Difference sets, divisible difference families and codes over Galois rings of characteristic 2^n

Mieko Yamada
Faculty of Mathematics and Physics
Institute of Science and Engineering
Kanazawa University

IMS Workshop, 2011

Galois rings $GR(2^n, s)$

Let $f(x) \in \boldsymbol{Z}/2^n\boldsymbol{Z}[x]$ be a primitive basic irreducible polynomial of degree s and ξ be a root of $f(x)$.
The ring $\boldsymbol{Z}/2^n\boldsymbol{Z}[x]/(f(x))$ is called a Galois ring of characteristic 2^n with the extension degree s and is denoted by $GR(2^n, s)$.

- $\boldsymbol{Z}/2^n\boldsymbol{Z}(\xi) \cong GR(2^n, s) = \mathcal{R}_n$.
- A unique maximal ideal $\mathfrak{p}_n = 2\mathcal{R}_n$.
- Every ideal of $\mathcal{R}_n$ is $\mathfrak{p}_n^l = 2^l\mathcal{R}_n, 1 \leq l \leq n-1$.
- $\mathcal{R}_n^\times = \mathcal{R}_n - \mathfrak{p}_n$ is the unit group of $\mathcal{R}_n$.

Any element of α of $GR(2^n, s)$ is uniquely represented as

$$\alpha = \alpha_0 + 2\alpha_1 + \cdots + 2^{n-1}\alpha_{n-1}, \quad \alpha_i \in \mathcal{T}_n \quad (0 \leq i \leq n-1)$$

where $\mathcal{T}_n = \{0, 1, \xi, \cdots, \xi^{2^s-2}\}$ as a set of complete representatives of $GR(2^n, s)/\mathfrak{p}_n$.

The unit group $\mathcal{R}_n^\times$ of $GR(2^n, s)$ is a direct product of a cyclic group $\langle \xi \rangle$ and $\mathcal{E} = \{1 + 2a | a \in \mathcal{R}_{n-1}\}$. An arbitrary element α of $\mathcal{R}_n^\times$ is uniquely represented as

$$\alpha = \xi^t e = \xi^t(1 + 2a), \ a \in GR(2^{n-1}, s), e \in \mathcal{E}.$$

$(2^{(n+1)s}, 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}} - 1), 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}-1} - 1)$ difference sets

We prove the following theorem.

Theorem 1. *For every odd integer n and every extension degree s, there exists a difference set D_{n+1} with parameters*

$$v = 2^{(n+1)s}, k = 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}} - 1), \lambda = 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}-1} - 1)$$

over a Galois ring $GR(2^{n+1}, s)$.
This difference set D_{n+1} is embedded in the ideal part of a difference set D_{n+3} over $GR(2^{n+3}, s)$. It means that there exists an infinite family of difference sets with the embedding system over Galois rings.

A new operation

We define a new operation,

$$\boldsymbol{\alpha * \beta = \alpha + \beta + 2\alpha\beta}$$

for $\alpha, \beta \in \mathcal{R}_n$.

Theorem 2. *Let $g_1 = 1, g_2, \cdots, g_s$ be a free $\boldsymbol{Z}/2^n\boldsymbol{Z}$-basis. Let $\mu : \mathcal{R}_n \to GF(2^s)$ be the map defined by $\mu(\alpha) \equiv \alpha \pmod 2$ and b be an element of $\mathcal{R}_n$ such that $x^2 + x = \mu(b)$ has no solution in $GF(2^s)$. Then $\mathcal{R}_n$ is an abelian group with respect to the operation $*$,*

$$\mathcal{R}_n = \langle -1 \rangle * \langle 2b \rangle * \prod_{j=2}^{s} \langle g_j \rangle$$

where $|\langle -1 \rangle| = 2$, $\quad |\langle 2b \rangle| = 2^{n-1}$ and $|\langle g_j \rangle| = 2^n$, $2 \le j \le s$.

The subsets of $\mathcal{R}_n$ and $\mathcal{R}_{n-l}(1 \le l \le \frac{n-1}{2})$ for s even

In what follows. we assume that $n \equiv 1 \pmod 2$. We define the subsets as follows.

