ACTA ARITHMETICA
118.4 (2005)

On linear recursion and pseudorandomness

by

Katalin Gyarmati (Budapest), Attila Pethő (Debrecen) and
András Sárközy (Budapest)

1. Introduction. C. Mauduit and A. Sárközy [3, pp. 367–370] introduced the following finite measures of pseudorandomness of binary sequences.

For a binary sequence

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

write

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

and, for $D = (d_1, \ldots, d_l)$ with non-negative integers $0 \le d_1 < \cdots < d_l$,

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

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

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

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

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

where the maximum is taken over all $D = (d_1, \ldots, d_l)$ and M such that $M + d_l \le N$.

2000 *Mathematics Subject Classification*: Primary 11K45.

Key words and phrases: pseudorandom, linear recursion, Legendre symbol, character sums.

Research partially supported by Hungarian National Foundation for Scientific Research, Grants No. T038225, T042985, T043623, T043631 and T049639.

In this paper we will study finite binary pseudorandom sequences which are defined by a linear recursion over $\mathbb{F}_p$. More exactly, let $x_1, \dots, x_h \in \mathbb{F}_p$ be the first h elements of the sequence, $c_1, \dots, c_h \in \mathbb{F}_p$ be the coefficients in the linear recursion, so for $n > h$,

$$x_n \equiv c_1 x_{n-1} + c_2 x_{n-2} + \dots + c_h x_{n-h} \pmod p. \tag{1}$$

In order to transform the sequence $\{x_1, x_2, \dots\}$ into a binary sequence $\{e_1, e_2, \dots\}$ we define

$$e_n = \begin{cases} \left(\dfrac{x_n}{p}\right) & \text{if } p \nmid x_n, \\ 1 & \text{if } p \mid x_n, \end{cases} \tag{2}$$

where $\left(\frac{x_n}{p}\right)$ denotes the Legendre symbol.

From the definition of x_n it is clear that the sequence $\{x_n\}$ is periodic with a period T, and then the sequence $\{e_n\}$ is also periodic with period T. Considering only the first T elements of the sequence $\{e_n\}$ we get a finite binary sequence $\{e_1, \dots, e_T\} = E_T$, and we will study the pseudorandom properties of this last sequence.

Unfortunately we cannot estimate the pseudorandom measures of all sequences E_T defined this way, but we will describe a large class of linear recursions for which the sequence E_T has strong pseudorandom properties.

It is well known that the elements of the sequence $\{x_n\}$ defined in (1) can be expressed by the roots of the characteristic polynomial

$$x^h - c_1 x^{h-1} - c_2 x^{h-2} - \dots - c_h \equiv 0 \pmod p.$$

Suppose that this polynomial has h distinct roots in $\mathbb{F}_p^*$: $\lambda_1, \dots, \lambda_h$. Then there exist constants $a_1, \dots, a_h \in \mathbb{F}_p$ such that

$$x_n \equiv a_1 \lambda_1^n + \dots + a_h \lambda_h^n \pmod p$$

for all $n \in \mathbb{N}$. Let $\lambda \in \mathbb{F}_p$ be such that all roots λ_i $(1 \le i \le h)$ are powers of λ (e.g. λ can be a primitive root, or in the special case when all λ_i are quadratic residues modulo p, then λ can be the square of a primitive root modulo p). Let $\lambda_i = \lambda^{k_i}$ for $1 \le i \le h$ and $\max\{k_1, \dots, k_h\} = k$. Then

$$x_n \equiv a_1 \lambda^{k_1 n} + \dots + a_h \lambda^{k_h n} = f(\lambda^n) \pmod p,$$

where $f(x) \in \mathbb{F}_p[x]$ is a polynomial of degree k. Then for the sequence $\{e_1, e_2, \dots\}$ we have

$$e_n = \begin{cases} \left(\dfrac{f(\lambda^n)}{p}\right) & \text{if } p \nmid f(\lambda^n), \\ 1 & \text{if } p \mid f(\lambda^n). \end{cases} \tag{3}$$

The sequence $\{e_n\}$ is periodic with a period T, where now T can be the multiplicative order of λ.

Since not for every linear recursion $\{x_n\}$ can we write the sequence $\{e_n\}$ in the form (3), it is more practical to define the sequence $\{e_n\}$ by (3), and determine the linear recursion from this form. More exactly:

Definition 1. Let p be an odd prime, $\lambda \in \mathbb{F}_p^*$ be of multiplicative order T and $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree k. Then we define the sequence $E_T = \{e_1, \dots, e_T\}$ by (3).

Throughout the paper we will use this definition and these notations: the numbers p, k, λ, T and the polynomial $f(x)$ will be as in Definition 1.

The next question is how to determine the linear recursion for the sequence $\{x_n\}$ (where $x_n \equiv f(\lambda^n) \bmod p$) from the polynomial $f(x) \in \mathbb{F}_p[x]$ and the number $\lambda \in \mathbb{F}_p$. Write $f(x)$ in the form

$$f(x) = a_1 x^{k_1} + \cdots + a_h x^{k_h}.$$

Then by computing the coefficients $-c_i$ of the characteristic polynomial

$$(x - \lambda^{k_1}) \cdots (x - \lambda^{k_h}) = x^h - c_1 x^{h-1} - \cdots - c_h,$$

we find that the linear recursion for the sequence $\{x_n\}$ is

$$x_n \equiv c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_h x_{n-h} \pmod p.$$

We will give estimates for the pseudorandom measures of E_T defined in Definition 1, but these upper bounds will be non-trivial only if k, the degree of the polynomial $f(x)$, is $\ll p^{1/2-\varepsilon}$ for some $\varepsilon > 0$. For the well-distribution measure we obtain the following:

Theorem 1. *Suppose that $f(x)$ is not of the form $cx^\alpha(g(x))^2$ with $c \in \mathbb{F}_p$, $\alpha \in \mathbb{N}$, $g(x) \in \mathbb{F}_p[x]$. Then*

$$W(E_T) < 5kp^{1/2} \log p.$$

Clearly, if $f(x)$ is of the form $c(g(x))^2$, then either the sequence E_T contains only $+1$'s, or all but at most $k/2$ of the elements of E_T are -1's, since if $g(i) \equiv 0 \pmod p$ then $e_i = 1$ and otherwise $e_i = \big(\frac{c(g(\lambda^i))^2}{p}\big) = \big(\frac{c}{p}\big)$. If $f(x)$ is of the form $cx(g(x))^2$, then $e_i = \big(\frac{c}{p}\big)\big(\frac{\lambda}{p}\big)^i$ for $g(i) \not\equiv 0 \pmod p$, and thus the sequence E_T is almost (apart from at most $k/2$ pieces of e_i's) periodic with period 2.

