誤り訂正符号の原理と応用について

溝口, 佳寛
九州大学マス・フォア・インダストリ研究所

出版情報：pp.1-80, 2024-07-28
バージョン：
権利関係：

誤り訂正符号の原理と応用について

溝 口 佳 寛

九州大学マス・フォア・インダストリ研究所

http://imi.kyushu-u.ac.jp/~ym/

2024 年 7 月 28 日 (日)

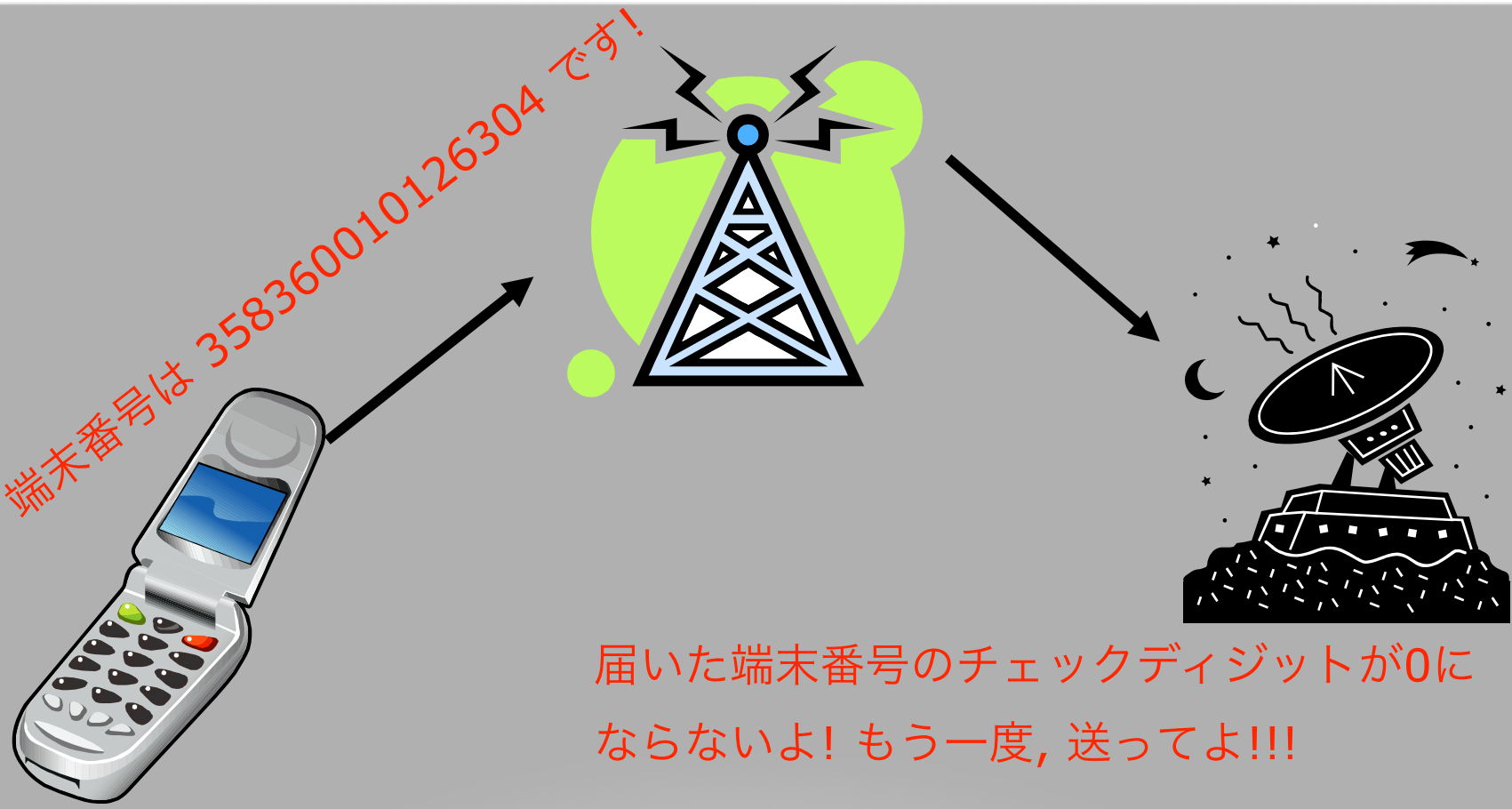
「九州大学未来創成科学者育成プロジェクト（QFC-SP）」
QFC-SP プライマリーコース 講義配布資料 (抜粋)

https://qfcsp.kyushu-u.ac.jp/

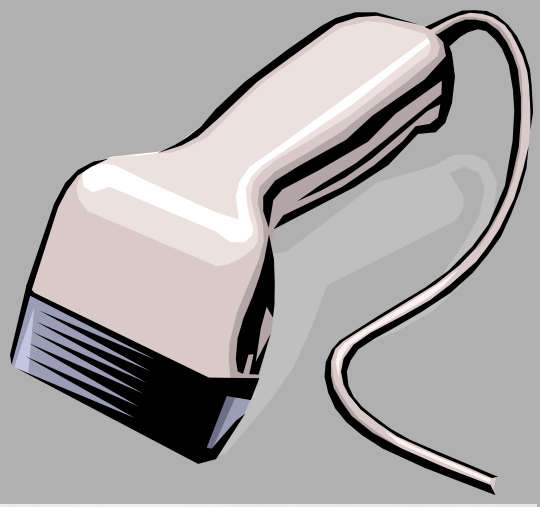
目次

[1] はじめに

なぜ, 誤り訂正符号が必要なのか?



通信中に周囲の環境によって電波障害が起き、いつも正確なデータが届くとは限りません。正しく届いたか、誤った数字なのかを判断出来る手段は、情報通信において非常に重要な役割を果たします。



スーパーのレジで正しくバーコードが読み込めると、ピッと音がします。どうやって正しく読み込んだことが、わかるのでしょうか？

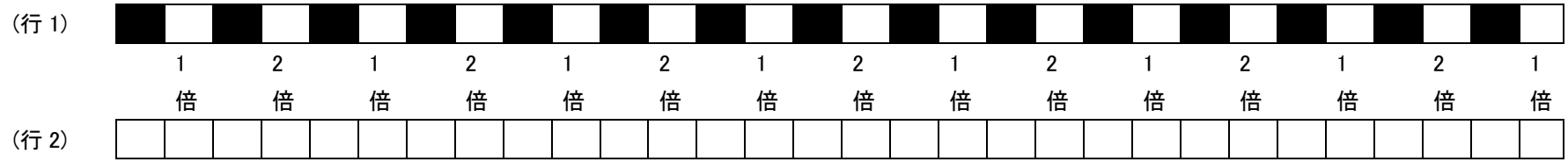
読み込めないときは、何度も読み込み操作を繰り返します。

誤った金額が入ることを防いでいます。

誤りを検出する計算の仕組みが使われています。

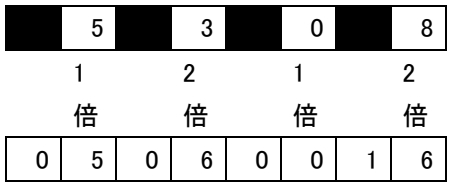
携帯電話機のIMEI番号のチェックディジット

携帯電話で ＊＃０６＃ に電話をかけてみて下さい。
大丈夫です。どこにも電話は、かかりません。あなたの携帯電話固有の１５桁の製品番号が画面に表示されるだけです。
さあ、この１５桁で、あなたの運命が、わかります。



Step 1: (行 1)の 15 個の白います目の中に表示された１５桁の数字を *表示された通りに* 左から順番に入れて下さい。
Step 2: (行 1)のます目の下にある指示に従って数字を 1 倍(そのまま), あるいは, 2 倍します. 結果は(行 2)の 1 つの結果 2 つのます目を使って
数字 1 つずつ入れます. 結果が 2 桁にならないときは上の位のます目には 0 を入れます。
下図の例を参照して下さい。５は１倍すると０と５に、８は２倍すると１と６になります.

(例)



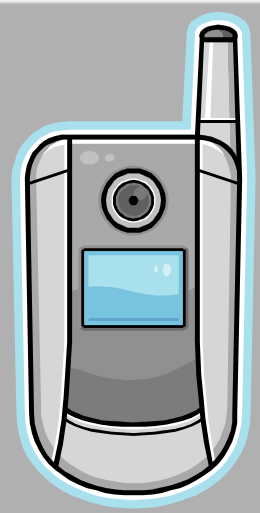
… + 0 + 5 + 0 + 6 + 0 + 0 + 1 + 6 + …

Step 3: (行 2)の各ます目の３０個の１桁の数字を全て加えます。そして、その総和の１の位の数で占いをします。
１の位の数字が少ないほどラッキーです。すなわち、１の位が 0 になると「大吉」です。

あなたの結果は、　　合計　＝　＿＿＿＿＿＿＿＿　　１の位の数　＝　＿＿

人工衛星からの画像などの通信においては、途中でエラーが起きたからといって、何度も同じデータを送ることは難しいのです。
そこで、データのエラーを基地局側で修復可能なデータを送る仕組みが必要です。そこに新たな計算の仕組みが出てきます。

誤り訂正符号化技術にも計算の仕組みが必要です。


携帯電話で使われるバーコード
(QRコード)では誤り訂正の計算
の仕組みが組み込まれています.

汚れても読めるバーコードや傷ついても音が悪くならない
音楽CDでは, 誤り訂正符号の計算の仕組み使われています.

「数学」の社会との関わりは「算数」で学ぶ (1/2)

幼稚園の算数「数」の**概念**を理解する
積み木の数を数えることができる
1から10まで数えることができる

小学生の算数「数」の**性質**を理解する
数そのものを対象に計算ができる
1から100まで数えることができる

中学生の数学「数」の性質を導ける
数そのものが持つ性質が理解できる
1から10000まで数えることができる
※実際に数えなくても「数えることができる」
と理解している.「**数学**」**の理解とは？**

大きな数を数えたり計算したりするのは,
コンピューターを使って良い. 使うべき!
計算するのはコンピューターでも「計算できる」
と理解できていることが, とても大切！

「数学」の社会との関わりは「算数」で学ぶ (2/2)

幼稚園：算数「数」の**概念**を理解する
積み木の数を数えることができる
1から10まで数えることができる

有限体 $F(2)$，$F(4)$ の計算

小学生：算数「数」の**性質を理解**する
数そのものを対象に計算ができる
1から100まで数えることができる

有限体 $F(8)$，$F(11)$ の計算

中学生：数学「数」の**性質を導ける**
数そのものが持つ性質が理解できる
1から10000まで数えることができる
※実際に数えなくても「数えることができる」
と**理解**している．**「数学」の理解とは？**

大きな数を数えたり計算したりするのは，
コンピューターを使って良い．使うべき！
計算するのはコンピューターでも「計算できる」
と理解できていることが，とても大切！

有限体 $F(256)$，QRコードの計算

[2] 有限体の例

符号を実現する「数」の集合 = 有限体

「体」とは,

- **体** とは, 逆元の存在や分配法則等の規則が成り立つ
  四則演算 $(+,\times,-,\div)$ を備えた**集合**である. (※ 厳密な**体**の定義は, 別途, 文献を参照して下さい!)
  - **N**(自然数) : $+$ と $\times$ 演算の逆元がない!
    (例. $2+x=1$, $2\times x=3$ が解けない. 自然数 x が存在しない.)
  - **Z**(整数) : 四則演算を備えているが, $\times$ 演算の逆元がない!
    (例. $2\times x=3$ が解けない. 整数 x が存在しない.)
  - **Q** (有理数) : 体! (例. $2\times x=3$ の解 $x=\dfrac{3}{2}$ は有理数.)
  - **R** (実数) : 体!
  - $\mathbf{C}=\{a+bi \mid a,b\in R\}$: 複素数 (体)
  - $\mathbf{H}=\{a+bi+cj+dk \mid a,b,c,d\in R\}$: 四元数体 (非可換)
  - $\mathbf{F}(p)=\{0,1,\cdots,p-1\}$: p が素数のとき有限体!
  - $\mathbf{F}(p^n)=\{0,1,\cdots,p-1\}$: 位数 p^n の有限体 (拡大体)!
  - $\cdots$

「有限体」の理論を勉強したい! (ポイント!)

- 体は, 四則演算 (+,-,x, ÷) ができる!
- -(引き算) は, +(足し算) の逆演算である.
- ÷ (割り算) は, x(掛け算) の逆演算である.
- 「符号」とは「情報源」に演算を施して作られる.
- 「逆演算」は「符号」の逆操作「復号」に必要!
- 情報通信に利用する「情報源」は有限個である.
  (cf. ひらがな, 五十音, アルファベット, 26 文字, ...)

