Nonlinearity of bent functions over finite fields

Vladimir RYABOV

Moscow
June 1-4, 2021
Notation and definitions

• Let $F_q$ be a finite field of $q$ elements, where $q = p^m$, $p \in P$, $m \in N^*$ and $F_q^n$ – an $n$-dimensional vector space over the field $F_q$, where $n \in N^*$.

• Denote by $P_q^n$ the set of all mappings of $F_q^n$ into $F_q$ or functions of $q$-valued logic of $n$ variables, and by $A_q^n$ its subset of affine mappings.

• Let’s assign the affine function

$$a(x) = a_0 \oplus a_1 \otimes x_1 \oplus ... \oplus a_n \otimes x_n, \quad (1)$$

where $a_0, a_1, ..., a_n \in F_q$, $\oplus$ and $\otimes$ are addition and multiplication operations in $F_q$, to the vector $\alpha = (a_0, a_1, ..., a_n) \in F_q^{n+1}$. Denote by $\rho_f^\alpha$ the Hamming distance between functions $f(x) \in P_q^n$ and $a(x) \in A_q^n$ in the space $F_q^n$.

• Define the nonlinearity of the function $f(x) \in P_q^n$ by the formula

$$N_f = \min_{\alpha \in F_q^{n+1}} \rho_f^\alpha. \quad (2)$$

• Functions with the maximum possible value of nonlinearity will be called maximally nonlinear and the class of such functions will be denoted by $MN_q^n$. 
Research of Soviet and American cryptographers on nonlinearity of Boolean functions


1960s

1976

Rothaus O.S. for even values of n described a class of Boolean functions, which he called bent functions (let’s denote it $B_2^n$), for which all Fourier coefficients in the expansions of the corresponding integer functions of the form $(-1)^{f(x)}$ are equal in absolute value. These functions have the maximum possible nonlinearity equal to $2^{n-1} - 2^{n/2} - 1$, and in the Boolean case, for even n, $B_2^n = MN_2^n$ is true, and for odd n, $B_2^n = \emptyset$ is true. (“1-plateaued” nonlinearity equal to $2^{n-1} - 2^{n-1/2}$)


1985

Kumar, P. V., Scholtz, R. A., Welch, L. R. generalized the concept of a bent function to the case of a residue ring $\mathbb{Z}_k$ ($\mathbb{Z}_k$ is a field for $k \in P$)

Ambrosimov A. S. generalized the concept of a bent function to the case of an arbitrary finite field. He gave the definition of the $q$-valued bent function (further this definition is used and the class of $q$-valued bent functions is denoted by $B_q^n$), described all the quadratic bent functions and counted their number. For $q > 2$, in the case of fields of odd characteristic, for odd values of $n$ $q$-valued bent functions also exist. The generalized Rothaus criterion was also proved, which states that a necessary and sufficient condition for a $q$-valued function to be bent is the balance of any of its nontrivial derivatives (functions for which all nontrivial derivatives are balanced are also called perfect nonlinear)


Coulter, R. S., Matthews, R. W. gave a similar bent function definition and presented their proof of the coincidence of the classes of bent functions and completely nonlinear functions in the case of a finite field

2002

Solodovnikov V. I. generalized the concept of a bent function to the case of an arbitrary finite abelian group (The definitions of Ambrosimov and also of Coulter and Matthews of the $q$-valued bent function fall under the general definition of Solodovnikov)


2004 - ...

Later, a number of papers have appeared on the topic of $q$-valued bent functions for $q > 2$. Special mention should be made of the work of Carlet C., Ding C., in which generalizations of Maiorana-McFarland's and Dillon's families of bent functions were given to the case of an arbitrary finite field. As it turned out, for $q > 2$ an arbitrary bent function is not necessarily maximally nonlinear and the question of nonlinearity remained open

Recent results

• In the works of the author


• for \( \forall f(x) \in P_q^n \), the following upper bound for nonlinearity was obtained

\[
N_f \leq (q-1)q^{n-1} - q^{n/2-1}; \quad (3)
\]

• for \( n = 1 \) it can be refined:

\[
N_f \leq q-2; \quad (4)
\]
• for \( q > 2 \) and even \( n \) it was shown that the set of quadratic bent functions splits into two classes of Extended-Affine (EA-) equivalent functions. For functions of one class, the equality

\[
N_f = (q-1)q^{n-1} - q^{n/2-1}
\]

holds, and this class consists of maximally nonlinear functions, while for functions of another class the equality

\[
N_f = (q-1)(q^{n-1} - q^{n/2-1})
\]

holds, and this class does not contain of maximally nonlinear functions;

• for odd \( p \) and \( n \) was shown that all quadratic q-valued bent functions have the same nonlinearity equal to

\[
N_f = (q-1)q^{n-1} - q^{(n-1)/2},
\]

and are maximally nonlinear in the case \( n = 1 \).

• Thus, the equality (5) is a criterion of maximum nonlinearity for even \( n \).
### Necessary condition for maximum nonlinearity

#### Theorem 1.

Let \( f(\mathbf{x}) \in MN_q^n \), where \( q > 2 \) and \( n \) is even. Then in the space \( \mathbb{F}_q^n \) there is no linear manifold of dimension greater than or equal to \( n/2 \) on which the restriction of the function \( f(\mathbf{x}) \) coincides with the restriction of some affine function.

The proof of the theorem is based on the properties of the restrictions of functions of \( q \)-valued logic on the linear manifolds of the vector space of the domain of definition, studied in the author's work “On the approximation”.

In the case of Boolean functions, Theorem 1 does not work.

