Computing and Informatics, Vol. 22, 2003, 85–99

EXTREMAL GENERALIZED S–BOXES[*]

Ladislav Satko, Otokar Grošek

Slovak University of Technology
Faculty of Electrical Engineering and Information Technology
812 19 Bratislava, Slovakia
e-mail: {grosek, satko}@kmat.elf.stuba.sk

Karol Nemoga

Institute of Mathematics
Slovak Academy of Sciences
814 73 Bratislava, Slovakia
e-mail: nemoga@mau.savba.sk

Manuscript received 3 July 2002; revised 30 January 2003
Communicated by Juraj Hromkovič

Abstract. It is well known that there does not exist a Boolean function $f : Z_2^m \to Z_2^n$ satisfying both basic cryptologic criteria, balancedness and perfect nonlinearity. In [9] it was shown that, if we use as a domain quasigroup G instead of the group Z_2^n, one can find functions which are at the same time balanced and perfectly nonlinear. Such functions have completely flat difference table. We continue in our previous work, but we turn our attention to the worst case when all lines of Cayley table of G define so called linear structure of f ([5]). We solve this problem in both directions: We describe all such bijections $f : G \to Z_2^n$, for a given quasigroup $|G| = 2^n$, and describe such quasigroups for a given function f.

Keywords: Quasigroups, linear structures, Boolean functions, perfect nonlinearity

[*] Work of authors supported by VEGA grant 1/7611/20 and by VEGA grant 5123/99.

1 INTRODUCTION

It is well known that basic building blocks used in product ciphers are relatively small S–boxes in connection with P-boxes. S–boxes are in fact Boolean functions $f : Z_2^m \to Z_2^n$ driven by relatively small keys. They provide confusion for the ciphering algorithm. P–boxes are not controlled by a key, and provide diffusion for the ciphering algorithm. As a rule they are permutations. Connection of these two blocks produces so called S–P blocks, i.e. permutations

$$f : Z_2^n \to Z_2^n,$$

where $Z_2^n = Z_2 \times Z_2 \times \ldots \times Z_2$, $Z_2 = \{0, 1\}$. Elements of Z_2^n are usually represented as binary numbers, and thus hereafter we use notation like $101 = [5]_b$. Clearly, there is a bijection J from the set $A = \{0, 1, 2, \ldots, 2^n - 1\}$ to Z_2^n defined as follows: $J(i) = [i]_b$ iff $i = i_{n-1}2^{n-1} + i_{n-2}2^{n-2} + \ldots + i_0 2^0 \in A$ and $[i]_b = (i_{n-1}, i_{n-2}, \ldots, i_0) \in Z_2^n$. The inverse mapping is $J^{-1} : Z_2^n \to A$, $J^{-1}([i]_b) = i$.

A design itself has in each iteration — called round — one layer consisting of an affine mappings $T : Z_2^n \to Z_2^n$, and one layer of S-boxes f. It is a generalization of substitution/permutation networks in which the affine mapping T is just a bit permutation. Affine layer provides diffusion and layer with S-boxes provides confusion according to classical Shannon's encryption paradigm. This view enables to make analysis of block diagram structure of a cipher (see [2]). Our generalization is not going into structural analysis, but into layer with S-boxes. We simply change a traditionally considered S-box, i.e. the Boolean function f, to a mapping $f : S \longrightarrow Z_2^n$ defined on a quasigroup S. This change yields that the difference table of S-box (one of the basic parameters) can be completely "flat" (perfectly nonlinear — see below) even in the case of identity mapping $f = id$. One possible design of this kind is visualized in Figure 1, where $k, x, y, x'y' \in S = (A, *)$.

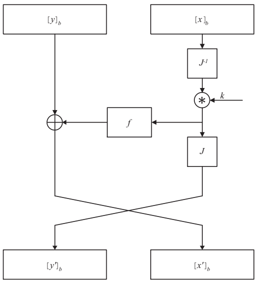


Fig. 1. One round of a Feistel-like cipher with a quasigroup

For reader's convenience we briefly recall some facts from algebra [3]:

groupoid Let S be a finite set. If there is a binary operation, "$*$", defined on S, then $(S, *)$ is called a finite groupoid. The full information on S is then given by so called Cayley table, i.e the table which shows how to multiply elements of S. Here is a small example for $S = \{e, b, c\}$:

$(S, *)$	e	b	c
e	e	b	c
b	b	c	b
c	c	e	b

left unit e of a groupoid S is an element satisfying $e * s = s$ for all $s \in S$. Groupoid from the previous example possesses such element. Similarly, one can define a *right unit.* An element i of a groupoid S is called *identity* if it is both left and right unit.

