ACTA ARITHMETICA
139.3 (2009)

A construction of pseudorandom binary sequences using both additive and multiplicative characters

by

László Mérai (Budapest)

1. Introduction. In order to study the pseudorandomness of finite binary sequences, Mauduit and Sárközy introduced several definitions in [6]. 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

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

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

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

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

The sequence E_N is considered to be a "good" pseudorandom sequence if both these measures $W(E_N)$ and $C_l(E_N)$ (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, Mauduit and Sárközy [6] showed an example of a "good" pseudorandom sequence. They defined a binary sequence by putting $N = p - 1$ where p is a prime number, and

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

2000 *Mathematics Subject Classification*: Primary 11K45.

Key words and phrases: pseudorandom, binary sequence, hybrid character sum, rational function.

They proved that

$$W(E_{p-1}) \ll p^{1/2}\log p, \qquad C_l(E_{p-1}) \ll lp^{1/2}\log p.$$

Other large families of binary sequences with strong pseudorandom properties were studied in [4], [3], [5], [8], [7], [10].

In this paper a new construction of a large family of pseudorandom binary sequences is presented which uses both additive and multiplicative characters.

Let p be a prime, ψ an additive character, χ a multiplicative character in $\mathbb{F}_p$, $\alpha \in \mathbb{C}$ with $|\alpha| = 1$, and $f(x), g(x), q(x), r(x) \in \mathbb{F}_p[x]$. Let us define E_p by

$$e_n = \begin{cases} +1 & \text{if } \mathfrak{Re}\left(\alpha\psi\left(\dfrac{f(n)}{g(n)}\right)\chi\left(\dfrac{q(n)}{r(n)}\right)\right) \geq 0 \\ & \qquad\qquad \text{and } g(n), r(n), q(n) \neq 0, \\ -1 & \text{otherwise.} \end{cases} \tag{2}$$

Note that this construction generalizes several earlier ones:

Construction 1: If χ is the Legendre symbol, ψ is the trivial additive character, $\alpha = 1$, $r(x)$ is a non-zero constant polynomial, we get an extended variant of (1), studied in [3]:

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

Construction 2: If χ is a general multiplicative character, ψ is the trivial additive character, $\alpha = 1$, $r(x)$ is a non-zero constant polynomial, we get the construction studied in [8], [10], [9]:

$$e_n = \begin{cases} +1 & \text{if } \mathfrak{Re}(\chi(q(n))) \geq 0, \\ -1 & \text{otherwise,} \end{cases} \qquad \text{for } n = 1, \dots, p.$$

Construction 3: If ψ is the additive character of the form $\psi(n) = e(n/p)$ (where now $e(\alpha) = e^{2\pi i\alpha}$), χ is the trivial multiplicative character, $\alpha = i$, then we get a variant of pseudorandom sequences studied in [4], [5], [7]:

$$e_n = \begin{cases} +1 & \text{if } r_p\left(\dfrac{f(n)}{g(n)}\right) < \dfrac{p}{2} \text{ for } p \nmid g(n), \\ -1 & \text{otherwise,} \end{cases} \qquad \text{for } n = 1, \dots, p,$$

where $r_p(n)$ denotes the least non-negative residue of n modulo p.

Let us introduce the following notations: for a rational function $F(x) = f(x)/g(x)$ let $\deg F(x) = \deg f(x) - \deg g(x)$ and $\deg^* F(x) = \deg f(x) + \deg g(x)$. Finally, let us denote the algebraic closure of $\mathbb{F}_p$ by $\overline{\mathbb{F}}_p$.

