement ces deux notations sans risque de confusion. De plus nous notons $\pi(x;a,m) := \#\{p\le x : p\equiv a \bmod m\}$.

Il nous est nécessaire par la suite de définir des fonctions tronquées et de travailler sur le cercle unité $\mathbb{U}$. En effet, notre article repose sur les résultats de [15] qui utilisent des sommes d'exponentielles, et où le principe de troncation est essentiel.

Définition 3.1. Soit $(a(n))_{n\in\mathbb{N}}$ une suite β-récursive, et soit λ un entier naturel. On définit $(a^{(\lambda)}(n))_{n\in\mathbb{N}}$, la *suite tronquée en* λ, par

$$a^{(\lambda)}(n) = a(n \bmod q^\lambda),$$

où $n \bmod q^\lambda$ désigne le reste de la division euclidienne de n par q^λ. Soit α un nombre réel. On définit les applications $f : \mathbb{N} \to \mathbb{U}$ et $f^{(\lambda)} : \mathbb{N} \to \mathbb{U}$ par

$$f(n) = e(\alpha a(n)) \quad \text{et} \quad f^{(\lambda)}(n) = e(\alpha a^{(\lambda)}(n)).$$

On dit qu'elles sont *associées* aux suites $(a(n))_{n\in\mathbb{N}}$ et $(a^{(\lambda)}(n))_{n\in\mathbb{N}}$.

Les définitions 1.1 et 1.2 ainsi que le théorème 1.3 prennent ici un sens rigoureux. Tout comme Mauduit et Rivat, nous déduisons de ce théorème trois corollaires, dont les preuves sont identiques à [15, Corollaries 1–3] :

Corollaire 3.2. *Soit $b : \mathbb{N} \to \mathbb{N}$ telle que pour tout α irrationnel, la fonction $f(n) = e(\alpha b(n))$ vérifie les définitions* 1.1 *et* 1.2. *Alors pour tout entier relatif a et tout entier naturel m premier avec a, la suite $(\alpha b(p))_{p\in\mathcal{P}(a,m)}$ est uniformément distribuée si et seulement si α est irrationnel.*

Corollaire 3.3. *Soient $b : \mathbb{N} \to \mathbb{N}$ et m et m' des entiers plus grands que* 1, *tels que pour tout $1 \le j' < m'$, la fonction $f(n) = e\big(\frac{j'}{m'}b(n)\big)$ vérifie les définitions* 1.1 *et* 1.2. *Alors, pour tous a et a' telles que a soit premier avec m, on a, lorsque x tend vers l'infini,*

$$\#\{p \le x : p \in \mathcal{P}(a,m),\, b(p) \equiv a' \bmod m'\} = (1 + o(1))\frac{\pi(x; a, m)}{m'}.$$

Corollaire 3.4. *Soient $b : \mathbb{N} \to \mathbb{N}$ et m et m' des entiers plus grands que* 1, *tels que pour tout $1 \le j' < m'$, la fonction $f(n) = e\big(\frac{j'}{m'}b(n)\big)$ vérifie les définitions* 1.1 *et* 1.2. *Alors, pour tous a et a' tels que a soit premier avec m, la suite $(\vartheta p)_{\{p\in\mathcal{P}(a,m)\,:\,b(p)\equiv a' \bmod m'\}}$ est uniformément distribuée si et seulement si ϑ est irrationnel.*

La particularité des suites β-récursives permet de plus d'avoir le résultat suivant, qui répond partiellement à la question de Kalai (nous généralisons directement en base q arbitraire) :

Théorème 3.5. *Soient $k \ge 1$ et*

$$a(n) = \sum_{i=0}^{T_q(n)-k} P(\epsilon_{i+k}(n), \dots, \epsilon_i(n)),$$

où $\epsilon_0(n), \dots, \epsilon_{T_q(n)}(n)$ sont les chiffres de n en base q, et $P \in \mathbb{Z}[X_k, \dots, X_0]$ est un polynôme de degré $d \le k + 1$ de la forme

$$P(X_k, \dots, X_0) = X_k X_0 P_1(X_k, \dots, X_0) + P_2(X_k, \dots, X_0),$$

avec $P_1, P_2 \in \mathbb{Z}[X_k, \dots, X_0]$ tels que l'équation $P_1(1, X_{k-1}, \dots, X_1, 1) = 1$ ait une solution $(X_{k-1}, \dots, X_1) \in \{0, 1, \dots, q-1\}^{k-1}$, et il n'y ait pas de monôme non nul divisible par $X_k X_0$ dans P_2. Alors

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\le N} \mu(n)(-1)^{a(n)} = 0. \tag{10}$$

On remarque que $P(X_k,\dots,X_0) = \prod_{i=0}^{k} X_i$ ainsi que $P(X_k,\dots,X_0) = \prod_{i=0}^{k}(1-X_i)$ vérifient les conditions du théorème, contrairement à $P(X_k,\dots,X_0) = X_k + X_0$. Plus généralement, notons que les méthodes développées dans le présent article ne permettent pas de traiter le cas où le polynôme est bilinéaire en X_0, X_k, ni le cas $a(n) = \epsilon_{T_q(n)-2}(n)\epsilon_2(n)$, où l'indice dépend également de n.

4. Petite propagation. Ici, et désormais, nous fixons q et β des entiers supérieurs ou égaux à 2. Le but de cette partie est de démontrer que les fonctions associées aux suites β-récursives vérifient la faible propriété de petite propagation. L'idée principale consiste à exploiter la proposition 2.2 pour dire que sous certaines conditions, il n'y a pas de différence entre $f(n)$ et $f^{(\lambda)}(n)$.

PROPOSITION 4.1. *Soient $(a(n))_{n\in\mathbb{N}}$ une suite β-récursive et f sa fonction associée. Alors f a la faible propriété de petite propagation.*

Nous allons tout d'abord démontrer un résultat intermédiaire :

PROPOSITION 4.2. *Soient $(a(n))_{n\in\mathbb{N}}$ une suite β-récursive et f sa fonction associée. Soient $(\lambda,\kappa,\rho) \in \mathbb{N}^3$ avec $\rho < \lambda$ et $\kappa \geq 1$. Soient $l > q^\rho$ et $k_1 < q^\kappa$ des entiers. Supposons qu'il existe un entier m tel que $0 \leq m < \rho - \beta + 2$ avec $\epsilon_{\kappa+m}(lq^\kappa + k_1) \neq q-1$ et que, si on note i le plus petit de ces m, il existe un entier j vérifiant $i + \beta - 2 < j < \rho$ et $\epsilon_{\kappa+j}(lq^\kappa + k_1) \neq 0$. Alors pour tout entier $k_2 < q^\kappa$,*

$$f(lq^\kappa + k_1 + k_2)\overline{f(lq^\kappa + k_1)} = f^{(\kappa+\rho)}(lq^\kappa + k_1 + k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa + k_1)}.$$

Démonstration. On note $n_1 = lq^\kappa + k_1$, $n_1' = n_1 \bmod q^{\kappa+\rho}$, $N_1 = T_q(n_1)$ et $N_1' = T_q(n_1')$, autrement dit N_1 (respectivement N_1') est l'emplacement du dernier chiffre non nul de n_1 (respectivement n_1').

On remarque que pour tout $0 \leq k < \kappa + \rho$, $\epsilon_k(n_1) = \epsilon_k(n_1')$. Comme il existe un entier j tel que $\beta - 2 < j < \rho$ et $\epsilon_{\kappa+j}(n_1) \neq 0$ (car $i \geq 0$), on obtient $N_1 \geq N_1' \geq \kappa + j > \kappa + \beta - 2 \geq \beta - 2$. Donc $N_1 \geq N_1' \geq \beta - 1$, et la proposition 2.2 s'applique, si bien que

$$a(n_1) = a\big(\varphi\big(\epsilon_{N_1}(n_1)\cdot\epsilon_{N_1-1}(n_1)\cdot\ldots\cdot\epsilon_{N_1-\beta+2}(n_1)\big)\big) + \sum_{l=0}^{N_1-\beta+1} g\big(\epsilon_{l+\beta-1}(n_1)\cdot\ldots\cdot\epsilon_{l+1}(n_1)\cdot\epsilon_l(n_1)\big), \tag{11}$$

et on a une formule similaire pour n_1' (avec N_1' au lieu de N_1). On pose à présent $n_2 = n_1 + k_2$, $n_2' = n_2 \bmod q^{\kappa+\rho}$, et $N_2 = T_q(n_2)$, $N_2' = T_q(n_2')$ leurs tailles respectives. Alors pour tout $k > i$,

$$\epsilon_{\kappa+k}(n_1) = \epsilon_{\kappa+k}(n_2). \tag{12}$$

En effet, il ne peut y avoir de différence dans les chiffres d'indices supérieurs ou égaux à k de n_1 et n_2 que dans le cas d'une propagation sur les chiffres de n_1. Or, si on veut une propagation jusqu'au chiffre $\kappa + r$, il faut que les chiffres compris entre κ et $\kappa + r - 1$ de n_1 soient tous égaux à $q - 1$. Ainsi, par hypothèse, une propagation éventuelle s'arrête à $\kappa + i$.

Comme $N_1, N_1' \geq \kappa+j > \kappa+i+\beta-2 \geq \kappa+i$, on a $N_1' = N_2'$ et $N_1 = N_2$, et finalement on a une formule similaire à (11) pour n_2 et n_2'.