right simple groupoid A *right simple groupoid* S is a groupoid with the property that $x * S = S$ holds for all $x \in S$, i.e., each row of its Cayley table is a permutation of the elements of S. A *left simple groupoid* can be defined in a similar way, and each column of its Cayley table is a permutation of the elements of S. Clearly, groupoid from the example above is neither right nor left simple.

quasigroup A groupoid which is both right and left simple is called quasigroup. Clearly, its Cayley table should be a Latin square over the set S, i.e. a well known combinatorial structure containing permutations of elements of S in rows as well as in columns. Here is a small example for $S = \{a, b, c\}$:

$(S, *)$	a	b	c
a	b	a	c
b	c	b	a
c	a	c	b

A quasigroup may, or may not contain a left (right) unit. If there is no left unit we say that this is a *quasigroup without left units*, shortly QWLU.

group A groupoid which is both right and left simple, possessing a unit element i, and for any elements $a, b, c \in S$ the associative law is valid: $a * (b * c) = (a * b) * c$ is called a group.

The notion of *perfect nonlinearity* and *balancedness* [10] was defined for the case when $S = Z_2^n$. In [9] we extended this notions to the class of all quasigroups without left units.

Definition 1. Let $g : S \to Z_2$. Then g is balanced if

$$\sum_{x \in S} g(x) = \frac{|S|}{2}. \tag{1}$$

Obviously in this case there exists an integer ℓ such that $|S| = 2\ell$. If we denote $A_0 = \{i \in S \mid g(i) = 0\}$, and $A_1 = \{i \in S \mid g(i) = 1\}$, then $|A_0| = |A_1| = |S|/2$.

It is clear that the notion of balancedness is independent of the algebraic structure of S.

Let S be any nonempty set. Then to any subset $B \subset S$ we assign its characteristic function $f_B : S \to Z_2$. Conversely, any function $f : S \to Z_2$ can be considered as a characteristic function of the set $B = \{x \in S|\ f(x) = 1\}$. Hence, f_B is the membership function for B.

Hereafter Z_2^n is assumed together with the coordinate wise exclusive or operation $\oplus$, which is the group. Any S-P block is a permutation on this group. Changing the domain, say by A, one can study a similar situation on a quasigroup $G = (A, *)$, where for a fixed a, $g_a : A \to A, g_a(x) = a * x$ is a permutation. In fact permutation belonging to g_a is located in the row of Cayley table headed by a. The same is valid for columns as well. This yields that the Cayley table of G is a Latin square.

Definition 2. Let S be a quasigroup without left units. The characteristic function $f_A : S \to Z_2$ of a set $A \subset S$ is perfectly nonlinear (shortly PN) if for any $i \in S$, the function

$$D_i f_A :\ S \to Z_2,\ D_i f_A(x) = f_A(i * x) \oplus f_A(x) \tag{2}$$

is a balanced function.

In the same paper [9] we extended this definition to the case of vector functions $g : S \to Z_2^m$, $|S| \geq 2^m$.

Definition 3. Let S be a nonempty set, $|S| \geq 2^m$, and

$$g : S \to Z_2^m, \quad g = (g_1, g_2, \ldots, g_m).$$

Then g is balanced if for any $c = (c_1, c_2, \ldots, c_m) \in Z_2^m, \quad c \neq 0,\ c.g : S \to Z_2$, $c.g(x) = \bigoplus_{i=1}^m c_i g_i(x)$ is a balanced function. The dot product $c.g$ is assumed with $\oplus$ operation.

For example, let $S = \{0, 1, \ldots, 2^n - 1\}$ and π be any permutation on S. Then $J \circ \pi$ is balanced.

Definition 4. Let $(S, *)$ be a quasigroup without left units. A function $f : S \to Z_2^m$ is generalized perfectly nonlinear (shortly GPN) if for any $i \in S$, $D_i f : S \to Z_2^m$, $D_i f(x) = f(i * x) \oplus f(x)$ is a balanced function.

In [9] we define G such that $J : G \to Z_2^n, J(x) = [x]_b$ possesses ideal difference feature. By this we mean that for any $i \in G$ the function

$$(D_i J) : G \to Z_2^n, (D_i J)(x) = J(i * x) \oplus J(x) \tag{3}$$

is balanced, and J is (GPN). As a consequence, so called difference table possesses only one's. The difference table of J is a table with rows labeled by elements of G, and columns labeled by elements of Z_2^n. In the cell belonging to $i \in G$ and $[j]_b \in Z_2^n$ there is the number of $x \in G$ such that $(D_i J)(x) = J(i * x) \oplus J(x) = [j]_b$. The best one to be expected from the point of view of immunity to so called differential cryptanalysis is a table with all entries 1's only. A small example for $n = 4$ follows.

