情報通信研究室：活動報告

研究室代表者・准教授　松井　一

3rd スマート情報技術研究センター シンポジウム
19th ジョイントCSセミナー

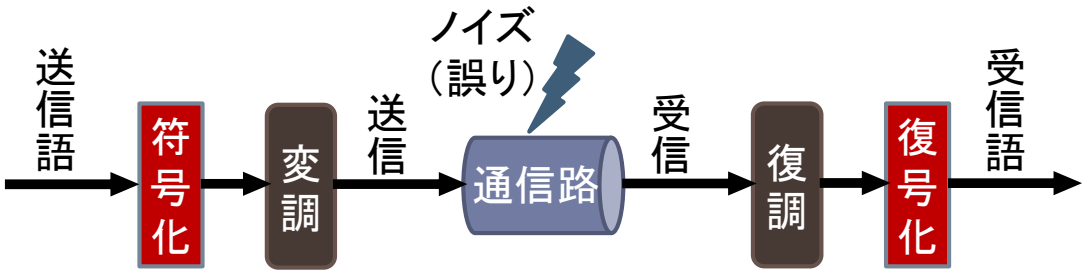
2023年10月12日（木）16:25-16:35

○目標

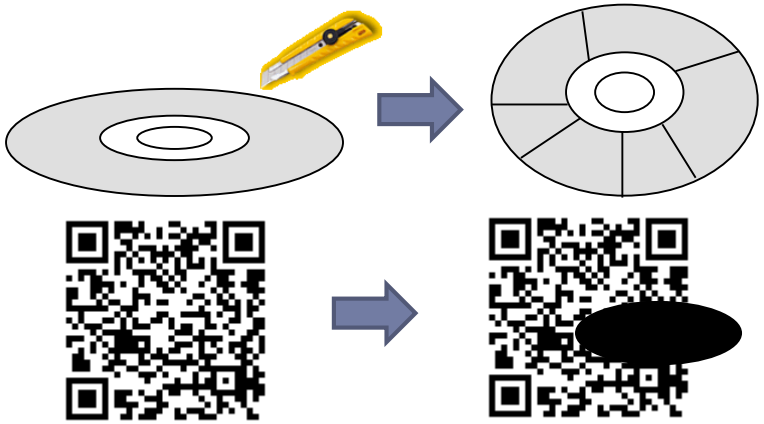
- 高性能な誤り訂正符号の構成
  - DNA記録や量子コンピューターなどへの応用

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

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）	2006年にシャノン限界に迫ることが判明
1993	Turbo符号（C. Berrou）	シャノン限界に迫る
1995	Shor符号（A.R. Calderbank, P. Shor）， Steane符号（A. Steane）	初の量子誤り訂正符号
2006	Polar符号（E. Arikan）	5Gに採用される

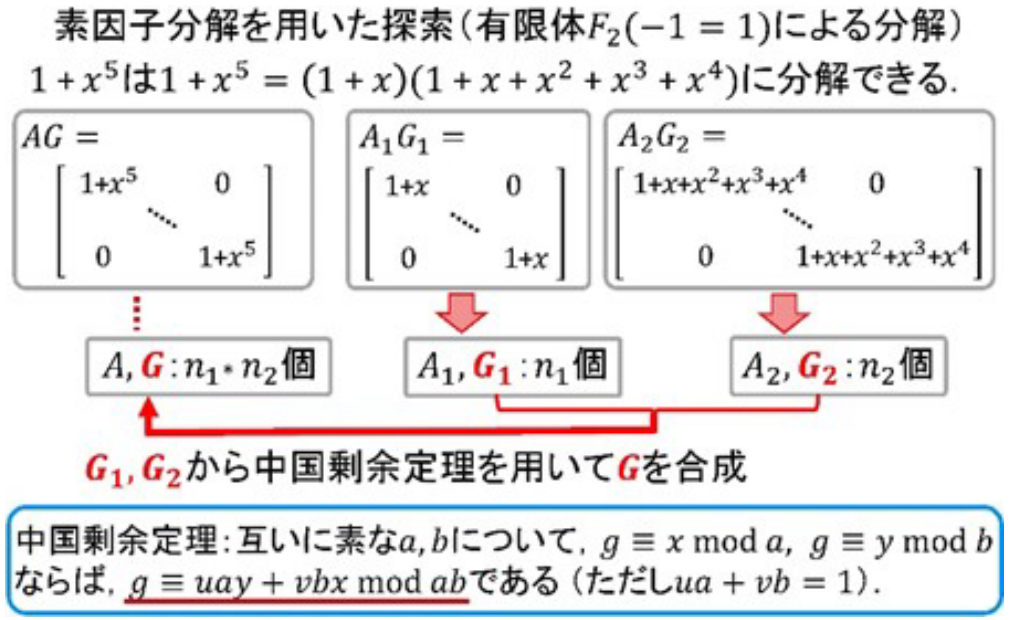
DNA記録・DNAストレージ…DNAに数ギガ～数テラ～数ペタの情報を記録
反転不変符号…DNA符号が満たすべき条件のひとつ，Reversibility（反転不変性）に注目

