情報通信研究室：活動報告

研究室代表者・准教授　松井　一

2nd スマート情報技術研究センターシンポジウム
2022年12月1日（木）16:00-16:15

○目標

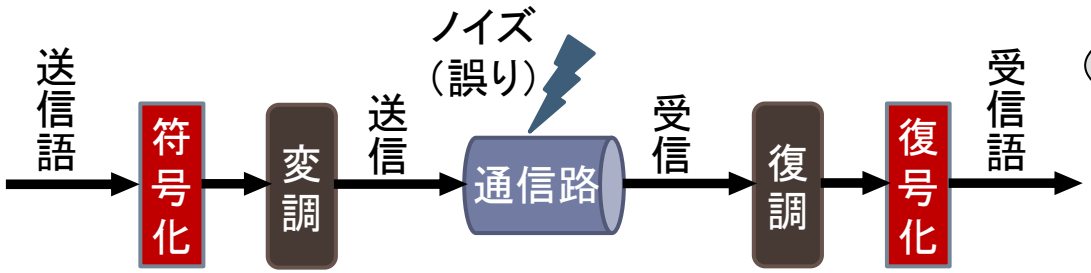
- 高性能な誤り訂正符号の構成
  - 未解決問題への挑戦やDNA記録などへの応用

報告内容

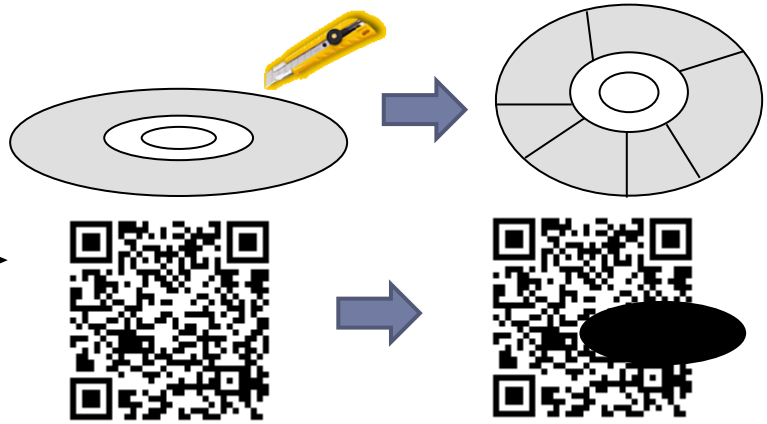
- 誤り訂正符号における構成・探索
- 最小重みが大きい準巡回符号の構成
- 反転不変符号・DNA符号

誤り訂正符号，符号理論

誤り訂正符号･･･デジタルデータに冗長部を定めノイズ耐性を付ける
符号理論･･･誤り訂正符号とその応用のための理論



図．通信のモデル．誤り訂正符号は
符号化と復号化からなる



図．キズや汚れをつける実験

- 誤り訂正符号(or符号)とは，ある長さのビット列のなす集合
  (線形代数の言葉では，2元ガロア有限体F2={0,1}上の線形空間)
- 研究室代表者の符号理論研究･･･1999年本学にPDとして着任以来継続

代数幾何符号　　準巡回符号　　自己双対･反転不変符号

1999　　2009　　2019

符号理論の歴史と現状

年代	トピック	備考
？	遺伝子符号	すべての生物の遺伝子に備わっている
1948	C. E. Shannon “A Mathematical Theory of Communication”	情報理論の創始， シャノン限界（誤り訂正符号の理論限界）
1950	Hamming符号	自明でない人類初の誤り訂正符号
1960	Reed-Solomon（RS）符号	CD，DVD，QRコード等広く応用される
1963	LDPC符号（R. G. Gallager）	（下で簡単に解説）
1993	Turbo符号（C. Berrou）	シャノン限界に迫る
2006	Polar符号（E. Arikan）	5Gに採用される

