Periodica Mathematica Hungarica Vol. 49 (2), 2004, pp. 45–63

ON A FAMILY OF PSEUDORANDOM BINARY SEQUENCES

KATALIN GYARMATI (Budapest)

[Communicated by: Attila Pethő]

Abstract

Recently, numerous constructions have been given for finite pseudorandom binary sequences. However, in many applications, e.g., in cryptography one needs "large" families of "good" pseudorandom sequences. Very Recently L. Goubin, C. Mauduit, A. Sárközy succeeded in constructing large families of pseudorandom binary sequences based on the Legendre symbol. In this paper we will generate another type of large family of pseudorandom sequences by using the notion of index (discrete logarithm).

1. Introduction

In a series of papers C. Mauduit and A. Sárközy (partly with coauthors) studied finite pseudorandom binary sequences

$$E_N = \{e_1, e_2, \dots, e_N\} \in \{-1, +1\}^N.$$

In particular, in Part I [6] first they introduced the following measures of pseudorandomness:

Write

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

and, for $D = (d_1, \dots, d_k,)$ with non-negative integers $d_1 < \cdots < d_k$,

$$V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2}, \dots e_{n+d_k}.$$

Mathematics subject classification number: 11K45.

Key words and phrases: pseudorandom, index, discrete logarithm, correlation, linear complexity.

Research partially supported by Hungarian National Foundation for Scientific Research, Grants OTKA T043631 and T043623.

0031-5303/2004/$20.00

Akadémiai Kiadó, Budapest
Kluwer Academic Publishers, Dordrecht

Then the *well-distribution measure* of E_N is defined as

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

where the maximum is taken over all a, b, t such that $a, b, t \in \mathbb{N}$ and $1 \le a \le a + (t-1)b \le N$, while 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 $D=(d_1, d_2, \dots, d_k)$ and M such that $M+d_k \le N$.

Then 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 of N (in particular, both are $o(N)$ as $N \to \infty$).

Moreover it was shown in [6] that the Legendre symbol forms a "good" pseudorandom sequence. More exactly, let p be an odd prime, and

$$N = p - 1, \quad e_n = \left(\frac{n}{p}\right), \quad E_N = \{e_q, \dots, e_N\}. \tag{1}$$

Then by Theorem 1 in [6] we have

$$W(E_N) \ll p^{1/2} \log p \ll N^{1/2} \log N$$

and

$$C_k(E_N) \ll k p^{1/2} \log p \ll k N^{1/2} \log N.$$

In [5] was introduced the *symmetry measure* of E_N:

$$S(E_N) = \max_{a<b} \left| \sum_{j=0}^{[(b-a)/2]-1} e_{a+j} e_{b-j} \right| = \max_{a<b} |H(E_N, a, b)|.$$

In [5] it was also shown that for the half of the Legendre symbol sequence, i.e., for the sequence

$$E_{(p-1)/2} = \left\{ \left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \dots, \left(\frac{(p-1)/2}{p}\right) \right\},$$

where p is an odd prime, we have

$$S(E_{(p-1)/2}) \le 18 p^{1/2} \log p.$$

Numerous other binary sequence have been tested for pseudorandomness by J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy. However, these constructions produce only "few" pseudorandom sequences, while in many applications, e.g., in cryptography one needs "large" families of "good" pseudorandom sequences. Very recently L. Goubin, C. Mauduit and A. Sárközy [4] succeeded in constructing large families of pseudorandom binary sequences, generalizing the construction (1). Their most important results can be summarized as follows:

THEOREM 1. *If p is a prime number, $f(x) \in F_p[x]$ (F_p being the field of the modulo p residue classes) has degree $k > 0$ and no multiple zero in $\overline{F_p}$ (=the algebraic closure of F_p), and the binary sequence $E_p = \{e_q, \dots, e_p\}$ is defined by*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{for } (f(n), p) = 1 \\ +1 & \text{for } p \mid f(n), \end{cases} \tag{2}$$

then we have

$$W(E_p) < 10kp^{1/2} \log p.$$

Moreover, assume that for $\ell \in \mathbb{N}$ one of the following assumption holds:

(i) $\ell = 2$;
(ii) $\ell < p$ *and 2 is a primitive root modulo* p;
(iii) $(4k)^\ell < p$.

Then we also have

$$C_\ell(E_p) < 10k\ell p^{1/2} \log p.$$

This theorem generates "large" families of "good" pseudorandom binary sequences. However, in most applications it is also very important that the "large" family $\mathcal{F}$ of "good" pseudorandom sequences had a "complex" structure, there are many "independent" sequences in it. In [1] a quantitative measure for this property of families of binary sequences was introduced.

DEFINITION 1. The complexity $C(\mathcal{F})$ of a family $\mathcal{F}$ of binary sequence $E_N \in \{-1, +1\}^N$ is defined as the greatest integer j so that for any $1 \le i_1 < i_2 < \cdots < i_j \le N$, and for $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_j \in \{-1, +1\}^j$, we have at least one $E_N = \{e_1, \dots, e_N\} \in \mathcal{F}$ for which

$$e_{i_1} = \varepsilon_1,\ e_{i_2} = \varepsilon_2, \dots,\ e_{i_j} = \varepsilon_j.$$

It is clear from Definition 1 that for $j < C(\mathcal{F})$, there exist at least $2^{C(\mathcal{F})-j}$ sequence $E_N \in \mathcal{F}$ with

$$e_{i_1} = \varepsilon_1,\ e_{i_2} = \varepsilon_2, \dots,\ e_{i_j} = \varepsilon_j.$$

In [1] it was also proved that the complexity measure of the family of the sequence E_p defined by (2) is large. More precisely: consider all the polynomials $f(x) \in F_p[x]$ with

$$0 < \deg f(x) \le K$$

(where $\deg f(x)$ denotes the degree of $f(x)$) and $f(x)$ has no multiple zero in F_p. For each of these polynomials $f(x)$, consider the binary sequence $E_p = E_p(f) = \{e_1 \dots, e_p\} \in \{-1, +1\}^p$ defined by (2), and let $\mathcal{F}$ denote the family of all binary sequences obtained in this way. Then we have

$$C(\mathcal{F}) > K.$$

In this paper, extending a construction given by A. Sárközy in [9], we will generate a large family of pseudorandom sequences based on the notion of the index (discrete logarithm). The following pseudorandom sequence was introduced and studied in [9].

