Tatra Mt. Math. Publ. **20** (2000), 127–137

Tatra Mountains
Mathematical Publications

GENERALIZED PERFECTLY NONLINEAR FUNCTIONS

Otokar Grošek — Karol Nemoga — Ladislav Satko

ABSTRACT. It is well known that it is not possible to find a Boolean function $\boldsymbol{f}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ satisfying basic cryptologie criteria — balancedness and perfect nonlinearity — at the same time. The best approximation to this target was done by Nyberg in [K. Nyberg: *Perfect nonlinear S-boxes. Advances in Cryptology–Proceedings of Eurocrypt '90*, in: Lecture Notes in Comput. Sci., Vol. 473, Springer-Verlag, Berlin, pp. 378–386, 1990]. In her construction she used slightly unbalanced functions, namely bent functions, providing $n = 2k$, $n \geq 2m$. Such functions satisfy also a condition of the minimal mutual input/output information.

In our contribution we show that a change of the domain (the group) Z_2^n by a quasigroup, say S, enables to construct balanced as well as (generalized) perfectly nonlinear functions. Such functions have completely flat difference table.

1. Introduction

Let $(S,*)$ be an arbitrary groupoid, $A \subset S$, f_A be the characteristic function of the subset A, and $\oplus$ the XOR operation on $\mathbb{Z}_2 = \{0,1\}$.

For any $A \subset S$ and $i \in S$ we define

$$R_A\colon S \to \{0,1,2,\dots,|S|\}, \qquad R_A(i) = \sum_{x\in S} f_A(i*x) \oplus f_A(x), \tag{1}$$

$$\lambda_A\colon S \to \{0,1,2,\dots,|A|\}, \qquad \lambda_A(i) = |i*A \cap A|. \tag{2}$$

Thus $R_A(i)$ is a function counting the changes of the membership or non-membership status of x in A when x is multiplied by i.

Now we state some basic properties of $R_A(i)$ which can be found in [GW]:

2000 Mathematics Subject Classification: 94A60, 11T71, 68P25.
Keywords: difference properties, perfect nonlinearity.

Supported by Grant VEGA 5123/99, 1/7611/20.

Lemma 1. *Let $(S,*)$ be a right simple groupoid, $A \subset S$, $A^c = S\backslash A$, and $i \in S$. Then*

(a) $R_A(i) = |i * A^c \cap A| + |i * A \cap A^c|$,

(b) $R_A(i) = R_{A^c}(i)$,

(c) $R_A(i) = 2\big(|A| - \lambda_A(i)\big)$,

(d) $R_A(i) = 0$ *for any* $A \subset S$, *if and only if* i *is a left unit of* S.

To prove the first assertion of this lemma it was necessary to use the structure of a right simple groupoid. This is conform with results known in the theory of S-boxes. From (d) it follows that the case when all elements of a groupoid are left units is not interesting. Therefore, in what follows we consider only a right simple groupoid containing at least one element different from a left unit.

The following is easy to prove:

(1) If $|A| = 1$ or $|A| = |S| - 1$ then $R_A(i) = 0$ or $R_A(i) = 2$.

(2) If $A = S$ or $A = \emptyset$ then $R_A(i) = 0$ for any $i \in S$.

Functions R_A and λ_A have a close relation to so called balancedness and perfect nonlinearity. An extension of these notions for a right simple groupoid is given in Section 2.

It is well known that there does not exist a Boolean function $\boldsymbol{f}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ satisfying both basic cryptologic criteria, balancedness and perfect nonlinearity. For n even, $n \geq 2m$, a construction which so far got closest to the target is due to Nyberg [Ny]. In her construction she used perfectly nonlinear functions, so called bent functions. In Section 3 we generalize this notion for a right simple groupoid.

In the last Section we show that if we use as a domain a quasigroup instead of the group $\mathbb{Z}_2^n$ we can find functions which are at the same time balanced and perfectly nonlinear. Such functions have the completely flat difference table.

2. Two generalizations

The notion of *perfect nonlinearity* and *balancedness* [Ny] have been defined so far only for the case when $S = \mathbb{Z}_2^n$. In this section we extend the notions to the class of all right simple groupoids.