Example 1. Our construction consists from the following steps:

- Select a transversal[1] of the group Z_2^2. (Marked below in Cayley table for Z_2^2 by boxes.)
- The selected transversal defines a permutation α on Z_2^2.
- Then β defined by
$$\beta([x]_b) = \alpha([x]_b) \oplus ([x]_b)$$
is a permutation on Z_2^2.
- The couple (α, β) yields one row of Cayley table of S, say for i. The operation $*$ on $S = \{0, 1, 2, 3\}$ is defined as follows:
$$i * x = J^{-1}(\alpha([x]_b)).$$
- Then clearly
$$(D_i J)(x) = J(i * x) \oplus J(x) = \alpha([x]_b) \oplus [x]_b = \beta([x]_b).$$
It is readily seen that $(D_i J)(x)$ is a permutation, and thus a balanced function. The i-th row of difference table described above possesses only 1's:

$S\backslash Z_2^2$	00	01	10	11
0				
$\vdots$				
i	1	1	1	1
3				

The result is visualized in the following Cayley tables:

$[x]_b$	00	01	10	11
α	00	10	11	01
β	00	11	01	10

Z_2^2	00	01	10	11
155 00	$\boxed{00}$	01	10	11
01	01	00	$\boxed{11}$	10
10	10	11	00	$\boxed{01}$
11	11	$\boxed{10}$	01	00

→

S	0	1	2	3
0				
$\vdots$				
i	0	2	3	1
3				

[1] A transversal of a Latin square of order N is a set of N cells, one in each row, one in each column, and such that no two of the cells contain the same symbol.

- The next transversal $\alpha'([x]_b)$ is obtained by adding a constant term, i.e. $\alpha'([x]_b) = \alpha([x]_b) \oplus [a]_b$. For, e.g. $[a]_b = 11$ we have $11, 01, 00, 10$. This yields another row of the Cayley table, namely: $3, 1, 0, 2$.
- The quasigroup is then as follows:

S	0	1	2	3
0	0	2	3	1
1	3	1	0	2
2	1	3	2	0
3	2	0	1	3

This represents a "positive extreme". The main toolkit for finding such Cayley tables was the existence of so called *transversals* in Latin squares.

Our main results in [9] are

Theorem 1. For any $n > 1$ there exists a quasigroup S without left units, $|S| = 2^n$, and a generalized perfectly nonlinear bijection $f : S \to Z_2^n$.

More quasigroups and functions of our interest can be obtained by the following costruction.

Corollary 1. Let S be a QWLU, $|S| = 2^n$, and $f : S \to Z_2^n$, f arbitrary generalized perfectly nonlinear bijection. Let ρ be a right regular permutation[2] of S, and $g : Z_2^n \to Z_2^n$ be a linear bijection. Then $F = g \circ f \circ \rho$ is a generalized perfectly nonlinear bijection.

Next we turn to a "negative extreme". It is well known that the existence of so called linear structures for Boolean function $f : Z_2^m \to Z_2^n$ is a weakness both for block and stream ciphers [6, 11, 5]. Thus it is of particular importance to avoid such cases. In this paper we continue in our previous work when we generalize the domain of f providing the best possible quality of S-boxes not accessible for Boolean functions.

In Section 2 we generalize the notion of a linear structure from [5], and in Section 3 we describe all such bijective functions. Special attention is devoted to quasigroups without left units playing the crucial role in the "positive case". While in previous section we discuss constructions of a quasigroup G to the given function f, in Section 4 we solve the converse, i.e. to given quasigroup G find functions which posses at least one linear structure.

[2] Let $(S, *)$ be a QWLU, and $\rho : S \to S$ be a permutation of elements of S such that for any $x, y \in S$, $\rho(x * y) = x * \rho(y)$. Then ρ is called a *right regular permutation* [1].

2 LINEAR STRUCTURES

Let us assume again the function $J : A \to Z_2^n$, $J(x) = [x]_b$ where $A = \{0, 1, \ldots, 2^n - 1\}$. Our aim is to define an operation $*$ on A such that

1. $G = (A, *)$ would be a quasigroup
2. there exists at least one $i \in G$, such that D_iJ from (3) is the constant function, i.e. there exists $[a]_b \in Z_2^n$ such that $(D_iJ)(x) = [a]_b$ for all $x \in G$.

If this is the case then the difference table for J, namely in the row labeled by $i \in G$, possesses zeroes only except of one entry 2^n.

