SHANGHAI JIAO TONG UNIVERSITY
SCHOOL OF ELECTRONIC INFORMATION AND ELECTRICAL ENGINEERING

Galois Ring, Kerdock codes and generalized Boolean function

Zhaole Li

Workshop of Galois Ring, 2021

Definition (Galois ring)

The **Galois ring** $GR(p^k, n)$ can be analogue to the finite field $\mathbb{F}_{p^n}$, constructed by $\frac{\mathbb{Z}_{p^k}[x]}{\langle f(x)\rangle} \cong \mathbb{Z}_{p^k}[\xi]$ where $f(x)$ is a basic[1] irreducible polynomial of degree n over $\mathbb{Z}_{p^k}$(a Hensel lift of a irreducible polynomial from $\mathbb{Z}_p[x]$) and $\xi = x + \langle f(x)\rangle$ is a root of $f(x)$.

[1]The basic irreducible polynomial $f(x)$ is defined as the polynomial $\mu(f(x)) \in \mathbb{F}_p[x]$ is irreducible in $\mathbb{F}_p[x]$.

Every element of $GR(p^k, n)$ can be uniquely written in the **"additive" form**:

$$a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{n-1}\xi^{n-1} \tag{1}$$

where $a_i \in \mathbb{Z}_{p^k}$. From this form we conclude the number of elements of $GR(p^k, n)$ is p^{kn}, also we confirm the characteristic is p^k.

We have $\xi^{p^n-1} = 1$ since ξ is a root of $f(x)$, which forms a cyclic group of order $p^n - 1$ with multiplication, also forms $\mathcal{T}_n$ by adjoining 0 called by *Teichmüller sets* isomorphism to $\mathbb{F}_{p^n}$.

Definition (*Teichmüller sets*)

Teichmüller sets of $GR(p^k, n)$ is of the form

$$\mathcal{T}_n = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^n-2}\}$$

clearly $\mathcal{T}_n$ is isomorphic to te finite field $\mathbb{F}_{2^n}$.

Thus we give another **multiplicative form** of $GR(p^k, n)$:

$$a_0 + pa_1 + p^2 a_2 + \cdots + p^{k-1} a_{k-1} \tag{2}$$

where $a_i \in \mathcal{T}_n = \{0, 1, \xi, \xi^p, \ldots, \xi^{p^n-2}\}$.

Example of Galois Ring

Assume $p = 2$, $k = 3$, $n = 3$ and set $f(x) = x^3 - 2x^2 - 3x - 1 \in \mathbb{Z}_8[x]$ then we obtain that $GR(8, 3) = \frac{\mathbb{Z}_8[x]}{\langle f(x) \rangle} \cong \mathbb{Z}_8[\xi]$ where $\xi = x + \langle f(x) \rangle$ is a root of monic primitive polynomial $f(x)$ of degree 3 over $\mathbb{Z}_8$. Notice that $\mu f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$ is clearly a primitive polynomial over $\mathbb{Z}_2$.
The residue class of the form

$$a_0 + a_1 x + a_2 x^2 + \langle f(x) \rangle$$

where $a_i \in \mathbb{Z}_8$, are all distinct elements of $\mathbb{Z}_8[x]/\langle f(x) \rangle$.
The additive form is listed below:

$$\mathbb{Z}_8[\xi] = \{a_0 + a_1 \xi + a_2 \xi^2, a_i \in \mathbb{Z}_8\}$$

and the multiplicative form is also listed below:

$$\mathbb{Z}_8[\xi] = \{a_0 + 2a_1 + 4a_2, a_i \in \mathcal{T}_3\}$$

Basic irreducible polynomial: we can always obtain a basic irreducible polynomial over $\mathbb{Z}_{p^k}$ from an irreducible polynomial over $\mathbb{Z}_p$ by Hensel Lifting.
Extension of Galois Rings: The extension of Galois ring is also parallel to the extension of finite fields and we have the commutative diagram: for all $m \mid n$

$$\begin{array}{ccc} & \xrightarrow{\mu} & \\ GR(p^r, m) & & \\ \downarrow & & \\ GR(p^r, n) & \xrightarrow{\mu} & \end{array}$$

Something:

The elements in $\mathcal{T}_n$ have some properties, for all $n \geq 2$(if not, $\mathcal{T}_1 = \{0, 1\}$ is trivil):

(i) $\pm\xi^i \pm \xi^j$ has an inverse element for $0 \leq j < i \leq 2^n - 2$. If not, we have $\pm\xi^i \pm \xi^j \in 2R$, after the projection we have $\theta^i + \theta^j = 0$, but it's impossible since θ is a primitive element in the finite field.