En rassemblant ces différentes formes, on obtient

$$\begin{aligned}
(13)\qquad & f(n_1)\overline{f(n_2)f(n_1')}f(n_2') \\
&= e\Big(\alpha\Big(a\big(\varphi\big(\epsilon_{N_1}(n_1)\cdot\epsilon_{N_1-1}(n_1)\cdot\ldots\cdot\epsilon_{N_1-\beta+2}(n_1)\big)\big) \\
&\quad - a\big(\varphi\big(\epsilon_{N_1}(n_2)\cdot\epsilon_{N_1-1}(n_2)\cdot\ldots\cdot\epsilon_{N_1-\beta+2}(n_2)\big)\big) \\
&\quad - a\big(\varphi\big(\epsilon_{N_1'}(n_1')\cdot\epsilon_{N_1'-1}(n_1')\cdot\ldots\cdot\epsilon_{N_1'-\beta+2}(n_1')\big)\big) \\
&\quad + a\big(\varphi\big(\epsilon_{N_1'}(n_2')\cdot\epsilon_{N_1'-1}(n_2')\cdot\ldots\cdot\epsilon_{N_1'-\beta+2}(n_2')\big)\big) \\
&\quad + \sum_{l=N_1'-\beta+2}^{N_1-\beta+1}\big[g\big(\epsilon_{l+\beta-1}(n_1)\cdot\ldots\cdot\epsilon_{l+1}(n_1)\cdot\epsilon_l(n_1)\big) \\
&\qquad\qquad - g\big(\epsilon_{l+\beta-1}(n_2)\cdot\ldots\cdot\epsilon_{l+1}(n_2)\cdot\epsilon_l(n_2)\big)\big]\Big)\Big).
\end{aligned}$$

Cependant, comme $N_1' \geq \kappa + j > \kappa + i + \beta - 2$, on a $N_1' - \beta + 2 > \kappa + i$, et donc, pour tout $N_1' - \beta + 2 \leq l \leq N_1$, par (12), $\epsilon_l(n_1) = \epsilon_l(n_2)$; par conséquent, la somme en l à droite de (13) est nulle. En appliquant le même raisonnement pour les autres composants de celle-ci, on trouve

$$f(n_1)\overline{f(n_2)f(n_1')}f(n_2') = 1,$$

ce qui est bien le résultat voulu. ∎

Démonstration de la proposition 4.1. Pour commencer, on remarque que si $lq^\kappa + 2(q^\kappa - 1) < q^{\kappa+\rho}$, on a

$$f(lq^\kappa + k_1 + k_2)\overline{f(lq^\kappa + k_1)} = f^{(\kappa+\rho)}(lq^\kappa + k_1 + k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa + k_1)}.$$

En effet, comme $k_1, k_2 \in \{0, \ldots, q^\kappa - 1\}$, on a toujours $lq^\kappa + k_1 + k_2 < q^{\kappa+\rho}$ et donc $lq^\kappa + k_1 + k_2 = lq^\kappa + k_1 + k_2 \bmod q^{\kappa+\rho}$.

Soit maintenant $l \geq q^\rho$. La proposition 4.2 donne des conditions à vérifier pour que (2) ne soit pas réalisée. On peut donc écrire que l'ensemble

$$\begin{aligned}
&\{0 \leq l < q^\lambda : \exists 0 \leq k_1, k_2 < q^\kappa : \\
&\qquad f(lq^\kappa + k_1 + k_2)\overline{f(lq^\kappa + k_1)} \neq f^{(\kappa+\rho)}(lq^\kappa + k_1 + k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa + k_1)}\}
\end{aligned}$$

est inclus dans l'union $A \cup B \cup C$ avec

$$A := \{q^\rho \le l < q^\lambda : \exists 0 \le k_1 < q^\kappa : \forall 0 \le i < \rho-\beta+2,\ \epsilon_{\kappa+i}(lq^\kappa+k_1) = q-1\},$$
$$B := \{q^\rho \le l < q^\lambda : \exists 0 \le k_1 < q^\kappa : \exists 0 \le i < \rho-\beta+2 : \epsilon_{\kappa+i}(lq^\kappa+k_1) \ne q-1,$$
$$\forall m < i,\ \epsilon_{\kappa+m}(lq^\kappa+k_1) = q-1,\ \forall i+\beta-2 < j < \rho,\ \epsilon_{\kappa+j}(lq^\kappa+k_1) = 0\},$$
$$C := \{l : lq^\kappa+2(q^\kappa-1) \ge q^{\kappa+\rho},\ lq^\kappa \le q^{\kappa+\rho}\}.$$

Cependant $lq^\kappa \le q^{\kappa+\rho}$ implique $l \le q^\rho$, et $(q^\rho-2)q^\kappa + 2(q^\kappa-1) = q^{\kappa+\rho}-2 < q^{\kappa+\rho}$ implique $l \ge q^\rho - 1$. On en déduit que $C = \{q^\rho-1, q^\rho\}$.

Il nous reste donc à évaluer les cardinaux de A et B. Pour ce faire on remarque que, quel que soit $k_1 < q^\kappa$, $\epsilon_{\kappa+i}(lq^\kappa+k_1) = \epsilon_i(l)$, ce qui nous donne

$$\begin{aligned} A &= \{q^\rho \le l < q^\lambda : \\ &\qquad \exists 0 \le k_1 < q^\kappa : \forall 0 \le i < \rho-\beta+2,\ \epsilon_{\kappa+i}(lq^\kappa+k_1) = q-1\} \\ &= \{q^\rho \le l < q^\lambda : \forall 0 \le i < \rho-\beta+2,\ \epsilon_i(l) = q-1\}, \end{aligned}$$

donc

$$\#A = \frac{q^\lambda - q^\rho}{q^{\rho-\beta+2}} = q^{\beta-2}(q^{\lambda-\rho}-1).$$

On peut d'autre part écrire $B = \bigcup_{i=0}^{\rho-\beta+1} B_i$ avec

$$B_i = \{q^\rho \le l < q^\lambda : \exists 0 \le k_1 < q^\kappa : \epsilon_{\kappa+i}(lq^\kappa+k_1) \ne q-1,$$
$$\forall m < i,\ \epsilon_{\kappa+m}(lq^\kappa+k_1) = q-1,\ \forall i+\beta-2 < j < \rho,\ \epsilon_{\kappa+j}(lq^\kappa+k_1) = 0\}.$$

Mais comme tous les B_i sont en bijection entre eux, on a

$$\#B = (\rho-\beta+2)\#B_0.$$

Enfin,

$$\begin{aligned} \#B_0 &= \#\{q^\rho \le l < q^\lambda : \forall \beta-2 < j < \rho,\ \epsilon_j(l) = 0\} = \frac{q^\lambda - q^\rho}{q^{\rho-\beta+1}} \\ &= q^{\beta-1}(q^{\lambda-\rho}-1). \end{aligned}$$

En mettant les trois estimations ensemble, on trouve

$$\begin{aligned} &\#\big\{0 \le l < q^\lambda : \exists 0 \le k_1, k_2 < q^\kappa : \\ &\quad f(lq^\kappa+k_1+k_2)\overline{f(lq^\kappa+k_1)} \ne f^{(\kappa+\rho)}(lq^\kappa+k_1+k_2)\overline{f^{(\kappa+\rho)}(lq^\kappa+k_1)}\big\} \\ &\qquad \le q^{\beta-2}(q^{\lambda-\rho}-1) + (\rho-\beta+2)q^{\beta-1}(q^{\lambda-\rho}-1) + 2 \ll q^\beta(q^{\lambda-\rho+\log\rho}). \end{aligned}$$

Comme q^β est une constante ne dépendant que de q, la fonction est bien de faible petite propagation. ■

Remarque 4.3. Dans [15], Mauduit et Rivat regardent le cas particulier de la suite Rudin–Shapiro. Pour cette suite, la décomposition de la proposition 2.2 ci-dessus se fait automatiquement car

(A) $a(k) = 0$ pour tout $0 \le k < q$;
(B) $g(a \cdot b) \neq 0 \Leftrightarrow a = b = 1$.

Ainsi on peut écrire, en notant $N = T_q(n)$ et $N_\lambda = T_q(n \bmod q^\lambda)$,

$$\begin{aligned} a(n) - a^{(\lambda)}(n) &= a(\epsilon_N(n)) - a(\epsilon_{N_\lambda}(n)) + \sum_{i=N_\lambda}^{N-1} g(\epsilon_{i+1}(n) \cdot \epsilon_i(n)) \\ &= \sum_{i=\lambda}^{N-1} g(\epsilon_{i+1}(n) \cdot \epsilon_i(n)) \end{aligned}$$

car on sait qu'alors, pour tout $N_\lambda < i < \lambda$, $\epsilon_i(n) = 0$, et donc $g(\epsilon_{i+1}(n) \cdot \epsilon_i(n)) = 0$, en vertu de (B). Ceci permet alors de dire, en reprenant les notations de la démonstration de la proposition 4.2, que

$$\begin{aligned} \text{(14)} \quad & a(n_1) - a(n_2) - a(n'_1) + a(n'_2) \\ &= \sum_{i=\lambda}^{N-1} g(\epsilon_{i+1}(n_1) \cdot \epsilon_i(n_1)) - \sum_{i=\lambda}^{N-1} g(\epsilon_{i+1}(n_2) \cdot \epsilon_i(n_2)), \end{aligned}$$

et pour s'assurer de la nullité de (14), il suffit de s'assurer que $\epsilon_i(n_1) = \epsilon_i(n_2)$ dès que i dépasse λ. Si on suppose uniquement l'existence d'un chiffre d'indice $m < \lambda$, $\epsilon_m(n_1) \neq q - 1$, alors cette condition est vérifiée (car la propagation ne pourra se faire au delà du m, et on a effectivement $\lambda > m$).

Dans le cas général, ce raisonnement ne tient plus, et nous sommes obligés d'introduire une fenêtre de sécurité. Il s'agit de la condition sur j dans la proposition 4.2. Cette condition dans la preuve de la proposition 4.1 entraîne la création de l'ensemble B (l'ensemble A est la contraposée de la condition sur m, et l'ensemble C, lui, est un ensemble exceptionnel). Enfin, c'est cet ensemble B qui donne la majoration en $q^{\log \rho}$.