Definition 1. Let S be a right simple groupoid. The characteristic function $f_A\colon S \to \mathbb{Z}_2$ of a set $A \subset S$ is said to be *perfectly nonlinear* (PN) if for any i different from a left unit

$$R_A(i) = \frac{|S|}{2}. \tag{3}$$

Thus the decision whether a characteristic function is PN depends exclusively on the multiplication $*$ on S.

Now we are going to deal with the notion of balancedness. This notion extends in a very natural way to a component functions:

Definition 2. Let $g\colon S \to \mathbb{Z}_2$. Then g is *balanced* if

$$\sum_{x \in S} g(x) = \frac{|S|}{2}. \tag{4}$$

Obviously in this case there exists an integer ℓ such that $|S| = 2\ell$. If we denote $A_0 = \{i \in S\colon g(i) = 0\}$, and $A_1 = \{i \in S\colon g(i) = 1\}$, then $|A_0| = |A_1| = |S|/2$. It is clear that the notion of balancedness is independent of the algebraic structure of S.

According to Definitions 1 and 2 we have:

Proposition 1. *Let S be a right simple groupoid. The characteristic function $f_A\colon S \to \mathbb{Z}_2$ of a set $A \subset S$ is PN iff for any $i \in S$, i different from a left unit, the function*

$$D_i f\colon\ S \to \mathbb{Z}_2, \qquad D_i f(x) = f(i * x) \oplus f(x), \tag{5}$$

is a balanced function.

Following [Ny] we extend this definition to the case of vector functions $\mathbf{g}\colon S \to \mathbb{Z}_2^m$, $|S| \ge 2^m$.

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

$$\mathbf{g}\colon S \to \mathbb{Z}_2^m, \qquad \mathbf{g} = (g_1, g_2, \dots, g_m).$$

Then $\mathbf{g}$ is *balanced* if for any $\mathbf{c} = (c_1, c_2, \dots, c_m) \in \mathbb{Z}_2^m$, $\mathbf{c} \neq \mathbf{0}$, $\mathbf{c} \cdot \mathbf{g}\colon S \to \mathbb{Z}_2$ is a balanced function. The dot product $\mathbf{c} \cdot \mathbf{g}$ is assumed with $\oplus$ operation.

Let S be any nonempty set, and $\mathbf{g}\colon S \to \mathbb{Z}_2^m$. Let $A_k = \{i\colon \mathbf{g}(i) = \mathbf{k}\}$ where k is the decimal expansion of the binary vector (number) $\mathbf{k}$.

Theorem 1. *A function $\mathbf{g}\colon S \to \mathbb{Z}_2^m$ is balanced iff $|S| = 2^m \ell$ and for any $\mathbf{k} \in \mathbb{Z}_2^m$, $|A_k| = |S|/2^m$.*

Proof. From Definition 3, a function $\mathbf{g}$ is balanced iff for any $\mathbf{c} = (c_1, c_2, \dots, c_m) \in \mathbb{Z}_2^m$, $\mathbf{c} \neq \mathbf{0}$, it is

$$\sigma = \sum_{i \in S} (-1)^{\mathbf{c} \cdot \mathbf{g}(i)} = 0.$$

However,

$$\sigma = \sum_{k=0}^{2^m-1} \sum_{i\,:\ \mathbf{g}(i)=\mathbf{k}} (-1)^{\mathbf{c}\cdot\mathbf{g}(i)} = \sum_{k=0}^{2^m-1} |A_k|(-1)^{\mathbf{c}\cdot\mathbf{k}} . \tag{6}$$

If $|A_k| = \ell$ for any k, then

$$\sigma = \sum_{k=0}^{2^m-1} |A_k|(-1)^{\mathbf{c}\cdot\mathbf{k}} = 0 \tag{7}$$

for any $\mathbf{c} \neq \mathbf{0}$. Thus, $\mathbf{g}$ is balanced.