In details, from (3) we have

$$\begin{array}{ccccc} J(i * x) \oplus J(x) & = & [i * x]_b \oplus [x]_b & = & [a]_b \\ \text{or} & & [i * x]_b & = & [a]_b \oplus [x]_b \\ \text{which yields} & & i * x & = & J^{-1}([a]_b \oplus [x]_b) \end{array}$$

$$\begin{tikzcd} G \arrow[r, "J"] \arrow[dr, "f"'] & Z_2^n \arrow[d, "\pi"] \\ & Z_2^n \end{tikzcd}$$

Fig. 2. Diagram for $f = \pi \circ J : G \to Z_2^n$

In other words, if we compare Cayley tables for G and Z_2^n, the row labeled by $i \in G$ in Cayley table for quasigroup G is the same as "decoded from binary" row labeled by $[a]_b \in Z_2^n$.

Recall that element $i \in G$ has the property that there exists $[a]_b \in Z_2^n$ such that $J(i * x) \oplus J(x) = [a]_b$. Following [11, 5] we call such element i *linear structure* of J. More precisely:

Definition 5. Let $G = (A, *)$ be a quasigroup, and $f : G \to Z_2^n$ be a function. An element $i \in G$ is called linear structure of f if there exists $[a]_b \in Z_2^n$ such that $f(i * x) \oplus f(x) = [a]_b$ for all $x \in G$.

First of all we emphasize a very close relation between linear structures and homomorphisms of quasigroups. Let $h : G \to Z_2^n$ be an arbitrary homomorphism. Then

$$h(i * x) = h(i) \oplus h(x)$$

yields

$$h(i * x) \oplus h(x) = (h(i) \oplus h(x)) \oplus h(x) = h(i) = [a]_b.$$

Thus, any $i \in G$ is the linear structure of a homomorphism h.

3 LINEAR BIJECTIVE STRUCTURES

Next we describe linear structures of a bijection f in the case $|G| = 2^n$. Clearly, any bijection f is a composition of our function J, and a permutation $\pi : Z_2^n \to Z_2^n$ (see Fig. 2):

$$f = \pi \circ J : G \to Z_2^n,$$

$$f(x) = (\pi \circ J)(x) = \pi(J(x)) = \pi([x]_b). \tag{4}$$

Let us suppose that there exists a linear structure $i \in G$ of f. Thus there exists $[a]_b \in Z_2^n$ such that for any $x \in G$

$$f(i * x) \oplus f(x) = [a]_b.$$

Using (4)

$$f(i * x) = [a]_b \oplus f(x) = [a]_b \oplus \pi([x]_b). \tag{5}$$

Since

$$\alpha_a : Z_2^n \to Z_2^n,\ \alpha_a([y]_b) = [a]_b \oplus [y]_b$$

is a permutation on Z_2^n we can write in (5)

$$f(i * x) = \alpha_a(\pi([x]_b)) = \alpha_a(f(x)),$$

or equivalently

$$i * x = (f^{-1} \circ \alpha_a \circ f)(x). \tag{6}$$

Hence relation (6) defines the row of Cayley table of G belonging to $i \in G$. Further, it is not difficult to prove that for $[a]_b \neq [u]_b$, the following two permutations g, h on G are different:

$$g = f^{-1} \circ \alpha_a \circ f \text{ and } h = f^{-1} \circ \alpha_u \circ f.$$

To define $\alpha_a \circ f : A \to Z_2^n$ one must assume the group structure of Z_2^n.

We summarize:

1. Let $f : A \to Z_2^n$ be a bijection, and $i \in A$ is fixed. Then on A there exists operation $*$ such that $G = (A, *)$ is a quasigroup, and i is a linear structure of $f : G \to Z_2^n$. This can be accomplished by choosing a fixed $[a]_b \in Z_2^n$, and the row of Cayley table of Z_2^n belonging to this element (see (6)). Other rows can be chosen arbitrarily to fill in a Latin square.
2. Let $f : A \to Z_2^n$ be a bijection. Then there exists operation $*$ such that $G = (A, *)$ is a quasigroup, and any i is a linear structure of $f : G \to Z_2^n$. This can be accomplished by choosing to each particular i a fixed $[a]_b \in Z_2^n$, and the row of Cayley table of Z_2^n belonging to this element $[a]_b$. Hence we use, step by step, all rows of Cayley table of Z_2^n.

We state this fact exactly as

Lemma 1. Let $f : A \to Z_2^n$ be a bijection. Then there exists $(2^n)!$ different ways to define an operation $*$ on A such that $G = (A, *)$ is a quasigroup, and each $i \in G$ is a linear structure of $f : G \to Z_2^n$.

