SHANGHAI JIAO TONG UNIVERSITY
SCHOOL OF ELECTRONIC INFORMATION AND ELECTRICAL ENGINEERING

Galois Ring and generalized Boolean function

Zhaole Li

Workshop of Galois Ring, 2021

Definition (Galois ring)

The **Galois ring** $\mathbb{GR}(p^k, n)$ constructed by $\frac{\mathbb{Z}_{p^k}[x]}{(h(x))} = \mathbb{Z}_{p^k}[\xi]$ where $h(x)$ 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 $\xi = x + (h(x))$ is a root of $h(x)$.

$$\frac{\mathbb{Z}_{p^k}[x]}{(h(x))} = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + (h(x)), a_i \in \mathbb{Z}_{p^k}\}.$$

Set $\xi = x + (h(x))$, then $h(\xi) = 0$ and $\xi^i = x^i + (h(x))$.

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

Examples of Galois Rings

Example

Consider the ring $\mathbb{Z}_{p^k}$ where p is a prime and k is a positive integer. Clearly 1 is the identity of the ring. And the set of zero divisors with 0 is the ideal $(p) = p\mathbb{Z}_{p^k}$.
Note that when $k = 1$, $\mathbb{Z}_{p^k} = \mathbb{F}_p$ is just the finite field with p elements.

Example

Set $h(x)$ is a monic basic irreducible polynomial of degree n in $\mathbb{Z}_{p^k}$, then consider the residue class of the ring $\mathbb{Z}_{p^k}[x]/(h(x))$.
Clearly the residue classes

$$a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + (h(x)),$$

where $a_i \in \mathbb{Z}_{p^k}$ are distinct elements of $\mathbb{Z}_{p^k}[x]/(h(x))$. $1 + (h(x))$ is the identity and $(h(x))$ is the zero. And the set of zero divisors with $(h(x))$ is the ideal $(p + h(x))$.

- We have all elements in $\mathbb{Z}_{p^k}$ of p-adic:
  $\mathbb{Z}_{p^k} = \{c_0 + pc_1 + p^2c_2 + \cdots + p^{k-1}c_{k-1}, c_i \in \mathbb{Z}_p\}$.
- Then we have a ring homomorphism:

$$\begin{array}{rcl} - : \quad \mathbb{Z}_{p^k} & \to & \mathbb{Z}_p \\ c_0 + pc_1 + p^2c_2 + \cdots + p^{k-1}c_{k-1} & \mapsto & c_0, \end{array}$$

  where $c_i \in \mathbb{Z}_p$, whose kernal is the ideal (p) of $\mathbb{Z}_{p^k}$.
- Meanwhile $-$ can be extended to

$$\begin{array}{rcl} - : \quad \mathbb{Z}_{p^k}[x] & \to & \mathbb{Z}_p[x] \\ a_0 + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1} & \mapsto & \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_{m-1}}x^{m-1}, \end{array}$$

  where $a_i \in \mathbb{Z}_{p^k}$, whose kernal is the ideal (p) of $\mathbb{Z}_{p^k}[x]$. Note that the image of the ideal $(h(x))$ under the homomorphism $-$ is $(\overline{h}(x))$.

By ring isomorphism theorem, we confirm the map

$$\begin{array}{ccc} \mathbb{Z}_{p^k}[x]/(h(x)) & \to & \mathbb{Z}_p[x]/(\overline{h}(x)) \\ a_0 + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1} + (h(x)) & \mapsto & \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_{m-1}}x^{m-1} + (\overline{h}(x)), \end{array}$$

is also a ring homomorphism, also denoted by $-$.
Clearly, the kernal of the above homomorphism is the ideal $(p + h(x))$. Thus, we have

$$(\mathbb{Z}_{p^k}[x]/(h(x)))/(p + (h(x))) \cong \mathbb{Z}_p[x]/(\overline{h}(x)).$$

Note that $\mathbb{Z}_p[x]/(\overline{h}(x))$ is the finite field $\mathbb{F}_{p^n}$, where $n = \deg(\overline{h}(x))$.