報告内容

- 誤り訂正符号における構成・探索
- 反転不変符号・DNA符号
- 量子誤り訂正符号

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.



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

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

$$g_{i,j} = \sum_{k=i}^{j} b_{i,k}^{(1)} g_{k,j}^{(1)} = \sum_{k=i}^{j} b_{i,k}^{(2)} g_{k,j}^{(2)}. \tag{1}$$

$$g_{i,j} \equiv u g_{j,j}^{(1)} \sum_{k=i}^{j-1} b_{i,k}^{(2)} g_{k,j}^{(2)} + v g_{j,j}^{(2)} \sum_{k=i}^{j-1} b_{i,k}^{(1)} g_{k,j}^{(1)} \mod g_{j,j}. \tag{2}$$

- 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

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.

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

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

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）

正方・6角格子上の自己双対符号の構成

H. Matsui, "An algorithm for finding self-orthogonal and self-dual codes over Gaussian and Eisenstein integer residue rings via Chinese remainder theorem," IEEE Access, vol.11, pp.23260-23267, Mar. 6, 2023.

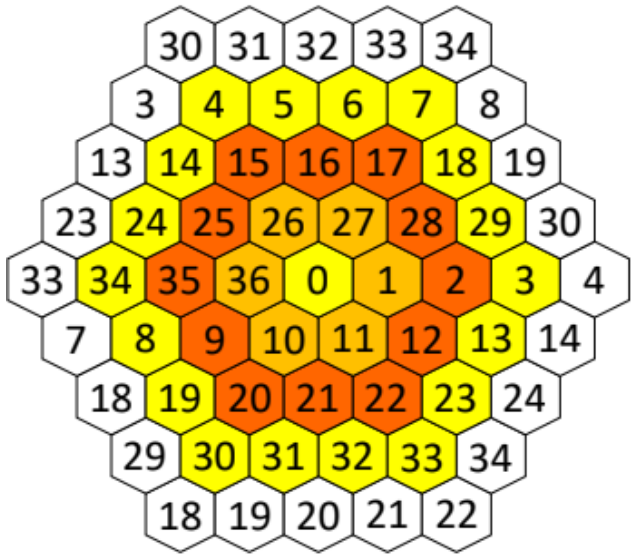


図. 6角格子上のリー距離

Example 9: All self-dual R-modules $\mathbb{L}G/6\mathbb{L}$ are derived from self-dual R-modules $\mathbb{L}G_1/2\mathbb{L}$ and $\mathbb{L}G_2/3\mathbb{L}$ by $\mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2$. We compute G with $G_1 = \begin{pmatrix} 1 & 1+\omega \\ 0 & 2\omega \end{pmatrix}$ and $G_2 = \begin{pmatrix} -2-\omega & 0 \\ 0 & -2-\omega \end{pmatrix}$. If $\mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2$, then

