Proceedings of the Conference on March 14 - International Day of Mathematics

Vuković, Mirjana, urednik; Nurkanović, Mehmed, urednik

2024-12-26

Academy of Sciences and Arts of Bosnia and Herzegovina

https://bastina.anubih.ba/handle/123456789/798

PROCEEDINGS OF THE CONFERENCE ON MARCH 14 – INTERNATIONAL DAY OF MATHEMATICS
Special Editions ANUBiH, Book CCXVI, OPMN Book 30
Sarajevo 2024, **p. 15–20** DOI: 10.5644/PI2024.216.03

PERFECT NONLINEAR FUNCTIONS AND THEIR APPLICATIONS

AMELA MURATOVIĆ-RIBIĆ

ABSTRACT. Perfect nonlinear functions are closely related to cryptoanalysis. They are defined on finite groups and represent a connection between computer science, algebra, number theory and combinatorics. In addition to the importance for formation of secure cryptological tools, they are used both in the theory of coding, and in pure mathematics. The most important related results of this significant subfield of mathematics, so far, are presented.

1. INTRODUCTION

Cryptology, due to the intensive development of information technologies, has a very important role and is intensively developing, adapting to new trends. For this reason,we also witness also the development of mathematics that has applications in cryptology, and these two lines of research are closely related. This is the motivation for the article about perfectly nonlinear functions that play a significant role in the development of symmetric cryptosystems.

The derivative over real and complex functions is very significant and represents the best affine approximation of functions in the neighborhood of a given point. On the other hand, when it is defined over finite groups, its meaning is somewhat different and has an application in combinatorics, in designs and other combinatorial structures such as differential sets. Cryptology, as a science, consists of encryption, decryption and cryptanalysis, i.e. attacks on encryption systems. In the late 1980s, Sean Murphy studied the FEAL encryption algorithm considering equations of the form $G(x+a) - G(x) = b$, and at the same time Eli Biham and Adi Shamir concluded that in DES equal differences in the plaintext produce equal differences in the chipertext more often than usual, which initiated development of differential cryptanalysis. APN over the field of characteristic 2 was found in 2009 which led to a new direction of development in this field of mathematics, see [1].

Definition 1.1. *Let A and B be finite Abelian groups i $F : A \to B$ a function. For a given $a \in A$, a function defined by*

$$D_a F : A \to B, \qquad x \mapsto F(x+a) - F(x)$$

2020 *Mathematics Subject Classification.* 68P25.
Key words and phrases. perfect nonlinear functions, bent functions, S-box.

is called the ***derivative of*** F.

For given $a \in A$ and $b \in B$ the relation

$$F(x+a) - F(x) = b. \tag{1.1}$$

it is called ***the derivative with input difference*** a ***and output difference*** b.

In computer science, it is common to write data using strings, i.e. zero and one strings of length n. Transformations are performed on these strings, especially during encryption and coding, and for this reason it is necessary to use the mathematical tools of first linear algebra and then finite fields for easier manipulation of strings.

Let q be a positive integer and let $\mathbb{Z}_q$ be a ring. Since we are looking at strings, we denote the function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ with the lowercase letter f, that is, $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$, and the functions with the domain of several variables with the uppercase letter $F : \mathbb{Z}_q^n \to \mathbb{Z}_q^m$. The introduction to differential cryptanalysis led to the study of differentials for nonlinear functions and to the study of the number of solutions of equation (1.1).

Definition 1.2. *Let $F : A \to B$ be a function. Denote by*

$$\delta(a,b) = |\{x | F(x+a) - F(x) = b\}|.$$

Let $\Delta_F = \max_{a \in A, a \neq 0} \delta(a,b)$. We say that F is Δ_F uniform.

It is easy to see that

$$|A| = \sum \delta(a,b) \leq \sum \Delta_F = \Delta_F |B| \quad \text{and thus} \quad \Delta_F \geq |B|/|A|.$$

Definition 1.3. *We call the function F perfectly nonlinear (PN) if $\Delta_F = |B|/|A|$.*

A function f is said to be Boolean if $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$. Perfect nonlinear functions in this case of Boolean functions were studied by Willi Meier and Othmar Staffelbach and in the case $\Delta_F = 2^{n-1}$.