For simplicity, write $\xi = x + (h(x))$, then $h(\xi) = 0$ and

$$a_0 + a_1 x + \cdots + a_{m-1} x^{m-1} + (h(x)) = a_0 + a_1 \xi + \cdots + a_{m-1} \xi^{m-1},$$

and then all elements of $\mathbb{Z}_{p^k}[x]/(h(x))$ can be expressed in the form

$$a_0 + a_1 \xi + \cdots + a_{m-1} \xi^{m-1}, \quad a_i \in \mathbb{Z}_{p^k}.$$

Thus, we have $\mathbb{Z}_{p^k}[\xi] = \mathbb{Z}_{p^k}[x]/(h(x))$ is a Galois ring.

We also have $\overline{\xi} = x + (\overline{h}(x))$ and $\overline{\xi}$ is a root of the monic irreducible polynomial $\overline{h}(x)$ over $\mathbb{F}_p$ and then

$$\mathbb{F}_p[x]/(\overline{h}(x)) = \mathbb{F}_p[\overline{\xi}] \cong \mathbb{F}_{p^n}.$$

Therefore, we have

$$\begin{array}{ccc} \mathbb{Z}_{p^k}[\xi] & \to & \mathbb{F}_p[\xi] \\ a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{m-1}\xi^{m-1} & \mapsto & \overline{a_0} + \overline{a_1}\xi + \cdots + \overline{a_{m-1}}\xi^{m-1}. \end{array}$$

$$\begin{array}{ccc} \mathbb{Z}_{p^k}[x] & \xrightarrow{\ \overline{\ }\ } & \mathbb{F}_p[x] \\ \downarrow & & \downarrow \\ \mathbb{Z}_{p^k}[\xi] & \xrightarrow{\ \overline{\ }\ } & \mathbb{F}_p[\overline{\xi}] \end{array}$$

Theorem

Any two Galois rings of the same characteristic and the same cardinality are isomorphic.

Therefore we can use the notation $\mathbb{GR}(p^k, n)$ to denote any Galois ring of characteristic p^k and cardinality p^{kn}.

Remark:
Any two finite fields with the same number of elements are isomorphic.

Every element of $\mathbb{GR}(p^k, n) = \mathbb{Z}_{p^k}/(h(x))$ 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 $a_i \in \mathbb{Z}_{p^k}$ and ξ is a root of $h(x)$. From this form we conclude the number of elements of $\mathbb{GR}(p^k, n)$ is p^{kn}, also we confirm the characteristic is p^k.

Remark:
Every elements of $\mathbb{F}_{p^n} = \mathbb{Z}_p/(f(x))$ can be uniquely written in the form;

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}, \quad a_i \in \mathbb{F}_p,$$

where α is a root of the irreducible polynomial $f(x)$ over $\mathbb{F}_2[x]$.

We have $\xi^{p^n-1} = 1$ if ξ is a root of $h(x)$, which is a monic basic primitive polynomial of degree n over $\mathbb{Z}_{p^k}$. ξ 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 $\mathbb{F}_{p^n}$.

Remark:

The existence of the monic basic primitive(irreducible) polynomial of degree n over $\mathbb{Z}_{p^k}$ is due to the Hensel's Lemma and the existence of the monic primitive(irreducible) polynomial of degree n over $\mathbb{F}_p$.

Definition (*Teichmüller sets*)

Teichmüller sets of $\mathbb{GR}(p^k, n) = \mathbb{Z}_{p^k}[\xi]$ is of the form

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

Thus we give **'multiplicative' form**(p-adic) of $\mathbb{GR}(p^k, n) = \mathbb{Z}_{p^k}[\xi]$:

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

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

> **Remark:**
> In a finite ring, every nonzero element is a zero divisor or a unit. Thus in the multiplicative form of the Galois ring, if $a_0 \neq 0$, the element is a unit, otherwise a zero divisor.

Thus $(p) = p\mathbb{GR}(p^k, n)$ is the collection of all zero divisors and a maximal ideal by counting. Hence $\mathbb{GR}(p^k, n)/(p)$ is the finite field $\mathbb{F}_{p^n}$.