Il convient désormais de considérer que les fonctions associées aux suites β-récursives vérifient l'équation

$$\text{(15)} \qquad \left| \frac{1}{q^N} \sum_{n<q^N} f(n) e(nt) \right| \le q^{-\gamma(N)},$$

avec $\gamma(N) \to \infty$ de manière croissante. La partie suivante sert à introduire des notions qui permettent ce genre de contrôle.

5. Généalogie des fonctions. Nous commençons par une définition générale.

DÉFINITION 5.1. Soient $f : \mathbb{N} \to \mathbb{U}$ une application et ω un mot. On pose

$$\text{(16)} \qquad f_\omega(n) := f(q^{|\omega|} n + \varphi(\omega)).$$

Le lemme suivant permet de donner une formule de récurrence pour $f_\omega(n)$ si f est associée à une suite β-récursive.

Lemme 5.2. *On a*

$$f_\omega(qn+r) = \begin{cases} f_{\hat{r}\cdot\omega}(n) & \text{si } |\omega| < \beta - 1, \\ f_{\hat{r}\cdot\overline{\omega}^{|\omega|-1}}(n)e(\alpha g(\hat{r}\cdot\omega)) & \text{si } |\omega| = \beta - 1. \end{cases}$$

Démonstration. Par l'équation (16),

$$\begin{aligned} f_\omega(qn+r) &= f(q^{|\omega|}(qn+r)+\varphi(\omega)) = f(q^{|\omega|+1}n + q^{|\omega|}r + \varphi(\omega)) \\ &= f(q^{|\hat{r}\cdot\omega|}n + \varphi(\hat{r}\cdot\omega)). \end{aligned}$$

Rappelons que $f(n) = e(\alpha a(n))$; on conclut en utilisant (16) si $|\omega| < \beta - 1$ (donc $|\hat{r}\cdot\omega| < \beta$), et en utilisant (6) ainsi que (16) si $|\omega| = \beta - 1$ (donc $|\hat{r}\cdot\omega| = \beta$). ■

Définition 5.3. On munit Σ^* de l'ordre $\preceq$ suivant : Si $|\omega| \le |\omega'|$, alors $\omega \preceq \omega'$. Si les deux tailles sont égales, on compare les deux mots par leur ordre lexicographique lu de gauche à droite ([1]). Si ψ désigne la fonction qui énumère Σ^*, alors on définit $\phi : \mathbb{N} \to \Sigma^*$ par $\phi = \psi^{-1}$.

Le but de cette partie est d'exploiter la structure des suites β-récursives afin de montrer qu'elles satisfont la définition 1.2. Pour ce faire, nous exploitons le lemme 5.2.

Définition 5.4. On définit le vecteur V_n de taille $(q^\beta-1)/(q-1)$ par

$$V_n[l] := f_{\phi(l)}(n), \qquad 0 \le l \le (q^\beta - 1)/(q-1) - 1.$$

On dira que V_n est le *n-ième vecteur généalogique* de f.

Par le lemme 5.2, il existe une matrice $M_l(\alpha,t)$ telle que

$$V_{qn+l}e((qn+l)t) = M_l(\alpha,t)V_n e(qnt),$$

et donc si on note $S(N,t) := \sum_{n<q^N} V_n e(nt)$, on peut alors écrire

$$\begin{aligned} S(N,t) &= \sum_{0\le n<q^{N-1}} \sum_{0\le l<q} V_{qn+l}e((qn+l)t) \\ &= \sum_{0\le n<q^{N-1}} \sum_{0\le l<q} M_l(\alpha,t)V_n e(qnt) = M(\alpha,t)S(N-1,qt), \end{aligned}$$

où on a posé $M(\alpha,t) = \sum_{0\le l<q} M_l(\alpha,t)$. En itérant β fois et en écrivant

$$\widetilde{M}(\alpha,t) := \prod_{0\le k<\beta} M(\alpha, q^k t),$$

([1]) Ainsi $00 \preceq 01 \preceq 10 \preceq 000$.

on déduit $S(N,t)=\widetilde{M}(\alpha,t)S(N-\beta,q^\beta t)$. On dit que $\widetilde{M}(\alpha,t)$ est la *matrice généalogique* de f. En continuant le raisonnement ci-dessus, on obtient

$$\tag{17}\begin{aligned}\Big\|\sum_{0\le n<q^N} V_n e(nt)\Big\|_\infty &\\ &\le \prod_{i=0}^{\lfloor N/\beta\rfloor-1}\|\widetilde{M}(\alpha,q^{i\beta}t)\|_\infty \sum_{n<q^{N \bmod \beta}}\|V_n e(q^{\beta\lfloor N/\beta\rfloor}nt)\|_\infty\\ &\le \prod_{i=0}^{\lfloor N/\beta\rfloor-1}\|\widetilde{M}(\alpha,q^{i\beta}t)\|_\infty q^{N \bmod \beta},\end{aligned}$$

où $N \bmod \beta$ désigne le reste de la division euclidienne de N par β.

La proposition suivante est destinée à faire le lien entre la matrice généalogique et l'estimation (15).

Proposition 5.5. *Pour tout entier $\kappa\ge 0$, on a*

$$\Big|\frac{1}{q^N}\sum_{0\le n<q^N} f(q^\kappa n)e(-nt)\Big| \le \frac{1}{q^{\beta\lfloor N/\beta\rfloor}}\prod_{i=0}^{\lfloor N/\beta\rfloor-1}\|\widetilde{M}(\alpha,q^{i\beta}t)\|_\infty.$$

Démonstration. Pour tout entier $\kappa\ge\beta$,

$$\Big|\sum_{n<q^N} f(q^\kappa n)e(nt)\Big| = \Big|\sum_{n<q^N} f(q^{\beta-1}n)e(-nt)\Big|.$$

En effet, une récurrence montre que, pour tout $0\le r\le \kappa-\beta+1$, $a(q^\kappa n) = a(q^{\kappa-r}n)+rg(0\cdot\ldots\cdot 0)$ où $0\cdot\ldots\cdot 0$ est de taille β. Plus précisément, si $a(q^\kappa n)=a(q^{\kappa-r}n)+rg(0\cdot\ldots\cdot 0)$, alors

$$\begin{aligned}a(q^\kappa n) &= a(q^{\kappa-r}n+\varphi(0\cdot\ldots\cdot 0))+rg(0\cdot\ldots\cdot 0)\\ &= a(q^{\kappa-r-1}n+\varphi(0\cdot\ldots\cdot 0))+(r+1)g(0\cdot\ldots\cdot 0)\\ &= a(q^{\kappa-r-1}n)+(r+1)g(0\cdot\ldots\cdot 0).\end{aligned}$$

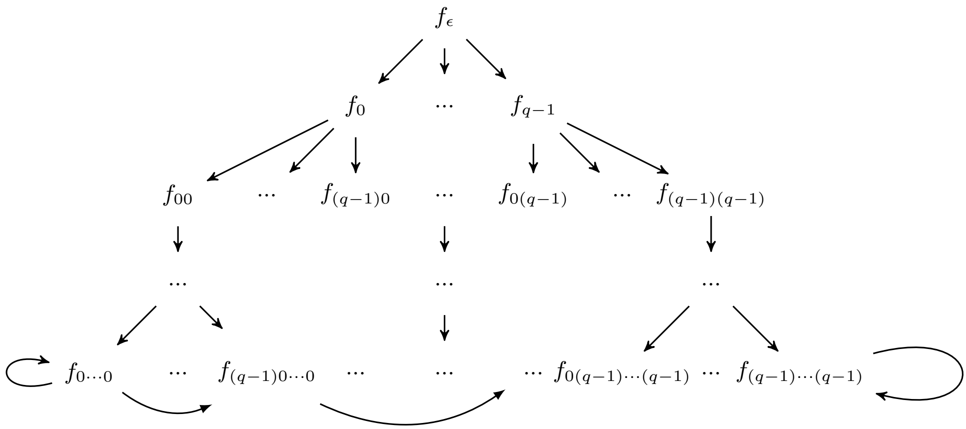
En particulier $a(q^\kappa n) = a(q^{\beta-1}n)+(\kappa-\beta+1)g(0\cdot\ldots\cdot 0)$. De plus, si $\kappa<\beta$, alors $f(q^\kappa n)$ est la $(q^\kappa-1)/(q-1)$-ième coordonnée de V_n. Nous concluons la preuve par l'équation (17) en observant que $N - N \bmod \beta = \beta\lfloor N/\beta\rfloor$. ∎

D'après la proposition 5.5, il est désormais important d'avoir un contrôle sur la norme infinie de la matrice $\widetilde{M}(\alpha,t)$. C'est l'objet du résultat qui suit.

Proposition 5.6.

$$\|\widetilde{M}(\alpha,t)\|_\infty = \sup_{\gamma\in\Sigma_{\beta-1}^*} \sum_{\omega\in\Sigma_{\beta-1}} \Big|\sum_{k\in\Sigma_1} e\Big(t(\hat{k}+q\varphi(\omega))+\alpha\Big(\sum_{m\leq|\gamma|} g(\underline{\omega}_{|\omega|-m}\cdot k\cdot\overline{\gamma}^m)\Big)\Big)\Big|. \tag{18}$$

Démonstration. Soit $\mathbb{G}$ le graphe suivant :



Alors $\mathbb{G}$ représente la manière dont peut évoluer en k étapes (k arbitraire) un mot γ donné selon le lemme 5.2. Décrivons-le.

