アルゴリズム論特論 （塩田）

2015 年 7 月 17 日

有限体で広がる世界

1 体

Def.1 体 (たい) = 加減乗除の四則演算を持つ数体系

Ex.2 実数体、複素数体、有理数体、二元体 $\mathbf{F}_2$

Th.3 体上でできること

- 線形代数 → 線形符号
- 多項式論・方程式論 → 代数幾何学 → $\begin{cases} \text{有限幾何} \rightarrow \text{ブロックデザイン} \\ \text{楕円曲線暗号} \end{cases}$
- 環構造 → RSA 暗号
- 乗法構造 → 離散対数問題 → $\begin{cases} \text{Diffie-Hellman 鍵交換システム} \\ \text{ElGamal 暗号} \end{cases}$

Def.4 有限体 = 有限集合であって体であるもの

☆ 有限体がたくさんあれば色んな暗号や符号を設計できる。

2 有限体 $\mathbf{F}_p$

Th.5 p が素数であれば、mod p の剰余類の集合 $\mathbf{Z}/p\mathbf{Z}$ は体になる。「体」であることを強調するためにこれを $\mathbf{F}_p$ という記号で表す。

Pf. もともと加法・除法・乗法は定義できていた。さらに、$\bar{0}$ 以外の剰余類 $\bar{a}$ については

$$a \not\equiv 0 \bmod p \Rightarrow \gcd(a,p) = 1 \Rightarrow \bar{a}^{-1} \text{ が存在}$$

がなりたつ。つまり $\bar{0}$ 以外の数で割ることが出来る。□

Ex.6（ $\mathbf{F}_3$ 上のブロックデザイン ）　$\mathbf{F}_3$ 上の xy-平面で

$$V = \{\, \text{点} \,\} = \{\, v_1, v_2, \cdots, v_9 \,\},$$

$$\mathcal{B} = \{\, \text{直線} \,\} = \{\, B_1, B_2, \cdots, B_{12} \,\}$$

$v_1 : (0,0)$	$v_2 : (0,1)$	$v_3 : (0,2)$
$v_4 : (1,0)$	$v_5 : (1,1)$	$v_6 : (1,2)$
$v_7 : (2,0)$	$v_8 : (2,1)$	$v_9 : (2,2)$
$B_1 : x = 0$	$B_2 : x = 1$	$B_3 : x = 2$
$B_4 : y = 0$	$B_5 : y = 1$	$B_6 : y = 2$
$B_7 : x + y = 0$	$B_8 : x + y = 1$	$B_9 : x + y = 2$
$B_{10} : x + 2y = 0$	$B_{11} : x + 2y = 1$	$B_{12} : x + 2y = 2$

とすると、接続行列は

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

となり、これから二進符号が作れる。

Ex.7（ リードソロモン符号 ）　位数 (元の個数) の大きい有限体をアルファベットとする符号をリードソロモン符号と総称する。これはバースト誤り (連続したビット誤り) に強い誤り訂正符号である。

例えば、$\mathbf{F}_{13}$ 上の、誤り訂正能力 3 の符号を設計したとする。アルファベット $\bar{0}, \cdots, \bar{12}$ は 4 ビットで表現できるので、連続 6 ビットまでの誤りは 3 つのアルファベットにおさまり、正しく訂正することができる。

$$\cdots\ 1\ 0 \,\big|\, 0\ 1\ 1\ 1 \,\big|\, 1\ \ 0\ \ 1\ \ 1 \,\big|\, 1\ 0\ 0\ 1 \,\big|\, 1\ 1\ \cdots$$

$$\downarrow$$

$$\cdots\ 1\ 0 \,\big|\, 0\ 1\ 1\ \times \,\big|\, \times\ \times\ \times\ \times \,\big|\, \times\ 0\ 0\ 1 \,\big|\, 1\ 1\ \cdots$$

3　有限体 $\mathbf{F}_{p^n}$

Th.8　p^n を素数べきとすると、位数 (元の個数) が p^n の有限体が存在する。これを $\mathbf{F}_{p^n}$ と表す。(逆に有限体の位数は素数べきに限ることも知られている。)

