ACTA ARITHMETICA
159.2 (2013)

Large families of pseudorandom binary sequences and lattices by using the multiplicative inverse

by

Huaning Liu (Xi'an)

1. Introduction. The need for pseudorandom binary sequences arises in many cryptographic applications. For example, common cryptosystems employ keys that must be generated in a random fashion. Many cryptographic protocols also require random or pseudorandom inputs at various points, e.g., for auxiliary quantities used in generating digital signatures, or for generating challenges in authentication protocols. Therefore a theoretical study of pseudorandom properties of binary sequences is of interest.

Motivated by these facts, in 1997 C. Mauduit and A. Sárközy [6] initiated a comprehensive study of finite pseudorandom binary sequences

$$E_N = (e_1, \ldots, e_N) \in \{-1, +1\}^N.$$

First they introduced the following pseudorandom measures.

Definition 1.1. The *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,t} \Big| \sum_{j=0}^{t-1} e_{a+jb} \Big|,$$

where the maximum is taken over all $a, b, t \in \mathbb{N}$ with $1 \le a \le a+(t-1)b \le N$.

Definition 1.2. The *correlation measure of order l* of E_N is defined by

$$C_l(E_N) = \max_{M,D} \Big| \sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_l} \Big|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_l)$ and M with $0 \le d_1 < \cdots < d_l \le N - M$.

The sequence E_N is considered to be a "good" pseudorandom sequence if both $W(E_N)$ and $C_l(E_N)$ (at least for small l) are "small" in terms of N.

2010 *Mathematics Subject Classification*: Primary 11K36; Secondary 11B50, 94A55.
Key words and phrases: binary sequence, lattice, well-distribution, correlation.

DOI: 10.4064/aa159-2-3

Later J. Cassaigne, C. Mauduit and A. Sárközy [3] proved that this terminology is justified since for almost all $E_N \in \{-1,+1\}^N$, both $W(E_N)$ and $C_l(E_N)$ are less than $N^{1/2}(\log N)^c$. In [1] and [2] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl continued the work in this direction and investigated the typical and minimal values of these measures.

In this paper we give a large family of pseudorandom binary sequences constructed by using the multiplicative inverse. We shall prove the following result in Section 2.

Theorem 1.1. *Suppose that p is a prime and $f(x) \in \mathbb{F}_p[x]$ has degree k with $0 < k < p$. Denote by $R_p(n)$ the least non-negative residue of n modulo p, and for $(a,p)=1$, denote by a^{-1} the multiplicative inverse of a satisfying $aa^{-1} \equiv 1 \pmod p$ and $1 \le a^{-1} \le p-1$. Define the binary sequence $E_p = (e_1,\dots,e_p)$ by*

$$e_n = \begin{cases} +1 & \text{if } (f(n),p)=1,\ R_p(f(n)^{-1}) < p/2, \\ -1 & \text{if either } (f(n),p)=1 \text{ and } R_p(f(n)^{-1}) > p/2, \text{ or } p \mid f(n). \end{cases}$$

Then

$$W(E_p) \ll kp^{1/2}(\log p)^2.$$

Furthermore, assume that 0 *is the unique zero of f in $\mathbb{F}_p$. Then also*

$$C_l(E_p) \ll klp^{1/2}(\log p)^{l+1}.$$

The same estimates were obtained by C. Mauduit and A. Sárközy [7] under the additional assumption that f has no multiple zero in $\overline{\mathbb{F}}_p$. For the estimate of $C_l(E_p)$, instead of the assumption that f has a unique zero at 0, they assumed that $l \in \mathbb{N}$ with $2 \le l \le p$, and one of the following conditions holds: (i) $l=2$; (ii) $(4k)^l < p$.