THEOREM 1. *Assume that p is a prime number, χ is a non-principal multiplicative character modulo p of order d, ψ is a non-principal additive character modulo p, $\alpha \in \mathbb{C}$ with $|\alpha| = 1$, $F(x) = f(x)/g(x)$, $Q(x) = q(x)/r(x) \in \mathbb{F}_p(x)$ are rational functions such that $(g(x), f(x)) = 1$ and $(q(x), r(x)) = 1$ and neither $q(x)$ nor $r(x)$ has a multiple zero in $\overline{\mathbb{F}}_p$, and the binary sequence $E_p = \{e_1, \dots, e_p\}$ is defined by* (2). *Then*

$$W(E_p) \ll (\deg^* F + d \deg^* Q) p^{1/2} (\log p)^2. \tag{3}$$

THEOREM 2. *Let $p, F(x), Q(x)$ and E_p be as in Theorem* 1. *Assume also that $l \in \mathbb{N}$, $2 \le l < p$ and one of the following conditions holds*:

(a) $l = 2$;
(b) $(4 \deg g)^l < p$, $(4 \deg^* Q)^l < p$;
(c) $g(x) = (x + a_1) \dots (x + a_k)$ (*with $a_i \ne a_j$ for $i \ne j$*) *and* $l \deg g < p/2$, $(4 \deg^* Q)^l < p$.

Then

$$C_l(E_p) \ll (l+1)(\deg^* F + d \deg^* Q) p^{1/2} (\log p)^{l+1}. \tag{4}$$

2. On hybrid character sums. The proofs of Theorems 1 and 2 will be based on hybrid character sum estimates. For rational functions $F(x), Q(x) \in \mathbb{F}_p(x)$ denote the union of the sets of poles of $F(x)$ and $Q(x)$ by $\mathcal{S}$.

DEFINITION 3. For $F(x)$, $Q(x) \in \mathbb{F}_q(x)$ the character sum

$$\sum_{n \notin \mathcal{S}} \psi(F(n)) \chi(Q(n))$$

is *degenerate* if

$$F(x) = H(x)^p - H(x) + b \quad \text{for some } b \in \mathbb{F}_q \text{ and } H(x) \in \mathbb{F}_q(x)$$

and

$$Q(x) = bH(x)^d \quad \text{for some } b \in \mathbb{F}_q \text{ and } H(x) \in \mathbb{F}_q(x).$$

If the character sum is degenerate, then all of the terms are constant, so one cannot give a non-trivial upper bound for the sum. For non-degenerate sums Perel'muter gave a non-trivial upper bound in [11]:

THEOREM 4. *Let $\mathbb{F}_q$ be a finite field of characteristic p, χ be a non-principal multiplicative character of $\mathbb{F}_q$ of order d, and ψ be a non-principal additive character of $\mathbb{F}_q$. Let $F(x) = f(x)/g(x), Q(x) = q(x)/r(x) \in \mathbb{F}_q(x)$. Assume that the hybrid character sum is not degenerate and the following conditions hold*:

(1) *If $F = f/g_1^{\lambda_1} \dots g_r^{\lambda_r}$, where the polynomials $g_1, \dots, g_r$ are non-constants and $(g_1, \dots, g_r) = 1$ then $p \nmid \lambda_i$ when $\lambda_i > 0$ for $i = 1, \dots, r$ and $p \nmid \deg F$ when $\deg F > 0$.*
(2) *If $Q = q_1^{n_1} \dots q_u^{n_u} / r_1^{m_1} \dots r_v^{m_v}$ then $0 < n_i, m_i < d$ for all i.*

Then

$$\Big|\sum_{n\notin\mathcal{S}}\psi(F(n))\chi(Q(n))\Big| \le (d_1+d_2-2)q^{1/2}+d_1+d_2+1 \tag{5}$$

with

$$d_1=\max\{\deg f,\deg g\}+s+\lambda,\qquad d_2=\deg q+\deg r+\mu,$$

where s *is the number of distinct zeros of* g, λ *is* 0 *if* $\deg g\ge \deg f$ *and* 1 *otherwise*, μ *is* 0 *if* $d\,|\deg Q$ *and* 1 *otherwise.*

