Generalized partially bent functions

Jiangin Zhou

(Dept. of Computer Science, Anhui University of Technology, Ma'anshan 243002, P. R. China)

(E-mail: zhou63@ahut.edu.cn)

Abstract: Based on the definition of generalized partially bent functions, using the theory of linear transformation, the relationship among generalized partially bent functions over ring Z_N , generalized bent functions over ring Z_N and affine functions is discussed. When N is a prime number, it is proved that a generalized partially bent function can be decomposed as the addition of a generalized bent function and an affine function. The result obtained here generalizes the main works concerning partially bent functions by Claud Carlet in [1].

Keywords: Bent functions; partially bent functions; generalized bent functions; generalized partially bent functions

Bent functions, a special class of Boolean functions, are of great interest in the fields of cryptography and communications due to their nonlinearity and stableness. However, bent functions are rare and they are neither balanced nor correlation-immune. So partially bent functions, a larger class of Boolean functions, presented by Claud Carlet in [1] to remedy the defects of bent functions. Now concepts of bent and partially bent functions have been extended onto ring Z_N , N is a natural number, called

generalized bent functions and generalized partially bent functions over Z_N , respectively.

Based on the definition of generalized partially bent functions, using the theory of linear transformation, the relationship among generalized partially bent functions over ring Z_N , generalized bent functions over ring Z_N and affine functions is discussed. When N is a prime number, such as N=2, it is proved that a generalized partially bent function can be decomposed as the addition of a generalized bent function and an affine function. The result obtained here generalizes the main works concerning partially bent functions by Claud Carlet in [1]. With these new results, we can easily understand and construct partially bent functions and generalized partially bent functions.

1. Preliminaries

Let Z_N , where N>1 is an integer, be a residue ring. If N is a prime number, then Z_N is a Galois field, denoted by F_N .

Let Z_N^n be the set of all vectors with n coordinates, where each coordinate takes a value from Z_N . If N is a prime number, then

 Z_N^n is a linear space of dimension n over F_N , denoted by F_N^n . Let f: $Z_N^n \to Z_N$ be a multivalued logical function.

Let $a = (a_1, \mathbf{L}, a_n) \in \mathbb{Z}_N^n$ and $x = (x_1, \mathbf{L}, x_n) \in \mathbb{Z}_N^n$, the inner product of a and x is defined as $a \cdot x = (a_1, \mathbf{L}, a_n) \in \mathbb{Z}_N^n$

 $\mathbf{a}_1\mathbf{x}_1 \oplus \mathbf{L} \oplus \mathbf{a}_n\mathbf{x}_n$.

Definition 1.1. The Chrestenson cyclic spectrum is defined as follows:

$$S_{(f)}(w) = N^{-n} \sum_{x \in \mathbb{Z}_N^n} u^{f(x)} u^{-w \bullet x}$$
, where $w \in \mathbb{Z}_N^n$, $u = \exp(2p\sqrt{-1/N})$;

The self-correlation function is defined as follows:

$$C_f(s) = \sum_{x \in \mathbb{Z}_N^n} u^{f(x+s) - f(x)}, \text{ where } s \in \mathbb{Z}_N^n, u = \exp(2p\sqrt{-1}/N).$$

We will denote by |X| the module of X, where X is real number or complex number.

Definition 1.2. The function f(x) is called generalized bent if

 $|\mathbf{S}_{(f)}(\mathbf{w})|^2 = \mathbf{N}^{-n}$ for all $\mathbf{w} \in \mathbf{Z}_N^n$;

The function f(x) is called generalized partially bent if

 $(N^{n} - N_{Cf})(N^{n} - N_{S(f)}) = N^{n}$, where $N_{Cf} = |\{s \in \mathbb{Z}_{N}^{n} | C_{f}(s) = 0\}|$ and $N_{S(f)} = |\{s \in \mathbb{Z}_{N}^{n} | S_{(f)}(s) = 0\}|$.

The following facts are well known.

Lemma 1.1. For any function
$$f(x): \mathbb{Z}_N^n \to \mathbb{Z}_N$$
, $\sum_{x \in \mathbb{Z}_N^n} |S_{(f)}(x)|^2 = 1$.

Lemma 1.2. For any function
$$f(x): \mathbb{Z}_N^n \to \mathbb{Z}_N$$
, $\mathbb{N}^{-n} \sum_{x \in \mathbb{Z}_N^n} \mathbb{C}_f(x) u^{-w \bullet x} = \mathbb{N}^n |\mathbb{S}_{(f)}(w)|^2$,

There are similar definitions and lemmas concerning bent functions and partially bent functions.

2. Main theorems

The following theorem 2.1 is needed by other theorems.

Theorem 2.1. Let $f(x): \mathbb{Z}_N^n \to \mathbb{Z}_N$ be a multivalued logical function and A be an inverse matrix over \mathbb{Z}_N and g(x)=f(xA),

PDF created with pdfFactory Pro trial version www.pdffactory.com

then $C_{g}(v) = C_{f}(vA); S_{g}(w) = S_{f}(w(A^{-1})^{t}).$

Proof: Let $e_i (1 \le i \le n)$ denote a vector of Z_N^n such that the *i*th coordinate is 1 while all other coordinates are 0.