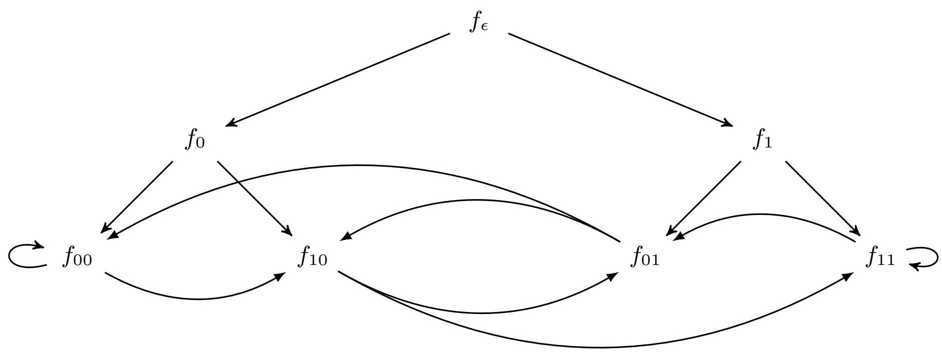
D'abord, $\mathbb{G}$ est un graphe descendant qui a β lignes. À chaque flèche correspond une altération de l'argument. Chaque élément donne q descendants, et donc le graphe a $\frac{q^\beta-1}{q-1}$ sommets. Si on se trouve sur la dernière ligne, avec un mot γ, un descendant γ' de γ sera donné par $\gamma' = \overline{\gamma'}^1\cdot\overline{\gamma}^{|\gamma|-1}$. On se promène sur le graphe en respectant les règles suivantes :

(i) On suit le sens des flèches.
(ii) Si à la k-ième étape, on passe d'un mot γ à un mot γ', avec la taille de γ strictement plus petite que $\beta-1$, on ajoute $q^{k-1}\overline{\gamma'}^1 t$ à l'argument.
(iii) Si à la k-ième étape, on passe d'un mot γ à un mot γ', avec la taille de γ égale à $\beta-1$, on ajoute $q^{k-1}\overline{\gamma'}^1 t+\alpha g(\overline{\gamma'}^1\cdot\gamma)$ à l'argument.

Désormais, nous appelons *encodage* d'un chemin la valeur $e(x)$, où x est l'argument total du chemin lorsque ce dernier est soumis aux règles ci-dessus.

Soit à présent $\mathrm{Enc}_k(\gamma,\omega)$ la somme des encodages concernant tous les chemins possibles en k étapes reliant γ à ω.

Exemple 5.7. Le graphe suivant correspond au cas $q = 2$, $\beta = 3$:



Dans ce graphe, il y a deux manières d'aller du mot ϵ au mot 00 en trois étapes : en faisant le chemin

$$\epsilon \underset{0}{\to} 0 \underset{0}{\to} 00 \underset{0}{\to} 00$$

et en faisant le chemin

$$\epsilon \underset{1}{\to} 1 \underset{0}{\to} 01 \underset{0}{\to} 00.$$

Ceci nous donne donc

$$\mathrm{Enc}_3(\epsilon, 00) = e(\alpha g(000)) + e(t + \alpha g(001)).$$

Continuons la démonstration de la proposition 5.6. Comme $M_l(\alpha, t)$ est la matrice de passage de V_n à V_{qn+l}, sommer sur l (c'est-à-dire regarder $M(\alpha, t)$) revient alors à déterminer tous les chemins à une étape possible. Et comme $\widetilde{M}(\alpha, t) = \prod_{i<\beta} M(\alpha, q^i t)$, on voit que $\widetilde{M}(\alpha, t)[i, j]$ correspond à la somme des encodages concernant tous les chemins possibles en β étapes reliant $\phi(i)$ à $\phi(j)$.

Nous avons donc

$$\|\widetilde{M}(\alpha, t)\|_\infty = \sup_i \sum_j |\mathrm{Enc}_\beta(\phi(i), \phi(j))|. \tag{19}$$

Cependant $\phi(i)$ et $\phi(j)$ parcourent l'ensemble des mots de taille au plus $\beta-1$. Ainsi (19) se transforme en

$$\|\widetilde{M}(\alpha, t)\|_\infty = \sup_{\gamma \in \Sigma^*_{\beta-1}} \sum_{\omega \in \Sigma^*_{\beta-1}} |\mathrm{Enc}_\beta(\gamma, \omega)|. \tag{20}$$

Cependant, par le lemme 5.2, pour tout γ, un descendant de γ à la β-ième génération est forcément de taille $\beta - 1$. En effet, la taille du mot va en croissant, strictement si la taille est strictement plus petite que $\beta - 1$, et devient constante dès que cette taille est atteinte. Or cette taille est atteinte, au pire, au bout de la $\beta-1$-ième étape. Donc (20) se transforme en

$$\|\widetilde{M}(\alpha,t)\|_\infty = \sup_{\gamma\in\Sigma^*_{\beta-1}} \sum_{\omega\in\Sigma_{\beta-1}} |\mathrm{Enc}_\beta(\gamma,\omega)|. \tag{21}$$

Il reste donc à comprendre $\mathrm{Enc}_\beta(\gamma,\omega)$.

Soit $\gamma\in\Sigma^*_{\beta-1}$. On pose $R\in\Sigma_{\beta-1-|\gamma|}$ et $S\in\Sigma_{|\gamma|+1}$. Les mots R et S interviendront dans le processus pour aller de γ à ω et seront déterminés ultérieurement. Arriver à un mot de taille $\beta-1$ se fait en $\beta-1-|\gamma|$ étapes, c'est-à-dire par l'adjonction de R. Nous avons donc, en suivant (ii), le chemin suivant :

$$\begin{aligned}\gamma \xrightarrow[\epsilon_0(R)t]{} \underline{R}_1\cdot\gamma \to \cdots \to \underline{R}_{i-1}\cdot\gamma \xrightarrow[\epsilon_{i-1}(R)q^{i-1}t]{} \underline{R}_i\cdot\gamma\to\cdots\\ \to \underline{R}_{|R|-1}\cdot\gamma \to \epsilon_{|R|-1}(R)q^{|R|-1}tR\cdot\gamma.\end{aligned} \tag{22}$$

Il nous reste $\beta-(\beta-1-|\gamma|)=|\gamma|+1$ étapes à parcourir. C'est-à-dire à concaténer S. Cependant comme on a atteint un mot de taille $\beta-1$, la fonction de propagation g s'adjoint à l'argument (il s'agit de la règle (iii)). Nous avons donc, en suivant (iii), la chaîne suivante (on ajoute à l'argument ce qui est en bas de la flèche) :

$$\begin{aligned}&R\cdot\gamma \xrightarrow[\epsilon_0(S)q^{|R|}t+\alpha g(\underline{S}_1\cdot\overline{R\cdot\gamma}^{|R\cdot\gamma|})]{} \underline{S}_1\cdot\overline{R\cdot\gamma}^{|R\cdot\gamma|-1}\to\cdots\\ &\underline{S}_i\cdot\overline{R\cdot\gamma}^{|R\cdot\gamma|-i} \xrightarrow[\epsilon_i(S)q^{i+|R|}t+\alpha g(\underline{S}_{i+1}\cdot\overline{R\cdot\gamma}^{|R\cdot\gamma|-i})]{} \underline{S}_{i+1}\cdot\overline{R\cdot\gamma}^{|R\cdot\gamma|-i-1}\to\cdots\\ &\underline{S}_{|\gamma|}\cdot\overline{R\cdot\gamma}^{|R\cdot\gamma|-|\gamma|} \xrightarrow[\epsilon_{|\gamma|}(S)q^{|\gamma|+|R|}t+\alpha g(\underline{S}_{|\gamma|+1}\cdot\overline{R\cdot\gamma}^{|R\cdot\gamma|-|\gamma|})]{}\\ &\qquad S\cdot\overline{R\cdot\gamma}^{|R\cdot\gamma|-|\gamma|-1} = S\cdot\overline{R}^{|R|-1}=\omega.\end{aligned} \tag{23}$$

De la dernière ligne on conclut que $S\cdot R=\omega\cdot k$, avec k un mot de taille 1. Il suit donc que

$$\begin{aligned}\underline{S}_{i+1}\cdot\overline{R\cdot\gamma}^{|R\cdot\gamma|-i} &= \underline{S}_{i+1}\cdot R\cdot\overline{\gamma}^{|\gamma|-i} = \underline{S\cdot R}_{|R|+i+1}\cdot\overline{\gamma}^{|\gamma|-i}\\ &= \underline{\omega\cdot k}_{\beta-(|\gamma|+1)+i+1}\cdot\overline{\gamma}^{|\gamma|-i} = \underline{\omega\cdot k}_{|\omega|+1-(|\gamma|+1)+i+1}\cdot\overline{\gamma}^{|\gamma|-i}\\ &= \underline{\omega}_{|\omega|-|\gamma|+i}\cdot k\cdot\overline{\gamma}^{|\gamma|-i}.\end{aligned}$$

Comme $0\le i\le|\gamma|$, on a

$$\begin{aligned}\{\underline{S}_{i+1}\cdot\overline{R\cdot\gamma}^{|R\cdot\gamma|-i} : 0\le i\le|\gamma|\} &= \{\underline{\omega}_{|\omega|-|\gamma|+i}\cdot k\cdot\overline{\gamma}^{|\gamma|-i} : 0\le i\le|\gamma|\}\\ &= \{\underline{\omega}_{|\omega|-i}\cdot k\cdot\overline{\gamma}^{i} : 0\le i\le|\gamma|\}.\end{aligned} \tag{24}$$

En réunissant (22) et (23), et en utilisant (24), nous déduisons qu'un encodage suivant le chemin $S \cdot R$ est égal à

$$\begin{aligned} e\Big(t\Big(\sum_{i=0}^{|R|-1} \epsilon_i(R)q^i + q^{|R|} \sum_{i=0}^{|S|-1} \epsilon_i(S)q^i\Big) + \alpha \sum_{m=0}^{|\gamma|} g(\underline{S}_{m+1} \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|-m})\Big) \\ = e\Big(t\varphi(S \cdot R) + \alpha \sum_{m=0}^{|\gamma|} g(\underline{S}_{m+1} \cdot \overline{R \cdot \gamma}^{|R\cdot\gamma|-m})\Big) \\ = e\Big(t\varphi(\omega \cdot k) + \alpha \sum_{m=0}^{|\gamma|} g(\underline{\omega}_{|\omega|-m} \cdot k \cdot \overline{\gamma}^m)\Big) \\ = e\Big(t(\hat{k} + q\varphi(\omega)) + \alpha \sum_{m\le|\gamma|} g(\underline{\omega}_{|\omega|-m} \cdot k \cdot \overline{\gamma}^m)\Big). \end{aligned}$$

En utilisant (21) et le fait que k prend toutes les valeurs de Σ_1, on obtient bien (18). ∎

Nous utilisons à présent cette estimation pour obtenir un contrôle uniforme en t de la norme infinie de $\widetilde{M}(\alpha, t)$.

