On non-polynomial Latin squares

Otokar Grošek and Tran van Trung

Abstract

A Latin square $L = L(\ell_{ij})$ over the set $S = \{0, 1, \ldots, n-1\}$ is called totally non-polynomial over Z_n iff

1. there are no polynomials $U_i(y) \in Z_n[y]$ such that $U_i(j) = \ell_{ij}$ for all $i, j \in Z_n$;
2. there are no polynomials $V_j(x) \in Z_n[x]$ such that $V_j(i) = \ell_{ij}$ for all $i, j \in Z_n$.

In the presented paper we describe four possible constructions of such Latin squares which might be of particular interest for cryptographers. Some estimations fro the number of such Latin squares is given as well.

Key-words: Latin squares, polynomial approximation, block ciphers.

1 Introduction and motivation

One of the basic parts of any block cipher algorithm (BCA), or substitution - permutation network (SPN), is a (group) composition of a piece of plaintext, say x, and a part of a round key, say κ. The simplest example of such a situation is probably the Vernam cipher. Another example is so called Extended Feistel Cipher [Čanda, Trung–2002], the round structure of which is visualized on Fig. 1. Symbols $\oplus, \odot, \boxplus$ can be assumed as quasigroup operations.

In [Grošek, Satko, Nemoga–2000] and related papers, the authors showed that using quasigroups instead of groups allows more possibilities to gain ideal parameters for some cryptographic primitives. One such situation is as follows:

Let an attacker has an access to outputs from a composition $x * \kappa$ of messages x and round keys κ, both belonging to a quasigroup $(S, *)$ where $S = \{0, 1, \ldots, n-1\}$. Let Z_n be the $\pmod n$ ring. If we assume Cayley table for $(S, *)$ as a Latin square, say $L = L(\ell_{ij})$

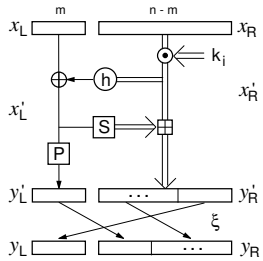

Figure 1: Round Structure

such that $i * j = \ell_{ij}$, his aim is then to find a polynomial function $f : Z_n \times Z_n \to Z_n$ in two variables

$$f(x, y) = a_0 + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \dots \qquad (1)$$

such that

1. for all $i \in Z_n$, $f(i, y) = U_i(x)$ is a permutation polynomial over Z_n;
2. for all $j \in Z_n$, $f(x, j) = V_j(y)$ is a permutation polynomial over Z_n;
3. for all $x, y \in S$, $x * y = \ell_{xy} = f(x, y)$.

As a simple example of such a "polynomial quasigroup" one may assume a quasigroup $(S, *)$ where multiplication is defined as

$$x * y \equiv ax + by + c \pmod{n},$$

where $\gcd(a, n) = \gcd(b, n) = 1$.

From the point of view of a designer, just the opposite is required - to use a Latin square with maximum degree of "non-polynomiality", and this is the main goal of this paper. It is clear that to speak about quasigroups, or Latin squares in this sense is equivalent. Below we show two kinds of constructions for such Latin squares. These constructions serve at least $\exp\{4n \ln n + 2 \ln \ln n\}$ such Latin squares.

2 Non-polynomial Latin squares

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ be the canonical form of n where $r > 1$. Hence, hereafter we assume that the set D of all non-trivial divisors

of n has cardinality at least 2. Recall, that due to *global Euler–Fermat theorem* [Schwarz–1981], for any $x \in Z_n$ we have

$$x^{\max \alpha_i + \lambda(n)} \equiv x^{\max \alpha_i} \pmod{n}$$

where λ is the Carlmichael function. This implies that the highest power in such a polynomial f is at most

$$w = \lambda(n) + \max \alpha_i - 1. \tag{2}$$

Clearly, a decision problem whether for a given quasigroup there exists a permutation polynomial of the form (1) towards to polynomial interpolation over the ring Z_n. We emphasize that in the case $n = p^k$, p-prime, a similar question about polynomial interpolation over the field $GF(p^k)$ is trivial[1]: to any Latin square of the size p^k there exists the unique polynomial such that if $i * j = \ell_{ij}$, $i, j \in S$ then

$$f(x,y) = \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} (1-(x-u)^{n-1})(1-(y-v)^{n-1})\ell_{uv}. \tag{3}$$

Thus any Latin square of the size $n = p^k$, p-prime, is polynomial over the field $GF(p^k)$.