Example of the Galois Ring $\mathbb{GR}(8,3)$

- Assume $p=2$, $k=3$, $n=3$ and set $h(x)=x^3-2x^2-3x-1\in\mathbb{Z}_8[x]$ then we obtain that $\mathbb{GR}(8,3)=\frac{\mathbb{Z}_8[x]}{(h(x))}\cong\mathbb{Z}_8[\xi]$ where $\xi=x+(h(x))$ is a root of basic primitive polynomial $h(x)$ of degree 3 over $\mathbb{Z}_8$. Notice that $\overline{h}(x)=x^3+x+1\in\mathbb{Z}_2[x]$ is clearly a primitive polynomial over $\mathbb{Z}_2$.
  The residue class of the form
  $$a_0+a_1x+a_2x^2+(h(x)),$$
  where $a_i\in\mathbb{Z}_8$, are all distinct elements of $\mathbb{Z}_8[x]/(h(x))$.
- 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:
  $$\mathbb{Z}_8[\xi]=\{a_0+2a_1+4a_2,a_i\in\mathcal{T}_3\}.$$

Theorem

Let $R = \mathbb{GR}(p^k, m)$ and $R' = \mathbb{GR}(p^k, n)$. If R' is a extension ring of R, then $m \mid n$.

We have the commutative diagram: for all $m \mid n$

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

Remark:

Let $\mathbb{F}_{p^m}$ be a finite field with p^m elements. If $\mathbb{F}_{p^n}$ is a extension field of $\mathbb{F}_{p^m}$, then $m \mid n$.

Conversely, we have

Theorem

Let $R = \mathbb{GR}(p^k, m)$ and $m \mid n$, then there is a Galois ring $R' = \mathbb{GR}(p^k, n)$ containing R as a subring.

And we arrive at

Theorem

Let $h(x)$ be a monic basic irreducible polynomial of degree l over $R = \mathbb{GR}(p^k, m)$, then the residue class ring $R[x]/(h(x))$ is a Galois ring of characteristic p^k and cardinality p^{kml} and containing R as a subring. Thus,

$$R[x]/(h(x)) = \mathbb{GR}(p^k, ml).$$

Besides, let $\xi = x + (h(x))$, then $h(\xi) = 0$ and then $R[x]/(h(x)) = R[\xi]$.

Generalized Trace

Let $R = \mathbb{GR}(p^k, m)$ and $R' = \mathbb{GR}(p^k, n)$, where $m \mid n$. Then for any $\alpha \in R'$, define

$$\mathrm{T}_R^{R'}(\alpha) = \alpha + \sigma(\alpha) + \sigma^2(\alpha) + \cdots + \sigma^{n/m-1}(\alpha),$$

where $\sigma(\alpha) = \sigma(a + 2b) = a^{p^m} + 2b^{p^m}$.

Theorem

For $\alpha, \beta \in R'$ and $a \in R$, we have

1. $\mathrm{T}_R^{R'}(\alpha) \in R$;
2. $\mathrm{T}_R^{R'}(\alpha + \beta) = \mathrm{T}_R^{R'}(\alpha) + \mathrm{T}_R^{R'}(\beta)$;
3. $\mathrm{T}_R^{R'}(a\alpha) = a\,\mathrm{T}_R^{R'}(\alpha)$, *in particular,* $\mathrm{T}_R^{R'}(a) = \frac{na}{m}$;
4. $\mathrm{T}_R^{R'}(\alpha^{p^{mk}}) = \mathrm{T}_R^{R'}(\alpha)$;

Remark:

For $F = \mathbb{F}_{p^m}$ and $F' = \mathbb{F}_{p^n}$ with $m \mid n$, we have for all $\alpha \in F$,

$$\mathrm{tr}_F^{F'}(\alpha) = \alpha + \alpha^{p^m} + \alpha^{p^{2m}} + \cdots + \alpha^{p^{(n-m)}}.$$

There exists the commutative relationship between maps:

$$- \circ \mathrm{T}_R^{R'} = \mathrm{tr}_1^n \circ -,$$

where tr_1^n is the trace function from the finite field $\mathbb{F}_{p^n}$ mapto $\mathbb{F}_p$.

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

1. $\pm\xi^i \pm \xi^j$ is a unit for $0 \leq j < i \leq 2^n - 2$. If not, we have $\pm\xi^i \pm \xi^j \in 2R$, after the projection $-$ with $\theta = \overline{\xi}$ we have $\theta^i + \theta^j = 0$, but it's impossible since θ is a primitive element in the finite field.
2. $\xi^i - \xi^j \neq \pm\xi^k$ 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. Therefore we arrive at $2\xi^a = 0$, a contradiction.This leads to the addition of $\mathcal{T}_n$ is not the addition of integers
3. 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 $\theta^c = 1$.
4. For odd $m \geq 3$, $\xi^i + \xi^j + \xi^k + \xi^l = 0 \Rightarrow i = j = k = l$: omit the proof.