- $$A^{\text{even}} = \bigcup_{m=0}^{2^{n-2}-1} \langle -1 \rangle * \prod_{j=2}^{s} \langle g_j \rangle * (2b)^{*m}, \quad A^{\text{even}} \subset \mathcal{R}_n.$$

- $$\mathcal{A}_l^{\text{even}} = \bigcup_{m=0}^{2^{n-2l-2}-1} \langle -1 \rangle * \prod_{j=2}^{s} \langle g_j \rangle * \langle 2b^{*2^{(n-1-2l)}} \rangle * (2b)^{*m}$$

  $\mathcal{A}_l^{\text{even}} \subset \mathcal{R}_{n-l}$, for $1 \le l \le \frac{n-3}{2}$.

- $$B = \prod_{j=2}^{s-1} \langle g_j \rangle * \langle -1 \rangle * \langle g_s^{*2} \rangle * \langle 2b \rangle, \quad B \subset \mathcal{R}_{\frac{n+1}{2}}.$$

The subsets of $\mathcal{R}_n$ and $\mathcal{R}_{n-l}(1 \leq l \leq \frac{n-1}{2})$ for s odd

For odd extension, we can choose at least 1 free-$\boldsymbol{Z}/2^n\boldsymbol{Z}$-base, say for instance g_s, which satisfies $2^{n-1} \in \langle -1 \rangle * \prod_{j=2}^{s-1} \langle g_j \rangle * \langle 2b \rangle$. We define the subsets as follows.

- $$A^{\text{odd}} = \bigcup_{m=0}^{2^{n-1}-1} \langle -1 \rangle * \prod_{j=2}^{s-1} \langle g_j \rangle * \langle 2b \rangle * (g_s)^{*m}, \quad A^{\text{odd}} \subset \mathcal{R}_n.$$

- $$\mathcal{A}_l^{\text{odd}} = \bigcup_{m=0}^{2^{n-2l-1}-1} \langle -1 \rangle * \prod_{j=2}^{s-1} \langle g_j \rangle * \langle 2b \rangle * \langle g_s^{*2^{n-2l}} \rangle * g_s^{*m},$$

  $\mathcal{A}_l^{\text{odd}} \subset \mathcal{R}_{n-l}$, for $1 \leq l \leq \frac{n-3}{2}$.

- $$B = \prod_{j=2}^{s-1} \langle g_j \rangle * \langle -1 \rangle * \langle g_s^{*2} \rangle * \langle 2b \rangle, \quad B \subset \mathcal{R}_{\frac{n+1}{2}}.$$

The subsets of $\mathcal{R}_{n+1}^{\times}$ and $\mathfrak{p}_{n+1}^{l}(1 \le l \le \frac{n-1}{2})$

- $D_{\mathcal{R}_{n+1}^{\times}} = \{(1+2\alpha)\xi^t | \alpha \in A^{\text{even}}(A^{\text{odd}}), t = 0, 1, \cdots, 2^s - 2\}$,
  $D_{\mathcal{R}_{n+1}^{\times}} \subset \mathcal{R}_{n+1}^{\times}$.
- $D_{\mathfrak{p}_{n+1}^{l}} = \{2^l(1+2\alpha)\xi^t | \alpha \in \mathcal{A}_l^{\text{even}}(\mathcal{A}_l^{\text{odd}}), t = 0, 1, \cdots, 2^s - 2\}$,
  $1 \le l \le \frac{n-3}{2}$, $\quad D_{\mathfrak{p}_{n+1}^{l}} \subset \mathfrak{p}_{n+1}^{l}$.
- $D_{\mathfrak{p}_{n+1}^{(n-1)/2}} = \{2^{\frac{n-1}{2}}(1+2\alpha)\xi^t | \alpha \in B, t = 0, 1, \cdots, 2^s - 2\}$.
  $D_{\mathcal{R}_{n+1}^{(n-1)/2}} \subset \mathfrak{p}_{n+1}^{\frac{n-1}{2}}$

$D_{n+1} = D_{\mathcal{R}_{n+1}^{\times}} \bigcup_{l=1}^{\frac{n-3}{2}} D_{\mathfrak{p}_{n+1}^{l}} \bigcup D_{\mathfrak{p}_{n+1}^{(n-1)/2}}$ is a difference set.

