On non-polynomial Latin squares

Otokar Grošek, Peter Horák and Tran van Trung

O. Grošek
Department of Mathematics, Slovak University of Technology,
812 19 Bratislava, Slovakia
grosek@kmat.elf.stuba.sk

P. Horák
Interdisciplinary Arts & Sciences, University of Washington at Tacoma,
87402 Tacoma WA, USA
horak@u.washington.edu

Tran van Trung
Institut für Experimentelle Mathematik, Universität Duisburg-Essen,
Ellernstraße 29, 45326 Essen, Germany
trung@exp-math.uni-essen.de

Keywords Latin squares, polynomial approximation, block ciphers

Abstract

It turns out that Latin squares which are hard to approximate by a polynomial are suitable to be used as a part of block cipher algorithms. In this paper we state basic properties of those Latin squares and provide their construction.

1 Introduction and motivation

Let Z_n be the ring of integers taken $\mod n$. In this paper we use $\mathcal{F}(n)$ for the set of all polynomial functions $f : Z_n \times Z_n \to Z_n$, $f(x,y) = a_0 + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + \ldots$, and $\mathcal{L}(n)$ for the set of all Latin squares of order n with the symbol set $\{0, 1, ..., n-1\}$.
One of the basic parts of any block cipher algorithm (BCA), or substitution - permutation network (SPN), is a (quasigroup) composition of a piece of plaintext, say x, and a part of a round key, say k. One of the simplest examples is probably the Vernam cipher. Another example is the so called Extended Feistel Cipher [Čanda, Trung–2002], the round structure of which is visualized in Fig. 1. The symbols $\oplus, \odot, \boxplus$ represent (quasi)group operations.
In [Grošek, Satko, Nemoga–2000] and related papers, the authors showed that using quasigroups instead of groups allows more options to gain ideal parameters for some cryptographic primitives.

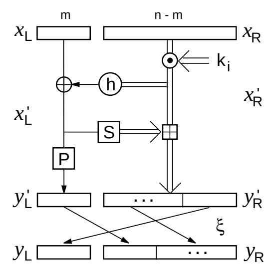

Figure 1: Round Structure

Consider the following scenario: An attacker has access to outputs from a composition $x * k$ of messages x and round keys k, both belonging to a quasigroup $(S, *)$ where $S = \{0, 1, \ldots, n-1\}$. Then his/her aim is to find a polynomial function $f \in \mathcal{F}(n)$ such that for all $x, y \in S$, $x * y = f(x, y)$. Thus, from the point of view of a designer, just the opposite is required - to use a quasigroup which is hard to approximate by a polynomial in $\mathcal{F}(n)$.

The main goal of this paper is to formalize the notion of those quasigroups, state some of their properties and provide their construction.

We will understand the Cayley table of a quasigroup $(S, *)$, $S = \{0, 1, \ldots, n-1\}$, as a Latin square $L = L(\ell_{ij}) \in \mathcal{L}(n)$ with $\ell_{ij} = i * j$. Therefore the notions of a quasigroup and a Latin square will be freely interchanged in the paper. Since it is more natural and handy to express definitions and results concerning the topic in the language of Latin squares, the notion of a quasigroup will be used only sporadically.

If there is a polynomial function $f \in \mathcal{F}(n)$ such that, for all $x, y \in S$, $x*y = \ell_{xy} = f(x, y)$ then the Latin square $L = L(\ell_{ij})$ (the quasigroup $(S, *)$) will be called polynomial, otherwise we call L ($(S, *)$) non-polynomial. A simple example of a polynomial quasigroup is the quasigroup $(S, *)$ with the operation $*$ defined by