Now we prove a basic lemma for the first type of constructions of non-polynomial Latin squares.

LEMMA 1 *Let d be a non-trivial divisor of n, and $\beta_i \in Z_n$ be distinct elements, where $0 \le i \le n-1$, such that $\beta_d \not\equiv \beta_0 \pmod{d}$. Then there is no polynomial $U(x) \in Z_n[x]$ such that $U(i) = \beta_i$ for all i.*

Proof. Let there exists a polynomial $U(x) = \sum_{k=0}^{w} a_k x^k$, where w has the same meaning as in (2). Then

$$U(d) - U(0) = d \sum_{k=1}^{w} a_k d^{k-1} \equiv \beta_d - \beta_0 \pmod{n}.$$

Since $d|n$ we necessarily have $d|(\beta_d - \beta_0)$, a contradiction with our supposition $\beta_d \not\equiv \beta_0 \pmod{d}$. This completes the proof.

■

[1]Clearly we suppose that there is a one to one mapping from the field $GF(p^k)$ to the set $S = \{0, 1, \ldots, n-1\}$.

COROLLARY 1 *Let d be a non-trivial divisor of n, and $\beta_i \in Z_n$ be distinct elements, where $0 \leq i \leq n-1$, such that $\beta_d \not\equiv \beta_0 \pmod{d}$. Let for a fixed $h \in Z_n$, $\gamma_i \equiv \beta_i + h \pmod{n}$. Then there is no polynomial $U(x) \in Z_n[x]$ such that $U(i) = \gamma_i$ for all i.*

The proof is straightforward by a contradiction with Lemma 1. ■

This Lemma, and Corollary yields the sufficient condition for a non-polynomial permutation over Z_n, and in fact outline the way for a construction of so called *totally non-polynomial Latin squares*.

DEFINITION 1 *A Latin square $L = L(\ell_{ij})$ over the set $S = \{0, 1, \ldots, n-1\}$ is called totally non-polynomial over Z_n iff*

1. *there are no polynomials $U_i(y) \in Z_n[y]$ such that $U_i(j) = \ell_{ij}$ for all $i, j \in Z_n$;*
2. *there are no polynomials $V_j(x) \in Z_n[x]$ such that $V_j(i) = \ell_{ij}$ for all $i, j \in Z_n$.*

Clearly, for totally non-polynomial Latin squares there is no function like (1). Not all Latin squares are polynomial, and in fact there are plenty of totally non-polynomial Latin squares.

Theorem 4.3.1 from [Ding,Pei,Salomaa–1996] yields another construction for finding totally non-polynomial Latin squares in a special case for a square free number n.

THEOREM 1 *Let n be a square free number, $n = p_1 p_2 \ldots p_r$, and $(S, *)$ a quasigroup with n elements. Let $I \subset S$, and $\beta_i \in Z_n$ where $i \in I$. There is a polynomial $U(x) \in Z_n[x]$ such that $U(i) = \beta_i$ for all $i \in I$ iff $i \equiv j \pmod{p_s}$ implies that $\beta_i \equiv \beta_j \pmod{p_s}$ for all possible $i, j \in I$, and $s = 1, 2, \ldots r$.*

3 Construction of a totally non-polynomial Latin square

In this section we present 4 different constructions of totally non-polynomial Latin squares. The first three are based on Lemma 1, and the last one is based on Theorem 1.

CONSTRUCTION 1 *Latin square will be constructed as follows:*

1. *Set* $\ell_{00} = 0$.

2. *Take a permutation* π *of the set* D *without fixed points. Let* $\ell_{0d} = \ell_{d0} = \pi(d)$ *for all* $d \in D$. *This condition is easy to see, since a fixed point would lead to a contradiction with the sufficient condition from Lemma 1.*

3. *Take a permutation* ρ *of the set* $S \setminus \{D \cup 0\}$. *Let* $\ell_{0a} = \ell_{a0} = \rho(a)$ *for all* $a \in S \setminus \{D \cup 0\}$. *As a result we have defined two non-polynomial permutations, namely for the first row and first column, respectively.*

4. *For* $i, j \neq 0$, *let* ℓ_{ij} *be defined as follows: if* $\ell_{i0} - \ell_{00} \equiv h \pmod{n}$ *then* $\ell_{ij} \equiv \ell_{0j} + h \pmod{n}$.