If p is a fixed prime and g is a fixed primitive root modulo p, and $(a,p)=1$, then let $\operatorname{ind} a$ denote the (modulo p) index of a (to the base g) so that

$$g^{\operatorname{ind} a} \equiv a \pmod p,$$

and to make the value of index unique, we may add the condition

$$1 \le \operatorname{ind} a \le p-1.$$

Write $N=p-1$ and define the sequence $E_N=\{e_, \dots, e_N\}$ by

$$e_n = \begin{cases} +1 & \text{if } 1 \le \operatorname{ind} n \le (p-1)/2 \\ -1 & \text{if } (p+1)/2 \le \operatorname{ind} n \le p-1. \end{cases}$$

Then we have

$$W(E_p) < 4p^{1/2}(\log p)^2 < 20N^{1/2}(\log N)^2$$

and, for all $k \in \mathbb{N}$, $k<p$,

$$C_k(E_N) < 9k4^k p^{1/2}(\log p)^{k+1} < 27k8^k N^{1/2}(\log N)^{k+1}.$$

We will generate a large family of pseudorandom sequences analogously to Theorem 1, i.e. replacing n by $f(n)$.

DEFINITION 2. Let p be an odd prime, g a primitive root modulo p. Define $\operatorname{ind} n$, by $1 \le \operatorname{ind} n \le p-1$ and $n \equiv g^{\operatorname{ind} n} \pmod p$. Let $f(x) \in F[p]$ be a polynomial of the degree k. Then define the sequence $E_{p-1}=\{e_1,\dots,e_{p-1}\}$ by

$$e_n = \begin{cases} +1 & \text{if } 1 \le \operatorname{ind} f(n) \le (p-1)/2 \\ -1 & \text{if } (p+1)/2 \le \operatorname{ind} f(n) \le p-1 \text{ or } p \mid f(n). \end{cases} \tag{3}$$

This paper is devoted to the study of family described in Definition 2. Throughout this paper we will use these notations: the numbers p, k, g the polynomial f and the sequence E_{p-1} will be defined as in Definition 2. First we give estimates for the well-distribution measure, the correlation measure and the symmetry measure of the sequence E_{p-1}.

THEOREM 2. *For all $f(x) \in F_p[x]$ we have*

$$W(E_{p-1}) < 38kp^{1/2}(\log p)^2.$$

Unlike the corresponding part of Theorem 1, here in Theorem 2 there is no condition on the roots of the polynomial $f(x)$. The case of the correlation measure will be slightly more difficult. As in Theorem 1, the upper bound holds under certain assumptions. The last two conditions are very similar to the conditions of Theorem 1, since these theorems are based on a similar addition lemma.

THEOREM 3. *Suppose that at least one of the following 4 condition holds:*

a) *f is irreducible.*

b) *If f has the factorization $f = \varphi_1^{\alpha_1}\varphi_2^{\alpha_2}\dots\varphi_u^{\alpha_u}$ where $\alpha_i \in \mathbb{N}$ and φ_i is irreducible over F_p, then there exists a β such that exactly one or two φ_i's have the degree β;*

c) *$\ell = 2$;*

d) *$(4\ell)^k < p$ or $(4k)^\ell < p$.*

Then $C_\ell(E_{p-1}) < 10k\ell 4^\ell p^{1/2}(\log p)^{\ell+1}$.

Clearly, condition b) implies condition a); however, the proof in case a) is simpler, and all the other cases will follow from it in several steps.

Next we will study the symmetry measure.

THEOREM 4. *Let $f(x) = a_k x^k + a_{k-1}x^{k-1} + \dots + a_0$, $a_k \not\equiv 0 \pmod p$, $k < p$, and define t by*

$$ka_k t \equiv -2a_{k-1} \pmod p.$$

Let

$$E'_{v-u+1} = \{e_u, e_{u+1}, \dots, e_v\} \subseteq E_p$$

where e_i was defined in Definition 2. If $t < 2u$ or $t > 2v$ or $f(x) \not\equiv \pm f(t-x)$, then

$$S(E'_{v-u+1}) < 88kp^{1/2}(\log p)^3.$$

Suppose that $f(x) \equiv \pm f(t'-x)$ for some t'. Considering the coefficients of x^k and x^{k-1} in $f(x)$ and $f(t'-x)$ we get

$$kt'a_k \equiv -2a_{k-1} \pmod p.$$

Thus it follows from $f(x) \equiv \pm f(t'-x) \pmod p$ that $t' \equiv t \pmod p$.

It is trivial from the definition of the e_i's, that in the case of $f(x) \equiv \pm f(t-x) \pmod p$ we have

$$H(E'_{v-u+1}, u, t-u) = \lceil (t-2u)/2 \rceil \quad \text{if } t \le u+v,$$

and

$$H(E'_{v-u+1}, t-v, v) = \lceil (2v-t)/2 \rceil \quad \text{if } t > u+v.$$

Therefore $S(E'_{v-u+1}) \gg \min\{t-2u, 2v-t\}$. So the condition of Theorem 4 is necessary apart from an additional term $O\big(p^{1/2}(\log p)^3\big)$, i.e., the conclusion of the

theorem fails if the inequalities $t < 2u$, $t > v$ are replaced by $t < 2u + c_1 p^{1/2}(\log p)^3$, $t > 2v - c_1 p^{1/2}(\log p)^3$, where c_1 is a large enough constant.

REMARK 1. All these theorems are trivial if $k \geq p^{1/2}$, thus throughout the paper we will assume that $k < p^{1/2}$.

Finally we will study the complexity measure of the family of pseudorandom sequences defined by (3).

THEOREM 5. *Consider all the polynomials $f(x) \in F_p[x]$ with*

$$0 < \deg f(x) \leq K.$$

For each of these polynomials $f(x)$, consider the binary sequence $E_p = E_p(f)$ defined by (3), and let $\mathcal{F}$ denote the family of all binary sequences obtained in this way. Then we have

$$C(\mathcal{F}) > K.$$

2. Proofs

PROOF OF THEOREM 1. We will need the following lemmas:

LEMMA 1. *Let $f(x)$ be a polynomial in $F_p[x]$, and let d be a divisor of $p-1$. The following 3 conditions are equivalent:*

(i) $f(x) = b\,(z(x))^d$ *with* $b \in F_p$, $z(x) \in F_p[x]$,
(ii) $f(x) = (h(x))^d$ *with* $h(x) \in \overline{F}_p[x]$,
(iii) $f(x) = b(x-x_1)^{\alpha_1}(x-x_2)^{\alpha_2}\dots(x-x_s)^{\alpha_s}$ *with* $x_i \in \overline{F}_p$ *and* $d \,|\, (\alpha_1, \alpha_2, \dots, \alpha_s)$.

