Uniform Distribution Theory **4** (2009), no.1, 35–49

uniform
distribution
theory

A CONSTRUCTION OF PSEUDORANDOM BINARY SEQUENCES USING RATIONAL FUNCTIONS

László Mérai

ABSTRACT. In this paper a large family of finite pseudorandom binary sequences is constructed by using rational function modulo p. This construction generalizes earlier ones based on the use of the multiplicative inverse modulo p and additive characters, respectively.

Communicated by Christian Mauduit

1. Introduction

In order to study the pseudorandomness of finite binary sequences, Mauduit and Sárközy introduced several definitions in [7]. 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

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

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

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

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

The sequence E_N is considered as a "good" pseudorandom sequence if both these measures $W(E_N)$ and $C_k(E_N)$ (at least for small k) are "small" in terms

2000 Mathematics Subject Classification: Primary 11K45.
Keywords: Pseudorandom, binary sequence, additive character, rational function.

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 $\ll \sqrt{N \log N}$ and $\gg \sqrt{N}$. (For a more precise version of this result see [1].)

Using the Legendre symbol, Mauduit and Sárközy [7] defined a binary sequence by putting $N = p - 1$ and

$$e_n = \left(\frac{n}{p}\right) \text{ for } n = 1, \dots, p-1, \tag{1}$$

where p is a prime number. They proved:

$$W(E_{p-1}) \ll p^{1/2} \log p, \quad C_k(E_{p-1}) \ll kp^{1/2} \log p.$$

In [5], Goubin, Mauduit and Sárközy constructed a large family of pseudorandom sequences by generalizing (1). Namely, if f is a polynomial of degree k satisfying certain conditions, and the sequence $E_p = (e_1, \dots, e_p)$ is defined by

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

then they proved:

$$W(E_p) \le 10kp^{1/2} \log p, \quad C_\ell(E_p) \le k\ell p^{1/2} \log p.$$

Later, in [4], Mauduit, Rivat and Sárközy showed using additive characters that if the sequence E_p is defined by

$$e_n = \begin{cases} +1 & \text{if } r_p(f(n)) < p/2, \\ -1 & \text{otherwise}, \end{cases} \tag{2}$$

where p is a prime number, $r_p(n)$ denotes the least nonnegative residue of n modulo p, and $f(x) \in \mathbb{F}_p[x]$, then

$$W(E_p) \ll kp^{1/2} (\log p)^2, \quad C_\ell(E_p) \le kp^{1/2} (\log p)^{\ell+1}.$$

where $k = \deg f(x)$ and $2 \le \ell \le k - 1$.

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.

Mauduit and Sárközy, in [6], suggested an other easily computable construction based on the multiplicative inverse. Namely, if p is a prime number, $g(x) \in \mathbb{F}_p[x]$, $g(x)$ has degree k $(0 < k < p)$ and no multiple zero in $\overline{\mathbb{F}}_p$, and the binary sequence $E_p = \{e_1, \dots, e_p\}$ defined by

$$e_n = \begin{cases} +1 & \text{if } (g(n), p) = 1 \text{ and } r_p(g^{-1}(n)) < \frac{p}{2} \\ -1 & \text{otherwise}, \end{cases} \tag{3}$$

then

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

Additionally, if $\ell \in \mathbb{N}$ with $2 \le \ell \le p$, and one of the following conditions holds:

(1) $\ell = 2$,

(2) $(4k)^\ell < p$,

(3) $k\ell < \frac{p}{2}$ and $g(x)$ is of the form $g(x) = (x+a_1)(x+a_2)\dots(x+a_k)$ over $\mathbb{F}_p$,

then we also have

$$C_\ell(E_p) \ll k\ell p^{1/2}(\log p)^{\ell+1}. \tag{4}$$

We can give a common generalization of construction (2) and (3). Instead of studying the distribution of $f(n)$ or $1/g(n)$ in the residue classes modulo p, we can study $f(n)/g(n)$. Here and henceforth $\frac{f(n)}{g(n)}$ is defined as $f(n)g(n)^{-1}$, if $g(n) \neq 0$.

We will show that this construction is an efficient generalization, namely if $f(x)/g(x)$ is a non-polynomial rational function, i.e. $g(x) \nmid f(x)$, then we can avoid a restrictive condition on the order of the correlation and we can also give a nontrivial upper bound for correlation of "large" order.