(ii) $\xi^i - \xi^j \neq \pm\xi^k$ for distinct $0 \leq i, j, k \leq 2^n - 2$. If not, we have $1 + \xi^a = \xi^b$ where $a \neq b$, then square the equation we obtain $1 + 2\xi^a + \xi^{2a} = \xi^{2b}$, meanwhile we obtain $1 + \xi^{2a} = \xi^{2b}$ under the Frobenius map[a]. Therefore we arrive at $2\xi^a = 0$, a contradiction.

(iii) When $n \geq 3$, then for $i \neq j$ and $k \neq l$, we have $\xi^i - \xi^j = \xi^k - \xi^l \Leftrightarrow i = k \ and \ j = l$: just like before we obtain $1 + \xi^a = \xi^b + \xi^c$ and $\xi^a = \xi^{b+c} \mod 2$, which means $\theta^a = \theta^b\theta^c$, meanwhile we also have $1 + \theta^a = \theta^b + \theta^c$, so $(\theta^b + 1)(\theta^c + 1) = 0$ implies $\theta^b = 1$ or $\theta^c = 1$.

(iv) For odd $m \geq 3$, $\xi^i + \xi^j + \xi^k + \xi^l = 0 \Rightarrow i = j = k = l$: omit the proof.

Notice that $\mathcal{T}_n$ is not closed under the addition, thus we define the new operation $\oplus$ of $\mathcal{T}_n$ by $a \oplus b = (a + b + \varepsilon)^2$ where $\varepsilon \in \mathcal{T}_n$ a constant. This new operation is closed since $(a \oplus b)^{2^n} = (a + b + \varepsilon)^{2^n \cdot 2} = (a + b + \varepsilon)^2 = a \oplus b$, i.e. the result is still in $\mathcal{T}_n$. And as (a, b) varies over $\mathcal{T}_n \times \mathcal{T}_n$, $a \oplus b$ also takes every element of $\mathcal{T}_n$ once. So we can also simply define $a \oplus b = (\sqrt{a} + \sqrt{b})^2 = a + b + 2\sqrt{ab}$.

Actually in $GR(4,n)$, the operation of addition of $\mathcal{T}_n$ is defined by $a \oplus b = (a+b)^{2^d}$ where $1 \leq d \leq n-1$, but we always set $d = n-1$:
$(a \oplus b)^{2^n} = (a+b)^{2^{n+d}} = \left((a+b)^{2^n}\right)^{2^d} = (a^{2^n} + b^{2^n})^{2^d} = (a+b)^{2^d} = a \oplus b$, coincide with the definition of $\mathcal{T}_n$.
But when $d = 0$, we have $1 \oplus 1 = 2 \notin \mathcal{T}_n$.
When $1 \leq d \leq n-2$, we obtain that $a \oplus b = (a+b)^{2^d} = a^{2^d}(1+b/a)^{2^d}$, since a^{2^d} must be in $\mathcal{T}_n$, the closed of addition is equal to $(1+b/a)^{2^d} \in \mathcal{T}_n$. If $b = 0$ or $a = 0$, the equation is trivilly true. Thus we have to prove that $(1+\xi^i)^{2^d} \in \mathcal{T}_n$ for all $0 \leq i \leq 2^n - 2$:

(i) when $i = 0$, we have $2^{2^d} \equiv 0 \mod 4$, thus $(1+1)^{2^d} = 0 \in \mathcal{T}_n$

(ii) when $i \neq 0$, we have for all $1 \leq i \leq 2^n - 2$, there is a $1 \leq j \leq 2^n - 2$ such that $(1+\xi^i)^{2^d} = \xi^j \Leftrightarrow 1 + \xi^i = \xi^{j2^{n-d}}$. According to something **??**,

I don't know how to go on this, or I have a wrong direction of the proof?. Therefore I have no idea why not use $1 \leq d \leq n-2$.
Use the trace function in $GR(4,n)$ and $y = x + z + 2\sqrt{zx}$ we have

$$T(x \oplus y) = T(x + (x + z + 2\sqrt{xz})) = 2T(x) + T(z) + 2T(\sqrt{xz})$$

where $x, y, z \in \mathcal{T}_n$.