LDPC符号（low-density parity-check code，低密度パリティ検査符号）

Turbo符号の成功の後，LDPC符号がシャノン限界に迫ることが示される（2006）．

現在最も高性能とされ，ディジタル放送の規格に採用（RS符号と共に用いられる）．

しかし構成や性能解析等が解明されていない⇒多数の未解決問題

準巡回符号による高性能な符号の探索

準巡回符号とは？・・・ある種の巡回性を持つ符号

$$(c_{1,1}, c_{1,2}, \cdots, c_{1,m} \mid c_{2,1}, c_{2,2}, \cdots, c_{2,m} \mid \cdots \mid c_{1,1}, c_{1,2}, \cdots, c_{1,m}) \in C$$

$$(c_{1,m}, c_{1,1}, \cdots, c_{1,m-1} \mid c_{2,m}, c_{2,1}, \cdots, c_{2,m-1} \mid \cdots \mid c_{l,m}, c_{l,1}, \cdots, c_{l,m-1}) \in C$$

準巡回符号の生成行列（行ベクトル基底から作られる行列）の例

$$\left(\begin{array}{ccc|ccc|c} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \rightarrow \begin{pmatrix} 1+x^2 & 1 & 0 \\ 1+x & x & 0 \\ x+x^2 & x^2 & 0 \\ 1+x+x^2 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1+x & 1 \\ 0 & 1+x+x^2 & 0 \\ 0 & 0 & 1+x \end{pmatrix}$$

生成多項式行列への変換

- 準巡回符号はLDPC符号を構成できる広範な符号のクラス

基本等式の応用（オリジナルなアイデア）

G：準巡回符号の生成多項式行列

$$G=\begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1\ell} \\ 0 & g_{22} & \cdots & g_{2\ell} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{\ell\ell} \end{bmatrix}$$

Gの基本等式

$$AG=\mathrm{diag}\left[x^{n_1}-1,\quad \cdots,\quad x^{n_\ell}-1\right]$$

（Aはある多項式行列）

Gは準巡回符号の生成多項式行列　⇔　Gは基本等式をみたす

∴ 基本等式を解くことにより，すべての準巡回符号が構成できる

(H. Matsui, Finite Fields and Their Applications, vol.34, pp.280–304, Jul. 2015)

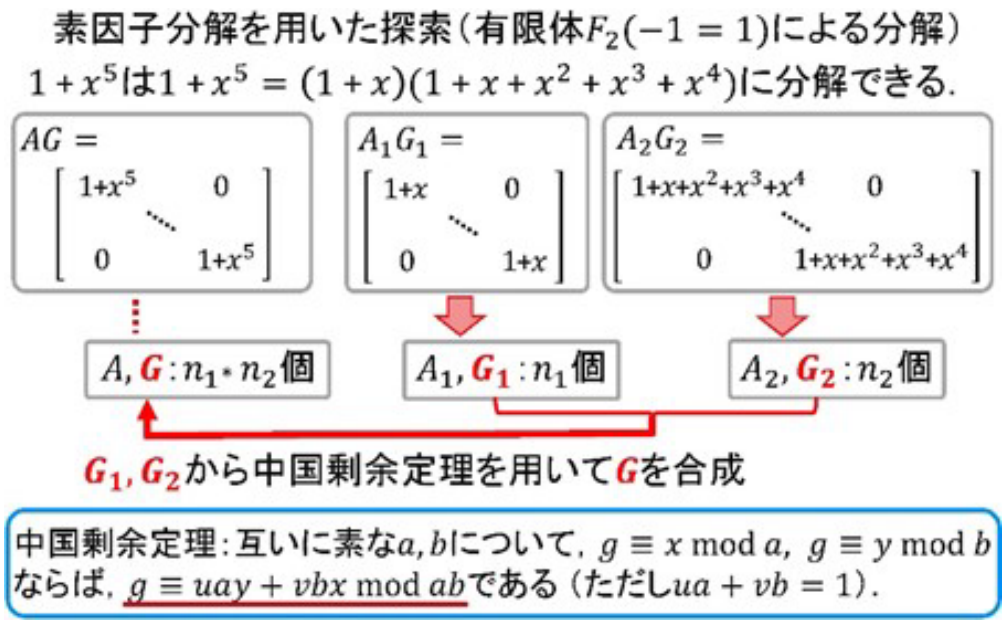
基本等式を軸とした，高性能な準巡回符号の探索が可能

メニーコアCPU，並列計算機の応用

中国剰余定理による準巡回符号の構成

H. Matsui, "A modulus factorization algorithm for self-orthogonal and self-dual quasi-cyclic codes via polynomial matrices," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E104-A, no.11, pp.1649-1653, Nov. 1, 2021.