In the case of the correlation measure there is no non-trivial general upper bound:

Let $l \mid T$ and $f(x)$ be of the form $f(x) = \varphi(x)\varphi(\lambda^{T/l}x)$, where $\varphi(x) \in \mathbb{F}_p[x]$ has no zero in $\mathbb{F}_p$. Then for the sequence E_T defined in (3) we will prove that

$$C_l(E_T) \geq \frac{T}{l},$$

which means that for small $l \mid T$, the correlation measure of order l is large.

Indeed, by the definition of the correlation measure of order l, the equality $\varphi(\lambda^{n+T}) = \varphi(\lambda^n)$, the multiplicative property of the Legendre symbol and $\varphi(\lambda^{n+iT/l}) \neq 0$ for $i \in \mathbb{N}$, we get

$$\begin{aligned} C_l(E_T) &\geq \left|\sum_{n=1}^{T/l} e_n e_{n+T/l} e_{n+2T/l} \cdots e_{n+(l-1)T/l}\right| \\ &= \left|\sum_{n=1}^{T/l} \left(\frac{\varphi(\lambda^n)\varphi(\lambda^{n+T/l})}{p}\right)\left(\frac{\varphi(\lambda^{n+T/l})\varphi(\lambda^{n+2T/l})}{p}\right)\cdots\right. \\ &\qquad\qquad \left.\left(\frac{\varphi(\lambda^{n+(l-1)T/l})\varphi(\lambda^n)}{p}\right)\right| \\ &= \left|\sum_{n=1}^{T/l} \left(\frac{\varphi(\lambda^n)\varphi(\lambda^{n+T/l})\cdots\varphi(\lambda^{n+(l-1)T/l})}{p}\right)^2\right| = \frac{T}{l}, \end{aligned}$$

which was to be proved.

Thus for $l \mid T$ there exists a polynomial $f(x)$ for which $C_l(E_T)$ is large. This example shows that to ensure that the correlation measure of order l is small one needs further assumptions on the polynomial $f(x)$ and the integers T and l. We will use the following definition.

Definition 2. We say that the polynomials $\varphi(x), \psi(x) \in \mathbb{F}_p[x]$ are *equivalent*:

$$\varphi \sim \psi, \tag{4}$$

if there are $c \in \mathbb{F}_p^*$ and $\gamma \in \mathbb{N}$ such that $\varphi(x) = c\psi(\lambda^\gamma x)$.

Clearly, this is an equivalence relation. Next we give an upper bound for the correlation measure of order l:

Theorem 2. *Let $\beta \in \mathbb{N}$ be the largest integer such that $x^\beta \mid f(x)$ (thus $x^{\beta+1} \nmid f(x)$). Suppose that at least one of the following conditions holds*:

(a) *$l = 2$, and $f(x)/x^\beta$ is not of the form $g(x^\sigma)$ or $c(g(x))^2$ with $\sigma \in \mathbb{N}$, $(\sigma, T) \geq 2$, $c \in \mathbb{F}_p$ and $g(x) \in \mathbb{F}_p[x]$.*

(b) *$f(x)/x^\beta$ is not of the form $c(g(x))^2$ with $c \in \mathbb{F}_p$ and $g(x) \in \mathbb{F}_p[x]$, T (the order of λ) is a prime and either* $\min\{(4k)^l, (4l)^k\} \leq T$ *or 2 is a primitive root modulo T.*

(c) *Consider the factorization $f(x)/x^\beta = \varphi_1^{\beta_1}(x) \cdots \varphi_u^{\beta_u}(x)$ where $\beta_i \in \mathbb{N}$ and $\varphi_i(x)$ is irreducible over $\mathbb{F}_p$. Suppose that there is an equivalence class defined by the relation $\sim$ in (4), which contains exactly one factor φ_j $(1 \leq j \leq u)$ amongst the irreducible factors of $f(x)/x^\beta$, moreover the multiplicity of this factor in the factorization of $f(x)/x^\beta$ is $\beta_j = 1$.*

(d) *$k - \beta$ (the degree of the polynomial $f(x)/x^\beta$) and l are odd.*

Then

$$C_l(E_T) \leq 5klp^{1/2}\log p.$$

In Theorem 2(a) we are able to handle the case $l = 2$ completely. Clearly, if $f(x)$ is of the form $g(x^\sigma)$ with $g(x) \in \mathbb{F}_p[x]$, $\sigma \in \mathbb{N}$ and $(\sigma, T) \geq 2$, then the sequence E_T is periodic with period $T/(T,\sigma)$, and thus the correlation measure of order 2 is greater than $\sum_{n=1}^{T-T/(T,\sigma)} e_n e_{n+T/(T,\sigma)} = T - T/(T,\sigma)$. (A similar situation occurs if $f(x)$ is of the form $xg(x^\sigma)$ since then $e_n = -e_{n+T/(T,\sigma)}$.)

In Theorem 2(b), (c) and (d) we study the case $l > 2$, and while these conditions are sufficient to ensure that the correlation measure is small, they are not necessary. It is an important open question to describe all polynomials $f(x)$, integers T and l for which the correlation measure of order l is small. (We remark that a similar additive problem with a prime modulus in place of T was studied in [1].)