PROOF OF LEMMA 1. See in [10, p. 51].

LEMMA 2. *Suppose that p is a prime, χ is a non-principal character modulo p of order d, $f(x) \in F_p[x]$ has s distinct roots in $\overline{F}_p$, and it is not a constant multiple of a d-th power of a polynomial over F_p. Let y be a real number with $0 < y \leq p$. Then for any $x \in \mathbb{R}$:*

$$\left| \sum_{x < n \leq x+y} \chi(f(n)) \right| < 9sp^{1/2} \log p.$$

POOF OF LEMMA 2. This is a trivial consequence of Lemma 1 and Lemma 2 in [2]. Indeed, there this result is deduced from Weil's theorem [11].

Now, we will prove Theorem 1. Let $f(x) = b(x-x_1)^{\alpha_1}\dots(x-x_s)^{\alpha_s}$ where $x_i \neq x_j$. By Lemma 1, there exists a polynomial $z(x)$ with $f(x) = b(z(x))^d$ where

$d = (\alpha_1, \dots, \alpha_s)$. It is also obvious from Lemma 1 that $f(x)$ is not a constant multiple of any d'-th power for any $d' \mid d$. Assume now that

$$1 \le a \le a + (t-1)b \le p-1.$$

The following computations and inequalities can be obtained in the same way as in [9], replacing $a + jb$ there by $f(a + jb)$.

$$|U(E_N, t, a, b)| = \frac{2}{p-1} \left| \sum_{\chi \neq \chi_0} \left(\sum_{j=0}^{t-1} \overline{\chi}(f(a+jb)) \right) \left(\sum_{k=0}^{(p-1)/2} \chi^k(g) \right) \right|.$$

By the triangle inequality we have

$$\begin{aligned} |U(E_N, t, a, b)| &\le \frac{2}{p-1} \left| \sum_{\chi^d \neq 1} \left(\sum_{j=0}^{t-1} \overline{\chi}(f(a+jb)) \right) \left(\sum_{k=1}^{(p-1)/2} \chi^k(g) \right) \right| \\ &\quad + \frac{2}{p-1} \left| \sum_{\substack{\chi \neq \chi_0 \\ \chi^d = 1}} \left(\sum_{j=0}^{t-1} \overline{\chi}(f(a+jb)) \right) \left(\sum_{k=1}^{(p-1)/2} \chi^k(g) \right) \right| \\ &= \sum\nolimits_1 + \sum\nolimits_2. \end{aligned} \tag{4}$$

Next we give an upper bound for $\sum_1$ in the same way as in [9]. If we consider a typical term in $\sum_1$: $\left(\sum_{j=0}^{t-1} \overline{\chi}(f(a+jb)) \right) \left(\sum_{k=0}^{(p-1)/2} \chi^k(g) \right)$ then the order of χ does not divide d because $\chi^d \neq 1$. Let the order of χ be d'. $d' \nmid d$ so $f(x)$ is not a constant multiple of a d'-th power. Thus we may use Lemma 2:

$$\left| \sum_{j=0}^{t-1} \overline{\chi}(f(a+jb)) \right| \le 9sp^{1/2} \log p. \tag{5}$$

We need an upper bound for $\sum_{\chi^d \neq 1} \left| \sum_{k=1}^{(p-1)/2} \chi^k(g) \right|$.

LEMMA 3. *Let $1 \le d \le p-1$ and $d \mid p-1$. Then*

$$\sum_{\substack{\chi \neq \chi_0 \\ \chi^d = 1}} \left| \sum_{k=1}^{(p-1)/2} \chi^k(g) \right| \le \sum_{\substack{\chi \neq \chi_0 \\ \chi^d = 1}} \frac{2}{|1 - \chi(g)|} < 2d \log(d+1).$$

PROOF OF LEMMA 3. The proof is nearly the same as in [10, p. 380–381]. The only difference is in [10, p. 381] at (10), where now we have:

$$\sum_{\substack{\chi\neq\chi_0\\ \chi^d=1}}\frac{1}{|1-\chi(g)|}=\sum_{n=1}^{d-1}\frac{1}{|1-e(n/d)|}\le\frac{1}{4}\sum_{n=1}^{d-1}\frac{1}{\|n/d\|}$$

$$\le\frac{1}{2}\sum_{n=1}^{[d/2]}\frac{1}{\|n/d\|}=\frac{1}{2}\sum_{n=1}^{[d/2]}\frac{d}{n}$$

$$<\frac{1}{2}d(1+\log(d/2))<d\log(d+1)$$

which completes the proof.

Since χ is a multiplicative character of order $p-1$, thus we have $\chi^{p-1}=1$. Applying Lemma 3 with $d=p-1$ we get:

$$\sum_{\chi\neq\chi_0}\left|\sum_{k=1}^{(p-1)/2}\chi^k(g)\right|\le\sum_{\chi\neq\chi_0}\frac{2}{|1-\chi(g)|}<2(p-1)\log(p).$$

It follows that

$$\frac{2}{p-1}\sum\nolimits_1\le 36sp^{1/2}(\log p)^2. \tag{6}$$

Finally we give an upper bound for $\sum_2$:

$$\frac{2}{p-1}\sum\nolimits_2=\frac{2}{p-1}\left|\sum_{\substack{\chi\neq\chi_0\\ \chi^d=1}}\left(\sum_{j=0}^{t-1}\overline{\chi}(bg^d(a+jb))\right)\left(\sum_{k=1}^{(p-1)/2}\chi^k(g)\right)\right|$$

$$=\frac{2}{p-1}\left|\sum_{\substack{\chi\neq\chi_0\\ \chi^d=1}}\left(\sum_{j=0}^{t-1}\overline{\chi}^d(z(a+jb))\right)\left(\sum_{k=1}^{(p-1)/2}\chi^k(g)\right)\right|$$

$$\le\frac{2}{p-1}\sum_{\chi\neq\chi_0}t\left|\sum_{k=1}^{(p-1)/2}\chi^k(g)\right|.$$