Conversely, let $\mathbf{g}$ be balanced in the sense of Definition 3. We prove that $|A_k| = |S|/2^m$ is the unique solution of (7). Under the supposition, equation (7) is satisfied for any $\mathbf{c} \neq \mathbf{0}$. Moreover, for $\mathbf{c} = \mathbf{0}$ we have

$$|S| = \sum_{k=0}^{2^m-1} |A_k| , \tag{8}$$

Hence, (7) and (8) represent simultaneous linear equations with unknowns $|A_k|$ with the Hadamard matrix $\mathbf{H}$:

$$\big(|S|, 0, 0, \dots, 0\big) = \big(|A_0|, |A_1|, \dots, |A_{2^m-1}|\big)\mathbf{H} .$$

Since $\det(\mathbf{H}) \neq 0$, the simultaneous equations have only one solution, namely $|A_k| = \ell = |S|/2^m$. □

3. Generalized perfect nonlinearity

A well known characterization of cryptographycaly good functions $\boldsymbol{f}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ (so called S–boxes), is their flat difference table. Nyberg [Ny] has proved that the best result can be obtained in the case when any linear combination of the components of $\boldsymbol{f}$ is a perfectly nonlinear function and $n \geq 2m$. We will generalize this idea to groupoids.

Recall that in the difference table, for a function (S–box) $\mathbf{f}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$, its entries give for any "difference" of arguments $\mathbf{i} \in \mathbb{Z}_2^n$, and for any $\mathbf{y} \in \mathbb{Z}_2^m$ the number of $\mathbf{x} \in \mathbb{Z}_2^n$ satisfying $\mathbf{y} = \boldsymbol{f}(\mathbf{i} \oplus \mathbf{x}) \oplus \boldsymbol{f}(\mathbf{x})$.

Since, for any $\mathbf{x} \in \mathbb{Z}_2^n$

$$\boldsymbol{f}(\mathbf{i} \oplus \mathbf{x}) \oplus \boldsymbol{f}(\mathbf{x}) = \boldsymbol{f}\big(\mathbf{i} \oplus (\mathbf{i} \oplus \mathbf{x})\big) \oplus \boldsymbol{f}(\mathbf{i} \oplus \mathbf{x}) , \tag{9}$$

the equation

$$\mathbf{y} = \boldsymbol{f}(\mathbf{i} \oplus \mathbf{x}) \oplus \boldsymbol{f}(\mathbf{x}) \tag{10}$$

has either no, or at least two solutions for any $\mathbf{i} \neq \mathbf{0}$. Therefore considering a bijection $\boldsymbol{f}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, in the best case one may expect a difference table consisting of 0's, and 2's appearing exactly 2^{n-1} times in all rows with nonzero difference. The row corresponding to the difference zero possesses one element 2^n, and the remaining elements are zeroes.

For the case $\boldsymbol{f}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$, the best one can expect (from the point of view of differential cryptanalysis) is that in all but one row all entries equal $2^{n-m} = |\mathbb{Z}_2^n|/2^m$. The row corresponding to the difference zero possesses one element 2^n, and remaining elements are zeroes. This is possible only for $n \geq 2m$, [Ny]. A function satisfying this condition is called *a generalized perfect nonlinear function*, shortly GPN function. If for any $\mathbf{i} \neq \mathbf{0}$ we define the function

$$D_i\boldsymbol{f}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m, \qquad D_i\boldsymbol{f}(\mathbf{x}) = \boldsymbol{f}(\mathbf{i} \oplus \mathbf{x}) \oplus \boldsymbol{f}(\mathbf{x}), \tag{11}$$

then the definition of GPN can be reformulated in the following way:

A function $\boldsymbol{f}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ is GPN iff for any $\mathbf{i} \neq \mathbf{0}$ the function $D_i\boldsymbol{f}\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ is a balanced function.

Now we will consider a right simple groupoid instead of the group $(\mathbb{Z}_2^n, \oplus)$, $(S, *)$. Then to any function $\boldsymbol{f}\colon S \to \mathbb{Z}_2^m$, and any $i \in S$, i different from a left unit, we assign a function

$$D_i\boldsymbol{f}\colon S \to \mathbb{Z}_2^m, \qquad D_i\boldsymbol{f}(x) = \boldsymbol{f}(i * x) \oplus \boldsymbol{f}(x). \tag{12}$$

Now the notion of GPN function can be generalized in the following way.

Definition 4. A function $\boldsymbol{f}\colon S \to \mathbb{Z}_2^m$ is GPN if for any $i \in S$, i different from a left unit, $D_i\boldsymbol{f}\colon S \to \mathbb{Z}_2^m$ is a balanced function.