The cardinalities of the subsets

- $|D_{\mathcal{R}_{n+1}^{\times}}| = 2^{ns-1}(2^s - 1)$.
- $|D_{\mathfrak{p}_{n+1}^{l}}| = 2^{(n-l)s-l}(2^s - 1)$.
- $|D_{\mathfrak{p}_{n+1}^{(n-1)/2}}| = 2^{(n+1)s/2-1}(2^s - 1)$.

Thus we have $|D_{n+1}| = 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}} - 1) = k$.

The additive character λ_β of $\mathcal{R}_{n+1}$

Lemma 1. *The additive character of $\mathcal{R}_{n+1}$ is given by*

$$\lambda_\beta(\alpha) = \zeta_{2^{n+1}}^{T_{n+1}(\beta\alpha)}.$$

where T_{n+1} is the trace function and $\beta \in \mathcal{R}_{n+1}$, and $\zeta_{2^{n+1}}$ is a primitive 2^{n+1}st root of unity.

A necessary and sufficient condition

The subset $D_{n+1} = D_{\mathcal{R}_{n+1}^{\times}} \bigcup_{l=1}^{\frac{n-3}{2}} D_{\mathfrak{p}_{n+1}^{l}} \bigcup D_{\mathfrak{p}_{n+1}^{(n-1)/2}}$ of $\mathcal{R}_{n+1}$ is a difference set with parameters

$$v = 2^{(n+1)s}, k = 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}} - 1), \lambda = 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}-1} - 1)$$

if and only if the element $\mathcal{D}_{n+1} = \sum_{\alpha \in D_{n+1}} \alpha$ of the group ring $\boldsymbol{Z}\mathcal{R}_{n+1}$ satisfies

$$\begin{aligned}
\lambda_0(\mathcal{D}_{n+1}) &= 2^{\frac{(n+1)s}{2}-1}(2^{\frac{(n+1)s}{2}} - 1) = |D_{n+1}|, \\
\lambda_\beta(\mathcal{D}_{n+1}) &= \lambda_\beta(\mathcal{D}_{\mathcal{R}_{n+1}^{\times}}) + \sum_{l=1}^{\frac{n-3}{2}} \lambda_\beta(\mathcal{D}_{\mathfrak{p}_{n+1}^{l}}) + \lambda_\beta(\mathcal{D}_{\mathfrak{p}_{n+1}^{(n-1)/2}}) \\
&= 2^{\frac{(n+1)s}{2}-1} u
\end{aligned}$$

for every additive character $\lambda_\beta, \beta \neq 0$ of $\mathcal{R}_{n+1}$, where u is a unit of a cyclotomic field $\boldsymbol{Q}(\zeta_{2^{n+1}})$.

The multiplicative character of $\mathcal{R}_{n+1}^{\times}$

Let $\tilde{\chi}$ be a multiplicative character of $\mathcal{R}_{n+1}^{\times}$ of order 2^m. $|\langle\xi\rangle| = 2^s - 1$.
Since $(2^m, 2^s - 1) = 1$, then $\tilde{\chi}(\xi) = 1$.

For $\xi^t(1 + 2\alpha), \xi^u(1 + 2\beta) \in \mathcal{R}_{n+1}^{\times}$, we have

$$\tilde{\chi}(\xi^t(1+2\alpha)\cdot\xi^u(1+2\beta)) = \tilde{\chi}((1+2\alpha)(1+2\beta)) = \tilde{\chi}(1+2(\alpha*\beta)).$$

Thus the multiplicative character $\tilde{\chi}$ of order 2^m can be regarded as a multiplicative character χ of the group $\mathcal{R}_n$ with respect to the new operation.

