巡回符号

$\mathcal{C}$: **巡回符号**

$$\Longleftrightarrow \sigma = (1\ 2\ \cdots\ n) \in \mathrm{Aut}(\mathcal{C})$$

$$\Longleftrightarrow$$

$$\big((c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C} \Rightarrow (c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}\big)$$

$\sigma = (1\ 2\ \cdots\ n) \in \mathfrak{S}_n, \sigma^n = 1$

$$\boldsymbol{F}_q[\langle\sigma\rangle] \simeq \boldsymbol{F}_q[X]/(X^n - 1) =: R \curvearrowright V = \boldsymbol{F}_q^n$$

により、V：階数 1 の自由 R-加群

$$V = \boldsymbol{F}_q^n \ \simeq \ R$$

$$(c_0, c_1, \ldots, c_{n-1}) \leftrightsquigarrow c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$$

$\mathcal{C}$：巡回符号 $\Longleftrightarrow$ $\mathcal{C}$：部分 R-加群

$V \simeq R$ と同一視するとき

$\Longleftrightarrow$ $\mathcal{C}$：R の ideal

$\mathcal{C}$: **巡回符号**

$\longleftrightarrow$ $R = \boldsymbol{F}_q[X]/(X^n - 1)$ **の ideal** $\mathfrak{a}$

$\longleftrightarrow$ $\mathfrak{a} \supset (X^n - 1)$ **なる** $\boldsymbol{F}_q[X]$ **の ideal** $\mathfrak{a}$

($\boldsymbol{F}_q[X]$ **: PID なので** $\exists f \in R : \mathfrak{a} = (f)$**)**

$\longleftrightarrow$ $f | X^n - 1$ **なる** $f \in \boldsymbol{F}_q[X]$

$X^n - 1 \in \boldsymbol{F}_q[X]$ **の分解が判れば、**
巡回符号が分類・構成できる !!

$X^n - 1 = g(X)h(X) \in \boldsymbol{F}_q[X]$ **のとき、**

$$\mathcal{C} := gR \text{：巡回符号} \simeq \boldsymbol{F}_q[X]/(h)$$
$$= \{c(X) \in R | h(X)c(X) = 0 \text{ in } R\}$$

g：**生成元多項式 (generator polynomial)**

h：**検査多項式 (check polynomial)**

$X^n - 1 \in \boldsymbol{F}_q[X]$ **の分解はどうなるのか ？**

代数学からの準備

$\longrightarrow$ **有限体の拡大・Galois 理論**

中国式剰余定理 (孫氏の定理)

m, n : **互いに素のとき**

$$\boldsymbol{Z}/mn\boldsymbol{Z} \simeq \boldsymbol{Z}/m\boldsymbol{Z} \times \boldsymbol{Z}/n\boldsymbol{Z}$$

$$x \bmod mn \leftrightsquigarrow (x \bmod m, x \bmod n)$$

$$bn \bmod mn \leftrightsquigarrow (1 \bmod m, 0 \bmod n)$$

$$am \bmod mn \leftrightsquigarrow (0 \bmod m, 1 \bmod n)$$

ここに、 a, b **は** $am + bn = 1$ **を満たす整数**
(Euclid の互除法)

有限体

$\boldsymbol{Z/mZ}$ **：体 (**0 **以外の元が全て可逆)**

$$\Longleftrightarrow m = p \text{ **：素数**}$$

$\boldsymbol{F_p := Z/pZ}$ **：** p **元体**

$F(X) \in \boldsymbol{F}_p[X]$ **：既約** $\Longrightarrow \boldsymbol{F}_p[X]/(F)$ **：体**

$\deg F = f$ **のとき、** $\#(\boldsymbol{F}_p[X]/(F)) = p^f =: q$

$\boldsymbol{F_q^\times = \langle g \rangle}$ **(**$\exists g \in \boldsymbol{F}_q^\times$**)：位数** $q-1$ **の巡回群**

Frobenius 自己同型・有限体の Galois 群

$q = p^f$, $a, b \in \boldsymbol{F}_q$ のとき、

$$(a+b)^p = a^p + b^p$$

$$(ab)^p = a^p b^p$$

$\varphi : \boldsymbol{F}_q \longrightarrow \boldsymbol{F}_q$: 体自己同型

$$x \longmapsto x^p$$

$$\varphi(x) = x \Longleftrightarrow x \in \boldsymbol{F}_p$$

$$\mathrm{Gal}(\boldsymbol{F}_q/\boldsymbol{F}_p) = \langle \varphi \rangle, \quad \varphi^f = 1$$