Remark 1.1. The family defined above is large, and it can be generated relatively fast. Indeed, for example all the polynomials of the form

$$f(x) = x(x^2-a_1)\cdots(x^2-a_k),$$

where $a_1,\dots,a_k$ are pairwise distinct quadratic non-residues modulo p, can be used in the construction above. The only difficulty is to find a quadratic non-residue b; then we may take any $b_1,\dots,b_k$ from $\mathbb{F}_p$ and define $a_i = bb_i^2$ for $i=1,\dots,k$. This construction becomes especially simple if we restrict ourselves to primes p of the form $p=4k-1$, because then we can take $b=-1$.

In 2006 P. Hubert, C. Mauduit and A. Sárközy [4] extended this constructive theory of pseudorandom binary sequences to several dimensions. Let

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

A function $\eta : I_N^n \to \{-1,+1\}$ is called an *n-dimensional binary N-lattice* or briefly a *binary lattice.*

The following pseudorandom measure was introduced in [4].

DEFINITION 1.3. Let $k\in\mathbb{N}$, and let $\mathbf{u}_i$ $(i=1,\dots,n)$ denote the n-dimensional vector whose ith coordinate is 1 and the others are 0. Then write

$$\mathbb{Q}_k(\eta) = \max_{\mathbf{B},\mathbf{d}_1,\dots,\mathbf{d}_k,\mathbf{T}} \Bigg| \sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1 b_1 \mathbf{u}_1 + \dots + j_n b_n \mathbf{u}_n + \mathbf{d}_1) \\ \times \dots \times \eta(j_1 b_1 \mathbf{u}_1 + \dots + j_n b_n \mathbf{u}_n + \mathbf{d}_k) \Bigg|,$$

where the maximum is taken over all n-dimensional vectors $\mathbf{B} = (b_1,\dots,b_n)$, $\mathbf{d}_1,\dots,\mathbf{d}_k$, $\mathbf{T} = (t_1,\dots,t_n)$ whose coordinates are non-negative integers, $b_1,\dots,b_n$ are non-zero, $\mathbf{d}_1,\dots,\mathbf{d}_k$ are distinct, and all the points $j_1 b_1 \mathbf{u}_1 + \dots + j_n b_n \mathbf{u}_n + \mathbf{d}_i$ occurring in the multiple sum belong to I_N^n. Then $\mathbb{Q}_k(\eta)$ is called the *pseudorandom measure of order k* of η.

An n-dimensional binary N-lattice η is considered to be a "good" pseudorandom binary lattice if $\mathbb{Q}_k(\eta)$ is "small" in terms of N for small k. P. Hubert, C. Mauduit and A. Sárközy [4] proved that this terminology is justified since for a fixed $k \in \mathbb{N}$ and for a truly random n-dimensional binary N-lattice η, we have $N^{n/2} \ll \mathbb{Q}_k(\eta) \ll N^{n/2}(\log N^n)^{1/2}$ with probability $> 1-\epsilon$.

In Section 3 we will prove the following result:

THEOREM 1.2. *Let $q=p^n$, $\mathbb{F}_q$ a finite field, $f(x) \in \mathbb{F}_q[x]$ with $\deg(f)>0$, and let $v_1,\dots,v_n$ be linearly independent elements of $\mathbb{F}_q$ over $\mathbb{F}_p$. Set*

$$B_1 = \Big\{ \sum_{i=1}^n u_i v_i : 0 \le u_1 \le (p-3)/2, u_2,\dots,u_n \in \mathbb{F}_p \Big\},$$

$$B_j = \Big\{ \sum_{i=1}^n u_i v_i : u_1 = \dots = u_{j-1} = (p-1)/2, \\ 0 \le u_j \le (p-3)/2, u_{j+1},\dots,u_n \in \mathbb{F}_p \Big\}$$

for $j=2,\dots,n$, and $B = \bigcup_{j=1}^n B_j$. Define

$$\eta(\mathbf{x}) = \eta((x_1,\dots,x_n)) = \begin{cases} +1 & \text{if } f(x_1v_1+\dots+x_nv_n) \neq 0 \\ & \text{and } f(x_1v_1+\dots+x_nv_n)^{-1} \in B, \\ -1 & \text{otherwise.} \end{cases}$$