Let
$$(\alpha_1, \alpha_2, \dots, \alpha_n)^t = A \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ \vdots \\ e_n \end{pmatrix}$$
, where a^t denotes the transpose of vector α .

Since A is an inverse matrix, $e_i (1 \le i \le n)$ can be expressed as a linear combination of (a_1, a_2, \dots, a_n) , thus (a_1, a_2, \dots, a_n) is a radix of \mathbb{Z}_N^n .

Let
$$y=(y_1, y_2, \dots, y_n)$$
 denote $y_1 \alpha_1 + y_2 \alpha_2 + \dots + y_n \alpha_n$ of \mathbb{Z}_N^n .
Note that $y_1 \alpha_1 + y_2 \alpha_2 + \dots + y_n \alpha_n = (y_1, y_2, \dots, y_n)(\alpha_1, \alpha_2, \dots, \alpha_n)^t = (y_1, y_2, \dots, y_n)A\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ \vdots \\ e_n \end{pmatrix}$

Thus
$$f(y_1 \alpha_1 + y_2 \alpha_2 + \dots + y_n \alpha_n) = f(yA) = g(y_1, y_2, \dots, y_n),$$

 $C_g(v) = \sum_{y \in \mathbb{Z}_N^n} u^{g(y+v)-g(y)} = \sum_{y \in \mathbb{Z}_N^n} u^{f(yA+vA)-f(yA)} = \sum_{w \in \mathbb{Z}_N^n} u^{f(w+vA)-f(w)} = C_f(vA),$
In fact, $v = (v_1, v_2, \dots, v_n)$ denotes $v_1 \alpha_1 + v_2 \alpha_2 + \dots + v_n \alpha_n = (v_1, v_2, \dots, v_n)A\begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ \vdots \\ e_n \end{pmatrix}$.
 $S_{(g)}(w) = N^{-n} \sum_{x \in \mathbb{Z}_N^n} u^{g(x)} u^{-xw^t} = N^{-n} \sum_{x \in \mathbb{Z}_N^n} u^{f(xA)} u^{-xw^t} = N^{-n} \sum_{y \in \mathbb{Z}_N^n} u^{f(y)} u^{-yA^{-1}w^t} = S_{(f)}(w(A^{-1})^t).$

This completes the proof. \blacksquare

We now discuss the generalized partially bent functions.

Theorem 2.2. Let $f(x):\mathbb{Z}_{N}^{n} \to \mathbb{Z}_{N}$, $\mathbb{N}_{Cf} = |\{s \in \mathbb{Z}_{N}^{n} | \mathbb{C}_{f}(s) = 0\}|, \mathbb{N}_{S(f)} = |\{s \in \mathbb{Z}_{N}^{n} | \mathbb{S}_{(f)}(s) = 0\}|$, then

(I)
$$(N^{n} - N_{cf})(N^{n} - N_{s(f)}) \ge N^{n}$$

(II) f(x) is generalized partially bent, namely $(N^n - N_{Cf})(N^n - N_{S(f)}) = N^n$, if and only if the following conditions are true:

There exists $t \in \mathbb{Z}_{N}^{n}$, such that for any $s \in \mathbb{Z}_{N}^{n}$, $\mathbb{C}_{f}(s)=0$ or $\mathbb{C}_{f}(s)=u^{-s \cdot t} \mathbb{N}^{n}$, and $|\mathbb{S}_{(f)}(w)|^{2}$ is a constant when

$$w \in \mathbb{Z}_{N}^{n}$$
 and $S_{(f)}(w) \neq 0$.

Proof:

(a). Since
$$|C_{f}(s)| \le N^{n}$$
, hence,
 $N^{n} - N_{Cf} = |\{s \in Z_{N}^{n} | C_{f}(s) \ne 0\}| \ge \sum_{s \in Z_{N}^{n}} |C_{f}(s)| / N^{n} \ge |\sum_{s \in Z_{N}^{n}} C_{f}(s)| / N^{n}$
 $= |\sum_{s \in Z_{N}^{n}} \sum_{x \in Z_{N}^{n}} u^{f(x+s)-f(x)}| / N^{n} = |\sum_{x \in Z_{N}^{n}} u^{-f(x)} \sum_{s \in Z_{N}^{n}} u^{f(x+s)}| / N^{n}$