$q = 2$, $n = l$: **奇素数のとき、**

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

$$X^5 - 1 = (X+1)(X^4 + X^3 + X^2 + X + 1)$$

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

$$X^{11} - 1 = (X+1)(X^{10} + X^9 + \cdots + X + 1)$$

$$X^{13} - 1 = (X+1)(X^{12} + X^{11} + \cdots + X + 1)$$

$$X^{17} - 1 = (X+1)(X^8 + X^5 + X^4 + X^3 + 1)$$
$$(X^8 + X^7 + X^6 + X^4 + X^2 + X + 1)$$

$$X^{19} - 1 = (X+1)(X^{18} + X^{17} + \cdots + X + 1)$$

$$X^{23}-1=(X+1)$$
$$(X^{11}+X^9+X^7+X^6+X^5+X+1)$$
$$(X^{11}+X^{10}+X^6+X^5+X^4+X^2+1)$$
$$X^{29}-1=(X+1)(X^{28}+X^{27}+\cdots+X+1)$$
$$X^{31}-1=(X+1)(X^5+X^2+1)(X^5+X^3+1)$$
$$(X^5+X^3+X^2+X+1)$$
$$(X^5+X^4+X^2+X+1)$$
$$(X^5+X^4+X^3+X+1)$$
$$(X^5+X^4+X^3+X^2+1)$$
$$X^{37}-1=(X+1)(X^{36}+X^{35}+\cdots+X+1)$$

$q = 2$, $n = l$: **奇素数のとき、**

2 : $\mathrm{mod} l$ **で平方剰余** $\Longleftrightarrow l \equiv \pm 1 \pmod 8$

(平方剰余の第 2 **補充法則)**

この時は、 $\langle 2 \bmod l \rangle \subset \boldsymbol{F}_l^{\times 2}$

$Q := \boldsymbol{F}_l^{\times 2}$: **平方剰余全体**

$N := \boldsymbol{F}_l^{\times} \setminus \boldsymbol{F}_l^{\times 2} = u\boldsymbol{F}_l^{\times 2}$: **平方非剰余全体**

(u : **平方非剰余の** 1 **つ)**

Q, N: **共に Galois 不変**

$$f_Q(X) := \prod_{a \in Q} (X - \zeta_l^a)$$

$$f_N(X) := \prod_{a \in N} (X - \zeta_l^a)$$

とすると、

$$f_Q(X), f_N(X) \in \boldsymbol{F}_2[X]$$

で、

$$X^l - 1 = (X - 1) f_Q(X) f_N(X)$$

と分解する

$l \equiv \pm 1 \pmod 8$ **の時、**

$$X^l - 1 = (X-1) f_Q(X) f_N(X)$$

これから構成される符号 $\longrightarrow$ **平方剰余符号**
(quadratic residue code, QR code)

実際にはこの因数分解を求めるのが面倒
$\longrightarrow$ **冪等生成元 (idempotent generator)**
を用いると便利

冪等生成元 (idempotent generator)

$l \equiv \pm 1 \pmod 8$ **の時、**

$$e_Q(X) := \sum_{a \in Q} X^a, \qquad e_N(X) := \sum_{a \in N} X^a$$

とすると、 $R = \boldsymbol{F}_2[X]/(X^l - 1)$ **内で**

$$e_Q(X)^2 = e_Q(X), \quad e_N(X)^2 = e_N(X)$$

$$1 + e_Q(X) + e_N(X) = X^{l-1} + \cdots + X + 1$$

定理

(ζ_l の取り方により)

$l \equiv -1 \pmod 8$ **の時、**

$$(e_Q) = (f_Q), \quad (1 + e_Q) = ((X-1)f_N)$$
$$(e_N) = (f_N), \quad (1 + e_N) = ((X-1)f_Q)$$

定理

$l \equiv \pm 1 \pmod 8$ **の時、**

QR code の最小距離 d **について、**

- $d^2 \geq l$ **(square root bound)**

  ($l \equiv -1 \pmod 8$ **なら** $d^2 - d + 1 \geq l$**)**

- $d \equiv 3 \pmod 4$

例: $l = 7$

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

$$f_Q(X) = X^3 + X + 1$$

$$e_Q(X) = X^4 + X^2 + X = X f_Q(X)$$

$\longrightarrow$ $[7, 4, 3]$-**Hamming 符号**

$\cdots$ **パリティ検査 bit を付け加えた拡張符号は**
位数 168 **の単純群** $\mathrm{PSL}(2, \boldsymbol{F}_7)$ **を**
自己同型群に持つ $[8, 4, 4]$-**符号**