以上より,

逆演算計算ができる「体」が必要.
そして, 有限個の要素の「体=(有限体)」を使うと効率が良い.

有限体 $F(2) = \{0, 1\}$

次のように演算 $+$, $\times$ を定義すると, $F(2)$ は体になる. o

和: $x + y \pmod 2$　　積: $x \times y \pmod 2$

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

例:

$1 + x = 0$ の解は, $x = 0 - 1 = 1$.

※ 体の厳密な定義を省略しているが,
$+$ と $\times$ の演算は,
分配法則 $a \times (b + c) = (a \times b) + (a \times c)$ などを
満たさなければならない.

有限体 $F(3) = \{0, 1, 2\}$

次のように演算 $+$, $\times$ を定義すると, $F(3)$ は体になる.

和: $x + y \pmod 3$　　積: $x \times y \pmod 3$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

例:

$1 + x = 0$ の解は, 演算表より $x = 0$.

$2 \div x = 2$ の解は, $2 = 2 \times x$ の解で, 演算表より $x = 1$

有限体 $F(5) = \{0, 1, 2, 3, 4\}$

和: $x + y \pmod 5$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

積: $x \times y \pmod 5$

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

※ 素数 p に対して,
$+$ と $\times$ を (mod p) で定義すると F(p) は体になる!

[2] 有限体 $F(2^k)$ の演算 (k=2 の例で)

符号を実現する「数」の集合 = 有限体
要素数が 2^k だと電子回路で実現しやすい!

8bit コンピュータ, 32bit コンピュータ, 64bit コンピュータ, ...

※ 有限体 $F(2^k)$ で, $k \geqq 2$ のときの演算定義は簡単ではない!!

有限体(?!) $F(4) = \{0, 1, 2, 3\}$?

和: $x + y \pmod 4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

積: $x \times y \pmod 4$

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	1	2
3	0	3	2	1

$x \times 2 = 2$ が解けない! $(x = 1??\ \ x = 3??)$

※ 上記の積 $(\times)$ の定義では, F(4) は体にならない!

有限体 $F(4)' = \{0, 1, \alpha, \alpha^2\}$ (その1)

$F(4)'$ の4つの元を 0, 1, α, α^2 と書いて,
$F(4)'$ が体となるように, ?のマスの値を決めたい!

和: $x + y \pmod 4$

積: $\times\times y \pmod 4$

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	?	?	?
α	α	?	?	?
α^2	α^2	?	?	?

$\times$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	?	?
α^2	0	α^2	?	?

演算 $+$, $\times$ を上手に定義したい!!

※ 逆元が存在するように「上手に」定義するとは, 同じ行, 同じ列に**同じ値**が出てこないこと!

有限体 $F(4)' = \{0, 1, \alpha, \alpha^2\}$ (その2)

和: $x + y \pmod 4$

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

積: $x \times y \pmod 4$

$\times$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

※ $\alpha^2 + \alpha + 1 = 0$ を仮定すると, 上記の $+$, $\times$ が**上手に**定義でき,

F(4)' は体になる!

$0 + 0 = 0$, $1 + 1 = 0$, $\alpha + \alpha = 0$, $\alpha^2 + \alpha^2 = 0$, $\alpha \times \alpha = \alpha^2$,
$\alpha^2 = \alpha + 1$, $\alpha = \alpha^2 + 1$, $\alpha^2 + \alpha = 1$,
$\alpha^3 = \alpha(\alpha^2) = \alpha(\alpha + 1) = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1$,
$\alpha^2 \times \alpha^2 = (\alpha + 1)(\alpha + 1) = \alpha^2 + 1 = \alpha$.

有限体 $F(4)'' = \{0, 1, x, x+1\}$ (その 3)

m 次の既約多項式 $f(x)$ を 1 つ定めたとき, 位数 2^m の有限体を係数が $F(2)$ の元である多項式を $f(x)$ で割った余りの剰余多項式で定める.

以下, $m = 2$ の**既約多項式** $f(x) = x^2 + x + 1$ の例で考える.

$f(x)$ で割った余りの多項式は, 0, 1, x, $x+1$ の 4 つになる. 和 $(+)$ や積 $(\times)$ は, 多項式の和や積を考え, $f(x)$ で割った余りの多項式とする.

- $x \times (x+1) = x^2 + x = (x^2 + x + 1) - 1 = (x^2 + x + 1) + 1 = 1$
- $(x+1) \times (x+1) = x^2 + 2x + 1 = (x^2 + x + 1) + x = x$
- $x \times x = x^2 = (x^2 + x + 1) + (x + 1) = x + 1$

和: $x + y \pmod 4$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

積: $x \times y \pmod 4$

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

有限体 $F(4)'' = \{0, 1, x, x+1\}$ (その 4)

和: $x + y \pmod 4$

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$+$	$\alpha^3 = 0$	$\alpha^0 = 1$	α	α^2
$\alpha^3 = 0$	0	1	α	α^2
$\alpha^0 = 1$	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

積: $x \times y \pmod 4$

$\times$	0	1	x	$x+1$
0	0	0	0	0
10	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$\times$	$\alpha^3 = 0$	$\alpha^0 = 1$	α	α^2
$\alpha^3 = 0$	0	0	0	0
$\alpha^0 = 1$	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

$a, b \in \{0, 1\}$ に対して, $ax + b$ を考える時, 多項式 $\{0, 1, x, x+1\}$ を表す (a, b) は, それぞれ, $\{(0,0), (0,1), (1,0), (1,1)\}$ となる.

$\alpha^0 = 1$, $\alpha^1 = x$, $\alpha^2 = x + 1$,$\alpha^3 = 0$ とすると
$\alpha^i \times \alpha^j = (a_i x + b_i)(a_j x + b_j) = a_k x + b_k = \alpha^k$ と対応している.

※ $\alpha^k = (l, m)$ の対応は, lm を 2 進数と考えたときの値が k であることにも注意!

【余談】九大数学入試問題 (2000 年理系) より

【1】 係数が 0 か 1 である x の整式を, ここでは, M 多項式と呼ぶことにする。整数を係数とする x の正式は, 偶数の係数を 0 でおきかえ, 奇数の計数を 1 でおきかえると M 多項式になる。2 つの整式は, このおきかえによって等しくなるとき合同であるという。たとえば、$5x^2+4x+3$ と x^2-1 とは対応する M 多項式がともに x^2+1 となるので, 合同である.
M 多項式は, 2 つの 1 次以上の M 多項式の積と合同になるとき可約であるといい, 可約でないとき既約であるという。たとえば, x^2+1 は $(x+1)^2$ と合同であるから, 可約である。

(1) x^2+x+1 は既約な M 多項式であることを示せ。

(2) 1 次から 3 次までの既約な M 多項式を全て求めよ。

(3) x^4+x+1 は既約な M 多項式かどうか判定せよ。

※ F'(4) を作るときに, 2 次の既約多項式 $\alpha^2+\alpha+1$ を利用した.
4 次の既約多項式 $\alpha^4+\alpha+1$ で, 有限体 F(2^4)=F(16) を作ることができる!

【余談】つづき (1)

$F(2)$ 係数の多項式と 2 進数表示の自然数とは, 1:1 に対応する.
自然数の列挙に対応して, $F(2)$ 係数の多項式を列挙できる.

自然数	2 進数表示	多項式
0	0000	0
1	0001	1
2	0010	x
3	0011	$x+1$
4	0100	x^2
5	0101	x^2+1
6	0110	x^2+x
7	0111	x^2+x+1
8	1000	x^3
9	1001	x^3+1
10	1010	x^3+x
$\vdots$	$\vdots$	$\vdots$

【余談】つづき (2) 【未完成】

$F(2)$ 係数の多項式と 2 進数表示の自然数とは, 1:1 に対応する.
$F(2)$ での多項式の積の一覧表を見れば, 例えば, x^4+x+1 が, $F(2)$ 係数の既約多項式かどうか判別するには, 定数項 1 を持つ 3 次以下の多項式の積を全て調べれば良い.

積	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1	$\cdots$
0	0	0	0	0	0	0	0	0	
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1	$\cdots$
x	0	x							
$x+1$	0	$x+1$	x^2+x	x^2+1	x^3+x^2	x^3+x^2+x+1	x^3+x	x^3+1	
x^2	0	x^2	x^3	x^3+x^2	x^4	x^4+x^2	x^4+x^3	$x^4+x^3+x^2$	
x^2+1	0	x^2+1							
x^2+x	0	x^2+x							
x^2+x+1	0	x^2+x+1							
x^3	0	x^3							
x^3+1	0	x^3+1							
x^3+x	0	x^3+x							
$\vdots$	$\vdots$								

$F(2)$ 係数の m 次既約多項式 (既約な M 多項式)

各 m に対する既約多項式は, $X^{2^m-1}-1$ の約数となる.

- (m=2) X^2+X+1

  $(X^3-1)=(X+1)(X^2+X+1)$

- (m=3) X^3+X+1, X^3+X^2+1

  $(X^7-1)=(X+1)(X^3+X+1)(X^3+X^2+1)$

- (m=4) X^4+X+1, X^4+X^3+1, $X^4+X^3+X^2+X+1$

  $(X^{15}-1)=$
  $(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1)$

※ $F(2)$ 係数の多項式の積の表を既約多項式で割った剰余多項式に制限すると, 積が重複しない. すなわち, 有限の範囲の多項式たちで, 割り算が可能になる.

[4] 符号空間 (有限体上の線形空間)

符号=ベクトル=有限体の元を並べたもの

符号全体の集合=符号空間=有限体上の n 次元線形空間

ベクトルと行列を使って符号の計算を行う

行列の掛け算の復習 (1/2)

行列の掛け算の復習

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} (ae+bg) & (af+bh) \\ (ce+dg) & (cf+dh) \end{pmatrix}$$

例

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} (5+14) & (6+16) \\ (15+28) & (18+32) \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix}$$

2 進数 $F_2 = \{0, 1\}$ の加減乗除を使うとき

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} (0+0) & (1+0) \\ (0+1) & (1+1) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

2 bitのデータ $(x_1\ x_2)$ を 3 bitの符号 $(y_1\ y_2\ y_3)$ で送ると嬉しいことは！？

$$(x_1\ x_2) \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = (x_1\ x_2\ (x_1+x_2)) = (y_1\ y_2\ y_3)$$

符号間距離を2にすることができる→通信の誤りを検出できる!
→誤った情報を届けることを避ける!

行列の掛け算の復習 (2/2) 文科省高等学校数学科教材 (行列入門)

高等学校数学科教材（行列入門）

本教材は，行列の基本的な性質を学ぶために作成したものです。

行列については，平成21年告示の学習指導要領における新設科目「数学活用」の「社会生活における数理的な考察」の「数学的な表現の工夫」の内容となりました。行列は現代数学の基礎的な内容として様々な場面で活用されているにもかかわらず，繁雑な計算の意味やどのような場面で活用されるのかがわかりにくかったことから，「数学活用」の内容としたものです。ただし，「数学活用」の内容としたことから内容は大綱的に示すことになりました。そこで，専門教科理数科の「理数数学特論」の内容としてはそれ以前のもの（平成11年告示の学習指導要領における数学Cの内容）をそのまま残すとともに，高等学校数学を超える内容に興味をもつ生徒には「数学活用」の内容を踏まえ「線型代数学入門」のような学校設定科目を設けて指導することを推奨してきました。

平成30年告示の学習指導要領では数学Cを新設し，「数学活用」の各内容を科目の性格に基づいて数学A，数学B，数学Cに移行することとしました。行列を含んでいた従前の「数学活用」の「数学的な表現の工夫」の内容は科目の性格から数学Cの内容としました。数学Cで扱われる行列の内容も学習指導要領で考えられている行列の扱いも従前と比べて大きな変更はありません。

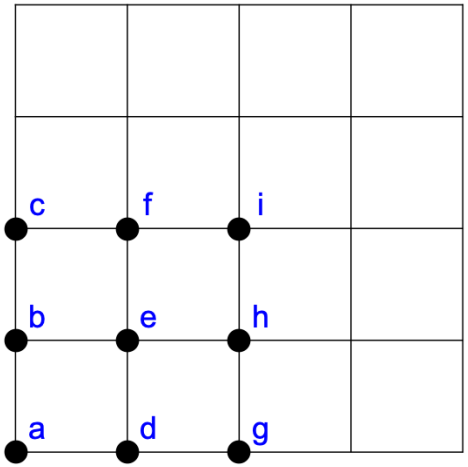
今回，AI人材育成の観点から，大学等におけるデータサイエンス教育と円滑に接続することができるよう学校設定科目等で扱うことが可能な行列の教材として数学Cの「数学的な表現の工夫」の内容も踏まえ，本教材を作成しました。しかし，本教材は，学校設定科目等だけの使用を想定しているわけではなく，行列に興味をもつ生徒が自学自習できるものとしても作成しておりますので，ぜひ本教材の積極的な活用をお願いします。

行列入門（※令和4年8月23日に更新いたしました） (PDF:2.2MB)

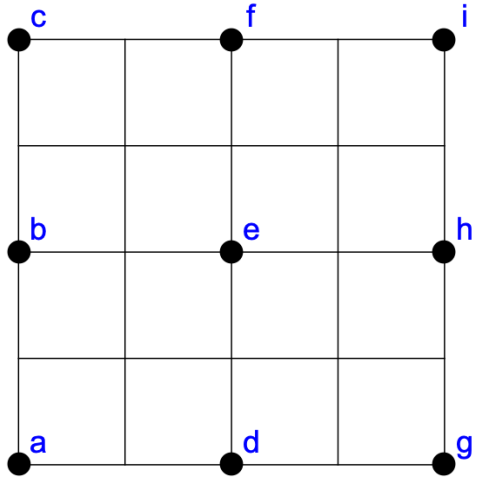
(リンク) https://bit.ly/4bSEBAH

情報源 (文字) を符号化する (1/2) 雑音による誤りを検知したい!

