Bent partitions

Nurdagül Anbar* and Wilfried Meidl**

*Sabancı University, MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey
**RICAM, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria

Abstract

Spread and partial spread constructions are the most powerful bent function constructions. For instance, every function from a $2m$-dimensional vector space $\mathbb{V}_{2m}^{(p)}$ over $\mathbb{F}_p$ into $\mathbb{F}_p$, for which every element of $\mathbb{F}_p$ has the same number of subspaces (0 excluded) from the spread in its preimage set, except from 0 (w.l.o.g) which has one more subspace (0 included) in its preimage, is bent. Further, from spreads one obtains not only bent functions between elementary abelian groups, but bent functions from $\mathbb{V}_{2m}^{(p)}$ to B, where B can be any abelian group of order p^k, $k \leq m$.

As recently shown (Meidl, Pirsic 2021), partitions from spreads are not the only partitions of $\mathbb{V}_{2m}^{(2)}$ with these remarkable properties. In this talk we present first such partitions (other than (partial) spreads), which we call bent partitions, for $\mathbb{V}_{2m}^{(p)}$, p odd. We investigate general properties of bent partitions, like number and cardinality of the subsets of the partition. Moreover, we show that bent functions from $\mathbb{V}_{2m}^{(p)}$ into a cyclic group $\mathbb{Z}_{p^k}$ are obtained from bent partitions.

1 Introduction

The perhaps most powerful construction of bent functions is based on spreads of $\mathbb{V}_n^{(p)}$, $n = 2m$. This ubiquitous construction does not only yield a large variety of bent functions between elementary abelian groups, but also a large variety of bent functions from $\mathbb{V}_n^{(p)}$ to B, where B can be any finite abelian group of order p^k, $k \leq m$. Until very recently, the (partial) spread construction has been the only construction which yields also bent functions from $\mathbb{V}_n^{(p)}$ into the cyclic group $\mathbb{Z}_{p^k}$, $k \geq 3$, which we will also call $\mathbb{Z}_{p^k}$-bent functions. Recall that a function $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ is bent if $|\mathcal{H}_f(c,u)| = p^{n/2}$ for all $u \in \mathbb{V}_n^{(p)}$ and nonzero $c \in \mathbb{F}_{p^k}$, where

$$\mathcal{H}_f(c,u) = \sum_{x \in \mathbb{V}_n^{(p)}} \epsilon_{p^k}^{cf(x)} \epsilon_p^{\langle u,x\rangle_n}, \quad \epsilon_{p^k} = e^{2\pi i/p^k}.$$

Furthermore, a function f which satisfies the much weaker condition that $|\mathcal{H}_f(1,u)| = p^{n/2}$ for all $u \in \mathbb{V}_n^{(p)}$, is called a generalized bent function.

In [2] a construction of $\mathbb{Z}_{2^k}$-bent functions is proposed, which is based on partitions Γ_1, Γ_2 of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, which have similar properties as a spread of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. The resulting bent functions are provably not coming from the (partial) spread construction. Now we describe the main result in [2] on bent functions obtained from these partitions.

Let m, k be integers such that k divides m and $\gcd(2^m - 1, 2^k + 1) = 1$, let $e = 2^m - 2^k - 2$ and d such that $de \equiv 1 \bmod 2^m - 1$. For an element $s \in \mathbb{F}_{2^m}$ define

$$U_s := \{(x, sx^{-e}) \ : \ x \in \mathbb{F}_{2^m}\}, \ U_s^* = U_s \setminus \{(0,0)\}, \text{ and } U = \{(0,y) \ : \ y \in \mathbb{F}_{2^m}\}.$$

Then U, U_s^*, $s \in \mathbb{F}_{2^m}$, form a partition of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Similarly, for an element $s \in \mathbb{F}_{2^m}$ we define

$$V_s := \{(x^{-d}s, x) \ : \ x \in \mathbb{F}_{2^m}\}, \ V_s^* = V_s \setminus \{(0,0)\}, \text{ and } V = \{(x,0) \ : \ x \in \mathbb{F}_{2^m}\}.$$