（準巡回符号）



Algorithm 1 (cf. Proof of Proposition 1)

input $G_1 \in \{G_1\}_{d_1}$, $G_2 \in \{G_2\}_{d_2}$ with $\gcd(d_1, d_2) = 1$

output $\begin{cases} G \in \{G\}_{d_1 d_2} \text{ with } \mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2 \\ B_1, B_2 \in M_l(\mathbb{Z}) \text{ with } G = B_1G_1 = B_2G_2 \end{cases}$

for $j = 1$ to l **do**
  $g_{j,j} = g^{(1)}_{j,j} g^{(2)}_{j,j}$, $b^{(1)}_{j,j} = g^{(2)}_{j,j}$, $b^{(2)}_{j,j} = g^{(1)}_{j,j}$
  for $i = j - 1$ to 1 **do**
    $\left(g_{i,j}, b^{(1)}_{i,j}, b^{(2)}_{i,j}\right)$ given by (1) and (2)
  end for
end for

$$g_{i,j} = \sum_{k=i}^{j} b^{(1)}_{i,k} g^{(1)}_{k,j} = \sum_{k=i}^{j} b^{(2)}_{i,k} g^{(2)}_{k,j}. \quad (1)$$

$$g_{i,j} \equiv u g^{(1)}_{j,j} \sum_{k=i}^{j-1} b^{(2)}_{i,k} g^{(2)}_{k,j} + v g^{(2)}_{j,j} \sum_{k=i}^{j-1} b^{(1)}_{i,k} g^{(1)}_{k,j} \mod g_{j,j}. \quad (2)$$

- 多項式行列を用いた準巡回符号の構成の基礎理論を与えた
- 自己直交符号および自己双対符号に対しローカル→グローバルに構成
- 従来手法および提案手法の計算量評価を行い有効性を示した

報告内容

- 誤り訂正符号における構成・探索
- 最小重みが大きい準巡回符号の構成
- 反転不変符号・DNA符号

反転不変符号・DNA符号（DNA記録の誤り訂正符号）

DNA記録・DNAストレージ…DNAに数ギガ～数テラ～数ペタの情報を記録

A. Extance, “How DNA could store all the world’s data,” Nature, vol.537, no.7618, pp.22–24, 2016.

反転不変符号…DNA符号が満たすべき条件のひとつ，Reversibility（反転不変性）に注目

（反転不変符号）

Ramy Taki ElDin（元PD研究員（2019年9月～2020年8月），Ain Shams University, Egypt），尾白典文PD研究員との共同研究

参考：ヌクレオチド3組からなる64コドンと，それらに対応する20種類のアミノ酸.

		2nd base			
		U（ウラシル）	C（シトシン）	A（アデニン）	G（グアニン）
1st base	U	UUU フェニルアラニン UUC フェニルアラニン UUA ロイシン UUG ロイシン	UCU セリン UCC セリン UCA セリン UCG セリン	UAU チロシン UAC チロシン UAA Ochre (*終止*) UAG Amber (*終止*)	UGU システイン UGC システイン UGA Opal (*終止*) UGG トリプトファン
	C	CUU ロイシン CUC ロイシン CUA ロイシン CUG ロイシン	CCU プロリン CCC プロリン CCA プロリン CCG プロリン	CAU ヒスチジン CAC ヒスチジン CAA グルタミン CAG グルタミン	CGU アルギニン CGC アルギニン CGA アルギニン CGG アルギニン
	A	AUU イソロイシン AUC イソロイシン AUA イソロイシン, (*開始*) AUG メチオニン, *開始*	ACU スレオニン ACC スレオニン ACA スレオニン ACG スレオニン	AAU アスパラギン AAC アスパラギン AAA リシン AAG リシン	AGU セリン AGC セリン AGA アルギニン AGG アルギニン
	G	GUU バリン GUC バリン GUA バリン GUG バリン, (*開始*)	GCU アラニン GCC アラニン GCA アラニン GCG アラニン	GAU アスパラギン酸 GAC アスパラギン酸 GAA グルタミン酸 GAG グルタミン酸	GGU グリシン GGC グリシン GGA グリシン GGG グリシン