Theorem 1. *Assume that p is a prime number, $f(x), g(x) \in \mathbb{F}_p[x]$, $g(x) \nmid f(x)$ and $g(x)$ has no multiple zero in $\overline{\mathbb{F}}_p$. Define the binary sequence $E_p = \{e_1, \dots, e_p\}$ by*

$$e_n = \begin{cases} +1 & \text{if } (g(n),p) = 1 \text{ and } r_p\left(\frac{f(n)}{g(n)}\right) < \frac{p}{2} \\ -1 & \text{otherwise.} \end{cases}$$

Then we have

$$W(E_p) \ll (\deg f + \deg g)p^{1/2}(\log p)^2. \tag{5}$$

Theorem 2. *Define $p, f(x), g(x)$ and E_p in the same way as in Theorem 1. Assume also that $(f(x), g(x)) = 1$, $\ell \in \mathbb{N}$ with $2 \le \ell \le p$, and one of the following conditions holds:*

(1) $\ell = 2$,

(2) $(4 \deg g)^\ell < p$.

Then we also have

$$C_\ell(E_p) \ll (\deg f + (\ell+1)\deg g)p^{1/2}(\log p)^{\ell+1}. \tag{6}$$

Theorem 3. *Assume that p is a prime number, $\ell \in \mathbb{N}$, $2 \le \ell \le p$,*

$$\ell \deg g < \frac{p}{2}, \tag{7}$$

and $g(x), f(x) \in \mathbb{F}_p[x]$, $g(x) \nmid f(x)$ and $g(x)$ is of the form

$$g(x) = (x + a_1)(x + a_2) \dots (x + a_k) \tag{8}$$

with $a_i \neq a_j$ for $i \neq j$. Then defining E_p in the same way as in Theorem 1, (6) *also holds.*

2. The Eichenauer-Herrmann–Niederreiter inequality

The proofs will be based on the following variant of a result of Eichenauer-Herrmann and Niederreiter [3]:

Lemma 4. *Let p be a prime, let $Q(x), R(x) \in \mathbb{F}_p[x]$ such that $R(x) \nmid Q(x)$, and let s be the number of distinct roots of the polynomial R in $\overline{\mathbb{F}}_p$. Furthermore, let χ be a nontrivial additive character of $\mathbb{F}_p$ and $1 \leq N < p$.*

If $\deg Q \leq \deg R$, *then*

$$\left| \sum_{\substack{0 \leq n < N \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right) \right| < (\deg R + s) p^{1/2} \left(\frac{4}{\pi} \log p + 0.38 + \frac{0.64}{p} \right) + \\ + \frac{N}{p} \left((\deg R + s - 2) p^{1/2} + 1 \right),$$

and if $\deg Q > \deg R$, *then*

$$\left| \sum_{\substack{0 \leq n < N \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right) \right| < (\deg Q + s - 1) p^{1/2} \left(\frac{4}{\pi} \log p + 0.38 + \frac{0.64 + N}{p} \right).$$

It follows from these inequalities that in both cases we have:

$$\left| \sum_{\substack{0 \leq n < N \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right) \right| < 3(\max\{\deg Q, \deg R\} + s) p^{1/2} \log p.$$

The proof of the lemma is based on the Bombieri-Weil bound [2] in the following form given by Moreno and Moreno (Theorem 2 in [9]).

Lemma 5. *Let q be an arbitrary prime power, Q/R be a rational function over $\mathbb{F}_q$ which is not of the form $A^p - A$ with $A \in \overline{\mathbb{F}}_q(x)$ and p the characteristic of $\mathbb{F}_q$. Let s be the number of distinct roots of the polynomial R in $\overline{\mathbb{F}}_q$. If χ is a nontrivial additive character of $\mathbb{F}_q$, then*

$$\left| \sum_{\substack{0 \le n < N \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right) \right| \le \big(\max\{\deg Q, \deg R\} + s^* - 2\big) q^{1/2} + \delta$$

where $s^* = s$ and $\delta = 1$ if $\deg Q \le \deg R$, and $s^* = s + 1$ and $\delta = 0$ otherwise.

Now we can prove Lemma 4:

Proof of Lemma 4. Since the proof is similar to the proof of the original version of the lemma in [3], we will leave some details to the reader.