Using Lemma 3 we get:

$$\frac{2}{p-1}\sum\nolimits_2\le\frac{4}{p-1}td\log d<4d\log d.$$

Using that d is less than the degree of f, which is k, and $k<p^{1/2}$ we get

$$\frac{2}{p-1}\sum\nolimits_2\le 4k\log k<2p^{1/2}\log p. \tag{7}$$

From (4), (6) and (7) we get

$$|U(E_N, t, a, b)| \le 38kp^{1/2}(\log p)^2.$$

PROOF OF THEOREM 2. We will use addition theorems as in [4]. First we need the following definition:

DEFINITION 3. Let $\mathcal{A}$ and $\mathcal{B}$ be multi-sets of the elements of $\mathbb{Z}_p$. If $\mathcal{A}+\mathcal{B}$ represents every element of $\mathbb{Z}_p$ with multiplicity divisible by $p-1$, i.e., for all $c \in \mathbb{Z}_p$, the number of solutions of

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

(the a's and b's are counted with their multiplicities) is divisible by $p-1$, then the sum $\mathcal{A}+\mathcal{B}$ is said to have property $\mathcal{P}$.

LEMMA 4. *Let $\mathcal{A} = \{a_1, \dots, a_1, \dots, a_r \dots, a_r\}$ and $\mathcal{D} = \{d_1, \dots, d_1, \dots, d_\ell, \dots, d_\ell\}$ be multi-sets of the elements of $\mathbb{Z}_p$ where the multiplicity of a_i is α_i in $\mathcal{A}$ and the multiplicity of d_i is δ_i in $\mathcal{D}$. If one of the following two conditions holds:*

(i) $\min\{r, \ell\} \le 2$ *and* $\max\{r, \ell\} \le p-1$,
(ii) $(4\ell)^r \le p$ *or* $(4r)^\ell \le p$,

then there exists $c \in \mathbb{Z}_p$ such that

$$a + d = c \qquad a \in \mathcal{A},\ d \in \mathcal{D}$$

has exactly $\alpha_i\delta_j$ solutions for some $1 \le i \le r$, $1 \le j \le \ell$ (i.e. the solution is unique apart from the multiplicities).

PROOF OF LEMMA 4. Consider the simple sets $\mathcal{A}' = \{a_1, a_2, \dots, a_r\}$, $\mathcal{D}' = \{d_1, d_2, \dots, d_r\}$. It was proved in [4, Theorem 2] that under any of these conditions there is a $c \in \mathbb{Z}_p$ such that

$$a + d = c \qquad a \in \mathcal{A}',\ d \in \mathcal{D}'$$

has exactly one solution. The statement of the lemma follows easily from this.

To prove Theorem 2, consider any $\mathcal{D} = (d_1, d_2, \dots, d_\ell)$ with non-negative integers $d_1 < d_2 < \cdots < d_\ell$ and positive integers M with $M + d_\ell \le N$. Then arguing as in [9, p. 382] with $f(x + d_j)$ in place of $n + d_j$, we have

$$|V(E_N, M, D)| \le \frac{2^\ell}{(p-1)^\ell} \sum_{\chi_1 \ne \chi_0} \cdots \sum_{\chi_\ell \ne \chi_0} \left| \sum_{x=1}^{M} \chi_1(f(x+d_1)) \cdots \chi_\ell(f(x+d_\ell)) \right|$$

$$\times \prod \left| \sum_{\ell_j=1}^{(p-1)/2} \overline{\chi}_j\big(g^{\ell_j}\big) \right|. \tag{8}$$

Now, let χ be a generator of the group modulo p characters, e.g. χ can be chosen as the character χ uniquely defined by $\chi(g) = e\left(\frac{1}{p-1}\right)$. The order of χ is $p-1$. Let

$$\chi_u = \chi^{\delta_u} \qquad \text{for } u = 1, 2, \dots, \ell$$

where, by $\chi_1 \neq \chi_0, \dots, \ \chi_\ell \neq \chi_0$, we may take

$$1 \leq \delta_u < p-1 \qquad \text{for } u = 1, 2, \dots, \ell.$$

Thus in (8) we have

$$\left|\sum_{x=1}^{M} \chi_1 f(x+d_1)\dots\chi_\ell f(x+d_\ell)\right| = \left|\sum_{x=1}^{M} \chi^{\delta_1} f(x+d_1)\dots\chi^{\delta_\ell} f(x+d_\ell)\right|$$

$$= \left|\sum_{x=1}^{M} \chi\left(f^{\delta_1}(x+d_1)\cdots f^{\delta_\ell}(x+d_\ell)\right)\right|.$$

If $f^{\delta_1}(x+d_1)\cdots f^{\delta_\ell}(x+d_\ell)$ is not a perfect $(p-1)$-th power, then this sum can be estimated by Lemma 3, whence

$$\left|\sum_{x=1}^{M} \chi\left(f^{\delta_1}(x+d_1)\cdots f^{\delta_\ell}(x+d_\ell)\right)\right| \leq 9s\ell p^{1/2}\log p.$$

Therefore by (8) and the triangle-inequality we get:

$$|V(E_N, M, D)| \leq \frac{2^\ell}{(p-1)^\ell}\left|\sum_{\chi_1\neq\chi_0}\dots\sum_{\chi_\ell\neq\chi_0} 9s\ell p^{1/2}\log p \prod_{j=1}^{\ell}\left(\sum_{l_j=1}^{(p-1)/2}\chi^{\delta_j}\left(g^{\ell_j}\right)\right)\right|$$

$$+ \frac{2^\ell}{(p-1)^\ell}\left|\sum_{\substack{1\leq\delta_1,\dots,\delta_\ell\leq p-2,\\ f^{\delta_1}(x+d_1)\cdots f^{\delta_\ell}(x+d_\ell) \text{ is}\\ \text{a perfect } (p-1)\text{-th power}}} (p-1)\prod_{j=1}^{\ell}\left(\sum_{l_j=1}^{(p-1)/2}\chi^{\delta_j}\left(g^{\ell_j}\right)\right)\right|$$

$$= \frac{2^\ell}{(p-1)^\ell}\sum\nolimits_1 + \frac{2^\ell}{(p-1)^\ell}\sum\nolimits_2. \tag{9}$$

By [9, p. 384] we have

$$\frac{2^\ell}{(p-1)^\ell}\sum\nolimits_1 \leq 9s\ell 4^\ell p^{1/2}(\log p)^{\ell+1}. \tag{10}$$

It remains give an upper bound for $\sum_2$. If f is irreducible it is obvious that $f^{\delta_1}(x+d_1)\dots f^{\delta_\ell}(x+d_\ell)$ is a perfect $(p-1)$-th power if and only if $p-1 \mid \delta_1, \dots, \delta_\ell$. But in $\sum_2$ we have $1 \leq \delta_1, \dots, \delta_\ell \leq p-2$, therefore $\sum_2 = 0$ which proves Theorem 2 in case a). In cases b), c), d) we will prove that $\sum_2$ is small. We need the following lemma to estimate $\sum_2$.