PDF created with pdfFactory Pro trial version www.pdffactory.com

$$\begin{split} &= |\mathbf{S}_{(f)}(0)|^{\bullet}|\sum_{x\in Z_{N}^{n}} u^{-f(x)}|= |\mathbf{S}_{(f)}(0)|^{\bullet}|\sum_{x\in Z_{N}^{n}} u^{f(x)}|= \mathbf{N}^{n} |\mathbf{S}_{(f)}(0)|^{2} .\\ &\text{Let } \mathbf{f}_{1}(\mathbf{x}) = \mathbf{f}(\mathbf{x}) + \mathbf{t}^{\bullet}\mathbf{x}, \text{ then,} \\ &\mathbf{C}_{f_{1}}(\mathbf{s}) = \sum_{x\in Z_{N}^{n}} u^{f(x+s)-f(x)} u^{st} = u^{st} \mathbf{C}_{f}(\mathbf{s}), \\ &\mathbf{S}_{(f_{1})}(\mathbf{s}) = \mathbf{N}^{-n} \sum_{x\in Z_{N}^{n}} u^{f(x)} u^{t\bullet x-s\bullet x} = \mathbf{S}_{(f)}(\mathbf{s}-t). \\ &\text{Thus, for any } \mathbf{t} \in \mathbf{Z}_{N}^{n}, \mathbf{N}^{n} - \mathbf{N}_{Cf} = \mathbf{N}^{n} - \mathbf{N}_{Cf_{1}} \geq \mathbf{N}^{n} |\mathbf{S}_{(f_{1})}(0)|^{2} = \mathbf{N}^{n} |\mathbf{S}_{(f)}(-t)|^{2} = \mathbf{N}^{n} |\mathbf{S}_{(f)}(t)|^{2} \\ &\text{Therefore, } \mathbf{N}^{n} - \mathbf{N}_{Cf} \geq \mathbf{N}^{n} \max\{|\mathbf{S}_{(f)}(t)|^{2} | \mathbf{t} \in \mathbf{Z}_{N}^{n}\} \\ &\text{Since } \mathbf{N}^{n} - \mathbf{N}_{Cf} \geq \sum_{t\in Z_{N}^{n}} |\mathbf{S}_{(f)}(t)|^{2} / \max\{|\mathbf{S}_{(f)}(t)|^{2} | \mathbf{t} \in \mathbf{Z}_{N}^{n}\} = 1 / \max\{|\mathbf{S}_{(f)}(t)|^{2} | \mathbf{t} \in \mathbf{Z}_{N}^{n}\} \\ &\text{Then we have } (\mathbf{N}^{n} - \mathbf{N}_{Cf})(\mathbf{N}^{n} - \mathbf{N}_{S(f)}) \geq \mathbf{N}^{n}, \text{ we have completed the proof of part one.} \\ &(\mathbf{b}). \text{ If } (\mathbf{N}^{n} - \mathbf{N}_{Cf})(\mathbf{N}^{n} - \mathbf{N}_{S(f)}) = \mathbf{N}^{n}, \text{ then} \\ &\mathbf{N}^{n} - \mathbf{N}_{Cf} = \mathbf{N}^{n} \max\{|\mathbf{S}_{(f)}(t)|^{2} | \mathbf{t} \in \mathbf{Z}_{N}^{n}\} \text{ and } \mathbf{N}^{n} - \mathbf{N}_{S(f)} = 1 / \max\{|\mathbf{S}_{(f)}(t)|^{2} | \mathbf{t} \in \mathbf{Z}_{N}^{n}\} \\ &\text{ Suppose } \mathbf{t} \in \mathbb{Z}_{N}^{n}, \text{ and } |\mathbf{S}_{(f)}(t)|^{2} = \max\{|\mathbf{S}_{(f)}(u)|^{2} | u\in \mathbb{Z}_{N}^{n}\}, \text{ let } \mathbf{f}_{1}(\mathbf{x}) = \mathbf{f}(\mathbf{x}+\mathbf{t}, \text{ then} \\ &\sum_{s\in \mathbb{Z}_{N}^{n}} C_{f_{1}}(s) = \mathbf{N}^{2n} |\mathbf{S}_{(f_{1})}(0)|^{2} = \mathbf{N}^{2n} |\mathbf{S}_{(f)}(t)|^{2} = \mathbf{N}^{n} (\mathbf{N}^{n} - \mathbf{N}_{Cf}) = \mathbf{N}^{n} (\mathbf{N}^{n} - \mathbf{N}_{Cf_{1}}) = \sum_{s\in \mathcal{C}_{f_{1}}(s)\neq 0} \mathbf{N}^{n}, \text{ hence } \mathbf{C}_{f_{1}}(s) = 0 \text{ or } \mathbf{N}^{n}, \text{ namely } \mathbf{C}_{f}(s) = 0 \text{ or } \mathbf{C}_{f}(s) = \mathbf{U}^{-st} \mathbf{N}^{n}; \\ &\text{ since } |\mathbf{C}_{f_{1}}(s)| \leq \mathbf{N}^{n}, \text{ hence } \mathbf{C}_{f_{1}}(s) = 0 \text{ or } \mathbf{N}^{n}, \text{ namely } \mathbf{C}_{f}(s) = 0 \text{ or } \mathbf{C}_{f}(s) = \mathbf{U}^{-st} \mathbf{N}^{n}; \\ &\text{ since } |\mathbf{C}_{f_{1}}(s)| \leq \mathbf{N}^{n}, \text{ hence } \mathbf{C}_{f_{1}}(s) = 0 \text{ or } \mathbf{N}^{n}, \text{ namely } \mathbf{C}_{f}(s) = 0 \text{ or } \mathbf{C}_{f}(s) = \mathbf{U}^{-st} \mathbf{N}^{n}; \\ &\text{ sin$$

Consider Nⁿ - N_{S(f)} = $|\{s \in \mathbb{Z}_N^n | S_{(f)}(s) \neq 0\}| = \sum_{t \in \mathbb{Z}_N^n} |S_{(f)}(t)|^2 / \max\{|S_{(f)}(t)|^2 | t \in \mathbb{F}_N^n\}$, we know that $|S_{(f)}(w)|^2$ is a

constant when $w \in \mathbb{Z}_N^n$ and $\mathbb{S}_{(f)}(w) \neq 0$.

