Perfect nonlinear S-boxes

KAISA NYBERG

Finnish Defense Forces and University of Helsinki

Abstract. A perfect nonlinear S-box is a substitution transformation with evenly distributed directional derivatives. Since the method of differential cryptanalysis presented by E. Biham and A. Shamir makes use of nonbalanced directional derivatives, the perfect nonlinear S-boxes are immune to this attack. The main result is that for a perfect nonlinear S-box the number of input variables is at least twice the number of output variables. Also two different construction methods are given. The first one is based on the Maiorana-McFarland construction of bent functions and is easy and efficient to implement. The second method generalizes Dillon's construction of difference sets.

1. Introduction

The study of the properties of the substitution transformations of DES has resulted in a wealth of nonlinearity criteria for Boolean functions, whose applications are not restricted to DES-like block ciphers but are useful in the analysis of any cryptographic algorithm where nonlinear transformations are used. An overview of nonlinearity criteria with extensive bibliography is given in [16].

The two most successful publicly presented attacks on DES make use of the so called linear structures of S-boxes. Chaum and Evertse [3] were able to find six-bit blocks such that when they are xored to the input of an S-box the output is always changed by a same (zero or nonzero) block. By chaining these linear structures they are able to successfully attack DES up till six rounds.

Biham and Shamir develop in [2] this idea further and are able to attack more rounds. They only require that with certain changes in the input of an S-box the change in the output is known with a high probability. Therefore they look for input changes with most unevenly distributed output changes.

In this paper we study substitution transformations with evenly distributed output changes. Their importance is also noticed in [4] We shall show that such perfect nonlinear transformations exist and can be efficiently implemented but only when the input block is twice as long as the output block.

In [12] Meier and Staffelbach discuss perfect nonlinear Boolean functions, which are defined to be at maximum distance from linear structures. These functions are the same as the previously known bent functions [15]. To construct perfect nonlinear S-boxes it is necessary that each output bit is a perfect nonlinear function of the input. But it is not sufficient, indeed, also every linear combination of the output variables have to be perfect nonlinear. We present two different constructions to achieve this property.

In §2 we recall the basic facts of q-ary bent functions as their definition and construction by the Maiorana-McFarland method. We also present a second construction which makes use of the field structure of $GF(p^n)$ and generalizes Dillon's construction of difference set in $GF(2^n)$ given in [6]. The property of perfect nonlinearity for functions from $\mathbf{Z}_p^n$ to $\mathbf{Z}_p^m$, p prime, is studied in §3. The main result is that perfect nonlinear functions, such that all linear combinations of output variables are regular bent functions of the input, exist only if $n \geq 2m$. Using a linear feedback shift register to generate a

D.W. Davies (Ed.): Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp. 378-386, 1991.

suitable set of permutations an efficient construction of perfect nonlinear functions is given in §4. Since perfect nonlinear functions are quite rare it might be a good idea to begin a construction of a cryptographic function from a perfect nonlinear function and then modify it to satisfy other requirements. In §4 we present an example how balancedness can be achieved without completely destroying the original good property. In §5 a different construction is presented which also gives a wealth of perfect nonlinear functions.

2. Bent functions

Let q be a positive integer and denote the set of integers modulo q by $\mathbf{Z}_q$. Let

$$u = e^{i\frac{2\pi}{q}}$$

be the qth root of unity in $\mathbf{C}$, where $i = \sqrt{-1}$. Let f be a function from the set $\mathbf{Z}_q^n$ of n-tuples of integers modulo q to $\mathbf{Z}_q$. Then the *Fourier transform* of u^f is defined as follows

$$F(\mathbf{w}) = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{x} \in \mathbf{Z}_q^n} u^{f(\mathbf{x}) - \mathbf{w}\cdot\mathbf{x}}, \quad \mathbf{w} \in \mathbf{Z}_q^n.$$

The following definition is given in [7].