LEMMA 5. *For all* $1 \le \delta_1, \dots, \delta_\ell \le p-2$ *such that* $f^{\delta_1}(x+d_1)\dots f^{\delta_\ell}(x+d_\ell)$ *is a perfect* $(p-1)$*-th power, there is a* δ_i $(1 \le i \le \ell)$ *and an integer* $1 \le \alpha \le k$ *(where* k *is the degree of the polynomial* $f(x)$*) such that* $p-1 \mid \alpha\delta_i$.

We will prove Lemma 5 later. Now, from this lemma we verify that

$$\frac{2^\ell}{(p-1)^\ell}\sum\nolimits_2 \le k(k+1)\ell\, 2^{2\ell-1}(\log p)^{\ell-1}.$$

Consider a fixed ℓ-tuples $\{\delta_1, \dots, \delta_\ell\}$ for which $f^{\delta_1}(x+d_1)\dots f^{\delta_\ell}(x+d_\ell)$ is a perfect $(p-1)$-th power and $1 \le \delta_1, \dots, \delta_\ell \le p-2$. By Lemma 5, then there exits a δ_i with

$$p-1 \mid \delta_i\alpha.$$

But $0 < \alpha\delta_i < \alpha(p-1)$ and $\alpha \le k$:

$$p-1 \le \delta_i\alpha \le (\alpha-1)(p-1)$$

$$\frac{1}{\alpha} \le \frac{\delta_i}{p-1} \le 1 - \frac{1}{\alpha}$$

$$\frac{1}{k} \le \frac{1}{\alpha} \le \left\| \frac{\delta_i}{p-1} \right\|.$$

By $|1 - e(\alpha)| \ge 4\,\|\alpha\|$ we have

$$\frac{2}{|1-\chi^{\delta_i}(g)|} = \frac{2}{|1-e(\delta_i/(p-1))|} \le \frac{1}{2\,\|\delta_i/(p-1)\|} < \frac{k}{2}. \tag{11}$$

By Lemma 5, we have

$$\sum\nolimits_2 \le (p-1)\sum_{i=1}^{\ell}\sum\nolimits_{2,i} \tag{12}$$

where

$$\sum\nolimits_{2,i} = \sum_{\substack{1\le\delta_1,\dots,\delta_\ell\le p-2,\\ f^{\delta_1}(x+d_1)\cdots f^{\delta_\ell}(x+d_\ell) \text{ is}\\ \text{a perfect } (p-1)\text{-th power},\\ \exists\ 1\le\alpha\le k,\ p-1\mid\alpha\delta_i}} \prod_{j=1}^{\ell}\left|\sum_{\ell_j=1}^{(p-1)/2}\chi^{\delta_j}\left(g^{\ell_j}\right)\right|.$$

By (11) and $\left|\sum_{\ell_j=1}^{(p-1)/2}\chi^{\delta_j}\left(g^{\ell_j}\right)\right| \le \frac{2}{|1-\chi^{\delta_j}(g)|}$ we get:

$$\sum\nolimits_{2,i} \le \frac{k}{2}\sum_{1\le\delta_1,\dots,\delta_{i-1},\delta_{i+1},\dots,\delta_\ell\le p-2}\ \prod_{j\ne i}\frac{2}{|1-\chi^{\delta_j}(g)|}\sum_{\substack{1\le\delta_i\le p-2,\\ f^{\delta_1}(x+d_1)\cdots f^{\delta_\ell}(x+d_\ell) \text{ is}\\ \text{a perfect } (p-1)\text{-th power}}} 1. \tag{13}$$

Next we give an upper bound for

$$\sum_{\substack{1\le\delta_i\le p-2,\\ f^{\delta_1}(x+d_1)\cdots f^{\delta_\ell}(x+d_\ell)\text{ is}\\ \text{a perfect }(p-1)\text{-th power}}} 1 \stackrel{\text{def}}{=} r.$$

For fixed $\delta_1,\dots,\delta_{i-1},\delta_{i+1},\dots,\delta_\ell$ let $1\le x_1<x_2<\dots<x_r\le p-2$ denote the numbers for which $f^{\delta_1}(x+d_1)\cdots f^{\delta_{i-1}}(x+d_{i-1})f^{x_j}(x+d_i)f^{\delta_{i+1}}(x+d_{i+1})\cdots f^{\delta_\ell}(x+d_\ell)$ is a perfect $(p-1)$-th power. It is clear that the quotient of two polynomials of this form is a $(p-1)$-th power, so

$$f^{x_j-x_{j-1}}(x+d_i) \qquad (\text{for } j=2,3,\dots,r)$$

is a perfect $(p-1)$-th power. The degree of $f^{x_j-x_{j-1}}(x+d_i)$ is $(x_j-x_{j-1})k$, and this degree is divisible by $p-1$, therefore

$$x_j-x_{j-1}\ge\frac{p-1}{k}.$$

So

$$p-1>x_r>\sum_{j=2}^{r}(x_j-x_{j-1})\ge(r-1)\frac{p-1}{k}.$$

By this:

$$\sum_{\substack{1\le\delta_i\le p-2,\\ f^{\delta_1}(x+d_1)\cdots f^{\delta_\ell}(x+d_\ell)\text{ is}\\ \text{a perfect }(p-1)\text{-th power}}} 1 = r\le k+1.$$

Thus we get from (13):

$$\sum\nolimits_{2,i}\le\frac{k(k+1)}{2}\sum_{1\le\delta_1,\dots,\delta_{i-1},\delta_{i+1},\dots,\delta_\ell\le p-2}\ \prod_{j\ne i}\frac{2}{|1-\chi^{\delta_j}(g)|}$$

$$=\frac{k(k+1)}{2}2^{\ell-1}\left(\sum_{\chi\ne\chi_0}\frac{1}{|1-\chi(g)|}\right)^{\ell-1}.$$

By Lemma 3 we have

$$\sum\nolimits_{2,i}\le\frac{k(k+1)}{2}2^{\ell-1}(p-1)^{\ell-1}(\log p)^{\ell-1}.$$

From this and (12):

$$\sum\nolimits_{2}\le k(k+1)\ell\ 2^{\ell-2}(p-1)^{\ell}(\log p)^{\ell-1}.$$

By this, (9), (10) and $k<p^{1/2}-1$, we get the statement of Theorem 2. It remains to prove Lemma 5.