Proposition 2. *A function $\boldsymbol{f}\colon S \to \mathbb{Z}_2^m$ is* GPN *iff for any $\mathbf{c} \in \mathbb{Z}_2^m \backslash \mathbf{0}$ the function $\mathbf{c} \cdot (D_i\boldsymbol{f})\colon S \to \mathbb{Z}_2$ is a balanced function.*

Let S be a nonempty set. Then to any subset $A \subset S$ we assign its characteristic function $f_A\colon S \to \mathbb{Z}_2$. Conversely, any function $f\colon S \to \mathbb{Z}_2$ can be considered as a characteristic function of the set $A = \{x \in S\colon f(x) = 1\}$.

Thus there exists a bijection between the set of all functions $f\colon S \to \mathbb{Z}_2$ and the power set $\mathscr{S} = 2^S$. It is well known that the power set $\mathscr{S}$ together with the operation *symmetric difference* $\triangle$ is an Abelian group. Recall that $A \triangle B = (A \setminus B) \cup (B \setminus A)$. The identity element of the group $(\mathscr{S}, \triangle)$ is the empty set, and $A \triangle A = \emptyset$ for any $A \in \mathcal{S}$. Let $C_2 = (\mathbb{Z}_2, \oplus)$. It is known that (cf. [Bu], p. 280) the Abelian group $(\mathscr{S}, \triangle)$ is isomorphic with the group $C_2 \times C_2 \times \cdots \times C_2 = C_2^{|S|}$. This isomorphism $\varphi\colon \mathscr{S} \to C_2^{|S|}$ is given by

$$\varphi(A) = f_A$$

for any $A \in \mathscr{S}$. From the basic property of isomorphism we have

$$f_{A \triangle B} = \varphi(A \triangle B) = \varphi(A) \oplus \varphi(B) = f_A \oplus f_B\,. \tag{13}$$

If we consider a vector function $\boldsymbol{f}\colon S \to \mathbb{Z}_2^m$, $\boldsymbol{f} = (f_1, f_2, \dots, f_m)$, then for any component $f_i\colon S \to \mathbb{Z}_2$ there exists a subset $A_i \subset S$ such that $A_i = \{x \in S\colon f_i(x) = 1\}$. Therefore f_i is a characteristic function of the set A_i. Hence to the function $\boldsymbol{f} = (f_1, f_2, \dots, f_m)$ there is assigned the m-tuple $(A_1, A_2, \dots, A_m)$ of subsets of S such that $\boldsymbol{f} = (f_1, f_2, \dots, f_m) = \big(f_{A_1}, f_{A_2}, \dots, f_{A_m}\big)$. Conversely, to any m-tuple $(A_1, A_2, \dots, A_m)$ of subsets of S there exists the function $\boldsymbol{f} = \big(f_{A_1}, f_{A_2}, \dots, f_{A_m}\big)\colon S \to \mathbb{Z}_2^m$.

Notation 1. Let $\mathbf{c} = (c_1, c_2, \dots, c_m) \in \mathbb{Z}_2^m$, and $A_1, A_2, \dots, A_m$ be subsets of a groupoid S. Then by

$$\triangle_{j=1}^m c_j A_j$$

we denote the symmetric difference of these sets A_j for which $c_j = 1$.

Theorem 2. *Let $(A_1, A_2, \dots, A_m)$ be an m-tuple of subsets of a right simple groupoid S, $\mathscr{S} = 2^S$, and*

$$\boldsymbol{f} = (f_{A_1}, f_{A_2}, \dots, f_{A_m})\colon S \to \mathbb{Z}_2^m .$$

Let $\mathfrak{M} = [A_1, A_2, \dots, A_m]$ be the smallest subgroup of $(\mathscr{S}, \triangle)$ generated by subsets $A_i \subset S$. Then $\boldsymbol{f}$ is GPN *iff for any $B \in \mathfrak{M}$, $B \neq \emptyset$, the function f_B is PN.*

P r o o f. According to Definition 4 and Proposition 2, a function $\boldsymbol{f}$ is GPN iff for any $\mathbf{c} \in \mathbb{Z}_2^m \backslash \mathbf{0}$, the function $\mathbf{c}.D_i\boldsymbol{f}$ is balanced. This is equivalent to

$$\sum_{w \in S} \mathbf{c} \cdot D_i\boldsymbol{f}(w) = \frac{|S|}{2}$$

for any $i \in S$, i different from a left unit. Using (13) we have

$$\begin{aligned}
\sum_{w \in S} \mathbf{c} \cdot D_i\boldsymbol{f}(w) &= \sum_{w \in S} (c_1, c_2, \dots, c_m) \cdot \big(f_{A_1}(i * w) \oplus f_{A_1}(w), \\
&\qquad f_{A_2}(i * w) \oplus f_{A_2}(w), \dots, f_{A_m}(i * w) \oplus f_{A_m}(w)\big) \\
&= \sum_{w \in S} f_{\triangle_{j=1}^m c_j A_j}(i * w) \oplus f_{\triangle_{j=1}^m c_j A_j}(w) \\
&= R_{\triangle_{j=1}^m c_j A_j}(i) = R_B(i) = \frac{|S|}{2} .
\end{aligned}$$