This completes the necessity proof of part two.

(c). Suppose that there exists $t \in \mathbb{Z}_N^n$, such that for any $s \in \mathbb{Z}_N^n$, $\mathbb{C}_f(s)=0$ or $\mathbb{C}_f(s)=u^{-st}\mathbb{N}^n$, and $|S_{(f)}(w)|^2$ is a constant when $w \in \mathbb{Z}_N^n$ and $S_{(f)}(w) \neq 0$.

Let $E = \{s \in Z_N^n \mid C_f(s) = u^{-s \cdot t} N^n\}$, $f_1(x) = f(x) + t \cdot x$, then $C_{f_1}(s) = u^{-s \cdot t} C_f(s) = 0$ or N^n , hence $E = \{s \in Z_N^n \mid C_{f_1}(s) = N^n\}$. Let $E^{\perp} = \{x \in Z_N^n \mid \text{ for any } y \in E, y \cdot x = 0\}$, then for any $v \in E^{\perp}$, by Lemma 1.2, we have

$$|\mathbf{S}_{(f_1)}(\mathbf{v})|^2 = \frac{1}{N^{2n}} \sum_{\mathbf{w} \in Z_N^n} \mathbf{C}_{f_1}(\mathbf{w}) \mathbf{u}^{-\mathbf{w} \cdot \mathbf{v}} = \frac{1}{N^n} \sum_{\mathbf{w} \in E} \mathbf{u}^{-\mathbf{w} \cdot \mathbf{v}} = \frac{1}{N^n} |\mathbf{E}|.$$

As $f_1(x) = f(x)+t \cdot x$, so $S_{(f_1)}(s) = S_{(f)}(s-t)$; consider $|S_{(f)}(w)|^2$ is a constant when $w \in \mathbb{Z}_N^n$ and $S_{(f)}(w) \neq 0$, hence $|S_{(f_1)}(w)|^2$ is a constant when $w \in \mathbb{Z}_N^n$ and $S_{(f_1)}(w) \neq 0$.

When $v \notin E^{\perp}$, the real part of $\sum_{w \in E} u^{-w \cdot v} < |E|$,

Therefore
$$|\mathbf{S}_{(f_1)}(\mathbf{v})|^2 = \frac{1}{N^n} \sum_{w \in E} u^{-w \cdot v} \neq \frac{1}{N^n} |\mathbf{E}|$$
, so $|\mathbf{S}_{(f_1)}(\mathbf{v})|^2 = 0$.

By Lemma 1.1, $\sum_{w \in Z_N^n} |S_{(f_1)}(w)|^2 = 1$, so $|E^{\perp}| \cdot \frac{1}{N^n} |E| = 1$, we have $|E^{\perp}| = \frac{N^n}{|E|}$.

Thus $(N^n - N_{Cf}) = |E|, (N^n - N_{S(f)}) = \frac{N^n}{|E|}$, namely $(N^n - N_{Cf})(N^n - N_{S(f)}) = N^n$, f(x) is generalized partially bent.

This completes the sufficiency proof of part two. \blacksquare

Theorem 2.3. Let $f(w): \mathbb{Z}_N^n \to \mathbb{Z}_N$ be generalized partially bent, then there exist a subgroup E in the additive group \mathbb{Z}_N^n , such that, there exists $t \in \mathbb{Z}_N^n$ and for any $x \in E$, $y \in \mathbb{Z}_N^n \setminus E = \{x | x \in \mathbb{Z}_N^n \text{ but } x \notin E\}$, satisfying $f(x+y) = f(y) - t \cdot x$.

Proof: Since f(x) is generalized partially bent, let $E = \{s \in Z_N^n | C_f(s) = u^{-s \cdot t} N^n\}$, here $t \in Z_N^n$ and the definition of t is from theorem 2.2; let $f_1(x) = f(x) + t \cdot x$, then $C_{f_1}(s) = u^{s \cdot t} C_f(s)$, $E = \{s \in Z_N^n | C_{f_1}(s) = N^n\}$.

Since $C_{f_1}(s) = \sum_{x \in \mathbb{Z}_N^n} u^{f_1(x+s) - f_1(x)}$, hence $\alpha \in E$ if and only if that

 $\text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \boldsymbol{\alpha} \) - \ \mathbf{f}_1(\mathbf{x}) = 0, \ \text{namely } \mathbf{f}(\mathbf{x} + \boldsymbol{\alpha} \) + \mathbf{t}^{\bullet}(\mathbf{x} + \boldsymbol{\alpha} \) - \ \mathbf{f}(\mathbf{x}) \ - \mathbf{t}^{\bullet} \mathbf{x} = 0, \\ \text{so } \mathbf{f}(\mathbf{x} + \boldsymbol{\alpha} \) + \mathbf{t}^{\bullet} \ \boldsymbol{\alpha} = \mathbf{f}(\mathbf{x}), \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \boldsymbol{\alpha} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \boldsymbol{\alpha} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \boldsymbol{\alpha} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \boldsymbol{\alpha} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \boldsymbol{\alpha} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \boldsymbol{\alpha} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \boldsymbol{\alpha} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \boldsymbol{\alpha} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \boldsymbol{\alpha} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \mathbf{x} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \mathbf{x} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \mathbf{x} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \mathbf{x} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \mathbf{x} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \mathbf{x} \) - \mathbf{f}_1(\mathbf{x}) = 0, \\ \text{for any } \mathbf{x} \in \operatorname{Z}_N^n, \ \mathbf{f}_1(\mathbf{x} + \mathbf{x} \) - \mathbf{f}_1(\mathbf{$