The resulting Latin square satisfies:

- *Each row is a translation of the first row due to the differences served by the first column;*
- *Each column is a translation of the first column due to symmetry* $h + \ell_{0j} \equiv \ell_{j0} + h \equiv \ell_{ij} \pmod{n}$;
- *According to Lemma 1 and its Corollary, all rows and columns represent a non-polynomial permutation.*

EXAMPLE 1 *Let* $n = 6$, *i.e. the set of all non-trivial divisors is* $D = \{2, 3\}$. *Then there are only 3!=6 possible Latin squares. Two of them are displayed below:*

$i \setminus j$	0	1	2	3	4	5
0	0	4	3	2	5	1
1	4	2	1	0	3	5
2	3	1	0	5	2	4
3	2	0	5	4	1	3
4	5	3	2	1	4	0
5	1	5	4	3	0	2

$i \setminus j$	0	1	2	3	4	5
0	0	5	3	2	1	4
1	5	4	2	1	0	3
2	3	2	0	5	4	1
3	2	1	5	4	3	0
4	1	0	4	3	2	5
5	4	3	1	0	5	2

where

D	2	3
π	3	2

$S \setminus \{D \cup 0\}$	1	4	5
ρ_1	4	5	1
ρ_2	5	1	4

Next we need a well known result: number $\mathcal{D}(n)$, of permutations without fixed points over a set of the cardinality n is given by the formula

$$\mathcal{D}(n) = n!\Big(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^n \frac{1}{n!}\Big) \approx n!e^{-1}. \qquad (4)$$

For $n = 0$, $\mathcal{D}(n) = 1$ by definition, and $\mathcal{D}(1) = 0$.

From Construction 1 one can see that

- There is no need to assume permutation π on the whole set of divisors D only. In fact the necessary condition for this construction is to take a nonempty subset of D, say of the cardinality k, and not to allow fixed points. This yields the number $\mathcal{D}(k)$ of possibilities in the case $0 \le k \le |D| - 2$, and one possibility in the case $k = 1$ respectively.

- There are no conditions on the permutation ρ over the set of cardinality $m = n - k - 1$ which gives $m!$ possibilities to choose the rest of the first row in the constructed totally non-polynomial Latin square. This yields the total number of possibilities for the first row as

$$(n-2)!\binom{|D|}{|D|-1} + \sum_{k=0}^{|D|-2} \mathcal{D}(k)\binom{|D|}{k}(n-k-1)! =$$

$$(n-2)!|D| + \sum_{k=0}^{|D|-2} \mathcal{D}(k)\binom{|D|}{k}(n-k-1)!$$

- Finally, the same generalization can be made with the first column.

  Thus we have a lower bound $\mathcal{L}_{np}$ for the number of totally non-polynomial Latin squares over a set of the size n:

$$\mathcal{L}_{np} \ge \Big((n-2)!|D| + \sum_{k=0}^{|D|-2} \mathcal{D}(k)\binom{|D|}{k}(n-k-1)!\Big)^2. \qquad (5)$$

  Recall that the number of divisors of $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ is

$$\sigma(n) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_r + 1), \qquad (6)$$

and for large $n, |D| = \sigma(n) \approx \ln n$ in average. Then for a randomly chosen and large n this number is of the size $\approx \exp\{4n \ln n + 2 \ln \ln n\}$.

CONSTRUCTION 2

1. *Set* $\ell_{00} = 0$.
2. *Take a permutation* π_r *of the subset of* D *without fixed points. This condition is easy to see, since a fixed point would lead to a contradiction with the sufficient condition from Lemma 1.*
3. *Take a permutation* ρ_r *of the set* $S \setminus \{D \cup 0\}$. *As a result we have defined a non-polynomial permutation for the first row.*
4. *Take a permutation* π_c *of the subset of* D *without fixed points. This condition is easy to see, since a fixed point would lead to a contradiction with the sufficient condition from Lemma 1.*
5. *Take a permutation* ρ_c *of the set* $S \setminus \{D \cup 0\}$. *As a result we have defined a non-polynomial permutation for the first column.*
6. *For* $i, j \neq 0$, *let* ℓ_{ij} *be defined as follows: if* $\ell_{i0} - \ell_{00} \equiv h \pmod{n}$ *then* $\ell_{ij} \equiv \ell_{0j} + h \pmod{n}$.