Usually, for a fixed polynomial $f(x)$ it is not easy to check whether condition (c) in Theorem 2 holds. We will show that for a large class of polynomials $f(x) \in \mathbb{F}_p[x]$ condition (c) holds, and thus the correlation measure is small. These polynomials will be characterized by their zeros:

Corollary 1. *Suppose that $f(x)$ has a zero $\varrho \neq 0 \in \overline{\mathbb{F}}_p$ of multiplicity* 1 *such that no other zero of $f(x)$ is of the form $\lambda^i\varrho$ with $1 \leq i \leq T-1$. Then*

$$C_l(E_T) \leq 5klp^{1/2}\log p.$$

Using this corollary we get, e.g., the following:

Corollary 2. *Suppose that the order of λ is $T = (p-1)/2$, all the k zeros of $f(x)$ are in $\mathbb{F}_p$, and one of the zeros is a quadratic non-residue modulo p, while the other $k-1$ zeros are quadratic residues modulo p. Then*

$$C_l(E_{(p-1)/2}) \leq 5klp^{1/2}\log p.$$

Finally, we would like to specify our results to the case when $h = 2$, i.e., the order of the linear recursion is 2:

Corollary 3. *Assume that $h = 2$, i.e.,* (1) *is of the form*

$$x_n \equiv c_1x_{n-1} + c_2x_{n-2} \pmod p \tag{5}$$

and assume that

$$\left(\frac{c_1^2 + 4c_2}{p}\right) = 1.$$

Denote the zeros of the characteristic polynomial of the linear recursion (5) *by λ_1 and λ_2 ($\lambda_i^2 - c_1\lambda_i - c_2 \equiv 0 \pmod p$); then $\lambda_1, \lambda_2 \in \mathbb{F}_p$. Suppose that $\lambda_i \not\equiv x_2/x_1 \pmod p$ for $i = 1, 2$. Denote the multiplicative order of λ_2/λ_1*

by T, and define the sequence $E_T = \{e_1, \dots, e_T\}$ by (2). Then

$$W(E_T) \le 9p^{1/2} \log p, \qquad C_l(E_T) \le 9lp^{1/2} \log p.$$

Here, the condition that x_2/x_1 is not a root of the characteristic polynomial is necessary, since if $\lambda_1 \equiv x_2/x_1 \pmod p$, then $x_n \equiv x_1\lambda_1^n$, and thus the sequence $\{e_n\}$ is periodic with period 2.

2. Proofs. The following lemma is a generalization of Lemma 3.3 in [4], and the proof is also similar. Indeed, in [4] only that case is studied when λ is a primitive root, while Lemma 1 holds for all $\lambda \in \mathbb{F}_p^*$.

Lemma 1. *Let p be a prime, χ be a multiplicative character of order d with $2 \le d \in \mathbb{N}$, let $\lambda \in \mathbb{F}_p^*$ be of multiplicative order T, and let $M, K \in \mathbb{N}$ with $K \le T$. Suppose that $f(x) \in \mathbb{F}_p[x]$ has exactly s distinct zeros.*

(i) *If $f(x)$ is not of the form $cx^\alpha(g(x))^d$ with $c \in \mathbb{F}_p$, $\alpha \in \mathbb{N}$ and $g(x) \in \mathbb{F}_p[x]$, then*

$$\Big|\sum_{n=M+1}^{M+K} \chi(f(\lambda^n))\Big| \le 4sp^{1/2} \log p. \tag{6}$$

(ii) *If $f(x) = cx^\alpha(g(x))^d$ with $c \in \mathbb{F}_p^*$, $\alpha \in \mathbb{N}$ and $g(x) \in \mathbb{F}_p[x]$, where $T \nmid \frac{p-1}{d}\alpha$, then*

$$\Big|\sum_{n=M+1}^{M+K} \chi(f(\lambda^n))\Big| \le \frac{d}{2}. \tag{7}$$

Proof. If p or $T \le 2$, Lemma 1 is trivial, therefore we may assume that $p, T \ge 3$. We will reduce the problem to estimating complete sums:

Lemma 2. *Let p be a prime, χ be a multiplicative character of order d with $2 \le d \in \mathbb{N}$, and $\lambda \in \mathbb{F}_p^*$ be an element of multiplicative order T. Suppose that $f(x) \in \mathbb{F}_p[x]$ has s distinct zeros, and $f(x)$ is not of the form $cx^\alpha(g(x))^d$ with $c \in \mathbb{F}_p^*$, $\alpha \in \mathbb{N}$ and $g(x) \in \mathbb{F}_p[x]$. Then*

$$\Big|\sum_{n=1}^{T} \chi(f(\lambda^n))\Big| \le sp^{1/2}. \tag{8}$$

Proof. The order of λ is T, so λ^n (for $n = 1, \dots, T$) runs over all the T different $((p-1)/T)$th powers modulo p except 0. Moreover for fixed λ and n,

$$\lambda^n = x^{(p-1)/T}$$

has exactly $(p-1)/T$ solutions in x. Thus replacing λ^n by $x^{(p-1)/T}$ in (8) we get

$$\Big|\sum_{n=1}^{T}\chi(f(\lambda^n))\Big| = \frac{T}{p-1}\Big|\sum_{n=1}^{p-1}\chi(f(x^{(p-1)/T}))\Big|. \tag{9}$$

Now, we will need the following lemma:

Lemma 3. *Let p be a prime, χ be a character of order $d>1$. Suppose that $f(x)\in\mathbb{F}_p[x]$ has exactly s distinct zeros and it is not of the form $f(x)=c(g(x))^d$ with $c\in\mathbb{F}_p$, $g(x)\in\mathbb{F}_p[x]$. Then*

$$\Big|\sum_{n=1}^{p-1}\chi(f(x))\Big| \le (s-1)p^{1/2}.$$

This can be derived from A. Weil's theorem [6] (an elementary proof of which can be found in [5]); see [2], [3].