Suppose $\alpha, \beta \in E$, then for any $x \in \mathbb{Z}_N^n$, $f(x + \alpha + \beta) + t \cdot (\alpha + \beta) = f(x + \alpha + \beta) + t \cdot \beta + t \cdot \alpha = f(x + \alpha) + t \cdot \alpha = f(x)$, thus $\alpha + \beta \in E$,

For any $k \in \mathbb{Z}_N$, it is easy to show that $k \in \mathbb{Z}$. Since $(N-1) \in \mathbb{Z}$ and $\alpha + (N-1) = 0 \in \mathbb{Z}$, so the inverse element of α still belongs to E.

Therefore, E is a subgroup of the additive group Z_N^n . It is obvious that for any $x \in E$, $y \in Z_N^n \setminus E$, satisfying $f(x+y)=f(y)-t \cdot x$. This completes the proof.

Lemma 2.1. Let $m_i = \min\{\alpha_i > 0 | (\alpha_1, \dots, \alpha_i, \dots, \alpha_n) \in E\}$, $1 \le i \le n$, the definition of E is from theorem 2.3, if m_i is not defined then let $m_i = 0$. Our conclusion is that if m_i is neither 0 nor 1, then m_i must be a factor of N but m_i is neither N nor 1.

Proof: Suppose that m_i is neither 0 nor 1, let $q=(m_i, N)$, then q>0 and there exists an integer r and an integer s, such that $q=rm_i+sN$, namely $q=rm_i \pmod{N}$,

From the definition of m_i , we have $q=m_i$, thus m_i is a factor of N but m_i is neither N nor 1.

This completes the proof. ■

For the convenience of discussions, we give a new definition.

Definition 2.1. Let $f(w): \mathbb{Z}_N^n \to \mathbb{Z}_N$ be generalized partially bent, $\mathbb{E} = \{s \in \mathbb{Z}_N^n | \mathbb{C}_f(s) = u^{-s \cdot t} \mathbb{N}^n\}, t \in \mathbb{Z}_N^n, m_i = \min\{\alpha_i > 0 | (\alpha_1, \dots, \alpha_i, \dots, \alpha_n) \in \mathbb{E}\}, 1 \le i \le n$, if m_i is not defined then let $m_i = 0$. If $m_i \ne 1$ for any i, $1 \le i \le n$, then we call f(w) as pure generalized partially bent.

If N is a prime number, as N has only factor 1 and N, then if f(w) is pure generalized partially bent, namely $m_i = 0$ for any i, $1 \le i \le n$, we have $E = \{0\}$, thus f(w) must be generalized bent.

The following theorem 2.4 is our main result.

Theorem 2.4. $f(x): \mathbb{Z}_N^n \to \mathbb{Z}_N$ be generalized partially bent, but not pure generalized partially bent, if and only if f(x) is equivalent to the addition of pure generalized partially bent $g(y): \mathbb{Z}_N^{n-m} \to \mathbb{Z}_N$ and affine function $-t_1 \cdot \alpha : \mathbb{Z}_N^m \to \mathbb{Z}_N$, here m is a positive integer, and f(x) is equivalent to h(x) means that there exists an inverse matrix A over \mathbb{Z}_N , such that h(x)=f(xA).

Proof: Let $f(w): \mathbb{Z}_N^n \to \mathbb{Z}_N$ be generalized partially bent, $\mathbb{E}_f = \{s \in \mathbb{Z}_N^n | \mathbb{C}_f(s) = u^{-s \cdot t} \mathbb{N}^n\}$, $t \in \mathbb{Z}_N^n$ and the definition of t is from theorem 2.2. If f(x) is not pure generalized partially bent, then there exists $m_i = 1$ and the definition of m_i is from theorem 2.3. That is to say, there exist $(\alpha_1, \dots, \alpha_i, \dots, \alpha_n) \in \mathbb{E}_f$, $\alpha_i = 1$.

$$\operatorname{Let} A_{1} = \begin{pmatrix} 1 & 0 & \mathbf{L} & 0 \\ 0 & 1 & \mathbf{L} & 0 \\ \mathbf{L} & \mathbf{L} & \mathbf{L} \\ a_{1} & a_{2} & \mathbf{L} & a_{i} \mathbf{L} & a_{n} \\ \mathbf{L} & \mathbf{L} & \mathbf{L} \\ 0 & 0 & \mathbf{L} & 1 \end{pmatrix}, \text{ then } A_{1}^{-1} = \begin{pmatrix} 1 & 0 & \mathbf{L} & 0 \\ 0 & 1 & \mathbf{L} & 0 \\ \mathbf{L} & \mathbf{L} & \mathbf{L} \\ -a_{1} & -a_{2} & \mathbf{L} & a_{i} \mathbf{L} & -a_{n} \\ \mathbf{L} & \mathbf{L} & \mathbf{L} \\ 0 & 0 & \mathbf{L} & 1 \end{pmatrix}, \text{ where } \alpha_{i} = 1.$$

where A₂ is obtained by move the ith row of a unit matrix to the top row, then $A_2^{-1} = A_2^{t}$.