EXAMPLE 2 *Let* $n = 6$, *i.e. the set of all non-trivial divisors is* $D = \{2, 3\}$. *Then there are other possible Latin squares not mentioned in Example 1, namely:*

1. *For* $k = 0$ *we have 3! = 6 permutations over the set* $\{1, 4, 5\}$ *and one permutation without fixed points.*
2. *For* $k = 1$, *i.e. the subset* $\{2\} \subset D$ *we have 4!=24 permutations over the set* $\{1, 3, 4, 5\}$.
3. *Similarly, for* $k = 1$, *and the subset* $\{3\} \subset D$ *we have another 24 possibilities.*
4. *Thus we have* $2 * 4! + 3! = 54$ *choices for the first row, and the same number for the first column, i.e. at least* $54^2 = 2916$ *non-polynomial Latin squares in total. Two of them are displayed below.*

$i \setminus j$	0	1	2	3	4	5
0	0	4	3	2	5	1
1	5	3	2	1	4	0
2	3	1	0	5	2	4
3	2	0	5	4	1	3
4	1	5	4	3	0	2
5	4	2	1	0	3	5

$i \setminus j$	0	1	2	3	4	5
0	0	5	3	2	1	4
1	4	3	1	0	5	2
2	3	2	0	5	4	1
3	2	1	5	4	3	0
4	5	4	2	1	0	3
5	1	0	4	3	2	5

Here is a modification of the previous Construction allowing fixed points:

CONSTRUCTION 3

1. *Set* $\ell_{00} = 0$.
2. *Choose* $j_0 \in D$ *and* $u \in S$ *such that* $u \not\equiv 0 \pmod{j_0}$.
3. *Take a permutation* π_r *of the set* $S \setminus \{0, u\}$.
4. *Set* $\ell_{0j_0} = u, \ell_{0,j} = \pi_r(j)$ *for the remaining elements* $j \neq j_0$.
5. *Choose* $i_0 \in D$ *and* $v \in S$ *such that* $v \not\equiv 0 \pmod{i_0}$.
6. *Take a permutation* π_c *of the set* $S \setminus \{0, v\}$.
7. *Set* $\ell_{i_0 0} = v, \ell_{i0} = \pi_c(i)$ *for the remaining elements* $i \neq i_0$.
8. *Having the first row and the first column of* L *fill the empty cells with*

$$\ell_{ij} \equiv \ell_{i0} + \ell_{0j} \pmod{n}.$$

Remark that as in previous constructions for all $i, j \in S$

$$\ell_{ij} - \ell_{i0} \equiv \ell_{0j} - \ell_{00} \pmod{n}$$

$$\ell_{ij} - \ell_{0j} \equiv \ell_{i0} - \ell_{00} \pmod{n},$$

i.e. each row (resp. column) of L *is a translation of another row (resp. column). By Lemma 1 the row* i_0 *(resp. column* j_0*) is non-polynomial. Therefore each row (resp. column) is non-polynomial.*

EXAMPLE 3 *Again for $n = 6$ one possible Latin square is as follows (chosen elements $u = 3, v = 5$ are in box):*

$i \setminus j$	0	1	2	3	4	5
0	$\boxed{0}$	1	$\boxed{3}$	2	5	4
1	4	5	1	0	3	2
2	2	3	5	4	1	0
3	$\boxed{5}$	0	2	1	4	3
4	3	4	0	5	2	1
5	1	2	4	3	0	5

In the Construction 3 we have $(n - \frac{n}{j_0})$ possibilities for u. For each such chosen u there are $(n-2)!$ possibilities to fill the first row of L. Similarly, there are $(n - \frac{n}{i_0})$ choices for v, and for all such v we have $(n-2)!$ possibilities to fill the first column of L. Hence the number of Latin squares is

$$\mathcal{L}_{np} \geq (n - \frac{n}{j_0})(n - \frac{n}{i_0})(n-2)! \tag{7}$$

Our last construction is based on Theorem 1.