PROOF OF LEMMA 5. The following equivalence relation was defined in [4]: We will say that the polynomials $\varphi(x), \psi(x) \in F_p[x]$ are equivalent, if there is an $a \in F_p$ such that $\psi(x) = \phi(x+a)$. Clearly, this is an equivalence relation.

Write $f(x)$ as the products of irreducible polynomials over F_p. Let us group these factors so that in each group the equivalent irreducible factors are collected. Consider a typical group $\phi(x+a_1), \dots, \phi(x+a_r)$. Then $f(x)$ is of the form $f(x) = \varphi^{\alpha_1}(x+a_1)\dots\varphi^{\alpha_r}(x+a_r)z(x_r)$ where $z(x)$ has no irreducible factors equivalent with any $\varphi(x+a_i)$ $(1 \le i \le r)$.

Let $h(x) = f^{\delta_1}(x+d_1)\cdots f^{\delta_\ell}(x+d_\ell)$ be a perfect $(p-1)$-th power where $1 \le \delta_1, \dots \delta_\ell \le p-2$. Then writing $h(x)$ as the product of irreducible polynomials over F_p, all the polynomials $\varphi(x+a_i+d_j)$ with $1 \le i \le r$, $1 \le i \le r$, $1 \le j \le \ell$ occur amongst the factors. All these polynomials are equivalent, and no other irreducible factor belonging to this equivalence class will occur amongst the irreducible factors of $h(x)$.

Since distinct irreducible polynomials cannot have a common zero in the algebraic closured of F_p, therefore each of the zeros of h is of multiplicity divisible by $p-1$, if and only if in each group, formed by equivalent irreducible factors $\varphi(x+a_i+d_j)$ of $h(x)$, every polynomial of form $\varphi(x+c)$ occurs with multiplicity divisible by $p-1$. In other words writing $\mathcal{A} = \{a_1, \dots, a_1, \dots, a_r, \dots, a_r\}$, $\mathcal{D} = \{d_1, \dots, d_1, \dots, d_\ell, \dots, d_\ell\}$ where a_i has the multiplicity α_i in $\mathcal{A}$ (α_i is the exponent of $\varphi(x+a_i)$ in the factorization of $f(x)$) and d_i has the multiplicity δ_i in $\mathcal{D}$, then for each group $\mathcal{A}+\mathcal{D}$ must possess property $\mathcal{P}$.

If condition b) holds in Theorem 2, then considering the degrees of the irreducible factors of $f(x)$, we see that there exists a group for which $r \le 2$, i.e., $\mathcal{A}$ contains at most two distinct elements. So if one of the conditions of Theorem 2 holds then there exists a group for which the multi-sets $\mathcal{A}$ and $\mathcal{D}$ satisfy the conditions of Lemma 4, we get that there exists a c such that

$$a + d = c \qquad a \in \mathcal{A},\ d \in \mathcal{D}$$

has exactly $\alpha_i\delta_j$ solution for some $1 \le i \le r$ and $1 \le j \le \ell$. But $\mathcal{A}+\mathcal{D}$ possess property $\mathcal{P}$, therefore $p-1 \mid \alpha_i\delta_j$. Because α_i is the exponent of an irreducible factor in $f(x)$, we also have $1 \le \alpha_i \le k$. Which completes the proof of Lemma 5.

PROOF OF THEOREM 3. We will use the following lemma.

LEMMA 6. *If $f(x) \equiv \pm f(t-x) \bmod p$, then there exists a permutation $\{x_1, \dots, x_s\}$ of the distinct roots of $f(x)$ such that*

$$t \equiv x_1 + x_s \equiv x_2 + x_{s-1} \equiv \cdots \equiv x_{\lceil s/2\rceil} + x_{s+1-\lceil ss/2\rceil}$$

and denoting the multiplicity of the root x_i by α_i $(1 \le i \le s)$ we also have $\alpha_i = \alpha_{s+1-i}$.

PROOF OF LEMMA 6. This is a consequence of the fact every polynomial has unique factorization over F_p. Now we can return to the proof of Theorem 3.

In the same way as the estimates of the correlation measure we obtain:

$$H(E_N,a,b)\le\frac{4}{(p-1)^2}\sum_{\chi_1\ne\chi_0}\sum_{\chi_2\ne\chi_0}18sp^{1/2}\log p\prod_{j=1}^{2}\left|\sum_{l_j=1}^{(p-1)/2}\chi_j(g^{l_j})\right|$$

$$+\frac{4}{(p-1)^2}\sum_{\substack{1\le\delta_1,\delta_2\le p-2,\\ f^{\delta_1}(a+x)f^{\delta_2}(b-x)\text{ is a}\\ \text{perfect }p-1\text{-th power}}}(p-1)\prod_{j=1}^{2}\left|\sum_{l_j=1}^{(p-1)/2}\chi_j(g^{l_j})\right|$$

$$=\frac{4}{(p-1)^2}\sum\nolimits_1+\frac{4}{(p-1)^2}\sum\nolimits_2. \tag{14}$$

Again as in [9, p. 384] we have

$$\frac{4}{(p-1)^2}\sum\nolimits_1\le 72kp^{1/2}(\log p)^3. \tag{15}$$

To give an upper bound for $\sum_2$ we have to handle the case when the polynomial $f^{\delta_1}(a+x)f^{\delta_2}(b-x)$ is a perfect $(p-1)$-th power. Suppose that there is no permutation $\{x_1\dots,x_s\}$ with

$$t\equiv x_1+x_s\equiv x_2+x_{s-1}\equiv\dots\equiv x_{\lceil s/2\rceil}+x_{s+1-\lceil ss/2\rceil}.$$