Ex.9　(4 元体 $\mathbf{F}_4$)　$\mathbf{F}_4 = \{\, 0,\, 1,\, \alpha,\, \beta \,\}$　$(\beta = \alpha + 1)$　の四則演算は

$$\begin{cases} \bmod 2 \\ \alpha^2 = \alpha + 1 \end{cases}$$

のルールに従って行う。加法・減法は mod 2 で行えばよく、乗法の演算表は次のようになる：

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

例えば、

$$\alpha + \beta = \alpha + (\alpha + 1) = 2\alpha + 1 = 0\alpha + 1 = 1$$

$$\beta^2 = (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = (\alpha + 1) + 0\alpha + 1 = \alpha + 2 = \alpha$$

除法は、逆数を

$$\frac{1}{1} = 1, \quad \frac{1}{\alpha} = \beta, \quad \frac{1}{\beta} = \alpha$$

として計算すればよい。

Ex.10　(16 人麻雀)　16 人のプレーヤーが、4 卓 $\times$ 4 人 $\times$ 5 回の半荘で麻雀をして、どの 2 人も対戦できるように組み合わせを決めよう。

$\mathbf{F}_4$ 上の xy-平面で $V = \{\, \text{点} \,\}$, $\mathcal{B} = \{\, \text{直線} \,\}$ を考え、点とプレーヤー、直線と卓を対応付ける。

- $\mathcal{B}$ は 4 本の平行な直線からなる 5 つのグループに分かれる
- 2 つの点を通る直線は 1 本しかない

ことに着目すれば、次のような組み合わせができる：

1回目の半荘	$x=0$	:	00	01	0α	0β	が対戦
	$x=1$	:	10	11	1α	1β	が対戦
	$x=\alpha$	:	$\alpha 0$	$\alpha 1$	$\alpha\alpha$	$\alpha\beta$	が対戦
	$x=\beta$	:	$\beta 0$	$\beta 1$	$\beta\alpha$	$\beta\beta$	が対戦
2回目の半荘	$x+y=0$	:	00	11	$\alpha\alpha$	$\beta\beta$	が対戦
	$x+y=1$	:	01	10	$\alpha\beta$	$\beta\alpha$	が対戦
	$x+y=\alpha$	:	0α	1β	$\alpha 0$	$\beta 1$	が対戦
	$x+y=\beta$	:	0β	1α	$\alpha 1$	$\beta 0$	が対戦
3回目の半荘	$x+\alpha y=0$	:	00	1β	$\alpha 1$	$\beta\alpha$	が対戦
	$x+\alpha y=1$	:	0β	10	$\alpha\alpha$	$\beta 1$	が対戦
	$x+\alpha y=\alpha$	:	01	1α	$\alpha 0$	$\beta\beta$	が対戦
	$x+\alpha y=\beta$	:	0α	11	$\alpha\beta$	$\beta 0$	が対戦
4回目の半荘	$x+\beta y=0$	:	00	1α	$\beta 1$	$\alpha\beta$	が対戦
	$x+\beta y=1$	:	0α	10	$\beta\beta$	$\alpha 1$	が対戦
	$x+\beta y=\beta$	:	01	1β	$\beta 0$	$\alpha\alpha$	が対戦
	$x+\beta y=\alpha$	:	0β	11	$\beta\alpha$	$\alpha 0$	が対戦
5回目の半荘	$y=0$	:	00	10	$\alpha 0$	$\beta 0$	が対戦
	$y=1$	:	01	11	$\alpha 1$	$\beta 1$	が対戦
	$y=\alpha$	:	0α	1α	$\alpha\alpha$	$\beta\alpha$	が対戦
	$y=\beta$	:	0β	1β	$\alpha 1\beta$	$\beta\beta$	が対戦

Th.11 $\mathbf{F}_{p^n}$ は $\mathbf{F}_p$ 係数の多項式で法演算を行うことで定義でき、$\mathbf{F}_p$ 係数の多項式計算ルーティンを用いて実装される。例えば除法は「多項式のユークリッドアルゴリズム」の応用である。

☆ 工学系の教科書では $\mathbf{F}_{p^n}$ をガロワ体と呼び、$\mathrm{GF}(p^n)$ と書くことも多い。

4 まとめ

- 暗号編：整数計算を、上手にやると高速にできる計算と、高速にはできない計算に分類し、そのギャップを利用して公開鍵暗号は設計されている。
- 符号編：有限体、行列、有限幾何、ブロックデザインなどの数理構造を利用すると、誤り訂正能力などの性能の高い符号を設計できる。