Think about $c \in \mathbb{Z}_4$, we can uniquely decompose it into $c = a + 2b$ where $a, b \in \mathbb{Z}_2$ from (**??**), then we have a canonical projection $\mu : \mathbb{Z}_4 \to \mathbb{Z}_2$ such as $\mu(c) = a$, which is the module 2 map in fact. Thus we have a natural extension $\mu : \mathbb{Z}_4[x] \to \mathbb{Z}_2[x]$ acts as

$$\mu\left(\sum_{i=0}^{k} a_i x^k = \sum_{i=0}^{k} (a_i \mod 2) x^k\right)$$

Also from this canonical map we can induces the surjection from $GR(4, n)$ to $\mathbb{F}_{2^n}$:

$$\mu(c) = \mu(a + 2b) = \mu(\xi^r + 2\xi^s) = \mu(\xi^r) = \theta^r, \forall c \in GR(4, n), \xi^r, \xi^s \in \mathcal{T}_n$$

therefore we have the isomorphism from $\mathcal{T}_n$ to $\mathbb{F}_{2^n}$.

Not all elements in ring is a unit, such that the elements of the form $2\xi^r$ in $GR(4,n)$ are zero divisors. Denote $R^* = R \setminus 2R$ the set of all units of $GR(4,n)$, then every elements of R^* has the unique representation in the form $\xi^r(1+2t)$ where $t \in \mathcal{T}_n$.

Remark:
In $GR(4,n)$, all zero divisors are of the form $2\xi^r$ with cardinality 2^n-1 and units are of the form $\xi^r(1+2t)$ with cardinality $(2^n-1)2^n$.

We denote the *Frobenius map* σ the ring isomorphism from $GR(4,n)$ to itself taking elements $c = a + 2b$ to $\sigma(c) = a^2 + 2b^2$. So we have the *relative trace* from $GR(4,n)$ to $\mathbb{Z}_4$ defined by

$$T_1^n(c) = \sum_{i=0}^{n-1} \sigma^i(c) = \sum_{i=0}^{n-1} \sigma^i(a) + 2\sigma^i(b) = \sum_{i=0}^{n-1} a^{2^i} + 2b^{2^i}$$

There exists the commutative relationship between maps:

$$\mu \circ T_1^n = tr_1^n \circ \mu$$

where tr_1^n is the trace function from the finite field $\mathbb{F}_{2^n}$ mapto $\mathbb{F}_2$. For simplicity, we use T and tr instead of T_1^n and tr_1^n when there is no ambiguity.

In $GR(4,n)$, we confirm 2-multiplication is the projection from $\mathbb{Z}_4[x]$ to $\mathbb{Z}_2[x]$, then

$$\begin{aligned} 2T(c) =& 2T(a+2b) = 2\left(\sum_{i=0}^{n-1} a^{2^i} + 2\sum_{i=0}^{n-1} b^{2^i}\right) \\ =& \sum_{i=0}^{n-1} 2a^{2^i} = tr(2a) = tr(2(a+2b)) = tr(2c) \end{aligned}$$

where $c \in GR(4,n)$ and $c = a + 2b$ with $a, b \in \mathcal{T}_n$.
The Trace function over $GR(4,n)$ has the 2-adic expansion:

$$T(x) = tr(\mu(x)) + 2p(\mu(x))$$

where $p(x)$ is defined as

$$p(x) = \begin{cases} \sum_{i=1}^{(n-1)/2} tr(x^{2^i+1}) \\ n/2-1 \end{cases}$$

Definition (Walsh transform of generalized Boolean function[2])

An extension of Boolean function was introduced by Schmidt, and is a mapping from $\mathcal{T}_n$ to $\mathbb{Z}_{2^s}$. When $s = 2$, we can define the walsh transform $W_f : \mathcal{T}_n \to \mathbb{C}$ of $\mathbb{Z}_4$-boolean functions $f : \mathcal{T}_n \to \mathbb{Z}_4$ as below

$$W_f(u) = \sum_{x \in \mathcal{T}_n} i^{f(x)+2T(ux)}, \quad u \in \mathcal{T}_n$$

where i is the 4-nth root and $T(ux)$ is the Trace function over Galois Ring $GR(4, n)$.