Then there exists a root of $f(a+x)$ which is not the root of $f(b-x)$ (x is the variable). Denote this root by x_i-a and let α_i the multiplicity of the root x_i-a in $f(a+x)$. Then $p-1\mid\alpha_i\delta_1$ because $f^{\delta_1}(a+x)f^{\delta_2}(b-x)$ is a perfect $(p-1)$-th power. But also $1\le\alpha_i\le k$, so in this special case in the same way as we get the result of Theorem 2 from Lemma 5, we obtain:

$$\frac{4}{(p-1)^2}\sum\nolimits_2\le 16k(k+1)(\log p)^3.$$

From this, (14), (15) we get

$$H(E_N,a,b)\le 88kp^{1/2}(\log p)^3.$$

The case when

$$t\equiv x_1+x_s\equiv x_2+x_{s-1}\equiv\dots\equiv x_{\lceil s/2\rceil}+x_{s+1-\lceil ss/2\rceil}$$

holds is slightly more difficult. Considering the multiplicity of the roots $x_i-a\equiv b-x_{s+1-i}$, $x_{s+1-i}-a\equiv b-x_i \bmod p$ in the polynomial $f^{\delta_1}(a+x)f^{\delta_2}(b-x)$ we get:

$$p-1\mid\delta_1\alpha_i+\delta_2\alpha_{s+1-i}\,,$$

$$p-1\mid\delta_1\alpha_{s+1-i}+\delta_2\alpha_i\,.$$

Taking the sum and the difference we obtain

$$\begin{aligned} &p-1 \mid (\delta_1-\delta_2)(\alpha_i-\alpha_{s+1-i}),\\ &p-1 \mid (\delta_1+\delta_2)(\alpha_i+\alpha_{s+1-i}) \qquad (1\le i\le s). \end{aligned} \tag{16}$$

By Lemma 6 we know that there exists an i for which $\alpha_i \neq \alpha_{s+1-i}$. By $1 \le |\alpha_i-\alpha_{s+1-i}| \le k$, $1 \le |\alpha_i+\alpha_{s+1-i}| \le 2k$ and (16), we obtain that both $\delta_1-\delta_2$ and $\delta_1+\delta_2$ may assume at most $2k$ different values. Therefore at most $(2k)^2$ pairs $\{\delta_1,\delta_2\}$ exist for which $f^{\delta_1}(a+x)f^{\delta_2}(b-x)$ is a perfect $(p-1)$-th power.

By $|1-e(\alpha)| \ge 4\,\|\alpha\|$, $\chi_i = \chi^{\delta_i}$, we have:

$$\begin{aligned} \prod_{j=1}^{2}\left|\sum_{\ell_j=1}^{(p-1)/2}\chi_j\left(g^{\ell_j}\right)\right| &\le \frac{4}{|1-\chi^{\delta_1}(g)|\,|1-\chi^{\delta_2}(g)|}\\ &\le \frac{1}{4\left\|\frac{\delta_1}{p-1}\right\|\left\|\frac{\delta_2}{p-1}\right\|}. \end{aligned} \tag{17}$$

Next we will prove:

$$\frac{1}{\left\|\frac{\delta_1}{p-1}\right\|\left\|\frac{\delta_2}{p-1}\right\|} \le 2pk. \tag{18}$$

LEMMA 7. *If $x,y\in\mathbb{N}$, $y\neq 0$, $p-1 \mid xy$, but $p-1 \nmid x$ then we have $\left\|\frac{x}{p-1}\right\| \ge \frac{1}{y}$.*

PROOF OF LEMMA 7. Let $x = r(p-1)+q$ where $1\le q\le p-2$. Then

$$r(p-1)y < xy < (r+1)(p-1)y.$$

But $p-1 \mid xy$, so:

$$(p-1)(ry+1) \le xy \le (p-1)(ry+y-1),$$

$$r+\frac{1}{y} \le \frac{x}{p-1} \le r+1-\frac{1}{y},$$

$$\left\|\frac{x}{p-1}\right\| \ge \frac{1}{y}$$

which was to be proved.

If $p-1 \mid \delta_1-\delta_2$ and $p-1 \mid \delta_1+\delta_2$ then by $1\le\delta_1,\delta_2\le p-2$ we have $\delta_1=\delta_2=\frac{p-1}{2}$ and (18) is trivial. We may suppose that at least one of $\delta_1-\delta_2$, $\delta_1+\delta_2$ is not divisible by $p-1$. If $p-1\nmid\delta_1-\delta_2$ then $p-1 \mid (\delta_1-\delta_2)(\alpha_i-\alpha_{s+1-i})$, and using Lemma 8 we get:

$$\left\|\frac{\delta_1-\delta_2}{p-1}\right\| \ge \frac{1}{|\alpha_i-\alpha_{s+1-i}|} \ge \frac{1}{k}.$$

If $p-1 \nmid \delta_1+\delta_2$ then $p-1 \mid (\delta_1+\delta_2)(\alpha_i+\alpha_{s+1-i})$, and using again Lemma 8 we get:

$$\left\|\frac{\delta_1+\delta_2}{p-1}\right\| \geq \frac{1}{|\alpha_i+\alpha_{s+1-i}|} \geq \frac{1}{2k}\,.$$

By the triangle-inequality in both cases we have:

$$\left\|\frac{\delta_1}{p-1}\right\| + \left\|\frac{\delta_2}{p-1}\right\| \geq \left\|\frac{\delta_1 \pm \delta_2}{p-1}\right\| \geq \frac{1}{2k}\,.$$

But $\frac{1}{p-1} \leq \left\|\frac{\delta_1}{p-1}\right\|, \left\|\frac{\delta_2}{p-1}\right\|$, so trivially

$$\left\|\frac{\delta_1}{p-1}\right\| \left\|\frac{\delta_2}{p-1}\right\| \geq \frac{1}{2k(p-1)} \geq \frac{1}{2kp}\,,$$

from which (18) follows. By (17), (18), and since there are at least $(2k)^2$ pairs for which $f^{\delta_1}(a+x)f^{\delta_2}(b-x)$ is a perfect $(p-1)$-th power, we have

$$\sum\nolimits_2 \leq \sum_{\substack{1\leq\delta_1,\delta_2\leq p-2,\\ f^{\delta_1}(a+x)f^{\delta_2}(b-x) \text{ is a}\\ \text{perfect } (p-1)\text{-th power}}} (p-1)\frac{1}{2}pk \leq \frac{1}{2}(p-1)pk(2k)^2 = 2(p-1)pk^3. \qquad (19)$$

From (14), (15) and (19) we get

$$H(E_N,a,b) \leq 88kp^{1/2}(\log p)^3$$

which proves the theorem.