Let A=A₂A₁, (
$$\beta_1, \beta_2, \dots, \beta_n$$
)^t=A $\begin{pmatrix} e_1 \\ e_2 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ e_n \end{pmatrix}$

where $e_i (1 \le i \le n)$ denotes a vector of \mathbb{Z}_N^n such that the *i*th coordinate is 1 while all other coordinates are 0.

Since A is an inverse matrix, $e_i (1 \le i \le n)$ can be expressed as a linear combination of $(\beta_1, \beta_2, \dots, \beta_n)$, thus $(\beta_1, \beta_2, \dots, \beta_n)$, thus $(\beta_1, \beta_2, \dots, \beta_n)$ is a radix of \mathbb{Z}_N^n , where $\beta_1 = \alpha_1 e_1 + \dots + \alpha_i e_i + \dots + \alpha_n e_n$, $\beta_2 = e_1, \dots, \beta_i = e_{i-1}, \beta_{i+1} = e_{i+1}, \dots, \beta_n = e_n$.

Let g(y)=f(yA), by theorem 2.1, we know that $|S_{(f)}(w)|^2$ is a constant when $w \in \mathbb{Z}_N^n$ and $S_{(f)}(w) \neq 0$; $C_g(s)=0$ or $C_g(s)=C_f(sA)=u^{-sAt^t}N^n=u^{-s(tA^t)^t}N^n$. By theorem 2.2, g(y) is till generalized partially bent.

Let
$$t'=tA^t$$
, $g_1(x) = g(x)+t' \cdot x$, then $C_{g_1}(s) = u^{s \cdot t'}C_g(s) = u^{s \cdot At'}C_g(s) = N^n$, here $s \cdot t = s \cdot t^t$.

Let $\operatorname{E}_{g_1} = \{ s \in \operatorname{Z}_N^n | \operatorname{C}_{g_1}(s) = \operatorname{N}^n \}$ and Z_N^1 denote the generated subgroup by β_1 , since $(\alpha_1, \dots, \alpha_i, \dots, \alpha_n) \in \operatorname{E}_f$ and $\beta_1 = \alpha_1 e_1 + \dots + \alpha_i e_i + \dots + \alpha_n e_n$, hence $\beta_1 \subset \operatorname{E}_{g_1}$, it follows that $\operatorname{Z}_N^1 \subset \operatorname{E}_{g_1}$.

Let $(Z_N^1)^{\perp} = \{ x \in Z_N^n | \text{for any } y \in Z_N^1, y \cdot x = 0 \}$, then $(Z_N^1)^{\perp} = Z_N^{n-1}$, it is obvious that $Z_N^n = Z_N^1 \oplus Z_N^{n-1}$, where \oplus denotes the inner direct product of two subgroups.

For any $\alpha \in \mathbb{Z}_N^1$ and $y \in \mathbb{Z}_N^{n-1}$, $g_1(y+\alpha) - g_1(y) = 0$, namely $g(y+\alpha) + t' \cdot (y+\alpha) - g(y) - t' \cdot x = 0$, thus $g(y+\alpha) + t' \cdot \alpha = g(y)$. We know that there exist $t_1 \in \mathbb{Z}_N^1$ and $t_2 \in \mathbb{Z}_N^{n-1}$, such that $t' = t_1 + t_2$, therefore, for any $\alpha \in \mathbb{Z}_N^1$ and $y \in \mathbb{Z}_N^{n-1}$, $g(y) = g(y+\alpha) + t' \cdot \alpha = g(y+\alpha) + (t_1+t_2) \cdot \alpha = g(y+\alpha) + t_1 \cdot \alpha$.

We have $g(y+\alpha) = g(y) - t_1 \cdot \alpha$, and $g(y+\alpha)$ is an affine function restricted within Z_N^1 .

Furthermore, we now prove $g(y+\alpha)$ is generalized partially bent restricted within Z_N^{n-1} .

Take $v \in \mathbb{Z}_N^{n-1}$, for any $w \in \mathbb{Z}_N^n$, there exit $x \in \mathbb{Z}_N^1$ and $y \in \mathbb{Z}_N^{n-1}$, such that w=x+y, hence $g(w+v)-g(w)=g(x+y+v)-g(x+y)=g(y+v)-t_1 \cdot x=g(y+v)-g(y)$, thus,

$$C_{g}(\mathbf{v}) = \sum_{w \in Z_{N}^{n}} \mathbf{u}^{g(w+v)-g(w)} = \sum_{x \in Z_{N}^{1}} \sum_{y \in Z_{N}^{n-1}} \mathbf{u}^{g(y+v)-g(y)} = \mathbf{N} \sum_{y \in Z_{N}^{n-1}} \mathbf{u}^{g(y+v)-g(y)},$$

$$\therefore \sum_{y \in Z_{N}^{n-1}} \mathbf{u}^{g(y+v)-g(y)} = 0 \text{ or } \sum_{y \in Z_{N}^{n-1}} \mathbf{u}^{g(y+v)-g(y)} = C_{g}(\mathbf{v})/\mathbf{N} = \mathbf{u}^{-v\cdot t} \mathbf{N}^{n-1} = \mathbf{u}^{-v\cdot t_{2}} \mathbf{N}^{n-1}, t_{2} \in Z_{N}^{n-1};$$