$$x * y \equiv ax + by + c \mod n,$$

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

To be able to measure "how far" a Latin square $L = L(\ell_{ij}) \in \mathcal{L}(n)$ is from a polynomial one we introduce some more notation. For $f \in \mathcal{F}(n)$ we use $c(L, f)$ to be the number of pairs (i, j) for which $\ell_{ij} = f(i, j)$. Further, we define $c(L) = \max c(L, f)$ where the maximum runs over all $f \in \mathcal{F}(n)$ and say that $c(L)$ is the coincidence number of L. We call $f \in \mathcal{F}(n)$ a best polynomial approximation of L if $c(L, f) = c(L)$. Finally, we call a Latin square L most non-polynomial if $c(L) \leq c(L')$ for all $L' \in \mathcal{L}(n)$. Thus, a Latin square L is most non-polynomial if L has the smallest coincidence number of all squares in $\mathcal{L}(n)$.

Example 1.1 It has been found, by an exhaustive computer search, that $f_0 \in \mathcal{F}(6)$, $f_0(x,y) = 4 + 3x + 3y$ is a best polynomial approximation of the Latin square L given below. Hence, $c(L, f_0) = c(L) = 12$. The cells in which L and f_0 coincide are typeset in bold.

$i \setminus j$	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

2 Non-polynomial Latin squares

In this section we show that, given a Latin square $L \in \mathcal{L}(n)$, we can decide in a finite time whether L is polynomial and find its polynomial function or its best polynomial approximation. Further we show that nearly all Latin squares in $\mathcal{L}(n)$ are non-polynomial.

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ be the prime number factorization of n. With respect to the global Euler–Fermat theorem [Schwarz–1981], for any $x \in Z_n$ we have

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

where λ is the Carmichael function. This implies that to each $f \in \mathcal{F}(n)$ there exists $f^* \in \mathcal{F}(n)$ so that $f(x,y) = f^*(x,y)$ for all $x, y \in Z_n$, and the degree of $f^* \leq w$, where $w = \lambda(n) + \max \alpha_i - 1$. Therefore, to determine whether a Latin square is polynomial, and to find its polynomial function or its best polynomial approximation it is sufficient to calculate the coincidence number $c(L, f)$ only for a finite number of polynomials f. More precisely, the number of polynomials one needs to test equals the number of polynomials $f \in \mathcal{F}(n)$ with maximum degree at most w. However, the total number of polynomials in $\mathcal{F}(n)$ of the maximum degree at most w is n^m where $m = (1 + 2 + ... + (w+1)) = \frac{(w+2)(w+1)}{2}$.
We recall now that the Carmichael function λ can be bounded from above by the Euler totient function φ. Then

$$\frac{(w+2)(w+1)}{2} \approx (w+1)^2/2 = (\lambda(n) + \max \alpha_i)^2/2 \leq \varphi(n)^2/2.$$

Since on average $\varphi(n) \approx \frac{6n}{\pi^2}$, we have $\varphi(n)^2/2 \approx 0.20n^2$. This yields

$$n^{2+\frac{(w+2)(w+1)}{2}} \approx \exp\{0.20n^2 \ln(n)\}.$$

Thus, it is needed to calculate the coincidence number $c(L, f)$ for approximately $\exp\{2n^2 \ln(n)\}$ functions in $\mathcal{F}(n)$. Therefore this exhaustive search for a larger value of n is unrealistic.
Further, it follows from the above discussion that the number of distinct polynomials (we consider two polynomials f and g distinct if there is at least one pair (x, y) so that $f(x, y) \neq g(x, y)$) in $\mathcal{F}(n)$ is at most n^m. Thus, the number of polynomial Latin squares in $\mathcal{L}(n)$ is at most of that order as well. As the total number of Latin squares in $\mathcal{L}(n)$ is more than $n!(n-1)!\dots 2!1!$ (see, e.g. [Dénes, Keedwell–1974], [Godsil, McKay–1990]), nearly all Latin squares are non-polynomial.
We emphasize that in the case $n = p^r$, p being a prime, a similar question about polynomial interpolation over the field $GF(p^r)$ is trivial. To any Latin square $L = L(\ell_{ij})$ of order p^r there exists a unique polynomial f such that for all i, j, $f(i, j) = \ell_{ij}$. This polynomial is given by

$$f(x, y) = \sum_{u=0}^{n-1} \sum_{v=0}^{n-1} \left(1 - (x-u)^{n-1}\right)\left(1 - (y-v)^{n-1}\right)\ell_{uv}. \qquad (2.1)$$

Thus any Latin square of size $n = p^r$, p prime, is polynomial over the field $GF(p^r)$. This immediately implies that each Latin square of a prime power order n is polynomial over $GF(p^r)$.

