Uniform distribution and quasi-Monte Carlo methods

Linz, 16 october 2013

Distribution of Rudin-Shapiro sequences along prime numbers

Christian Mauduit

Institut de Mathématiques de Luminy CNRS-FRE 3529,

Université Aix-Marseille, France.

work in collaboration with *Joel RIVAT*

Introduction

The difficulty of the transition from the representation of an integer in a number system to its multiplicative representation (as a product of prime factors) is at the origine of many important open problems in mathematics and computer science.

Our talk concerns the study of independence between prime numbers and various "deterministic" functions, i. e. functions produced by a dynamical system of zero entropy or defined using a simple algorithm.

Representation of integers in base q

If q is an integer greater than or equal to 2, any positive integer n can be written in a unique way in base q in the form $n = \sum_{j=0}^{\ell} n_j q^j, \quad n_j \in \{0, \ldots, q-1\}, \quad n_\ell \geq 1$ and we denote by $rep_q(n) = n_\ell \ldots n_0 \in \{0, \ldots, q-1\}^*$ the representation of n in base q (for any finite alphabet A, we denote by A^* the set of finite words over A).

To any $E \subset \mathbb{N}$ we associate the language $L_q(E) = \{rep_q(n), n \in E\} \subset \{0, \ldots, q-1\}^*$.

Many questions concerning arithmetic sequences can then be expressed in the framework of the theory of formal languages, thus establishing a link between number theory, language theory and combinatorics on words.

Prime numbers and q-finite automata

If $E = \mathbb{P}$ is the set of primes, it is natural to ask whether there is a simple algorithm for deciding whether a given integer n does belong to E or not.

Minsky and Papert had shown in 1966 that $L_q(\mathbb{P})$ is never a rational language, i. e. the set of prime numbers is not recognizable by a q-finite automaton.

This fundamental result has been generalized by Hartmanis and Shank and Schützenberger in 1968, showing that no infinite subset of primes is recognizable by a finite automaton (or even by a pushdown automaton).

Mauduit showed in 1992 that the set of prime numbers can not be generated by a morphism (or substitution) on a finite alphabet and introduced in 2006 a notion of q-infinite automaton for which Cassaigne and Le Gonidec showed the non-recognizability of the set of primes.

This question has received a new light with the development by Agrawal, Kayal and Saxena in 2004 of a polynomial time algorithm to solve it.

Prime numbers in q-automatic sets

The search of prime numbers in a set recognizable by a q-finite automaton is a problem in general extremely difficult. Thus, the sets $\{2^n+1, n \in \mathbb{N}\}$ and $\{2^n-1, n \in \mathbb{N}\}$ are both recognizable by a 2-finite automaton and the associate problems correspond respectively to the research of Fermat and Mersenne primes.

When E is a set recognizable by an irreducible q-finite automaton (i. e. that the graph of the automaton is strongly connected), it follows from a remark due to Fouvry-Mauduit (1996) that the set E contains infinitely many almost prime numbers But the following problem remains open :

Problem 1. For any $E \subset \mathbb{N}$ recognizable by an irreducible q-finite automaton,
i) find an asymptotic estimate of the number of primes $p \equiv a(m)$ less than x belonging to the set E ;
ii) study the distribution modulo 1 of the sequence $(p\alpha)_{p\in E}$.

When the finite automaton is not irreducible, the situation becomes very difficult. The first problem to be studied in this direction is probably the following, that concerns the search of prime numbers with missing digits.

Problem 2. For any given $D \subset \{0, \ldots, q-1\}$, find an asymptotic estimate for $\mathrm{card}\{p \leq x,\ rep_q(p) \in D^*\}$.

Resolution of the Gelfond conjecture for prime numbers and generalizations

Let f the q-digital function defined by $f(n) = \sum_{j<q} \alpha_j |n|_j$, where $(\alpha_0, ..., \alpha_{q-1}) \in \mathbb{R}^q$ and for any positive integer n such that $rep_q(n) = n_\ell \dots n_0$, we denote by $|n|_j = \mathrm{card}\{k, 0 \leq k \leq \ell, n_k = j\}$

The following theorem generalizes the theorem by Mauduit-Rivat solving the Gelfond conjecture concerning the sum of digits of prime numbers (i.e. the case $(\alpha_0, ..., \alpha_{q-1}) = (0, ..., q-1)$).