Actually in $\mathbb{GR}(4,n)$, the operation of addition of $\mathcal{T}_n$ is defined by $a \oplus b = (a+b)^{2^n}$:

- Firstly, $\forall c = a + 2b \in \mathbb{GR}(4,n)$, we have $c^{2^n} = (a+2b)^{2^n} = a \in \mathcal{T}_n$, where $a, b \in \mathcal{T}_n$. So we confirm that for all $a, b \in \mathcal{T}_n$, we obtain $a \oplus b = (a+b)^{2^n} = ((a+b)_0 + 2((a+b)_1))^{2^n} = (a+b)_0 \in \mathcal{T}_n$;
- Secondly we have $0 \oplus 0 = 0^{2^n} = 0$, i.e. 0 is the zero of $\mathcal{T}_n$;
- And then if $a \oplus b = (a+b)^{2^d}$ where $d \neq n$, we have $a \oplus 0 = a^{2^d} \neq a$ for some $a \in \mathcal{T}_n$, which means 0 is not the zero. Contradiction.
- Also $a \oplus a = (a+a)^{2^n} = (2a)^{2^n} = 0$, which means that the inverse of a is a.

Theorem (Lucas Theorem)

For non-negative integers m and n and a prime p, the following congruence relation holds:

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \mod p,$$

where

$$m = m_k p^k + \cdots + m_1 p + m_0,$$

and

$$n = n_k p^k + \cdots + n_1 p + n_0,$$

are the base p expansions of m and n respectively. Note that the convention $\binom{m}{n} = 0$ if $m < n$.

We have $(\mathcal{T}_n, \oplus)$ forms a group and we can confirm that $a \oplus b = (a+b)^{2^n} = a + b + 2(ab)^{2^{n-1}}$:
Since $\binom{2^n}{t} = \frac{2^n}{t}\binom{2^n-1}{t-1}$, assume $2^f || t$, then $2^{n-f} | \binom{2^n}{t}$. Hence we only consider t such as $2^{n-1}||t$ or $2^n||t$, the latter is $t = 2^n$ which is not in consideration. When $2^{n-1}||t$, we obtain $t = 2^{n-1}$, so $\binom{2^n}{2^{n-1}} = 2\binom{2^n-1}{2^{n-1}-1}$. Notice that $2 \nmid \binom{2^n-1}{2^{n-1}-1}$ by Lucas Theorem. So we have $4 \mid \binom{2^n}{t}$ for all $t \neq 2^{n-1}$ and $\binom{2^n}{2^{n-1}} \equiv 2 \mod 4$. So $(a+b)^{2^n} = a + b + 2(ab)^{2^{n-1}}$.

Consequence of Lucas Theorem

A binomial coefficient $\binom{m}{n}$ is divisible by 2 if and only if at least one of the base 2 digits of n is greater than the corresponding digit of m.

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

Remark:
In $\mathbb{GR}(4,n)$, 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 $(2^n-1)2^n$.

Generalized Trace of $\mathbb{GR}(4, n)$

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

$$\begin{aligned} 2\,\mathrm{T}_R^{R'}(c) =& 2\,\mathrm{T}_R^{R'}(a+2b) = 2\left(\sum_{i=0}^{n-1} a^{2^i} + 2\sum_{i=0}^{n-1} b^{2^i}\right) \\ =& 2\sum_{i=0}^{n-1} a^{2^i} = 2\,\mathrm{tr}_1^n(\bar{a}) = 2\,\mathrm{tr}_1^n(\overline{a+2b}) = 2\,\mathrm{tr}_1^n(\bar{c}), \end{aligned}$$

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

$$\mathrm{T}_R^{R'}(x) = \mathrm{tr}_1^n(\bar{x}) + 2p(\bar{x}),$$

where $p(x)$ is defined as

$$p(x) = \begin{cases} \sum_{i=1}^{(n-1)/2} \mathrm{tr}_1^n(x^{2^i+1}) \\ \sum_{i=1}^{n/2-1} \mathrm{tr}_1^n(x^{2^i+1}) + \mathrm{tr}_1^{n/2}(x^{2^{n/2}+1}). \end{cases}$$

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

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

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

[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:

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

Generalize bent Z4-quadratic forms

Assume $R = \mathbb{Z}_4$ and $R' = \mathbb{GR}(4, m)$. Let l be a positive integer and $1 = e_0 \leq e_1 < \cdots < e_l = m$ with $e_i \mid e_{i+1}$. Let $f_i = m/e_i$ is odd, then define

$$Q_j(x) = \mathrm{T}_R^{R'}\left(\sum_{i=1}^{\frac{f_j-1}{2}} x^{2^{ie_j}+1}\right).$$