送信するときに, 文字 $\{a, b, c, d, e, f, g, h\}$ に数字 (x, y) を割り当て, 数字を送る.
受信するときに, 数字から, 文字に変換して認識する.



$a = (0, 0), b = (0, 1), \cdots$
$\cdots h = (2, 1), i = (2, 2)$

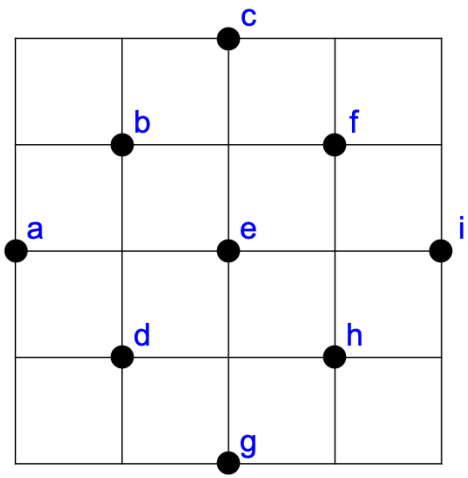


$a = (0, 0), b = (0, 2), \cdots$
$\cdots h = (4, 2), i = (4, 4)$

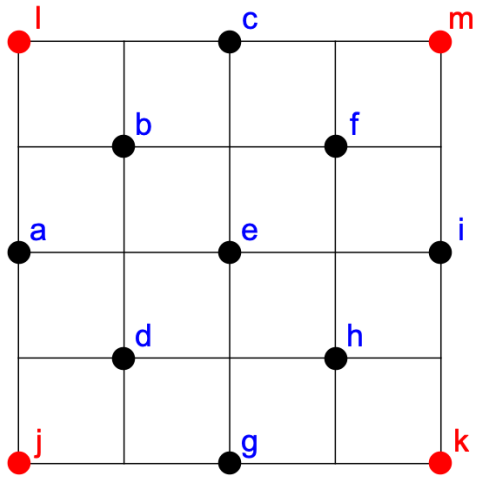
左図の数字を使うと x 座標, y 座標どちらかに雑音が入り座標が 1 ずれると別の文字として認識される. 右図の数字を使うと x 座標のどちらかが, 1 つずれた場合には, 雑音が入ったことは認識できる. しかし, 雑音が小さくても, 元の近くの座標は決定できないので, 誤り訂正は出来ない.

情報源 (文字) を符号化する (2/2) 空間内でより多くの符号使う!

送信するときに, 文字 $\{a, b, c, d, e, f, g, h\}$ に数字 (x, y) を割り当て, 数字を送る.
受信するときに, 数字から, 文字に変換して認識する.



$a = (0, 2), b = (1, 3), \cdots$
$\cdots h = (3, 1), i = (4, 2)$



$a = (0, 2), b = (1, 3), \cdots$
$\cdots h = (3, 1), i = (4, 2)$

左図の座標の特徴は, **x 座標と y 座標の和が常に偶数**となっていることである.
座標が 1 ずれると座標の和が奇数となり誤りに気がつくことが出来る. 前スライドと同様, 誤り訂正は出来ないが, 同じ格子の中の符号をより多く使うことが出来, 誤り検出が可能な点が優れる.

$F(2)$ 上の 3 次元空間 $F(2)^3$ (2 進数, 3bit) **(1/2)** $(F(2)^2 \to F(2)^3)$

$F(2)^3$ において, 4個のベクトル
a=(000), b=(011), c=(101), d=(110) だけを使うとき,
1箇所の誤りでは, 他の符号にならないので,
通信路での1箇所の誤りに気づくことができる.
{a,b,c,d}は, 3次元線型空間$F(2)^3$の2次元部分空間になっている.
(011)+(101)=(110) より, b+c=d, {a,b,c,d}の空間は2次元!
$G0 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ とするとき, $F(2)^2$= {(00), (01), (10), (11)} の元 (xy)に対して
$(x\ y)\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$を計算すると {a, b, c, d} が得られる.
この行列 $G0 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ をこの符号の生成行列という.
また, 3ビット符号で, 最小距離が2の符号であるので, (3,2)符号と言う.

$F(2)$ 上の 3 次元空間 $F(2)^3$ (2 進数, 3bit) **(2/2)** $(F(2)^2 \to F(2)^3)$

距離	000	001	010	011	100	101	110	111
000	0	1	1	2	1	2	2	3
001	1	0	2	1	2	1	3	2
010	1	2	0	1	2	3	1	2
011	2	1	1	0	3	2	2	1
100	1	2	2	3	0	1	1	2
101	2	1	3	2	1	0	2	1
110	2	3	1	2	1	2	0	1
111	3	2	2	1	2	1	1	0

距離	00	01	10	11
00	0	2	2	2
01	2	0	2	2
10	2	2	0	2
11	2	2	2	0

生成行列 $G0 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ を使って,

$(x\ y)\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = (x\ y\ x+y)$ で,

$F(2)^2 = \{(00), (01), (10), (11)\}$ の元 $(x\ y)$ に

$F(2)^3$ の元 $\{(000), (011), (101), (110)\}$ が対応する.

$(0\ 0)\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = (0\ 0\ 0),\ (0\ 1)\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = (0\ 1\ 1),$

$(1\ 0)\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = (1\ 0\ 1),\ (1\ 1)\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = (1\ 1\ 0)$

[5] 誤り訂正符号

ベクトルと行列を使って符号の計算を行う

符号化 (符号ベクトルの生成) を行う行列=生成行列

符号ベクトルの誤りを検査する行列=検査行列

$F(2)$ 上の (6,3) 符号 **(1/3)** 生成行列 G $(F(2)^3 \to F(2)^6)$

$G = \begin{pmatrix} 1&0&0&1&1&0 \\ 0&1&0&1&0&1 \\ 0&0&1&0&1&1 \end{pmatrix}$ によって定められる（6，3）符号の検査行列Hを求める．

Hは，３ｘ６行列で，Gで生成された符号（$x_1\ x_2\ x_3\ x_4\ x_5\ x_6$）全てに対して

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_5 \end{pmatrix}$$

となる行列 $H = \begin{pmatrix} 1&1&0&1&0&0 \\ 1&0&1&0&1&0 \\ 0&1&1&0&0&1 \end{pmatrix}$ である

すなわち，$H\,G^{\mathsf{T}} = O$，$\begin{pmatrix} 1&1&0&1&0&0 \\ 1&0&1&0&1&0 \\ 0&1&1&0&0&1 \end{pmatrix} \cdot \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \\ 1&1&0 \\ 1&0&1 \\ 0&1&1 \end{pmatrix} = O$ となる行列である

$(F(2)^3 \to F(2)^6)$ 計算中 (1) 生成行列 G による符号化

$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix} G = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

$(1,0,1) \in F(2)^3$ の符号 $(0,1,0)G \in F(2)^6$ を計算したい!

$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1x1 + 0x0 + 1x0 \end{pmatrix} = 1$$

$$\vdots$$

$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1x0 + 0x1 + 1x1 \end{pmatrix} = 1$$

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

$(F(2)^3 \to F(2)^6)$ 計算中 (2) 検査行列 H による誤り検査

計算中 (1) で求めた $(1,0,1)$ の符号語 $w = (1,0,1,1,0,1)$ について検査行列 H を用いて, 誤りがないことを確認する. 誤り確認は, 検査行列 H に, w を縦ベクトルにした w^t を掛けて確認する. 結果が零ベクトル $(0,0,0)$ であれば誤り検出なし!

$$
\begin{aligned}
Hw^t &= \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} \\
&= \begin{pmatrix} 1x1 + 1x0 + 0x1 + 1x1 + 0x0 + 0x1 \\ 1x1 + 0x0 + 1x1 + 0x1 + 1x0 + 0x1 \\ 0x1 + 1x0 + 1x1 + 0x1 + 0x0 + 1x1 \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}
\end{aligned}
$$

$(F(2)^3 \to F(2)^6)$ 計算中 (3) 検査行列 H による誤り訂正

受信語 $w = (1, 0, 1, 1, 1, 1)$ を検査行列 H で確認.

$$
\begin{aligned}
Hw^t &= \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \\
&= \begin{pmatrix} 1x1 + 1x0 + 0x1 + 1x1 + 0x1 + 0x1 \\ 1x1 + 0x0 + 1x1 + 0x1 + 1x1 + 0x1 \\ 0x1 + 1x0 + 1x1 + 0x1 + 0x1 + 1x1 \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}
\end{aligned}
$$

※ Hw^t のベクトルが検査行列 H の 5 列目と等しいので, 誤りが, w の 5 番目の要素が誤りであることが, わかる! (注. 誤りが 1 箇所の場合.)

$(F(2)^3 \to F(2)^6)$ 計算中 (4) 検査行列 H による誤り訂正

受信語 $w = (1,0,1,1,1,1)$ の 5 番目の要素を訂正するとは,
$w' = w + (0,0,0,0,1,0) = (1,0,1,1,0,1)$ にするということである.

$$
\begin{aligned}
H(w+w')^t &= \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \right) \\
&= \begin{pmatrix} 1x1 + 1x0 + 0x1 + 1x1 + 0x1 + 0x1 \\ 1x1 + 0x0 + 1x1 + 0x1 + 1x1 + 0x1 \\ 0x1 + 1x0 + 1x1 + 0x1 + 0x1 + 1x1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}
\end{aligned}
$$

※ 本符号では, 2 箇所の誤りは検出出来ない! 何故!?

$F(2)$ 上の (6,3) 符号 **(2/3)** 符号間距離

［例題 1］生成行列 G と検査行列 H が,

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

によって定められる $(6,3)$ 符号の誤り訂正を考える.
受信語が (001111) だったとき, 符号間距離を考えて, 誤り訂正せよ.

(解答) (001111) は, G で生成される符号にはない.

$$(000), (001), (010), (011), (100), (101), (110), (111)$$

から, G で生成される符号を調べると

$$(000000), (001011), (010101), (011110), (100110), (101101), (110011), (111000)$$

である. 受信語 (011111) との距離を調べると

$$(4, 1, 3, 2, 3, 4, 2, 3, 4, 5)$$

となり, (001011) と一番近いので, (001011) が誤り訂正符号である. □

有限体 $F(2)$ 上の (6,3) 符号 **(3/3)** 誤り訂正

［例題 2］[例題 1] の生成行列 G と検査行列 H によって定められる $(6,3)$ 符号の誤り訂正を考える.
受信語が (001111) だったとき, 検査行列 H を使って, 誤り訂正せよ.

(解答) 受信語 (001111) を検査行列 H で検査すると.

$$H\cdot(001111)^t=\begin{pmatrix}0\\1\\1\end{pmatrix}+\begin{pmatrix}1\\0\\0\end{pmatrix}+\begin{pmatrix}0\\1\\0\end{pmatrix}+\begin{pmatrix}0\\0\\1\end{pmatrix}=\begin{pmatrix}1\\0\\0\end{pmatrix}$$

となる. 一方, このベクトルは, H の第 4 列と等しいので,

$H\cdot(000100)^t=\begin{pmatrix}1\\0\\0\end{pmatrix}$ であり, 受信語の 4 番目に誤りがあることが, わかる.