Theorem 5. *Let* p *be a prime*, *let* ψ *be a non-principal additive character of* $\mathbb{F}_p$, *and* χ *a non-principal multiplicative character of* $\mathbb{F}_p$ *of order* d. *Furthermore*, *let* $F=f/g$, $Q=q/r$ *be non-zero rational functions over* $\mathbb{F}_p$, *and let* s *be the number of distinct zeros of* g *in* $\overline{\mathbb{F}}_p$. *Suppose that* $g(x)\nmid f(x)$ *and* $Q(x)$ *is not of the form* $bB(x)^d$ *for any* $b\in\mathbb{F}_p$ *and* $B(x)\in\mathbb{F}_p(x)$. *If* $1\le N<p$ *then*

$$\Big|\sum_{\substack{0\le n<N\\ n\notin\mathcal{S}}}\psi(F(n))\chi(Q(n))\Big| \le 3(\max\{\deg f,\deg g\}+s+\deg q+\deg r)p^{1/2}\log p. \tag{6}$$

Proof. We can assume that the degrees of all the polynomials are less than p since the result is trivial otherwise.

It follows from the basic properties of additive characters that

$$\sum_{r=0}^{N-1}\frac{1}{p}\sum_{u=0}^{p-1}\psi(u(n-r))=\begin{cases}1 & \text{if } 0\le n<N,\\ 0 & \text{otherwise.}\end{cases}$$

Let us denote the character sum in (6) by S_N. We have

$$\begin{aligned} S_N &= \sum_{n\notin\mathcal{S}}\psi(F(n))\chi(Q(n))\sum_{r=0}^{N-1}\frac{1}{p}\sum_{u=0}^{p-1}\psi(u(n-r))\\ &=\frac{1}{p}\sum_{u=0}^{p-1}\Big(\sum_{r=0}^{N-1}\psi(-ur)\Big)\Big(\sum_{n\notin\mathcal{S}}\psi(F(n)+un)\chi(Q(n))\Big)\\ &=\frac{1}{p}\sum_{u=1}^{p-1}\Big(\sum_{r=0}^{N-1}\psi(-ur)\Big)\Big(\sum_{n\notin\mathcal{S}}\psi(F(n)+un)\chi(Q(n))\Big)\\ &\quad+\frac{N}{p}\sum_{n\notin\mathcal{S}}\psi(F(n))\chi(Q(n))\end{aligned}$$

and so

$$|S_N| \le \frac{1}{p}\sum_{u=1}^{p-1}\Big|\sum_{r=0}^{N-1}\psi(ur)\Big|\,\Big|\sum_{n\notin\mathcal{S}}\psi(F(n)+un)\chi(Q(n))\Big| + \frac{N}{p}\Big|\sum_{n\notin\mathcal{S}}\psi(F(n))\chi(Q(n))\Big|. \tag{7}$$

For a fixed u we consider the rational function

$$F_u(x) = F(x) + ux = \frac{f(x)}{g(x)} + ux.$$

To show that $F_u(x)$ satisfies the conditions of Theorem 4, it suffices to prove that $F_u(x)$ is not of the form $A(x)^p - A(x)$ with $A(x) \in \overline{\mathbb{F}}_p(x)$. Suppose that

$$F_u(x) = \left(\frac{K(x)}{L(x)}\right)^p - \frac{K(x)}{L(x)} \tag{8}$$

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

$$L(x)^p(f(x) + uxg(x)) = (K(x)^{p-1} - L(x)^{p-1})K(x)g(x),$$

so $L(x)^p \mid g(x)$ as $(K(x), L(x)) = 1$. Since $\deg g(x) < p$, it follows that $L(x)$ is a nonzero constant polynomial. Thus we get

$$f(x) + uxg(x) = (\alpha K(x)^p + \beta K(x))g(x),$$

and hence

$$f(x) = (\alpha K(x)^p + \beta K(x) - ux)g(x),$$

for some $\alpha, \beta \in \overline{\mathbb{F}}_p$ with $\alpha\beta \ne 0$.