Theorem 1.1. *Let the function $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ be perfect nonlinear. Then, for every y from the domain of F $|F^{-1}(y)| = |\{x \in \mathbb{Z}_2^n | F(x) = y\}| = b_y 2^{\frac{n}{2}-m}$, holds where b_y is an odd integer.*

As $|F^{-1}(y)|$ is a positive integer for at least one $y \in \mathbb{Z}_2^m$ it follows that PN functions from $\mathbb{Z}_2^n$ in $\mathbb{Z}_2^m$ exist only if $\frac{n}{2} - m \geq 0$, i.e. $n \geq 2m$. Although the research of these functions is related to cryptography, so $q = 2$ is mostly taken, the terms are extended to other values of q.

In the case of Abelian groups, where $|A| = |B|$, PN functions are called planar functions. As the derivative is then a bijective function, for each $a \in A, \quad a \neq 0$, each equation $F(x+a) - F(x) = b$ has exactly one solution, so especially for fixed a there is exactly one x such that $F(x+a) - F(x) = 0$. Hence $F(x+a) = F(x)$ where $x + a \neq x$. Therefore, the planar function is not bijective. However, planar functions can be used for purposes other than cryptology. Let a finite additive Abelian group $A = \{a_1, a_2, \ldots, a_n\}$ be given. The Latin square over the elements of the group can be defined by $L_{ij} = (a_i + f(a_j)), 1 \leq i, j \leq n$ where $f : A \to A$ is a bijection. A Latin square is a matrix in which the elements in each row and each column are different from each other. Kelly's

table of groups gives some of the Latin squares, but not all. If $A = \mathbb{Z}_3, \quad f(x) = 2x$ we have

$$L = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}.$$

Mutually orthogonal Latin squares L and H are Latin squares of equal dimensions and such that for $1 \leq i, j, s, l \leq n$,$(L_{ij}, H_{ij}) \neq (L_{sl}, H_{sl})$, for $(i, j) \neq (s, l)$. They are important for making schedules, designing experiments, etc. The maximal family of mutually orthogonal Latin squares is obtained for $n = p^s$ where p is a prime number and the largest number of mutually orthogonal pairs is equal to $n - 1$. If we have a planar mapping F on A, then the Latin squares defined by $L_{ij}^a = (a_i + F(a_j + a) - F(a_j))$ for all $a \in A, \quad a \neq 0$ form the maximal family of mutually orthogonal Latin squares.

Planar functions do not exist for $q = 2$, because $F(x + a) - F(x) = F((x + a) + a) - F(x + a)$. In the case of vector Boolean functions, equation (1.1), if it is consistent, has at least two solutions $(x, x + a)$. Therefore, the minimum value for differential uniformity is 2. If this minimum value is reached, the function is said to be almost perfectly nonlinear (APN).

Definition 1.4. *A function $F : A \to B$ is called APN or almost perfectly nonlinear if it is differentially $(2|B|)/(|A|)$ uniform.*

2. BENT AND ALMOST BENT FUNCTIONS

Let $q > 1$ be an integer and denote by $\omega \in \mathbb{C}$ the q-th root of unity, i.e. $\omega = e^{(2\pi i/q)}$.

Definition 2.1. *The Walsh transform of the q-ary function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ computed in $\mathbb{C}$ is defined by*

$$\hat{f}(a) = \sum_{x \in \mathbb{Z}_q^n} \omega^{f(x) - \langle a, x \rangle}$$

where $a \in \mathbb{Z}_q^n$ and for $a = (a_1, a_2, \ldots, a_n)$, $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_q^n$

$$\langle a, x \rangle = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n.$$

If $q = 2$, then $\omega = -1$. If $q = p$ is a prime number, then $\mathbb{Z}_p^n$ is a vector space over the field $\mathbb{Z}_p$ and $\langle a, x \rangle$ is a scalar product. Now let $q = p^n$ and $\mathbb{F}_q$ be a finite field. Then $\mathbb{F}_q$ is a vector space over $\mathbb{Z}_p$ with base $(\beta_1, \beta_2 \ldots, \beta_n)$. All elements from $\mathbb{F}_q$ can be uniquely represented by $x = a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n$ where the coefficients are $a_1, a_2, \ldots, a_n \in \mathbb{Z}_p$.

Then, the correspondence

$$(a_1, a_2 \ldots, a_n) \to a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n$$

is an isomorphism of the vector spaces $\mathbb{Z}_p^n$ and $\mathbb{F}_q$ over the field $\mathbb{Z}_p$. The scalar product is a linear function and can be defined in $\mathbb{F}_q$ via the absolute trace function with $\langle a, x \rangle = Tr(ax) = \sum_{i=0}^{n-1} (ax)^{p^i}$.