PROOF OF THEOREM 4. The proof is exactly the same as in [1, Theorem 1], the only difference is in the definitions of q and r: now we choose q, r as integers with $(q,p)=(r,p)=1$ and $1 \leq \operatorname{ind} q \leq \frac{p-1}{2}$, $\frac{p-1}{2} < \operatorname{ind} r \leq p-1$.

3. Numerical calculations

In this chapter our goal is to carry out numerical calculations. Partly to see how far our theoretical estimates are from the probable truth, partly to gather numerical data in cases when we cannot prove any theoretical estimates (linear complexity and the correlation measure of higher order). In particular, one might like to gather information on the linear complexity (see, e.g. [8]) which is another characteristic closely related to pseudorandomness. The linear complexity is defined as it follows.

DEFINITION 4. The linear complexity of a finite binary sequence $\{s_0,\dots,s_{N-1}\} \in \{0,1\}^N$ is the smallest integer L for which there exist numbers $c_1,\dots,c_{L-1}$

$\in \{0,1\}$ such that

$$s_n \equiv c_1 s_{n-1} + c_2 s_{n-2} + \cdots + c_{L-1} s_{n-(L-1)} + s_{n-L} \bmod 2 \qquad \text{for all } n \geq L.$$

We construct a sequence $\{s_0, \ldots, s_{p-2}\} \in \{0,1\}^{p-1}$ from our sequence $E_{p-1} = \{e_1, \ldots, e_{p-1}\} \in \{-1,+1\}^{p-1}$ in the following way: $s_i = \frac{1}{2}(1 - e_{i+1})$ for all $0 \leq i \leq p-2$. One might like to study the linear complexity of this sequence. Unfortunately we haven't been able to prove any non-trivial theoretical result. Thus all we can do in this direction is, again, to carry out numerical computations; we will use the Berlekamp–Massey algorithm [3], [7] (L denotes the linear complexity).

p prime	$\sqrt{p}$	polynomial	W	C_2	C_3	C_4	S	L
1009	31.764	$x^3 + 1$	38	98	132	152	72	503
		$x^4 + 511x^2 + 123x + 851$	45	102	138	157	68	504
		$122x^4 + 1000x^3 + 22x^2 + 626x + 500$	37	88	126	158	75	505
		$212x^{20} + 567x^{13} + 333x^8 + 9x + 12$	60	96	130	146	72	504
1013	31.827	$x^3 + 1$	38	123	129	151	84	507
		$x^4 + 511x^2 + 123x + 851$	40	104	136	146	67	508
		$122x^4 + 1000x^3 + 22x^2 + 626x + 500$	42	102	128	165	77	506
		$212x^{20} + 567x^{13} + 333x^8 + 9x + 12$	59	103	144	150	72	508

p prime	$\sqrt{p}$	polynomial	W	C_2	S	L
100069	316.336	$x^3 + 1$	623	1284	923	50036
		$x^4 + 75638x^2 + 54322x + 81512$	689	1348	1150	50034
		$x^4 + 34879x^3 + 98537x^2 + 12378x + 68921$	402	1373	861	50034
		$x^{100} + 45623x^{89} + 98254x^{63} + 74563x^{30} + 78346x^{17}$	445	1365	963	50033
100237	316.602	$x^3 + 1$	885	1392	919	50117
		$x^4 + 5433x^2 + 5432x + 23789$	383	1297	859	50118
		$x^4 + 50000x^3 + 28657x^2 + 112211x + 854$	410	1367	975	50118
		$x^{100} + x^{84} + 456789x^{73} + x^{72} + 8789x^4 + 4$	614	1315	970	50119

The data above seem to point to the direction that our condition on k and ℓ can be relaxed considerably, and that the correlation of not very high order tends to be relatively small also for k, ℓ values not covered by Theorem 2. Perhaps this data also indicate that the dependence on the degree of the polynomial in the upper bounds for the pseudorandom measures need not be as strong as in our theorems. Most of the time the linear complexity seems to be around $p/2$ as it would happen for truly random sequences, so that our sequence also satisfies the requirement of high linear complexity.

4. Conclusion

By using the notion of index (discrete logarithm) we have constructed large families of binary sequences with strong pseudorandom properties. However, the weak point of this construction is that the generation of these sequences is very slow (since there is no fast algorithm for computing the discrete logarithm). One might like to improve on this construction by trying to modify the construction so that we should obtain sequences which still have relatively good pseudorandom properties, however, they can be generated much faster. I will return to this problem in a subsequent paper.

ACKNOWLEDGEMENTS. I would like to thank Professors Julien Cassaigne, Joël Rivat, András Sárközy for the valuable discussions.

References

[1] R. AHLSWEDE, L. H. KHACHATRIAN, C. MAUDUIT and A. SÁRKÖZY, A complexity measure for families of binary sequences, *Periodica Math. Hungar.* **46** (2003), 107–118.

[2] R. AHLSWEDE, C. MAUDUIT and A. SÁRKÖZY, Large families of pseudorandom sequences of k symbols and their complexity, Parts I and II, *Proceedings on General theory of information transfer and combinatorics* (to appear).

[3] E. R. BERLEKAMP, *Algebraic coding theory*, McGraw Hill, New York, 1968.

[4] L. GOUBIN, C. MAUDUIT and A. SÁRKÖZY, Construction of large families of pseudorandom binary sequences, *J. Number Theory* (to appear).

[5] K. GYARMATI, On a pseudorandom property of binary sequences, *Ramanujan J.* (to appear).

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

[7] J. L. MASSEY, Shift-register synthesis and BCH decoding, *IEEE Transactions on Information Theory* **15** (1969), 122–127.

[8] A. MENEZES, P. VAN OORSCHOT and S. VANSTONE, *Handbook of applied cryptography*, CRC Press, 1996.

[9] A. SÁRKÖZY, A finite pseudorandom binary sequence, *Studia Sci. Math. Hungar.* **38** (2001), 377–384.

[10] W. M. Schmidt, Equation over finite fields, An elementary approach, *Lecture Notes in Math.,* Vol. 536, Springer, 1976.

[11] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, *Act. Sci. Ind.,* Vol. 1041, Hermann, Paris, 1948.

(Received: March 27, 2003)

Katalin Gyarmati
E-mail: gykati@cs.elte.hu