Eötvös Loránd University
Institute of Mathematics

László Mérai

Pseudorandom sequences and lattices

theses of the doctoral thesis

Doctoral school: Mathematics
Director: Professor Miklós Laczkovich

Doctoral program: Pure mathematics
Director: Professor András Szűcs

Supervisor: András Sárközy

Budapest, 2010.

1 Introduction

Pseudorandom sequences play a crucial role in many areas such as cryptography and communication systems. There are many definitions to pseudorandomness depending on specific applications.

In order to study the pseudorandomness of finite binary sequences, Mauduit and Sárközy introduced several definitions in [11]. For a given binary sequence

$$E_N = \{e_1, \dots, e_N\} \in \{-1, +1\}^N$$

the *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,t} |U(E_N, t, a, b)| = \max_{a,b,t} \left| \sum_{j=1}^{t} e_{a+jb} \right|,$$

where the maximum is taken over all $a, b, t \in \mathbb{N}$ such that $1 \le a \le a + (t-1)b \le N$. The *correlation measure of order* k of E_N is defined as

$$C_\ell(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell} \right|,$$

where the maximum is taken over all $D = (d_1, \dots, d_\ell)$ and M such that $0 \le d_1 < d_2 < \dots < d_\ell \le N - M$.

The sequence E_N is considered as a "good" pseudorandom sequence if both these measures $W(E_N)$ and $C_\ell(E_N)$ (at least for small ℓ) are "small" in terms of N (in particular, both are $o(N)$ as $N \to \infty$). This terminology is justified since for a truly random sequence E_N each of these measures is $\ll \sqrt{N \log N}$. (For a more precise version of this result see [1].)

Using the Legendre symbol Goubin, Mauduit and Sárközy [4] constructed a large family of pseudorandom sequences by generalizing the construction of Mauduit and Sárközy [11]:

Construction 1 (Goubin, Mauduit, Sárközy)**.** Let p be a prime, $f \in \mathbb{F}_p[x]$ and let us define the sequence $E_p = \{e_1, \dots, e_p\}$ by

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right), & \text{if } p \nmid f(n), \\ 1, & \text{if } p \mid f(n), \end{cases}$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

Later Mauduit, Rivat and Sárközy [10] define a well-computable construction based on the residue of a polynomial:

Construction 2 (Mauduit, Rivat, Sárközy). Let p be a prime, $f \in \mathbb{F}_p[x]$. Define the sequence $E_p = \{e_1, \dots, e_p\}$ by

$$e_n = \begin{cases} +1, & \text{if } f(n) \in \{1, 2, \dots, \frac{p-1}{2}\} \\ -1, & \text{otherwise.} \end{cases}$$

Although this construction can be computed fast, they showed by an example that if the order of the correlation is greater than the degree of the polynomial, then the correlation can be large.

In order to avoid this restriction to the degree of the polynomial, Mauduit and Sárközy replaced the polynomial with its multiplicative inverse:

Construction 3 (Mauduit, Sárközy). Let p be a prime, $f \in \mathbb{F}_p[x]$. Define the sequence $E_p = \{e_1, \dots, e_p\}$ by

$$e_n = \begin{cases} +1, & \text{if } f(n) \neq 0 \text{ és } f(n)^{-1} \in \{1, 2, \dots, \frac{p-1}{2}\} \\ -1, & \text{otherwise,} \end{cases}$$

where a^{-1} $(a \neq 0)$ is the multiplicative inverse of the element $a \in \mathbb{F}_p$.