Gauss sums over $\mathcal{R}_{n+1}$

For a multiplicative character $\tilde{\chi}$ of $\mathcal{R}_{n+1}$ and an additive character λ_β of $\mathcal{R}_{n+1}$, we define the Gauss sum over $\mathcal{R}_{n+1}$.

$$G(\tilde{\chi}, \lambda_\beta) = \sum_{\alpha \in \mathcal{R}_{n+1}} \tilde{\chi}(\alpha)\lambda_\beta(\alpha).$$

The determination of $\lambda_\beta(\mathcal{D}_{\mathcal{R}_{n+1}^\times})$

We define the multiplicative character χ of $\mathcal{R}_n$ as follows:
For an even extension,

$$\chi(\delta * (2b)^{*e}) = \chi((2b)^{*e}) = \zeta_{2^{n-1}}^e,$$

where $\delta \in \langle -1 \rangle * \prod_{j=2}^{s} \langle g_j \rangle \subset A^{\text{even}}$ and $0 \leq e \leq 2^{n-1} - 1$.

For an odd extension,

$$\chi(\delta * (g_s)^{*e}) = \chi((g_s)^{*e}) = \zeta_{2^n}^e,$$

where $\delta \in \langle -1 \rangle * \langle 2b \rangle * \prod_{j=2}^{s-1} \langle g_j \rangle \subset A^{\text{odd}}$ and $0 \leq e \leq 2^{n-1} - 1$.

We define the multiplicative character $\tilde{\chi}$ of $\mathcal{R}_{n+1}$ by letting $\tilde{\chi}((1+2\alpha)\xi^t) = \chi(\alpha)$.

For $\beta \neq 0$, we have

$$\lambda_\beta(\mathcal{D}_{\mathcal{R}_{n+1}^\times}) = \frac{1}{2^n}\left\{\sum_{\substack{m=0\\ m:\text{odd}}}^{2^n-1} G(\tilde{\chi}^m, \lambda_\beta)\sum_{j=0}^{2^{n-1}-1}\zeta_{2^n}^{-mj} + 2^{n-1}G(\tilde{\chi}^0, \lambda_\beta)\right\}.$$

Theorem 3. *Assume that m is odd. Then*

$$G(\tilde{\chi}^m, \lambda_1) = 2^{\frac{n+1}{2}s}\zeta_{2^n}^x, \quad G(\tilde{\chi}^0, \lambda_1) = 0$$

where $\tilde{\chi}^0$ is a trivial character of $\mathcal{R}_{n+1}^\times$ and x is some positive integer.

Substituting these values to the equation, we have the following lemma.

Lemma 2.

$$\lambda_\beta(\mathcal{D}_{\mathcal{R}_{n+1}^\times}) = \begin{cases} \pm 2^{\frac{(n+1)s}{2}-1} & \text{if} \quad \beta \in \mathcal{R}_{n+1}^\times, \\ 0 & \text{if} \quad \beta \in \mathfrak{p}_{n+1} - \mathfrak{p}_{n+1}^n, \\ -2^{ns-1} & \text{if} \quad \beta \in \mathfrak{p}_{n+1}^n - \{0\}. \end{cases}$$

The determination of $\lambda_\beta(\mathcal{D}_{\mathfrak{p}_{n+1}^l})$ for $1 \leq l \leq \frac{n-1}{2}$

In what follows, we treat the odd extension.

We also have the following lemmas by using Gauss sums.

Lemma 3. *Put* $\mathfrak{p} = \mathfrak{p}_{n+1}$ *and* $\mathcal{R}^\times = \mathcal{R}^\times_{n+1}$.

$$\lambda_\beta(\mathcal{D}_{\mathfrak{p}^l}) = \begin{cases} 0 & \textit{if} \quad \beta \in \mathcal{R}^\times - \mathfrak{p}^l, \\ \pm 2^{\frac{(n+1)s}{2}-1} & \textit{if} \quad \beta \in \mathfrak{p}^l - \mathfrak{p}^{l+1}, \\ 0 & \textit{if} \quad \beta \in \mathfrak{p}^{l+1} - \mathfrak{p}^{n-l}, \\ -2^{(n-l)s-1} & \textit{if} \quad \beta \in \mathfrak{p}^{n-l} - \mathfrak{p}^{n-l+1}, \\ 2^{(n-l)s-1}(2^s - 1) & \textit{if} \quad \beta \in \mathfrak{p}^{n-l+1} - \{0\}. \end{cases}$$

Lemma 4. *Put* $\mathfrak{p} = \mathfrak{p}_{n+1}$ *and* $\mathcal{R}^\times = \mathcal{R}^\times_{n+1}$.