Returning to the proof of Lemma 2, we now prove that $f(x^{(p-1)/T})$ is not of the form $c(g(x))^d$ with $c\in\mathbb{F}_p^*$, $g(x)\in\mathbb{F}_p[x]$. Consider the factorization of $f(x)$ over $\overline{\mathbb{F}}_p$:

$$f(x)=c(x-\alpha_1)^{k_1}\cdots(x-\alpha_s)^{k_s},$$

where $c\in\mathbb{F}_p$ and $\alpha_1,\ldots,\alpha_s\in\overline{\mathbb{F}}_p$ are different numbers. Let $\varepsilon_1,\ldots,\varepsilon_{(p-1)/T}\in\mathbb{F}_p$ be the $(p-1)/T$ different solutions of the congruence

$$x^{(p-1)/T}\equiv 1 \pmod p$$

in x, and for each α_i $(1\le i\le s)$ let $\varrho_i\in\overline{\mathbb{F}}_p$ be a number with

$$\varrho_i^{(p-1)/T}=\alpha_i.$$

Then the factorization of $f(x^{(p-1)/T})$ over $\overline{\mathbb{F}}_p$ is

$$\begin{aligned} f(x^{(p-1)/T}) &= c\prod_{i=1}^{s}(x^{(p-1)/T}-\varrho_i^{(p-1)/T})^{k_i} \\ &= c\prod_{i=1}^{s}(x-\varepsilon_1\varrho_i)^{k_i}\cdots(x-\varepsilon_{(p-1)/T}\varrho_i)^{k_i}. \end{aligned}$$

Suppose that in $\overline{\mathbb{F}}_p$,

$$\varepsilon_u\varrho_i=\varepsilon_y\varrho_j \tag{10}$$

for some $1\le u,y\le (p-1)/T$ and $1\le i,j\le s$. Then

$$(\varepsilon_u\varrho_i)^{(p-1)/T}=(\varepsilon_y\varrho_j)^{(p-1)/T},$$

and so $\alpha_i=\alpha_j$, that is, $i=j$. If $u\ne y$ (so $\varepsilon_u\ne\varepsilon_y$), then from (10) we obtain $\varrho_i=\varrho_j=0$ $(i=j)$, so $\alpha_i=0$.

Since $f(x)$ is not of the form $cx^{\alpha}(g(x))^d$ with $c\in\mathbb{F}_p^*$, $\alpha\in\mathbb{N}$ and $g(x)\in\mathbb{F}_p[x]$, it follows that $f(x)$ has zero of multiplicity t_v at $\alpha_v\ne 0$ $(1\le v\le s)$, where $d \nmid t_v$. Then $\varepsilon_1 \varrho_v$ is a zero of $f(x^{(p-1)/T})$ with the same multiplicity t_v, and since $d \nmid t_v$, we infer that $f(x^{(p-1)/T})$ is not of the form $c(g(x))^d$ with $c \in \mathbb{F}_p^*$, $g(x) \in \mathbb{F}_p[x]$.

The polynomial $f(x)$ has exactly s distinct zeros, so the polynomial $f(x^{(p-1)/T})$ (in x) has at most $s\frac{p-1}{T}$ distinct zeros. Using Lemma 3 and (9) we get

$$\Big|\sum_{n=0}^{T-1} \chi(f(\lambda^n))\Big| \le \frac{T}{p-1}\Big(s\,\frac{p-1}{T}\,p^{1/2}\Big) = sp^{1/2},$$

which completes the proof of Lemma 2.

We now return to the proof of Lemma 1. Since the order of λ is T, there exists a character χ_1 of order $p-1$ for which

$$\chi_1(\lambda) = e(1/T). \tag{11}$$

Throughout the proof of Lemma 1, χ_1 will denote a character of order $p-1$ satisfying (11). Since χ is a character of order d, there exists an integer m such that $(m,d)=1$ and

$$\chi = \chi_1^{m(p-1)/d}. \tag{12}$$

First we prove Lemma 1(i). Let $1 \le \gamma \le p-2$ be an integer. We prove that the polynomial $x^\gamma (f(x))^{m(p-1)/d}$ is not of the form $cx^\alpha (g(x))^{p-1}$ with $c \in \mathbb{F}_p$, $\alpha \in \mathbb{N}$ and $g(x) \in \mathbb{F}_p[x]$. Indeed, $f(x)$ has a zero $0 \ne \beta \in \mathbb{F}_p$ with multiplicity t, which is not divisible by d. Then the multiplicity of β in $x^\gamma (f(x))^{m(p-1)/d}$ is $tm(p-1)/d$, and as $d \nmid tm$ the integer $tm(p-1)/d$ is not divisible by $p-1$.

Using (12) and Lemma 2 we obtain

$$\Big|\sum_{n=0}^{T-1} \chi(f(\lambda^n))\chi_1(\lambda^{n\gamma})\Big| = \Big|\sum_{n=0}^{T-1} \chi_1(\lambda^{n\gamma}(f(\lambda^n))^{m(p-1)/d})\Big| \le (s+1)p^{1/2}. \tag{13}$$

By (11) we have

$$\sum_{\gamma=0}^{T-1} \chi_1(\lambda^{\gamma(n-y)}) = \begin{cases} T & \text{if } T \mid n-y, \\ 0 & \text{otherwise.} \end{cases}$$

From this and $K \le T$ we get

$$\begin{aligned}\Big|\sum_{n=M+1}^{M+K} \chi(f(\lambda^n))\Big| &= \Big|\sum_{n=M+1}^{M+T} \chi(f(\lambda^n)) \sum_{y=M+1}^{M+K} \frac{1}{T}\sum_{\gamma=0}^{T-1} \chi_1(\lambda^{\gamma(n-y)})\Big| \\ &= \Big|\frac{1}{T}\sum_{\gamma=0}^{T-1}\Big(\sum_{y=M+1}^{M+K}\chi_1(\lambda^{-\gamma y})\Big)\Big(\sum_{n=M+1}^{M+T}\chi(f(\lambda^n))\chi_1(\lambda^{n\gamma})\Big)\Big|\end{aligned}$$

$$\leq \frac{1}{T}\sum_{\gamma=0}^{T-1}\Big|\sum_{y=M+1}^{M+K}\chi_1(\lambda^{-\gamma y})\Big|\Big|\sum_{n=0}^{T-1}\chi(f(\lambda^n))\chi_1(\lambda^{n\gamma})\Big|.$$

For $\gamma = 0$ we have $|\sum_{n=0}^{T-1}\chi(f(\lambda^n))\chi_1(\lambda^{n\gamma})| = |\sum_{n=0}^{T-1}\chi(f(\lambda^n))|$, which is less than $sp^{1/2}$ by Lemma 2, and thus

$$\sum_{n=M+1}^{M+K}\chi(f(\lambda^n)) \leq \frac{1}{T}\sum_{\gamma=1}^{T-1}\Big|\sum_{y=M+1}^{M+K}\chi_1(\lambda^{-\gamma y})\Big|\Big|\sum_{n=0}^{T-1}\chi(f(\lambda^n))\chi_1(\lambda^{n\gamma})\Big| + sp^{1/2}. \tag{14}$$