反転不変と自己双対との関係

R. Taki ElDin, H. Matsui, "Linking reversed and dual codes of quasi-cyclic codes," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol.E105-A, no.3, pp.381-388, Mar. 1, 2022. （反転不変符号）

$$F = \left(\mathrm{diag}[x^{m+d_i}]G\left(\frac{1}{x}\right) + (1-x^m)\mathrm{diag}[g^*_{i,i}]\right)J \qquad (7)$$

$$J = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ \vdots & \iddots & 1 & 0 \\ 0 & \iddots & \iddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix}$$

Theorem 1. *The polynomial matrix F given by (7) is a generator polynomial matrix of the reversed code $\mathcal{R}$ of C.*

Table 1 Optimal binary reversible self-orthogonal QC codes.

ℓ	n	k	$d_{\min}$	$G = (g_{i,j})$
2	64	32	12	$g_{1,1} = \langle 0\rangle$, $g_{1,2} = \langle 2,5,6,7,8,9,10,11,12,15,16,18,19,20,22,24,25,28,29,30,31\rangle$, $g_{2,2} = \langle 0,32\rangle$
3	36	6	16	$g_{1,1} = \langle 0,1,2,4,5,6\rangle$, $g_{1,2} = \langle 1,5,7,11\rangle$, $g_{1,3} = \langle 0,6,7,8,10,11\rangle$, $g_{2,2} = g_{3,3} = \langle 0,12\rangle$
4	68	34	12	$g_{1,1} = g_{1,2} = \langle 0\rangle$, $g_{1,3} = \langle 0,3,4,7,10,11,14\rangle$, $g_{1,4} = \langle 1,2,6,7,10,12,14\rangle$, $g_{2,2} = \langle 0,1\rangle$, $g_{2,3} = \langle 1,4,5,9,10,15\rangle$, $g_{2,4} = \langle 0,3,4,7,8,9,12,14\rangle$, $g_{3,3} = g_{3,4} = \langle 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16\rangle$, $g_{4,4} = \langle 0,17\rangle$
5	25	8	8	$g_{1,1} = g_{2,2} = \langle 0,1\rangle$, $g_{1,4} = g_{2,5} = \langle 1,4\rangle$, $g_{1,5} = g_{2,4} = \langle 1,2,3,4\rangle$, $g_{3,3} = g_{4,4} = g_{5,5} = \langle 0,5\rangle$
6	36	18	8	$g_{1,1} = g_{1,3} = g_{2,2} = g_{2,5} = \langle 0\rangle$, $g_{1,4} = \langle 2,4\rangle$, $g_{1,5} = g_{4,4} = g_{4,6} = \langle 0,1,2,3,4,5\rangle$, $g_{1,6} = \langle 0,1,3,5\rangle$, $g_{2,4} = \langle 3\rangle$, $g_{2,6} = \langle 0,1,2,4,5\rangle$, $g_{3,3} = \langle 0,1\rangle$, $g_{3,4} = \langle 0,3,4\rangle$, $g_{3,5} = \langle 3,4\rangle$, $g_{3,6} = \langle 0,2,5\rangle$, $g_{5,5} = g_{6,6} = \langle 0,6\rangle$
7	42	14	12	$g_{1,1} = \langle 0\rangle$, $g_{1,3} = \langle 0,1,2,3\rangle$, $g_{1,4} = \langle 0,3\rangle$, $g_{1,5} = \langle 5\rangle$, $g_{1,6} = \langle 2,3,4,5\rangle$, $g_{2,2} = \langle 0,1\rangle$, $g_{2,3} = \langle 2\rangle$, $g_{2,4} = \langle 1,4\rangle$, $g_{2,5} = \langle 0,1,4,5\rangle$, $g_{2,6} = g_{3,6} = g_{4,4} = g_{4,6} = \langle 0,1,2,3,4,5\rangle$, $g_{2,7} = \langle 1\rangle$, $g_{3,3} = \langle 0,2,4\rangle$, $g_{3,7} = \langle 1,3,5\rangle$, $g_{5,5} = g_{6,6} = g_{7,7} = \langle 0,6\rangle$