Indeed, for Boolean bent functions from Maiorana-McFarland's and Dillon's families, there are always manifolds of dimension \( n/2 \) on which their restrictions coincide with affine functions.
The Mayorana-McFarland's construction for $q$-valued bent functions of $n$ variables has the following form

$$f(x) = \langle \mathbf{x}', \pi(\mathbf{x}'') \rangle \oplus g(\mathbf{x}''), \quad (8)$$

where $\mathbf{x}' = (x_1, \ldots, x_{n/2})$, $\mathbf{x}'' = (x_{n/2+1}, \ldots, x_n) \in F_{q}^{n/2}$, $\pi$ is an arbitrary substitution on the set $F_{q}^{n/2}$, $\langle \ast, \ast \rangle$ is the scalar product of vectors in the space $F_{q}^{n/2}$, and $g$ is an arbitrary function from $P_{q}^{n/2}$

**Corollary 1.** Let $q > 2$, $n$ is even and $f(\mathbf{x})$ belongs to the Mayorana-MacFarland’s family of $q$-valued bent functions of $n$ variables. Then $f(\mathbf{x}) \notin MN_{q}^{n}$. 
Results for known families of bent functions (continued)

Using the correspondence of the vector space $F_q^{n/2}$ to the field $F_{q^{n/2}}$, the Dillon's construction for $q$-valued bent functions of $n$ variables are defined as follows

$$f(x) = h(x' \otimes (x'')^{q^{n/2}-2}), \quad (9)$$

where $x', x'' \in F_{q^{n/2}}$, $\otimes$ and $\ast$ are operations of multiplication and exponentiation in the field $F_{q^{n/2}}$, respectively, and the mapping $h : F_{q^{n/2}} \rightarrow F_q$ is balanced function.

**Corollary 2.** Let $q > 2$, $n$ is even and $f(x)$ belongs to the Dillon's family of $q$-valued bent functions of $n$ variables. Then $f(x) \notin MN_q^n$. 
New construction of maximally nonlinear bent functions

Theorem 2.
Let \( q > 2 \), \( n \) is even, \( \mathbf{x}' = (x_1, x_2) \in \mathbb{F}_q^{n/2} \), \( \mathbf{x}'' = (x_3, \ldots, x_{n/2+1}) \), \( \mathbf{x}''' = (x_{n/2+2}, \ldots, x_n) \in \mathbb{F}_q^{n/2-1} \), \( \pi \) is an arbitrary substitution on the set \( \mathbb{F}_q^{n/2} \), \( \langle \ast, \ast \rangle \) is the scalar product of vectors in the space \( \mathbb{F}_q^{n/2} \), and \( g \) is an arbitrary function from \( \mathbb{P}_q^{n/2} \). Then

a) for fields of even characteristic with respect to the function
\[
f(\mathbf{x}) = x_1 \otimes x_2 \oplus x_1^2 \oplus c \otimes x_2^2 \oplus \langle \mathbf{x}'', \pi (\mathbf{x}''') \rangle \oplus g(\mathbf{x}'''),
\]
where \( c \) is a free term of an irreducible polynomial \( x^2 \oplus x \oplus c \), the statements \( f(\mathbf{x}) \in B_q^n \) and \( f(\mathbf{x}) \in MN_q^n \) are true;

b) for fields of odd characteristic with respect to the function
\[
f(\mathbf{x}) = x_1^2 \oplus d \otimes x_2^2 \oplus \langle \mathbf{x}'', \pi (\mathbf{x}''') \rangle \oplus g(\mathbf{x}'''),
\]
where \( d \) is a quadratic nonresidue, the statements \( f(\mathbf{x}) \in B_q^n \) and \( f(\mathbf{x}) \in MN_q^n \) are true.
The proof of the theorem is based

- on the properties of the restrictions of functions of $q$-valued logic on the linear manifolds, studied in the author's work “On the approximation”,

- as well as on the results obtained in another author's work “Maximally nonlinear functions” that

  - for fields of even characteristic the quadratic form
    \[ x_1 \otimes x_2 \oplus x_1^2 \oplus c \otimes x_2^2, \quad (12) \]
    where $c$ is a free term of an irreducible polynomial $x^2 \oplus x \oplus c$, is a maximally nonlinear bent function, and

  - for fields of odd characteristic the quadratic form
    \[ x_1^2 \ominus d \otimes x_2^2, \quad (13) \]
    where $d$ is a quadratic nonresidue, also is a maximally nonlinear bent function.
In similar ways, one can show that for $q > 2$ and $n$ is odd, for the function

$$f(x) = x_1^2 \oplus \langle x'', \pi (x''') \rangle \oplus g(x''')$$

(14)

the following inequality holds

$$N_f \geq (q-1)q^{n-1} - q^{(n-1)/2},$$

(15)

and for $n = 1$ this function is maximally nonlinear.

In the case of a field with an odd characteristic, $f(x)$ is a bent function, while for a field of an even characteristic, it is a balanced function and not a bent function.

The families of functions of $q$-valued logic constructed above can be extended by adding EA-equivalent functions from $P_q^n$. 
The results obtained here confirm that for $q > 2$ and even values $n$, some famous families of $q$-valued bent functions do not possess the property of maximum nonlinearity. At the same time a new family of bent functions over finite fields is constructed, which are both bent and maximally nonlinear. Moreover, the functions of this family can have an arbitrary degree of the polynomial in the range from 2 to $\max \{2; (q-1)(n/2-1)\}$.

For odd values of $n$, a family of $q$-valued functions with a sufficiently high degree of nonlinearity is indicated. In the case of fields of odd characteristic, this family belongs to the class of bent functions, and for fields of even characteristic, it belongs to the class of balanced functions.
Thank you for your attention!

E-mail: 4vryabov@gmail.com