Example 2. Let $n = 3$. Then Cayley table for Z_2^3 is as follows:

Z_2^3	$[0]_b$	$[1]_b$	$[2]_b$	$[3]_b$	$[4]_b$	$[5]_b$	$[6]_b$	$[7]_b$
$[0]_b$	$[0]_b$	$[1]_b$	$[2]_b$	$[3]_b$	$[4]_b$	$[5]_b$	$[6]_b$	$[7]_b$
$[1]_b$	$[1]_b$	$[0]_b$	$[3]_b$	$[2]_b$	$[5]_b$	$[4]_b$	$[7]_b$	$[6]_b$
$[2]_b$	$[2]_b$	$[3]_b$	$[0]_b$	$[1]_b$	$[6]_b$	$[7]_b$	$[4]_b$	$[5]_b$
$[3]_b$	$[3]_b$	$[2]_b$	$[1]_b$	$[0]_b$	$[7]_b$	$[6]_b$	$[5]_b$	$[4]_b$
$[4]_b$	$[4]_b$	$[5]_b$	$[6]_b$	$[7]_b$	$[0]_b$	$[1]_b$	$[2]_b$	$[3]_b$
$[5]_b$	$[5]_b$	$[4]_b$	$[7]_b$	$[6]_b$	$[1]_b$	$[0]_b$	$[3]_b$	$[2]_b$
$[6]_b$	$[6]_b$	$[7]_b$	$[4]_b$	$[5]_b$	$[2]_b$	$[3]_b$	$[0]_b$	$[1]_b$
$[7]_b$	$[7]_b$	$[6]_b$	$[5]_b$	$[4]_b$	$[3]_b$	$[2]_b$	$[1]_b$	$[0]_b$

This means that e.g. $[5]_b \oplus [3]_b = 101 \oplus 011 = 110 = [6]_b$. Let the mapping $f : A \to Z_2^n$ be given by the table

x	0	1	2	3	4	5	6	7
$f(x)$	$[1]_b$	$[2]_b$	$[4]_b$	$[7]_b$	$[6]_b$	$[3]_b$	$[5]_b$	$[0]_b$

One can write $f = \pi \circ J$ as a composition of $J(x) = [x]_b$, and the permutation $\pi : Z_2^3 \to Z_2^3$:

$[x]_b$	$[0]_b$	$[1]_b$	$[2]_b$	$[3]_b$	$[4]_b$	$[5]_b$	$[6]_b$	$[7]_b$
$\pi([x]_b)$	$[1]_b$	$[2]_b$	$[4]_b$	$[7]_b$	$[6]_b$	$[3]_b$	$[5]_b$	$[0]_b$

Then $(\alpha_a \circ f)(x) = [a]_b \oplus f(x)$. Tables for all such mappings are easy to get if we change the heading line of the Cayley table for Z_2^n by permutation π, and change columns with respect of this permutation. Rows represent values for fixed $[a]_b$.

$[a]_b \diagdown f(x)$	$[1]_b$	$[2]_b$	$[4]_b$	$[7]_b$	$[6]_b$	$[3]_b$	$[5]_b$	$[0]_b$
$[0]_b$	$[1]_b$	$[2]_b$	$[4]_b$	$[7]_b$	$[6]_b$	$[3]_b$	$[5]_b$	$[0]_b$
$[1]_b$	$[0]_b$	$[3]_b$	$[5]_b$	$[6]_b$	$[7]_b$	$[2]_b$	$[4]_b$	$[1]_b$
$[2]_b$	$[3]_b$	$[0]_b$	$[6]_b$	$[5]_b$	$[4]_b$	$[1]_b$	$[7]_b$	$[2]_b$
$[3]_b$	$[2]_b$	$[1]_b$	$[7]_b$	$[4]_b$	$[5]_b$	$[0]_b$	$[6]_b$	$[3]_b$
$[4]_b$	$[5]_b$	$[6]_b$	$[0]_b$	$[3]_b$	$[2]_b$	$[7]_b$	$[1]_b$	$[4]_b$
$[5]_b$	$[4]_b$	$[7]_b$	$[1]_b$	$[2]_b$	$[3]_b$	$[6]_b$	$[0]_b$	$[5]_b$
$[6]_b$	$[7]_b$	$[4]_b$	$[2]_b$	$[1]_b$	$[0]_b$	$[5]_b$	$[3]_b$	$[6]_b$
$[7]_b$	$[6]_b$	$[5]_b$	$[3]_b$	$[0]_b$	$[1]_b$	$[4]_b$	$[2]_b$	$[7]_b$

Finally, applying f^{-1} to all rows we get all functions $f^{-1} \circ \alpha_a \circ f : A \to A$.