$$\lambda_\beta(\mathcal{D}_{\mathfrak{p}^{\frac{n-1}{2}}}) = \begin{cases} 0 & \textit{if} \quad \beta \in \mathcal{R}^\times \ or \ \beta \in \mathfrak{p} - \mathfrak{p}^{\frac{n-1}{2}}, \\ 2^{\frac{n+1}{2}s-1}u & \textit{if} \quad \beta \in \mathfrak{p}^{\frac{n-1}{2}} - \mathfrak{p}^{\frac{n+1}{2}}, \\ -2^{\frac{n+1}{2}s-1} & \textit{if} \quad \beta \in \mathfrak{p}^{\frac{n+1}{2}} - \mathfrak{p}^{\frac{n+3}{2}}, \\ 2^{\frac{n+1}{2}s-1}(2^s-1) & \textit{if} \quad \beta \in \mathfrak{p}^{\frac{n+3}{2}} - \{0\}, \end{cases}$$

where u *is a unit of a cyclotomic field* $\boldsymbol{Q}(\zeta_4)$.

The proof of Theorem 1

From Lemmas 1,2 and 3, we obtain for $\beta \neq 0$,

$$\begin{aligned} \lambda_\beta(\mathcal{D}_{n+1}) &= \lambda_\beta(\mathcal{D}_{\mathcal{R}_{n+1}^\times}) + \sum_{l=1}^{\frac{n-3}{2}} \lambda_\beta(\mathcal{D}_{\mathfrak{p}_{n+1}^l}) + \lambda_\beta(\mathcal{D}_{\mathfrak{p}_{n+1}^{(n-1)/2}}) \\ &= 2^{\frac{(n+1)s}{2}-1} u \end{aligned}$$

where u is a unit of a cyclotomic field $\boldsymbol{Q}(\zeta_{2^{n+1}})$.

The table of $\lambda_\beta(\mathcal{D}_{n+1})$

β	$\lambda_\beta(\mathcal{D}_{\mathcal{R}^\times})$	$\lambda_\beta(\mathcal{D}_{\mathfrak{p}})$	$\lambda_\beta(\mathcal{D}_{\mathfrak{p}^l})$	$\lambda_\beta(\mathcal{D}_{\mathfrak{p}^{\frac{n-1}{2}}})$
$\mathcal{R}^\times$	$\pm 2^{\frac{n+1}{2}s-1}$	0	0	0
$\mathfrak{p}-\mathfrak{p}^2$	0	$\pm 2^{\frac{n+1}{2}s-1}$	0	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathfrak{p}^l-\mathfrak{p}^{l+1}$	0	0	$\pm 2^{\frac{n+1}{2}s-1}$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathfrak{p}^{\frac{n-3}{2}}-\mathfrak{p}^{\frac{n-1}{2}}$	0	0	0	0
$\mathfrak{p}^{\frac{n-1}{2}}-\mathfrak{p}^{\frac{n+1}{2}}$	0	0	0	$2^{\frac{n+1}{2}s-1}u$
$\mathfrak{p}^{\frac{n+1}{2}}-\mathfrak{p}^{\frac{n+3}{2}}$	0	0	0	$-2^{\frac{n+1}{2}s-1}$
$\mathfrak{p}^{\frac{n+3}{2}}-\mathfrak{p}^{\frac{n+5}{2}}$	0	0	0	$2^{\frac{n+1}{2}s-1}(2^s-1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathfrak{p}^{n-l}-\mathfrak{p}^{n-l+1}$	0	0	$-2^{(n-l)s-1}$	$2^{\frac{n+1}{2}s-1}(2^s-1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathfrak{p}^{n-1}-\mathfrak{p}^n$	0	$-2^{(n-1)s-1}$	$2^{(n-l)s-1}(2^s-1)$	$2^{\frac{n+1}{2}s-1}(2^s-1)$
$\mathfrak{p}^n-\{0\}$	-2^{ns-1}	$2^{(n-1)s-1}(2^s-1)$	$2^{(n-l)s-1}(2^s-1)$	$2^{\frac{n+1}{2}s-1}(2^s-1)$