DEFINITION 2.1. *A function $f : \mathbf{Z}_q^n \to \mathbf{Z}_q$ is bent if $|F(\mathbf{w})| = 1$, for all $\mathbf{w} \in \mathbf{Z}_q^n$.*

Let f and g be two functions from $\mathbf{Z}_q^n$ to $\mathbf{Z}_q$. Then their *shifted cross-correlation*

$$c(f,g)(\mathbf{w}) = \frac{1}{q^n} \sum_{\mathbf{x} \in \mathbf{Z}_q^n} u^{f(\mathbf{x}+\mathbf{w}) - g(\mathbf{x})}.$$

From these definitions the following characterization is immediate.

THEOREM 2.1. *A function $f : \mathbf{Z}_q^n \to \mathbf{Z}_q$ is bent if and only if*

$$|c(f,L)(\mathbf{w})| = \frac{1}{\sqrt{q^n}}$$

for all linear (or affine) functions $L : \mathbf{Z}_q^n \to \mathbf{Z}_q$ and $\mathbf{w} \in \mathbf{Z}_q^n$.

Analogously to the binary case it then follows that the q-ary bent functions have the minimum correlation to the set of all affine functions (see Theorem 3.5 in [12]).

In [7] also the following result can be found.

THEOREM 2.2. *A function $f : \mathbf{Z}_q^n \to \mathbf{Z}_q$ is bent if and only if*

$$c(f,f)(\mathbf{w}) = 0, \text{ for all } \mathbf{w} \neq \mathbf{0}.$$

This is in the binary case exactly the property of perfect nonlinearity used by Meier and Staffelbach [12] to define bent functions. In [13] the following generalization is made.

DEFINITION 2.2. *A function* $f : \mathbf{Z}_q^n \to \mathbf{Z}_q$ *is perfect nonlinear if for every fixed* $\mathbf{w} \in \mathbf{Z}_q^n$, $\mathbf{w} \neq 0$, *the difference*

$$f(\mathbf{x} + \mathbf{w}) - f(\mathbf{x})$$

obtains each value $k \in \mathbf{Z}_q$ *for exactly* q^{n-1} *values of* $\mathbf{x} \in \mathbf{Z}_q^n$.

THEOREM 2.3. *A perfect nonlinear function from* $\mathbf{Z}_q^n$ *to* $\mathbf{Z}_q$ *is bent. The converse is true if* q *is a prime.*

The following theorem is due to Kumar, Scholtz and Welch [7]. For $q = 2$ it was proved by Maiorana (unpublished, see [6]) generalizing the construction method of Rothaus [15]. An equivalent method is given by McFarland in [11].

THEOREM 2.4. *Let* $g : \mathbf{Z}_q^m \to \mathbf{Z}_q$ *be any function and* $\pi : \mathbf{Z}_q^m \to \mathbf{Z}_q^m$ *any permutation. Then the function*

$$f : \mathbf{Z}_q^{2m} = \mathbf{Z}_q^m \times \mathbf{Z}_q^m \to \mathbf{Z}_q,\ f(\mathbf{x}_1, \mathbf{x}_2) = \pi(\mathbf{x}_1) \cdot \mathbf{x}_2 + g(\mathbf{x}_1)$$

is a regular bent function.

A third equivalent way of looking at this construction in the binary case is to make use of Hadamard matrices as described in [8]. This method is also discussed in [14]. The constructions given in [1] and [17] are special cases of the Maiorana-MacFarland construction.

A completely different construction of bent functions in $GF(2^n)$ with an even n is due to Dillon. Indeed, the main result of [5] is that this method gives bent functions which are not affinely equivalent to any Maiorana function. We have the following generalization of Dillon's construction.

THEOREM 2.5. *Let* p *be a prime and* $n = 2m$. *Denote by* $G = GF(p^m)$ *the subfield of* $F = GF(p^n)$ *and let* α *be a primitive element in* F. *Then the cosets of* G^*

$$H_i = \alpha^i G^*,\ i = 0, 1, \ldots, p^m,$$

are all distinct and their union is the set of non-zero elements of F. *Assume that the set of indices* $1, 2, \ldots, p^m$ *is divided into* p *disjoint subsets* $A_0, A_1, \ldots, A_{p-1}$ *of cardinality* p^{m-1} *each. Then the function* $f : GF(p^n) \to GF(p)$,

$$\begin{aligned} &f(0) = 0 \\ &f(\mathbf{x}) = 0,\ \text{for } x \in H_0, \\ &f(\mathbf{x}) = k,\ \text{for } x \in H_i,\ i \in A_k,\ k = 0, 1, \ldots, p-1, \end{aligned}$$

is a bent function in F.