Theorem 1. *(Martin-Mauduit-Rivat, 2013) For any $(\alpha, \beta) \in \mathbb{R}^2$ such that $(q-1)\alpha \in \mathbb{R} \setminus \mathbb{Z}$, there exists $\sigma_q(\alpha) > 0$ such that for any $x \geq 1$,*

$$\sum_{p \leq x} \exp\Big(2i\pi(\alpha s_q(p) + \beta p)\Big) \ll_{q,\alpha} x^{1-\sigma_q(\alpha)}.$$

Remark 1. The full version of Theorem 1 answer Problem 1 for the finite q-automata recognizing digital functions in arithmetic progressions.

Remark 2. In a recent work, Drmota generalized these results to a much larger class of finite q-automata (invertible q-automata).

Digits of prime numbers

In a recent paper, Bourgain gave an asymptotic for the number of prime numbers with some preassigned digits, improving previous results due to Harman-Kátai (2008), Harman (2006), Wolke (2005) and Kátai (1986) :

Theorem 2. *(Bourgain, 2013) There exists* $c > 0$ *such that, for any positive integers* t *and* k *such that*

$$1 \leq t \leq ck,$$

for any $0 \leq j_1 < \cdots < j_t \leq k$ *and for any* $(b_1, \ldots, b_t) \in \{0, \ldots, q-1\}^t$ *such that* $(b_1, q) = 1$ *when* $j_1 = 0$ *and* $b_t \neq 0$ *when* $j_t = k$*, we have, for* $N = q^k$*,* $k \to \infty$*,*

$$\mathrm{card}\{p < N,\ p = \sum_{j=0}^{k} p_j q^j,\ (p_{j_1}, \ldots, p_{j_t}) = (b_1, \ldots, b_t)\} \sim \begin{cases} \frac{1}{q^t} \frac{N}{\log N} & \text{if } j_1 > 0 \\ \frac{1}{q^t} \frac{q}{\varphi(q)} \frac{N}{\log N} & \text{if } j_1 = 0. \end{cases}$$

Problem 3. What is the best possible value for c ?

Möbius randomness principle

We denote by μ the Möbius function, defined by $\mu(1) = 1, \mu(p_1 \dots p_k) = (-1)^k$ if $p_1, \dots, p_k$ are distinct prime numbers and $\mu(n) = 0$ if n is divisible by the square of a prime number. The function μ is multiplicative, i. e. $\mu(mn) = \mu(m)\mu(n)$ for any coprime positive integers m and n and μ^2 is the characteristic function of square-free numbers.

$$\mu = (\mu(n))_{n\geq 1} = 1, -1, -1, 0, -1, 1, -1, 0, 0, 1, -1, 0, -1, 1, 1, 0, -1, 0, -1, 0, \dots$$

The results and problems presented in the previous paragraph turn out to show the independence between the multiplicative property "to be a prime number" and q-automatic or q-additive properties. They are naturally connected to the Möbius randomness principle for q-automatic or q-multiplicative sequences $\mathbf{u}$. This principle often stated vaguely in the literature, says that "for any reasonable sequence $\mathbf{u} = (u(n))_{n\in\mathbb{N}}$ of complex numbers, the sum $\sum_{n\leq x} \mu(n)u(n)$ is relatively small ".

The conjecture of Sarnak

Sarnak gave in 2011 a more accurate version of the Möbius randomness principle by setting it in the context of the theory of dynamical systems. Let X be a compact metric space, T be a continuous transformation of X and (X,T) the associated dynamical system.

Definition 1. A sequence $\mathbf{u} = (u(n))_{n\in\mathbb{N}}$ of elements of X is produced by (X,T) if there exist $x_0 \in X$ and f continuous on X such that for any integer n, we have $u(n) = f(T^n(x_0))$.

Conjecture (Sarnak) : For any bounded sequence of complex numbers $\mathbf{u} = (u(n))_{n\in\mathbb{N}}$ produced by a zero topological entropy dynamical system, we have $\sum_{n\leq x} \mu(n)u(n) = o(x)$.

(The topological entropy of the dynamical system (X,T) corresponds to the rate of increase of the number of ϵ-different orbits of lenght n, when n goes to infinity and ϵ to zero).