$(A,*)$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	7	5	6	4	3	1	2	0
2	5	7	4	6	2	0	3	1
3	1	0	3	2	6	7	4	5
4	6	4	7	5	1	3	0	2
5	2	3	0	1	5	4	7	6
6	3	2	1	0	7	6	5	4
7	4	6	5	7	0	2	1	3

By this construction we have one quasigroup $G = (A,*)$ where each line, say i, is a linear structure of the bijection f, and

$$f(i*x) \oplus f(x) = [i]_b.$$

To change the constant value $[i]_b$ in the row it is sufficient to interchange rows, say by permutation $\sigma : A \to A$, in this Cayley table. Then for each $i, x \in G$

$$f(i*x) \oplus f(x) = [\sigma^{-1}(i)]_b.$$

3.1 Linear Structures and QWLU

It was shown in the papers [8, 9] that quasigroups without left units are of particular interest for cryptography. Next we study relations between the existence of a linear structure and left units.

For $\alpha_0 : Z_2^n \to Z_2^n, \alpha_0([x]_b) = [0]_b \oplus [x]_b = [x]_b$, and for arbitrary $f : G \to Z_2^n$ we have

$$\alpha_0 \circ f : G \to Z_2^n, \alpha_0(f(x)) = [0]_b \oplus f(x) = f(x).$$

Hence $\alpha_0 \circ f = f$, and for the corresponding row for $i*x$ of Cayley table of G we have

$$i*x = (f^{-1} \circ \alpha_0 \circ f)(x) = x \tag{7}$$

which yields $i \in G$ is a left unit.

Lemma 2. Let $f : A \to Z_2^n$ be a bijection. Then there is no operation $*$ such that $G = (A,*)$ would be a QWLU, and at the same time each $i \in G$ would be a linear structure of $f : G \to Z_2^n$.

One can read equation (7) as follows: in Cayley table of such a special G there exists a row (generated by $[0]_b$) which “coincide” with the first row of Cayley table of Z_2^n. Now the question arise: Under which circumstances we will have other rows which coincide with rows of Z_2^n? This problem may be rephrased by decomposition of f.

Recall that according (4) any bijection $f : G \to Z_2^n$ can be expressed in the form $f = \pi \circ J$. If $i \in G$ is a linear structure of f then due to (6) there exists a permutation α_a such that $i * x = (f^{-1} \circ \alpha_a \circ f)(x)$ for all $x \in G$. Combining these two expressions we have

$$i * x = \Big(f^{-1} \circ \alpha_a \circ f\Big)(x) = \Big(J^{-1} \circ \pi^{-1} \circ \alpha_a \circ \pi \circ J\Big)(x). \tag{8}$$

Clearly, if

$$\alpha_a \circ \pi = \pi \circ \alpha_a \tag{9}$$

then

$$i * x = \Big(J^{-1} \circ \alpha_a \circ J\Big)(x) = J^{-1}(\alpha_a([x]_b)) = J^{-1}([a]_b \oplus [x]_b). \tag{10}$$

We just proved that the row labeled by $i \in G$ coincide in this case with the row labeled by $[a]_b \in Z_2^n$.

To finish our task we identify all permutations $\pi : Z_2^n \to Z_2^n$ for which (9) is valid. In fact this requires for any $[x]_b \in Z_2^n$

$$[a]_b \oplus \pi([x]_b) = (\alpha_a \circ \pi)([x]_b) = (\pi \circ \alpha_a)([x]_b) = \pi([a]_b \oplus [x]_b).$$

Such permutation on a group is right regular. On the other hand, let $\pi : Z_2^n \to Z_2^n$ be a right regular permutation. Then $(\alpha_a \circ \pi)([x]_b) = (\pi \circ \alpha_a)([x]_b)$ for any $[a]_b \in Z_2^n$, and (10) is valid. We summarize

Lemma 3. *Let $f = \pi \circ J : A \to Z_2^n$ be a bijection. Let $G = (A, *)$ be a quasigroup such that all $i \in G$ are linear structures of $f : G \to Z_2^n$. Then each row of Cayley table of G can be obtained from appropriate row of Cayley table of Z_2^n iff $\pi : Z_2^n \to Z_2^n$ is a right regular permutation.*

Remark 1. Let $H = (A, \odot)$ be a quasigroup, and let $\pi : H \to H$ be a right regular permutation. If H possesses a right unit, say e, then $\pi(x) = \pi(x \odot e) = x \odot \pi(e)$ for any $x \in H$. Then all values of π are uniquely determined by $\pi(e)$.

4 CONSTRUCTION OF BIJECTIONS HAVING NO LINEAR STRUCTURES

Finally we solve the following problem: under which circumstances for a given quasigroup $G = (A, *)$ there exists a bijection with a linear structure.

We start with Example.