Assume that 0 is the unique zero of f in $\mathbb{F}_q$, and its multiplicity is $c<p$. Then

$$\mathbb{Q}_k(\eta) \ll 2^k k \deg(f) n^k q^{1/2} (\log p + 2)^{n+k}.$$

In [8], with the assumption "f has a unique zero at 0, of multiplicity $< p$" replaced by "f has no multiple zero in $\overline{\mathbb{F}}_q$, $0 < k, \deg(f) < p$, $k + \deg(f) \le p+1$ and $k \deg(f) < q/2$", C. Mauduit and A. Sárközy obtained the estimate

$$\mathbb{Q}_k(\eta) < (2^{k+3} + 1)k \deg(f) n^k q^{1/2} (\log p + 2)^{n+k}.$$

Remark 1.2. Our family is large, since there are many polynomials $f(x)$ satisfying the given conditions.

2. Proof of Theorem 1.1. We need the following lemmas.

Lemma 2.1 ([5, Lemma 2]). *For $n \in \mathbb{Z}$ and p an odd prime, we have*

$$\frac{1}{p} \sum_{|a|<p/2} v_p(a) e(an/p) = \begin{cases} +1 & \text{if } R_p(n) < p/2, \\ -1 & \text{otherwise,} \end{cases}$$

where $v_p(a)$ is a function of period p such that $v_p(0) = 1$, and

$$v_p(a) = \begin{cases} O(1) & \text{if } a \text{ is even}, \\ -\dfrac{2ip}{\pi a} + O(1) & \text{if } a \text{ is odd}. \end{cases} \blacksquare$$

Lemma 2.2 ([10, Theorem 1]). *Let p be a prime number and ψ be a non-trivial additive character of $\mathbb{F}_p$. Let Q/R be a rational function over $\mathbb{F}_p$ such that the polynomial R has s distinct roots in $\overline{\mathbb{F}}_p$, and assume that Q/R is not a constant or linear polynomial. Write $d = \max(\deg(R), \deg(Q) - 1)$. Then for $1 \le N \le p$, we have*

$$\Bigg| \sum_{\substack{0 \le n \le N-1 \\ R(n) \ne 0}} \psi\left(\frac{Q(n)}{R(n)}\right) \Bigg| \le (d+s)\sqrt{p}\left(\frac{4}{\pi^2} \log p + 0.38 + \frac{N + 0.64}{p}\right). \blacksquare$$

Now we prove Theorem 1.1. For a, b, t with $1 \le a \le a + (t-1)b \le p$, by Lemmas 2.1 and 2.2 we have

$$\begin{aligned} \sum_{j=0}^{t-1} e_{a+jb} &= \frac{1}{p} \sum_{|h|<p/2} v_p(h) \sum_{\substack{j=0 \\ f(a+jb) \ne 0}}^{t-1} e\left(\frac{hf(a+jb)^{-1}}{p}\right) + O(k) \\ &\ll \frac{1}{p} \sum_{\substack{|h|<p/2 \\ h \ne 0}} |v_p(h)| \cdot kp^{1/2} \log p + k \ll kp^{1/2} (\log p)^2. \end{aligned}$$

Therefore

$$W(E_p) = \max_{a,b,t} \Bigg| \sum_{j=0}^{t-1} e_{a+jb} \Bigg| \ll kp^{1/2} (\log p)^2.$$