Corollaire 5.8. *Soient $\omega_1, \omega_2 \in \Sigma_{\beta-1}$ ([2]) tels que $\underline{\omega_1}_{(\beta-2)} = \underline{\omega_2}_{(\beta-2)}$ mais $\omega_1 \neq \omega_2$ et $k_1, k_2 \in \Sigma_1$ tels que $k_1 \neq k_2$. Alors*

$$(25) \quad \|\widetilde{M}(\alpha, t)\|_\infty \le q^\beta - 8\Big(\sin \frac{\pi\|\alpha(g(\omega_1 \cdot k_1) - g(\omega_1 \cdot k_2) - g(\omega_2 \cdot k_1) + g(\omega_2 \cdot k_2))\|_{\mathbb{Z}}}{4}\Big)^2.$$

Tout d'abord, présentons un lemme trigonométrique, dont on peut retrouver la démonstration dans [15]. Nous rappelons que $\|x\|_{\mathbb{Z}}$ représente la distance du réel x au plus proche entier.

Lemme 5.9. *Soient x, x', ξ, α des nombres réels. Alors*

$$(26) \quad |e(x + \alpha') + e(x)| + |e(x' + \xi) + e(x')| \le 4 - 8\Big(\sin \frac{\pi\|\xi - \alpha'\|_{\mathbb{Z}}}{4}\Big)^2.$$

Démonstration du corollaire 5.8. En majorant trivialement (18), dans les cas où $\omega \neq \omega_1, \omega_2$ et $k \neq k_1, k_2$, nous obtenons

$$\|\widetilde{M}(\alpha, t)\|_\infty = \sup_{\gamma \in \Sigma^*_{\beta-1}} \Big(q^\beta - 4 + \sum_{i=1,2} \Big|\sum_{j=1,2} e\Big(t(\hat{k}_j + q\varphi(\omega_i)) + \alpha\Big(\sum_{m\le|\gamma|} g(\underline{\omega_i}_{|\omega_i|-m} \cdot k_j \cdot \overline{\gamma}^m)\Big)\Big)\Big|\Big).$$

([2]) Les mots ω_1 et ω_2 diffèrent de $\epsilon_{\beta-2}$, par exemple $\omega_1 = 10000000$ et $\omega_2 = 00000000$.

On pose alors

$$
(27)\quad \begin{aligned}
x &= t(\hat{k}_1+q\varphi(\omega_1))+\alpha \sum_{m\le|\gamma|} g(\underline{\omega_1}_{|\omega_1|-m}\cdot k_1\cdot\overline{\gamma}^m),\\
\alpha' &= t(\hat{k}_2-\hat{k}_1)+\alpha \sum_{m\le|\gamma|} \big(g(\underline{\omega_1}_{|\omega_1|-m}\cdot k_2\cdot\overline{\gamma}^m)-g(\underline{\omega_1}_{|\omega_1|-m}\cdot k_1\cdot\overline{\gamma}^m)\big),\\
x' &= t(\hat{k}_1+q\varphi(\omega_2))+\alpha \sum_{m\le|\gamma|} g(\underline{\omega_2}_{|\omega_2|-m}\cdot k_1\cdot\overline{\gamma}^m),\\
\xi &= t(\hat{k}_2-\hat{k}_1)+\alpha \sum_{m\le|\gamma|} \big(g(\underline{\omega_2}_{|\omega_2|-m}\cdot k_2\cdot\overline{\gamma}^m)-g(\underline{\omega_2}_{|\omega_2|-m}\cdot k_1\cdot\overline{\gamma}^m)\big),
\end{aligned}
$$

si bien que

$$
(28)\quad \|\widetilde{M}(\alpha,t)\|_\infty = \sup_{\gamma\in\Sigma^*_{\beta-1}} \big(q^\beta-4+|e(x)+e(\alpha'+x)|+|e(x')+e(x'+\xi)|\big).
$$

Or

$$
(29)\quad \begin{aligned}
\xi-\alpha' = \alpha\Big(&\sum_{m\le|\gamma|}\big(g(\underline{\omega_2}_{|\omega_2|-m}\cdot k_2\cdot\overline{\gamma}^m)-g(\underline{\omega_2}_{|\omega_2|-m}\cdot k_1\cdot\overline{\gamma}^m)\big)\\
&-\sum_{l\le|\gamma|}\big(g(\underline{\omega_1}_{|\omega_1|-l}\cdot k_2\cdot\overline{\gamma}^l)-g(\underline{\omega_1}_{|\omega_1|-l}\cdot k_1\cdot\overline{\gamma}^l)\big)\Big).
\end{aligned}
$$

Et comme $\underline{\omega_1}_{|\omega_1|-m}=\underline{\omega_2}_{|\omega_1|-m}$ pour tout $1\le m\le|\omega_1|$, le seul terme non nul dans (29) est $m=0$, d'où

$$
(30)\quad \xi-\alpha' = \alpha\big(g(\omega_1\cdot k_1)-g(\omega_1\cdot k_2)-g(\omega_2\cdot k_1)+g(\omega_2\cdot k_2)\big),
$$

ce qui conclut notre preuve. ∎

6. Démonstration du théorème 1.3. Nous suivons de près la preuve très technique du résultat de Mauduit et Rivat dans [15]. Nous ne présentons ici que les éléments modifiés. Nous conseillons donc au lecteur de suivre notre raisonnement en ayant [15] sous les yeux.

Classiquement, Mauduit et Rivat utilisent d'abord une identité de Vaughan pour ramener l'estimation de la somme impliquant la fonction de von Mangoldt à l'évaluation de sommes de type I ($S_{\mathrm{I}}(\vartheta)$) et de type II ($S_{\mathrm{II}}(\vartheta)$). Chacune de ces sommes est ensuite séparée en deux parties. Dans la première partie, on a remplacé la fonction basée sur les chiffres qui intervient par une version tronquée de cette fonction. La troncature permet d'obtenir des fonctions périodiques et d'utiliser l'analyse de Fourier pour évaluer ces premières sommes. Ces estimations ne sont pas altérées par nos modifications. Dans la seconde partie en revanche, on estime la contribution de l'erreur commise lors du remplacement des fonctions par leurs versions tronquées. Pour cette seconde partie, Mauduit et Rivat utilisent les propriétés de petite propagation des fonctions qu'ils considèrent. Nous avons introduit à la définition 1.1 une propriété alternative plus faible qui sera vérifiée par les fonctions que nous considérons. L'affaiblissement de cette propriété amènera des modifications dans les estimations de ces secondes sommes.

Pour cette partie, nous notons $y \sim q^k$ pour $q^{k-1} \leq y < q^k$.

6.1. Sommes de type I. Soient M et N des entiers, avec $1 \leq M \leq N$ et $M \leq (MN)^{1/3}$. Nous notons μ et ν les entiers tels que $T_q(M) + 1 = \mu$ et $T_q(N) + 1 = \nu$. Soit f une application vérifiant les définitions 1.1 et 1.2. Soit $\vartheta \in \mathbb{R}$ et $I(M,N) \subset [0, MN]$ un intervalle. Nous cherchons à estimer

$$S_I(\vartheta) := \sum_{M/q \leq m < M} \Big| \sum_{n:\, mn \in I(M,N)} f(mn) e(\vartheta mn) \Big|.$$

Comme expliqué précédemment, la somme $S_I(\theta)$ est séparée en deux parties, nommées $S'_{\mathrm{I},1}(\vartheta')$ et $S'_{\mathrm{I},2}(\vartheta')$ (voir [15, équations (30), (31) et (35)]). Dans la première somme, la fonction f est remplacée par sa fonction tronquée, la seconde somme prend en compte l'erreur engendrée par cette substitution. L'estimation de la première somme reste inchangée et on a donc comme Mauduit et Rivat

$$\begin{aligned} S_{\mathrm{I}}(\theta) &\ll q^{\mu+\nu} (\log q^{\mu+\nu}) \big(S'_{\mathrm{I},1}(\theta') + S'_{\mathrm{I},2}(\theta') \big) \\ &\ll q^{\mu+\nu} (\log q^{\mu+\nu}) \big(\mu (\log q)^{3/2} q^{\rho_1/2 - \gamma((\mu+\nu)/3)} + S'_{\mathrm{I},2}(\theta') \big), \end{aligned} \tag{31}$$

où ρ_1 est un entier vérifiant $1 \leq \rho_1 \leq \mu + \nu - \kappa$ avec κ un entier tel que $1 \leq \kappa \leq (\mu+\nu)/3$, paramètres que l'on optimisera ultérieurement.