The correspondence between $B \in \mathfrak{M}$ and $\triangle_{j=1}^m c_j A_j$ is obvious. $\square$

4. On the existence of generalized perfectly nonlinear bijections

Let S be a right simple groupoid with cardinality $|S| = 2^n$. Here we show that it is possible to find balanced and generalized perfectly nonlinear functions

$\boldsymbol{f}\colon S \to \mathbb{Z}_2^m$ with completely flat difference table. Recall that in the case $S = \mathbb{Z}_2^n$ a function $\boldsymbol{f}\colon S \to \mathbb{Z}_2^n$ is balanced iff $\boldsymbol{f}$ is a bijection.

First we confine ourselves to the case $|S| = 4$. As mentioned in Section 3, perfect nonlinear functions do not exist for the case $S = \mathbb{Z}_2^n$. To clarify the situation we start with an example.

EXAMPLE 1. We define the multiplication on a groupoid $S = \{0,1,2,3\}$, and $\boldsymbol{f} = \left(f_{A_1}, f_{A_2}\right)$ with components being characteristic functions of the subsets $A_1 = \{0,1,2\}$, $A_2 = \{0,1,3\}$ by

$*$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	1	3	0
3	3	0	1	2

x	f_{A_1}	f_{A_2}	$f_{A_1 \triangle A_2}$
0	1	1	0
1	1	1	0
2	1	0	1
3	0	1	1

By direct computation it is easy to verify that

- f_{A_1}, f_{A_2} are not balanced. Hence $\mathbf{f}$ is not a balanced function (in fact f is not a bijection);
- for any $i \in S$, $i \neq 0$, and any $B \in \{A_1, A_2, A_1 \triangle A_2\}$, $R_B(i) = 2$. Hence $\boldsymbol{f}$ is GPN.

The difference table in this case is as follows:

$i/\mathbf{y}$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
0	4	0	0	0
1	1	1	1	1
2	1	1	1	1
3	1	1	1	1

Our aim is to find a GPN function, defined on a right simple groupoid S, which is at the same time balanced, and possibly with the completely flat difference table. Clearly S cannot possess a left unit. In each row of a multiplication table there is a permutation of elements, and for any $B \in \{A_1, A_2, A_1 \triangle A_2\}$, $R_B(i)$ equals $|S|/2$. To satisfy this requirement we can use the same permutation in each row.

EXAMPLE 2. We define the multiplication on a groupoid $S = \{0,1,2,3\}$, and $\boldsymbol{f} = \left(f_{A_1}, f_{A_2}\right)$ is a pair of characteristic functions of the subsets $A_1 = \{2,3\}$, $A_2 = \{1,3\}$ by

$*$	0	1	2	3
0	0	2	3	1
1	0	2	3	1
2	0	2	3	1
3	0	2	3	1

x	f_{A_1}	f_{A_2}	$f_{A_1 \triangle A_2}$
0	0	0	0
1	0	1	1
2	1	0	1
3	1	1	0

By direct computation it is easy to verify that

- $f_{A_1}, f_{A_2}, f_{A_1 \triangle A_2}$ are balanced. Hence $\boldsymbol{f}$ is a balanced function, and thus $\mathbf{f}\colon S \to \mathbb{Z}_2^2$ is a bijection;
- for any $i \in S$, and any $B \in \{A_1, A_2, A_1 \triangle A_2\}$, $R_B(i) = 2$. Hence $\boldsymbol{f}$ is GPN;

The difference table in this case is as follows:

$i/\mathbf{y}$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
0	1	1	1	1
1	1	1	1	1
2	1	1	1	1
3	1	1	1	1

Thus we have found (for the case $|S| = 4$) a generalized perfectly nonlinear bijection with a completely flat difference table.