Take $\gamma_0, \gamma_1, \ldots, \gamma_{l-1} \in \mathcal{T}$, where $\overline{\gamma_0} = 1$, $\overline{\gamma_j} \in \mathbb{F}_{2^{e_j}}$ and $1 + \sum_{j=1}^{t} \overline{\gamma_j}^2 \neq 0$ for $t \leq l-1$. Thus, for any $a \in \mathcal{T}^*$, define the $\mathbb{Z}_4$-quadratic forms:

$$f_a(x) = \mathrm{T}_R^{R'}(ax) + 2\sum_{j=1}^{l-1} Q_j\left(\gamma_j a x\right).$$

By some calculation we have

$$2B_{f_a}(x,y) = f_a(x \oplus y) - f_a(x) - f_a(y) = 2\,\mathrm{tr}_1^m\left(\bar{y}\left(\bar{a}^2\bar{x} + \sum_{j=1}^{l-1}\overline{\gamma_j a}\left(\mathrm{tr}_{e_j}^m\left(\overline{\gamma_j a x_j}\right) + \overline{\gamma_j a x}\right)\right)\right).$$

For simplicity we denote tr_1^m the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^1}$.

Thus we have

$$2B_{f_a-f_b}(x,y) = 2\,\mathrm{tr}_1^m\Big(\bar{y}\,\big((\bar{a}^2+\bar{b}^2)\bar{x} + \sum_{j=1}^{l-1}\Big(\overline{\gamma_j a}\,\Big(\mathrm{tr}_{e_j}^m\left(\overline{\gamma_j a x}\right)+\overline{\gamma_j a x}\Big)+\overline{\gamma_j b}\,\Big(\mathrm{tr}_{e_j}^m\left(\overline{\gamma_j b x}\right)+\overline{\gamma_j b x}\Big)\Big)\Big)\Big).$$

Next it's to prove that $\mathrm{rad}(B_{f_a-f_b}) = \{0\}$.
Suppose that $x \in \mathrm{rad}(B_{f_a-f_b})$ and $x \neq 0$, then $\bar{x}$ is a nonzero solution of

$$(\bar{a}^2 + \bar{b}^2)\bar{x} + \sum_{j=1}^{l-1} \left(\overline{\gamma_j a} \left(\mathrm{tr}_{e_j}^m \left(\overline{\gamma_j a x} \right) + \overline{\gamma_j a x} \right) + \overline{\gamma_j b} \left(\mathrm{tr}_{e_j}^m \left(\overline{\gamma_j b x} \right) + \overline{\gamma_j b x} \right) \right) = 0.$$

Multiply x and $\mathrm{tr}_{e_j}^m(\overline{\gamma_j x}) = \overline{\gamma_j}\,\mathrm{tr}_{e_j}^m(\overline{x})$ we have

$$(1 + \sum_{j=1}^{l-1} \overline{\gamma_j}^2)(\bar{a}^2 + \bar{b}^2)\bar{x}^2 + \sum_{j=1}^{l-1} \gamma_j^2 x \left(\overline{a}\,\mathrm{tr}_{e_j}^m \left(\overline{a x} \right) + \overline{b}\,\mathrm{tr}_{e_j}^m \left(\overline{b x} \right) \right) = 0.$$

Note that $\mathrm{tr}_{e_j}^m(y^2) = (\mathrm{tr}_{e_j}^m(y))^2$ for all $y \in \mathbb{F}_{2^m}$. Set above equation be A, then we have

$$\begin{aligned}\mathrm{tr}_{e_{l-1}}^m(A) =&(1+\sum_{j=1}^{l-2}\overline{\gamma_j}^2)\,\mathrm{tr}_{e_{l-1}}^m((\bar{a}^2+\bar{b}^2)\bar{x}^2)\\ &+\sum_{j=1}^{l-2}\gamma_j^2\left(\mathrm{tr}_{e_{l-1}}^m(\overline{ax})\,\mathrm{tr}_{e_j}^m\left(\overline{ax}\right)+\mathrm{tr}_{e_{l-1}}^m(\overline{bx})\,\mathrm{tr}_{e_j}^m\left(\overline{bx}\right)\right).\end{aligned}$$