The proof of this theorem is a straightforward but lengthy checking of the condition on perfect nonlinearity. The main argument is that for every nonzero $\mathbf{w}$ the elements $\mathbf{x} + \mathbf{w}$ belong to distinct cosets of G for distinct elements $\mathbf{x}$ in a fixed coset.

3. Perfect nonlinear transformation

We give the following further generalization of perfect nonlinearity.

DEFINITION 3.1. *A function* $\mathbf{f} : \mathbf{Z}_q^n \to \mathbf{Z}_q^m$ *is perfect nonlinear if for every fixed* $\mathbf{w} \in \mathbf{Z}_q^n$ *the difference*

$$\mathbf{f}(\mathbf{x}+\mathbf{w}) - \mathbf{f}(\mathbf{x})$$

obtains each value $\mathbf{y} \in \mathbf{Z}_q^m$ *for* q^{n-m} *values of* $\mathbf{x}$.

We call the function

$$D_{\mathbf{w}}\mathbf{f} : \mathbf{Z}_q^n \to \mathbf{Z}_q^m,\ \mathbf{x} \mapsto \mathbf{f}(\mathbf{x}+\mathbf{w}) - \mathbf{f}(\mathbf{x}),$$

the derivative of $\mathbf{f}$ to the direction $\mathbf{w}$. Then we can say that $\mathbf{f}$ is perfect nonlinear if and only if its derivatives to all nonzero directions are balanced functions. By definition, a function $\mathbf{g} : \mathbf{Z}_q^n \to Z_q^m$ is balanced if and only if for every $\mathbf{c} \in \mathbf{Z}_q^m,\ \mathbf{c} \neq \mathbf{0}$ the function $\mathbf{x} \mapsto \mathbf{c} \cdot \mathbf{g}(\mathbf{x})$ is balanced. Since moreover,

$$D_{\mathbf{w}}(\mathbf{c} \cdot \mathbf{f}) = \mathbf{c} \cdot D_{\mathbf{w}}\mathbf{f},$$

we have the following characterization.

THEOREM 3.1. *A function* $\mathbf{f} : \mathbf{Z}_q^n \to \mathbf{Z}_q^m$ *is perfect nonlinear if and only if for every nonzero* $\mathbf{c} \in \mathbf{Z}_q^m$ *the function*

$$\mathbf{x} \mapsto \mathbf{c} \cdot \mathbf{f}(\mathbf{x})$$

is perfect nonlinear in the sense of Definition 2.2.

In other words, a blockfunction is perfect nonlinear if and only if every linear combination of its output coordinates is perfect nonlinear.

Assume now that p is a prime. Then perfect nonlinearity and bentness of a $\mathbf{Z}_p$-valued function in $\mathbf{Z}_p^n$ are equivalent concepts, see Theorem 2.3. The value distributions of p-ary bent functions are derived in [13]. Let us now consider the value distributions of perfect nonlinear blockfunctions. Recall that a function $f : \mathbf{Z}_p^n \to \mathbf{Z}_p$ is called a regular bent function if there is a function $g : \mathbf{Z}_p^n \to \mathbf{Z}_p$ such that $F(\mathbf{w}) = u^{g(\mathbf{w})}$, for all $\mathbf{w} \in \mathbf{Z}_p^n$ ([7], [13]). If $p = 2$ then all bent functions are regular.