8	40	20	8	$g_{1,1} = g_{2,2} = g_{3,3} = g_{4,4} = \langle 0\rangle$, $g_{1,5} = g_{4,8} = \langle 0,2,4\rangle$, $g_{1,6} = g_{2,5} = g_{3,8} = g_{4,7} = \langle 0,1,4\rangle$, $g_{1,7} = g_{2,8} = \langle 0,2\rangle$, $g_{1,8} = \langle 1,2,4\rangle$, $g_{2,6} = g_{3,7} = \langle 3\rangle$, $g_{2,7} = \langle 2\rangle$, $g_{3,5} = g_{4,6} = \langle 1\rangle$, $g_{3,6} = \langle 1,4\rangle$, $g_{4,5} = \langle 1,2,3,4\rangle$, $g_{5,5} = g_{6,6} = g_{7,7} = g_{8,8} = \langle 0,5\rangle$
9	54	24	12	$g_{1,1} = g_{1,2} = g_{3,3} = g_{3,4} = \langle 0\rangle$, $g_{1,6} = \langle 1\rangle$, $g_{1,7} = \langle 1,3,5\rangle$, $g_{1,8} = \langle 0,2\rangle$, $g_{1,9} = g_{2,5} = g_{3,5} = g_{4,5} = \langle 1,2,4,5\rangle$, $g_{2,2} = g_{4,4} = \langle 0,1\rangle$, $g_{2,6} = g_{4,8} = \langle 0,1,4\rangle$, $g_{2,7} = \langle 0,1,2,3,4\rangle$, $g_{2,8} = \langle 1,4\rangle$, $g_{2,9} = \langle 0,2,3,4\rangle$, $g_{3,6} = \langle 3,4\rangle$, $g_{3,7} = \langle 0,1,3,5\rangle$, $g_{3,8} = \langle 2\rangle$, $g_{3,9} = \langle 2,3,5\rangle$, $g_{4,6} = \langle 0,1,2,3\rangle$, $g_{4,7} = \langle 0,1,2,5\rangle$, $g_{4,9} = \langle 0,2,4\rangle$, $g_{5,5} = g_{7,7} = g_{9,9} = \langle 0,6\rangle$, $g_{6,6} = g_{6,7} = g_{8,8} = g_{8,9} = \langle 0,1,2,3,4,5\rangle$
10	40	20	8	$g_{1,1} = g_{2,2} = g_{3,3} = g_{4,4} = g_{5,5} = g_{3,6} = g_{5,8} = \langle 0\rangle$, $g_{1,6} = g_{3,8} = g_{5,10} = \langle 0,1\rangle$, $g_{1,7} = g_{1,9} = g_{2,10} = g_{4,10} = g_{5,6} = \langle 2,3\rangle$, $g_{1,8} = g_{2,7} = g_{3,10} = g_{4,9} = \langle 1,2\rangle$, $g_{1,10} = g_{4,6} = g_{5,7} = \langle 3\rangle$, $g_{2,6} = g_{5,9} = \langle 0,1,2\rangle$, $g_{2,8} = g_{3,9} = \langle 1\rangle$, $g_{2,9} = g_{4,7} = \langle 2\rangle$, $g_{3,7} = g_{4,8} = \langle 0,2,3\rangle$, $g_{6,6} = g_{7,7} = g_{8,8} = g_{9,9} = g_{10,10} = \langle 0,4\rangle$

- 反転不変性と自己双対性とのある種の関係を示す
- Best possibleな反転不変かつ自己直交な準巡回符号を計算機により多数発見
- 電子情報通信学会論文賞（2022年6月9日受賞）

整数符号に対する反転不変性と自己双対性

N. Ojiro, H. Matsui, "Construction of reversible integer codes with large moduli via Chinese remainder theorem," International Symposium on Information Theory and Its Applications (ISITA2022), pp.188-192, Oct. 19 (Oct. 17-19), 2022.