Hamming の球充填上界

(F_2 上の線型符号の場合)

F_2 上の $[n, k, 2t+1]$-符号について

$$\sum_{s=0}^{t} \binom{n}{s} \leq 2^{n-k}$$

例: $l = 23$

$$X^{23} - 1 = (X + 1)$$
$$(X^{11} + X^9 + X^7 + X^6 + X^5 + X + 1)$$
$$(X^{11} + X^{10} + X^6 + X^5 + X^4 + X^2 + 1)$$

$$e_Q(X) = X + X^2 + X^4 + X^8 + X^{16} + X^9$$
$$+ X^{18} + X^{13} + X^3 + X^6 + X^{12}$$

$\longrightarrow$ **Goley 符号**

$\cdots$ **Matthew 群** M_{23} **を自己同型群に持つ**

$[23, 12, 7]$-**符号**

誤り訂正符号には、他にも、

- **Reed-Muller 符号**
- **BCH 符号**
  (Bose,Ray-Chaudhuri,Hocquenghem)
- **Reed-Solomon 符号**
- **Goppa 符号**

など、重要なものがあるが、

本講義ではここまで。

情報通信を行なう際の要請

- **効率的に** $\longrightarrow$ **情報理論**
- **確実に** $\longrightarrow$ **符号理論**
- **安全に** $\longrightarrow$ **暗号理論**

情報通信を行なう際の要請

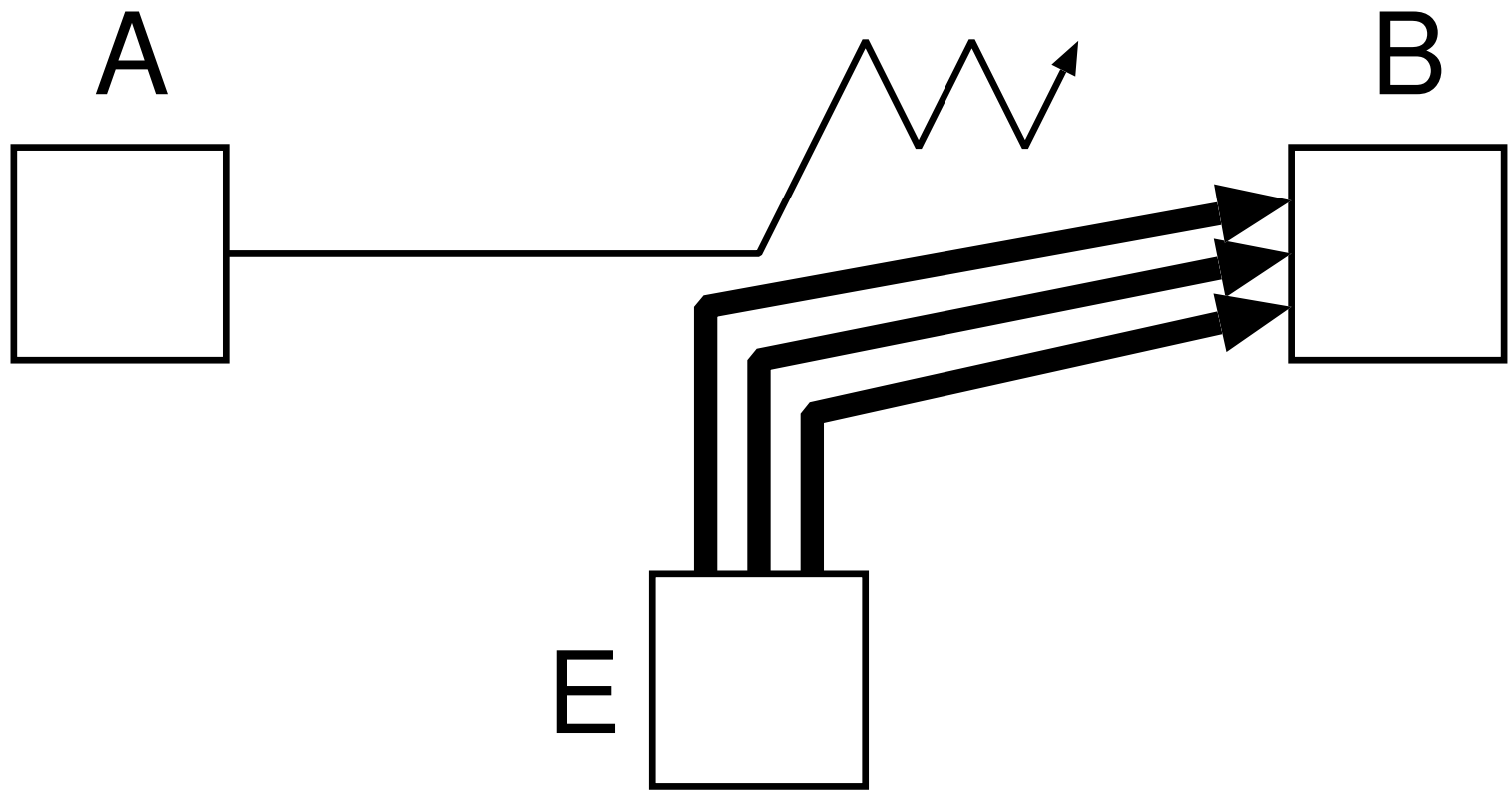
- **効率的に** $\longrightarrow$ **情報理論**
- **確実に** $\longrightarrow$ **符号理論**
- **安全に** $\longrightarrow$ **暗号理論**