Since $g(x) \nmid f(x)$ and either

$$\deg(\alpha K(x)^p + \beta K(x) - ux) > p$$

or

$$\deg(\alpha K(x)^p + \beta K(x) - ux) = 1$$

we see that (8) cannot hold.

Since $F(x) + ux$, $F(x)$ and $Q(x)$ satisfy the conditions of Theorem 4, we deduce from (7) that

$$|S_N| \le \frac{1}{p}\Big(\sum_{u=1}^{p-1}\Big|\sum_{r=0}^{N-1}\psi(ur)\Big| + N\Big) \cdot 2(\max\{\deg f, \deg g\} + s + \deg q + \deg r)p^{1/2}$$

and

$$\sum_{u=0}^{p-1}\Big|\sum_{r=0}^{N-1}\psi(ur)\Big| < \frac{4}{\pi}\,p\log p + 0.38p + 0.64,$$

by Theorem 1 in [2]. ∎

3. The well-distribution measure. To express the terms of E_p, we will need the generalization of Lemma 2 in [4].

LEMMA 6. *Let $m \in \mathbb{N}$, and let ε be an mth root of unity. Then*

$$\frac{1}{m} \sum_{-[m/2]<a\le[m/2]} v_m(a)\varepsilon^a = \begin{cases} +1 & \text{if } -\pi/2 \le \arg(\varepsilon) < \pi/2, \\ -1 & \text{otherwise}, \end{cases}$$

where $v_m(a)$ is a function of period m such that $v_m(0) = 1$, and if m is odd, then

$$v_m(a) = i^a\left(1 + i\,\frac{(-1)^a - \cos(\pi a/m)}{\sin(\pi a/m)}\right) \qquad \text{if } 1 \le |a| < m/2,$$

while if m is even, then

$$v_m(a) = \begin{cases} 0 & \text{if } a \text{ is even} \\ i^a\left(2 - 2i\,\dfrac{\cos(a\pi/m)}{\sin(a\pi/m)}\right) & \text{if } a \text{ is odd} \end{cases} \qquad \text{if } 1 \le |a| \le m/2.$$

Furthermore, in both cases, $v_m(a) \ll m/a$ if $a \ne 0$.

Proof. For m odd, the statement has been proved in [4]; for m even the proof is similar. ∎

Proof of Theorem 1. To prove the desired inequality, consider $a \in \mathbb{Z}$ and $b, t \in \mathbb{N}$ such that

$$1 \le a \le a + (t-1)b \le p, \qquad b < p. \tag{9}$$

Then by Lemma 6 we have

$$\begin{aligned} U(E_p, t, a, b) &= \sum_{j=0}^{t-1} e_{a+jb} \\ &= \frac{1}{dp} \sum_{-[dp/2]<h\le[dp/2]} v_{dp}(h)\alpha^h \\ &\quad \cdot \Bigg(\sum_{\substack{0\le j\le t-1 \\ a+jb\notin\mathcal{S}}} \psi(F(a+jb))^h \chi(Q(a+jb))^h + \mathcal{O}\Big(\sum_{\substack{0\le j\le p \\ a+jb\in\mathcal{S}}} 1\Big)\Bigg) + \mathcal{O}(\deg f) \\ &= \frac{1}{dp} \sum_{-[dp/2]<h\le[dp/2]} v_{dp}(h)\alpha^h \Bigg(\sum_{\substack{0\le j\le t-1 \\ a+jb\notin\mathcal{S}}} \psi(F(a+jb))^h \chi(Q(a+jb))^{r_d(h)} \Bigg) \\ &\quad + \mathcal{O}(|\mathcal{S}|) + \mathcal{O}(\deg f), \end{aligned}$$

since $\chi(Q(n))^h = \chi(Q(n))^{r_d(h)}$ for $n \in \mathbb{F}_p$.