（反転不変符号）

We denote by ${}^{\mathrm{r}}\{G\}_m$ the set consisting of reversible codes contained in $\{G\}_m$.

Lemma 2. *Let $m, m_1, m_2, \alpha, \beta$ be as in Proposition 1. Then the restriction maps*

$$\alpha : {}^{\mathrm{r}}\{G\}_{m_1} \times {}^{\mathrm{r}}\{G\}_{m_2} \longrightarrow {}^{\mathrm{r}}\{G\}_m$$
$$\beta : {}^{\mathrm{r}}\{G\}_m \longrightarrow {}^{\mathrm{r}}\{G\}_{m_1} \times {}^{\mathrm{r}}\{G\}_{m_2}$$

are bijections with $\alpha^{-1} = \beta$.

The iteration of Lemma 2 brings the following theorem:

Theorem 1. *Let α be as in Proposition 1 and $m = \prod_{i=1}^{r} p_i^{a_i}$ is a prime factorization in $\mathbb{Z}$, where $p_i \neq p_j$ for $i \neq j$. Then α induces a bijection from ${}^{\mathrm{r}}\{G\}_{p_1^{a_1}} \times \cdots \times {}^{\mathrm{r}}\{G\}_{p_r^{a_r}}$ to ${}^{\mathrm{r}}\{G\}_m$.*

Let $l = 4$ and $m = p_1^a \times p_2^b$, where $p_1, p_2 \in \{2, 3, 5, 7\}$ and $a, b \in \{1, 2, 3\}$ with $a, b \leq 2$ if $p_i = 7$. The computing result for (m, S_m, d) except the case where $S_m = 0$ is as follows:

TABLE III
THE NUMBERS OF ${}^{\mathrm{rd}}\{G\}_m$ FOR $l = 4$ AND THE MAXIMUM OF THEIR MINIMUM LEE WEIGHTS

m, p_1^a, p_2^b	$S_m, S_{p_1^a}, S_{p_2^b}$	d	m, p_1^a, p_2^b	$S_m, S_{p_1^a}, S_{p_2^b}$	d
$10, 2, 5$	$12, 3, 4$	6	$200, 2^3, 5^2$	$27, 3, 9$	28
$18, 2, 3^2$	$3, 3, 1$	6	$225, 3^2, 5^2$	$9, 1, 9$	27
$20, 2^2, 5$	$12, 3, 4$	8	$245, 5, 7^2$	$4, 4, 1$	21
$36, 2^2, 3^2$	$3, 3, 1$	12	$250, 2, 5^3$	$48, 3, 16$	30
$40, 2^3, 5$	$12, 3, 4$	12	$441, 3^2, 7^2$	$1, 1, 1$	21
$45, 3^2, 5$	$4, 1, 4$	9	$500, 2^2, 5^3$	$48, 3, 16$	44
$50, 2, 5^2$	$27, 3, 9$	14	$1000, 2^3, 5^3$	$48, 3, 16$	60
$72, 2^3, 3^2$	$3, 3, 1$	12	$1125, 3^2, 5^3$	$16, 1, 16$	63
$98, 2, 7^2$	$3, 3, 1$	14	$1225, 5^2, 7^2$	$9, 9, 1$	63
$100, 2^2, 5^2$	$27, 3, 9$	20			
$196, 2^2, 7^2$	$3, 3, 1$	28			