For $0 \le d_1 < \cdots < d_l \le p - M$, by Lemma 2.1 we get

$$\sum_{n=1}^{M} e_{n+d_1} \cdots e_{n+d_l} = \frac{1}{p^l} \sum_{\substack{n=1 \\ f(n+d_1)\cdots f(n+d_l)\neq 0}}^{M} \sum_{|h_1|<p/2} v_p(h_1) e\left(\frac{h_1 f(n+d_1)^{-1}}{p}\right)$$
$$\times \cdots \times \sum_{|h_l|<p/2} v_p(h_l) e\left(\frac{h_l f(n+d_l)^{-1}}{p}\right) + O(kl)$$
$$= \frac{1}{p^l} \sum_{|h_1|<p/2} v_p(h_1) \cdots \sum_{|h_l|<p/2} v_p(h_l)$$
$$\times \sum_{\substack{n=1 \\ f(n+d_1)\cdots f(n+d_l)\neq 0}}^{M} e\left(\frac{h_1 f(n+d_1)^{-1} + \cdots + h_l f(n+d_l)^{-1}}{p}\right) + O(kl)$$
$$= \frac{1}{p^l} \sum_{\substack{|h_1|<p/2 \\ h_1\neq 0}} v_p(h_1) \cdots \sum_{\substack{|h_l|<p/2 \\ h_l\neq 0}} v_p(h_l)$$
$$\times \sum_{\substack{n=1 \\ f(n+d_1)\cdots f(n+d_l)\neq 0}}^{M} e\left(\frac{h_1 f(n+d_1)^{-1} + \cdots + h_l f(n+d_l)^{-1}}{p}\right)$$
$$+ O((\log p)^{l-1}) + O(kl).$$

Define

$$Q(n) = \sum_{i=1}^{l} h_i \prod_{\substack{j=1 \\ j\neq i}}^{l} f(n+d_j) \quad \text{and} \quad R(n) = \prod_{j=1}^{l} f(n+d_j).$$

Then

$$\sum_{\substack{n=1 \\ f(n+d_1)\cdots f(n+d_l)\neq 0}}^{M} e\left(\frac{h_1 f(n+d_1)^{-1} + \cdots + h_l f(n+d_l)^{-1}}{p}\right)$$
$$= \sum_{\substack{n=1 \\ R(n)\neq 0}}^{M} e\left(\frac{Q(n)}{R(n)p}\right).$$

As $f(x) = 0 \Leftrightarrow x = 0$, we have $Q(n) \neq 0$ for $n = -d_1, \ldots, -d_l$ since the h_i's are nonzero. Thus $Q(n)$ cannot be the 0 polynomial. Since $\deg(Q) < \deg(R)$, Q/R is not a constant or linear polynomial. By Lemmas 2.1 and 2.2 we get

$$\sum_{n=1}^{M} e_{n+d_1}\cdots e_{n+d_l} \ll \frac{1}{p^l}\Big(\sum_{\substack{|h|<p/2\\ h\neq 0}} |v_p(h)|\Big)^l \cdot klp^{1/2}\log p + (\log p)^{l-1} + kl$$
$$\ll klp^{1/2}(\log p)^{l+1}.$$

Therefore

$$C_l(E_p) = \max_{M,D}\Big|\sum_{n=1}^{M} e_{n+d_1}\cdots e_{n+d_l}\Big| \ll klp^{1/2}(\log p)^{l+1}.$$

This proves Theorem 1.1.

3. Proof of Theorem 1.2. We need the following lemma.

Lemma 3.1 ([8, Lemma 4]). *Assume that $q = p^n$ is a prime power; $Q(x)/R(x)$ is a nonzero rational function over $\mathbb{F}_q$ such that $\deg(Q) < \deg(R)$ and there is no polynomial $L(x) \in \mathbb{F}_q[x]$ with $(L(x))^p \mid R(x)$ and $\deg(L) > 0$; ψ is a nontrivial additive character of $\mathbb{F}_q$; and $\overline{B} \subseteq \mathbb{F}_q$ is a box of the form*

$$\overline{B} = \Big\{\sum_{j=1}^{n} j_i v_i : 0 \le j_i \le t_i,\ i = 1,\dots,n\Big\},$$

where $v_1,\dots,v_n$ are linearly independent over the prime field of $\mathbb{F}_q$. Then

$$\Big|\sum_{\substack{z\in\overline{B}\\ R(z)\neq 0}} \psi\Big(\frac{Q(z)}{R(z)}\Big)\Big| < 3(\deg(R)+1)q^{1/2}(2+\log p)^n. \ \blacksquare$$