よって, 誤り訂正符号は, $(001111)-(000100)=(001011)$ である. □

有限体 $F(11)$ 上の (10,6,5) 符号 **(1/3)** 生成行列 G $(F(11)^6 \to F(11)^{10})$

$F(11)$ の生成元は, $\alpha = 2$ であり, $(10, 6, 5)$ RS 符号の生成行列は,

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\ 1 & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 \\ 1 & 8 & 9 & 6 & 4 & 10 & 3 & 2 & 5 & 7 \\ 1 & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 \\ 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 \end{pmatrix}$$

となり, 検査行列は,

$$H = \begin{pmatrix} 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\ 1 & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 \\ 1 & 8 & 9 & 6 & 4 & 10 & 3 & 2 & 5 & 7 \\ 1 & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 \end{pmatrix}$$

となる.

$(F(11)^6 \to F(11)^{10})$ 計算中 (1)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} \mathbf{1} & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \mathbf{1} & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\ \mathbf{1} & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 \\ \mathbf{1} & 8 & 9 & 6 & 4 & 10 & 3 & 2 & 5 & 7 \\ \mathbf{1} & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 \\ \mathbf{1} & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 \end{pmatrix}$$

を計算したい!

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} \mathbf{1} \\ \mathbf{1} \\ \mathbf{1} \\ \mathbf{1} \\ \mathbf{1} \\ \mathbf{1} \end{pmatrix} &= (1x1 + 2x1 + 3x1 + 4x1 + 5x1 + 6x1) \\ &= (1 + 2 + 3 + 4 + 5 + 6 \ (\mathbf{mod}\ 11)) \\ &= (21 \ (\mathbf{mod}\ 11)) \\ &= 10 \end{aligned}$$

$(F(11)^6 \to F(11)^{10})$ 計算中 (2)

$$
\begin{pmatrix}
\mathbf{1x1} & 1x1 & 1x1 & 1x1 & 1x1 & 1x1 & 1x1 & 1x1 & 1x1 & 1x1 \\
\mathbf{2x1} & 2x2 & 2x4 & 2x8 & 2x5 & 2x10 & 2x9 & 2x7 & 2x3 & 2x6 \\
\mathbf{3x1} & 3x4 & 3x5 & 3x9 & 3x3 & 3x1 & 3x4 & 3x5 & 3x9 & 3x3 \\
\mathbf{4x1} & 4x8 & 4x9 & 4x6 & 4x4 & 4x10 & 4x3 & 4x2 & 4x5 & 4x7 \\
\mathbf{5x1} & 5x5 & 5x3 & 5x4 & 5x9 & 5x1 & 5x5 & 5x3 & 5x4 & 5x9 \\
\mathbf{6x1} & 6x10 & 6x1 & 6x10 & 6x1 & 6x10 & 6x1 & 6x10 & 6x1 & 6x10
\end{pmatrix}
$$

$$
= \begin{pmatrix}
\mathbf{1} & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\mathbf{2} & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 & 1 \\
\mathbf{3} & 1 & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 \\
\mathbf{4} & 10 & 3 & 2 & 5 & 7 & 1 & 8 & 9 & 6 \\
\mathbf{5} & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 & 1 \\
\mathbf{6} & 5 & 6 & 5 & 6 & 5 & 6 & 5 & 6 & 5
\end{pmatrix}
$$

上の行列の列の和を $F(11)$ で計算すると

$$
\begin{pmatrix} \mathbf{10} & 2 & 4 & 5 & 10 & 8 & 8 & 3 & 3 & 1 \end{pmatrix}
$$

$(F(11)^6 \to F(11)^{10})$ 計算中 (3)

計算中 (1), 計算中 (2) より, 生成行列 G での符号化の計算は

$$
\begin{aligned}
& \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \mathbf{G} \\
= \; & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}
\begin{pmatrix}
\mathbf{1} & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\mathbf{1} & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\
\mathbf{1} & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 \\
\mathbf{1} & 8 & 9 & 6 & 4 & 10 & 3 & 2 & 5 & 7 \\
\mathbf{1} & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 \\
\mathbf{1} & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10
\end{pmatrix} \\
= \; & \begin{pmatrix} \mathbf{10} & 2 & 4 & 5 & 10 & 8 & 8 & 3 & 3 & 1 \end{pmatrix}
\end{aligned}
$$

以上より, 送りたい情報である $F(11)^6$ の元 $(1, 2, 3, 4, 5, 6)$ を符号化して,
$F(11)^{10}$ の元 $(10, 2, 4, 5, 10, 8, 8, 3, 3, 1)$ が得られることがわかる!
以下, この符号について誤り訂正の手順を考える!

有限体 $F(11)$ 上の (10,6,5) 符号 **(2/3)** 1 箇所の誤り訂正

$$\text{生成行列 } G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\ 1 & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 \\ 1 & 8 & 9 & 6 & 4 & 10 & 3 & 2 & 5 & 7 \\ 1 & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 \\ 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 \end{pmatrix}, \text{検査行列 } H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 4 & 8 & 5 \\ 4 & 5 & 9 & 3 \\ 8 & 9 & 6 & 4 \\ 5 & 3 & 4 & 9 \\ 10 & 1 & 10 & 1 \\ 9 & 4 & 3 & 5 \\ 7 & 5 & 2 & 3 \\ 3 & 9 & 5 & 4 \\ 6 & 3 & 7 & 9 \end{pmatrix}$$

によって定められる $(10, 6, 3)$ 符号の誤り訂正を考える

$F(11)^6$ の元 $(1 \times 2 \times 3 \times 4 \times 5 \times 6)$ を生成行列Gで符号化したものが，

$t0 = (10 \times 2 \times 4 \times 5 \times 10 \times 8 \times 8 \times 3 \times 3 \times 1)$ である．その中で，

1 箇所の誤りが起きた $t1 = (10 \times 2 \times 4 \times 5 \times \mathbf{8} \times 8 \times 8 \times 3 \times 3 \times 1)$ および，

2 箇所の誤りが起きた $t2 = (10 \times 2 \times 4 \times 5 \times \mathbf{8} \times \mathbf{10} \times 8 \times 3 \times 3 \times 1)$ の誤り訂正を考える

$t0$, $t1$, $t2$ を検査行列Hをかけると

$t0.H = (0, 0, 0, 0)$, $t1.H = \mathbf{(1, 5, 3, 4)}$, $t2.H = (10, 7, 1, 6)$ となる．

1 箇所の誤りは，$0 \le x \le 10$ として，$v = (x, 0, 0, 0, 0, 0, 0, 0, 0, 0)$，

$(0, x, 0, 0, 0, 0, 0, 0, 0, 0)$，...，$(0, 0, 0, 0, 0, 0, 0, 0, 0, x)$ に対して，

$v.H = (a, b, c, d)$ を計算し，$v.H = \mathbf{(1, 5, 3, 4)}$ となる v を探す

このとき，$x = 9$ で，$v = (0, 0, 0, 0, 9, 0, 0, 0, 0, 0)$ のとき，

$v.H = (1, 5, 3, 4)$ となることがわかる $t1.H$ も $(1, 5, 3, 4)$ なので，

$(t1 - v).H = 0$ となる．すなわち，$t1$を$t1 - v$に訂正することで誤り訂正が完成する

$(10 \times 2 \times 4 \times 5 \times \mathbf{8} \times 8 \times 8 \times 3 \times 3 \times 1) - (0, 0, 0, 0, \mathbf{9}, 0, 0, 0, 0, 0)$

$= (10 \times 2 \times 4 \times 5 \times \mathbf{10} \times 8 \times 8 \times 3 \times 3 \times 1)$ が，1 箇所の誤り訂正である

有限体 $F(11)$ 上の (10,6,5) 符号 **(3/3)** 2 箇所の誤り訂正

$$\text{生成行列 } G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\ 1 & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 \\ 1 & 8 & 9 & 6 & 4 & 10 & 3 & 2 & 5 & 7 \\ 1 & 5 & 3 & 4 & 9 & 1 & 5 & 3 & 4 & 9 \\ 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 \end{pmatrix}, \text{検査行列 } H = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 4 & 8 & 5 \\ 4 & 5 & 9 & 3 \\ 8 & 9 & 6 & 4 \\ 5 & 3 & 4 & 9 \\ 10 & 1 & 10 & 1 \\ 9 & 4 & 3 & 5 \\ 7 & 5 & 2 & 3 \\ 3 & 9 & 5 & 4 \\ 6 & 3 & 7 & 9 \end{pmatrix}$$

によって定められる $(10, 6, 3)$ 符号の誤り訂正を考える

$F(11)^6$ の元 $(1 \times 2 \times 3 \times 4 \times 5 \times 6)$ を生成行列Gで符号化したものが，

$t0 = (10 \times 2 \times 4 \times 5 \times 10 \times 8 \times 8 \times 3 \times 3 \times 1)$ である．その中で，

1 箇所の誤りが起きた $t1 = (10 \times 2 \times 4 \times 5 \times \mathbf{8} \times 8 \times 8 \times 3 \times 3 \times 1)$ および，

2 箇所の誤りが起きた $t2 = (10 \times 2 \times 4 \times 5 \times \mathbf{8} \times \mathbf{10} \times 8 \times 3 \times 3 \times 1)$ の誤り訂正を考える

$t0$, $t1$, $t2$ を検査行列Hをかけると

$t0.H = (0, 0, 0, 0)$, $t1.H = (1, 5, 3, 4)$, $t2.H = \mathbf{(10, 7, 1, 6)}$ となる．

2 箇所の誤りは，$0 \le x, y \le 10$ として，$v = (x, y, 0, 0, 0, 0, 0, 0, 0, 0)$，

$(x, 0, y, 0, 0, 0, 0, 0, 0, 0)$，...，$(0, 0, 0, 0, 0, 0, 0, 0, x, y)$ に対して，

$v.H = (a, b, c, d)$ を計算し，$v.H = \mathbf{(10, 7, 1, 6)}$ となる v を探す

このとき，$x = 9$, $y = 2$ で，$v = (0, 0, 0, 0, 9, 2, 0, 0, 0, 0)$ のとき，

$v.H = \mathbf{(10, 7, 1, 6)}$ となることがわかる $t2.H$ も $(1, 5, 3, 4)$ なので，

$(t2 - v).H = 0$ となる．すなわち，$t2$を$t2 - v$に訂正することで誤り訂正が完成する

$(10 \times 2 \times 4 \times 5 \times \mathbf{8} \times \mathbf{10} \times 8 \times 3 \times 3 \times 1) - (0, 0, 0, 0, \mathbf{9}, \mathbf{2}, 0, 0, 0, 0)$

$= (10 \times 2 \times 4 \times 5 \times \mathbf{10} \times \mathbf{8} \times 8 \times 3 \times 3 \times 1)$ が，2 箇所の誤り訂正である

[6] 拡大体 ($F(2^k)$) (k=3,4,8 の例で)

※ 有限体 $F(2^k)$ で, $k \geqq 2$ のときの演算定義は簡単ではない!!

ここでは, $F(2^3)$, $F(2^4)$, $F(2^8)$ の演算表を紹介します.