For the divisor k of m and an element γ of $\mathbb{F}_{2^k}$ let

$$\mathcal{A}(\gamma) = \bigcup_{\substack{s\in\mathbb{F}_{2^m}\\ \mathrm{Tr}_k^m(s)=\gamma}} U_s^* \quad \text{and} \quad \mathcal{B}(\gamma) = \bigcup_{\substack{s\in\mathbb{F}_{2^m}\\ \mathrm{Tr}_k^m(s)=\gamma}} V_s^*.$$

With these definitions we obtain two partitions of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$,

$$\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{2^k}\} \quad \text{and} \quad \Gamma_2 = \{V, \mathcal{B}(\gamma); \gamma \in \mathbb{F}_{2^k}\},$$

into $2^k + 1$ subsets, that have similar properties as spreads have. In fact, for $k = m$, both partitions reduce to the Desarguesian spread.

Theorem 1.1 *[2] Let m, k be integers such that k divides m and $\gcd(2^m - 1, 2^k + 1) = 1$, let $e = 2^m - 2^k - 2$ and d such that $de \equiv 1 \bmod 2^m - 1$.*

I. Every Boolean function of which the support is the union of 2^{k-1} of the sets $\mathcal{A}(\gamma)$ is a bent function. Likewise, their complements, i.e., the Boolean functions with U and 2^{k-1} of the sets $\mathcal{A}(\gamma)$ as their support, are bent.

II. Every Boolean function of which the support is the union of 2^{k-1} of the sets $\mathcal{B}(\gamma)$ is a bent function. Likewise the Boolean functions with V and 2^{k-1} of the sets $\mathcal{B}(\gamma)$ as their support, are bent.

The duals of the bent functions of the class in I are in the class in II (and vice versa).

As for spreads, we also obtain bent functions from $\mathbb{V}_n^{(2)}$ into various abelian groups B, in particular into cyclic groups.

Theorem 1.2 *[2] Let m, k be integers such that k divides m and $\gcd(2^m - 1, 2^k + 1) = 1$, and let $\pi(i) = \gamma_i$ be a one-to-one map from $\mathbb{Z}_{2^k}$ to $\mathbb{F}_{2^k}$. Then the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{Z}_{2^k}$ given as*

- *$f(x, y) = i$ if $(x, y) \in \mathcal{A}(\gamma_i)$ ($(x, y) \in \mathcal{B}(\gamma_i)$),*
- *$f(0, y) = 0$ w.l.o.g. ($f(x, 0) = 0$ w.l.o.g.) for all $y \in \mathbb{F}_{2^m}$ ($x \in \mathbb{F}_{2^m}$),*

is a $\mathbb{Z}_{2^k}$-bent function.

2 Bent partitions

Motivated by the above partitions as well as the partitions from spreads, and also from partial spreads, we introduce a class of partitions of an elementary abelian p-group $\mathbb{V}_n^{(p)}$, which possess similar properties.

Definition 2.1 *Let $\Omega = \{U, A_1, \ldots, A_K\}$ be a partition of $\mathbb{V}_n^{(p)}$. Suppose that every function with the following properties is bent:*

I Every $c \in \mathbb{F}_p$ has exactly K/p of the sets $A_1, \ldots, A_K$ in its preimage set,

II $f(x) = c_0$ for all $x \in U$ and some fixed $c_0 \in \mathbb{F}_p$.

Then we call Ω a bent partition of $\mathbb{V}_n^{(p)}$.

From the definition of a bent partition Ω of $\mathbb{V}_n^{(p)}$ we obtain the following theorem on the number and on the cardinalities of the sets in the partition.

Theorem 2.2 *Let $\Omega = \{U, A_1, \ldots, A_K\}$ be a bent partition of $\mathbb{V}_n^{(p)}$. Then n is an even integer, p divides K, and the following holds.*

(i)

$$|U| = p^{n/2} \quad \text{and} \quad |A_j| = \frac{p^{n/2}(p^{n/2} - 1)}{K}, 1 \le j \le K.$$

(ii) U is an affine subgroup of $\mathbb{V}_n^{(p)}$, $K \le 2p^{n/2} - p$, and $|A_j| \ge 2^{n/2-1}$ if $p = 2$ and $|A_j| \ge \frac{p^{n/2}+1}{2}$ if p is odd.