We can assume that $\deg Q, \deg R < p$ and $p > 5$ since the result is trivial otherwise. Denote the exponential sum in the lemma by S_N, then

$$S_N = \sum_{\substack{0 \le n < N \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right) = \sum_{\substack{n \in \mathbb{F}_p \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)}\right) \sum_{r=0}^{N-1} \frac{1}{p} \sum_{u=0}^{p-1} \chi(u(n-r)).$$

The absolute value of S_N can be estimated in the following way

$$|S_N| \le \frac{1}{p} \sum_{u=0}^{p-1} \left| \sum_{r=0}^{N-1} \chi(ur) \right| \left| \sum_{\substack{n \in \mathbb{F}_p \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)} + un\right) \right| + $$

$$+ \frac{N}{p} \left| \sum_{\substack{n \in \mathbb{F}_p \\ R(n) \neq 0}} \chi\left(\frac{Q(n)}{R(n)} + un\right) \right|. \qquad (9)$$

For fixed $u \in \mathbb{F}_p$ we consider the rational function

$$\frac{Q_u(x)}{R(x)} = \frac{Q(x)}{R(x)} + ux.$$

To use Lemma 5 it is sufficient to show that $Q_u(x)/R(x)$ is not of the form $A^p - A$ with $A \in \overline{\mathbb{F}}_p(x)$. Suppose that

$$\frac{Q_u}{R} = \left(\frac{K}{L}\right)^p - \frac{K}{L} \qquad (10)$$

with polynomials $K(x), L(x) \in \overline{\mathbb{F}}_p[x]$ with $\gcd(K(x), L(x)) = 1$. Then

$$L^p Q_u = (K^{p-1} - L^{p-1})KR.$$

$L^p \mid R$ by $\gcd(K(x), L(x)) = 1$. Since $\deg R < p$ then L is a nonzero constant polynomial. Thus

$$Q_u = (\alpha K^p + \beta K)R$$

some $\alpha, \beta \in \overline{\mathbb{F}}_p$ with $\alpha\beta \neq 0$. By the definition of $Q_u(x) = Q(x) + uxR(x)$ we can rewrite the previous equation in the following way:

$$Q(x) = (\alpha K^p(x) + \beta K(x) - ux)R(x).$$

Since $R(x) \nmid Q(x)$ and either $\deg(\alpha K^p(x) + \beta K(x) - ux) > p$ or $\deg(\alpha K^p(x) + \beta K(x) - ux) = 1$ (if $K(x)$ is the constant polynomial) we get that (10) cannot hold.

Thus, we can use Lemma 5 to the complete exponential sum in (9). If $\deg Q \leq \deg R$, then we have

$$|S_N| \;\leq\; \frac{1}{p}\sum_{u=0}^{p-1}\left|\sum_{r=0}^{N-1}\chi(ur)\right|(\deg R + s)p^{1/2} + \frac{N}{p}\big((\deg R + s - 2)p^{1/2} + 1\big)$$

and

$$\sum_{u=0}^{p-1}\left|\sum_{r=0}^{N-1}\chi(ur)\right| < \frac{4}{\pi}p\log p + 0.38p + 0.64.$$

This establishes the bound in the case when $\deg Q \leq \deg R$, the bound for $\deg Q > \deg R$ can be proved similarly. □

3. Proof of Theorem 1

For the proof of each theorem we will need the following result from harmonic analysis (Lemma 2 in [4]):

Lemma 6. *If $n \in \mathbb{Z}$ and p is an odd integer, then we have*

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

where $v_p(a)$ is a function of period p such that

$$v_p(0) = 1$$

and

$$v_p(a) = 1 + i\frac{(-1)^a - \cos(\pi a/p)}{\sin(\pi a/p)} \quad \text{for } 1 \leq |a| < p/2.$$

Furthermore, $v_p(a)$ satisfies

$$v_p(a) = \begin{cases} \mathcal{O}(1) & \text{if } a \text{ is even,} \\ -\frac{2p}{\pi a} i + \mathcal{O}(1) & \text{if } a \text{ is odd.} \end{cases}$$

Here we used the notation $e_p(a) = e^{2\pi i a/p}$ (and the letter i is used in the sense $\sqrt{-1}$).

We are ready to prove Theorem 1.