THEOREM 3.2.. *Let* n *be even and* $\mathbf{f} : \mathbf{Z}_p^n \to \mathbf{Z}_p^m$ *a perfect nonlinear function such that the functions*

$$\mathbf{x} \mapsto \mathbf{c} \cdot \mathbf{f}(\mathbf{x}),\ \mathbf{c} \in \mathbf{Z}_p^m, \mathbf{c} \neq \mathbf{0},$$

are regular bent functions. Let

$$a_{\mathbf{y}} = \#\{\mathbf{x} \in \mathbf{Z}_p^n \mid \mathbf{f}(\mathbf{x}) = \mathbf{y}\},\ \mathbf{y} \in \mathbf{Z}_p^m.$$

Then

$$a_{\mathbf{y}} = p^{\frac{n}{2}-m} b_{\mathbf{y}},\ \text{ for every } \mathbf{y},$$

where $b_{\mathbf{y}}$ *is a positive integer not divisible by* p. *Also,*

$$p^{n-m} + p^{\frac{n}{2}-m} - p^{\frac{n}{2}} \leq a_{\mathbf{y}} \leq p^{n-m} - p^{\frac{n}{2}-m} + p^{\frac{n}{2}}.$$

PROOF: Let $\mathbf{c} \in \mathbf{Z}_p^m$, $\mathbf{c} \neq 0$ and denote the Fourier transform of the function $\mathbf{x} \mapsto \mathbf{c} \cdot \mathbf{f}(\mathbf{x})$ by $F_{\mathbf{c}}(0)$. Then

$$p^{\frac{n}{2}} F_{\mathbf{c}}(0) = \sum_{\mathbf{x} \in \mathbf{Z}_p^n} u^{\mathbf{c} \cdot \mathbf{f}(\mathbf{x})} = \sum_{\mathbf{y} \in \mathbf{Z}_p^m} a_{\mathbf{y}} u^{\mathbf{c} \cdot \mathbf{y}}.$$

Taking the sum over $\mathbf{c} \neq 0$ we obtain

$$\sum_{\mathbf{y}} a_{\mathbf{y}} \sum_{\mathbf{c} \neq 0} u^{\mathbf{c} \cdot \mathbf{y}} = p^{\frac{n}{2}} \sum_{\mathbf{c} \neq 0} F_{\mathbf{c}}(0).$$

Let $S = \sum_{\mathbf{c} \neq 0} F_{\mathbf{c}}(0)$. Then we have

$$\sum_{\mathbf{y} \neq 0} a_{\mathbf{y}}(-1) + a_0(p^m - 1) = p^{\frac{n}{2}} S$$

from which

$$S = p^{n - \frac{n}{2}} + a_0 p^{m - \frac{n}{2}}.$$

To prove the claim it suffices to show that S is an integer not divisible by p. Since n is even, S is a rational number. Let

$$r_k = \#\{\mathbf{c} \in \mathbf{Z}_p^m \setminus \{0\} \mid F_{\mathbf{c}}(0) = u^k\}, \quad k = 0, 1, \ldots, p-1.$$

Then, due to the regularity assumption,

$$\sum_{k=0}^{p-1} r_k = p^m - 1 \quad \text{and} \quad S = \sum_{k=0}^{p-1} r_k u^k$$

and hence

$$r_0 - S = r_1 = r_2 = \cdots = r_{p-1},$$

from which it follows that S is an integer and p devides $\sum r_k - S = p^m - 1 - S$, which proves the claim.

The estimates for $a_{\mathbf{y}}$ follow from the estimates

$$-p^m + 1 \leq S \leq p^m - 1.$$

Indeed, in the context of this theorem, we always have $n \geq 2m$. Since $a_{\mathbf{y}}$ is an integer and binary bent functions are regular and exist only if the input space is of even dimension, we have the following

COROLLARY. *For a perfect nonlinear binary S-box the dimension of the input space is at least twice the dimension of the output space.*