拡大体 (1/2)

q: 素数,
α : $F(q)$ 係数の m 次の既約多項式で $f(\alpha) = 0$ となる $F(q^m)$ の元
$1, \alpha, ..., \alpha^{m-1}$ は拡大体の基
$q = 2$, $m = 2$, $F(2^2) = F(4)$: 拡大体
$f(X) = x^2 + aX + b (a, b \in F(2))$
$c \in 0, 1 = F(2)$
$f(0) = b \neq 0$
$f(1) = a + b + 1 \neq 0$
となる a, b を探す.
$a, b \in F(2)$ より $b = 1$, $a = 1$ しかない.
$f(X) = x^2 + x + 1$
$\alpha^2 + \alpha + 1$ を満たす元 α を $F(2)$ に追加する.
$F(2^2) = 0, 1, \alpha, \alpha + 1$: 元の数は $4 = 2^2$

拡大体 (2)

$q = 2$, $m = 3$: $F(2^3) = F(8)$: 拡大体
$f(X) = x^3 + ax^2 + bX + c$ $(a, b, c \in F(2))$
$f(X) = x^3 + x + 1$, $x^3 + x^2 + 1$ などあるけど, 拡大体は同じになる!(証明省略)
$F(2^3) = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$: 元の数は $8 = 2^3$

$q = 2$, $m = 4$: $F(2^4)$: 拡大体 $\Leftarrow$ QR コードの形式情報に使われる.
$f(X) = x^4 + x + 1$ で拡大体を作る.
$F(2^4) = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1,$
$\alpha^3 + 0, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2,$
$\alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}$: 元の数は $16 = 2^4$

有限体 $F(2^3) = \{0, 1, x, x^2, x+1, x^2, x^2+1\}$ (その 1)

m 次の既約多項式 $f(x)$ を 1 つ定めたとき, 位数 2^m の有限体を係数が $F(2)$ の元である多項式を $f(x)$ で割った余りの剰余多項式で定める.
以下, $m = 3$ の既約多項式 $f(x) = x^3 + x + 1$ の例で考える. $f(x)$ で割った余りの多項式は, $a + bx + cx^2$ $(a, b, c \in \{0, 1\})$ なので, 0, 1, x, $x+1$, x^2, x^2+1, x^2+x, x^2+x+1 の 8 つになる. 和 $(+)$ や積 $(\times)$ は, 多項式の和や積を考え, $f(x)$ で割った余りの多項式とする.
eg. $(x+1) \times (x^2+1) = x^3 + x^2 + x + 1 = (x^3 + x + 1) + x^2 = x^2$
$x \times x^2 = x^3 = (x^3 + x + 1) + (x + 1) = x + 1$

有限体 $F(2^3) = \{\alpha^0 = 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7 = 0\}$

和: $x + y \pmod 8$

+	0	x	x^2	$1+x$	$x+x^2$	$1+x+x^2$	$1+x^2$	1
0	0	x	x^2	$1+x$	$x+x^2$	$1+x+x^2$	$1+x^2$	1
x	x	0	$x+x^2$	1	x^2	$1+x^2$	$1+x+x^2$	$1+x$
x^2	x^2	$x+x^2$	0	$1+x+x^2$	x	$1+x$	1	$1+x^2$
$1+x$	$1+x$	1	$1+x+x^2$	0	$1+x^2$	x^2	$x+x^2$	x
$x+x^2$	$x+x^2$	x^2	x	$1+x^2$	0	1	$1+x$	$1+x+x^2$
$1+x+x^2$	$1+x+x^2$	$1+x^2$	$1+x$	x^2	1	0	x	$x+x^2$
$1+x^2$	$1+x^2$	$1+x+x^2$	1	$x+x^2$	$1+x$	x	0	x^2
1	1	$1+x$	$1+x^2$	x	$1+x+x^2$	$x+x^2$	x^2	0

+	α^7	α	α^2	α^3	α^4	α^5	α^6	1
α^7	α^7	α	α^2	α^3	α^4	α^5	α^6	1
α	α	α^7	α^4	1	α^2	α^6	α^5	α^3
α^2	α^2	α^4	α^7	α^5	α	α^3	1	α^6
α^3	α^3	1	α^5	α^7	α^6	α^2	α^4	α
α^4	α^4	α^2	α	α^6	α^7	1	α^3	α^5
α^5	α^5	α^6	α^3	α^2	1	α^7	α	α^4
α^6	α^6	α^5	1	α^4	α^3	α	α^7	α^2
1	1	α^3	α^6	α	α^5	α^4	α^2	α^7

積: $x \times y \pmod 8$

x	0	x	x^2	$1+x$	$x+x^2$	$1+x+x^2$	$1+x^2$	1
0	0	0	0	0	0	0	0	0
x	0	x^2	$1+x$	$x+x^2$	$1+x+x^2$	$1+x^2$	1	x
x^2	0	$1+x$	$x+x^2$	$1+x+x^2$	$1+x^2$	1	x	x^2
$1+x$	0	$x+x^2$	$1+x+x^2$	$1+x^2$	1	x	x^2	$1+x$
$x+x^2$	0	$1+x+x^2$	$1+x^2$	1	x	x^2	$1+x$	$x+x^2$
$1+x+x^2$	0	$1+x^2$	1	x	x^2	$1+x$	$x+x^2$	$1+x+x^2$
$1+x^2$	0	1	x	x^2	$1+x$	$x+x^2$	$1+x+x^2$	$1+x^2$
1	0	x	x^2	$1+x$	$x+x^2$	$1+x+x^2$	$1+x^2$	1

x	α^7	α	α^2	α^3	α^4	α^5	α^6	1
α^7	α^7	α^7	α^7	α^7	α^7	α^7	α^7	α^7
α	α^7	α^2	α^3	α^4	α^5	α^6	1	α
α^2	α^7	α^3	α^4	α^5	α^6	1	α	α^2
α^3	α^7	α^4	α^5	α^6	1	α	α^2	α^3
α^4	α^7	α^5	α^6	1	α	α^2	α^3	α^4
α^5	α^7	α^6	1	α	α^2	α^3	α^4	α^5
α^6	α^7	1	α	α^2	α^3	α^4	α^5	α^6
1	α^7	α	α^2	α^3	α^4	α^5	α^6	1

※ 最小多項式は, $x^3 + x + 1$

有限体 $F(2^4) = \{\alpha^0 = 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \cdots, \alpha^{14}, \alpha^{15} = 0\}$ (1/2)

和: $x + y$ $F(2^4)$

+	0	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1
0	0	x	x^2	$1+x$	$1+x$	$x+x^2$	$1+x+x^2$	0	$1+x^2$	1	$1+x+x^2$	$1+x^2$	x^2	$x+x^2$	x	1
x	x	0	$x+x^2$	1	1	x^2	$1+x^2$	x	$1+x+x^2$	$1+x$	$1+x^2$	$1+x+x^2$	$x+x^2$	x^2	0	$1+x$
x^2	x^2	$x+x^2$	0	$1+x+x^2$	$1+x+x^2$	x	$1+x$	x^2	1	$1+x^2$	$1+x$	1	0	x	$x+x^2$	$1+x^2$
x^3	$1+x$	1	$1+x+x^2$	0	0	$1+x^2$	x^2	$1+x$	$x+x^2$	x	x^2	$x+x^2$	$1+x+x^2$	$1+x^2$	1	x
$1+x$	$1+x$	1	$1+x+x^2$	0	0	$1+x^2$	x^2	$1+x$	$x+x^2$	x	x^2	$x+x^2$	$1+x+x^2$	$1+x^2$	1	x
$x+x^2$	$x+x^2$	x^2	x	$1+x^2$	$1+x^2$	0	1	$x+x^2$	$1+x$	$1+x+x^2$	1	$1+x$	x	0	x^2	$1+x+x^2$
x^2+x^3	$1+x+x^2$	$1+x^2$	$1+x$	x^2	x^2	1	0	$1+x+x^2$	x	$x+x^2$	0	x	$1+x$	1	$1+x^2$	$x+x^2$
$1+x+x^3$	0	x	x^2	$1+x$	$1+x$	$x+x^2$	$1+x+x^2$	0	$1+x^2$	1	$1+x+x^2$	$1+x^2$	x^2	$x+x^2$	x	1
$1+x^2$	$1+x^2$	$1+x+x^2$	1	$x+x^2$	$x+x^2$	$1+x$	x	$1+x^2$	0	x^2	x	0	1	$1+x$	$1+x+x^2$	x^2
$x+x^3$	1	$1+x$	$1+x^2$	x	x	$1+x+x^2$	$x+x^2$	1	x^2	0	$x+x^2$	x^2	$1+x^2$	$1+x+x^2$	$1+x$	0
$1+x+x^2$	$1+x+x^2$	$1+x^2$	$1+x$	x^2	x^2	1	0	$1+x+x^2$	x	$x+x^2$	0	x	$1+x$	1	$1+x^2$	$x+x^2$
$x+x^2+x^3$	$1+x^2$	$1+x+x^2$	1	$x+x^2$	$x+x^2$	$1+x$	x	$1+x^2$	0	x^2	x	0	1	$1+x$	$1+x+x^2$	x^2
$1+x+x^2+x^3$	x^2	$x+x^2$	0	$1+x+x^2$	$1+x+x^2$	x	$1+x$	x^2	1	$1+x^2$	$1+x$	1	0	x	$x+x^2$	$1+x^2$
$1+x^2+x^3$	$x+x^2$	x^2	x	$1+x^2$	$1+x^2$	0	1	$x+x^2$	$1+x$	$1+x+x^2$	1	$1+x$	x	0	x^2	$1+x+x^2$
$1+x^3$	x	0	$x+x^2$	1	1	x^2	$1+x^2$	x	$1+x+x^2$	$1+x$	$1+x^2$	$1+x+x^2$	$x+x^2$	x^2	0	$1+x$
1	1	$1+x$	$1+x^2$	x	x	$1+x+x^2$	$x+x^2$	1	x^2	0	$x+x^2$	x^2	$1+x^2$	$1+x+x^2$	$1+x$	0

積: $x \times y$ $F(2^4)$

x	0	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x	0	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1	x
x^2	0	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1	x	x^2
x^3	0	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1	x	x^2	x^3
$1+x$	0	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1	x	x^2	x^3	$1+x$
$x+x^2$	0	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1	x	x^2	x^3	$1+x$	$x+x^2$
x^2+x^3	0	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3
$1+x+x^3$	0	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$
$1+x^2$	0	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$
$x+x^3$	0	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$
$1+x+x^2$	0	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$
$x+x^2+x^3$	0	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$
$1+x+x^2+x^3$	0	$1+x^2+x^3$	$1+x^3$	1	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$
$1+x^2+x^3$	0	$1+x^3$	1	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$
$1+x^3$	0	1	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$
1	0	x	x^2	x^3	$1+x$	$x+x^2$	x^2+x^3	$1+x+x^3$	$1+x^2$	$x+x^3$	$1+x+x^2$	$x+x^2+x^3$	$1+x+x^2+x^3$	$1+x^2+x^3$	$1+x^3$	1

※ 最小多項式は, $x^4 + x + 1$

有限体 $F(2^4) = \{\alpha^0 = 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \cdots, \alpha^{14}, \alpha^{15} = 0\}$ (2/2)

和: $x + y$ $F(2^4)$

+	α^{15}	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1
α^{15}	α^{15}	α	α^2	α^4	α^4	α^5	α^{10}	α^{15}	α^8	1	α^{10}	α^8	α^2	α^5	α	1
α	α	α^{15}	α^5	1	1	α^2	α^8	α	α^{10}	α^4	α^8	α^{10}	α^5	α^2	α^{15}	α^4
α^2	α^2	α^5	α^{15}	α^{10}	α^{10}	α	α^4	α^2	1	α^8	α^4	1	α^{15}	α	α^5	α^8
α^3	α^4	1	α^{10}	α^{15}	α^{15}	α^8	α^2	α^4	α^5	α	α^2	α^5	α^{10}	α^8	1	α
α^4	α^4	1	α^{10}	α^{15}	α^{15}	α^8	α^2	α^4	α^5	α	α^2	α^5	α^{10}	α^8	1	α
α^5	α^5	α^2	α	α^8	α^8	α^{15}	1	α^5	α^4	α^{10}	1	α^4	α	α^{15}	α^2	α^{10}
α^6	α^{10}	α^8	α^4	α^2	α^2	1	α^{15}	α^{10}	α	α^5	α^{15}	α	α^4	1	α^8	α^5
α^7	α^{15}	α	α^2	α^4	α^4	α^5	α^{10}	α^{15}	α^8	1	α^{10}	α^8	α^2	α^5	α	1
α^8	α^8	α^{10}	1	α^5	α^5	α^4	α	α^8	α^{15}	α^2	α	α^{15}	1	α^4	α^{10}	α^2
α^9	1	α^4	α^8	α	α	α^{10}	α^5	1	α^2	α^{15}	α^5	α^2	α^8	α^{10}	α^4	α^{15}
α^{10}	α^{10}	α^8	α^4	α^2	α^2	1	α^{15}	α^{10}	α	α^5	α^{15}	α	α^4	1	α^8	α^5
α^{11}	α^8	α^{10}	1	α^5	α^5	α^4	α	α^8	α^{15}	α^2	α	α^{15}	1	α^4	α^{10}	α^2
α^{12}	α^2	α^5	α^{15}	α^{10}	α^{10}	α	α^4	α^2	1	α^8	α^4	1	α^{15}	α	α^5	α^8
α^{13}	α^5	α^2	α	α^8	α^8	α^{15}	1	α^5	α^4	α^{10}	1	α^4	α	α^{15}	α^2	α^{10}
α^{14}	α	α^{15}	α^5	1	1	α^2	α^8	α	α^{10}	α^4	α^8	α^{10}	α^5	α^2	α^{15}	α^4
1	1	α^4	α^8	α	α	α^{10}	α^5	1	α^2	α^{15}	α^5	α^2	α^8	α^{10}	α^4	α^{15}

積: $x \times y$ $F(2^4)$

x	α^{15}	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1
α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}	α^{15}
α	α^{15}	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α
α^2	α^{15}	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2
α^3	α^{15}	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3
α^4	α^{15}	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4
α^5	α^{15}	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5
α^6	α^{15}	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6
α^7	α^{15}	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7
α^8	α^{15}	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8
α^9	α^{15}	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9
α^{10}	α^{15}	α^{11}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}
α^{11}	α^{15}	α^{12}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}
α^{12}	α^{15}	α^{13}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}
α^{13}	α^{15}	α^{14}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}
α^{14}	α^{15}	1	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}
1	α^{15}	α	α^2	α^3	α^4	α^5	α^6	α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}	1

有限体 $F(2^8) = \{\alpha^0 = 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \cdots, \alpha^{254}, \alpha^{255} = 0\}$

QR コードに使われます!