Proof of Theorem 1. To prove (5), consider any $a, b, t \in \mathbb{N}$ with $a \le a + (t-1)b \le p$, $b < p$. Then by Lemma 6 we get

$$U(E_p, t, a, b) = \sum_{j=0}^{t-1} e_{a+jb} =$$
$$= \frac{1}{p} \sum_{|h|<p/2} v_p(h) \left(\sum_{\substack{0 \le j \le t-1 \\ g(a+jb) \ne 0}} e_p\left(h \frac{f(a+jb)}{g(a+jb)} \right) + \mathcal{O}\left(\sum_{\substack{0 \le j \le p \\ g(a+jb)=0}} 1 \right) \right). \quad (11)$$

It follows from the condition on b that $(b, p) = 1$. Thus writing $Q(j) = f(a + jb)$ and $R(j) = g(a + jb)$, we have

$$\deg f = \deg Q \quad \text{and} \quad \deg g = \deg R.$$

For $h \ne 0$ the inner sum in (11) can been estimated by Lemma 4 with $\max\{\deg f, \deg g\} + s \le 2(\deg f + \deg g)$ (where s is the number of distinct zeros of R) :

$$|U(E_p, a, b, t)| \ll |v_p(0)| + \frac{1}{p} \sum_{1<|h|<p/2} |v_p(h)| \cdot$$
$$\cdot ((\deg f + \deg g) p^{1/2} \log p + \deg g). \quad (12)$$

By Lemma 3 we have

$$|v_p(h)| \ll \frac{p}{h}$$

uniformly for $h \ne 0$. Thus by Lemma 6, it follows from (12) that

$$\begin{aligned} |U(E_p, a, b, t)| &\ll (\deg f + \deg g) p^{1/2} \log p \sum_{1<|h|<p/2} \frac{1}{h} \ll \\ &\ll (\deg f + \deg g) p^{1/2} (\log p)^2 \end{aligned}$$

which completes the proof of Theorem 1. □

4. Proof of Theorem 2

In order to prove the theorem we will need the following lemma (Lemma 4 in [6]):

Lemma 7. *Assume that p is a prime number, $k, \ell \in \mathbb{N}$ and $k, \ell < p$. Assume also that one of the following conditions holds:*

(1) $\ell \leq 2$,

(2) $(4k)^\ell < p$.

Then for all $\mathcal{A}, \mathcal{B} \subset \mathbb{Z}_p$ with $|\mathcal{A}| = k$, $|\mathcal{B}| = \ell$, there is a $c \in \mathbb{Z}_p$ so that the equation

$$a + b = c, \quad a \in \mathcal{A}, \quad b \in \mathcal{B} \tag{13}$$

has exactly one solution in a, b.

Proof of Theorem 2. In order to prove the theorem consider any $D = (d_1, d_2, \dots, d_\ell)$ and M such that $0 \leq d_1 < d_2 < \dots < d_\ell \leq p - M$. Then by Lemma 6 we have

$$\begin{aligned} V(E_p, M, D) &= \sum_{n=1}^{M} e_{n+d_1} \dots e_{n+d_\ell} = \\ &= \frac{1}{p^\ell} \sum_{\substack{1 \leq n \leq M \\ g(n+d_1), \dots, g(n+d_\ell) \neq 0}} \prod_{i=1}^{\ell} \sum_{|h_i| < p/2} v_p(h_i) e_p\left(h_i \frac{f(n+d_i)}{g(n+d_i)}\right) + \\ &\qquad + \mathcal{O}\left(\sum_{\substack{1 \leq n \leq M \\ g(n+d_1)=0}} 1 + \dots + \sum_{\substack{1 \leq n \leq M \\ g(n+d_\ell)=0}} 1\right) \end{aligned}$$

whence, separating the contribution of the term with $h_1 = \dots = h_\ell = 0$,

$$\begin{aligned} & V(E_p, M, D) = \\ = \ & \frac{1}{p^\ell}(M + \mathcal{O}(\ell \deg g)) + \\ & + \frac{1}{p^\ell} \sum_{\substack{|h_1| < p/2 \\ (h_1, \dots, h_\ell) \neq (0, \dots, 0)}} \cdots \sum_{|h_\ell| < p/2} v_p(h_1) \dots v_p(h_\ell) \quad \cdot \end{aligned} \tag{14}$$

$$\cdot \sum_{\substack{1\le n\le M\\ g(n+d_1),\dots,g(n+d_\ell)\neq 0}} e_p\left(h_1\frac{f(n+d_1)}{g(n+d_1)}+\dots+h_\ell\frac{f(n+d_\ell)}{g(n+d_\ell)}\right)+$$
$$+\mathcal{O}(\ell\deg g)=$$
$$=\frac{1}{p^\ell}\sum_{\substack{|h_1|<p/2\\ (h_1,\dots,h_\ell)\neq(0,\dots,0)}}\cdots\sum_{|h_\ell|<p/2} v_p(h_1)\dots v_p(h_\ell)\quad\cdot$$
$$\cdot \sum_{\substack{1\le n\le M\\ g(n+d_1),\dots,g(n+d_\ell)\neq 0}} e_p\left(h_1\frac{f(n+d_1)}{g(n+d_1)}+\dots+h_\ell\frac{f(n+d_\ell)}{g(n+d_\ell)}\right)+$$
$$+\mathcal{O}(\ell\deg g).$$