安全な情報伝達を阻害するもの

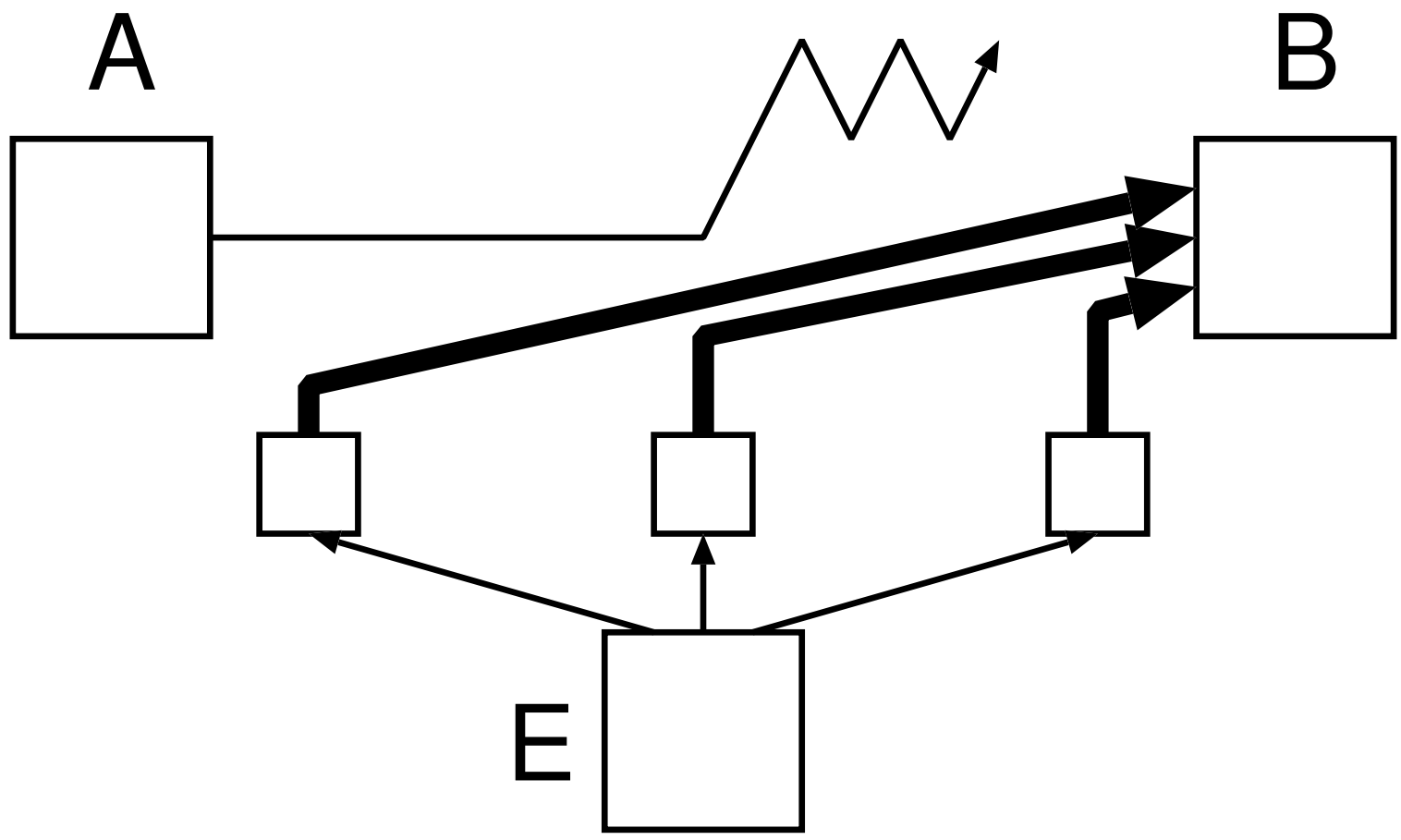
- 妨害 (DoS 攻撃など)
- 盗聴
- 改竄
- なり済まし

など