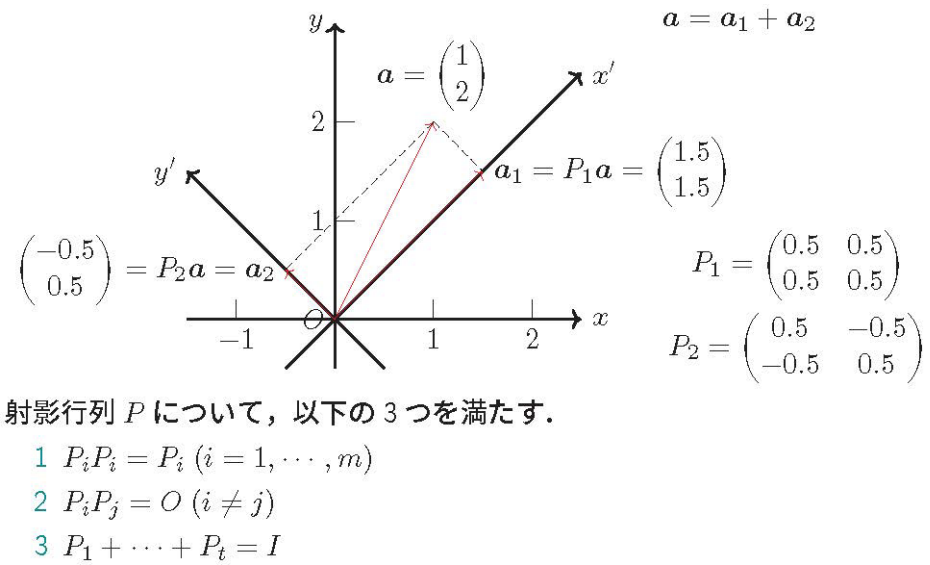
$$G = G_1 G_2 = \begin{pmatrix} -2-\omega & -1-2\omega \\ 0 & 2-2\omega \end{pmatrix},$$

$$AG = \begin{pmatrix} -2+2\omega & -1-2\omega \\ 0 & 2+\omega \end{pmatrix}\begin{pmatrix} -2-\omega & -1-2\omega \\ 0 & 2-2\omega \end{pmatrix} = 6I.$$

- （背景）正方・6角格子上のリー距離誤り訂正符号において近年進展あり
- 中国剰余定理を利用した自己双対符号のlocal→globalな構成が可能
- この種の符号を量子誤り訂正に応用したという報告あり

量子誤り訂正符号の構成

兼子駿，松井一，“準巡回性をもつLCD符号を用いたEAQECCの構成,” 第46回
情報理論とその応用シンポジウム，11月28日-12月1日，2023.（発表予定）



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）

表 1: $m = 3, 5, 7, 9$ における QC-LCD 符号から作られる EAQECC の最小重み

m	l \ k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
3	2	3	3	2	2	1	1																					
	3	9	6	3	4	3	2	2	2	1																		
	4	9	6	6	4	4	4	3	2	2	2	1	1															
5	2	5	5	–	4	3	3	–	2	1	1																	
	3	15	10	5	6	5	6	4	4	4	3	2	2	2	2	1												
	4	15	10	5	10	9	8	5	6	6	6	5	4	4	4	3	2	2	2	1	1							
7	2	7	7	–	–	–	4	4	3	–	–	–	2	1	1													
	3	21	14	7	–	–	8	7	7	6	–	–	4	4	4	3	–	–	2	2	2	1						
9	2	9	9	6	6	3	6	6	6	5	4	3	3	2	2	2	2	1	1									
	3	27	18	9	12	9	12	10	10	9	9	8	6	6	6	6	6	5	4	4	4	3	2	2	2	2	2	1

※下線は既存の最小重みと一致，上線は既存の最小重みを改良．

- LCD（linear complementary dual）符号によるエンタングルメント支援
  量子誤り訂正符号（EAQECC）の構成を行った
- 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
- 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

情報通信研究室：活動報告

研究室代表者・准教授　松井　一

3rd スマート情報技術研究センター シンポジウム
19th ジョイントCSセミナー

2023年10月12日（木）16:25-16:35

ご清聴ありがとうございました.