和: $x + y$ $F(2^8)$

(表が大きくて表示できません.
cf. G28atable0.csv)

積: $x \times y$ $F(2^8)$

(表が大きくて表示できません.
cf. G28mtable0.csv)

$F(2)$ 上の 7 次の多項式を用いて計算して表を作ります.
最小多項式は, $x^8 + x^4 + x^3 + x^2 + 1$.

[7] QR コード

※ QR コードは, 白と黒, すなわち, $F(2)$ の元で構成されてますが, そのデータ部分は, 8 ブロックずつに分かれていて, $F(2^8)$ の元が埋め込まれてます.

QRコード作成 (1.漢字モード)

漢字モードでは漢字6文字まで符号化可能

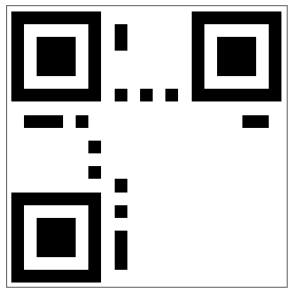
```
q1 = ArrayPlot[ListXor[QRcode[KanjiMode["九州大学"]], MaskPositions]]
```

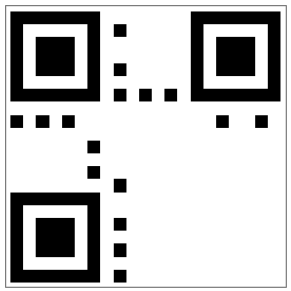
QRコード作成 (2. 英数字モード)

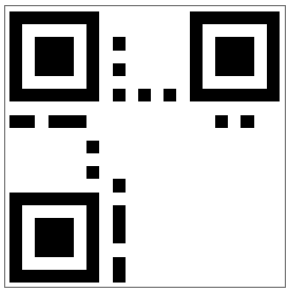
8bitコードモードでは, 英数字11文字まで符号化可能

```
ArrayPlot[ListXor[QRcode[Char8bitMode["Kyushu Univ"]], MaskPositions]]
```

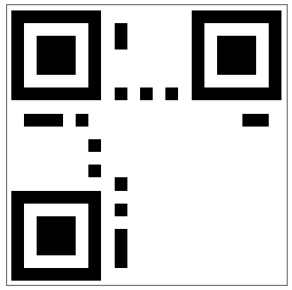
QR コード作成 (3. データ埋め込み方法)

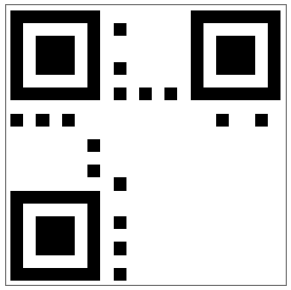

形式情報

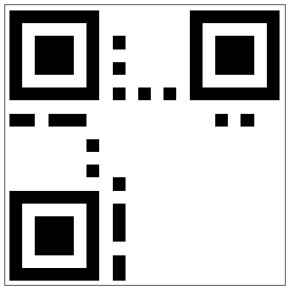

形式情報マスクパターン


形式情報マスク処理

QR コードで, どの符号形式を使うかの形式情報は, 15bit のデータとして, 形式情報の場所に保存されます.

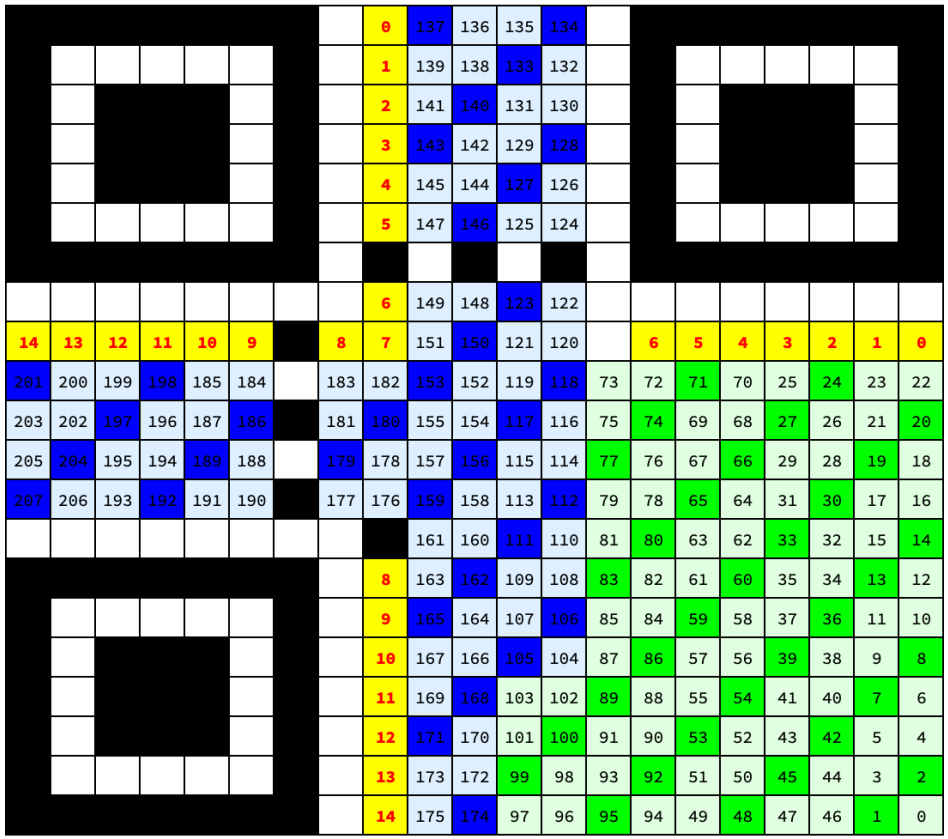

形式情報


形式情報マスクパターン


形式情報マスク処理

※ 送信データは, データ情報部分に保存されます. 送信データの特徴が, わからないようにするために, アスクパターンを用いて, 決まった場所の白黒を反転します. ※ 今日は形式情報 15bit は固定です!

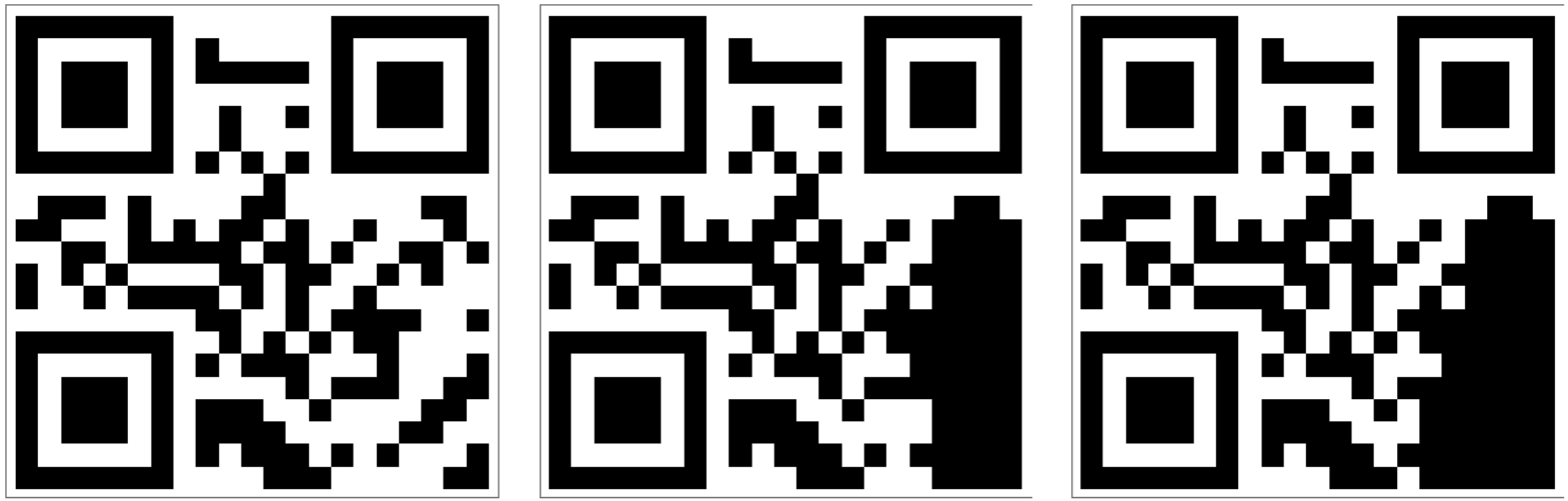
QR コード作成 (4. データ埋め込み場所)



黄色部分 (2 箇所) に形式情報 (符号方式の情報)15bit が入っています. 緑部分と青部分の 2 箇所にそれぞれ, 送信情報 (送信文等)104bit が入っています.

緑と青の濃い色の部分は bit を反転し, データの特徴が現れないよう工夫します.

QR コード (5. 誤り訂正能力確認 (1))



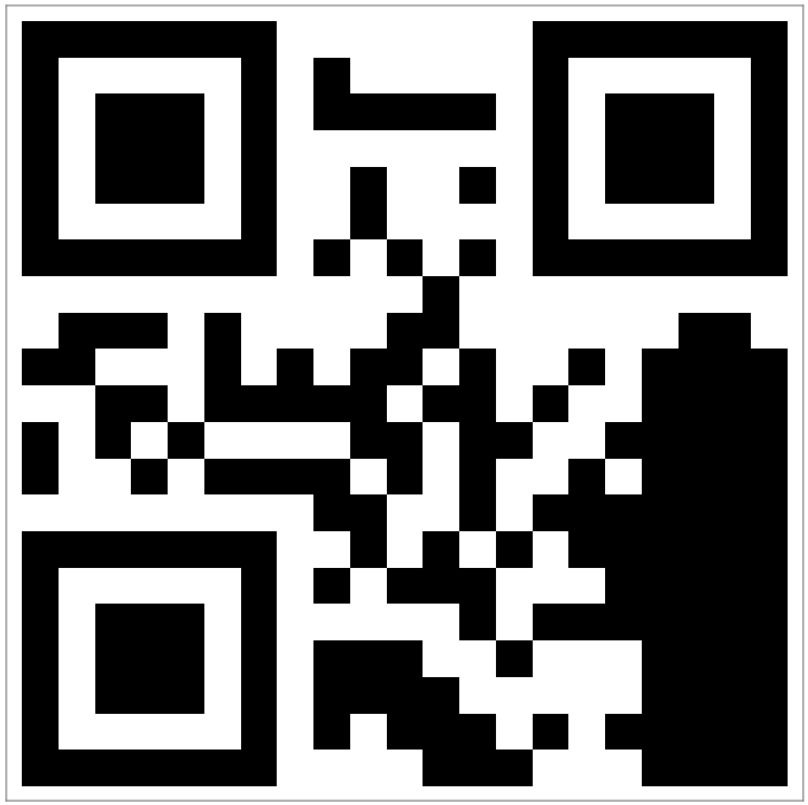
※ 左端がある文字列を符号化して QR コードにしたものです. 真ん中のコードは, 左の QR コードのうち, 24(8x3) マス黒く塗りつぶしたものです. 右端のコードは, 左端の QR コードのうち, 32(8x4) マス黒く塗りつぶしたものです.
真ん中のコードは誤り訂正可能です. 右端のものは誤り訂正不可能です.

※ 前ページにあるように, 緑色の部分と青色の部分はマスク処理が異なりますが, 同じデータが埋め込まれていますので, 高度な処理を行えば, 青色部分から復元できるかもしれません!?!?)

QR コード (5. 誤り訂正能力確認 (2))

データ部分のうち6ブロックを塗りつぶしてみる (訂正可能!)