Pour estimer $S'_{\mathrm{I},2}(\vartheta')$, on a comme Mauduit et Rivat

$$S'_{\mathrm{I},2}(\vartheta') \ll \sum_{1 \leq d \leq M} \frac{1}{d} \bigg(\frac{\log q}{q^{\mu+\nu}} \sum_{\omega \in \mathcal{W}_{\kappa_d}} 2^2 \bigg)^{1/2}, \tag{32}$$

où κ_d est choisi de sorte que $M^2/d^2 \sim q^{\kappa_d}$, $\mathcal{W}_\kappa = \{u + vq^\kappa : (u,v) \in \widetilde{\mathcal{W}}_\kappa\}$ et $\widetilde{\mathcal{W}}_\kappa$ désigne l'ensemble des paires d'entiers $(u,v) \in \{0, \dots, q^\kappa - 1\} \times \{0, \dots, q^{\mu+\nu-\kappa} - 1\}$ pour lesquelles

$$f(u + vq^\kappa) \overline{f(vq^\kappa)} \neq f^{(\kappa+\rho_1)}(u + vq^\kappa) \overline{f^{(\kappa+\rho_1)}(vq^\kappa)}.$$

Il n'est pas étonnnant de voir apparaître ici une somme sur $\mathcal{W}_\kappa$ puisque cette partie de la somme mesure l'erreur commise en remplaçant une fonction par sa troncature. C'est dans l'estimation du cardinal de $\widetilde{\mathcal{W}}_\kappa$ qu'un changement apparaît. En utilisant la définition 1.1, nous obtenons

$$\operatorname{card} \widetilde{\mathcal{W}}_\kappa \ll q^{\mu+\nu-\rho_1+\log \rho_1}, \tag{33}$$

alors que Mauduit et Rivat avaient $\operatorname{card} \widetilde{\mathcal{W}}_\kappa \ll q^{\mu+\nu-\rho_1}$.

Finalement en combinant (31)–(33) avec le choix $\rho_1 = \gamma((\mu+\nu)/3)$, nous obtenons

$$S_{\mathrm{I}}(\vartheta) \ll (\log q)^{5/2}(\mu+\nu)^2 q^{\mu+\nu-\gamma((\mu+\nu)/3)/2+\log(\gamma((\mu+\nu)/3))/2}, \tag{34}$$

ce qui, en utilisant le fait que $\gamma(\lambda) \le \lambda/2$ [15, équation (26)], donne

$$S_I(\vartheta) \ll (\log q)^{5/2}(\mu+\nu)^{2+\log q} q^{\mu+\nu-\gamma((\mu+\nu)/3)/2}.$$

6.2. Sommes de type II. Nous reprenons les notations introduites pour les sommes de type I ; nous supposons de plus

$$\tfrac{1}{4}(\mu+\nu) \le \mu \le \nu \le \tfrac{3}{4}(\mu+\nu).$$

Nous introduisons $a_m \in \mathbb{C}$ et $b_n \in \mathbb{C}$ avec $|a_m|, |b_n| \le 1$. Les sommes de type II sont définies par

$$S_{\mathrm{II}}(\vartheta) := \sum_{M/q \le m < M} \sum_{N/q \le n < N} a_m b_n f(mn) e(\vartheta mn).$$

Dès le début de l'estimation de cette somme dans [15], une première troncation est introduite. On est alors amené à majorer le nombre de paires $(m,n) \in \{q^{\mu-1}, \dots, q^{\mu}-1\} \times \{q^{\nu-1}, \dots, q^{\nu}-1\}$ telles qu'il existe $k < q^{\mu+\rho}$ avec $f(mn+k)\overline{f(mn)} \neq f^{(\mu+2\rho)}(mn+k)\overline{f^{(\mu+2\rho)}(mn)}$ où $\rho \le \mu/7$ est un paramètre que l'on choisira ultérieurement. Avec la faible propriété de petite propagation, nous déduisons que ce nombre est un $O((\log q) q^{\mu+\nu-\rho+\log\rho})$ au lieu de $O(q^{\mu+\nu-\rho})$ dans [15, Lemme 8]. Ceci conduit à la majoration

$$|S_{\mathrm{II}}(\vartheta)|^4 \ll q^{4(\mu+\nu)-2\rho+2\log\rho} + q^{3(\mu+\nu-\rho)} \sum_{1 \le r < q^{\rho}} \sum_{1 \le s < q^{2\rho}} |S_2'(r,s)|, \tag{35}$$

où $S_2'(r,s)$ est une somme faisant intervenir la fonction doublement tronquée $f^{(\mu_1,\mu_2)}(n) := f^{(\mu_2)}(n)\overline{f^{(\mu_1)}(n)}$ avec $\mu_1 = \mu - 2\rho$ et $\mu_2 = \mu + 2\rho$.

Dans la somme $S_2'(r,s)$, Mauduit et Rivat remplacent la fonction $f^{(\mu_1,\mu_2)}(n)$ par la quantité $f^{(\mu_1,\mu_2)}(r_{\mu_0,\mu_2}(n))$, où $\mu_0 = \mu - 2\rho - 2\rho'$ avec $0 \le \rho' \le \rho$ et $r_{\mu_0,\mu_2}(n)$ est l'entier u_1 dans l'écriture unique

$$n = u_2 q^{\mu_2} + u_1 q^{\mu_0} + u_0, \qquad 0 \le u_1 < q^{\mu_2-\mu_0},\ u_2 \ge 0,\ 0 \le u_0 < q^{\mu_0}.$$

L'erreur engendrée par cette substitution est contrôlée par le cardinal de l'ensemble des paires (m,n) avec $M/q < m \le M$ et $N/q < n \le N$ (où $M \sim q^{\mu}$ et $N \sim q^{\nu}$) pour lesquelles

$$f^{(\mu_1,\mu_2)}(mn + q^{\mu_1} sn + q^{\mu_1} sr) \neq f^{(\mu_1,\mu_2)}(q^{\mu_0} r_{\mu_0,\mu_2}(mn + q^{\mu_1} sn + q^{\mu_1} sr))\,;$$

cet ensemble est noté $\mathcal{E}_{\mu_0,\mu_1,\mu_2}(r,s)$.

L'estimation de ce cardinal fait appel à la propriété de petite propagation, et en utilisant notre propriété plus faible on obtient

$$\operatorname{card} \mathcal{E}_{\mu_0,\mu_1,\mu_2}(r,s) \ll \max(\tau(q), \log q)(\mu+\nu)^{\omega(q)} q^{\mu+\nu-2\rho'+\log\mu_1}, \tag{36}$$

ce qui implique

$$(37)\qquad |S_{\mathrm{II}}(\vartheta)|^4 \ll q^{4(\mu+\nu)-2\rho+2\log\rho} + \max(\tau(q),\log q)(\mu+\nu)^{\omega(q)} q^{4(\mu+\nu)-2\rho'+\log(\mu-2\rho)} + q^{3(\mu+\nu-\rho)} \sum_{1\le r<q^\rho} \sum_{1\le s<q^{2\rho}} |S_3(r,s)|,$$

où $S_3(r,s)$ est une somme dans laquelle la fonction $f^{(\mu_1,\mu_2)}(r_{\mu_0,\mu_2}(n))$ intervient.

De manière à introduire des transformées de Fourier de $f^{(\mu_1,\mu_2)}$, Mauduit et Rivat identifient la décomposition en base q avec un sous-ensemble de l'intervalle $[0,1)$ translaté sur l'ensemble des entiers :

$$r_{\mu_0,\mu_2}(n) = u \;\Leftrightarrow\; \frac{n}{q^{\mu_2}} \in \left[\frac{u}{q^{\mu_2-\mu_1}}, \frac{u+1}{q^{\mu_2-\mu_1}}\right) + \mathbb{Z}.$$

Ils introduisent alors des fonctions indicatrices d'intervalles qu'ils contrôlent à l'aide des polynômes de Vaaler. Ils trouvent une nouvelle décomposition de $S_3(r,s)$ constituée du terme principal des polynômes, qu'ils nomment $S_4(r,s)$, et des termes d'erreurs qui sont contrôlés par les méthodes usuelles et ne sont pas affectés par notre modification. Ainsi, nous pouvons écrire

$$(38)\qquad S_3(r,s) = S_4(r,s) + O\big(\max(\log q^{\mu-2(\rho+\rho')}, \tau(q^{\mu-2(\rho+\rho')}))q^{\mu+\nu-2\rho}\big).$$

Le fait d'avoir introduit les polynômes de Vaaler permet de travailler sur les transformées de Fourier de $g(n) = f^{(\mu_1,\mu_2)}(q^{\mu_0}n)$, si bien que $S_4(r,s)$ s'écrit

$$S_4(r,s) = q^{2(\mu_2-\mu_0)} \sum_{|h_0|,|h_1|\le H} a_{h_0}(q^{\mu_0-\mu_2},H)a_{h_1}(q^{\mu_0-\mu_2},H) \times \sum_{0\le h_2,h_3<q^{\mu_2-\mu_0}} e\bigg(\frac{h_3sr}{q^{\mu_2-\mu_1}}\bigg)\hat{g}(h_0-h_2)\overline{\hat{g}(h_3-h_1)\hat{g}(-h_2)}\hat{g}(h_3) \times \sum_{m,n} e\bigg(\frac{(h_0+h_1)mn + h_1mr + (h_2+h_3)q^{\mu_1}sn}{q^{\mu_2}}\bigg),$$

où $a_0(\alpha,H) = \alpha$, $|a_h(\alpha,H)| \le \min(\alpha, 1/(\pi|h|))$, selon le lemme de Vaaler (voir [15, lemme 1]). Dans la somme $\sum_{1\le s<q^{2\rho}} |S_4(r,s)|$, seule l'estimation des termes diagonaux ($h_0+h_1=0$) pour les petites valeurs de $|h_1|$ (avec $|h_1| \le q^{2\rho}$) sera affectée par nos changements. Pour les autres quantités, l'estimation $\sum_{0\le h<q^{\mu_2-\mu_0}} |\hat{g}(h)|^2 = 1$ suffit. Ainsi, comme dans [15], on se

ramène à une estimation de

$$S_8(r) = q^{2(\mu_2-\mu_0)} \sum_{|h_1|\le q^{2\rho}} |a_{h_1}(q^{\mu_0-\mu_2}, H)|^2 \min\left(q^{\mu}, \frac{q^{\mu_2}}{r|h_1|}\right) \times \sum_{0\le h'<q^{\mu_2-\mu_0}} |\hat{g}(h'-h_1)\hat{g}(h')|^2. \tag{39}$$