3 Totally non-polynomial Latin square.

As mentioned above, the aim of a designer of a block cipher algorithm is to find a Latin square which is hard to approximate polynomially. Hypothetically, a most non-polynomial Latin square might possess a row or a column that is polynomial, which would significantly simplify breaking the cipher for an attacker, e.g. using a chosen plaintext attack, or related keys attack. Therefore, from a block cipher prospective, the designer is interested to construct a Latin square L with the property that no row and no column of L is polynomial.
Formally, a permutation π of the set $\{0, 1, ..., n-1\}$ is polynomial if there is a polynomial $U(x) \in Z_n[x]$ so that $U(x) = \pi(x)$ for all $x \in Z_n$, otherwise π is called non-polynomial. Since each row/column of a Latin square $L \in \mathcal{L}(n)$ is a permutation of $\{0, 1, ..., n-1\}$ we will speak of a polynomial (non-polynomial) row/column of L in the sense of the above definition.
Now we are ready to define what is meant by a totally non-polynomial Latin square, and in what follows we focus on Latin squares with this property.

Definition 3.1 *A Latin square L is called totally non-polynomial if each row and each column of L is non-polynomial.*

To construct a totally non-polynomial Latin square L with a small coincidence number $c(L)$ we now focus on permutations that are "far" from being polynomial.

Definition 3.2 *Let π be a permutation on the set $\{0, 1, \ldots, n-1\}$. Then a set $J \subset \{0, 1, \ldots, n-1\}$ is called a non-polynomial support of π if for each polynomial $U(x) \in Z_n[x]$ we have $U(j) = \pi(j)$ for at most one element of $j \in J$.*

We start with a simple lemma which provides a fundamental ingredient for our construction of a totally non-polynomial Latin square.

Lemma 3.3 *Let $J \neq \varnothing$ be a non-polynomial support of a permutation π on $\{0, 1, ..., n-1\}$, and $h \in \{0, 1, ..., n-1\}$. Then the permutation β on $\{0, 1, ..., n-1\}$ given by $\beta(x) = \pi(x+h)$ for all $x \in \{0, 1, ..., n-1\}$ has a non-polynomial support J' of size $|J'| = |J|$. In particular, there is a permutation β on $\{0, 1, ..., n-1\}$ with a non-polynomial support J' so that $|J| = |J'|$, and $0 \in J'$.*

The sum and the difference of two elements of $\{0, 1, ..., n-1\}$ in the lemma and its proof are taken $\mod n$.

Proof. Let J be a non-polynomial support of π. Set $J' = \{y,$ there is $x \in J, y = x - h\}$. To see that J' is a non-polynomial support of β, suppose by the way of contradiction that there is a polynomial $U(x) \in Z_n[x]$ and $u, v \in J'$ so that $U(u) = \beta(u)$ and $U(v) = \beta(v)$. Set $V(x) = U(x-h)$. Obviously, $V(x) \in Z_n[x]$ as well. Further, $u, v \in J'$ implies $u + h, v + h \in J$. However, $V(u+h) = U(u) = \beta(u) = \pi(u+h)$ and $V(v+h) = U(v) = \beta(v) = \pi(v+h)$ contradict the assumption that J is a non-polynomial support of π. Thus, J' is a non-polynomial support of β. As $|J'| = |J|$, the proof of the first part of the statement is complete. To see the second part, set $h = b$, where b is an element of J. ■

Now we are ready to describe a construction of totally non-polynomial Latin squares. Recall that the sum of two elements of $\{0, 1, ..., n-1\}$ is taken $\mod n$.