Since f_{j+1} is odd, then $tr_{e_j}^m(\mathrm{tr}_{e_{j+1}}^m(y)) = \mathrm{tr}_{e_j}^m(y)$ for all $y \in \mathbb{F}_{2^m}$. We have

$$\mathrm{tr}_{e_1}^m\left(\mathrm{tr}_{e_2}^m\left(\cdots\mathrm{tr}_{e_{l-1}}^m(A)\cdots\right)\right) = \mathrm{tr}_{e_1}^m\left(\left(\bar{a}^2+\bar{b}^2\right)\bar{x}^2\right) = \left(\mathrm{tr}_{e_1}^m((\bar{a}+\bar{b})\bar{x})\right)^2 = 0.$$

Thus, $\mathrm{tr}_{e_1}^m((\bar{a}+\bar{b})\bar{x}) = 0$, i.e. there exists a t s.t. $\mathrm{tr}_{e_{t+1}}^m((\bar{a}+\bar{b})\bar{x}) \neq 0$ but $\mathrm{tr}_{e_t}^m((\bar{a}+\bar{b})\bar{x}) = 0$.

Note that when $j \geq t+1$, $\mathrm{tr}_{e_{t+1}}^m\left(\overline{\gamma_j a x}\left(\mathrm{tr}_{e_j}^m\left(\overline{\gamma_j a x}\right) + \overline{\gamma_j a x}\right)\right) = 0$.

And let $u_j = \mathrm{tr}_{e_j}^m(\overline{ax}) = \mathrm{tr}_{e_j}^m(\overline{bx})$ since $\mathrm{tr}_{e_j}^m((\bar{a}+\bar{b})\bar{x}) = 0$ for $j \leq t$.

Contradiction

Consider $\mathrm{tr}_{e_{t+1}}^m(A)$, we can arrive at

$$= \mathrm{tr}_{e_{t+1}}^m((\bar{a}+\bar{b})\bar{x}) \left(\left(1 + \sum_{j=1}^{t} \bar{\gamma}_j^2 \right) \mathrm{tr}_{e_{t+1}}^m((\bar{a}+\bar{b})\bar{x}) + \sum_{j=1}^{t} \overline{\gamma_j}^2 u_j \right) = 0.$$

So we have

$$\left(1 + \sum_{j=1}^{t} \bar{\gamma}_j^2 \right) \mathrm{tr}_{e_{t+1}}^m((\bar{a}+\bar{b})\bar{x}) + \sum_{j=1}^{t} \overline{\gamma_j}^2 u_j = 0.$$

which means $\mathrm{tr}_{e_{t+1}}^m((\bar{a}+\bar{b})\bar{x}) \in \mathbb{F}_{2^{e_t}}$.
But we also have

$$0 = \mathrm{tr}_{e_t}^m((\bar{a}+\bar{b})\bar{x}) = \mathrm{tr}_{e_t}^{e_{t+1}} \left(\mathrm{tr}_{e_{t+1}}^m((\bar{a}+\bar{b})\bar{x}) \right) = \mathrm{tr}_{e_{t+1}}^m((\bar{a}+\bar{b})\bar{x})\, \mathrm{tr}_{e_t}^{e_{t+1}}(1) = \mathrm{tr}_{e_{t+1}}^m((\bar{a}+\bar{b})\bar{x}).$$

Contradiction with t.

Examples of generalized bent functions

- For simplicity, T_1^m denotes the generalized trace from $\mathbb{GR}(4, m)$ to $\mathbb{Z}_4$.
- $Q(x) = \mathrm{T}_1^m(x + 2x^{1+2^{2k}} + 2x^{1+2^{3k}})$, $x \in \mathcal{T}_m$ bent iff $\gcd(m, k) = \gcd(m, 3k)$. When $m = 4$ and $k = 1$, the generalized bent function is of the form $\mathrm{T}_1^4(x + 2x^5 + 2x^9)$.
- Truthtable is [0, 0, 2, 2, 1, 2, 2, 1, 3, 2, 1, 2, 3, 1, 3, 3], corresponding to $x \in [0, 1, \xi, ..., \xi^{2^4-2}]$. And its Walsh spectra [$-$4, $-$4, 4, 4, 4i, 4, 4, $-$4i, 4i, 4, $-$4i, 4, 4i, $-$4i, 4i, 4i].
- Also we have its gray-map $b(x)$, with truthtable [0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1] and Walsh spectra [$-$4, $-$4, 4, 4, $-$4, 4, 4, $-$4, 4, 4, $-$4, 4, 4, $-$4, 4, 4].
- Its gray-map $a(x) + b(x)$ with truthtable [0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0] and Walsh spectra [$-$4, $-$4, 4, 4, 4, 4, 4, 4, $-$4, 4, 4, 4, $-$4, 4, $-$4, $-$4].