The values of the Walsh transformation for a fixed a, denoted by $\hat{f}(a)$, are called the Walsh coefficients of f. They are used to measure the distance from f to the function

$x \mapsto \langle a, x\rangle$. For a prime number p these are the only linear functions in the vector space $\mathbb{Z}_p^n$.

Definition 2.2. *Linearity $\mathcal{L}(f)$ of function f is defined by*

$$\mathcal{L}(f) = max_{a\in\mathbb{Z}_q^n}|\hat{f}(a)|.$$

For vector functions $F : \mathbb{Z}_q^n \to \mathbb{Z}_q^m$ linearity is defined by the linearity of non-trivial linear combinations of its coordinate functions. For a given $\lambda \in \mathbb{Z}_q^m$ the q-ary function $f_\lambda(x) = \langle \lambda, F(x)\rangle$ is called the λ-component of F.

The Walsh spectrum of F is the set of all values $\hat{f_\lambda}(a)$ for all $a \in \mathbb{Z}_q^n$ and all $\lambda \in \mathbb{Z}_q^m \setminus \{0\}$.

The linearity of the function F is defined by

$$\mathcal{L}(F) = max_{\lambda\in\mathbb{Z}_q^m\setminus\{0\}}\mathcal{L}(f_\lambda).$$

Using Parseval's theorem, we obtain that $q^{\frac{n}{2}} \leq \mathcal{L}(F)$, and for the functions $x \mapsto \langle a, \cdot\rangle$, $\mathcal{L}(F) = q^n$ holds, so we have $q^{n/2} \leq \mathcal{L}(F) \leq q^n$ for all functions F.

Definition 2.3. *We call function F for $q = 2$ bent, (and for $q > 2$ generalized bent functions) if $q^{n/2} = \mathcal{L}(F)$ holds.*

If $m = n$ bent functions do not exist. When n is odd, the lower limit for $\mathcal{L}(F)$ is $2^{(n+1)/2}$.

Definition 2.4. *For $q = 2$, the vector Boolean function for which $\mathcal{L}(F) = 2^{(n+1)/2}$ holds is called is almost-bent (AB).*

For even values of n, functions are known for which $\mathcal{L}(F) = 2^{\frac{n}{2}+1}$ is valid, but no function with minimal linearity has yet been found. For bijective functions $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ the smallest known linearity is $2^{(\lfloor n/2\rfloor+1)}$. Chabaud and Vaudenay proved a result that gives a connection between perfectly nonlinear functions and bent functions. A Boolean function is a bent function if and only if it is perfectly nonlinear. For the q-ary case, the perfectly nonlinear function is bent, and the reverse holds if q is a prime number. The same is true for near-PN and near-bent functions. Let F be a vector Boolean function. If F is almost-bent, then it is almost perfectly nonlinear. If F is almost perfectly nonlinear and the Walsh coefficients of $\langle 1, F(x)\rangle$ are divisible by 2^{m+1}, then F is almost-bent. Almost perfectly non-linear vector Boolean functions are also used in coding theory, to form linear codes with a specific weight. More details can be found in [1].

3. Equivalence of bent-functions

Due to the bijective affine transformations $G(x) = L_1(F(L_2(x))) + L_3(x)$ where $L_1(x)$ and $L_2(x)$ are bijections, the linearity of the Boolean vector functions F remains preserved and we call such functions EA-equivalent. So, we study the classes of equivalent bent functions. The concept of CCZ-equivalent functions is used in coding theory. Namely, the functions F and G are CCZ-equivalent if the corresponding codes C_F and

C_G are equivalent, where the code parity check matrix is defined by

$$H_F = \begin{pmatrix} \cdots & 1 & \cdots \\ \cdots & x & \cdots \\ \cdots & F(x) & \cdots \end{pmatrix}.$$

CCZ equivalence is very hard to establish, but it coincides with EA-equivalence for planar, Boolean functions, vector bent functions if $q = p = 2$ and vector bent functions if $p = q$ is an odd prime and $m = n$.