2 General construction of pseudorandom binary sequences

Construction mentioned above are the special cases of the following construction:

Construction 4. Let p be a prime, ψ additive, χ multiplicative character of $\mathbb{F}_p$, and let $F(x)$, $Q(x) \in \mathbb{F}_p(x)$ be rational functions. Define the sequence $E_p = \{e_1, \dots, e_p\}$ by

$$e_n = \begin{cases} +1 & \text{if } \arg\big(\psi\left(F(n)\right) \cdot \chi\left(Q(n)\right)\big) \in [0, \pi) \text{ and } n \notin S \\ -1 & \text{otherwise.} \end{cases}$$

Clearly, if χ is the Legendre symbol, the rational function F is constant, then we get construction 1. On the other hand, if χ is a multiplicative character such that $\chi(g) = e^{\frac{2\pi i}{p-1}}$, where g is a generator of $\mathbb{F}_p$ then we get constructions of Gyarmati [5] and Sárközy [16] which are based on the discrete logarithm.

Furthermore, if the rational function Q is constant, we get construction 2 and 3, as long as the function F is a polynomial, or its multiplicative inverse.

At first this general construction studied by Oon [14, 15] in the case, where the rational function F is constant. However, he could give non-trivial bound to the measures, if the order of the character is large: $\Omega(p^{1/2})$. If the order is small and odd, nontrivial bound does not exist (see chapter 3, example 1.). On the other hand it can be shown that construction (4) can be extended to small and even order.

Befor I state the theorem, I recall the definition of admissibility, which describes which rational function can be used in the construction.

Definition 1. The triple (k, ℓ, m) is said to be *d-admissible triple* $(k, \ell < m)$, if there are no multiset $\mathcal{A}, \mathcal{B}$ which satisfy the following criteria:

(i) $|\mathcal{A}| = k$, $|\mathcal{B}| = \ell$;

(ii) the multiplicity of each element of $\mathcal{A}$ and $\mathcal{B}$ is less than d, and the multiplicity of each element of $\mathcal{A}$ is co-prime to d;

(iii) for each c, the number of solutin of the equation

$$a + b = c, \quad a \in \mathcal{A}, b \in \mathcal{B}$$

is divisible by d.

(Here $|\mathcal{A}|$ is the number of the distinct element of $\mathcal{A}$.)

Furthermore the triple (k, ℓ, G) is said to be *admissible triple* $(k, \ell < m)$ if for each sets $\mathcal{A}, \mathcal{B} \subset G$ ($|\mathcal{A}| \leq k$, $|\mathcal{B}| \leq \ell$) there is an element $c \in G$ such that the equation

$$a + b = c \quad a \in \mathcal{A}, \ b \in \mathcal{B}$$

has exactly one solution.

Theorem 2 ([M1])**.** *If the sequence E_p is defined by construction 4, where the order d of the multiplicative character χ is even, $Q \in \mathbb{F}_p[x]$ is a polynomial which is not a d-th power, and the function F is constant, then*

$$W(E_p) \leq 36 s p^{1/2} \log p \log d + s,$$

where s is the number of distinct roots of Q.

Additionally, if the multiplicity of each root of Q is co-prime to d or divisible by d, and the triple (s, ℓ, p) is d-admissible, then

$$C_\ell(E_p) \leq 9\, 4^\ell \ell s p^{1/2} \log p (\log d)^\ell + \ell s.$$

If the function F is not a constant function, then the order of χ can be odd:

Theorem 3 ([M3])**.** *Assume that $\psi \neq \psi_0$ is additive, $\chi \neq \chi_0$ is multiplicative character of order d, $F(x) = \frac{f(x)}{g(x)}, Q(x) = \frac{q(x)}{r(x)} \in \mathbb{F}_p(x)$ are rational functions such that $(g(x), f(x)) = 1$ and $(q(x), r(x)) = 1$ and neither $q(x)$ nor $r(x)$ has multiple zero in $\overline{\mathbb{F}}_p$ and the binary sequence $E_p = \{e_1, \dots, e_p\}$ is defined by Construction 4. Then we have*

$$W(E_p) \ll (\deg^* F + z) \cdot p^{1/2} (\log p)^2,$$

where z is the number of distinct roots of q and r.