We know that, for any $v, w \in \mathbb{Z}_N^n$, there exit $v_1, x \in \mathbb{Z}_N^1$ and $v_2, y \in \mathbb{Z}_N^{n-1}$, such that $v = v_1 + v_2$, w = x + y, $g(w) - w \cdot v = g(v) - t_1 \cdot v_2(x+v_1) \cdot (v_1 + v_2) = g(v) - v \cdot v_2 - (t_1 + v_2) \cdot x$ thus,

$$S_{(g)}(v) = N^{-n} \sum_{w \in \mathbb{Z}_N^n} u^{g(w) - w \cdot v} = \sum_{x \in \mathbb{Z}_N^1} \sum_{y \in \mathbb{Z}_N^{n-1}} u^{g(y) - y \cdot v_2 - (t_1 + v_1) \cdot x} = N^{-1} \sum_{x \in \mathbb{Z}_N^1} u^{-(t_1 + v_1) \cdot x} N^{-n+1} \sum_{y \in \mathbb{Z}_N^{n-1}} u^{g(y) - y \cdot v_2} = S_{(g)}(v_2) \text{ restricted within } \mathbb{Z}_N^{n-1}.$$

Since $|S_{(g)}(v)|^2$ is a constant when $v \in \mathbb{Z}_N^n$ and $S_{(g)}(v) \neq 0$, $\therefore |S_{(g)}(v_2)|^2$ restricted within \mathbb{Z}_N^{n-1} is a constant when $v_2 \in \mathbb{Z}_N^{n-1}$ and $S_{(g)}(v_2) \neq 0$

From theorem 2.2, we know that g(y) is generalized partially bent restricted within Z_N^{n-1} .

Therefore, the equality $g(y+\alpha) = g(y)-t_1 \cdot \alpha$ means that g is the addition of the generalized partially bent function restricted within Z_N^{n-1} and the affine function restricted within Z_N^1 .

If g restricted within Z_N^{n-1} is not pure generalized partially bent, then repeat the process above we can obtain another unitary affine function.

Therefore, we can conclude that after m decompositions, where m is a positive integer, f(x) is equivalent to the addition of

the generalized partially bent function $g(y): Z_N^{n-m} \to Z_N$ and the affine function $-t_1 \cdot \alpha : Z_N^m \to Z_N$.

The sufficiency of the theorem is obvious. This completes the proof. ■

If N is a prime number, then F_N is a Galois field, and F_N^n is a linear space of dimension n over F_N . Since N has only factor 1 and N, from theorem 2.4, we have the following theorem.

Theorem 2.5. Let N be a prime number, and $f(x): F_N^n \to F_N$ be generalized partially bent, but not generalized bent, if and only if f(x) is equivalent to the addition of generalized bent g(y): $F_N^{n-m} \to F_N$ and affine function $-t_1 \cdot \alpha : F_N^m \to F_N$, here m is a positive integer, and f(x) is equivalent to h(x) means that there exists an inverse matrix A over F_N , such that h(x)=f(xA).

The following is an example of pure generalized partially bent functions.

Example 2.1.Let
$$I_{\{1,3\}}(x) = \begin{cases} 1, x = 1, 3 \\ 0, x = 0, 2 \end{cases}$$
, and $f(x,y) = I_{\{1,3\}}(x) + I_{\{1,3\}}(y) + x + y. \end{cases}$

We first show that f(x,y) is a generalized partially bent function.

Here N=4, u= exp(2
$$p \sqrt{-1}/N$$
)= exp($p \sqrt{-1}/2$)=cos $p /2$ +isin $p /2$ =i.
Obviously, C_f (0,0)= $\sum_{(x,y)\in Z_4^2}$ u^{f(x+0,y+0)-f(x,y)} =16.
C_f (0,2) = $\sum_{(x,y)\in Z_4^2}$ u^{f(x+0,y+2)-f(x,y)}
=i $f^{(0,2)-f(0,0)}$ + i $f^{(0,3)-f(0,1)}$ + i $f^{(0,0)-f(0,2)}$ + i $f^{(0,1)-f(0,3)}$
+ i $f^{(1,2)-f(1,0)}$ + i $f^{(1,3)-f(1,1)}$ + i $f^{(1,0)-f(1,2)}$ + i $f^{(1,1)-f(1,3)}$
+ i $f^{(2,2)-f(2,0)}$ + i $f^{(2,3)-f(2,1)}$ + i $f^{(2,0)-f(2,2)}$ + i $f^{(2,1)-f(2,3)}$
+ i $f^{(3,2)-f(3,0)}$ + i $f^{(3,3)-f(3,1)}$ + i $f^{(3,0)-f(3,2)}$ + i $f^{(3,1)-f(3,3)}$
=i $^{2-0}$ + i $^{0-2}$ + i $^{2-0}$ + i $^{0-2}$
+i $^{0-2}$ + i $^{2-0}$ + i $^{0-2}$
+i $^{0-2}$ + i $^{2-0}$ + i $^{0-2}$
+i $^{0-2}$ + i $^{0-2}$ + i $^{2-0}$ =-16,
Similarly, C_f (2,0)=-16, C_f (2,2)=16.