4. KNOWN CONSTRUCTIONS OF PN MAPPING

In this section we denote the monomial as the function $F_d : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $x \mapsto x^d$. Monomials are bijective if and only if the exponent d is relatively prime with $p^n - 1$. The mappings $w \to w^{p^n}$ are linear isomorphisms such that all monomials $F_e(x) = x^e$, when e is in the same cyclotomic class $\{p^i \cdot d | 0 \le i < n\}$ have the same differential uniformity and nonlinearity as well as the monomial $F_d(x) = x^d$ and therefore the monomial with the smallest exponent in the class is usually studied. Further, for $a \neq 0, \delta(a,b) = |\{x|F(x+a) - F(x) = b\}| = |\{x|(x=a)^d - x^d = b\}| = |\{x|(x=1)^d - x^d = \frac{b}{a^d}\}| = \delta(1, \frac{b}{a^d})$.

If $b = 0$, then $\delta(1,0) = \gcd(d, p^n - 1) - 1$, and in particular the monomial is bijective if and only if $\delta(1,0) = 0$.

There are plenty of monomials that are APN in fields of characteristic 2, and for odd characteristic the known PN monomials are x^2, x^{p^t+1} where $\frac{n}{\gcd(n,t)}$ is odd, $x^{(p^t=1)/2}$ where $p = 3$, t is odd and $\gcd(n,t) = 1$. Bent functions for infinitely many fields and are called exceptional. Many polynomials with these properties have also been found. An interesting example is the mapping $G : x \mapsto c^x$ because for each $a \neq 0$ we have the difference $G(x+a) - G(x) = c^{x+a} - c^x = (c^a - 1)G(x)$.

When observing functions from $\mathbb{Z}_2^m$ in $\mathbb{Z}_2$ strings can be divided into several parts whose sum length is m. So, for example, functions $F(X,Y) = g(X) + h(Y)$are bent on $\mathbb{Z}_2^{2m}$, if g and h are bent on $\mathbb{Z}_2^m$. The same is true for symmetric functions, but such decompositions are not interesting in practice.

One of the more significant constructions is Maiorana McFarland: Let g and π be permutations on $\mathbb{Z}_2^m$, then$f(X,Y) = \pi(X)Y + g(X)$ is bent on $\mathbb{Z}_2^{2m}$.

The other significant construction is using partial spreads. Let $\mathbb{Z}_2^{2m}$ be a vector space.

Let's define the family $\mathcal{PC}^-$: Let $H_1, H_2, ..., H_{2m-1}$ be vector spaces such that $H_i \cap H_j = 0, \quad i \neq j$. Let $H^* = \cup_{i=1}^{2m-1}(H_i \setminus \{0\})$. Then the characteristic function of H^* is bent on $\mathbb{Z}_2^{2m}$.

Now define the family $\mathcal{PC}^+$: The union of any $2m+1$ subspaces with $H_i \cap H_j = 0, \ i \neq j$ is called a cover and its characteristic function is bent on $\mathbb{Z}_2^{2m}$.

These construction can be found in [2]. There are many known bent functions and classes of planar functions, but this area continues to attract the attention of mathematicians and is intensively developed.

5. Applications

The most significant application of APN functions is in the construction of S-boxes in symmetric cryptosystems. Encryption is a mapping $S_k : \mathbb{F}_q \to \mathbb{F}_q$ where k is the key, i.e. field element on which the encryption function depends and which is secret. In general, all parts of symmetric cryptosystems are linear except for S-boxes. The good construction of S-boxes guarantees the security of the cryptosystem and the avalanche effect which means that small changes in the input data cause large changes in the ciphertext. In his hardware-oriented MISTY design, Matsui split the 16-bit state into two odd parts of different lengths so that he could use APN permutations. The designers Daemen and Rijmen of the AES algorithm, which was aimed at software implementation, could not go that far, so they settled on a suboptimal choice which is a differentially 4-uniform inverse function. It is considered that large S-boxes provide greater security against cryptographic attacks, and this area is intensively studied in the wider mathematical community, where the APN functions are of greatest importance.

References

[1] Celine Blondean, Kaisa Nyberg, *Perfect nonlinear functions and cryptography*, Finite Fields and Their Applications 32, 120-147, 2015.

[2] John F. Dillon, E.M. Wright *Elementary Hadamard difference sets*, PhD thesis, University of Maryland, 1974.

(Received: May 15, 2024)
(Revised: 11 September, 2024)

Amela Muratović-Ribić
University of Sarajevo
Faculty of science and mathematics
Department of mathematics and computer sciences
Zmaja od Bosne 33-35
71 000 Sarajevo
Bosnia and Herzegovina
e-mail: *amela@pmf.unsa.ba*