Assume also that $\ell \in \mathbb{N}$ such that $2 \le \ell < p$ and one of the following conditions holds:

(i) $\ell = 2$;

(ii) $(4 \cdot \deg g)^\ell < p$, $(4 \cdot \deg^* Q)^\ell < p$;

(iii) $g(x) = (x + a_1)(x + a_2) \dots (x + a_k)$ ($a_i \ne a_j$, $i \ne j$) *and* $\ell \cdot \deg g < \frac{p}{2}$, $(4 \cdot \deg^* Q)^\ell < p$,

then

$$C_\ell(E_p) \ll (\ell + 1)(\deg^* F + d \cdot \deg^* Q) \cdot p^{1/2} (\log p)^{\ell+1}.$$

In a similar way, we can handle the case, when Q is a constant function [M2].

3 Pseudorandom binary lattices

In applications one may need *pseudorandom lattices* instead of pseudorandom sequences, for example to encrypt 2-dimensional pictures via the analogue of the Vernam cipher. In [9], Hubert, Mauduit and Sárközy extended the notion of binary sequences to n-dimensional binary lattices in the following way:

Denote I_N^n the set of the n-dimensional vectors whose coordinates are selected from the set $\{0, 1, \dots, N-1\}$:

$$I_N^n = \big\{ \mathbf{x} = (x_1, \dots, x_n) : \ x_1, \dots, x_n \in \{0, 1, \dots, N-1\} \big\}.$$

The n-dimensional binary lattice is defined by the function

$$\eta : I_N^n \to \{-1, +1\}.$$

They also defined the following measures of pseudorandomness:

Let $\mathbf{u}_1, \dots, \mathbf{u}_n$ be n linearly independent vectors, where the i-th coordinate of $\mathbf{u}_i$ is a positive integer, and the others are zeros. Let $t_1, \dots, t_n$ be integers such that $0 \le t_1, \dots, t_n < N$. Then we call the set

$$B_N^n = \{ \mathbf{x} = x_1 \mathbf{u}_1 + \dots + x_n \mathbf{u}_n : 0 \le x_i |\mathbf{u}_i| \le t_i \text{ for all } i = 1, \dots, n \}$$

n-dimensional box N-lattice or briefly a box N-lattice.

Definition 4. The *pseudorandom measure of order ℓ of η* is

$$Q_\ell(\eta) = \max_{B, \mathbf{d}_1, \dots, \mathbf{d}_\ell} \left| \sum_{\mathbf{x} \in B} \eta(\mathbf{x} + \mathbf{d}_1) \dots \eta(\mathbf{x} + \mathbf{d}_\ell) \right|,$$

where the maximum is taken over all distinct $\mathbf{d}_1, \dots, \mathbf{d}_\ell \in I_N^n$ and all box N-lattices B such that $B + \mathbf{d}_1, \dots, B + \mathbf{d}_\ell \subseteq I_N^n$.

The binary lattice η is said to have strong pseudorandom properties if for fixed n and ℓ, $Q_\ell(\eta)$ is small (much smaller, than the trivial upper bound N^n) at least for small ℓ. This terminology is justified by the fact that for a truly random lattice η the measure $Q_\ell(\eta) \ll N^{n/2+\varepsilon}$ (see [9]).

Moreover, in [9] and [13] the analogue of Construction **??** was proposed for a "good" n-dimensional binary lattice, for any n, by using the quadratic characters of finite fields:

Construction 5 (Mauduit és Sárközy)**.** Let $q = p^n$ be a prime power, γ is the quadratic character of $\mathbb{F}_q$, $f(x) \in \mathbb{F}_q[x]$. Then define the lattice η by:

$$\eta(\mathbf{x}) = \begin{cases} \gamma(f(x_1b_1 + \cdots + x_nb_n)) & \text{if } f(x_1b_1 + \cdots + x_nb_n) \neq 0, \\ 1 & \text{otherwise,} \end{cases}$$

where $b_1, \ldots, b_n$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ and $\mathbf{x} = (x_1, \ldots, x_n)$.