Construction 3.4 *Let π be a permutation on $\{0, 1, ..., n-1\}$ and let $L = L(\ell_{ij})$ be an $n \times n$ array.*

Step 1. The first row of L is formed by π, i.e. $\ell_{0j} = \pi(j)$.

Step 2. For $i > 0$ and $j = 0, 1, \ldots, n-1$, $\ell_{ij} = \pi(i+j)$.

It is easy to see that L defined above is a Latin square. Such a Latin square is known as *back circulant.* We use $L(\pi)$ to denote the Latin square obtained by the above construction. As each row of L is a cyclic shift of π, Lemma 3.3 guarantees that if π is a non-polynomial permutation each row of $L(\pi)$ is totally non-polynomial and has a non-polynomial support of the same size

as π does. Clearly, $L(\pi)$ is symmetric, hence we have the same property for its columns. Hence $L(\pi)$ is totally non-polynomial.
To estimate the coincidence number of L we state:

Theorem 3.5 *Let J be a non-polynomial support of a permutation π on $\{0, 1, ..., n-1\}$. Then the coincidence number $c(L(\pi)) \leq n(n - |J| + 1)$.*

Proof. Let $f \in \mathcal{F}(n)$ be a best polynomial approximation of $L(\pi)$. Then, by the definition of the non-polynomial support, for each $i = 0, 1, \ldots, n-1$, $f(i, x) \in Z_n[x]$ coincides with at most $n - |J| + 1$ elements in the i-th row of $L(\pi)$. Thus, f coincides with at most $n(n - |J| + 1)$ elements of $L(\pi)$, hence $c(L(\pi)) \leq n(n - |J| + 1)$. ■

To get Latin squares with small coincidence number, in the rest of the section we deal with non-polynomial permutations that are hard to approximate.
The next theorem provides, for a general natural number n, a sufficient condition for a set to be a non-polynomial support.

Theorem 3.6 *Let $J \subset \{0, 1, \ldots, n-1\}$ and π be a permutation on $\{0, 1, \ldots, n-1\}$ such that the following condition holds:*

(A) *for each $x, y \in J, x \neq y$, there is a non-trivial divisor $d = d(x, y)$ of n so that $x \equiv y \mod d$ and $\pi(x) \not\equiv \pi(y) \mod d$.*

Then J is a non-polynomial support of π.

Proof. Let there exist a polynomial $U(x) \in Z_n[x], U(x) = \sum_{k=0}^{w} a_k x^k$, and $x, y \in Z_n$, $x \neq y$, so that $U(x) = \pi(x)$ and $U(y) = \pi(y)$. By [Schwarz–1981] we may assume that w is a finite number. Then $U(x) - U(y) \equiv \sum_{k=0}^{w} a_k (x^k - y^k) \mod n$. By the condition (A), $x \equiv y \mod d$, d being a non-trivial divisor of n, that is, $x = rd + y$, where r is a natural number. Applying the binomial theorem we get $x^k - y^k = (rd + y)^k - y^k = \sum_{i=1}^{k} b_i d^i = d \sum_{i=1}^{k} b_i d^{i-1}$, where $b_i \in Z_n$. Hence, $U(x) - U(y) \equiv d \sum_{k=1}^{w} c_k d^{k-1} \equiv \pi(x) - \pi(y) \mod n$, and $c_k \in Z_n$. Since $d|n$ we necessarily have $d|(\pi(x) - \pi(y))$, a contradiction with our assumption $\pi(x) \not\equiv \pi(y) \mod d$. This completes the proof. ■

The next theorem shows that for each n there is a permutation with relatively large non-polynomial support.