Example 3. We continue in Example 2. Let $\sigma : A \to A$ be as follows:

i	0	1	2	3	4	5	6	7
$\sigma(i)$	2	7	0	1	5	3	6	4

Then we can define a quasigroup G, where[3]

$$f(i * x) \oplus f(x) = [\sigma^{-1}(i)]_b$$

[3] For definition of f see Example 2.

for any $i, x \in G$. Its Cayley table is as follows

$(A,*)$	0	1	2	3	4	5	6	7
0	5	7	4	6	2	0	3	1
1	1	0	3	2	6	7	4	5
2	0	1	2	3	4	5	6	7
3	2	3	0	1	5	4	7	6
4	4	6	5	7	0	2	1	3
5	6	4	7	5	1	3	0	2
6	3	2	1	0	7	6	5	4
7	7	5	6	4	3	1	2	0

and one can verify that

$f(x)$	$[1]_b$	$[2]_b$	$[4]_b$	$[7]_b$	$[6]_b$	$[3]_b$	$[5]_b$	$[0]_b$
$f(4*x)$	$[6]_b$	$[5]_b$	$[3]_b$	$[0]_b$	$[1]_b$	$[4]_b$	$[2]_b$	$[7]_b$
$f(4*x)\oplus f(x)$	$[7]_b$	$[7]_b$	$[7]_b$	$[7]_b$	$[7]_b$	$[7]_b$	$[7]_b$	$[7]_b$

and

$$f(4*x)\oplus f(x) = [\sigma^{-1}(4)]_b = [7]_b.$$

Moreover, $f(4*(4*x))\oplus f(4*x) = [7]_b$, or $f(4*(4*x)) = f(4*x)\oplus [7]_b = f(x)$ in this case. Since f is a bijection $4*(4*x) = x$ is valid as well. Thus the row labeled by 4 in Cayley table is an involution.

Obviously, there is nothing special on the choice $i = 4$, and we have

Lemma 4. A necessary condition for $i \in G$ to be a linear structure of a bijection $f : G \to Z_2^n$ is that

$$\sigma_i : G \to G,\ \sigma_i(x) = i * x \tag{11}$$

is an involution (without fixed elements), or identity.

Now we turn our attention to sufficient conditions. Below we show one possible construction of f. Clearly, when σ_i from (11) is identity mapping, then $i*x = x$ and since $f(i*x)\oplus f(x) = [0]_b$ we conclude i is a linear structure of arbitrary bijection $f : G \to Z_2^n$.

Let σ_i be an involution without fixed elements. Then for any $k \in G$ we have: if $i*k = \ell$ then $i*\ell = k$ and $k \neq \ell$. Let us call it (k,ℓ)-cycle. All together we have 2^{n-1} such cycles for $k < \ell$. Since i is a linear structure, there is an $[a]_b \in Z_2^n$ such that $f(\ell)\oplus f(k) = [a]_b$. This yields a definition of f for each cycle (k,ℓ) as follows:

1. Let

   $$G_K = \{k \in G \mid \text{there exists } (k,\ell)-\text{cycle},\ k < \ell\}$$

   and

   $$G_L = \{\ell \in G \mid \text{there exists } (k,\ell)-\text{cycle},\ k < \ell\}.$$

   Obviously, $G_K \cup G_L = G, G_K \cap G_L = \emptyset$.

2. The necessary condition for $f : G \to Z_2^n$ is
$$f(\ell) = [a]_b \oplus f(k)$$
for any $\ell \in G_L$ and $k \in G_K$.
3. Hence, arranging all cycles $(k_j, \ell_j) \in G_K \times G_L, j = 0, 1, \ldots, 2^{n-1} - 1$ we conclude that the bijection must establish a partition $K \cup L$ of the group Z_2^n, where
$$K = f(G_K) = \{f(k_j) : j = 0, 1, \ldots, 2^{n-1} - 1\}$$
$$L = f(G_L) = [a]_b \oplus f(G_K) = \{[a]_b \oplus f(k_j) : j = 0, 1, \ldots, 2^{n-1} - 1\}.$$

One of possible solutions is to take a subgroup K of the order 2^{n-1} and its coset $L = [a]_b \oplus K, [a]_b \notin K$. The definition of bijection f follows: assume a subgroup $K \subset Z_2^n$ of the order 2^{n-1}, and arbitrary bijection

$$f : \{k_j : k_j \in G, j = 0, 1, \ldots, 2^{n-1} - 1\} \to K, \tag{12}$$

and extend it due to cycles (k_j, ℓ_j) by $f(\ell_j) = [a]_b \oplus f(k_j)$.