They showed, that if f satisfies certain conditions. Then

$$Q_\ell(\eta) < \deg f\, \ell(q^{1/2}(1 + \log p)^n + 2).$$

I remark, that the notion of binary lattice can be extend to lattice of k symbol, see [M5].

Construction 5 can be extend in a similar way, replacing the quadratic character to an arbitrary multiplicative character:

Construction 6. Let $q = p^n$ be a prime power, $f(x) \in \mathbb{F}_q[x]$, χ multiplicative character of $\mathbb{F}_q$. Then define the lattice η by:

$$\eta(\mathbf{x}) = \begin{cases} +1 & \text{if } \arg\big(\chi(f(x_1b_1 + \cdots + x_nb_n))\big) \in [0, \pi), \\ -1 & \text{otherwise,} \end{cases}$$

where $b_1, \ldots, b_n$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ and $\mathbf{x} = (x_1, \ldots, x_n)$.

This is a good construction:

Theorem 5 ([M4])**.** *Let $q = p^n$ be the power of an odd prime, χ be a multiplicative character of $\mathbb{F}_q$ of even order d. Let $f(x) \in \mathbb{F}_q[x]$ which is not a d-power, and the multiplicity of each root of f is co-prime to d or divisible by d, and the triple $(\deg f, \ell, \mathbb{F}_q)$ is admissible, then*

$$Q_\ell(\eta) \leq 4^\ell \ell \deg f (\log d)^\ell q^{1/2}(1 + \log p)^n \ell \deg f.$$

4 Pseudorandom binary sequences and lattices over elliptic curves

It is well known than elliptic curves over finite fields have good pseudorandom properties thus they are widely used for generating pseudorandom sequences. Namely, in 1994 Hallgren [8] proposed the *linear congruent generator* from elliptic curves. The linear congruent generator builds a sequence of points on the curve $\mathcal{E}$ by the rule $s_0 = P_0$ for some $P_0 \in \mathcal{E}$ and $s_n = P \oplus s_{n-1} = nP \oplus P_0$.

By using the definition of pseudorandomness given in [11], Chen [2], and Chen, Li and Xiao [3] studied binary sequences derived from this generator where they used the Legendre symbol and the discrete logarithm of finite fields.

The general construction can be defined in the following way:

Construction 7. Let $p > 3$ be a prime, $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_p$, $G \in \mathcal{E}(\mathbb{F}_p)$ be an element with order T, $f \in \mathbb{F}_p(\mathcal{E})$, χ be multiplicative character of order d. Then, define the sequence $E_T = \{e_1, \dots, e_T\}$ by:

$$e_n = \begin{cases} +1, & \text{if } nG \notin \operatorname{Supp}(f) \text{ és } \arg\big(\chi(f(nG))\big) \in [0, \pi), \\ -1, & \text{otherwise.} \end{cases}$$

If χ is the Legendre symbol we get construction of Chen [2], while if χ is a multiplicative character of order $p-1$, then we get construction of Chen, Li and Xiao [3] which is based on the discrete logarithm.

Theorem 6 ([M7]). *Let p be an odd prime, χ be a multiplicative character of $\mathbb{F}_p$ of even order d, $f \in \mathbb{F}_p(\mathcal{E})$ which is not a d-th power in $\overline{\mathbb{F}}_p(\mathcal{E})$. If we define the binary sequence $E_T = \{e_1, \dots, e_T\}$ by Construction 7 then we have*

$$W(E_T) \leq 4|\operatorname{Supp}(f)|p^{1/2}(1 + \log T)\log d + |\operatorname{Supp}(f)|. \tag{1}$$

Moreover, let us assume that the order of zeros and poles of f which are not divisible by d are co-prime to d, and $\ell \in \mathbb{N}$ such that the triple $(|\operatorname{Supp}(f)|, \ell, T)$ is d-admissible. Then we have

$$C_\ell(E_T) \leq 4^\ell \ell |\operatorname{Supp}(f)|p^{1/2}(1 + \log T)(\log d)^\ell + \ell|\operatorname{Supp}(f)|. \tag{2}$$