Theorem 3.7 *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, k \geq 2$, where $p_1, p_2, ..., p_k$ are distinct primes, and $p_1^{\alpha_1} < p_2^{\alpha_2} < \cdots < p_k^{\alpha_k}$. Then there exists a permutation π on $\{0, 1, 2, \ldots, n-1\}$ with a non-polynomial support of size $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{k-1}^{\alpha_{k-1}}$.*

It turns out that it is very handy for our purpose to use a one-to-one representation of $x \in Z_n$ by means of a $k-$tuple $(x \mod p_1^{\alpha_1}, x \mod p_2^{\alpha_2}, \dots, x \mod p_k^{\alpha_k})$. Here in fact we are utilizing a well-known fact, namely the Chinese Remainder Theorem, that two rings Z_n and $Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \dots Z_{p_k^{\alpha_k}}$ are isomorphic and the mapping $x \to (x \mod p_1^{\alpha_1}, x \mod p_2^{\alpha_2}, \dots, x \mod p_k^{\alpha_k})$ is their isomorphism. For the sake of simplicity we will write shortly $x = (x \mod p_1^{\alpha_1}, x \mod p_2^{\alpha_2}, \dots, x \mod p_k^{\alpha_k})$, and use $(x)_i$ for the i-th coordinate of x in the representation. Clearly, for $x, y \in Z_n$, $x \equiv y \mod p_i^{\alpha_i}$ iff $(x)_i = (y)_i$.

Proof. Consider the set $J \subset Z_n$, $J = \{(a_1, a_2, \dots, a_{k-1}, 0), 0 \le a_i \le p_i^{\alpha_i} - 1, i = 1, 2, \dots, k-1\}$. Hence $|J| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{k-1}^{\alpha_{k-1}}$. Further, let π be a permutation on $\{0, 1, \dots, n-1\}$ so that if $x = (a_1, a_2, \dots, a_{k-1}, 0)$ then $\pi(x) = (0, a_1, a_2, \dots, a_{k-1})$. Note that as $(\pi(x))_{i+1} = (x)_i, i = 1, 2, \dots, k-1$, we have $(\pi(x))_{i+1} < p_i^{\alpha_i} < p_{i+1}^{\alpha_{i+1}}$. This means that the k-tuple $\pi(x) = (0, a_1, a_2, \dots, a_{k-1})$ is a representation of a number $y \in Z_n$.
Let $x, y \in J, x \ne y$. Then there is an index $i, 1 \le i \le k-1$ so that $(x)_i \ne (y)_i$. Let j be the largest index with the property. This implies that $(x)_j \ne (y)_j$ and $(x)_{j+1} = (y)_{j+1}$. In turn this implies that $(\pi(x))_{j+1} \ne (\pi(y))_{j+1}$. Hence $x \equiv y \mod p_{j+1}^{\alpha_{j+1}}$ and $\pi(x) \not\equiv \pi(y) \mod p_{j+1}^{\alpha_{j+1}}$, i.e. J satisfies the condition (A) of Theorem 3.6. Therefore J is a non-polynomial support of π. As J is of size $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{k-1}^{\alpha_{k-1}}$ the proof is complete. ■

As an immediate consequence of Theorem 3.5 and 3.7 we get

Corollary 3.8 *Let* $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, k \ge 2$, *where* $p_1, p_2, \dots, p_k$ *are distinct primes, and* $p_1^{\alpha_1} < p_2^{\alpha_2} < \dots < p_k^{\alpha_k}$. *Then there is a Latin square* $L \in \mathcal{L}(n)$ *with* $c(L) \le n(n - \frac{n}{p_k^{\alpha_k}} + 1)$.

Although we believe that Theorem 3.7 gives a permutation with the largest possible non-polynomial support among all permutations on $\{0, 1, \dots, n-1\}$, we are able to provide some evidence in this regard only for n being a square free number. To be able to do so first we state a necessary and sufficient condition for a set to be a non-polynomial support in this case. This condition is similar to the condition (A) in Theorem 3.6.