Now consider one of the innermost sums (where now $(h_1,\dots,h_\ell)\neq(0,\dots,0)$), and let $h_{i_1}<\dots<h_{i_r}$ denote the h_i's with $1\le i\le \ell$, $h_i\neq 0$. Then we have

$$\sum_{\substack{1\le n\le M\\ g(n+d_1),\dots,g(n+d_\ell)\neq 0}} e_p\left(h_1\frac{f(n+d_1)}{g(n+d_1)}+\dots+h_\ell\frac{f(n+d_\ell)}{g(n+d_\ell)}\right)= \tag{15}$$
$$=\sum_{\substack{1\le n\le M\\ g(n+d_{i_1}),\dots,g(n+d_{i_r})\neq 0}} e_p\left(h_{i_1}\frac{f(n+d_{i_1})}{g(n+d_{i_1})}+\dots+h_{i_r}\frac{f(n+d_{i_r})}{g(n+d_{i_r})}\right)+$$
$$+\mathcal{O}(\ell\deg g)=$$
$$=\sum_{\substack{1\le n\le M\\ R_{h_1,\dots,h_r}(n)\neq 0}} e_p\left(\frac{Q_{h_1,\dots,h_r}(n)}{R_{h_1,\dots,h_r}(n)}\right)+\mathcal{O}(\ell\deg g)$$

with

$$Q_{h_1,\dots,h_\ell}(n)=\sum_{t=1}^{r} h_{i_t} f(n+d_{i_t})\prod_{\substack{1\le j\le r\\ j\neq t}} g(n+d_{i_j}) \tag{16}$$

and

$$R_{h_1,\dots,h_\ell}(n)=\prod_{j=1}^{r} g(n+d_{i_j})$$

so that

$$\deg Q_{h_1,\dots,h_\ell}(n)=\deg f+(r-1)\deg g\le \deg f+(\ell-1)\deg g \tag{17}$$

and

$$\deg R_{h_1,\dots,h_\ell}(n) = r\deg g \le \ell \deg g. \tag{18}$$

In order to apply the Lemma 4, we need the following result:

Lemma 8. *If p, the polynomials $f(x), g(x)$, and ℓ satisfy the assumptions in Theorem 2 then*

$$R_{h_1,\dots,h_\ell}(n) \nmid Q_{h_1,\dots,h_\ell}(n) \tag{19}$$

for $(h_1,\dots,h_\ell) \neq (0,\dots,0)$.

Then by Lemma 8 we can use Lemma 4 to estimate each of the sum (15). By (18), we obtain that uniformly in $(h_1,\dots,h_\ell) \neq (0,\dots,0)$, each of these sums is

$$\begin{aligned} &\ll (\max\{\deg Q_{h_1,\dots,h_\ell}, \deg R_{h_1,\dots,h_\ell}\} + s_{h_1,\dots,h_\ell})p^{1/2}\log p \le \\ &\le 2(\deg f + (\ell+1)\deg g)p^{1/2}\log p, \end{aligned}$$

where $s_{h_1,\dots,h_\ell}$ is the number of the distinct zeros of $R_{h_1,\dots,h_\ell}$.

Thus by Lemma 6, it follows from (14) that

$$\begin{aligned} & V(E_p, M, D) \ll \\ \ll\; & \frac{1}{p^\ell} \sum_{\substack{|h_1|<p/2 \\ (h_1,\dots,h_\ell)\neq(0,\dots,0)}} \cdots \sum_{|h_\ell|<p/2} v_p(h_1)\dots v_p(h_\ell) \cdot \\ & \cdot(\deg f + (\ell+1)\deg g)p^{1/2}\log p + \mathcal{O}(\ell \deg g) \le \\ \le\; & (\deg f + (\ell+1)\deg g)p^{1/2-\ell}\log p \left(\sum_{|h|<p/2} |v_p(h)|\right)^\ell + \\ & + \mathcal{O}(\ell\deg g) \ll \\ \ll\; & (\deg f + (\ell+1)\deg g)p^{1/2-\ell}\log p \left(1 + \sum_{0<|h|<p/2} \frac{p}{h}\right)^\ell + \\ & + \mathcal{O}(\ell\deg g) \ll \\ \ll\; & (\deg f + (\ell+1)\deg g)p^{1/2}(\log p)^{\ell+1} \end{aligned}$$

which proves (6). □

Finally, it remains to prove the lemma.