Further good construction can be given by the residue of rational functions:

Construction 8. Let $G \in \mathcal{E}(\mathbb{F}_p)$ with order T and $f \in \mathbb{F}_p(\mathcal{E})$. Then define the sequence $E_T = \{e_1, \dots, e_T\}$ by

$$e_n = \begin{cases} +1, & \text{if } f(nG) \in \{0, 1, \dots, \frac{p-1}{2}\}, \\ -1, & \text{otherwise.} \end{cases}$$

Theorem 7 ([M8]). *Let $p > 3$ be a prime number, $G \in \mathcal{E}(\mathbb{F}_p)$ with order T, $f \in \mathbb{F}_p(\mathcal{E})$ be a non-constant function. If we define the sequence $E_T = \{e_1, \dots, e_T\}$ by Construction 8 then we have*

$$W(E_T) << \deg f\, p^{1/2} \log p \log T.$$

Additionally, if one of the following condition holds

(i) $\deg f < p(T)$ *and* $\ell = 2$*;*

(ii) $\deg f < p(T)$ *and* $(4 \deg f)^\ell < p(T)$*,*

where $p(T)$ is the least prime divisor of $|T|$, then

$$C_\ell(E_T) << \ell \deg f p^{1/2} (\log p)^\ell \log T.$$

Finally, I show how wecan construct good pseudorandom binary lattice over elliptic curves:

Construction 9. Let χ be a multiplicative character, $f \in \mathbb{F}_p(\mathcal{E})$ and $P_1, \dots, P_n$ be weakly independent points of $\mathcal{E}(\mathbb{F}_p)$ such that the order of each point is greater than N. Then define the mapping $\eta : I_N^n \to \{-1, +1\}$ by

$$\eta(x_1, \dots, x_n) = \begin{cases} +1 & \text{if } \arg\big(\chi(f(x_1 P_1 \oplus \cdots \oplus x_n P_n))\big) \in [0, \pi), \\ -1 & \text{otherwise.} \end{cases} \tag{3}$$

Theorem 8 ([M6]). *Let $p > 3$ be a prime, χ be a multiplicative character of $\mathbb{F}_p$ with even order d, $\mathcal{E}(\mathbb{F}_p)$ be an elliptic curve over $\mathbb{F}_p$, $f \in \mathbb{F}_p(\mathcal{E})$ which is not a d-th power in $\overline{\mathbb{F}}_p(\mathcal{E})$ and the orders of zeros and poles of f are co-primes to d. Let N be an integer and $P_1, \dots, P_n$ be weakly independent elements such that the order of each point is greater than N. If we define the binary lattice by (3) and the pair $(|\operatorname{Supp}(f)|, \ell)$ is admissible then we have*

$$Q_\ell(\eta) \le 2 \cdot 3^n 4^\ell \ell d \deg(f) p^{1/2} (\log |\mathcal{E}(\mathbb{F}_p)|)^n (\log d)^\ell + \ell |\operatorname{Supp}(f)|. \tag{4}$$

5 Admissibility

In this last section I give some sufficient criteria to d-admissibility and admissibility.

Theorem 9 ([M7]). *Let us denote the least prime factor of m by $p(m)$. Then*

(i) If $k, m, d \in \mathbb{N}$, $k < p(m)$ then the triple $(k, 2, m)$ is d-admissible.

(ii) If $k, \ell, m, d \in \mathbb{N}$, $k < m$ and $(4\ell)^k < p(m)$, then the triple (k, ℓ, m) is d-admissible.

(iii) If m is prime, and all of the prime factors of d are primitive roots modulo m, then for every pair $k, \ell \in \mathbb{N}$ with $k < m$, $\ell < m$, the triple (k, ℓ, m) is d-admissible.