An embedding system of difference sets

We see

$$D_{\mathfrak{p}_{n+3}} \supset 2D_{\mathcal{R}_{n+1}^{\times}},\ D_{\mathfrak{p}_{n+3}^{l}} \supset 2D_{\mathfrak{p}_{n+1}^{l-1}},\ \text{for } 1 \leq l \leq \frac{n+1}{2}.$$

If we write the subset $D_{n+3} = D_{\mathcal{R}_{n+3}^{\times}} \bigcup D_{\mathfrak{P}}$, $D_{\mathfrak{P}} = \bigcup_{l=1}^{\frac{n+1}{2}} D_{\mathfrak{p}_{n+3}^{l}}$, then

$$D_{\mathfrak{P}} \supset 2D_{n+1}.$$

Divisible difference family

Let G be a finite abelian group and N be a subgroup of G.
Let $\{B_1, B_2, .., B_b\}$ be k_i-subsets of G, $1 \leq i \leq b$.
Put $\theta_i(d) = |\{(x, y)|xy^{-1} = d, x, y \in B_i\}|$ and
$\theta(d) = \sum_{i=1}^{b} \theta_i(d)$.

A family $\{B_1, B_2, ..., B_b\}$ is called a $(G, N, \{k_1, ..., k_b\}, \mu, \lambda)$ divisible difference family if and only if

$$\theta(d) = \begin{cases} \mu, & \text{if } d \in N \setminus \{1\}, \\ \lambda, & \text{if } d \in G \setminus N \end{cases}$$

for $d \neq 1 \in G$.

Difference sets over $GR(2^2.s)$

Denote the absolute trace from $\mathbb{F}_{2^s}$ to $\mathbb{F}_2$ by tr.
Let $E_u = \{\alpha \in \mathbb{F}_{2^s} | tr(u\alpha) = 0\}$ for $u \in \mathbb{F}_{2^s}$ such that $tr(u) = 0$.

$$D = \{a(1+2b) | a \in \mathcal{T}_2,\ b \in E_u\}$$

is a $(2^{2s}, 2^{s-1}(2^s-1), 2^{s-1}(2^{s-1}-1)$ difference set
where $\mathcal{T}_2 = \{0, 1, \xi, \cdots, \xi^{2^s-2}\}$.

Notice that D is a multiplicative subgroup of the unit group $GR(2^2, s)^\times$.

Divisible difference family obtained from D

Theorem 4. *Let D be a difference set over $GR(2^2, s)$ and $\mathcal{E} = \{1 + 2a | a \in \mathbb{F}_{2^s}\}$.*
Let $S = \{1, y\}$ be a complete representaives of $GR(2^2, s)^\times / D$ and put $L = D \cap \mathcal{E}$.

We define the subsets

$$B_1 = (D - 1) \cap D, \quad B_2 = y(D - 1) \cap D.$$

Then $\{B_1, B_2\}$ is a $(D, L, \{2^{s-1}(2^{s-1}-1), 2^{s-1}(2^{s-1}-1)\}, 2^{s-1}(2^{s-2} - 1), 2^{s-1}(2^{s-1} - 1) - 2^{s-2})$ divisible difference family.

Notice that we construct a symmetric Hadamard matrix of order s^2 from this DDF.

An example of a divisible difference family over $GR(2^2, s)$

Let $g(x) = x^3 + 3x^2 + 2x + 3 \in \boldsymbol{Z}/2^2\boldsymbol{Z}[x]$ be a basic irreducible polynomial of $GR(4,3)$ and ξ be a root of $g(x)$. Let xyz denote the element $x\xi^2 + y\xi + z \in GR(4,3)$.

$$\begin{aligned} B_1 &= \{103, 232, 322, 112, 211, 111, 231, 121, 300, 332, 212, 331\} \text{ and} \\ B_2 &= \{233, 322, 332, 113, 213, 121, 010, 333, 103, 300, 112, 030\} \end{aligned}$$

forms a $(D, L, \{12, 12\}, 8, 10)$-DDF.

Defintion of codes over Galois rings $GR(2^n, s)$

Denote $\boldsymbol{Z}/2^n\boldsymbol{Z}$ by $\boldsymbol{Z}_{2^n}$.