If $0 < |h| \le dp/2$ then $h \nmid p$ or $h \nmid d$ (and so $r_d(h) \nmid d$), thus the hybrid character sums are not degenerate. Furthermore,

$$\max\{\deg f, \deg g\} + s \le 2(\deg f + \deg g)$$

and

$$\deg^* Q^{r_d(h)} = r_d(h) \deg^* Q \le d \deg^* Q,$$

thus by Theorem 5 we have

$$\begin{aligned}
|U(E_p,t,a,b)| &= \Big|\sum_{j=0}^{t-1} e_{a+jb}\Big| \\
&\le \frac{1}{dp} \sum_{\substack{-[dp/2]<h\le[dp/2]\\ h\ne 0}} |v_{dp}(h)| \Big| \sum_{\substack{0\le j\le t-1\\ a+jb\notin\mathcal{S}}} \psi(F(a+jb))^h \chi(Q(a+jb))^{r_d(h)}\Big| \\
&\quad + |v_{dp}(0)| + \mathcal{O}(|\mathcal{S}|) + \mathcal{O}(\deg f) \\
&\ll \frac{1}{dp} \sum_{\substack{-[dp/2]<h\le[dp/2]\\ h\ne 0}} |v_{dp}(h)|(\deg^* F + \deg^* Q^{r_d(h)}) p^{1/2} \log p + |v_{dp}(0)| \\
&\ll (\deg^* F + \deg^* Q^{r_d(h)}) p^{1/2} \log p \sum_{\substack{-[dp/2]<h\le[dp/2]\\ h\ne 0}} \frac{1}{|h|} \\
&\ll (\deg^* F + d \deg^* Q) p^{1/2} (\log p)^2. \ \blacksquare
\end{aligned}$$

4. The correlation measure

Proof of Theorem 2. Consider any $M < p$ and $D = (d_1, \dots, d_l)$ such that $0 \le d_1 < \dots < d_l \le p - M$. Then

$$\begin{aligned}
V(E_p, M, D) &= \sum_{n=1}^{M} e_{n+d_1} \dots e_{n+d_l} \\
&= \frac{1}{(dp)^l} \sum_{\substack{1\le n\le M\\ n+d_1,\dots,n+d_l\notin\mathcal{S}}} \prod_{i=1}^{l} \sum_{-[dp/2]<h_i\le[dp/2]} v_{dp}(h_i) \\
&\quad \cdot \alpha^{h_i} (\psi(F(n+d_i))\chi(Q(n+d_i)))^{h_i} \\
&\quad + \mathcal{O}\Big(\sum_{\substack{1\le n\le M\\ n+d_1\in\mathcal{S}}} 1 + \dots + \sum_{\substack{1\le n\le M\\ n+d_l\in\mathcal{S}}} 1 \Big) + \mathcal{O}(l \deg f),
\end{aligned}$$

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

$$V(E_p, M, D) = \frac{1}{(dp)^l}\left(M + \mathcal{O}(|\mathcal{S}|l)\right) \tag{10}$$

$$+ \frac{1}{(dp)^l} \underset{(h_1,\dots,h_l)\neq(0,\dots,0)}{\sum_{-[dp/2]<h_1\leq[dp/2]} \cdots \sum_{-[dp/2]<h_l\leq[dp/2]}} v_{dp}(h_1)\dots v_{dp}(h_l) \prod_{i=1}^{l} \alpha^{h_i}$$

$$\cdot \sum_{\substack{1\leq n\leq M \\ n+d_1,\dots,\, n+d_l\notin\mathcal{S}}} \prod_{i=1}^{l} (\psi(F(n+d_i))\chi(Q(n+d_i)))^{h_i}$$

$$+ \mathcal{O}(|\mathcal{S}|l) + \mathcal{O}(l \deg f).$$

Now consider one of the innermost sums (where $(h_1, \dots, h_l) \neq (0, \dots, 0)$), and let $h_{i_1} < \dots < h_{i_r}$ be the non-zero h_i's. Then