Proof of Lemma 8. We will use the approach used in [6]. We will say that the polynomials $\varphi(x), \psi(x) \in \mathbb{F}_p[x]$ are equivalent: $\varphi \sim \psi$ if there is an $a \in \mathbb{F}_p$ such that $\varphi(x+a) = \psi(x)$. Clearly, this is an equivalence relation.

Write $g(x)$ as the product of irreducible polynomials over $\mathbb{F}_p$. It follows from our assumption on $g(x)$ that these irreducible factors are distinct and co-prime to $f(x)$. Let us group these factors so that in each group the equivalent irreducible factors are collected. Consider a typical group $\varphi(x+a_1), \dots, \varphi(x+a_r)$ (where $r \le k$), and consider the polynomial

$$\phi_t(x) = \prod_{\substack{1 \le j \le r \\ j \ne t}} g(x + d_{i_j})$$

occurring in the t-th term in the definition of $Q_{h_1,\dots,h_r}(x)$, and write $\phi_t(x)$ as constant times the product of unitary irreducible polynomials. Then all polynomials $\varphi(x + a_u + d_{i_j})$ with $1 \le u \le s$, $1 \le j \le r$, $j \ne t$ will occur amongst these irreducible factors of $\phi_t(x)$. All these polynomials are equivalent, and no other irreducible factor belonging to this equivalence class will occur amongst the irreducible factors of $\phi_t(x)$.

Now set $\mathcal{A} = \{a_1, \dots, a_s\}$, $\mathcal{B} = \{d_{i_1}, \dots, d_{i_r}\}$. It follows from assumption (1) and (2) in Theorem 2 that either

$$|\mathcal{B}| = r \le \ell = 2$$

or

$$(4|\mathcal{A}|)^{|\mathcal{B}|} \le (4 \deg g(x))^{\ell} \le (4k)^{\ell} < p$$

holds, so that one of the assumptions (1) or (2) in Lemma 7 holds, and thus the lemma can be applied. We obtain that there is a $c \in \mathbb{F}_p$ so that it has exactly one representation in form (13), i.e., in form

$$a_u + d_{i_j} = c, \quad 1 \le u \le s, \quad 1 \le j \le r;$$

denote the unique u, j in this representation of c by U, resp. J. Then clearly, the J-th term in the sum (16) is not divisible by the polynomial $\varphi(n+c)$, but all the other terms in this sum are divisible by $\varphi(n+c)$. Thus their sum, $Q_{h_1,\dots,h_\ell}(n)$ is not divisible by this polynomial so it is not divisible by $R_{h_1,\dots,h_\ell}(n)$. □

5. Proof of Theorem 3

Using the notations in the proof of Theorem 2 it suffices to prove the following lemma.

Lemma 9. *If p, the polynomials $f(x), g(x)$, and ℓ satisfy the assumptions in Theorem 3 then*

$$R_{h_1,\dots,h_r}(n) \nmid Q_{h_1,\dots,h_r}(n) \tag{20}$$

for every $(h_1, \dots, h_\ell) \ne (0, \dots, 0)$ (with $|h_i| < p/2$ for $i = 1, \dots, \ell$).

To prove Lemma 9 we will need the following result of Mauduit and Sárközy (Lemma 7 in [6]).

Lemma 10. *Let $t \in \mathbb{N}$ and $L(x) \in \mathbb{F}_p$ be a nonzero polynomial of the form*

$$L(x) = \lambda_1 x^{n_1} + \lambda_2 x^{n_2} + \cdots + \lambda_t x^{n_t} \tag{21}$$

with $0 \leq n_1 < n_2 < \cdots < n_t \leq p-1$, and for a nonzero polynomial $g(x) \in \mathbb{F}_p[x]$, let $J(g(x))$ denotes the greatest nonnegative integer J with $(x-1)^J \mid g(x)$. Then we have

$$J(L(x)) \leq t-1.$$

Proof of Lemma 9. Write the rational function $f(x)/g(x)$ in the following form

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)},$$

where $q(x), r(x) \in \mathbb{F}_p[x]$ and $0 < \deg r(x) < \deg g(x)$ (since $g(x) \nmid f(x)$).