Le lemme 11 de [15] permet ensuite à Mauduit et Rivat de majorer la somme des coefficients de Fourier en moyenne. Son analogue dans notre cas est l'estimation suivante :

Lemme 6.1. *Soient μ et ρ des entiers tels que $\mu \le (2+4c/3)\rho$, où c est la constante introduite dans la définition 1.2. Alors, uniformément pour λ entiers compris entre $(\mu_2-\mu_0)/3$ et $4(\mu_2-\mu_0)/5$ et t réels, on a*

$$\sum_{0\le k<q^{\mu_2-\mu_0-\lambda}} |\hat{g}(k+t)|^2 \ll (\gamma(\lambda)-\mu_1+\mu_0)\, q^{(\mu_1-\mu_0-\gamma(\lambda))/2}(\log q^{\mu_2-\mu_1})^2.$$

Ce lemme permet de dire que

$$\sum_{|h_1|\le q^{2\rho}} \sum_{0\le h'<q^{\mu_2-\mu_0}} |\hat{g}(h'-h_1)\hat{g}(h')|^2 \ll (\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0)q^{-(\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0)/2},$$

ce qui conduit à

$$\frac{1}{q^{2\rho}} \sum_{1\le r<q^{2\rho}} S_8(r) \ll (\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0)q^{\mu-(\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0)/2} + q^{\mu-\rho}\log q^{\rho},$$

puis à

$$\begin{aligned}\frac{1}{q^{3\rho}} \sum_{1\le r<q^{\rho}} \sum_{1\le s<q^{2\rho}} |S_4(r,s)| &\ll (\log q)^3(\mu+\nu)^3 q^{\mu+\nu+3(\mu_2-\mu_0)+2\rho}(q^{-\nu}+q^{-\mu_2}) + q^{\mu+\nu+\mu_1-\mu_0}\\ &\times \big((\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0)q^{-(\gamma(\mu_2-\mu_0-2\rho)-\mu_1+\mu_0)/2} + q^{-\rho}\log q^{\rho}\big)\\ &\times (\tau(q^{\mu_2-\mu_1}) + q^{\mu_2-\mu_1-\nu}\log q^{\mu_2-\mu_1}).\end{aligned} \tag{40}$$

Démonstration du lemme 6.1. On a par hypothèse $\mu_1-\mu_0 \le \lambda \le \mu_2-\mu_0$, donc, en séparant la somme définissant $\hat{g}(t)$ selon les restes de la division euclidienne par q^λ, on obtient

$$\hat{g}(t) = \frac{1}{q^{\mu_2-\mu_0-\lambda}} \sum_{0\le v<q^{\mu_2-\mu_0-\lambda}} f(vq^{\mu_0+\lambda}) e\Big(-\frac{vt}{q^{\mu_2-\mu_0-\lambda}}\Big)$$
$$\times \frac{1}{q^\lambda} \sum_{0\le u<q^\lambda} f(uq^{\mu_0}+vq^{\mu_0+\lambda})\overline{f(vq^{\mu_0+\lambda})f^{(\mu_1)}(uq^{\mu_0})} e\Big(-\frac{ut}{q^{\mu_2-\mu_0}}\Big).$$

Dans la ligne du bas, Mauduit et Rivat remplacent f par la fonction tronquée $f^{(\mu_0+\lambda+\rho_3)}$ associée, où ρ_3 est un paramètre qui sera optimisé. À nouveau, le traitement de la partie correspondant à la fonction tronquée est inchangé. Dans le traitement de l'erreur en revanche, on est amené à majorer le cardinal de l'ensemble $\mathcal{W}_\lambda$ des entiers $w = u + vq^\lambda$ tels que

$$f(uq^{\mu_0}+vq^{\mu_0+\lambda})\overline{f(vq^{\mu_0+\lambda})} \ne f^{(\mu_0+\lambda+\rho_3)}(uq^{\mu_0}+vq^{\mu_0+\lambda})\overline{f^{(\mu_0+\lambda+\rho_3)}(vq^{\mu_0+\lambda})}.$$

La faible propriété de petite propagation (2) donne alors

$$|\mathcal{W}_\lambda| \ll q^{\mu_2-\mu_0-\rho_3+\log\rho_3}$$

et permet de démontrer le lemme. ∎

Nous n'avons plus qu'à réunir les équations (37), (38) et (40) et à utiliser $\mu_2 = \mu + 2\rho$, $\mu_1 = \mu - 2\rho$ et $\mu_0 = \mu_1 - 2\rho'$ pour obtenir :

$$(41)\qquad |S_{\mathrm{II}}(\vartheta)|^4$$
$$\ll \max(\log q^{\mu-2(\rho+\rho')}, \tau(q^{\mu-2(\rho+\rho')}))q^{4(\mu+\nu)-2\rho+2\log\rho}$$
$$+ \max(\tau(q),\log q)(\mu+\nu)^{\omega(q)}q^{4(\mu+\nu)-2\rho'+\log(\mu-2\rho)}$$
$$+ q^{3(\mu+\nu)}(\log q)^3(\mu+\nu)^3 q^{\mu+\nu+3(2(\rho+\rho'))+2\rho}(q^{-\nu}+q^{-\mu_2})$$
$$+ q^{3\mu+3\nu}\big[q^{\mu+\nu+2\rho'}\big(\gamma((2\rho+2\rho')-2\rho')q^{-(\gamma(2\rho+2\rho')-2\rho')/2} + q^{-\rho}\log q^\rho\big)$$
$$\times\,(\tau(q^{4\rho}) + q^{4\rho-\nu}\log q^{4\rho})\big].$$

En utilisant $\gamma(x) \le x/2$ [15, (26)] et $\nu \ge 6\rho$, on obtient

$$(41) \ll q^{4(\mu+\nu)+3/2(\mu_1-\mu_0)-\gamma(2\rho)}(\log q^\rho)\tau(q)(\mu_2-\mu_1)^{\omega(q)}.$$

Notre estimation de $|S_{\mathrm{II}}|^4$ devient de la même forme que celle trouvée dans [15] ; on peut alors déduire, en faisant les mêmes choix que là-dedans,

$$(42)\qquad |S_{\mathrm{II}}(\vartheta)|^4 \ll \max(\tau(q)\log q, (\log q)^3)$$
$$\times (\mu+\nu)^{2+\log q+\max(\omega(q),2)}q^{4\mu+4\nu-\gamma(2\lfloor\mu/15\rfloor)}.$$

En rappelant que $q^{\mu+\nu-1} \le x < q^{\mu+\nu}$, et en utilisant [14, lemme 1] avec les estimations (34) et (42), nous obtenons

$$\Big|\sum_{x/q<n\le x} \Lambda(n)f(n)e(\vartheta n)\Big| \ll (\log x)^2(S_{\mathrm{I}}+S_{\mathrm{II}})\,;$$

or par l'estimation (34),

$$S_{\mathrm{I}}(\vartheta) \ll (\log q)^{5/2}(\mu+\nu)^{2+\log q} q^{\mu+\nu-\gamma((\mu+\nu)/3)/2},$$

et par l'estimation (42),

$$\begin{aligned}|S_{\mathrm{II}}(\vartheta)| \ll\ & \max\bigl(\tau(q)\log q, (\log q)^3\bigr)^{1/4} \\ & \times (\mu+\nu)^{1/2+(\log q)/4+\max(\omega(q),2)/4} q^{\mu+\nu-\gamma(2\lfloor \mu/15\rfloor)/20}.\end{aligned}$$

Nous pouvons conclure la preuve de ce théorème comme le font Mauduit et Rivat.

7. Applications. Dans cette partie nous appliquons les résultats des parties 4 et 5 pour obtenir une large classe de fonctions qui vérifient un théorème des nombres premiers.

Nous avons vu que si une fonction vérifiait la faible propriété de petite propagation et la propriété de Fourier (15), alors elle vérifiait la majoration (3). De plus, nous avons vu dans la partie 4 que les fonctions associées aux suites β-récursives vérifiaient la faible propriété de petite propagation (proposition 4.1). Enfin, nous avons vu dans la partie 5 que, pour une fonction associée à une suite β-récursive, vérifier la propriété de Fourier (15) revenait à trouver α réel, ω_1, ω_2 de taille $\beta-1$ de même suffixe, et k_1 et k_2 de telle sorte que

$$\alpha\bigl(g(\omega_1\cdot k_1) - g(\omega_1\cdot k_2) - g(\omega_2\cdot k_1) + g(\omega_2\cdot k_2)\bigr) \notin \mathbb{Z}. \tag{43}$$

Notons

$$K = K(g,\omega_1,\omega_2,k_1,k_2) = g(\omega_1\cdot k_1) - g(\omega_1\cdot k_2) - g(\omega_2\cdot k_1) + g(\omega_2\cdot k_2).$$

Nous allons ici donner des exemples de suites β-récursives, et montrer que pour certains $k_1, k_2, \omega_1, \omega_2$ leurs fonctions de propagation vérifient (43) si et seulement si α n'est pas un entier. Il y a deux grandes classes de fonctions, que nous traitons séparément :

7.1. Nombre d'occurrences

Proposition 7.1. *Soit $k \geq 2$, et soit $B \subset \Sigma_k$ tel qu'il existe $\omega \in B$ de sorte que*

$$\exists l_1 : l_1 \cdot \underline{\omega}_{(k-1)} \notin B, \tag{44}$$

$$\exists l_2 : \overline{\omega}^{(k-1)} \cdot l_2 \notin B, \tag{45}$$

$$l_1 \cdot \epsilon_{k-2}(\omega)\cdot \ldots \cdot \epsilon_1(\omega)\cdot l_2 \notin B. \tag{46}$$

Soit $(a(n))_{n\in\mathbb{N}}$ une suite k-récursive de fonction de propagation $g = \sum_{\chi\in B} \mathbb{1}_\chi$. Alors $K = 1$ et $(a_n)_{n\in\mathbb{N}}$ vérifie un théorème des nombres premiers.

