# 有限群の一様巡回群分解

品川（茨城）

## §1 イントロ

**Notations**

$G$ : 有限群

$\mathcal{H} = (H_1, \cdots, H_k)$ : $G$の部分集合の族.

$H_1 \cdots H_k := \{ h_1 h_2 \cdots h_k \in G \mid h_1 \in H_1, \cdots, h_k \in H_k \}$

**Definition**

$G = H_1 \cdots H_k$ のとき, $\mathcal{H} = (H_1, \cdots, H_k)$ を $G$の分解 (factorization) という.

### 有限群論の文脈

**Theorem** [Szép '50, 51]

$G = H_1 H_2$ で $H_1, H_2$: maximal non-normal subgroups & $\gcd(|H_1|, |H_2|) = 1$.

このとき, $G$は単純群.

⇝ いつ $G$は maximal な分解をもつか？ は自然な問いになった.

### 暗号理論の文脈

**Definition**

$\mathcal{H}$が$G$の分解で, $|G| = |H_1| \cdots |H_k|$ となるものを exact と呼ぶ.

⇝ [Magliveras '86] : exact factorization を用いた暗号方式を構成

$\parallel$

logarithmic signature. (LS).

LSのサイズ $:= \sum_{i=1}^{k} |H_i|$ で定義する.

**Theorem** [Gonzalez-Vasso, Steinwandt '02]

$G$の任意のLSについて, $|G| = p_1^{a_1} \cdots p_\ell^{a_\ell}$ なら

$$(\text{LSのサイズ}) \geq \sum_{i=1}^{\ell} a_i p_i$$

である.

等号を成立させるLSを 最小対数シグネチャ (minimal logarithmic signature) という.

⇝ 任意の有限群がMLSをもつか？

## §2 一様巡回群分解

$G$：有限群
$\mathcal{H} := (H_1, \cdots, H_t)$：$G$の部分集合の列．
$g \in G$に対して，

$$fac_{\mathcal{H}}(g) := \{ (h_1, \cdots, h_t) \in H_1 \times \cdots \times H_t \mid h_1 \cdots h_t = g \}$$

とおく．

$t$を為重度と呼ぶ．

**Definition**

- $\mathcal{H}$が$G$の一様分解（uniform factorization） $\overset{\text{def}}{\Leftrightarrow}$ $\#(fac_{\mathcal{H}}(g)) = {}^{\exists}t$ for $^{\forall}g \in G$.
- $\mathcal{H}$が$G$の一様群分解（uniform group factorization）
  $\overset{\text{def}}{\Leftrightarrow}$ $\mathcal{H}$は一様分解，$H_1, \cdots, H_t \leq G$.
- $\mathcal{H}$が$G$の一様巡回群分解（uniform cyclic group factorization）
  $\overset{\text{def}}{\Leftrightarrow}$ $\mathcal{H}$は一様群分解，$H_1, \cdots, H_t$は巡回部分群

**Remark**

・分解のとり方はたくさんある．例えば，$\mathfrak{S}_5$について，

$$H = (\langle (1,2) \rangle, \langle (123) \rangle, \langle (1234) \rangle, \langle (12345) \rangle)$$
$$H' = (\langle (12345) \rangle, \langle (1243) \rangle, \langle (123)(45) \rangle).$$

は共にUCF.

・$G$自身は自明なUF（UGF）である．

$\mathcal{H} = (H_1, \cdots, H_t)$の$H_1, \cdots, H_t$が真部分集合のとき non-trivial な分解 と呼ぶ．

**Remark**

$G = C_n$（巡回群）のとき，

- $|G| = 1$ or 素数冪 $\Rightarrow$ $C_n$はnon-trivialなUGFをもたない．

☺

$n = p^k$, $C_n = \langle \sigma \rangle$ $\rightsquigarrow$ $C_n$の非自明な部分群は $\langle \sigma^p \rangle, \cdots, \langle \sigma^{p^{k-1}} \rangle$ のみ．
これらをどのように用いても$\sigma$を構成できない．

- $n$が素数冪でない $\Rightarrow$ $C_n$はnon-trivialなUGFをもたない．

☺

| $n = n_1 n_2$ $(\gcd(n_1, n_2) = 1)$ とすれば, $C_n = \langle \sigma^{n_2} \rangle \langle \sigma^{n_1} \rangle$.

## §3 主結果.

| | | non-trivial UGF |
|---|---|---|
| ・ 自明群 | | × |
| ・ 巡回群 | —— 素数冪 | × |
| | 素数冪 ではない | ○ |
| ・ 非巡回群 | —— 非単純群 | ? |
| | 単純群 | ? |

$\mathcal{G}_n := \{$位数 $n$ 以下の有限群$\} / \simeq$

∪|

$\mathcal{G}_n^+ := \{ G \in \mathcal{G}_n \mid G$ は自明群 および 素数冪の巡回群 $\in$ のぞく $\} / \simeq$

∪|

$\mathcal{G}_n^* := \{ G \in \mathcal{G}_n^+ \mid G$ は単純群$\} / \simeq$.

Main result

TFAE :

(a) $\forall G \in \mathcal{G}_n$ は UGF をもつ.

(b) $\forall G \in \mathcal{G}_n^+$ は non-trivial な UGF をもつ.

(c) $\forall G \in \mathcal{G}_n^*$ は non-trivial な UGF をもつ.

(b), (c) 非自明.

## §4 Application.

### Application 1

群要素の ランダム 生成

**愚直な方法**

1 : $G = \{g_1, \cdots, g_{|G|}\}$ を メモリに 展開
2 : $x \in \{1, 2, \cdots, |G|\}$ を 一様ランダムに 選ぶ.
3 : $g_x$ を出力.

**UCFを用いる方法**

1 : $G = \langle \sigma_1 \rangle \cdots \langle \sigma_k \rangle$ として, $\{\sigma_1, \cdots, \sigma_k\}$ を 展開.
2 : 各 $i$ について $x_i \in \{1, 2, \cdots, \mathrm{ord}(\sigma_i)\}$ を 一様ランダムに生成
3 : $g := \sigma_1^{x_1} \cdots \sigma_k^{x_k}$ を出力.

### Application 2.

カードベース暗号 の Shuffle.

$G \leq \mathfrak{S}_n$ に対して, カードを ランダムな $g \in G$ で 並び替える 操作を $G$-shuffle という.
$G = C_1 \cdots C_k$ なら, $G$-shuffle を $C_i$-shuffle で 置きかえられる.