By (13) we have

$$\Big|\sum_{n=M+1}^{M+K}\chi(f(\lambda^n))\Big| \leq \frac{(s+1)p^{1/2}}{T}\sum_{\gamma=1}^{T-1}\Big|\sum_{y=M+1}^{M+K}\chi_1(\lambda^{-\gamma y})\Big| + sp^{1/2}. \tag{15}$$

Denoting the distance of α to the nearest integer by $\|\alpha\|$, and using $|1-e(\alpha)| \geq 4\|\alpha\|$ and (11) we get $|1-\chi_1(\lambda^\gamma)| = |1-e(\gamma/T)| \geq 4\|\gamma/T\|$. By using this and the sum of a geometric progression we obtain

$$\sum_{\gamma=1}^{T-1}\Big|\sum_{y=M+1}^{M+K}\chi_1(\lambda^{-\gamma y})\Big| \leq \sum_{\gamma=1}^{T-1}\frac{2}{4\|\gamma/T\|} \leq \sum_{\gamma=1}^{T/2}\frac{T}{\gamma} \leq T(\log(T/2)+1) \leq 1.45\, T\log T. \tag{16}$$

Since $T \leq p-1$, from (15) and (16) we get the statement of Lemma 1(i).

It remains to prove Lemma 1(ii). Suppose that $f(x) = cx^\alpha(g(x))^d$ with $c \in \mathbb{F}_p^*$, $\alpha \in \mathbb{N}$ and $g(x) \in \mathbb{F}_p[x]$. Since the order of the character χ is d we have

$$\Big|\sum_{n=M+1}^{M+K}\chi(f(\lambda^n))\Big| = \Big|\sum_{n=M+1}^{M+K}\chi(\lambda^{\alpha n})\Big|.$$

Hence summing a geometric progression and applying (11), (12) and $|1-e(\alpha)| \geq 4\|\alpha\|$, we get

$$\Big|\sum_{n=M+1}^{M+K}\chi(f(\lambda^n))\Big| \leq \frac{2}{|1-\chi(\lambda^\alpha)|} = \frac{2}{\big|1-e\big(\frac{m(p-1)\alpha}{dT}\big)\big|} \leq \frac{1}{2\big\|\frac{m(p-1)\alpha}{dT}\big\|}. \tag{17}$$

Since $T \mid p-1$ the quotient $m(p-1)\alpha/T$ is an integer. On the other hand, by the condition of Lemma 1(ii) we have $T \nmid (p-1)\alpha/d$, so $d \nmid (p-1)\alpha/T$. As $(m,d) = 1$ we also have $d \nmid m(p-1)\alpha/T$. Therefore

$$\Big\|\frac{m(p-1)\alpha}{dT}\Big\| \geq \frac{1}{d}.$$

Using this and (17) we get Lemma 1(ii).

Proof of Theorem 1. Assume that $a, b, t \in \mathbb{N}$ and $1 \le a+b \le a+tb \le T$. We will give an upper bound for $U(E_N, t, a, b)$.

The order of λ^b is $T/(T,b)$. Clearly, for fixed a and b, $f(\lambda^a x) \equiv 0 \pmod p$ has at most k solutions in x, and thus $f(\lambda^{a+bj}) \equiv 0 \pmod p$ has at most k solutions in j with $1 \le j \le t \le T/(T,b)$. Write $h(x) = f(\lambda^a x)$. Then defining $\left(\frac{a}{p}\right)$ to be 0 for $p \mid a$, we have

$$\begin{aligned} |U(E_N,t,a,b)| &= \left|\sum_{j=1}^{t} e_{a+jb}\right| \le \left|\sum_{j=1}^{t}\left(\frac{f(\lambda^{a+bj})}{p}\right)\right| + k \\ &= \left|\sum_{j=1}^{t}\left(\frac{h((\lambda^b)^j)}{p}\right)\right| + k. \end{aligned} \tag{18}$$

Now $f(x)$ and $h(x)$ are of the same degree, and if $f(x)$ is not of the form $c(g(x))^2$ or $cx(g(x))^2$ with $c \in \mathbb{F}_p^*$ and $g(x) \in \mathbb{F}_p[x]$, then this also holds for $h(x)$. Thus we may apply Lemma 1 with $\left(\frac{n}{p}\right), 2, \lambda^b, T/(T,b)$ and $h(x)$ in place of $\chi(n), d, \lambda, T$ and $f(x)$, to obtain

$$|U(E_N,t,a,b)| \le \left|\sum_{j=0}^{t-1}\left(\frac{h((\lambda^b)^j)}{p}\right)\right| + k \le 4kp^{1/2}\log p + k \le 5kp^{1/2}\log p,$$

which completes the proof.

Proof of Theorem 2. Consider any $D = (d_1, \dots, d_l)$ with non-negative integers $d_1 < \dots < d_l$, and a positive integer M with $M + d_l \le T$. Clearly for fixed d, $f(\lambda^{n+d}) \equiv 0 \pmod p$ has at most k solutions in n with $1 \le n \le T$, so (defining $\left(\frac{0}{p}\right)$ to be 0) we have

$$\begin{aligned} &|V(E_N,M,D)| \\ &\quad= \left|\sum_{n=1}^{M} e_{n+d_1}\cdots e_{n+d_l}\right| \le \left|\sum_{n=1}^{M}\left(\frac{f(\lambda^{n+d_1})}{p}\right)\cdots\left(\frac{f(\lambda^{n+d_l})}{p}\right)\right| + kl \\ &\quad= \left|\sum_{n=1}^{M}\left(\frac{f(\lambda^{n+d_1})\cdots f(\lambda^{n+d_l})}{p}\right)\right| + kl. \end{aligned} \tag{19}$$

If $\varphi^2(x) \mid f(x)$ for a $\varphi(x) \in \mathbb{F}_p[x]$, then in Definition 1 the polynomials f and f/φ^2 generate almost the same sequences:

$$\left(\frac{f(\lambda^n)}{p}\right) = \left(\frac{f/\varphi^2(\lambda^n)}{p}\right)\left(\frac{\varphi(\lambda^n)}{p}\right)^2 = \left(\frac{f/\varphi^2(\lambda^n)}{p}\right)$$

if $\varphi(\lambda^n) \not\equiv 0 \pmod p$, so if $f(\lambda^n) \not\equiv 0 \pmod p$. It follows that (19) also holds with f/φ^2 in place of f, hence throughout the proof of Theorem 2 we may suppose that f is squarefree. We will use the following lemma.