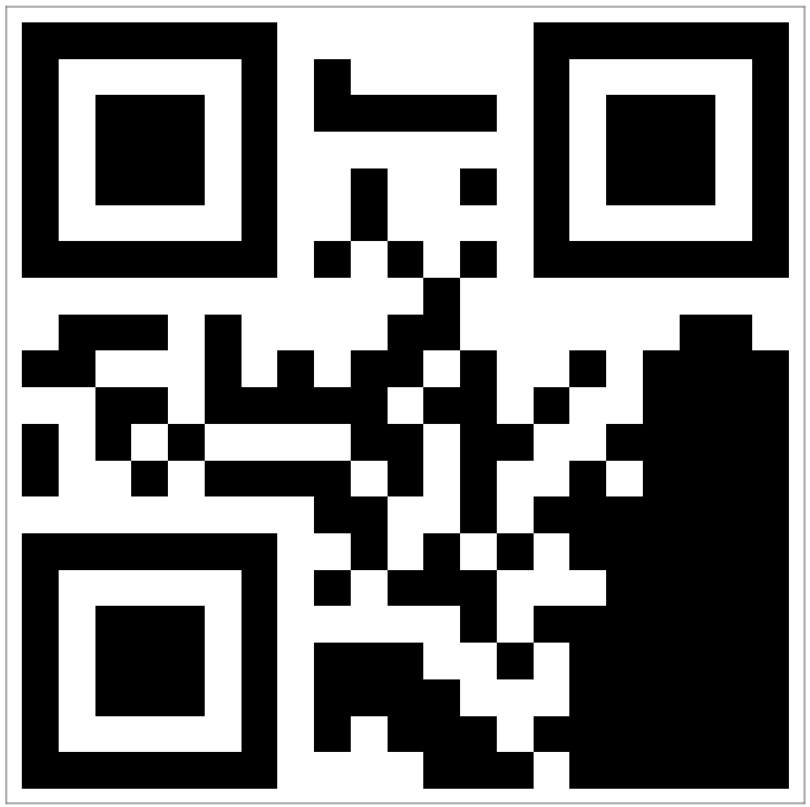
```
q2 = ArrayPlot[Listset[ListXor[QRcode[KanjiMode["九州大学"]], MaskPositions],
    Join[Mask[{20, 18}], Mask[{18, 18}], Mask[{20, 14}], Mask[{18, 14}],
     Mask[{20, 10}], Mask[{18, 10}]]]]
```



QR コード (5. 誤り訂正能力確認 (3))

データ部分のうち7ブロックを塗りつぶしてみる (訂正不可能!)

```
q3 = ArrayPlot[Listset[ListXor[QRcode[KanjiMode["九州大学"]], MaskPositions],
    Join[Mask[{20, 18}], Mask[{18, 18}], Mask[{20, 14}], Mask[{18, 14}],
     Mask[{20, 10}], Mask[{18, 10}], Mask[{16, 18}]
    ]]]
```



QR コード (6. 情報の埋め込み方法 (1))

先のスライド (4. データ埋め込み場所) にある緑と青の部分 8x26bit の場所にデータが埋め込まれる. その埋め込み方法を「九州大学」というデータを埋め込む例に沿って紹介する.

1. 送信文字列「九州大学」を漢字コードを用いて 8x13bit の情報元とする.
2. 情報元は $F(2^8) = \{\alpha^0(=1), \alpha^2, \cdots \alpha^{254}, \alpha^{255}(=0)\}$ 上の 13 次元ベクトルとする.
3. $F(2^8)$ の元は, 8 次の最小多項式 $x^8 + x^4 + x^3 + x^2 + 1$ を用いて, $F(2^8)$ の元を $F(2)$ 上の 7 次の多項式と同一視する.
4. 13 次の最小多項式

$$(x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{11})(x-\alpha^{12})$$

を用いて, $F(2^8)^{13}$ の元を $F(2^8)$ 上の 11 次の多項式と同一視する.
5. $F(2^8)^{13}$ の情報元を $F(2^8)^{26}$ の元に符号化する生成行列は, 次のように定める.

QR コード (6. 情報の埋め込み方法 (2)) [まとめ]

- 「九州大学」をコード化した, $F(256)^{13}$ の元は以下の通りです.

$$(\ \alpha^{128}\ \ \alpha^{100}\ \ \alpha^{17}\ \ \alpha^{170}\ \ \alpha^{9}\ \ \alpha^{148}\ \ \alpha^{166}\ \ \alpha^{247}\ \ 1\ \ 1\ \ 1\ \ 1\ \ \alpha^{236}\ )$$

- $F(256)^{13}$ を $F(256)^{26}$ に符号化する生成行列 (13x26) は以下の通りです.

$$\begin{pmatrix}
\alpha & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha^{125} & \alpha^{69} & \alpha^{134} & \alpha^{119} & \alpha^{168} & \alpha^{53} & \alpha^{62} & \alpha^{108} & \alpha^{61} & \alpha^{131} & \alpha^{125} & \alpha^{2} & \alpha^{198} \\
1 & \alpha & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha^{177} & \alpha^{155} & \alpha^{78} & \alpha^{6} & \alpha^{25} & \alpha^{211} & \alpha^{91} & \alpha^{188} & \alpha^{194} & \alpha^{254} & \alpha^{15} & \alpha^{55} & \alpha^{74} \\
1 & 1 & \alpha & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha^{249} & \alpha^{150} & \alpha^{85} & \alpha^{231} & \alpha^{212} & \alpha^{216} & \alpha & \alpha^{229} & \alpha^{29} & \alpha^{35} & \alpha^{37} & \alpha^{158} & \alpha^{177} \\
1 & 1 & 1 & \alpha & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha^{29} & \alpha^{42} & \alpha^{112} & \alpha^{192} & \alpha^{55} & \alpha^{165} & \alpha^{8} & \alpha^{63} & \alpha^{100} & \alpha^{60} & \alpha^{107} & \alpha^{220} & \alpha^{204} \\
1 & 1 & 1 & 1 & \alpha & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha^{140} & \alpha^{216} & \alpha^{18} & \alpha^{84} & \alpha^{100} & \alpha^{158} & \alpha & \alpha^{122} & \alpha^{173} & \alpha^{47} & \alpha^{241} & \alpha^{106} & \alpha^{139} \\
1 & 1 & 1 & 1 & 1 & \alpha & 1 & 1 & 1 & 1 & 1 & 1 & \alpha^{115} & \alpha^{127} & \alpha^{133} & \alpha^{239} & \alpha^{68} & \alpha^{141} & \alpha^{142} & \alpha^{117} & \alpha^{103} & \alpha^{227} & \alpha^{195} & \alpha^{150} & \alpha^{132} \\
1 & 1 & 1 & 1 & 1 & 1 & \alpha & 1 & 1 & 1 & 1 & 1 & \alpha^{222} & \alpha^{60} & \alpha^{134} & \alpha^{142} & \alpha^{80} & \alpha^{22} & \alpha^{50} & \alpha^{114} & \alpha^{74} & \alpha^{229} & \alpha^{224} & \alpha^{68} & \alpha^{230} \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha & 1 & 1 & 1 & 1 & \alpha^{211} & \alpha^{58} & \alpha^{199} & \alpha^{142} & \alpha^{236} & \alpha^{172} & \alpha^{116} & \alpha^{151} & \alpha^{28} & \alpha^{51} & \alpha^{36} & \alpha^{199} & \alpha^{206} \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha & 1 & 1 & 1 & \alpha^{39} & \alpha^{187} & \alpha^{13} & \alpha^{101} & \alpha^{227} & \alpha^{127} & \alpha^{193} & \alpha^{54} & \alpha^{9} & \alpha^{127} & \alpha^{235} & \alpha^{50} & \alpha^{49} \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha & 1 & 1 & \alpha^{136} & \alpha^{252} & \alpha^{186} & \alpha^{130} & \alpha^{133} & \alpha^{180} & \alpha^{159} & \alpha^{99} & \alpha^{144} & \alpha^{250} & \alpha^{30} & \alpha^{187} & \alpha^{79} \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha & 1 & \alpha^{105} & \alpha^{48} & \alpha^{165} & \alpha^{65} & \alpha^{53} & \alpha^{45} & \alpha^{3} & \alpha^{89} & \alpha^{220} & \alpha^{53} & \alpha^{143} & \alpha^{36} & \alpha^{188} \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha & \alpha^{27} & \alpha^{171} & \alpha^{125} & \alpha^{64} & \alpha^{247} & \alpha^{197} & \alpha^{155} & \alpha^{133} & \alpha^{246} & \alpha^{25} & \alpha^{135} & \alpha^{129} & \alpha^{73} \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \alpha & \alpha^{137} & \alpha^{73} & \alpha^{227} & \alpha^{17} & \alpha^{177} & \alpha^{17} & \alpha^{52} & \alpha^{13} & \alpha^{46} & \alpha^{43} & \alpha^{83} & \alpha^{132} & \alpha^{120}
\end{pmatrix}$$

- 符号化された $F(256)^{26}$ の元は以下の通りです.

$$(\ \alpha^{128}\ \ \alpha^{100}\ \ \alpha^{17}\ \ \alpha^{170}\ \ \alpha^{9}\ \ \alpha^{148}\ \ \alpha^{166}\ \ \alpha^{247}\ \ 1\ \ 1\ \ 1\ \ 1\ \ \alpha^{236}\ \ \alpha^{215}\ \ \alpha^{40}\ \ \alpha^{67}\ \ \alpha^{182}\ \ \alpha^{69}\ \ \alpha^{112}\ \ \alpha^{151}\ \ \alpha^{124}\ \ \alpha^{106}\ \ \alpha^{213}\ \ \alpha^{130}\ \ \alpha^{26}\ \ \alpha^{140}\ )$$

※ 13 次元ベクトルの情報源を (13x26) 行列に掛けることで, 誤り訂正可能な 26 次元ベクトルを得ます. 行列計算時の加算と乗算は $F(256)$ の加算表と乗算表にある演算です.

QR コード (7.Mathematica で計算)

- 「九州大学」をコード化した, $F(256)^{13}$ の元を求める.

```
In[116]:= α^FromDigits[#,2] & /@ KanjiMode["九州大学"]
```

$$\text{Out[116]}= \{\alpha^{128}, \alpha^{100}, \alpha^{17}, \alpha^{170}, \alpha^{9}, \alpha^{148}, \alpha^{166}, \alpha^{247}, 1, 1, 1, 1, \alpha^{236}\}$$

- 「九州大学」を符号化した $F(256)^{26}$ の元を求める.

```
In[114]:= α^FromDigits[#,2] & /@
            (Reverse[CoefficientList[#, α, 8]] & /@
              (CoefficientsToPolynomial[#, α] & /@ QRdata104to208[KanjiMode["九州大学"]]))
```

$$\text{Out[114]}= \{\alpha^{128}, \alpha^{100}, \alpha^{17}, \alpha^{170}, \alpha^{9}, \alpha^{148}, \alpha^{166}, \alpha^{247}, 1, 1, 1, 1, \alpha^{236},$$
$$\alpha^{215}, \alpha^{40}, \alpha^{67}, \alpha^{182}, \alpha^{69}, \alpha^{112}, \alpha^{151}, \alpha^{124}, \alpha^{106}, \alpha^{213}, \alpha^{130}, \alpha^{26}, \alpha^{140}\}$$

[8] レポート課題

- 課題 1. $F(2)$ 上の (6,3) 符号の誤り訂正
- 課題 2. $F(2)$ 上の 3 次以下の既約多項式の列挙
- 課題 3.
  有限体を用いた誤り訂正符号の話題 (すべてでなく興味のあった部分のみでもよい) について, 自分の言葉で 200 字以内でまとめて下さい.
- 自由課題 4.
  Python 言語による QR コード作成 (何でも ok)
- 自由課題 5. $F(11)$ 上の (10,6,5) 符号の誤り訂正

課題1. $F(2)$ 上の (6,3) 符号の誤り訂正

課題 1. $F(2)$ 上の (6,3) 符号の符号化と誤り訂正
次の生成行列 G と検査行列 H を持つ $F(2)$ 上の符号を考える.

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \qquad H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(1) $w_1 = (1,1,1) \in F(2)^3$ を符号化したベクトル $w_1.G \in F(2)^6$ を求めよ.

(2) 1 箇所の誤りを含む符号化されたベクトル $v_2 = (1,1,1,1,1,0) \in F(2)^6$ に対して, 検査行列で検査したベクトル $H.(v_2)^t \in F(2)^3$ を求めよ.

(3) (2) のベクトル v_2 を誤り訂正して, 正しい情報源 $w \in F(2)^3$ を求めよ.

課題 2. $F(2)$ 上の 3 次以下の既約多項式の列挙

課題 2: (スライド 21) の問題 (2) に $F(2)$ 上の 1 次から 3 次までの全ての既約多項式の列挙が求められています. この問題 (2) の解答を考えてみて下さい.