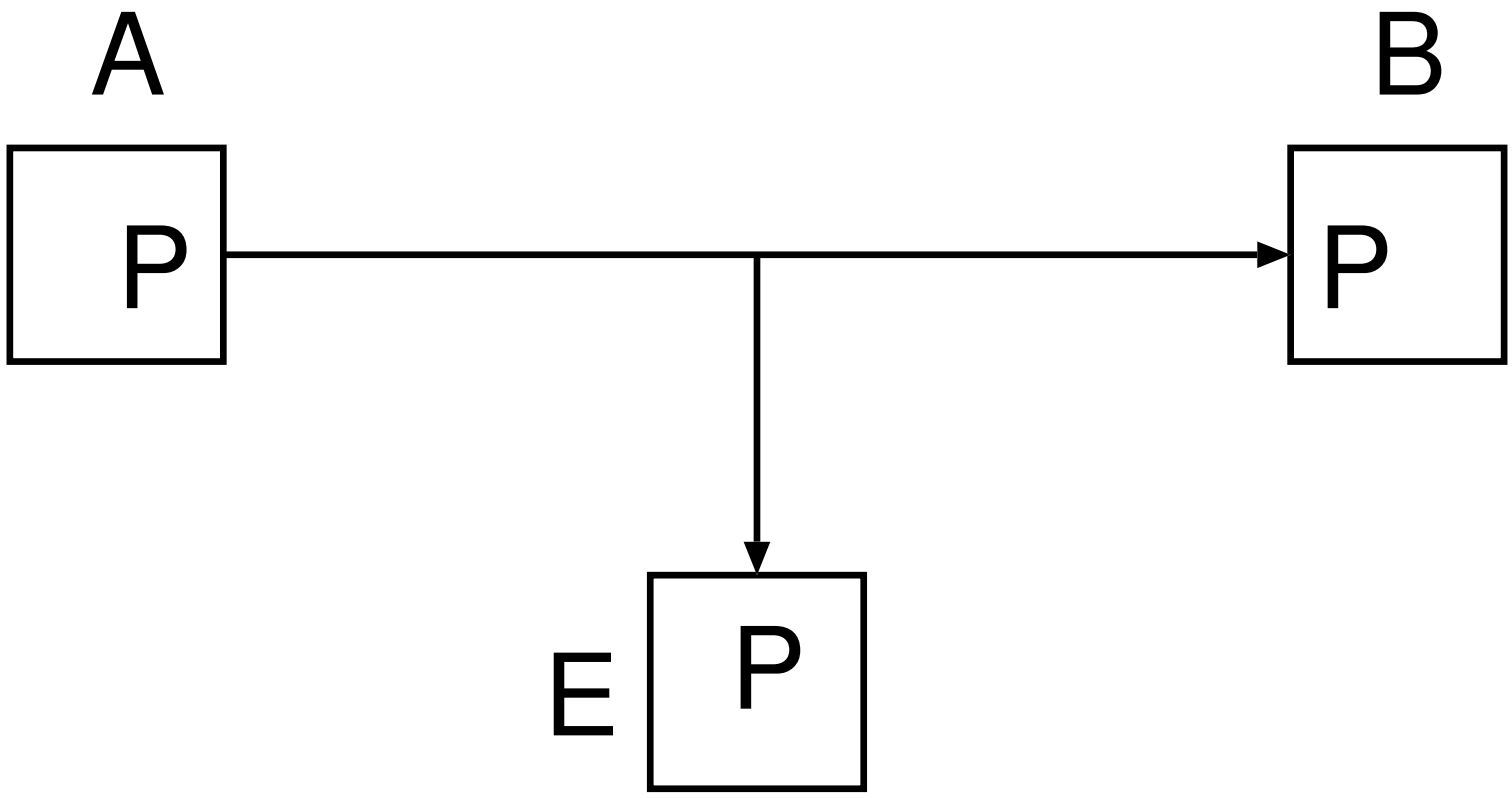
DoS (Denial of Service) 攻撃



DoS (Denial of Service) 攻撃



盗聴



暗号通信で盗聴対策