LEMMA 4. *Suppose that $f(x)$ is squarefree, and at least one of the conditions* (a), (b), (c), (d) *of Theorem* 2 *holds. Then the polynomial*

$$h(x) := f(\lambda^{d_1}x)\cdots f(\lambda^{d_l}x)$$

cannot be of the form $c(g(x))^2$ or $cx(g(x))^2$ with $c\in\mathbb{F}_p^*$ and $g(x)\in\mathbb{F}_p[x]$.

We will prove Lemma 4 below. The degree of the polynomial $h(x)$ is kl, so from (19), by using Lemmas 1 and 4, we obtain

$$|V(E_N,M,D)| \le 4klp^{1/2}\log p + kl \le 5klp^{1/2}\log p,$$

which was to be proved. Thus to complete the proof of Theorem 2 it remains to prove Lemma 4.

Proof of Lemma 4. Write $f(x)$ in the form $x^\beta q(x)$, where $x\nmid q(x)$. Then $x\nmid q(\lambda^{d_1}x)\cdots q(\lambda^{d_l}x)$, so $h(x)=f(\lambda^{d_1}x)\cdots f(\lambda^{d_l}x)$ is of the form $c(g(x))^2$ or $cx(g(x))^2$ with $c\in\mathbb{F}_p$ and $g(x)\in\mathbb{F}_p[x]$ if and only if $q(\lambda^{d_1}x)\cdots q(\lambda^{d_l}x)$ is of the form $c(g(x))^2$ with $c\in\mathbb{F}_p$ and $g(x)\in\mathbb{F}_p[x]$.

In order to complete the proof of Lemma 4 we will prove that

$$\widetilde{h}(x) := q(\lambda^{d_1}x)\cdots q(\lambda^{d_l}x)$$

is not of the form $c(g(x))^2$ with $c\in\mathbb{F}_p$ and $g(x)\in\mathbb{F}_p[x]$.

First consider the case when condition (a) of Theorem 2 holds. We prove that the polynomial $\widetilde{h}(x)=q(\lambda^{d_1}x)q(\lambda^{d_2}x)$ cannot be of the form $c(g(x))^2$ with $c\in\mathbb{F}_p^*$ and $g(x)\in\mathbb{F}_p[x]$.

Let $\mathbb{L}$ denote the splitting field of $q(x)$. Then

$$q(x)=c\prod_{i=1}^{k}(x-\alpha_i)$$

with $c\in\mathbb{F}_p$, $\alpha_i\in\mathbb{L}$, $i=1,\dots,k$ and $\alpha_1,\dots,\alpha_k$ are pairwise distinct. It follows that

$$q(\lambda^{d_1}x)=c\lambda^{d_1k}\prod_{i=1}^{k}(x-\alpha_i/\lambda^{d_1}),$$

$$q(\lambda^{d_2}x)=c\lambda^{d_2k}\prod_{i=1}^{k}(x-\alpha_i/\lambda^{d_2}).$$

We have $\alpha_i/\lambda^{d_1}\ne\alpha_j/\lambda^{d_1}$ whenever $i\ne j$. Assume that $\widetilde{h}(x)=c(g(x))^2$. Then all the roots of $\widetilde{h}(x)$ have multiplicity 2 and there exists a permutation $\pi:\{1,\dots,k\}\to\{1,\dots,k\}$ such that

$$\alpha_i/\lambda^{d_1}=\alpha_{\pi(i)}/\lambda^{d_2},\qquad 1\le i\le k.$$

We obtain

$$\alpha_{\pi(i)}=\lambda^{d_2-d_1}\alpha_i,\qquad 1\le i\le k.$$

This implies

$$\alpha_{\pi^s(i)} = \lambda^{s(d_2-d_1)}\alpha_i$$

for any $s \in \mathbb{Z}$ and $1 \le i \le k$.

Let σ denote the multiplicative order of $\lambda^{d_2-d_1}$, i.e. let $\lambda^{\sigma(d_2-d_1)} = 1$. Then π^σ is the identical permutation and we obtain

$$(x-\alpha_i)(x-\lambda^{(d_2-d_1)}\alpha_i)\cdots(x-\lambda^{(\sigma-1)(d_2-d_1)}\alpha_i) \\ = x^\sigma \pm \alpha_i^\sigma, \qquad i = 1,\dots,k.$$

Thus $\sigma \,|\, k$ and $\sigma > 1$ because $\lambda^{d_2-d_1} \ne 1$. Hence $q(x)$ splits into factors of the form $x^\sigma - \alpha_i^\sigma$, i.e. $q(x) = g(x^\sigma)$ with $\sigma > 1$.

Since σ is the order of $\lambda^{d_2-d_1}$ and T is the order of λ, we also have $T \,|\, \sigma(d_2-d_1)$. As $|d_2-d_1| < T$, it follows that $(\sigma, T) \ge 2$, which contradicts condition (a) in Theorem 2.

In order to prove Lemma 4 if (b) or (c) of Theorem 2 holds, write $q(x)$ as the product of irreducible polynomials over $\mathbb{F}_p$; then these irreducible factors are distinct. Let us group these factors so that in each group the equivalent irreducible factors are collected (under the equivalence relation described in Definition 2). We will use the following lemma.