課題 3. 有限体を用いた誤り訂正符号の計算例

課題 3:

有限体を用いた誤り訂正符号の話題 (すべてでなく興味のあった部分のみでもよい) について, 自分の言葉でまとめて報告して下さい.

自由課題 4. Python 言語による QR コード作成

課題 4: (本課題は自由課題です. 提出は任意です.)

スライド [付録] にある,

Python 言語による QR コード作成

を参考にして, 自分で Python 言語で QR コードを作成してみて下さい. その作成過程のまとめ, 苦労した点などを報告して下さい.

※ Python 言語は, Google Colaboratory を利用すると良いでしょう.

`https://colab.research.google.com`

自由課題5. $F(11)$ 上の $(10,6,5)$ 符号の誤り訂正

課題 5. (本課題は自由課題です. 提出は任意です.)
(スライド 40) の生成行列 G と検査行列 H を持つ $F(11)$ 上の符号を考える.

(1) $w_1 = (1,1,1,1,1,1) \in F(11)^6$ を符号化したベクトル $w_1.G \in F(11)^{10}$ を求めよ.

(2) 1 箇所の誤りを含む符号化されたベクトル $v_2 = (10,2,4,5,8,8,8,3,3,1) \in F(2)^{10}$ に対して, 検査行列で検査したベクトル $H.(v_2)^t \in F(11)^4$ を求めよ.

(3) (2) のベクトル v_2 を誤り訂正して, 正しい情報源 $w_2 \in F(11)^6$ を求めよ.

(4) 2 箇所の誤りを含む符号化されたベクトル $v_3 = (10,2,4,5,8,10,8,3,3,1) \in F(2)^{10}$ に対して, 検査行列で検査したベクトル $H.(v_2)^t \in F(11)^4$ を求めよ.

(5) (4) のベクトル v_3 を誤り訂正して, 正しい情報源 $w_3 \in F(11)^6$ を求めよ.

[9] 付録

1. Python 言語で QR コード作成と解読
2. 【紹介】IPSJ 中高生情報学研究コンテスト
3. 【紹介】マス・フォア・インダストリって何？
4. 【紹介】メビウス・カライドサイクル (発明)

[付録 1] Python 言語で QR コード作成と解読 (1)

qrcode ライブラリを使って QR コード作成
`https://pypi.org/project/qrcode/`

```
!pip install qrcode > /dev/null
!pip install pillow > /dev/null
```

```
import qrcode
from IPython.display import Image,display_png

qr = qrcode.QRCode(
    version=1,
    error_correction=qrcode.constants.ERROR_CORRECT_Q,
    box_size=10,
    border=4,
)
qr.add_data("九州大学".encode('shift_jis'))
qr.make()
img = qr.make_image()
img.save("qrcode_qdai1.png")
display_png(Image('qrcode_qdai1.png'))
```

漢字文字列「九州大学」の QR コードを作成する Python プログラム
完成した画像は, PNG 画像ファイルとして保存されます.

[付録 1] Python 言語で QR コード作成と解読 (2)

pyqrcode ライブラリを使って QR コード作成 https://pypi.org/project/PyQRCode/

[付録 1] Python 言語で QR コード作成と解読 (3)

Pyzbar ライブラリを利用した QR コード解読
`https://pypi.org/project/pyzbar/`

```
1 !apt install libzbar0 >& /dev/null
2 !pip install pyzbar >& /dev/null
```

```
1 import pyzbar.pyzbar
2 from PIL import Image
3
4 qr = pyzbar.pyzbar.decode(Image.open('qr003.png'))
5 print(qr)
6 print(qr[0].data.decode())
```

```
[Decoded(data=b'\xe4\xb9\x9d\xe5\xb7\x9e\xe5\xa4\x
九州大学
```

あらかじめ作っておいた QR コード画像ファイル qr003.png の解読結果を変数 qr に読み込みます. 画像ファイルに複数の QR コードが一緒に入っている場合 qr[0], qr[1], ... に読み込み結果が入ります.

[付録2] IPSJ中高生情報学研究コンテスト (1/2)

昨年度の HP `https://www.dreamnews.jp/press/0000292406/` 本年度は, 2025 年 3 月に, 立命館大学にて開催予定.

情報処理学会第 86 回全国大会併催

本年より ブロック大会やります！

第6回 中高生情報学研究コンテスト

https://www.ipsj.or.jp/event/taikai/86/86PosterSession/

詳細はホームページで順次お知らせしていきます。

受付開始：2023 年 9 月 1 日（金）
申込締切：2023 年 10 月 10 日（火）
※申込多数の場合は早期に締め切ります。
ポスター締切：2023 年 11 月 10 日（金）
ブロック大会：2023 年 12 月 9 日（土）～17 日（日）頃
全国大会：2024 年 3 月 16 日（土）

全国大会日時：2024 年 3 月 16 日（土）13:20-15:20

全国大会会場：神奈川大学 横浜キャンパス（神奈川県横浜市神奈川区六角橋 3 丁目 27-1）

主催：一般社団法人情報処理学会 情報処理教育委員会・初等中等教育委員会
共催：国立情報学研究所
後援：文部科学省、国立研究開発法人科学技術振興機構、独立行政法人情報処理推進機構、独立行政法人国立高等専門学校機構、公益社団法人全国高等学校文化連盟、全国高等学校情報教育研究会（予定）、全国専門学科情報科高等学校長会（予定）、一般社団法人 情報オリンピック日本委員会、情報学科・専攻協議会

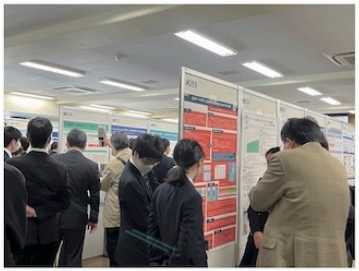
概要

情報処理学会では、第 86 回全国大会で、第 6 回目となる「中高生情報学研究コンテスト」を開催します。高校生なら「情報」、中学生なら「技術・家庭」技術分野「情報技術」に沿った探究活動など、日頃の情報学分野での学習成果のポスター発表を大募集します。

募集テーマ

高等学校共通教科情報科および中学校技術・家庭科技術分野「D 情報に関する技術」の趣旨に即した以下の分野

(1) 情報技術による問題解決
(2) 情報倫理とセキュリティ
(3) 情報システムとプログラミング
(4) 情報通信ネットワークとコミュニケーション
(5) 情報管理とデータベース
(6) 情報活用とデータサイエンス
(7) 情報デザインとコンテンツ



提出書類

(1) ポスター 1 枚
(2) 400 字の説明テキスト
(3) 2 分以内の動画または音声ファイル（オプション）

著作権について

第三者の図・表・写真を掲載する場合は、その出典を明記してください。その際、引用の条件を満たさない場合は必ず許諾を得てください。また、提出いただいた PDF、説明文、動画は情報処理学会のホームページ、学会誌等に掲載することがありますので予めご了承ください。

応募資格・参加費用

中学生や高校生、高専生（3 年まで）で構成されたチーム（4 名以下）でご応募ください。保護者または指導者など責任者が必要です。チームメンバーの少なくとも 1 名は情報処理学会ジュニア会員であること。ジュニア会員は、会費無料です（大学 3 年生まで会費無料）。
参加費は無料です（交通費、宿泊費は参加者負担）。

参加証

参加チームのメンバー全員に参加証明書を発行します。

参加（観覧）費用

ポスターセッションは参加費無料のセッションです。参加を希望する発表者、引率者・父母・学校関係者（職員・生徒）の方々は、無料でご参加いただけます。全国大会の他の無料のイベント企画も視聴できます。

発表に対するコメントと表彰について

全国大会初日から一般公開し、全国大会期間にコメントも受け付けます。全国大会終了後に各賞を発表します。なお、いただいたコメントについては、後日公開します。

中高生研究賞最優秀賞・文部科学大臣賞（1 件）
中高生研究賞優秀賞（最優秀賞とあわせて 3 件以内）
中高生研究賞奨励賞（数件）

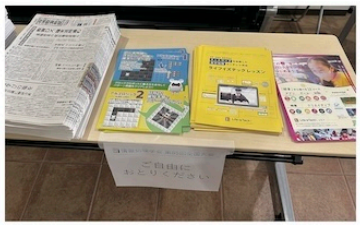
これ以外にも賞を設けることがあります。
中高生研究賞最優秀賞および優秀賞を受賞したチームは若手奨励賞候補として推薦されます。

応募をご検討の方へ（指導者向け）

情報処理学会初等中等教育委員会では、第 81 回全国大会から「中高生情報学研究コンテスト」を開始しました。募集分野は高校の共通教科情報と中学校の「技術・家庭」技術分野「情報技術」に基づいて挙げてありますので、高校生や高専生（3 年生以下）だけでなく中学生の応募も歓迎いたします。全国大会は毎年 3 月に実施され、その年ごとに違う都市で開催されます。今後も「中高生情報学研究コンテスト」は継続的に開催予定です。年間カリキュラムの一環、学習成果の発表の場、他校との情報交換の場としてぜひご活用くださいますようお願いいたします。

問合せ先

〒101-0062　東京都千代田区神田駿河台 1-5　化学会館 4F
一般社団法人情報処理学会　中高生情報学研究コンテスト
Tel: 03-3518-8373　Email: ipsjtaikaiPoster@ipsj.or.jp



[付録 2] IPSJ 中高生情報学研究コンテスト (2/2)

情報処理学会 (IPSJ) 第 6 回中高生情報学研究コンテスト受賞者

(https://bit.ly/46dQDU1)

中高生研究賞最優秀賞・文部科学大臣賞（1件）

- #2105　梶田光 ：数論的関数における数値計算の高速化
  梶田　光（横浜市立あざみ野中学校 3年）

中高生研究賞優秀賞（2件）

- #2016　トマールくん×マモールくん：スマート自転車「トマールくん」の開発ー交通事故防止アプリ「マモールくん」との連携プロジェクトを目指してー
  猪熊　蓮音（群馬県立前橋高等学校 2年），大嶋　輝希（群馬県立前橋高等学校 2年），金澤　侑一郎（群馬県立前橋高等学校 2年），湯澤　拓哉（群馬県立前橋高等学校 2年）
- #2034　齋藤智郎：広尾学園学園祭おける決済サービス「HirooPay」の開発について
  齋藤　智郎（広尾学園高等学校 2年）

中高生研究賞奨励賞・初等中等教育委員会 委員長賞（1件）

- #2013　エレウィルコンパニオン：車椅子安全装置(リアルタイムバックウオッチャー) ~AI搭載車椅子による身体障がい者外出支援~
  清水　孝一（群馬県立高崎高等学校 1年），清田　侑希（群馬県立高崎高等学校 1年）

中高生研究賞奨励賞・情報処理教育委員会 委員長賞（1件）

- #2085　玉川学園サイエンスクラブ協調作業班：仮想現実におけるコミュニケーションを用いた人との協調作業を行うロボットの機械学習モデルの検証
  國吉　仁志（玉川学園高等部 2年）

[付録3] マス・フォア・インダストリって何？

九州大学マス・フォア・インダストリ研究所の
中学 . 高校生向けアウトリーチ広報冊子
「マス・フォア・インダストリってなに？」
が出来上がりました。
以下の URL を参照して PDF ファイルをダウンロード下さい.

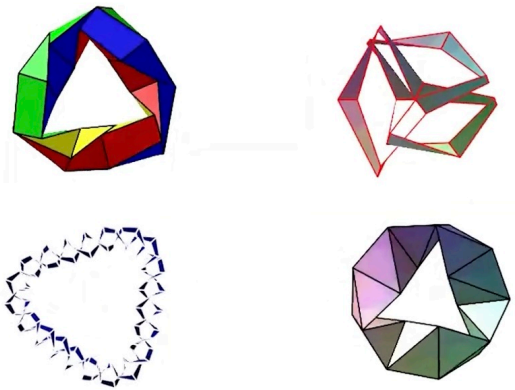
https://www.imi.kyushu-u.ac.jp/public/whats_mfi/

スマホ閲覧用 QR コード

[付録4] メビウス・カライドサイクル(発明)

計算された四面体で綺麗に回り続ける新しいカライドサイクルを発見
現代数学と折紙から生まれた新しい機構「メビウス・カライドサイクル」
by 九州大学マス・フォア・インダストリ研究所 鍛冶静雄教授

https://github.com/shizuo-kaji/Kaleidocycle/blob/master/README.ja.md



https://youtu.be/NULtOlnuVFU?si=WPtcuhLDileuikaE