Proof: (i) We only consider the case of p odd as the argument for $p = 2$ is very similar. We can order the sets A_i so that we have

$$|A_1| \leq |A_2| \leq \cdots \leq |A_{K-1}| \leq |A_K|. \tag{1}$$

With [4, Theorem 3.2] on the value distribution of a p-ary bent function, one easily sees that n must be even, and then for a p-ary bent function f we have $b_c = |\{x \in \mathbb{V}_n^{(p)} : f(x) = c\}| = p^{n-1} \pm (p-1)p^{\frac{n}{2}-1}$ for a unique $c \in \mathbb{F}_p$, and $b_\ell = p^{n-1} \mp p^{\frac{n}{2}-1}$ for all $\ell \in \mathbb{F}_p \setminus \{c\}$. For some bent function f obtained from the bent partition Ω, we can arbitrarily choose K/p of the sets A_i as the preimage of ℓ in $\mathbb{F}_p \setminus \{c\}$. Hence we can suppose that for $\ell \in \mathbb{F}_p \setminus \{c\}$

$$b_\ell = \sum_{i=1}^{K/p} |A_i| = \sum_{i=K-\frac{K}{p}+1}^{K} |A_i|,$$

which implies by Equation (1) that $|A_1| = |A_2| = \cdots = |A_K|$. In this case, U has to lie in the preimage of c, i.e., $b_c > b_\ell$ for $\ell \neq c$. Therefore, we have $b_c = p^{n-1} + (p-1)p^{\frac{n}{2}-1}$ and $b_\ell = p^{n-1} - p^{\frac{n}{2}-1}$ for all $\ell \in \mathbb{F}_p \setminus \{c\}$. Hence, $|U| = b_c - b_\ell = p^{\frac{n}{2}}$. Consequently, $|A_i| = (p^n - p^{n/2})/K$ for all $i = 1, \ldots, K$.
(ii) By the definition of a bent partition Ω we can obtain bent functions f, g which only differ on the set U of cardinality $p^{n/2}$. Then f and g have the minimal possible distance between bent functions, and U must be an affine subspace of $\mathbb{V}_n^{(p)}$, see [5]. Exchanging two sets A_{j_1} and A_{j_2} in the preimages of c_1 and c_2 we get two bent functions f, g with distance $d(f,g) = 2|A_j| = 2\frac{p^{n/2}(p^{n/2}-1)}{K} \geq p^{n/2}$, and $K \leq 2(p^{n/2}-1)$, $|A_j| \geq p^{n/2}/2$ follows. Since p must divide K, we must have $K \leq 2p^{n/2} - p$. With this, from $|A_j| = p^{n/2}(p^{n/2}-1)/K$ we obtain $|A_j| \geq (p^{n/2}+1)/2$. □

3 Vectorial bent functions and $\mathbb{Z}_{p^k}$-bent functions from bent partitions

We first show that bent partitions induce vectorial bent functions.

Theorem 3.1 *Let $\Omega = \{U, A_1, \ldots, A_K\}$ be a bent partition of $\mathbb{V}_n^{(p)}$, and suppose that $K = p^k$. Then every function $F : \mathbb{V}_n^{(p)} \to \mathbb{V}_k^{(p)}$ such that every element $c \in \mathbb{V}_k^{(p)}$ has the elements of exactly one of the sets A_j, $1 \leq j \leq K$, in its preimage, and U is mapped to c_0, is a vectorial bent function.*

Proof: It suffices to show that for every nonzero $v \in \mathbb{V}_k^{(p)}$ the component function $F_v(x) = \langle v, F(x)\rangle_k$ is a p-ary (Boolean) bent function. For $x \in A_j$ we have $F_v(x) = \langle v, c_j\rangle_k$ if F maps A_j to c_j. Since the inner product $\langle , \rangle_k$ on $\mathbb{V}_k^{(p)}$ is balanced, every element of $\mathbb{F}_p$ has a exactly p^{k-1} of the sets A_j, $1 \leq j \leq K$, in its preimage. As F_v is also constant on U, by the definition of a bent partition, F_v is bent. □