Remark 3. As pointed by Sarnak, the results of Agrawal, Kayal and Sexana (2004) suggest that the values of $\mu(n)$ could be computed in $O((\log n)^c)$ steps, so that the stronger conjecture saying that μ is orthogonal to any sequence of polynomial computational complexity is probably wrong.

Prime number theorem and Sarnak conjecture

The Sarnak conjecture does not imply the existence of a prime number theorem, that is to say a control of the sums $\sum_{n \leq x} \Lambda(n) u(n)$ or $\sum_{p \leq x} u(p)$. It can be much more difficult to get a prime number theorem than to show the Sarnak conjecture, the difference being roughly speaking in the treatment of sums of type II in the Vinogradov method.

Sarnak conjecture, with or without a prime number theorem (PNT), is proved in the following specific cases :

1) X finite (1896, Hadamard and de La Vallée Poussin, with PNT) ;

2) $X = \mathbb{R}/\mathbb{Z}$ and $T(x) = x + \alpha$ (1937, Davenport, with PNT) ;

3) $(X, T) =$ Thue-Morse dynamical system (2010, Mauduit-Rivat, with PNT) ;

4) $(X, T) =$ Translation on a compact nilmanifold (2012, Green-Tao, with PNT) ;

5) $(X, T) =$ Horocycle flow (2012, Bourgain-Sarnak-Ziegler, without PNT) ;

6) $(X, T) =$ Rudin-Shapiro dynamical system (2013, Mauduit-Rivat, with PNT).

The Sarnak conjecture for binary sequences

Some recent works of Green and Bourgain concern the particular case where $\mathbf{u}$ is a sequence with values in the finite alphabet $A = \{-1, 1\}$ and are motivated by the study of the computational complexity of μ. The goal is to prove the orthogonality of the Möbius function with certain classes of Boolean functions in relation with a series of questions stated by Kalai on his blog.

In 2012, Green shows that if $\mathbf{u} \in \{-1, 1\}^{\mathbb{N}}$ is computable by a Boolean function representable by a circuit of depth at most d and size at most n^d, then

$$\sum_{n<2^\nu} \mu(n)u(n) = O(2^\nu \exp(d \log \nu - \nu^{1/6d})). \tag{1}$$

From a result of Linial-Mansour-Nisan, the problem turns into giving good estimates for the Fourier-Walsh transform $\sum_{n<2^\nu} \mu(n)(-1)^{s_E(n)}$, where $E \subset \mathbb{N}$ verifies $\operatorname{card} E = O(\frac{\sqrt{\nu}}{\log \nu})$ and s_E is the restricted sum of binary digits function, defined by $s_E(n) = \sum_{\substack{j \le \ell \\ j \in E}} n_j$ if $rep_q(n) = n_\ell \dots n_0$.

Bourgain theorems

By generalizing the method introduced by Mauduit-Rivat to study the extreme case where $E = \mathbb{N}$ in the proof of Theorem 1, Bourgain extended in 2012 the estimate (1) to any set E by showing that

$$\max_{E \subset \{0,\ldots,\nu-1\}} \sum_{n<2^\nu} \mu(n)(-1)^{s_E(n)} = O(2^{\nu-\nu^{1/10}}), \tag{2}$$

and therefore the Sarnak conjecture (with PNT) for every sequence $\mathbf{u} = ((-1)^{s_E(n)})_{n\in\mathbb{N}}$.

Moreover, by studying precisely the distribution of these Fourier-Walsh coefficients, Bourgain deduced in 2013, using a result of Bshouty-Tamon concerning the localization of the Walsh-Fourier spectrum of monotone Boolean functions, a proof of the Sarnak conjecture (without PNT) for these functions and in very recent paper a lower bounds for the number of prime numbers captured by these functions.

Generalized Rudin-Shapiro sequences

The estimate (2) means that for any polynomial $P \in \mathbb{Z}[X_0, \ldots, X_{\nu-1}]$ of degree 1 we have

$$\sum_{n<2^\nu} \mu(n)(-1)^{P(\varepsilon_0(n),\ldots,\varepsilon_{\nu-1}(n))} = O(2^{\nu-\nu^{1/10}}).$$

But the question asked by Kalai in 2012 concerning the case of polynomials of degree greater than 1 is open. The simplest case of polynomial of degree 2 is given by the Rudin-Shapiro sequence $\left((-1)^{\sum_{i\geq 1}\varepsilon_{i-1}(n)\varepsilon_i(n)}\right)_{n\in\mathbb{N}}$, for which Tao suggested on *mathoverflow* a strategy to prove the Sarnak conjecture (without PNT).