[2]Kai-Uwe Schmidt. Quaternary Constant-Amplitude Codes for Multicode CDMA

Definition (generalized bent functions)

The generalized Boolean function f is generalized bent if $|W_f(u)| = 2^{n/2}$ for all $u \in \mathcal{T}_n$.

It's well known that the finite field $\mathbb{F}_{2^n}$ is isomorphic to $\mathbb{F}_2^n$, so the Walsh transform is also in this form:

$$W_f(u) = \sum_{x \in \mathbb{Z}_2^n} i^{f(x)+2u\cdot x}, \quad u \in \mathbb{Z}_2^n$$

Definition (Gray-map)

Denote φ as the *Gray-map* and we rewrite elements c in $\mathbb{Z}_4$ as $a + 2b$, where $a, b \in \mathbb{Z}_2$. We clearly confirm that $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ by $\varphi(c)$ to $(\beta(c), \gamma(c))$ is an isomorphism, where $\beta(c) = b$ and $\gamma(c) = a + b$. Extending this map to $\varphi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ is clear given by $\varphi(\boldsymbol{c}) = (\beta(\boldsymbol{c}), \gamma(\boldsymbol{c}))$.

Proposition

The Gray-map is distance preseving: the Lee weight[3] *of* $u - v$ *is equal to the Hamming distance between binary words* $\varphi(u)$ *and* $\varphi(v)$.

[3] Lee weight of a quaternary word is defined to be the Hamming weights of the images of the quaternary word under the Gray-map

It also defined a generalized Gray-map[4] from $\mathbb{Z}_{2^k}$ to the Reed-Muller code of order 1, $\mathcal{RM}(1, k-1)$:

$$G : \mathbb{Z}_{2^k} \to \mathcal{RM}(1, k-1)$$
$$u \longmapsto u_k + \sum_{i=1}^{k-1} u_i y_i$$

where y_i are varieties of Boolean functions and $u = \sum_{i=1}^{k-1} 2^{i-1} u_i$ is binary expansion of an element of $\mathbb{Z}_{2^k}$. Note that the Boolean function of $\mathbb{F}_2^k$ is one-to-one coresppponding to its truth table, which is a binary 2^k-tuple vector(The view of RS codes). Thus we obtain $G : \mathbb{Z}_{2^k} \hookrightarrow \mathbb{F}_2^{2^{k-1}}$ is a nonsurjective mapping. Actually it is since the image are only the Boolean functions of degree 1 or 0.

[4] Z_{2^k}-Linear Codes

Example of Gray-map

Example

When $k = 3$, the images of elements of $\mathbb{Z}_8$ are listed below with even weights:

$$G(0) = (0,0,0,0); G(1) = (0,1,0,1); G(2) = (0,0,1,1); G(3) = (0,1,1,0);$$
$$G(4) = (1,1,1,1); G(5) = (1,0,1,0); G(5) = (1,1,0,0); G(7) = (1,0,0,1);$$

Definition ($\mathbb{Z}_4$-linearity)

The binary codes are $\mathbb{Z}_4$-linearity if they can be constructed as binary images under the Gray map of linear codes over $\mathbb{Z}_4$

Proposition

Kerdock code is $\mathbb{Z}_4$-Linearity.

Definition of the binary Kerdock code

Original definition of *Kerdock codes* $\mathcal{K}_n$ of length $m = 2^n$ uses the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, and we can also take the Kerdock codes as the union of some cosets of Reed-Muller codes $\mathcal{RM}(1, n)$ with coset representants in $\mathcal{RM}(2, n)$, but we will give another method defining the Kerdock codes $\mathcal{K}_n$ as images of $\mathbb{Z}_4$-linear codes quaternary Kerdock codes $\mathcal{K}(n-1)$ by Gray-map[5].