Thus $C_f(s)=u^{-s \cdot (1,1)} 4^2$, $s \in \{0,2\} \times \{0,2\}$. It is easy to verify that $C_f(s)=0$ for $s \notin \{0,2\} \times \{0,2\}$.

$$\begin{split} \mathbf{S}_{(f)}\left(1,1\right) &= \frac{1}{16} \sum_{(x,y) \in \mathbb{Z}_{4}^{2}} \mathbf{u}^{f(x,y)} \mathbf{u}^{-x-y} \\ &= \frac{1}{16} \left(\mathbf{i}^{f(0,0)-0} + \mathbf{i}^{f(0,1)-1} + \mathbf{i}^{f(0,2)-2} + \mathbf{i}^{f(0,3)-3} + \mathbf{i}^{f(1,0)-1} + \mathbf{i}^{f(1,1)-2} + \mathbf{i}^{f(1,2)-3} + \mathbf{i}^{f(1,3)-0} + \mathbf{i}^{f(2,0)-2} + \mathbf{i}^{f(2,1)-3} + \mathbf{i}^{f(2,2)-0} + \mathbf{i}^{f(2,3)-1} + \mathbf{i}^{f(3,0)-3} + \mathbf{i}^{f(3,1)-0} + \mathbf{i}^{f(3,2)-1} + \mathbf{i}^{f(3,3)-2} \right) \\ &= \frac{1}{16} \left(\mathbf{i}^{0-0} + \mathbf{i}^{2-1} + \mathbf{i}^{2-2} + \mathbf{i}^{0-3} + \mathbf{i}^{2-0} + \mathbf{i}^{2-1} + \mathbf{i}^{0-3} + \mathbf{i}^{2-0} + \mathbf{i}^{2-1} + \mathbf{i}^{0-2} + \mathbf{i}^{2-1} + \mathbf{i}^{0-2} \right) \\ &+ \mathbf{i}^{2-2} + \mathbf{i}^{0-3} + \mathbf{i}^{2-0} + \mathbf{i}^{2-1} + \mathbf{i}^{0-2} \right) = \frac{1}{2} \mathbf{i} \end{split}$$

Similarly, $S_{(f)}(1,3) = S_{(f)}(3,1) = S_{(f)}(3,3) = \frac{1}{2}i$.

Since
$$\sum_{(x,y)\in Z_4^2} |S_{(f)}(x,y)|^2 = 1$$
, thus $S_{(f)}(v) = 0$ for $v \notin \{1,3\} \times \{1,3\}$.

By definition 1.2, f(x,y) is a generalized partially bent function.

Due to $E=\{s \in \mathbb{Z}_4^2 \mid C_f(s)=u^{-st}4^2\}=\{0,2\}\times\{0,2\}$, and $m_1=m_2=2$, thus f(x,y) is a pure generalized partially bent function.

Obviously, $Z_4^2 = (\{0,2\} \times \{0,2\}) \oplus (\{0,1\} \times \{0,1\})$, for example, (2,3) = (2,2) + (0,1); (3,3) = (2,2) + (1,1).

PDF created with pdfFactory Pro trial version www.pdffactory.com

By theorem 2.3, for any $w \in \mathbb{Z}_4^2$, there exist $w_1 \in \{0,2\} \times \{0,2\}$ and $w_2 \in \{0,1\} \times \{0,1\}$, such that $w = w_1 + w_2$ and $f(w_1 + w_2) = f(w_2) - (1,1) \cdot w_1$.

3. Remarks

Since 2 is a prime number, F_2 is a Galois field, thus the results obtained here can be applied to partially bent functions, we have that a partially bent function can be decomposed as the addition of a bent function and an affine function. So the result has generalized the main works concerning partially bent functions by Claud Carlet.

Based on the definition of generalized partially bent functions, using the theory of linear transformation, the relationship between generalized partially bent functions over ring Z_N and generalized bent functions over ring Z_N is discussed. As there have been many results about bent functions and generalized bent functions, and the structure of affine functions is very simple, so it is easy to analyse or construct partially bent functions and generalized partially bent functions with the results obtained here.

A method to decompose the non-pure generalized partially bent function is introduced. However, how to decompose the pure generalized partially bent function, or how to analyse the structure of pure generalized partially bent function, is still an open problem.

References

- Claud Carlet, Partially Bent Functions[A], In:Brikell,E.,ed., Advance in Cryptology-Crypto'92[C], Springer-Verlag, Berlin, 1992, 280~291.
- [2] P.V. Kumar, R.A. Scholtz, L.R. Welch, Generalized bent functions and their properties, J. Combin. Theory A 40 (1985) 90-107.
- [3] O.S. Rothaus, On "bent" functions, J. Combin. Theory Ser. A 20(1976) 300–305.