4. A construction based on Maiorana-McFarland method

Let n be an even positive integer, $\mathbf{f} : \mathbf{Z}_p^n \to \mathbf{Z}_p^m$ a function and denote the m output coordinate functions of f by $f_1, f_2, \ldots, f_m$. Assume that every f_i, $i = 1, 2, \ldots, m$, is a Maiorana function, i.e., has the form

$$f_i(\mathbf{x}) = f_i(\mathbf{x}_1, \mathbf{x}_2) = \pi_i(\mathbf{x}_1) \cdot \mathbf{x}_2 + g_i(\mathbf{x}_1),$$

where π_i is a permutation of the space $\mathbf{Z}_p^{\frac{n}{2}}$ and g_i is a function from $\mathbf{Z}_p^{\frac{n}{2}}$ to $\mathbf{Z}_p$. Then $\mathbf{f} = (f_1, f_2, \ldots, f_m)$ is perfect nonlinear if every nonzero linear combination of the permutations π_i, $i = 1, 2, \ldots, m$ is again a permutation of $\mathbf{Z}_p^{\frac{n}{2}}$. Since Maiorana functions are regular bent we have by the remark at the end of §3 that $n \geq 2m$.

One way of constructing a family of permutations with the required property, is to use a linear feedback shift register of length $\frac{n}{2}$ and with a primitive feedback polynomial. Let A be the state transition function of such a shift register. Then A is a permutation of the space $\mathbf{Z}_p^{\frac{n}{2}}$ as well as the powers A^i of A,

$$A^i = \overbrace{A \circ \cdots \circ A}^{i \text{ times}}, \quad i = 1, 2, \ldots.$$

Moreover, it is a wellknown property of linear feedback shift registers that generate maximal length sequences that every non-trivial linear combination of the permutations

$$I, A, A^2, \ldots, A^{\frac{n}{2}-1}$$

is a power of A and hence a permutation.

Now an elementary implementation of a perfect nonlinear S-box with n input variables and m output variables, $n \geq 2m$, is obtained in the following way. Take a $\frac{n}{2}$-shift register with a primitive feedback polynomial. Devide the input block of length n into two halves $\mathbf{x}_1$ and $\mathbf{x}_2$. The first digit of the output block of length m is obtained by calculating the dot product $\mathbf{x}_1 \cdot \mathbf{x}_2$. To obtain the second digit the shift register is shifted once and the dot product of its new contents with $\mathbf{x}_2$ is calculated. In this manner every shift of the register produces a new output digit. This basic arrangement is very efficient and suitable for on-line applications. If the functions g_i are used their complexity may cause reduction of the speed.

Let us still consider the properties of the basic arrangement,

$$\mathbf{f} = (f_1, f_2, \ldots, f_m), \quad f_i(\mathbf{x}_1, \mathbf{x}_2) = A^{i-1}(\mathbf{x}_1) \cdot \mathbf{x}_2.$$

This perfect nonlinear function $f : \mathbf{Z}_p^n \to \mathbf{Z}_p^m$ is not balanced. The all-zero output block is obtained for

$$p^{n-m} - p^{\frac{n}{2}-m} + p^{\frac{n}{2}}$$

different inputs and the other possible outputs are obtained for equally many, i.e., for

$$p^{n-m} - p^{\frac{n}{2}-m}$$

different inputs. In some applications it might be possible that the first half $\mathbf{x}_1$ of the input that goes to the shift register is never the all zero block. With this restriction the function $\mathbf{f}$ is balanced. Let us see what is the effect of this restriction to the directional derivatives.

Let the nonzero increment $\mathbf{w}$ have two halves $\mathbf{w}_1$ and $\mathbf{w}_2$ corresponding to the division of the input. Then

$$f_i(\mathbf{x}+\mathbf{w}) - f_i(\mathbf{x}) = A^{i-1}(\mathbf{x}_1)\cdot\mathbf{w}_2 + A^{i-1}(\mathbf{w}_1)\cdot\mathbf{x}_2 + A^{i-1}(\mathbf{w}_1)\cdot\mathbf{w}_2,$$

for every $i = 1, 2, \ldots, m,$. Now we have two cases.

1° $\mathbf{w}_1 = \mathbf{0}$. In this case the directional derivative

$$D_{\mathbf{w}}\mathbf{f}(\mathbf{x}) = \mathbf{f}(\mathbf{x}+\mathbf{w})) - \mathbf{f}(\mathbf{x})$$

is a linear function of $\mathbf{x}_1$ and obtains each nonzero value for p^{n-m} different inputs and the zero value for $p^{n-m} - p^{\frac{n}{2}}$ different inputs.