CONSTRUCTION 4

1. *Set $\ell_{00} = 0$.*
2. *Choose $j_0 \in \{p_1, p_2, \ldots, p_r\}$ and $u \in S$ such that $u \not\equiv 0 \pmod{j_0}$.*
3. *Choose $i_0 \in \{p_1, p_2, \ldots, p_r\}$ and $v \in S$ such that $v \not\equiv 0 \pmod{i_0}$.*
4. *Take a permutation π_r of the set $S \setminus \{0, u\}$ for the row i_0 such that for $j \neq 0$ is*

$$\ell_{i_0 j} - \ell_{0j} \not\equiv 0 \pmod{i_0}.$$

5. *Take a permutation π_c of the set $S \setminus \{0, v\}$ for the column j_0 such that for $i \neq 0$ is*

$$\ell_{ij_0} - \ell_{i0} \not\equiv 0 \pmod{j_0}.$$

6. *Having the row i_0 and the column j_0 of L try to fill the remaining cells with ℓ_{ij}. If the partially constructed Latin square by*

steps 1–5 can be extended to the Latin square over the set S, then it is totally non-polynomial. To prove it, let t be any row of L. Take $i = 0$ and $j = j_0$. Then $i \equiv j \pmod{j_0}$. But

$$\ell_{tj_0} - \ell_{t0} \not\equiv 0 \pmod{j_0}$$

by construction. By Theorem 1 the row t cannot be described by any polynomial. Similarly we can use the same arguments for any column. Therefore each row (resp. column) is non-polynomial.

At this place we should point out that steps 2-5 from Construction 4 can be extended to a larger subset of $\{p_1, p_2, \ldots, p_r\}$.

4 The best polynomial approximation

One may also wonder about the best polynomial approximation of some cells for a totally non-polynomial Latin square. What does it mean we present on the Latin square from Example 1.

Let us assume the Latin square from Example 1, and a polynomial function $g(x, y) = 4x + 4y$. This function coincide with the following values of this Latin square: $\ell_{00}, \ell_{01}, \ell_{10}, \ell_{11}, \ell_{25}, \ell_{45}, \ell_{52}, \ell_{54}$, i.e. with 8 out of 36 values. In this sense one may look for a better approximation, i.e. for a polynomial which coincide with more values than the presented g.

To find the best polynomial approximation for a given Latin square of the size n, based on the exhaustive computer search (a non-polynomial algorithm) needs

1. searching for all possible functions $g(x, y)$ (coefficients a_{ij}, $i, j = 0, 1, 2, \ldots, (w + 1)$), i.e.

   $$1 + 2 + \ldots + (w + 1) = \frac{(w + 2)(w + 1)}{2}$$

   steps;

2. n choices for each a_{ij}, i.e.

   $$n^{\frac{(w+2)(w+1)}{2}}$$

   steps;

3. to each possible function $g(x, y)$ find its n^2 values, and

4. compare them to ℓ_{ij}.

This represents

$$n^{2+\frac{(w+2)(w+1)}{2}}$$

steps, and at most n^2 comparisons in each tested case. Finally the best polynomial with the highest number $N_c(n)$ of fitting with numbers in cells is found.

The function $g(x, y) = 4x + 4y$, mentioned above, is not the best possible of this kind. One of the best one, found by exhaustive computer search is $f(x, y) = 2 + 2x + 2y + 4xy + xy^2 + x^2y + x^2y^2$ with the number of coincidence 13. Coincidence is marked in bold:

$i \setminus j$	0	1	2	3	4	5
0	0	**4**	3	**2**	5	1
1	**4**	2	1	0	3	**5**
2	3	1	0	5	**2**	**4**
3	**2**	0	5	4	1	**3**
4	5	3	**2**	1	**4**	0
5	1	**5**	**4**	**3**	0	2

Now the question arises naturally: for a given totally non-polynomial Latin square find some lower and upper bound of the number $N_c(n)$ of the best coincidence accomplished by polynomial approximation. Trivial bounds are $n \leq N_c(n) \leq (n-1)^2$. The Latin square from Example 3 has one of the best polynomial approximations $f(x, y) = 1 + x + 5y + y^2 + 3xy$ with $N_c(6) = 13$.

A better non-polynomial Latin square based on Construction 4 is presented in the next example. In this example, the set from steps 2-5 is extended to 3 elements. In fact, for $n = 6$ it is the best we have found.