Definition 1. *An additive subgroup C of $\boldsymbol{Z}_{2^n}^N$ is called a linear code of length N over $\boldsymbol{Z}_{2^n}$.*

Definition 2.
- *The Lee weight of the vector $\boldsymbol{x} = (x_1, x_2, \cdots, x_N)$ is defined by $w_L(\boldsymbol{x}) = \sum_{i=1}^{N} \min\{x_i, 2^n - x_i\}$*
- *The Lee distance $d_L(\boldsymbol{x}, \boldsymbol{y})$ is given by $d_L(\boldsymbol{x}, \boldsymbol{y}) = w_L(\boldsymbol{x} - \boldsymbol{y})$.*
- *The minimum Lee weight of the code C is $\min_{\substack{\boldsymbol{c}\in C\\ \boldsymbol{c}\neq 0}}(w_L(\boldsymbol{c}))$.*
- *The vector $\boldsymbol{x} * \boldsymbol{y} = (x_1y_1, x_2y_2, ..., x_Ny_N)$ is a componentwise product of the vectors $\boldsymbol{x}$ and $\boldsymbol{y}$.*

Reed-Muller codes over Galois rings $GR(2^n, s)$

We put $q = 2^n$ and $N = 2^s - 1$.

Definition 3. *We let*

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \xi & \xi^2 & \cdots & \xi^{N-1} \end{pmatrix} = \begin{pmatrix} \mathbf{1} \\ \boldsymbol{g_1} \\ \boldsymbol{g_2} \\ \vdots \\ \boldsymbol{g_s} \end{pmatrix}$$

where each element in the second row of G is assumed to be an s-tuples over $\boldsymbol{Z}_q$, and $\boldsymbol{g_i}, 1 \le i \le s$ is the row vector and $\mathbf{1}$ is the all one vector.
The rth order Reed-Muller code $Z_q RM(r, s)$ of length 2^s is the code generated by all tuples of the form

$$\boldsymbol{g}_1^{i_1} * \boldsymbol{g}_2^{i_2} * \cdots * \boldsymbol{g}_s^{i_s}$$

such that $i_j = 0, 1$, $\sum_{j=1}^{s} i_j \le r$ and $\boldsymbol{g}_j^0 = \mathbf{1}$.

Properties of Reed-Muller code $Z_q RM(r, s)$

We have the following results easily.

- $\left| Z_q RM(r, s) \right| = q^k, \; k = \sum_{l=0}^{r} \binom{s}{l}$
- $Z_q RM(r, s) \subset Z_q RM(r+1, s), \; r < s$
- For $q = 2$, $\quad Z_2 RM(r, s) = RM(r, s)$
- If $q \leq 2^s$, then $Z_q RM(r, s)^{\perp} = Z_q RM(s-r-1, s)$

An embedding system of $Z_q RM(r,s)$

Theorem 5. $Z_q RM(r,s)$

$$= \bigcup_{e_0,e_1,\cdots,e_{k-1}\in Z_2} \Big(2Z_{\frac{q}{2}} RM(r,s) + e_0 \mathbf{1} + e_1 \boldsymbol{g_1} + \cdots + e_m \boldsymbol{g_s} + e_{s+1} \boldsymbol{g_1} * \boldsymbol{g_2} + \cdots + e_{k-1} \boldsymbol{g_{s-r+1}} * \boldsymbol{g_{s-r+2}} * \cdots * \boldsymbol{g_s} \Big)$$

$Z_{\frac{q}{2}} RM(r,s)$ is embedded in the ideal part of $Z_q RM(r,s)$.

The minimum weights of $Z_qRM(r,s)$

Theorem 6. *The minimum Hamming weight of* $Z_qRM(r,s)$ *is* 2^{s-r}.

Theorem 7. *Assume that* $q \geq 8$. *The minimum Lee weight of* $Z_qRM(1,s)$ *is* 2^s *except for* $q = 8$ *and* $s = 3$. *The vector* $\mathbf{1}$ *and* $-\mathbf{1}$ *have Lee weight of* 2^s. *The minimum Lee weight of* $Z_8RM(1,3)$ *is* 6.

Theorem 7 is proved by the estimate of the character sum over $GR(2^n, s)$.

Thank you for your attention.