Theorem 3.9 *Let* n *be a square free number,* $n = p_1 p_2 \dots p_k$, *where the* $p_i' s$ *are distinct primes. Let* π *be a permutation on* $\{0, 1, 2, \dots, n-1\}$. *Then a set* $J \subset \{0, 1, 2, \dots, n-1\}$ *is a non-polynomial support of* π *iff the following condition holds:*

(A') *for each* $x, y \in J$, $x \ne y$, *there is* $i = i(x, y)$ *so that* $x \equiv y \mod p_i$ *and* $\pi(x) \not\equiv \pi(y) \mod p_i$.

We start by stating a result of Ding et al. that is a key ingredient of our proof.

Theorem 3.10 *(Theorem 4.3.1 in [Ding, Pei, Salomaa–1996]) Let n be a square free number, $n = p_1 p_2 \dots p_k$, the p_i's primes, and let $\beta_i \in \{0, 1, 2, \dots, n-1\}$ for $i \in I \subset \{0, 1, 2, \dots, n-1\}$. Then there is a polynomial $U(x) \in Z_n[x]$ such that $U(i) = \beta_i$ for all $i \in I$ iff $i \equiv j \mod p_s$ for some $s, 1 \leq s \leq k$, and $i, j \in I$, implies that $\beta_i \equiv \beta_j \mod p_s$.*

Proof. (of Theorem 3.9)
Sufficiency. Suppose, by the way of contradiction, that there exists a polynomial $U(x) \in Z_n[x]$ and there are $x, y \in J, x \neq y$, so that $U(x) = \pi(x)$ and $U(y) = \pi(y)$. As $x, y \in J$ the condition (A') implies that there exists i so that $x \equiv y \mod p_i$ and $\pi(x) \not\equiv \pi(y) \mod p_i$. However, in such a case Theorem 3.10 states that $\pi(x) \equiv \pi(y) \mod p_i$, a contradiction.
Necessity. Let $x, y \in J, x \neq y$. As J is a non-polynomial support of π there is no $U(x) \in Z_n[x]$ so that $U(x) = \pi(x)$ and $U(y) = \pi(y)$. Theorem 3.10 implies that there is an i so that $x \equiv y \mod p_i$ and $\pi(x) \not\equiv \pi(y) \mod p_i$. ∎

We strongly believe that the following is true:

Conjecture 3.11 *Let n be a square free number, $n = p_1 p_2 \dots p_k, k \geq 2$, where $p_1 < p_2 < \dots < p_k$, are primes. Let J be a non-polynomial support of a permutation π on $\{0, 1, 2, \dots, n-1\}$. Then $|J| \leq p_1 p_2 \dots p_{k-1}$.*

As a support for the conjecture we state:

Theorem 3.12 *Let n be a square free number, $n = p_1 p_2 \dots p_k$, where $p_1 < \dots < p_k, k \leq 4$, are primes, and let J be a non-polynomial support of a permutation π on $\{0, 1, \dots, n-1\}$. Then $|J| \leq p_1 p_2 \dots p_{k-1}$.*