Now we want to show that a bent function from $\mathbb{V}_n^{(p)}$ into the cyclic group $\mathbb{Z}_{p^k}$ can be obtained from a bent partition with $K = p^k$. Recall that a function $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ can be uniquely written as

$$f(x) = a_0(x) + a_1(x)p + \cdots + a_{k-1}(x)p^{k-1} \tag{2}$$

for some p-ary functions a_i, $0 \leq i \leq k-1$. The following lemma will be our essential tool to show the bentness property coming from bent partitions.

Lemma 3.2 *(i) $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ is bent if and only if $p^t f$ is generalized bent for every t, $0 \leq t \leq k-1$, see e.g. [1].*

(ii) [3] *$f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ given as in (2) is generalized bent if and only if every p-ary function of the form $a_{k-1}(x) \oplus C(x)$ is bent, where C is a p-ary function which is constant on the sets of the partition $\mathcal{P}_f = \{A(d) : 0 \le d \le p^{k-1} - 1\}$ with*

$$A(d) = \{x \in \mathbb{V}_n^{(p)} : \sum_{i=0}^{k-2} a_i(x)p^i = d\}. \tag{3}$$

Let $\Omega = \{U, A_0, \ldots, A_{p^k-1}\}$ be a bent partition of $\mathbb{V}_n^{(p)}$. By adding a constant to $f(x)$ and reordering the partition, we can without loss of generality suppose that $f(x) = j$ if $x \in A_j$ and $f(x) = 0$ if $x \in U$. With this convention we first show that f is a generalized bent function.

Proposition 3.3 *Let $\Omega = \{U, A_0, \ldots, A_{p^k-1}\}$ be a bent partition of $\mathbb{V}_n^{(p)}$. Then the function $f : \mathbb{V}_n^{(p)} \mapsto \mathbb{Z}_{p^k}$ such that $f(x) = j$ if $x \in A_j$ and $f(x) = 0$ if $x \in U$ is generalized bent.*

Proof: According to Lemma 3.2 (ii), we need to investigate two partitions, namely the ones coming from $a_{k-1}(x)$ and the ones given in Equation (3). For $j \in \{0, \ldots, p^k - 1\}$, we can write $j = d + \ell p^{k-1}$ for some $d \in \{0, \ldots, p^{k-1} - 1\}$ and $\ell \in \{0, \ldots p - 1\}$. Note that $a_{k-1}(x) = \ell$ on A_j if $j = d + \ell p^{k-1}$ for $d = 0, \ldots, p^{k-1} - 1$. Also, for $d = 1, \ldots, p^{k-1} - 1$ we have

$$A(d) = \bigcup_{\ell=0}^{p-1} A_{d+\ell p^{k-1}} \quad \text{and} \quad A(0) = U \cup \bigcup_{\ell=0}^{p-1} A_{\ell p^{k-1}}.$$

Say $C(x) = c_d$ on $A(d)$ for some $c_d \in \mathbb{F}_p$. We fix $d \in \{0, \ldots, p^{k-1} - 1\}$. Then every element of $\mathbb{F}_p$ is attained as an image of $a_{k-1}(x) \oplus C(x)$ on exactly one A_j lying in $A(d)$ while ℓ runs in $\{0, \ldots, p - 1\}$. That is, for each $d \in \{0, \ldots, p^{k-1} - 1\}$ and $b \in \mathbb{F}_p$, there exists a unique $A_j \subseteq A(d)$ such that $a_{k-1}(x) \oplus C(x) = b$ for all $x \in A_j$. Moreover, $a_{k-1}(x) \oplus C(x) = c_0$ for all $x \in U$. Hence, the inverse image of $b \in \mathbb{F}_p \setminus \{c_0\}$ consists of the union of p^{k-1} sets A_j in Ω, and the inverse image of c_0 consists of the union of p^{k-1} sets A_j in Ω and U. Since Ω is a bent partition, this implies that $a_{k-1}(x) \oplus C(x)$ is a bent function. □