$$\sum_{\substack{1\leq n\leq M \\ n+d_1,\dots,\, n+d_l\notin\mathcal{S}}} \prod_{i=1}^{l} (\psi(F(n+d_i))\chi(Q(n+d_i)))^{h_i} \tag{11}$$

$$= \sum_{\substack{1\leq n\leq M \\ n+d_1,\dots,\, n+d_l\notin\mathcal{S}}} \psi\Big(\sum_{i=1}^{l} h_i F(n+d_i)\Big)\chi\Big(\prod_{i=1}^{l} Q(n+d_i)^{h_i}\Big)$$

$$= \sum_{\substack{1\leq n\leq M \\ n+d_{i_1},\dots,\, n+d_{i_r}\notin\mathcal{S}}} \psi\Big(\sum_{j=1}^{r} h_{i_j} F(n+d_{i_j})\Big)\chi\Big(\prod_{j=1}^{r} Q(n+d_{i_j})^{r_d(h_{i_j})}\Big)$$

$$= \sum_{\substack{1\leq n\leq M \\ n+d_{i_1},\dots,\, n+d_{i_r}\notin\mathcal{S}}} \psi\left(\frac{f_{h_1,\dots,h_l}(n)}{g_{h_1,\dots,h_l}(n)}\right)\chi\left(\frac{q_{h_1,\dots,h_l}(n)}{r_{h_1,\dots,h_l}(n)}\right)$$

with

$$f_{h_1,\dots,h_l}(x) = \sum_{t=1}^{r} h_{i_t} f(x+d_{i_t}) \prod_{\substack{1\leq j\leq r \\ j\neq t}} g(x+d_{i_j}),$$

$$g_{h_1,\dots,h_l}(x) = \prod_{j=1}^{r} g(x+d_{i_j}),$$

$$q_{h_1,\dots,h_l}(x) = \prod_{j=1}^{r} q(x+d_{i_j})^{r_d(h_{i_j})},$$

$$r_{h_1,\dots,h_l}(x) = \prod_{j=1}^{r} r(x+d_{i_j})^{r_d(h_{i_j})},$$

so that

$$\begin{aligned}\deg f_{h_1,\dots,h_l} &\le \deg f + (r-1)\deg g \le \deg f + (l-1)\deg g,\\ \deg g_{h_1,\dots,h_l} &= r\deg g \le l\deg g,\\ \deg^*\left(\frac{q_{h_1,\dots,h_l}}{r_{h_1,\dots,h_l}}\right) &\le \sum_{j=1}^{r} r_d(h_{i_j})\deg^* Q \le ld\deg^* Q.\end{aligned}$$

In order to give an upper bound for the character sum in (11), we have to show that this sum is not degenerate for every $(h_1,\dots,h_l) \ne (0,\dots,0)$.

First, suppose that $p \nmid h_{i_j}$ for all $j = 1,\dots,r$. The following lemma (Lemmas 8 and 9 in [7]) shows that the character sum is not degenerate.

Lemma 7. *If p, $f(x), g(x)$ and l satisfy the conditions in Theorem 2 and $p \nmid h_{i_j}$ for $j = 1,\dots,r$, then $g_{h_1,\dots,h_l}(x) \nmid f_{h_1,\dots,h_l}(x)$.*