Proof. We prove the theorem for $k = 2$ and $k = 3$ only. The proof for $k = 4$ uses the same ideas as in the case of $k = 3$ but it is very involved and distinguishes many cases, and therefore is omitted.
$k = 2$. By Lemma 3.3 we assume that $(0, 0) \in J$. Thus, by Theorem 3.9, for each $x \in J$, either $(x)_1 = 0$ or $(x)_2 = 0$, i.e. either $J \subseteq \{(0, a_2), 0 \leq a_2 \leq p_2 - 1\}$ or $J \subseteq \{(a_1, 0), 0 \leq a_1 \leq p_1 - 1\}$. In the latter case clearly $|J| \leq p_1$. In the former case $(\pi(x))_1 \neq (\pi(y))_1$ for all $x, y \in J, x \neq y$. As $0 \leq (\pi(x))_1 < p_1$ the proof follows.
$k = 3$. By Lemma 3.3 we may assume that $(0, 0, 0) \in J$, and, by Theorem 3.9 $(x)_i = 0$ for at least one coordinate. Set $A_1 = \{(0, a_2, a_3), 0 \leq a_2 \leq p_2 - 1, 0 \leq a_3 \leq p_3 - 1\}$, $A_2 = \{(a_1, 0, a_3), 0 \leq a_1 \leq p_1 - 1, 0 \leq a_3 \leq p_3 - 1\}$, and $A_3 = \{(a_1, a_2, 0), 0 \leq a_1 \leq p_1 - 1, 0 \leq a_2 \leq p_2 - 1\}$. We consider two cases.
I. There is an $i, 1 \leq i \leq 3$, so that $J \subset A_i$. For $J \subset A_3$ the proof is obvious as $|A_3| = p_1 p_2$. Suppose now that $J \subset A_1$. For $0 \leq a \leq p_1 - 1$, we define $J_a = \{x \in J, (\pi(x))_1 = a\}$. Clearly, $|J| = |J_0| + |J_1| + \dots + |J_{p_1 - 1}|$ as the

$J_i's$ are pairwise disjoint. Thus, it suffices to show that $|J_i| \le p_2$ for all $i = 0, 1, \ldots, p_1 - 1$.
Let $x = (0, x_2, x_3) \in J, y = (0, y_2, y_3) \in J$ be so that $x_2 \ne y_2$, and $x_3 \ne y_3$. Then, by Theorem 3.9, $(\pi(x))_1 \ne (\pi(y))_1$. Hence, if $(\pi(u))_1 = (\pi(v))_1$ for some $u = (0, u_2, u_3) \in J, v = (0, v_2, v_3) \in J$, then either $u_2 = v_2$ or $u_3 = v_3$, and consequently, for each $i = 0, 1, \ldots, p_1 - 1$, either $J_a \subset \{(0, c, a_3)$, where c is a fixed number, and $0 \le a_3 \le p_3 - 1\}$, or $J_a \subset \{(0, a_2, c)$, where c is a fixed number, and $0 \le a_2 \le p_2 - 1\}$. In the former case Theorem 3.9 implies $(\pi(x))_2 \ne (\pi(y))_2$ for all $x, y \in J_a, x \ne y$, which in turn implies $|J_a| \le p_2$. In the latter case $|J_a| \le p_2$ as the first and the third coordinates of all numbers in J_a are fixed.
For $J \subset A_2$ the proof is analogous.
II. $J \not\subseteq A_i$ for $i = 1, 2, 3$. Put $B_1 = \{(a_1, 0, 0), 1 \le a_1 \le p_1 - 1\}$, $B_2 = \{(0, a_2, 0), 1 \le a_2 \le p_2 - 1\}$, and $B_3 = \{(0, 0, a_3), 0 \le a_3 \le p_3 - 1\}$. Suppose first that $J \subset \cup_{i=1}^{3} B_i$. Then $J \cap B_i \ne \emptyset$ for $i = 1, 2, 3$.
Let $x = (x_1, 0, 0) \in J, (\pi(x))_2 = a$, let $y = (0, y_2, 0) \in J, (\pi(y))_1 = b$, and finally let $z = (0, 0, z_3) \in J, \pi(z) = (c, d, e)$, and $v = (0, 0, v_3) \in J, \pi(v) = (f, g, h)$. Then, by Theorem 3.9, it is $c \ne b \ne f$, $d \ne a \ne g$, and either $c \ne f$, or $d \ne g$. Therefore, $|J \cap B_3| \le (p_1 - 1)(p_2 - 1)$, and in aggregate, $|J| = |J \cap B_1| + |J \cap B_2| + |J \cap B_3| \le (p_1 - 1) + (p_2 - 1) + ((p_1 - 1)(p_2 - 1)) = p_1 p_2 - 1$.
Finally, assume that $J \subsetneq \bigcup_{i=1}^{3} B_i$. Suppose $x = (0, a, b) \in J, a \ne 0 \ne b$. (The cases $y = (a, 0, b) \in J$ and $z = (a, b, 0) \in J, a \ne 0 \ne b$ will be omitted as they can be treated in an analogous way). If there is $y = (c, 0, d) \in J, c \ne 0$, then Theorem 3.9 implies $b = d$, and $J \cap (A_1 \setminus (A_2 \cup A_3)) = \{(0, a_2, b), 1 \le a_2 \le p_2 - 1\}$ as well as $J \cap (A_2 \setminus (A_1 \cup A_3)) = \{(a_1, 0, b), 1 \le a_1 \le p_1 - 1\}$ and $J \cap A_3 = \varnothing$. Therefore, $J \subset \{(0, a_2, b), 1 \le a_2 \le p_2 - 1\} \cup \{(a_1, 0, b), 1 \le a_1 \le p_1 - 1\} \cup B_3$. The only difference between this case and the case $J \subset \bigcup_{i=1}^{3} B_i$ is that in the latter $b = 0$. As this fact has not been used in the proof, we are done with the last case as well. ■