Remark 1.

(1) Evidently GPN $\boldsymbol{f}\colon S \to \mathbb{Z}_2^n$ has a completely flat difference table if S possesses no left unit.

(2) From a cryptgraphic point of view it is not desirable to consider a groupoid with the same rows.

According to these two essential conditions our aim is to find a function with good cryptgraphic properties on a quasigroup without left units. To simplify this situation we consider only the basic bijections $\boldsymbol{f}\colon S \to \mathbb{Z}_2^n$, $S = \{0, 1, \dots, 2^n - 1\}$, and $\boldsymbol{f}(x) = x_b$, where x_b is the binary expansion of x.

It is possible, by an exhaustive search, to find for $|S| = 4$ eight bijections (permutations) such that if all rows in the multiplication table of $S = \{0, 1, 2, 3\}$ are equal to such a permutation then the basic bijection $\boldsymbol{f} = (f_{A_1}, f_{A_2})$ is a GPN. They are: (0,2,3,1), (0,3,1,2), (1,2,0,3), (2,0,1,3), (2,1,3,0), (3,1,0,2), (3,0,2,1), (1,3,2,0).

Combining these permutations we obtain exactly two quasigroups S_1, S_2 without left unit (up to a permutation of rows). If $A_1 = \{2, 3\}$, $A_2 = \{1, 3\}$ then for any $i \in S$, and any $B \in \{A_1, A_2, A_1 \triangle A_2\}$, $R_B(i) = 2$. Hence $\boldsymbol{f} = (f_{A_1}, f_{A_2})$ is GPN.

S_1	0	1	2	3
0	0	2	3	1
1	1	3	2	0
2	2	0	1	3
3	3	1	0	2

S_2	0	1	2	3
0	0	3	1	2
1	1	2	0	3
2	2	1	3	0
3	3	0	2	1

A further investigation of used permutations shows the following:

Let $S = \{0, 1, \dots, 2^n - 1\}$, and $(S, *)$ be a right simple groupoid. If we consider functions $\boldsymbol{f}\colon S \to \mathbb{Z}_2^n$, $\boldsymbol{f}(x) = x_b$, where x_b is the binary expansion of x, then the condition (12) can be reformulated as follows:

$$D_i \boldsymbol{f}(x) = (i * x)_b \oplus x_b\,, \tag{14}$$

where $(i * x)$, $x \in S$, represents the used permutation for the row of the Cayley table of S corresponding to i.

In this case the ith row of the difference table of $\mathbf{f}$ is completely flat iff it consists only of 1's. This implies that the function $D_i \boldsymbol{f}\colon S \to \mathbb{Z}_2^n$ is a balanced function. But this case is possible if $D_i \boldsymbol{f}$ is a bijection only. Therefore we must consider two permutations. The first one is $\alpha\colon S \to S$ given by $\alpha(x) = i * x$ which coincides with the ith row of the Cayley table of the groupoid S. The second permutation is $\beta\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, $\beta(x_b) = (i * x)_b \oplus x_b = D_i \boldsymbol{f}(x)$. Clearly the permutation α induces on $\mathbb{Z}_2^n$ a permutation $\alpha_b\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, $\alpha_b(x_b) = (i * x)_b$. Obviously the operation $\oplus$ is performed on C_2^n. Therefore to define the ith row of $(S, *)$ we must find two permutations α_b, β such that

$$\beta(x_b) = \alpha_b(x_b) \oplus x_b\,.$$

This fact leads directly [DK] to the notion of a *transversal of a quasigroup.*

Definition 5. 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.

Thus the permutation β is a transversal on C_2^n. Once a β is defined, we can describe the permutation α_b by the following way:

$$\beta(x_b) \oplus x_b = \big((i * x)_b \oplus x_b\big) \oplus x_b = (i * x)_b = \alpha_b(x_b)\,.$$

At the same time we define the ith row of $(S, *)$ by $\alpha(x) = i * x$. The existence of the permutation β is guaranteed by the more general Theorem 1.4.5 from [DK], p. 33. For Abelian groups we get

Theorem 3. *Let G be an Abelian group with elements $a_1, a_2, \dots, a_N$, and L be its Cayley table. Then L possesses a transversal if and only if $a_1 * a_2 * \cdots * a_N = e$, the identity element of G.*

It is readily seen that according to this theorem C_2^n possesses a transversal.