Theorem 3.4 *Let $\Omega = \{U, A_0, \ldots, A_{p^k-1}\}$ be a bent partition of $\mathbb{V}_n^{(p)}$, then the functions given by $f(x) = j$ if $x \in A_j$ and $f(x) = 0$ (w.l.o.g.) if $x \in U$, is a bent function from $\mathbb{V}_n^{(p)}$ to $\mathbb{Z}_{p^k}$.*

Proof: By Lemma 3.2 (i), it is enough to show that $p^t f(x)$ is generalized bent for any $0 \le t \le k - 1$. Since the argument holds for $t = 0$ by Proposition 3.3, we consider $t \ge 1$. Let $f(x) = a_0(x) + a_1(x)p + \cdots + a_{k-1}(x)p^{k-1}$. Then

$$p^t f(x) = a_0(x)p^t + \cdots + a_{k-t-1}(x)p^{k-1} + (a_{k-t}(x) + \cdots + a_{k-1}(x)p^{t-1})p^k \tag{4}$$

In this case, we have $A(d) = \{x \in \mathbb{V}_n^{(p)} : p^t \sum_{i=0}^{k-t-2} a_i(x)p^i = d\}$. By Lemma 3.2 (ii), we need to investigate two partitions of $\mathbb{V}_n^{(p)}$, namely the ones coming from the preimage of $a_{k-t-1}(x)$ and the ones coming from $A(d)$. For $A(d)$, we consider $d \in \mathbb{Z}_{p^k}$ such that $d \equiv 0 \mod p^t$; otherwise we know that $A(d) = \emptyset$. Hence, let $d = p^t\tilde{d}$, where $\tilde{d} \in \{0, \ldots, p^{k-t-1} - 1\}$, and say $C(x) = c_{\tilde{d}}$ on $A(d)$. We will show that $a_{k-t-1}(x) \oplus C(x)$ is a bent function.
For $j \in \{0, \ldots, p^k - 1\}$, we can write $j = \tilde{d} + \ell p^{k-t-1} + s_t p^{k-t} + \cdots + s_1 p^{k-1}$ for some $\tilde{d} \in \{0, \ldots, p^{k-t-1} - 1\}$ and $s_t, \ldots, s_1 \in \{0, \ldots, p - 1\}$. Then A_j belongs to $A(p^t\tilde{d})$, i.e., $C(x) = c_{\tilde{d}}$ on A_j, and $a_{k-t-1}(x) = \ell$. For a fixed $\tilde{d}$ and $s_t, \ldots, s_1$ running over $\mathbb{F}_p$, every element of $\mathbb{F}_p$ is attained as the image of $a_{k-t-1}(x) \oplus C(x)$ on exactly p^t sets A_j as ℓ runs over $\mathbb{F}_p$. Hence, the inverse image of $b \in \mathbb{F}_p \setminus \{c_0\}$ contains $p^t \times p^{k-t-1} = p^{k-1}$ sets A_j. Moreover, $a_{k-t-1}(x) \oplus C(x) = c_0$ on U. Hence, the inverse image of $b \in \mathbb{F}_p \setminus \{c_0\}$ consists of the union of p^{k-1} sets A_j, and the inverse image of c_0 consists of the union of p^{k-1} sets A_j and U. This implies that $a_{k-1}(x) \oplus C(x)$ is a bent function, as Ω is a bent partition. □

Now we generalize the class of bent partitions given in [2] to odd characteristic. We remark that the partition for $p = 2$ has been found by using a property of Boolean bent functions that are connected with some $\mathbb{Z}_{2^k}$-bent functions, see [1, Corollary 1]. This property does in general not hold for $\mathbb{Z}_{p^k}$-bent functions, hence per se, it is not clear that such a generalization for odd p exists. The proof with character sums, which naturaly is more elaborate than for the case $p = 2$, we omit in this extended abstract.