Example 6. The Leech lattice has a generator matrix $G/\sqrt{8}$, where

$$G = \begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&5\\
0&2&0&0&0&0&0&2&0&0&0&2&0&2&0&0&0&2&0&0&2&2&2&0\\
0&0&2&0&0&0&0&2&0&0&0&2&0&0&2&0&0&0&2&0&0&2&2&2\\
0&0&0&2&0&0&0&2&0&0&0&2&0&0&0&2&0&2&2&2&2&0&0&0\\
0&0&0&0&2&0&0&2&0&0&0&0&0&2&2&0&0&0&2&2&2&0&2&0\\
0&0&0&0&0&2&0&2&0&0&0&0&2&0&2&0&0&2&0&0&2&2&0&2\\
0&0&0&0&0&0&2&2&0&0&0&0&0&2&2&0&2&0&2&0&2&2&2&0\\
0&0&0&0&0&0&0&4&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4\\
0&0&0&0&0&0&0&0&2&0&0&2&0&2&2&0&0&2&2&0&2&2&0&2\\
0&0&0&0&0&0&0&0&0&2&0&2&0&2&0&2&0&2&0&2&2&0&2&2\\
0&0&0&0&0&0&0&0&0&0&2&2&0&0&2&2&0&2&2&0&0&2&2&2\\
0&0&0&0&0&0&0&0&0&0&0&4&0&0&0&0&0&0&0&0&0&0&0&4\\
0&0&0&0&0&0&0&0&0&0&0&0&2&2&2&2&0&0&0&2&2&2&2&2\\
0&0&0&0&0&0&0&0&0&0&0&0&4&0&0&0&0&0&0&0&0&0&0&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&4&0&0&0&0&0&0&0&0&0&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&0&0&0&0&0&0&0&0&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&2&2&2&2&2&2&2&2&2\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&0&0&0&0&0&0&0&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&0&0&0&0&0&0&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&0&0&0&0&0&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&0&0&4&0&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&0&4&0&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&4&0&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&4&4\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&8
\end{pmatrix},$$

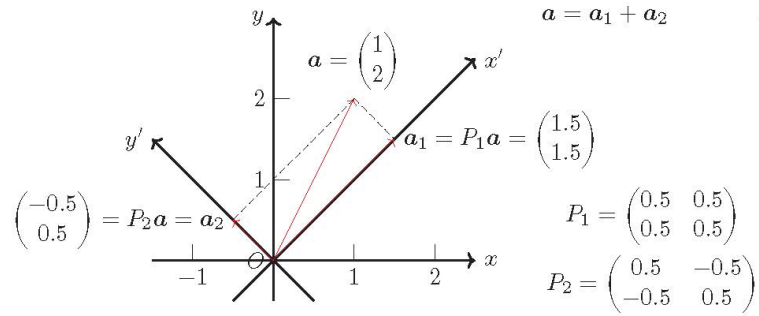
(cf. [3, Figure 4.12 of Chapter 4]). Then $AG = 8I$ for some $A \in M_{24}(\mathbb{Z})$, and so G is a self-dual code over $\mathbb{Z}/8\mathbb{Z}$ of length 24. In fact, it is known that G is an extremal Type II code over $\mathbb{Z}/8\mathbb{Z}$ of length 24, see [1, Section 4].

- 反転不変かつ自己双対な整数符号に対する中国剰余定理を用いた構成
- 「格子」との関係を示し，Leech格子等の有名な格子との関係を記述
- 4角および6角格子上の符号に対する一般化についても現在研究中

べき等元（射影分解）を用いた効率化

兼子駿，松井一，“反転不変かつ自己双対な準巡回符号に対するべき等元を用いた構成,” 第45回情報理論とその応用シンポジウム，pp.211-216，11月30日（11月29日-12月2日），2022.

（反転不変符号）



射影行列 P について，以下の 3 つを満たす．

1. $P_i P_i = P_i \ (i = 1, \cdots, m)$
2. $P_i P_j = O \ (i \neq j)$
3. $P_1 + \cdots + P_t = I$

図：ベクトルの射影分解（べき等元と類似）

Algorithm 1 べき等元を用いた QC 符号の構成方法

Input: $f, f_1, f_2 \in R$ s.t. $f = f_1 f_2$ and $\gcd(f_1, f_2) = 1$.
G_i s.t. $A_i G_i = f_i I \ (i = 1, 2)$.

Output: a generator matrix $\mathcal{B}$

for $i = 1$ to 2 do
  b_i s.t. $f_i a_i + (f/f_i) b_i = 1$
  $e_i \equiv (f/f_i) b_i \mod f \quad (\deg(e_i) < \deg(f))$
  Transform $e_i G_i$ to a generator matrix $\mathcal{B}_i$ via Remark 2
end for
$\mathcal{B} = \begin{pmatrix}\mathcal{B}_1\\\mathcal{B}_2\end{pmatrix}$

補題 1. $e_1, \cdots, e_t$ は以下の性質を持つ．

(i) $e_i e_i \equiv e_i \mod f$,
(ii) $e_i e_j \equiv 0 \mod f \ (i \neq j)$,
(iii) $e_1 + e_2 + \cdots + e_t = 1$.