Our aim is to define a binary operation $*$ on S such that $(S,*)$ is a quasigroup. If we have defined by α the ith row in $(S,*)$, the jth row, $j \neq i$, is defined by another permutation $\alpha'\colon S \to S$ such that

$$\alpha(x) \neq \alpha'(x)$$

for any $x \in S$. Evidently

$$\alpha_b(x_b) \neq \alpha'_b(x_b)\,.$$

Moreover

$$\beta(x_b) = \alpha_b(x_b) \oplus x_b \neq \alpha'_b(x_b) \oplus x_b = \beta'(x_b)$$

for any $x_b \in C_2^n$.

If all rows in $(S,*)$ are defined in such a way, i.e., S is a quasigroup, then the Cayley table of C_2^n has to be decomposed into 2^n disjoint transversals. The possibility of such a procedure is provided by Theorem 1.4.2 presented in [DK], p. 29. For Abelian groups we get

Theorem 4. *If a Cayley table L of an Abelian group G of order N possesses at least one transversal then L has a decomposition into N disjoint transversals.*

Proof of Theorem 4 in [DK] p. 29, suggests a way how to decompose such a latin square:

Let $\beta\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ be a transversal. Then any other transversal $\beta'\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ from the Theorem 4 can be formed by a choice of $y_b \in \mathbb{Z}_2^n$, $y_b \neq 0_b$, and the relation

$$\beta'(x_b) = \beta(x_b) \oplus y_b\,.$$

This proves our main result, Theorem 5, and confirms at the same time a conjecture we posed during a conference [GSN].

Theorem 5. *For any $n > 1$ there exists a quasigroup S of the cardinality $|S| = 2^n$, and a generalized perfectly nonlinear bijection $\boldsymbol{f}\colon S \to \mathbb{Z}_2^n$ with a completely flat difference table.*

For the case $n = 3$ we found 384 transversals of the Cayley table of C_2^3. Each of these transversals leads to one permutation $\alpha\colon S \to S$, $S = \{0,1,\dots,7\}$. One such permutation is, e.g., (0,2,4,6,3,1,7,5). As an example of the quasigroup we present the following:

Remark 2. Theorem 5 is crucial for solving the problem in the case $|S| = 2^m\ell$. One can divide S into 2^m parts, and then map elements from one class to the same point of a given transversal. The results will appear in a sequel to this paper.

S	0	1	2	3	4	5	6	7
0	0	2	4	6	3	1	7	5
1	1	3	5	7	2	0	6	4
2	2	0	6	4	1	3	5	7
3	3	1	7	5	0	2	4	6
4	4	6	0	2	7	5	3	1
5	5	7	1	3	6	4	2	0
6	6	4	2	0	5	7	1	3
7	7	5	3	1	4	6	0	2

REFERENCES

[Br] BRUALDI, R. A.—RYSER, H. J.: *Combinatorial Matrix Theory*, Cambridge University Press, Cambridge, 1991.

[Bu] BUDDEN, F. J.: *The Fascination of Groups*, Cambridge University Press, Cambridge, 1972.

[DK] DÉNES, J.—KEEDWELL, A. D.: *Latin Squares and their Applications*, Akadémiai Kiadó, Budapest, 1974.

[GW] GROŠEK, O., WEI, W.: *Bent-like functions on groupoids*, Pure Math. Appl. Budapest (H) & Siena (I) Publisher, 1998 (to appear).

[GSN] 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. 1 page.

[Ny] NYBERG, K.: *Perfect nonlinear S-boxes. Advances in Cryptology – Proceedings of Eurocrypt '90*, in: Lecture Notes in Comput. Sci., Vol. 473, Springer-Verlag, Berlin, pp. 378–386, 1990.

Received February 25, 2000

Otokar Grošek, Ladislav Satko
Department of Mathematics
Faculty of Electrical Engineering
and Computer Science
Slovak University of Technology
Ilkovičova 3
SK–812 19 Bratislava
SLOVAKIA

E-mail: grosek@kmat.elf.stuba.sk
satko@kmat.elf.stuba.sk

Karol Nemoga
Mathematical Institute
Slovak Academy of Sciences
Štafánikova 49
SK–814 73 Bratislava
SLOVAKIA

E-mail: nemoga@mat.savba.sk