With this notation, we have

$$\begin{aligned}\frac{Q_{h_1,\dots,h_\ell}(n)}{R_{h_1,\dots,h_\ell}(n)} = \sum_{j=1}^{r} h_{i_j} \frac{f(n+d_{i_j})}{g(n+d_{i_j})} = \\ = \sum_{j=1}^{r} h_{i_j} \left(q(n+d_{i_j}) + \frac{r(n+d_{i_j})}{g(n+d_{i_j})} \right) = \\ = S_{h_1,\dots,h_\ell}(n) + \sum_{j=1}^{r} h_{i_j} \frac{r(n+d_{i_j})}{g(n+d_{i_j})} = S_{h_1,\dots,h_\ell}(n) + \frac{Q'_{h_1,\dots,h_\ell}(n)}{R_{h_1,\dots,h_\ell}(n)},\end{aligned}$$

where $S_{h_1,\dots,h_\ell}(x), Q'_{h_1,\dots,h_\ell}(n) \in \mathbb{F}_p[x]$,

$$Q'_{h_1,\dots,h_\ell}(n) = \sum_{t=1}^{r} h_{i_t} r(n+d_{i_j}) \prod_{\substack{1 \leq j \leq r \\ j \neq t}} g(n+d_{i_j}) \tag{22}$$

and

$$\deg Q'_{h_1,\dots,h_\ell}(n) < \deg R_{h_1,\dots,h_\ell}(n). \tag{23}$$

To prove that (20) holds, it suffices to show that

$$R_{h_1,\dots,h_\ell}(n) \nmid Q'_{h_1,\dots,h_\ell}(n) \tag{24}$$

or equivalently that

$$Q'_{h_1,\dots,h_\ell}(x) \neq 0 \tag{25}$$

in $\mathbb{F}_p[x]$.

To show that this holds we can use the approach developed in [6]. Namely, if p is a prime number, $\frac{u(x)}{v(x)}$ is a rational function over $\mathbb{F}_p$ with $\deg u(x) < \deg v(x)$ and $v(x)$ is of the form $v(x) = (x+a_1) \cdot \dots \cdot (x+a_z)$ with $a_i \neq a_j$ for $i \neq j$ and

$$1 \leq z = \deg v(x) < \frac{p}{2}, \tag{26}$$

then $\frac{u(x)}{v(x)}$ has a unique partial fraction decomposition of the form

$$\frac{u(n)}{v(n)} = \frac{A_1}{n+a_1} + \dots + \frac{A_z}{n+a_z}$$

over $\mathbb{F}_p$ (this holds for all n with $n \neq -a_i$ for $i = 1, \dots z$), and this can be rewritten as

$$\frac{u(n)}{v(n)} = \frac{B_0}{n} + \frac{B_1}{n+1} + \dots + \frac{B_{p-1}}{n+p-1}, \tag{27}$$

where the numbers $B_i = B_i(u(n)/v(n))$ with $0 \leq i \leq p-1$ are also unique. For such a rational function $\frac{u(x)}{v(x)}$, define the polynomial $P(x) = P(u(n)/v(n); x)$ by

$$P(x) = B_0 + B_1 x + \dots + B_{p-1} x^{p-1}. \tag{28}$$

Now assume that contrary to (25) there exist $(h_1, \dots, h_\ell) \neq (0, \dots, 0)$ such that (25) does not hold, i.e.

$$Q'_{h_1,\dots,h_\ell}(n) \equiv 0. \tag{29}$$

It follows that the partial fraction decomposition of from (27) of the rational function $Q'_{h_1,\dots,h_\ell}(n)/R_{h_1,\dots,h_\ell}(n)$ is

$$\frac{Q'_{h_1,\dots,h_\ell}(n)}{R_{h_1,\dots,h_\ell}(n)} = \sum_{j=1}^{\ell} h_i \frac{r(n+d_i)}{g(n+d_i)} = \frac{0}{n} + \frac{0}{n+1} + \dots + \frac{0}{n+p-1}.$$