Now we prove Theorem 1.2. Let $q = p^n$ and $\mathbb{F}_q$ be a finite field, and let ψ_1 be the canonical additive character of $\mathbb{F}_q$. Let $b_1,\dots,b_n$ be positive integers, and write $\mathbf{d}_i = (d_1^{(i)},\dots,d_n^{(i)})$ for $i = 1,\dots,k$. Define

$$B' = \Big\{\sum_{i=1}^{n} j_i(b_i v_i) : 0 \le j_i \le t_i \text{ for } i = 1,\dots,n\Big\},$$
$$z = j_1(b_1v_1) + \cdots + j_n(b_nv_n), \qquad z_l = d_1^{(l)}v_1 + \cdots + d_n^{(l)}v_n, \qquad l = 1,\dots,k.$$

It is easy to show that

$$2\Big(\frac{1}{q}\sum_{b\in B}\sum_{r\in\mathbb{F}_q}\psi_1(r(x-b)) - \frac{1}{2}\Big) = \begin{cases} +1 & \text{if } x\in B,\\ -1 & \text{if } x\notin B.\end{cases}$$

Thus for $f(x_1v_1+\cdots+x_nv_n)\neq 0$ we have

$$\begin{aligned}\eta(\mathbf{x})&=\frac{2}{q}\sum_{r\in\mathbb{F}_q}\sum_{b\in B}\psi_1(-rb)\psi_1(rf(x_1v_1+\cdots+x_nv_n)^{-1})-1\\&=\frac{2}{q}\sum_{r\in\mathbb{F}_q^*}\sum_{b\in B}\psi_1(-rb)\psi_1(rf(x_1v_1+\cdots+x_nv_n)^{-1})\\&\quad+O(q^{-1/2}\log q\,(\log p)^n).\end{aligned}$$

Therefore

$$\begin{aligned}(3.1)\qquad &\sum_{j_1=0}^{t_1}\cdots\sum_{j_n=0}^{t_n}\eta(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_1)\\&\qquad\qquad\times\cdots\times\eta(j_1b_1\mathbf{u}_1+\cdots+j_nb_n\mathbf{u}_n+\mathbf{d}_k)\\&=\sum_{\substack{z\in B'\\ f(z+z_1)\cdots f(z+z_k)\neq 0}}\prod_{i=1}^{k}\Big(\frac{2}{q}\sum_{r_i\in\mathbb{F}_q^*}\sum_{b_i\in B}\psi_1(-r_ib_i)\psi_1(r_if(z+z_i)^{-1})\\&\qquad\qquad+O(q^{-1/2}\log q\,(\log p)^n)\Big)+O(k\deg f)\\&=\frac{2^k}{q^k}\sum_{r_1\in\mathbb{F}_q^*}\sum_{b_1\in B}\psi_1(-r_1b_1)\cdots\sum_{r_k\in\mathbb{F}_q^*}\sum_{b_k\in B}\psi_1(-r_kb_k)\\&\qquad\times\sum_{\substack{z\in B'\\ f(z+z_1)\cdots f(z+z_k)\neq 0}}\psi_1(r_1f(z+z_1)^{-1}+\cdots+r_kf(z+z_k)^{-1})\\&\quad+O(q^{1/2}\log q\,(\log p)^n).\end{aligned}$$

Define

$$Q(z)=\sum_{i=1}^{k}r_i\prod_{\substack{j=1\\ j\neq i}}^{k}f(z+z_j)\quad\text{and}\quad R(z)=\prod_{j=1}^{k}f(z+z_j).$$

Then

$$\sum_{\substack{z\in B'\\ f(z+z_1)\cdots f(z+z_k)\neq 0}}\psi_1(r_1f(z+z_1)^{-1}+\cdots+r_kf(z+z_k)^{-1})=\sum_{\substack{z\in B'\\ R(z)\neq 0}}\psi_1\Big(\frac{Q(z)}{R(z)}\Big).$$