[5] The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes

Exmaple of quaternary Kerdock code

Example of quaternary $\mathcal{K}(3)$: Assume $n = 3$ and $f(x) = x^3 - 2x^2 - 3x - 1$ be the basic primitive polynomial of degree 3. We find $g(x) = (x^{2^3-1} - 1)/(x - 1)f(x) = x^3 - x^2 - 2x - 1$, thus the generator matrix of quaternary $\mathcal{K}(3)$ is

$$\begin{bmatrix} 1 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 1 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 1 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 1 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{bmatrix}$$

And the $\mathcal{K}_4$ is the images of the gray-map of quaternary $\mathcal{K}(3)$.

Error?

Something:

The paper *The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes* gave the right(?)[a] polynomial $g(x) = x^3 - 2x^2 - 3x - 1 = f(x)$ as the two $f(x)$ are equal and got the same weight distribution. But can an incorrect generator matrix give the same weight distribution?

[a] In this paper it gave $f(x) = g(x) \Rightarrow f(x)^2(x-1) = x^7 - 1$ but I can't get this result

Kerdock code is $\mathbb{Z}_4$-linearity

And we describe the $\mathcal{K}(n)$ by trace function of $GR(4,n)$ as below:

$$\mathcal{K}(n) = \{\epsilon\mathbf{1} + \boldsymbol{u}^{(\lambda)}; \epsilon \in \mathbb{Z}_4, \lambda \in \mathbb{Z}_4[\xi]\}$$

where $\xi^{\infty} = 0$ and

$$\boldsymbol{u}^{(\lambda)} = \left(T(\lambda\xi^{\infty}), T(\lambda\xi^{0}), T(\lambda\xi^{1}), \ldots, T(\lambda\xi^{m-1})\right)$$

Thus it shows that each code of $\mathcal{K}(n)$ can be expreesd by this form:

$$c = (c_{\infty}, c_0, c_1, \ldots, c_{m-1})$$

where

$$c_i = T(\lambda\xi^i) + \epsilon, i \in \{0, 1, ..., m-1, \infty\}$$

and $\lambda = \xi^r + 2\xi^s$.

Kerdock code is $\mathbb{Z}_4$-linearity

Hence we can give the 2-adic expression of c_i as $c_i = a_i + 2b_i$, where

$$\begin{cases} a_i = tr(\pi\theta^i) + \alpha(\epsilon) & (3) \\ b_i = tr(\eta\theta^t) + Q(\pi\theta^i) + \alpha'(\epsilon) & (4) \end{cases}$$

where $\theta = \mu(\xi), \pi = \mu(\xi^r), \alpha(\epsilon) + 2\alpha'(\epsilon) = \epsilon, \eta = \mu(\epsilon\xi^r + \xi^s)$ and

$$Q(x) = \sum_{j=1}^{(n-1)/2} tr(x^{2^j+1}).$$

Therefore the images of quaternary Kerdock codes c_i can be expressed in this form:

$$\varphi(c_i) = (\beta(c_i), \gamma(c_i)) = (b_i, a_i + b_i).$$

Kerdock code is $\mathbb{Z}_4$-linearity

Besides the original definition of Kerdock codes[6] consist of two half: the left half has form as $c = (c_l, c_r)$

$$c_l(x) = tr(\eta x) + Q(\phi x) + A \tag{5}$$

and the right half is of the form

$$c_r(x) = tr(\eta x + \phi x) + Q(\phi x) + B. \tag{6}$$

Though the comparison**??????**, we conclude **the binary Kerdock codes can be expressed as images of quaternary Kerdock codes by Gray-map i.e. $\mathbb{Z}_4$-linear**.

[6] A Class of Low-Rate Nonlinear Binary Codes

Is $\mathcal{RM}(r,n)$ $\mathbb{Z}_4$-linearity?

Remark:
Since the $\mathcal{RM}(1,n)$ is contained in the $\mathcal{K}_n$, we have $\mathcal{RM}(1,n)$ is also $\mathbb{Z}_4$-linearity, so it's natural to think is there only one $\mathcal{RM}(r,n)$ with $\mathbb{Z}_4$-linearity.

Proposition

The binary Reed-Muller code $\mathcal{RM}(r,n)$ of length $m=2^n$ is $\mathbb{Z}_4$-linearity for $r=0,1,2,n-1$ and n.