表：B_1の最小重みごとの個数

l	$w_{\max}$	最小重みごとの個数											
		1	2	3	4	5	6	7	8	9	10	11	12
2	2	0	0	0	0	0	1						
4	4	0	0	0	0	0	3						
6	4	0	0	0	0	0	7						
8	8	0	0	0	0	0	25	0	0	0	0	0	14
10	6	0	0	0	0	0	151						

表：B_2の最小重みごとの個数

l	$w_{\max}$	最小重みごとの個数							
		1	2	3	4	5	6	7	8
2	2	0	0	0	3				
4	4	0	0	0	15				
6	4	0	0	0	81	0	0	0	54
8	8	0	0	0	1161	0	0	0	1134
10	6	0	0	0	28593	0	0	0	47142

- べき等元を用いて，中国剰余定理を用いた方法と同値な方法を確立
- “ローカル”な生成行列の最小重みを調べやすく探索候補を絞り込み易い
- 今後の課題として，符号の同型による同値類を用いた更なる高速化を行う

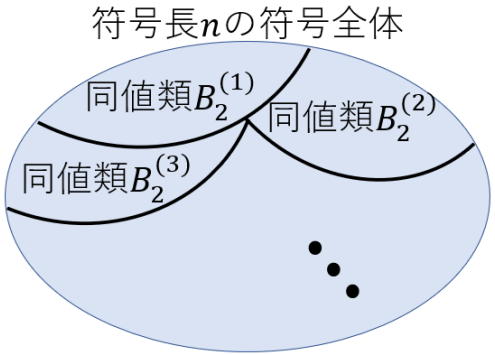
符号の同型を用いた効率化

平井智史，兼子駿，松井一，“反転不変かつ自己双対な準巡回符号の構成における自己同型群を用いた効率化，” 第45回情報理論とその応用シンポジウム，ポスター発表，12月1日（11月29日-12月2日），2022.

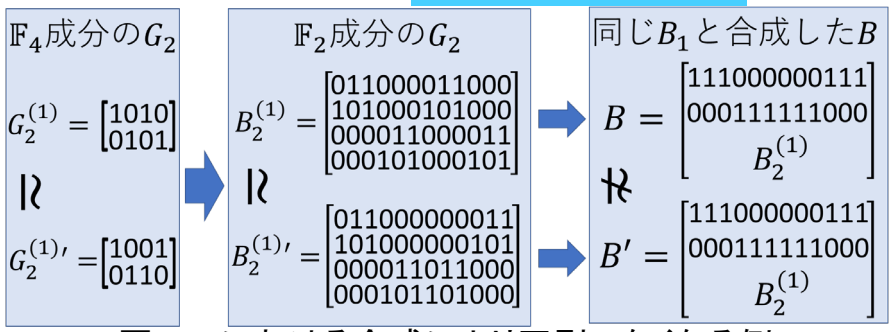
（反転不変符号）

$$B' = SBM$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



図：同型による符号の同値類への分類



図：l=4における合成により同型でなくなる例

表：構成した最小重みごとの生成行列Bの個数

従来の手法（B_2の全て）				
$l \setminus d$	2	4	6	8
2	1	0	0	0
4	1	1	0	0
6	2	1	0	0
8	3	**11**	1	1
10	**16**	**26**	8	0

本手法（B_2の同値類）				
$l \setminus d$	2	4	6	8
2	1	0	0	0
4	1	1	0	0
6	2	1	0	0
8	3	**10**	1	1
10	**13**	**24**	8	0

- 反転不変かつ自己双対な準巡回符号の構成の更なる効率化を目指す
- 同型による同値類（同型類）に含まれる符号は同じ最小重みをもつことを利用
- 自己同型群を用いて同型類の中から反転不変なものを見つける手法を開発中

情報通信研究室：活動報告

研究室代表者・准教授　松井　一

2nd スマート情報技術研究センターシンポジウム
2022年12月1日（木）16:00-16:15

ご清聴ありがとうございました.