Lemma 5. *Suppose that $q(x)$ is squarefree and $\widetilde{h}(x) = q(\lambda^{d_1}x)\cdots q(\lambda^{d_l}x)$ is of the form $c(g(x))^2$ with $c \in \mathbb{F}_p^*$ and $g(x) \in \mathbb{F}_p[x]$. Let*

$$c_1\varphi(\lambda^{a_1}x), \;\dots,\; c_r\varphi(\lambda^{a_r}x)$$

be a group formed by equivalent irreducible factors of $q(x)$, and write $\mathcal{A} = \{a_1,\dots,a_r\}$, $\mathcal{D} = \{d_1,\dots,d_l\}$. Then for all $\gamma \in \mathbb{Z}_T$ the congruence

$$a + d \equiv \gamma \pmod{T}, \qquad a \in \mathcal{A},\ d \in \mathcal{D},$$

has an even number of solutions.

Proof. If we write $\widetilde{h}(x) = q(\lambda^{d_1}x)\cdots q(\lambda^{d_l}x)$ as the product of irreducible polynomials over $\mathbb{F}_p$, then all the polynomials $\varphi(\lambda^{a_i+d_j}x)$ with $1 \le i \le r$, $1 \le j \le l$ 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 $\widetilde{h}(x)$.

Since distinct irreducible polynomials cannot have a common zero, each of the zeros of $\widetilde{h}(x)$ is of even multiplicity if and only if in each group formed by equivalent irreducible factors of $\widetilde{h}(x)$, every polynomial of the form $\varphi(\lambda^\gamma x)$ occurs with even multiplicity, i.e., for an even number of pairs (a_i, d_j). From this the statement of the lemma follows.

Next we return to the proof of Lemma 4. Clearly, if (b) or (c) of Theorem 2 holds, then there exists a group for which one of the following holds:

(i) T (the order of λ) is a prime, and either

$$|\mathcal{A}| = r, \quad |\mathcal{D}| = l \quad \text{with } \min\{(4r)^l, (4l)^r\} \le T$$

or 2 is a primitive root modulo T,

(ii) $|\mathcal{A}| = 1$.

In cases (i) and (ii) we may use the following addition theorem type lemma:

LEMMA 6. *Let* $\mathcal{A}, \mathcal{D} \subseteq \mathbb{Z}_T$ *with* $|\mathcal{A}| = r$, $|\mathcal{D}| = l$. *Suppose that one of the following conditions holds*:

(a) $\min\{r, l\} = 1$,

(b) *T is a prime and* $\min\{(4r)^l, (4l)^r\} \le T$,

(c) *T is a prime and* 2 *is a primitive root modulo T.*

Then there exists a $\gamma \in \mathbb{Z}_T$ such that

$$a + d \equiv \gamma \ (\operatorname{mod} T), \qquad a \in \mathcal{A}, \ d \in \mathcal{D},$$

has exactly one solution.

Using Lemma 6 we see that the conclusion of Lemma 5 cannot hold, so $\widetilde{h}(x) = q(\lambda^{d_1}x)\cdots q(\lambda^{d_l}x)$ cannot be of the form $c(g(x))^2$ with $c \in \mathbb{F}_p^*$ and $g(x) \in \mathbb{F}_p[x]$ if (a), (b) or (c) of Theorem 2 holds. This proves Lemma 4 in these cases, but it remains to prove Lemma 6.

Proof of Lemma 6. (a) If $\min\{r, l\} = 1$ without loss of generality we may suppose that $r = 1$, so $\mathcal{A} = \{a_1\}$ and $\mathcal{D} = \{d_1, \ldots, d_l\}$. Then all the sums of the form $a + d$ with $a \in \mathcal{A}$ and $d \in \mathcal{D}$ are $a_1 + d_1, \ldots, a_1 + d_l$ and they are different modulo T, which proves the assertion.

(b) See the proof of Theorem 2 in [1].

(c) See the proof of Theorem 3 in [1].

This completes the proof of Lemma 6. Thus we have verified the conclusion of Lemma 4 if (a), (b) or (c) of Theorem 2 holds. If (d) holds, then the assertion of Lemma 4 is trivial, since the degree of the polynomial $h(x) = f(\lambda^{d_1}x)\cdots f(\lambda^{d_l}x)$ is odd as k and l are odd, hence $h(x)$ cannot be of the form $c(g(x))^2$ with $c \in \mathbb{F}_p$ and $g(x) \in \mathbb{F}_p[x]$. So Lemma 4 always holds, and as we have seen, from this Theorem 2 follows.

Proof of Corollary 1. Since ϱ is a root of $f(x)$ of multiplicity 1, there is an irreducible factor $\varphi(x)$ of multiplicity 1 in the factorization of $f(x)$ for which ϱ is a root: $\varphi(x) \mid f(x)$ but $\varphi^2(x) \nmid f(x)$ and $\varphi(\varrho) = 0$.

All polynomials equivalent to $\varphi(x)$ are of the form $c\varphi(\lambda^\gamma x)$. These irreducible polynomials (except $\varphi(x)$) cannot be in the factorization of $f(x)$: $c\varphi(\lambda^\gamma x) \mid f(x)$ is not possible for $T \nmid \gamma$, since $f(x)$ has no root of the form $\lambda^i \varrho$ other than ϱ, but $c\varphi(\lambda^\gamma x)$ has a root of this form: $x = \lambda^{T-\gamma}\varrho$. Thus condition (c) of Theorem 2 holds, so Corollary 1 follows from Theorem 2.

Proof of Corollary 2. Let ϱ be the unique root which is a quadratic non-residue modulo p. Since the order of λ is $(p-1)/2$, λ is a quadratic residue modulo p. Thus $\lambda^i\varrho$ is a quadratic non-residue modulo p, but $f(x)$ has no quadratic residue root other than ϱ. Using Corollary 1 we get the statement.

Proof of Corollary 3. First we slightly extend Lemma 1 in the special case when the multiplicative character is the Legendre symbol.