Definition ($\mathbb{Z}_4$-valued quadratic form)

A $\mathbb{Z}_4$-valued quadratic form is a mapping $F : \mathcal{T}_n \to \mathbb{Z}_4$ with

(i) $F(0) = 0$;

(ii) $F(x \oplus y) = F(x) + F(y) + 2B(x, y)$

where $B : \mathcal{T}_n \times \mathcal{T}_n \to \mathbb{Z}_2$ is a symmetric bilinear form. And F is called alternating if $B(x, x) = 0$ for all $x \in \mathcal{T}_n$ meanwhile the rank of F is defined as the rank of B with $rank(B) = n - dim_{\mathbb{Z}_2}(rad(B))$ and $rad(B) = \{x \in \mathcal{T}_n : B(x, y) = 0, \forall y \in \mathcal{T}_n\}$.

Lemma

For a $\mathbb{Z}_4$-valued quadratic form $F(x)$, $F(x)$ is generalized bent iff $F(x)$ is of full rank.

Lemma

$G(x) = \sum_{i=0}^{n-1} \lambda^i x^{p^i} \in \mathbb{F}_p[x]$. Then $G(x) = 0$ has only one root in $\mathbb{F}_{p^n}$ iff $gcd(\sum_{i=0}^{n-1} \lambda^i x^i, x^n - 1)$

Then the construction of generalized bent functions $F(x)$ can be transformed into the calculation of rank of $B(x)$, while the specail form $F(x)$ can lead to some easy calculation.

Example of generalized bent function

Assume $F(x)$ the generalized Boolean function of the form

$$F(x) = T\left(x + 2\sum_{i=1}^{\lfloor\frac{n-1}{2}\rfloor} c_i x^{1+2^{ki}}\right) \quad c_i \in \mathbb{Z}_2, x \in \mathcal{T}_n$$

where k is any positive integer and clearly $F(x)$ is of $\mathbb{Z}_4$-valued quadratic forms. We can give the equation:

$$\begin{aligned} 2B(x,y) &= F(x \oplus y) - F(x) - F(y) \\ &= 2T\left(xy + \sum_{i=1}^{\lfloor\frac{n-1}{2}\rfloor}\left(c_i x^{2^{ki}} y + c_i x y^{2^{ki}}\right)\right) \\ &= 2T\left(y\left(x + \sum_{i=1}^{\lfloor\frac{n-1}{2}\rfloor}\left(c_i x^{2^{ki}} + c_i x^{2^{(n-i)k}}\right)\right)\right) \end{aligned}$$

Example of generalized bent function

Thus we only need to confirm the number of solution $x \in \mathcal{T}_n$ of the linearized polynomial

$$\mathcal{L}(x) = x + \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} \left(c_i x^{2^{ki}} + c_i x^{2^{(n-i)k}} \right)$$

is 1.

According to lemma **??**, we need to confirm whether the corresponding polynomial

$$Q(x) = 1 + \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} \left(c_i x^{ik} + c_i x^{(n-i)k} \right)$$

is coprime with $x^n - 1$

Links between generalized bent and bent function

The walsh transform of generalized Boolean functions is similar to the walsh transform of Boolean functions, besides the quaternary Kerdock codes can be transform into the binary Kerdock codes, so it's natural to think whether generalized bent functions have some links with bent functions. And it does.

$f : \mathbb{Z}_{2^n} \to \mathbb{Z}_4$ be any generalized Boolean function. Decompose it into $f(x) = a(\mu(x)) + 2b(\mu(x))$ for all $x \in \mathbb{Z}_{2^n}$, where $a, b : \mathbb{Z}_{2^n} \to \mathbb{Z}_2$ are both Boolean functions.

Lemma

If n is even(odd), then $f(x)$ is generalized bent(semibent) function iff both $b(x)$ and $a(x) + b(x)$ are both Boolean bent(semibent) functions.

Then we can construct some bent functions from above generalized bent functions.

Disappointment

It is not clear how to get the new Boolean bent functions of degree greater than 2 from the above method.

SHANGHAI JIAO TONG UNIVERSITY

Thank You

Zhaole Li · Galois Ring, Kerdock codes and generalized Boolean function