2° $\mathbf{w}_1 \neq \mathbf{0}$. Then the directional derivative is balanced.

As a conclusion we can say that the restriction to the inputs with nonzero first halves gives a balanced and almost perfect nonlinear function.

Other possible families of permutations $\{\pi_1, \pi_2, \ldots, \pi_m\}$ to be used in the Maiorana-McFarland based construction are, for example

$$\pi_i(\mathbf{x}) = \mathbf{a}_i\mathbf{x},$$

where $\{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m\}$ are linearly independent elements of the Galois field $GF(p^{\frac{n}{2}})$, or as a special case,

$$\pi_i(\mathbf{x}) = \alpha^i\mathbf{x},$$

where α is a primitive element of $GF(p^{\frac{n}{2}})$.

The problem of finding suitable permutations is related to the problem of complete mappings and orthogonal Latin squares (see [9],§9.4 and [10]). The following theorem illustrates this relationship. For more evolved constructions of orthogonal Latin squares we refer to [5], Ch. 7.

THEOREM 4.1.. *Let π and σ be permutations of $\mathbf{Z}_p^n$ and let $\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{p^n-1}$ be the elements of $\mathbf{Z}_p^n$. Then the $p^n \times p^n$ matrices*

$$(\pi(\mathbf{a}_i) + \mathbf{a}_j)_{ij} \text{ and } (\sigma(\mathbf{a}_i) + \mathbf{a}_j)_{ij}$$

are orthogonal Latin squares if and only if $\pi - \sigma$ is a permutation.

It is not difficult to check that if the sum of two permutations of $\mathbf{Z}_2^3$ is a permutation then these permutations are affinely equivalent mappings. For $n \geq 4$ nonlinear permutations can have a permutation sum even if they are not affinely equivalent.

Example. The following nonlinear permutations π and σ of $\mathbf{Z}_2^4$ have a sum which is a permutation.

$\mathbf{x}$	=	1	2	3	4	5	6	7	8	9	A	6	B	C	D	E	F
$\pi(\mathbf{x})$	=	0	2	D	1	3	8	A	9	C	F	B	E	7	5	4	6
$\sigma(\mathbf{x})$	=	0	3	4	2	1	D	E	F	6	7	C	5	8	B	9	A
$(\pi+\sigma)(\mathbf{x})$	=	0	1	9	3	2	5	4	6	A	8	7	B	F	E	D	C

Also π and σ are not affinely equivalent, i.e., $\pi^{-1}\sigma$ is nonlinear.

5. A second construction

Let f_i, $i = 1, 2, \ldots, m$ be bent functions from $GF(p^n)$ to $GF(p)$ constructed by the method given in Theorem 2.5. Assume that the assignments of the values $0, 1, \ldots, p-1$ to the different cosets of G for different f_i satisfy the following compatibility condition. For every nonzero $\mathbf{c} = (c_1, c_2, \ldots, c_m) \in GF(p^m)$ the function $c_1 f_1 + c_2 f_2 + \cdots + c_3 f_3$ obtains each of the values $1, 2, \ldots, p-1$ on $p^{\frac{n}{2}-1}$ cosets from $H_1, H_2, \ldots, H_{p^{\frac{n}{2}}}$. Then the function $\mathbf{f} = (f_1, f_2, \ldots, f_m)$ is perfect nonlinear. In fact, the given compatibility condition is also necessary for $\mathbf{f}$ to be perfect nonlinear.

The assignment of values for f_i can be done by using a function $h_i : \mathbf{Z}_{p^{\frac{n}{2}}} \to \mathbf{Z}_p$ defined in the following way. For $k \in \mathbf{Z}_p$ and $i = 1, 2, \ldots, m$ we set

$$h_i(a) = k, \text{ if } f_i(\mathbf{x}) = k \text{ for } \mathbf{x} \in H_{a+1}.$$

THEOREM 5.1. *Let f_i, $i = 1, 2, \ldots, m$ be bent functions in $GF(p^n)$ constructed by the generalization of Dillon's method. Let h_i be the value assignment function for f_i, $i = 1, 2, \ldots, m$. Then the function*

$$\mathbf{f} : GF(p^n) \to GF(p^m), \ \mathbf{f}(\mathbf{x}) = (f_1(\mathbf{x}), f_2(\mathbf{x}), \ldots, f_m(\mathbf{x})),$$

is perfect nonlinear if and only if for every nonzero $\mathbf{c} = (c_1, c_2, \ldots, c_m) \in GF(p^m)$ the function $c_1 h_1 + c_2 h_2 + \cdots + c_m h_m$ is balanced.