By the lemma, from (11) we have

$$(12)\quad \Bigg|\sum_{\substack{1\le n\le M\\ n+d_{i_1},\dots,n+d_{i_r}\notin\mathcal{S}}} \psi\left(\frac{f_{h_1,\dots,h_l}(n)}{g_{h_1,\dots,h_l}(n)}\right)\chi\left(\frac{q_{h_1,\dots,h_l}(n)}{r_{h_1,\dots,h_l}(n)}\right)\Bigg|$$
$$\le 3\left(\deg^*\left(\frac{f_{h_1,\dots,h_l}}{g_{h_1,\dots,h_l}}\right) + \deg^*\left(\frac{q_{h_1,\dots,h_l}}{r_{h_1,\dots,h_l}}\right)\right)p^{1/2}\log p$$
$$\le 3(l+1)(\deg^* F + d\deg^* Q)p^{1/2}\log p,$$

since

$$\begin{aligned}\max\{\deg f_{h_1,\dots,h_l}, \deg g_{h_1,\dots,h_l}\} + s_{h_1,\dots,h_l} &\le \deg f + (l+1)\deg g\\ &\le (l+1)\deg^* F\end{aligned}$$

where $s_{h_1,\dots,h_l}$ is the number of distinct zeros of $g_{h_1,\dots,h_l}$.

On the other hand, if there are some h_{i_j} such that $p \mid h_{i_j}$, then $d \nmid h_{i_j}$ since $0 < |h_{i_j}| \le [dp/2]$. Let

$$q'_{h_1,\dots,h_l}(x) = \prod_{\substack{j=1\\ d\nmid h_{i_j}}}^{r} q(x+d_{i_j})^{r_d(h_{i_j})}, \qquad r'_{h_1,\dots,h_l}(x) = \prod_{\substack{j=1\\ d\nmid h_{i_j}}}^{r} r(x+d_{i_j})^{r_d(h_{i_j})}.$$

From the assumption, none of these polynomials is constant. Thus it is enough to prove the following lemma:

Lemma 8. *If p, $q(x), r(x)$ and l satisfy the conditions in Theorem 2 and there exists an index j such that $d \nmid h_{i_j}$, then*

$$\frac{q'_{h_1,\dots,h_l}(x)}{r'_{h_1,\dots,h_l}(x)} = bB(x)^d$$

for no $b \in \mathbb{F}_p$ and $B(x) \in \mathbb{F}_p(x)$.

In order to prove this, we will need the following lemma from [5].

Lemma 9. *Assume that p is a prime number, $k,l \in \mathbb{N}$ and $k,l < p$. Assume also that one of the following conditions holds*:

(1) $l \le 2$,
(2) $(4k)^l < p$.

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

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

has exactly one solution in a, b.

Proof of Lemma 8. We use the approach developed in [3]. We say that $\varrho(x), \sigma(x) \in \mathbb{F}_p[x]$ are equivalent, $\sigma \sim \varrho$, if there is an $a \in \mathbb{F}_p$ such that $\varrho(x+a) = \sigma(x)$. Clearly, this is an equivalence relation.

Write $q(x)$ and $r(x)$ as the product of irreducible polynomials over $\mathbb{F}_p$. It follows from our assumption on the polynomials that all of these irreducible factors are distinct. Let us divide these factors into groups of equivalent factors. A typical group has the following form: $\varrho(x+a_1), \dots, \varrho(x+a_u)$ (where $u \le \deg q$) belong to $q(x)$, and $\varrho(x+b_1), \dots, \varrho(x+b_v)$ (where $v \le \deg r$) belong to $r(x)$, where the constants a_i, b_j are distinct by assumption.

By the definition of $q'_{h_1,\dots,h_l}$ and $r'_{h_1,\dots,h_l}$ the factors occurring in the polynomials for a given group have the following form: $\varrho(x + a_t + d_{i_j})$ for $t = 1, \dots, u$ and $j = 1, \dots, r$ and $\varrho(x + b_z + d_{i_j})$ resp. All these polynomials are equivalent, and no other irreducible factor belongs to this equivalence class.