In a recent work Mauduit and Rivat obtain a Prime Number Theorem for the sequences

$$\left((-1)^{r_d(n)}\right)_{n\in\mathbb{N}} = \left((-1)^{\sum_{i\geq d-1}\varepsilon_{i-d+1}(n)\cdots\varepsilon_{i-1}(n)\varepsilon_i(n)}\right)_{n\in\mathbb{N}}$$

for all integers $d \geq 2$, providing an answer to Kalai's question for the simplest case of polynomial of degree d.

PNT for digital sequences with uniformly small discrete Fourier transform

For $f : \mathbb{N} \to \mathbb{N}$ and any $\lambda \in \mathbb{N}$, let us denote by f_λ the q^λ-periodic function defined by $\forall n \in \{0, \dots, q^\lambda - 1\},\ \forall k \in \mathbb{Z},\ f_\lambda(n + kq^\lambda) = f(n)$.

Definition 2. A function $f : \mathbb{N} \to \mathbb{N}$ has the *carry property* if, uniformly for $(\lambda, \kappa, \rho) \in \mathbb{N}^3$ with $\rho < \lambda$, the number of integers $0 \leq \ell < q^\lambda$ such that there exists $(k_1, k_2) \in \{0, \dots, q^\kappa - 1\}^2$ with $f(\ell q^\kappa + k_1 + k_2) - f(\ell q^\kappa + k_1) \neq f_{\kappa+\rho}(\ell q^\kappa + k_1 + k_2) - f_{\kappa+\rho}(\ell q^\kappa + k_1)$ is at most $O_{q,f}(q^{\lambda-\rho})$.

We introduce a set of functions with uniformly small discrete Fourier transforms :

Definition 3. Given a non decreasing function $\gamma : \mathbb{R} \to \mathbb{R}$ satisfying $\lim_{\lambda \to +\infty} \gamma(\lambda) = +\infty$ and $c > 0$ we denote by $\mathcal{F}_{\gamma,c}$ the set of functions $f : \mathbb{N} \to \mathbb{N}$ such that for $(\kappa, \lambda) \in \mathbb{N}^2$ with $\kappa \leq c\lambda$ and $t \in \mathbb{R}$:

$$|q^{-\lambda} \sum_{0 \leq u < q^\lambda} \exp(2i\pi(f(uq^\kappa) - ut))| \leq q^{-\gamma(\lambda)}.$$

Theorem 3. *Let $\gamma : \mathbb{R} \to \mathbb{R}$ be a non decreasing function satisfying $\lim_{\lambda\to+\infty} \gamma(\lambda) = +\infty$, and $f : \mathbb{N} \to \mathbb{N}$ be a function satisfying Definition 2 and $f \in \mathcal{F}_{\gamma,c}$ for some $c \geq 10$ in Definition 3. Then there exist $c_1(q) > 0$ and $c_2(q) > 0$ such that for any $\beta \in \mathbb{R}$ we have*

$$|\sum_{p\leq x} \exp(2i\pi(f(p)+\beta p)| \ll c_1(q)(\log x)^{c_2(q)}\, x\, q^{-\gamma(2[(\log x)/80\log q])/20},$$

Remark 4. Theorem 3 gives a non trivial result if $\liminf_{\lambda\to\infty} \frac{\gamma(\lambda)}{\log\lambda} > \frac{20\, c_2(q)}{\log q}$.

The application to generalized Rudin-Shapiro sequences follows from the following property :

Proposition 1. *For any $d \geq 2$, $(\alpha,\beta) \in \mathbb{R}^2$ and $\lambda \in \mathbb{N}$ we have*

$$|2^{-\lambda} \sum_{0\leq n<2^\lambda} \exp(2i\pi(\alpha r_d(n)+\beta n)| \leq \left(1 - 2^{3-d}\left(\sin\frac{\pi\|\alpha\|}{4}\right)^2\right)^{[\lambda/d]}.$$

Problem 4. Answer Kalai's question for any polynomial $P \in \mathbb{Z}[X_0,\ldots,X_{\nu-1}]$ of degree d.