There is an isomorphim between the vector space $\mathbb{F}_2^4$ to $\mathbb{F}_{2^4}$. We can assume the basis of vector space is $\{1, \xi, \xi^2, \xi^3\}$, then we have

$$\begin{cases} 0 \to (0000), & \xi^7 \to (1101) \\ 1 \to (1000), & \xi^8 \to (1010) \\ \xi^1 \to (0100), & \xi^9 \to (0101) \\ \xi^2 \to (0010), & \xi^{10} \to (1110) \\ \xi^3 \to (0001), & \xi^{11} \to (0111) \\ \xi^4 \to (1100), & \xi^{12} \to (1111) \\ \xi^5 \to (0110), & \xi^{13} \to (1011) \\ \xi^6 \to (0011), & \xi^{14} \to (1001) \end{cases}$$

where ξ is a root of $x^4 + x + 1 = 0$.

Consider $\mathrm{tr}_1^4(x^3)$ where $x \in \mathbb{F}_{2^4} = \mathbb{F}_2[\xi]$, ξ is a root of $x^4 + x + 1$ in $\mathbb{F}_2[x]$. Assume $x = x_1 + \xi x_2 + \xi^2 x_3 + \xi^3 x_4$, then we have

$$\begin{aligned}
\mathrm{tr}_1^4(x^3) &= \mathrm{tr}_1^4((x_1 + \xi x_2 + \xi^2 x_3 + \xi^3 x_4)^3) \\
&= \mathrm{tr}_1^4((x_1 + \xi^2 x_2 + \xi^4 x_3 + \xi^6 x_4)(x_1 + \xi x_2 + \xi^2 x_3 + \xi^3 x_4)) \\
&= x_1 \,\mathrm{tr}_1^4(1) + x_1 x_2 \,\mathrm{tr}_1^4(\xi) + x_1 x_3 \,\mathrm{tr}_1^4(\xi^2) + x_1 x_4 \,\mathrm{tr}_1^4(\xi^3) + \cdots \\
&\quad + x_4 \,\mathrm{tr}_1^4(\xi^9)
\end{aligned}$$

Meanwhile we can give the value of $\mathrm{tr}_1^4(\xi^i)$, so we confirm $f(x) = f(x_1 + \xi x_2 + \xi^2 x_3 + \xi^3 x_4) = x_2 + x_3 + x_4 + x_2 x_4 + x_3 x_4$.

Truthtable of the Boolean function

vector	0000	1000	0100	1100	0010	1010	0110	1110	0001	1001
finite field	0	1	ξ^1	ξ^4	ξ^2	ξ^8	ξ^5	ξ^{10}	ξ^3	ξ^{14}
value	0	1	1	1	1	1	0	0	1	1

vector	0101	1101	0011	1011	0111	1111				
finitefield	ξ^9	ξ^7	ξ^6	ξ^{13}	ξ^{11}	ξ^{12}				
value	1	1	1	1	1	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

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 $\mathbb{GR}(4, n)$ 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 $\theta = \bar{\xi}, \pi = \overline{\xi^r}, \alpha(\epsilon) + 2\alpha'(\epsilon) = \epsilon, \eta = \overline{\epsilon\xi^r + \xi^s}$ 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 comparison356, 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

1. $F(0) = 0$;
2. $F(x \oplus y) = F(x) + F(y) + 2B(x, y)$

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 2, 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 $f(x) = a(\bar{x}) + 2b(\bar{x})$ 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.

Example

$F(x)$ is defined as before and if it's generalized bent function, then we have

$$b(x) = p(x) + \sum_{i=1}^{\lfloor \frac{n-1}{2} \rfloor} tr(c_i x^{1+2^{ki}}) \quad c_i \in \mathbb{Z}_2, x \in \mathbb{F}_{2^n}$$

is also bent function.

SHANGHAI JIAO TONG UNIVERSITY

Thank You

Zhaole Li · Galois Ring
and generalized Boolean function