Now set $\mathcal{A} = \{a_1, \dots, a_u, b_1, \dots, b_v\}$, $\mathcal{B} = \{d_{i_1}, \dots, d_{i_r}\}$. It follows from assumption of Theorem 2 that either

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

or

$$(4|\mathcal{A}|)^{|\mathcal{B}|} \le (4(\deg q + \deg r))^l \le (4 \deg^* Q)^l < p,$$

so that one of the assumptions (1) or (2) in Lemma 9 holds, and thus the lemma can be applied. Hence there is a $c \in \mathbb{F}_p$ that has exactly one representation (13). Thus either $\varrho(x+c) \nmid q'_{h_1,\dots,h_l}(x)$ or $\varrho(x+c) \nmid r'_{h_1,\dots,h_l}(x)$, so

$$\varrho(x+c) \mid q'_{h_1,\dots,h_l}(x) (r'_{h_1,\dots,h_l}(x))^{d-1}$$

but

$$(\varrho(x+c))^d \nmid q'_{h_1,\dots,h_l}(x) (r'_{h_1,\dots,h_l}(x))^{d-1}. \ \blacksquare$$

By Lemma 8 the character sum in (12) is not degenerate, so the inequality also holds if there are some h_{i_j} such that $p \mid h_{i_j}$.

Thus (10) and (12) yield

$$
\begin{aligned}
&|V(E_p, M, D)| \\
&\quad \ll \frac{1}{(dp)^l}\Big| \sum_{-[dp/2]<h_1\le[dp/2]} \cdots \sum_{\substack{-[dp/2]<h_l\le[dp/2] \\ (h_1,\dots,h_l)\neq(0,\dots,0)}} v_{dp}(h_1)\dots v_{dp}(h_l)\Big| \\
&\qquad \cdot \Big| \sum_{\substack{1\le n\le M \\ n+d_1,\dots,n+d_l\notin\mathcal{S}}} \psi\Big(\prod_{i=1}^{l} h_i F(n+d_i)\Big)\chi\Big(\sum_{i=1}^{l} Q(n+d_i)^{h_i}\Big)\Big| \\
&\qquad + \mathcal{O}(|\mathcal{S}|l) + \mathcal{O}(l\deg f) \\
&\quad \ll \frac{1}{(dp)^l}(l+1)(\deg^* F + d\deg^* Q)p^{1/2}\log p\Big(\sum_{|h|<dp/2}|v_{dp}(h)|\Big)^l \\
&\qquad + \mathcal{O}(|\mathcal{S}|l) + \mathcal{O}(l\deg f) \\
&\quad \ll \frac{1}{(dp)^l}(l+1)(\deg^* F + d\deg^* Q)p^{1/2}\log p\Big(1 + \sum_{0<|h|<dp/2}\frac{dp}{h}\Big)^l \\
&\qquad + \mathcal{O}(|\mathcal{S}|l) + \mathcal{O}(l\deg^* Q) \\
&\quad \ll (l+1)(\deg^* F + d\deg^* Q)p^{1/2}(\log p)^{l+1},
\end{aligned}
$$

which completes the proof of Theorem 2. ∎

References

[1] N. Alon, Y. Kohayakawa, C. Mauduit, C. G. Moreira and V. Rödl, *Measures of pseudorandomness for finite sequences: typical values*, Proc. London Math. Soc. (3) 95 (2007), 778–812.

[2] T. Cochrane, *On a trigonometric inequality of Vinogradov*, J. Number Theory 27 (1987), 9–16.

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

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

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

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

[7] L. Mérai, *A construction of pseudorandom binary sequences using rational functions*, Uniform Distribution, to appear.

[8] —, *Construction of large families of pseudorandom binary sequences*, Ramanujan J., to appear.

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

[10] S. M. Oon, *On pseudo-random properties of certain Dirichlet series*, Ramanujan J. 15 (2008), 19–30.

[11] G. I. Perel'muter, *On certain character sums*, Uspekhi Mat. Nauk 18 (1963), no. 2, 145–149.

Department of Algebra and Number Theory
Eötvös Loránd University
Pázmány Péter Sétány 1/c
1117 Budapest, Hungary
E-mail: merai@cs.elte.hu

Received on 18.8.2008
and in revised form on 13.2.2009 (5778)