Theorem 10 ([M6]). *Let $G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s}$ be a finite Abelian group, $p(G)$ be the least prime factor of $|G|$. Then:*

(i) for all $k < p(G)$ the pair $(2, k)$ is admissible;

(ii) If $k, \ell \in \mathbb{N}$ and $4^{s(k+\ell)} < p(G)$, then the pair (k, ℓ) is admissible.

The thesis are based on the following papers:

[M1] L. Mérai, Construction of large families of pseudorandom binary sequences, The Ramanujan Journal 18 (2009), 341–349.

[M2] L. Mérai, A construction of pseudorandom binary sequences using rational functions, Unif. Distrib. Theory, 4 (2009), no. 1, 35–49.

[M3] L. Mérai, A construction of pseudorandom binary sequences using both additive and multiplicative characters, Acta Arith. 139 (2009), 241–252.

[M4] L. Mérai, Construction of pseudorandom binary lattices based on multiplicative characters, Periodica Math. Hungar. 59 (2009) 43–51.

[M5] L. Mérai, On finite pseudorandom lattices of k symbols, Monatsh. Math. 161 (2010), no. 2, 173–191.

[M6] L. Mérai, Construction of pseudorandom binary lattices using elliptic curves, Proc. Amer. Math. Soc. 139 (2011), 407-420

[M7] L. Mérai, Construction of pseudorandom binary sequences over elliptic curves using multiplicative characters, beküldve

[M8] L. Mérai, Construction of pseudorandom binary sequences over elliptic curves, beküldve

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, Measures of pseudorandomness for finite sequences: typical values, Proc. Lond. Math. Soc. (3) 95 (2007) no. 3, 778–812.

[2] Z. Chen, Elliptic curve analogue of Legendre sequences, Monatsh. Math. 154 (2008) no. 1, 1–10.

[3] Z. Chen, S. Li, G. Xiao, G. Construction of pseudorandom binary sequences from elliptic curves by using discrete logarithm, Lecture Notes in Comput. Sci., 4086, Springer, Berlin, (2006) 285-294.

[4] L. Goubin, C. Mauduit, and A. Sárközy, Construction of large families of pseudorandom binary sequences, J. Number Theory 106 (2004), 56–69.

[5] K. Gyarmati, On a family of pseudorandom binary sequences, Periodica Math. Hungar. 49 (2004) 45-63.

[6] K. Gyarmati; C. Mauduit; A. Sárközy: Constructions of pseudorandom binary lattices. Unif. Distrib. Theory 4 (2009), no. 2, 59–80.

[7] K. Gyarmati; A. Sárközy; C. L. Stewart: On Legendre symbol lattices. Unif. Distrib. Theory 4 (2009), no. 1, 81–95.

[8] S. Hallgren, Linear congruential generators over elliptic curves, Tech. Report CS-94-143, Carnegie Mellon Unv., 1994.

[9] P. Hubert, C. Mauduit and A. Sárközy, On pseudorandom binary lattices, *Acta Arith.* **125** (2006), 51–62.

[10] C. Mauduit, J. Rivat and A. Sárközy, *Construction of pseudorandom binary sequence using additive characters*, Monatshefte Math. 141 (2004), 197–208

[11] C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences I: Measures of pseudorandomness, the Legendre symbol, Acta Arith. 82 (1997), 365–377.

[12] C. Mauduit, A. Sárközy, *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. 108 (2005), 239–252.

[13] C. Mauduit, A. Sárközy, On large families of pseudorandom binary lattices, *Unif. Distrib. Theory* **2** (2007), no. 1, 23–37.

[14] S. M. Oon, *Construction des suites binaires pseudo-aléatories*, PhD thesis, Nancy, 2005.

[15] S. M. Oon, *On pseudo-random properties of certain Dirichlet series*, Ramanujan J. 15 (2008), no. 1, 19–30

[16] A. Sárközy, A finite pseudorandom binary sequence, Studia Sci. Math. Hungar. 38 (2001), 377-384.