Recall that there exist exactly n subgroups of the order 2^{n-1} (each consisting of one coordinate fixed). Therefore, one can find $(2^{n-1})!$ mappings of the type (12). This yields $n \times (2^{n-1})!$ different bijections. Other constructions using subgroups of the lower order are possible too. We summarize:

Theorem 2. *Let G be a quasigroup, $|G| = 2^n$, and $\sigma_i : G \to G$, $\sigma_i(x) = i * x$ be an involution without fixed elements. Then there exists a bijection $f : G \to Z_2^n$ such that $i \in G$ is a linear structure of f.*

The last Theorem describes completely the quasigroups possessing linear structures. In fact, our main aim is to find quasigroups having no linear structures. Thus, the main relevance of this Theorem is to avoid involution without fixed elements from rows of used Cayley tables.

5 CONCLUSIONS

In this paper we have presented a construction of all bijections $f : G \to Z_2^n$ such that $i \in G$ is a linear structure of f for a given quasigroup $|G| = 2^n$. Moreover, quasigroups formed by linear structures only, for a given function f are described too. These elements are a nightmare for designers of block and stream ciphers since they allow various attacks on round functions or scrambled counters. The case $G = Z_2^n$ was treated in [5]. In particular, it was proven that they form a linear subspace of Z_2^n. Contrary to this case, for arbitrary quasigroup, they do not form any algebraic structure.

REFERENCES

[1] Belousov, V D.: Foundations of the Theory of Quasigroups and Loops. Nauka, Moscow, 1967.

[2] Biryukov, A.—Shamir, A.: Structural Analysis of SASAS. In: Eurocrypt 2001, Lecture Notes in Computer Science, Vol. 2045, Springer–Verlag, Berlin, 2001, pp. 408–416.

[3] Clifford, A. H.—Preston, G. B: The Algebraic Theory of Semigroups I. Amer. Math. Soc., Providence, R. I., 1961.

[4] Dénes, J.—Keedwell, A. D.: Latin Squares and Their Applications. Akadémiai Kiadó, 1974, Budapest.

[5] Dubuc, S.: Chracterization of Linear Structures. Design, Codes and Cryptography 22, 2001, pp. 33–45.

[6] Evertse, J. H.: Linear Structures in Block Ciphers. Advances in Cryptology — Eurocrypt '87. Lecture Notes in Computer Science, Vol. 304, 1988, Springer-Verlag, Berlin, pp. 249–266.

[7] Grošek, O.—Wei, W.: Bent–Like Functions on Groupoids. Pure Mathematics and Applications. Vol. 10, 1999, No. 3, Budapest & Siena Publisher, pp. 267–278.

[8] Grošek, O.—Satko, L.—Nemoga, K.: Generalized S–Boxes Serving Zero Mutual Information. Abstracts from the 14th Czech and Slovak International Conference on Number Theory. Liptovský Ján, September 6–10, 1999.

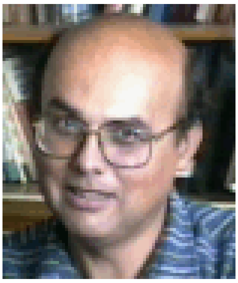
[9] Grošek, O.—Satko, L.—Nemoga, K.: Ideal Difference Tables from an Algebraic Point of View. Proceedings of VI RECSI, Tenerife, Spain, September 2000, P. Caballero-Gil and C. Hernández-Goya Eds., pp. 43–53.

[10] Nyberg, K.: Perfect Nonlinear S–Boxes. Advances in Cryptology — Proceedings of Eurocrypt '90. Lecture Notes in Computer Science, Vol. 473, 1990, Springer-Verlag, Berlin, pp. 378–386.

[11] Xueja, L.: Additive and Linear Structures of Cryptographic Functions. Proceedings of Fast Software Encryption '95. Lecture Notes in Computer Science, Vol. 1008, 1995, Springer-Verlag, Berlin, pp. 75–85.

Ladislav Satko graduated at the Comenius University (1962), assigned to Professor Š. Schwarz as a graduate student (PhD. — 1978), (Doc. — 1984). Since 1990 he is the head of Department of Mathematics, FEI STU in Bratislava. Since 1983 he is working in cryptology. Member of Society for Industrial and Appl. Mathematics., Slovak Mathematical Soc.

Otokar Grošek graduated at the Comenius University (1973), assigned to Professor Š. Schwarz as a graduate student (PhD. — 1978), (Prof. — 1998). He is working at the Department of Mathematics, FEI STU in Bratislava. Since 1983 he is working in cryptology. Member of American Mathematical Soc., Society for Industrial and Appl. Mathematics., Slovak Mathematical Soc., Editor of the Tatra Mountains Mathematical Publication.



Karol Nemoga graduated at the Charles University (1976), assigned to Professor Š. Schwarz as a graduate student (PhD. — 1988). He is with the Institute of Mathematics of the Slovak Academy of Sciences in Bratislava. His main field of interest is cryptology. Managing editor of the Tatra Mountains Mathematical Publication, Member of Slovak Mathematical Soc.