We finish this paper with two remarks concerning a general natural number n. The first is concerned with the coincidence number of a Latin square $L(\pi)$ obtained by the construction described in this paper. We believe that the upper bound on $c(L(\pi))$ given in Corollary 3.8 is far from a tight one, that is, we believe that the construction provides a Latin square with much lower coincidence number than indicated by the corollary. As an evidence we turn the reader's attention to the Latin square L in Example 1.1. It is easy to see that $L = L(\pi)$ for $\pi = (0, 2, 5, 1, 4, 3)$. We have verified by an exhaustive computer search that $12 = c(L(\pi)) \le c(L(\pi'))$ for all permutations π' on the set $\{0, 1, ..., 5\}$. On the other hand, by Corollary 3.8, for any permutation π' we get as an upper bound only $c(L(\pi')) \le 24$. We believe that the reason is the following: If $f(x, y) \in \mathcal{F}(n)$ is a best polynomial approximation of $L(\pi)$ then $f(0, y) \in Z_n$ is by far not the best polynomial approximation of the

permutation π. By Theorem 3.12, for each permutation π on $\{0, 1, 2, 3, 4, 5\}$ there is a polynomial $U(x) \in Z_n[x]$ that coincides with π in at least 4 of 6 arguments. On the other hand, a best polynomial approximation of $L(\pi)$ coincides with π in only 2 positions.
The second one is rather technical. Our construction of a non-polynomial support in Theorem 3.7 is based on the mapping

$$(a_1, a_2, \dots, a_{k-1}, 0) \to (0, a_1, a_2, \dots, a_{k-1}).$$

It is not difficult to see that one may use another mapping

$$(a_1, a_2, \dots, a_{k-1}) \to (\sum_{i=1}^{k-1} a_i \mod p_1, a_1, a_2, \dots, a_{k-1}).$$

This is nothing but a very poor "linear code with a control sum". Unfortunately we are unable to make use of the fact.

References

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

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

[Čanda, Trung–2002] Čanda, V., Trung, T.V. 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. *Latin Squares and their Applications.* Akadémiai Kiadó, Budapest, 1974.

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

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

[Grošek, Wei–1999] Grošek, O., Wei, W. 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] Grošek, O., Nemoga, K., Satko, L. Ideal difference tables from an Algebraic 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.

[Godsil, McKay–1990] Godsil, C.D., McKay, B.D. Asymptotic enumeration of Latin squares. J. Combinatorial Theory B, 48(1990), pp. 19-44.

[Satko, Grošek, Nemoga–2003] Satko, L., Grošek, O., Nemoga, K. Extremal generalized S–boxes. Computing and Informatics No 1, 22(2003), pp. 85-99.

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