Let m, k be integers such that k divides m and $\gcd(p^m-1, p^k+p-1) = 1$, let $e = p^m - p^k - p$ and d such that $de \equiv 1 \bmod p^m - 1$. For an element $s \in \mathbb{F}_{p^m}$ define

$$U_s := \{(x, sx^{-e}) \ : \ x \in \mathbb{F}_{p^m}\},\ U_s^* = U_s \setminus \{(0,0)\},\ \text{and}\ U = \{(0, y) \ : \ y \in \mathbb{F}_{2^m}\}.$$

Then U, U_s^*, $s \in \mathbb{F}_{p^m}$, form a partition of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. Similarly, for an element $s \in \mathbb{F}_{p^m}$ we define

$$V_s := \{(x^{-d}s, x) \ : \ x \in \mathbb{F}_{p^m}\},\ V_s^* = V_s \setminus \{(0,0)\},\ \text{and}\ V = \{(x, 0) \ : \ x \in \mathbb{F}_{p^m}\}.$$

For an element γ of $\mathbb{F}_{p^k}$ let then

$$\mathcal{A}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{p^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} U_s^* \quad \text{and} \quad \mathcal{B}(\gamma) = \bigcup_{\substack{s \in \mathbb{F}_{p^m} \\ \mathrm{Tr}_k^m(s) = \gamma}} V_s^*.$$

With these definitions we obtain two partitions of $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$,

$$\Gamma_1 = \{U, \mathcal{A}(\gamma); \gamma \in \mathbb{F}_{p^k}\} \quad \text{and} \quad \Gamma_2 = \{V, \mathcal{B}(\gamma); \gamma \in \mathbb{F}_{p^k}\},$$

into $p^k + 1$ subsets, that have similar properties as spreads have. In fact, for $k = m$, both partitions reduce to the Desarguesian spread.

Theorem 3.5 *Let m, k be integers such that k divides m and $\gcd(p^m - 1, p^k + p - 1) = 1$, let $e = p^m - p^k - p$ and d such that $de \equiv 1 \bmod p^m - 1$.*

I. Let f be a p-ary function from $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_p$, for which every $c \in \mathbb{F}_p$ has the union of exactly p^{k-1} of the sets $\mathcal{A}(\gamma)$ (respectively $\mathcal{B}(\gamma)$) in its preimage set. Further suppose that f is constant c_0 on U (respectively V) for some $c_0 \in \mathbb{F}_p$. Then f is a p-ary bent function. Conversely every p-ary bent function that is constant on the elements of Γ_1 (respectively Γ_2) is of this form.

II. Let $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{Z}_{p^k}$ such that every $c \in \mathbb{Z}_{p^k}$ has exactly one of the sets $\mathcal{A}(\gamma)$ (respectively $\mathcal{B}(\gamma)$) in its preimage set, and $F(x) = c_0$ for all $x \in U$ (respectively $x \in V$), for some $c_0 \in \mathbb{Z}_{p^k}$. Then F is a bent function.

Remark 3.6 *The bent partitions we present in this abstract can be seen as generalizations of the Desarguesian spread. We expect that there are many more classes of bent partitions. For the small value $k = 3$, some partitions are obtained from the values in Table 1 in [2].*

Acknowledgement: N.A. is supported by Tübitak Project 120F309.

References

[1] S. Hodžić, W. Meidl, E. Pasalic, Full characterization of generalized bent functions as (semi)-bent spaces, their dual, and the Gray image. IEEE Trans. Inform. Theory 64 (2018), 5432–5440. 3, 5

[2] W. Meidl, I. Pirsic, Bent and $\mathbb{Z}_{2^k}$-Bent functions from spread-like partitions, Des. Codes Cryptogr. 89 (2021), 75–89. 1, 2, 5

[3] S. Mesnager, C. Tang, Y. Qi, L. Wang, B. Wu, K. Feng, Further results on generalized bent functions and their complete characterization. IEEE Trans. Inform. Theory 64 (2018), 5441–5452. 4

[4] K. Nyberg, Construction of bent functions and difference sets, In: Advances in cryptology–EUROCRYPT '90 (Aarhus, 1990), Lecture Notes in Comput. Sci., 473, pp. 151–160, Springer, Berlin, 1991. 3

[5] V. Potapov, On minimal distance of q-ary bent functions, In: Problems of redundancy in information and control systems, pp. 115–116, IEEE (2016) 3