The condition (26) holds by (7) so that the representation (27) is unique. It follows that

$$P\left(\sum_{j=1}^{\ell} h_i \frac{r(n+d_i)}{g(n+d_i)}; x \right) \equiv 0.$$

On the other hand

$$P\left(\sum_{j=1}^{\ell} h_i \frac{r(n+d_i)}{g(n+d_i)}; x \right) = \sum_{j=1}^{\ell} h_i P\left(\frac{r(n+d_i)}{g(n+d_i)}; x \right) \equiv$$

$$\equiv \sum_{j=1}^{\ell} h_i \left(x^{d_i} P\left(\frac{r(n)}{g(n)}; x \right) \right) = H(x) P\left(\frac{r(n)}{g(n)}; x \right) \pmod{x^p - 1}, \tag{30}$$

where

$$H(x) = \sum_{j=1}^{\ell} h_i x^{d_i}.$$

Moreover, we have $x^p - 1 = (x-1)^p$ in $\mathbb{F}_p[x]$.

It follows from (29) and (30) that (in $\mathbb{F}_p[x]$) we have

$$(x-1)^p \mid (x^p - 1) \mid H(x) P\left(\frac{r(n)}{g(n)}; x\right)$$

therefore

$$J\left(H(x) P\left(\frac{r(n)}{g(n)}; x\right)\right) \geq p. \tag{31}$$

On the other hand by the definition of the polynomial $H(x)$, it is a polynomial of form (21) with ℓ in place t, so that by Lemma 10 we get

$$J(H(x)) \leq \ell - 1. \tag{32}$$

Now consider the polynomial $P\left(\frac{r(n)}{g(n)}; x\right)$. This is a nonzero polynomial of degree at most $p-1$, and t, the number of nonzero terms of it is equal to the number of the nonzero terms of the partial fraction decomposition of type (27) of $f(n)/g(n)$ which, by (8), is now of form

$$\begin{aligned} \frac{r(n)}{g(n)} &= \frac{r(n)}{(n+a_1)(n+a_2)\dots(n+a_k)} = \\ &= \frac{A_1}{n+a_1} + \frac{A_1}{n+a_2} + \dots + \frac{A_k}{n+a_k} \end{aligned}$$

so that now $t \leq k$. Thus by Lemma 10 we have

$$J\left(P\left(\frac{r(n)}{g(n)}; x\right)\right) \leq t - 1 \leq k - 1. \tag{33}$$

It follows from (7), (32) and (33) that

$$\begin{aligned} J\left(H(x) P\left(\frac{r(n)}{g(n)}; x\right)\right) &\leq J\left(H(x)\right) + J\left(P\left(\frac{r(n)}{g(n)}; x\right)\right) \leq k + \ell - 2 \leq \\ &\leq k + \ell - 2 + (k-1)(\ell-1) = k\ell - 1 < \frac{p}{2} - 1 \end{aligned}$$

which contradicts (31). Thus, indeed, the indirect assumption (29) leads to a contradiction which completes the proof of Lemma 9. □

REFERENCES

[1] ALON, N. – KOHAYAKAWA, Y. – MAUDUIT, C. – MOREIRA, C.G. – RÖDL, V.: *Measures of pseudorandomness for finite sequences: typical values*, Proc. Lond. Math. Soc. (3) **95** (2007), no. 3, 778–812.

[2] BOMBIERI, E.: *On exponential sums in finite fields*, Amer. J. Math **88** (1966), 71–105.

[3] EICHENAUER-HERRMANN, J. – NIEDERREITER, H.: *Bounds for exponential sums and their applications to pseudorandom numbers*, Acta Arith. **67** (1994), 269–281.

[4] MAUDUIT, C. – RIVAT, J. – SÁRKÖZY, A.: *Construction of pseudorandom binary sequence using additive characters*, Monatshefte Math. **141** (2004), 197–208.

[5] GOUBIN, L. – MAUDUIT, C. – SÁRKÖZY, A.: *Construction of large families of pseudorandom binary sequences*, J. Number Theory **106** (2004), 56–69.

[6] MAUDUIT, C. – SÁRKÖZY, A.: *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. **108** (2005), 239–252.

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

[8] MAUDUIT, C. – SÁRKÖZY, A.: *On finite pseudorandom binary sequences VII: Measures of pseudorandomness*, Acta Arith. **103** (2002) 97–118.

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

Received April 19, 2008
Accepted January 28, 2009

László Mérai
Eötvös Loránd University
Department of Algebra and Number Theory
Pázmány Péter sétány 1/c
1117 Budapest
HUNGARY
E-mail: merai@cs.elte.hu