EXAMPLE 4 *Again for $n = 6$ one possible Latin square is presented below. Elements which coincide are in bold. The best polynomial approximation is $f(x, y) = 4 + 3x + 3y$ with number of coincidence $N_c(6) = 12$.*

$i \setminus j$	0	1	2	3	4	5
0	0	2	5	**1**	**4**	3
1	2	**4**	**1**	3	0	5
2	5	**1**	**4**	0	3	2
3	**1**	3	0	2	5	**4**
4	**4**	0	3	5	2	**1**
5	3	5	2	**4**	**1**	0

NOTE The fact that $f(x, y)$ is the best polynomial approximation does not yields that $U_i(y) = f(i, y)$ or $V_j(x) = f(x, j)$ are the best polynomial approximations for rows or columns respectively.

5 Conclusions

Although there is some information about the set of divisors of n, the bit size of a secret for a randomly chosen totally non-polynomial Latin square is the same as to choose two specific permutations, one for the first row and another one for the first column, i.e. $2\log_2(n!) \approx n \ln n$.

To have an idea about the number of possible totally non-polynomial Latin squares one should compare it with the number of distinct normalized Latin squares which is of the magnitude of $L(n) \approx (e^{-2}n)^{n^2} \approx \exp\{n^2 \ln n\}$. Unfortunately, we do not have an upper bound for $N_c(n)$ accomplished by any of our Constructions 1 to 4. We finish with a Hypothesis:

Hypothesis Let n be a square free number, $n = p_1 p_2 \dots p_r$ where $p_1 < p_2 < \dots < p_r$. Then there exists a Latin square over the set $\{0, 1, 2, \dots, n-1\}$ such that the best polynomial approximation coincide with exactly np_1 cells and this result is the best possible one.

References

[Belousov–1967] Belousov, V.D. 1967. *Foundations of the Theory of Quasigroups and Loops.* Nauka, Moscow. (In Russian.)

[Brualdi–1991] Brualdi, R.A., Ryser, H.J. 1991. *Combinatorial Matrix Theory*, Cambridge University Press.

[Čanda, Trung–2002] Čanda, V., Trung, T.V. 2002. Scalable block ciphers based on Feistel-like structure. TATRA MOUNTAINS Mathematical Pub. 25(2002), pp. 39-66.

[Dénes, Keedwell–1974] Dénes, J., Keedwell A.D. 1974. *Latin Squares and their Applications.* Akadémiai Kiadó, Budapest.

[Ding,Pei,Salomaa–1996] Ding, C., Pei, D., Salomaa, A. 1996. Chinese Remainder Theorem. Applications in Computing, Coding, Cryptography. World Scientific, Singapore.

[Grošek, Nemoga, Satko–2000] Grošek, O., Nemoga, K., Satko, L. 2000. Generalized Perfectly nonlinear functions. TATRA MOUNTAINS Pub. 20(2000), pp. 121-131.

[Grošek, Wei–1999] Grošek, O., Wei, W. 1998. Bent–like functions on groupoids. Pure Mathematics and Applications. 10(1999), No.3, Budapest (H)& Siena (I) Publisher, pp. 267-278.

[Grošek, Satko, Nemoga–2000] O. Grošek, K. Nemoga, L. Satko 2000. Ideal difference tables from an Al gebraic point of view. Ammendment to CRIPTOLOGA y SEGURIDAD de la INFORMACIN. Editors - Pino Cabalero Gil and Candelaria Hernandez Goya, RA-MA, Madrid, 2000, pp. 453-454, 43-53.

[Satko, Grošek, Nemoga–2001] Satko, L., Grošek, O., Nemoga, K. 2001. Extremal generalized S–boxes. Abstracts of TATRACRYPT '01, to apperar in Computing and Informatics.

[Schwarz–1981] Š. Schwarz: The role of semigroups in the elementary theory of numbers. Math. Slovaca Vol. 31, 1981, 369–395.

Institut Für Experimentelle
Mathematik
Universität Essen 45326 Essen, Germany
e-mail: trung@exp-math.uni-essen.de

Slovak University of Technology
Department of Mathematics
812 19 Bratislava, Slovakia
e-mail: grosek@kmat.elf.stuba.sk