Lemma 7. *Let p be a prime, $\nu_1, \nu_2 \in \mathbb{F}_p^*$, where ν_2 is of multiplicative order T, and $K, M \in \mathbb{F}_p$ with $K \leq T$. Suppose that $f(x) \in \mathbb{F}_p[x]$ has exactly s distinct zeros, $x \nmid f(x)$ and $f(x)$ is not of the form $c(g(x))^2$ with $c \in \mathbb{F}_p$ and $g(x) \in \mathbb{F}_p[x]$. Then*

$$\left| \sum_{n=M+1}^{M+K} \left(\frac{\nu_1^n f(\nu_2^n)}{p} \right) \right| \leq 8sp^{1/2} \log p.$$

Proof. Using the triangle inequality, the multiplicative property of the Legendre symbol and $\left|\left(\frac{\nu_i}{p}\right)\right| = 1$, we get

$$\begin{aligned} \left| \sum_{n=M+1}^{M+K} \left(\frac{\nu_1^n f(\nu_2^n)}{p} \right) \right| &\leq \left| \sum_{\substack{n=M+1 \\ n\equiv 0 \ (\mathrm{mod}\ 2)}}^{M+K} \left(\frac{\nu_1^n f(\nu_2^n)}{p} \right) \right| + \left| \sum_{\substack{n=M+1 \\ n\equiv 1 \ (\mathrm{mod}\ 2)}}^{M+K} \left(\frac{\nu_1^n f(\nu_2^n)}{p} \right) \right| \\ &= \left| \sum_{\substack{n=M+1 \\ n\equiv 0 \ (\mathrm{mod}\ 2)}}^{M+K} \left(\frac{f(\nu_2^n)}{p} \right) \right| + \left| \sum_{\substack{n=M+1 \\ n\equiv 1 \ (\mathrm{mod}\ 2)}}^{M+K} \left(\frac{f(\nu_2^n)}{p} \right) \right|. \end{aligned}$$

From this by using Lemma 1 we get the statement of Lemma 7.

Next we return to the proof of Corollary 3. Since $\left(\frac{c_1^2+4c_2}{p}\right) = 1$, the two roots of the characteristic polynomial: λ_1 and λ_2 are different and in $\mathbb{F}_p$. Thus x_n is of the form

$$x_n \equiv a_1\lambda_1^n + a_2\lambda_2^n \equiv \lambda_1^n(a_1 + a_2(\lambda_2/\lambda_1)^n) \pmod p$$

with $a_1, a_2 \in \mathbb{F}_p$. Since x_2/x_1 is not a root of the characteristic polynomial, we have $a_i \not\equiv 0 \pmod p$ for $i = 1, 2$. Define $f(x) \in \mathbb{F}_p[x]$ by $f(x) = a_1 + a_2x$. Then

$$x_n \equiv \lambda_1^n f((\lambda_2/\lambda_1)^n) \pmod p.$$

Assume that $a, b, t \in \mathbb{N}$ and $1 \leq a + b \leq a + tb \leq T$. We will give an upper bound for $U(E_N, t, a, b)$.

For fixed a and b, $x_{a+jb} \equiv \lambda_1^{a+jb}(a_1 + a_2(\lambda_2/\lambda_1)^{a+jb}) \equiv 0 \pmod p$ has at most one solution in j with $1 \leq a + jb \leq T$. Then similarly to (18) we get

$$|U(E_N,t,a,b)| \le \left|\sum_{j=1}^{t}\left(\frac{\lambda_1^{a+jb} f((\lambda_2/\lambda_1)^{a+jb})}{p}\right)\right| + 1.$$

Using Lemma 7 we get

$$|U(E_N,t,a,b)| \le 8p^{1/2}\log p + 1 \le 9p^{1/2}\log p,$$

which was to be proved.

Consider any $D=(d_1,\dots,d_l)$ with non-negative integers $d_1<\dots<d_l$, and a positive integer M with $M+d_l\le T$. We give an upper bound for $V(E_N,M,D)$. Similarly to (19) we get

$$\begin{aligned}&|V(E_N,M,D)|\\ &\quad\le \left|\sum_{n=1}^{M}\left(\frac{\lambda_1^{nj}\lambda_1^{d_1+\dots+d_l} f((\lambda_2/\lambda_1)^{n+d_1})\cdots f((\lambda_2/\lambda_1)^{n+d_l})}{p}\right)\right| + l.\end{aligned}$$

If $f((\lambda_2/\lambda_1)^{d_1}x)\cdots f((\lambda_2/\lambda_1)^{d_l}x)$ is not of the form $c(g(x))^2$ with $c\in\mathbb{F}_p$ and $g(x)\in\mathbb{F}_p[x]$, then we can use Lemma 7 to obtain

$$|V(E_N,M,D)| \le 8lp^{1/2}\log p + l \le 9lp^{1/2}\log p,$$

which was to be proved.

In order to complete the proof of Corollary 3 we prove that

$$f((\lambda_2/\lambda_1)^{d_1}x)\cdots f((\lambda_2/\lambda_1)^{d_l}x)$$

is not of the form $c(g(x))^2$ with $c\in\mathbb{F}_p$ and $g(x)\in\mathbb{F}_p[x]$. The degree of each of the polynomials $f((\lambda_2/\lambda_1)^{d_i}x)$ $(1\le i\le l)$ (in x) is 1, so they are irreducible. Their product is a constant multiple of a square of a polynomial only if there exist $1\le i<j\le l$ and $c\in\mathbb{F}_p$ with

$$\begin{gathered}f((\lambda_2/\lambda_1)^{d_i}x) = cf((\lambda_2/\lambda_1)^{d_j}x),\\ a_1 + a_2(\lambda_2/\lambda_1)^{d_i}x = ca_1 + ca_2(\lambda_2/\lambda_1)^{d_j}x.\end{gathered}$$

Since $a_i\not\equiv 0 \pmod p$, it follows that $c\equiv 1 \pmod p$ and thus

$$d_i \equiv d_j \pmod T,$$

which is impossible, since $1\le d_i<d_j\le T$. This completes the proof.

References

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

[2] I. Hankala and A. Tietäväinen, *Codes and number theory*, in: Handbook of Coding Theory, Elsevier, 1998, 1141–1194.

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

[4] I. Shparlinski, *Cryptographic Applications of Analytic Number Theory*, Birkhäuser, Basel, 2003.

[5] W. M. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Math. 536, Springer, Berlin, 1976.

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

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

Department of Computer Science
University of Debrecen
P.O. Box 12
H-4010 Debrecen, Hungary
E-mail: pethoe@inf.unideb.hu

Received on 13.9.2004 (4847)