Démonstration. En choisissant $\omega_1 = \overline{\omega}^{(k-1)}$, $\omega_2 = l_1 \cdot \epsilon_{k-2}(\omega) \cdot \ldots \cdot \epsilon_1(\omega)$, $k_1 = \epsilon_0(\omega)$, $k_2 = l_2$, on a $\omega_1 \cdot k_1 = \omega$ et donc

$$\begin{aligned} K = g(\omega) - g(\overline{\omega}^{(k-1)} \cdot l_2) - g(l_1 \cdot \underline{\omega}_{(k-1)}) \\ + g(l_1 \cdot \epsilon_{k-2}(\omega) \ldots \cdot \epsilon_1(\omega) \cdot l_2) = 1. \ \blacksquare \end{aligned}$$

De ce résultat *a priori* tautologique, on tire de nombreuses conséquences. Le fait que K soit égal à 1 implique que (43) est équivalente à α non entier, ou encore que les suites β-récursives ayant une fonction de propagation correspondant aux conditions de la proposition 7.1 vérifient la propriété de Fourier (15) si et seulement si α n'est pas un entier.

Or ce type de fonction recouvre de nombreux cas classiques. Par exemple :

(I) Si on prend $B = \{\omega\}$, alors il est clair qu'il existe $\omega \in B$ vérifiant (44)–(46), et si on pose $a(k) = 0$ pour tout $k < q^{|\omega|}$, on trouve les suites qui comptent le nombre d'occurrences d'un mot quelconque de taille supérieure ou égale à 2.

(II) Soit $k \geq 1$. Si on prend $B = \{a \cdot \gamma \cdot b : \gamma \in \Sigma_k\}$, on trouve alors que $g = \mathbb{1}_{a \cdot z \cdot b}$, et donc le nombre d'occurrences des mots de la forme aZb où Z est un mot arbitraire. En particulier $q = 2$, $a = 1$, $b = 1$ donne la suite introduite par Allouche et Liardet [1]. On peut l'améliorer de sorte à assigner des lettres fixes entre les deux extremités en posant $B = \{a_0 \cdot \gamma_0 \cdot a_1 \cdot \ldots \cdot \gamma_k \cdot a_{k+1} : \gamma_i \in \Sigma_{\zeta(i)}\ \forall 0 \leq i \leq k\}$, où ζ est une fonction de $\mathbb{N}$ dans $\mathbb{N}$ arbitraire.

(III) Si on suppose qu'on n'est pas dans le cas $q = \beta = 2$, on peut prendre $B = \bigcup_{a \in \Sigma_1} \{a \cdot \ldots \cdot a\}$ pour compter le nombre d'occurrences des mots de même taille et ayant une seule lettre, comme 000, 111 et 222 pour $q = 3$ et $k = 3$.

Notre condition (43) permet de traiter de nombreux cas classiques. En revanche la suite $(a(n))_{n \in \mathbb{N}}$ qui compte le nombre de mots 00 et 11 dans l'écriture de n en base 2 n'entre pas dans ce cadre. En effet, sous ces conditions, la fonction de propagation $g(a \cdot b)$ vaut 1 si et seulement si $a = b = 0$ ou $a = b = 1$ et alors quels que soient ω_1, ω_2 de taille 1 et k_1, k_2 de taille 1, on a

$$\begin{aligned} |K| &= |g(\omega_1 \cdot k_1) - g(\omega_2 \cdot k_1) - g(\omega_1 \cdot k_2) + g(\omega_2 \cdot k_2)| \\ &= |g(00) - g(01) - g(10) + g(11)| = 2 \equiv 0 \bmod 2, \end{aligned}$$

et $\alpha = 1/2$ est également une valeur proscrite.

7.2. Polynômes sur les chiffres. Dans cette sous-partie, à travers la démonstration du théorème 3.5 nous résolvons partiellement la question posée par Kalai [12].

Démonstration du théorème 3.5. Soit $(x_{k-1},\ldots,x_1)\in\{0,1,\ldots,q-1\}^{k-1}$ tel que

$$P_1(1,x_{k-1},\ldots,x_1,1)=1.$$

On pose $g(\omega)=P(\epsilon_{i+k}(n),\ldots,\epsilon_i(n))$ et $\omega_1=1\cdot x_{k-1}\cdot x_{k-2}\cdot\ldots\cdot x_1$, $\omega_2=0\cdot x_{k-1}\cdot x_{k-2}\cdot\ldots\cdot x_1$, $k_1=1$ et $k_2=0$. Alors

$$\begin{aligned}K&=g(1\cdot x_{k-1}\cdot x_{k-2}\cdot\ldots\cdot x_1\cdot 1)-g(1\cdot x_{k-1}\cdot x_{k-2}\cdot\ldots\cdot x_1\cdot 0)\\&\quad-g(0\cdot x_{k-1}\cdot x_{k-2}\cdot\ldots\cdot x_1\cdot 1)+g(0\cdot x_{k-1}\cdot x_{k-2}\cdot\ldots\cdot x_1\cdot 0)\\&=P_1(1,x_{k-1},\ldots,x_1,1)=1,\end{aligned}$$

et donc (43) $\Leftrightarrow \alpha\notin\mathbb{Z}$. Par la remarque 1.4, le théorème 3.5 est démontré. ∎

Le fait qu'on ne puisse pas traiter le cas $P(X_1,X_0)=X_1+X_0$ vient du fait que dans ce cas, quels que soient x_0,x_0',x_1,x_1',

$$\begin{aligned}|K|&=|P(x_1,x_0)-P(x_1',x_0)-P(x_1,x_0')+P(x_1',x_0')|\\&=|x_1+x_0-x_1'-x_0-x_1-x_0'+x_1'+x_0'|=0,\end{aligned}$$

et cette remarque vaut pour tout polynôme $P(X_k,\ldots,X_0)$ bilinéaire en X_k et X_0.

Références

[1] J.-P. Allouche and P. Liardet, *Generalized Rudin–Shapiro sequences*, Acta Arith. 60 (1991), 1–27.

[2] J.-P. Allouche and J. Shallit, *Automatic Sequences. Theory, Applications, Generalizations*, Cambridge Univ. Press, Cambridge, 2004.

[3] J. Bourgain, *Möbius–Walsh correlation bounds and an estimate of Mauduit and Rivat*, J. Anal. Math. 119 (2013), 147–163.

[4] E. Cateland, *Suites digitales et suites k-régulières*, PhD thesis, Univ. Bordeaux, 1992.

[5] M. Drmota, C. Mauduit and J. Rivat, *The sum-of-digits function of polynomial sequences*, J. London Math. Soc. 84 (2011), 81–102.

[6] M. Drmota, C. Mauduit and J. Rivat, *The Thue–Morse sequence along squares is normal*, http://www.dmg.tuwien.ac.at/drmota/alongsquares.pdf (2015).

[7] A. O. Gelfond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. 13 (1967/1968), 259–265.

[8] E. Grant, J. Shallit and T. Stoll, *Bounds for the discrete correlation of infinite sequences on k symbols and generalized Rudin–Shapiro sequences*, Acta Arith. 140 (2009), 345–368.

[9] B. Green, *On (not) computing the Möbius function using bounded depth circuits*, Combin. Probab. Comput.

[10] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloq. Publ. 53, Amer. Math. Soc., Providence, RI, 2004.

[11] G. Kalai, *Walsh Fourier transform of the Möbius function*, http://mathoverflow.net/questions/57543/walsh-fourier-transform-of-the-mobius-function (2011).

[12] G. Kalai, *Möbius randomness of the Rudin–Shapiro sequence*, http://mathoverflow.net/questions/97261/mobius-randomness-of-the-rudin-shapiro-sequence (2012).

[13] B. Martin, C. Mauduit et J. Rivat, *Théorème des nombres premiers pour les fonctions digitales*, Acta Arith. 165 (2014), 11–45.

[14] C. Mauduit et J. Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Ann. of Math. (2) 171 (2010), 1591–1646.

[15] C. Mauduit and J. Rivat, *Prime numbers along Rudin–Shapiro sequences*, J. Eur. Math. Soc. 17 (2015), 2595–2642.

[16] C. Müllner, communication personnelle.

[17] M. Queffélec, *Une nouvelle propriété des suites de Rudin–Shapiro*, Ann. Inst. Fourier (Grenoble) 37 (1987), no. 2, 115–138.

[18] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. 10 (1959), 855–859.

[19] H. S. Shapiro, *Extremal problems for polynomials and power series*, PhD thesis, M.I.T., 1951.

[20] J. Vaaler, *Some extremal functions in Fourier analysis*, Bull. Amer. Math. Soc. 12 (1985), 183–216.

Gautier Hanna
Université de Lorraine et CNRS
Institut Élie Cartan de Lorraine, UMR 7502
F-54506 Vandœuvre-lès-Nancy, France
E-mail: gautier.hanna@univ-lorraine.fr