Since $f(z)=0\Leftrightarrow z=0$, we have $Q(z)\neq 0$ for $z=-d_1,\dots,-d_l$. Thus Q/R is a nonzero rational function over $\mathbb{F}_q$ with $\deg(Q)<\deg(R)$. On the other hand, since 0 is the unique zero of $f(z)$ in $\mathbb{F}_q$ with multiplicity $c<p$, it follows that $-z_1,\dots,-z_k$ are the zeros of $R(z)$ with multiplicity $c<p$

each. Therefore there is no polynomial $L(x) \in \mathbb{F}_q[x]$ with $(L(x))^p \mid R(x)$ and $\deg(L) > 0$. Then from Lemma 3.1 we have

$$\sum_{\substack{z \in B' \\ f(z+z_1)\cdots f(z+z_k) \neq 0}} \psi_1(r_1 f(z+z_1)^{-1} + \cdots + r_k f(z+z_k)^{-1}) < 3(k\deg(f)+1)q^{1/2}(2+\log p)^n. \tag{3.2}$$

By [8, (3.26) and (3.29)] we know that

$$\sum_{r \in \mathbb{F}_q^*} \Big| \sum_{z \in B} \psi_1(rz) \Big| < nq(\log p + 3/2). \tag{3.3}$$

Then from (3.1)–(3.3) we get

$$\begin{aligned}
&\sum_{j_1=0}^{t_1} \cdots \sum_{j_n=0}^{t_n} \eta(j_1 b_1 \mathbf{u}_1 + \cdots + j_n b_n \mathbf{u}_n + \mathbf{d}_1) \\
&\qquad\qquad \times \cdots \times \eta(j_1 b_1 \mathbf{u}_1 + \cdots + j_n b_n \mathbf{u}_n + \mathbf{d}_k) \\
&\ll \frac{2^k}{q^k} \Big(\sum_{r \in \mathbb{F}_q^*} \Big| \sum_{b \in B} \psi_1(-rb) \Big| \Big)^k \cdot k\deg(f) q^{1/2} (\log p + 2)^n + q^{1/2} \log q \, (\log p)^n \\
&\ll 2^k k \deg(f) n^k q^{1/2} (\log p + 2)^{n+k}.
\end{aligned}$$

Therefore

$$\mathbb{Q}_k(\eta) \ll 2^k k \deg(f) n^k q^{1/2} (\log p + 2)^{n+k}.$$

This completes the proof of Theorem 1.2.

Acknowledgements. This work was carried out at the Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, during the year 2012. The author expresses his gratitude to the referee for his/her helpful and detailed comments.

This research was supported by the National Natural Science Foundation of China (Grants No. 11201370, 10901128), the Natural Science Foundation of Shaanxi Province of China under Grant No. 2013JM1017, the Natural Science Foundation of the Education Department of Shaanxi Province of China under Grant No. 2013JK0558, and the Fundamental Research Funds for Central Universities.

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: minimal values*, Combin. Probab. Comput. 15 (2006), 1–29.

[2] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. London Math. Soc. 95 (2007), 778–812.

[3] J. Cassaigne, C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequencs VII: The measures of pseudorandomness*, Acta Arith. 103 (2002), 97–108.

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

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

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

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

[8] C. Mauduit and A. Sárközy, *Construction of pseudorandom binary lattices by using the multiplicative inverse*, Monatsh. Math. 153 (2008), 217–231.

[9] C. J. Moreno and O. Moreno, *Exponential sums and Goppa codes: I*, Proc. Amer. Math. Soc. 111 (1991), 523–531.

[10] J. Rivat and A. Sárközy, *Modular constructions of pseudorandom binary sequences with composite moduli*, Period. Math. Hungar. 51 (2005), 75–107.

Huaning Liu
Department of Mathematics
Northwest University
Xi'an, Shaanxi, P.R. China
E-mail: hnliumath@hotmail.com

Received on 22.5.2012
and in revised form on 7.11.2012 and 13.5.2013 (7074)