In the terminology of [9], Ch. 7, the statement of the theorem says that $\mathbf{f}$ is perfect nonlinear if and only if the functions h_i, $i = 1, 2, \ldots, m$, form an orthogonal system of permutation polynomials. Hence especially, for $m = \frac{n}{2}$, every permutation of the space $\mathbf{Z}_p^{\frac{n}{2}}$ gives, via this construction, a perfect nonlinear function from $\mathbf{Z}_p^n$ to $\mathbf{Z}_p^{\frac{n}{2}}$ and different permutations give different functions. Since the fixed coset H_0 can be chosen in $(p^{\frac{n}{2}} + 1)$ ways the number of perfect nonlinear functions with maximal output given by this construction is $(p^{\frac{n}{2}} + 1)!$.

Acknowledgement

I wish to thank Ossi Ojala for useful computer programs.

REFERENCES

1. C. M. Adams and S. E. Tavares, *The use of bent sequences to achieve higher-order strict avalanche criterion in S-box design*, IEE Proceedings (to appear).
2. E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, Proceedings of Crypto '90 (to appear).
3. D. Chaum and J. H. Evertse, *Cryptanalysis of DES with a reduced number of rounds*, Advances in Cryptology, Proceedings of Crypto '85, Springer-Verlag 1986, 192–211.
4. M. H. Dawson and S. E. Tavares, *An expanded set of s-box design criteria based on information theory and its relation to differential-like attacks*, These Proceedings.
5. J. Denes and A. D. Keedwell, "Latin squares and their applications," The English Universities Press Ltd, London, 1974.
6. J. F. Dillon, *Elementary Hadamard difference sets*, Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, Florida (1975), 237–249; Congressus Numerantium No. XIV, Utilitas Math., Winnipeg, Manitoba (1975).
7. P. V. Kumar, R. A. Scholtz and L. R. Welch, *Generalized bent functions and their properties*, J. Combinatorial Theory, Ser. A 40 (1985), 90–107.

8. A. Lempel and M. Cohn, *Maximal families of bent sequences*, IEEE Trans. Inform. Theory **IT-28** (1982), 865–868.
9. R. Lidl and H. Niederreiter, "Finite fields. Encyclopedia of Mathematics and its applications, Vol. 20," Addison-Wesley, Reading, Massachusetts, 1983.
10. H. B. Mann, *The construction of orthogonal Latin squares*, Ann. Math. Statist. **13** (1942), 418–423.
11. R. L. McFarland, *A family of difference sets in non-cyclic groups*, J. Combinatorial Theory, Ser. A **15** (1973), 1–10.
12. W. Meier and O. Staffelbach, *Nonlinearity criteria for cryptographic functions*, Proceedings of Eurocrypt '89, Springer 1990, 549–562.
13. K. Nyberg, *Constructions of bent functions and difference sets*, Proceedings of Eurocrypt '90, Springer-Verlag 1991, 151–160.
14. B. Preneel et al.,, *Propagation characteristics of Boolean bent functions*, Proceedings of Eurocrypt '90, Springer-Verlag 1991, 161–173.
15. O. S. Rothaus, *On "bent" functions*, J. Combinatorial Theory, Ser. A **20** (1976), 300–305.
16. R. A. Rueppel, *Stream Ciphers*, in "Contemporary Cryptology: The Science of Information Integrity," edited by Gustavus Simmons, IEEE Press (to appear).
17. R. Yarlagadda and J. E. Hershey, *Analysis and synthesis of bent sequences*, IEE Proceedings **136** (1989), 112–123.