On Compression Functions over Groups with Applications to Homomorphic Encryption

(arXiv:2208.02468)

Koji Nuida

Institute of Mathematics for Industry (IMI), Kyushu University
(nuida@imi.kyushu-u.ac.jp)

Algebra and Cryptology Seminar
(Stevens Institute of Technology, USA)
September 29, 2025

Contents

Contents

Public Key Encryption

- Plaintext m is concealed by encrypting it
  - Let $[[m]]$ denote a ciphertext for m
- **Encryption** $\mathsf{Enc}_{\mathsf{pk}} : m \mapsto [[m]]$
  - pk: public encryption key
- **Decryption** $\mathsf{Dec}_{\mathsf{sk}} : [[m]] \mapsto m$
  - sk: secret decryption key
- It should be computationally hard to guess any information on m from $[[m]]$ and pk (w/o sk)

Homomorphic Encryption (HE)

- Can compute a function for plaintexts inside ciphertexts w/o decryption
- **Homomorphic evaluation** (**operation**) $\mathsf{Eval}_{\mathsf{ek}}(f; [[m_1]], \dots, [[m_k]]) = [[f(m_1, \dots, m_k)]]$
  - ek: public evaluation key
- E.g., $[[m_1]] \boxplus [[m_2]] = [[m_1 + m_2]]$, $[[b_1]] \wedge [[b_2]] = [[b_1 \wedge b_2]]$

Fully Homomorphic Encryption (FHE)

- HE for **arbitrary** function
  - by combining hom. eval. of some fundamental operations (e.g., $\neg$, $\oplus$, $\wedge$, ...)
- Firstly realized by [Gentry, 2009]
- Almost all known FHE are lattice-based
- Some are based on approximate GCD
  - except for (doubtful) preprints on others

Example: [van Dijk et al., 2010]

- $[[m]] = p\alpha + 2r + m \ (m \in \{0,1\})$
  - p: secret prime, α, r: random
- $\mathrm{Dec}([[m]]) = ([[m]] \bmod p) \bmod 2$ **if the "noise" $2r$ is sufficiently small**
- $[[m_1]] \boxplus [[m_2]] = [[m_1]] + [[m_2]]$
  - $= p(\alpha_1 + \alpha_2) + 2(r_1 + r_2) + m_1 + m_2$
- $[[m_1]] \boxtimes [[m_2]] = [[m_1]] \times [[m_2]]$
  - $= p(\text{some complicated term})$
    $+ 2(\text{some complicated term}) + m_1 \times m_2$

- Ciphertext noise grows via Eval
  - Dec will fail finally
- A “bootstrapping” can reset the noise
  - but generally a heavy operation
- All known FHE are noise-based
- **Open Problem: not noise-based FHE**

Contents

Group Function (Univariate Case)

- on group G means a sequence of the form

$$g_0 x g_1 x g_2 \cdots g_{n-1} x g_n$$

($g_i \in G$, x: variable)

- Regarded as a function

$$G \to G \, , \; h \mapsto g_0 h g_1 h g_2 \cdots g_{n-1} h g_n$$

- E.g., for $F(x) := xgx^2g'$, $F(h) = hgh^2g' \in G$

An Ongoing Approach to FHE

(1) Encode bit b into an element σ_b of a group G

An Ongoing Approach to FHE

(1) Encode bit b into an element σ_b of a group G

(2) For each fundamental bit operation, implement it as a group function on G

- E.g., $F_{\mathrm{AND}}(\sigma_{b_1}, \sigma_{b_2}) = \sigma_{\mathrm{AND}(b_1,b_2)}$, i.e., $F_{\mathrm{AND}}(\sigma_0, \sigma_0) = F_{\mathrm{AND}}(\sigma_0, \sigma_1) = F_{\mathrm{AND}}(\sigma_1, \sigma_0) = \sigma_0$, $F_{\mathrm{AND}}(\sigma_1, \sigma_1) = \sigma_1$

(1) Encode bit b into an element σ_b of a group G

(2) For each fundamental bit operation, implement it as a group function on G

- E.g., $F_{\mathrm{AND}}(\sigma_{b_1}, \sigma_{b_2}) = \sigma_{\mathrm{AND}(b_1, b_2)}$, i.e., $F_{\mathrm{AND}}(\sigma_0, \sigma_0) = F_{\mathrm{AND}}(\sigma_0, \sigma_1)$ $= F_{\mathrm{AND}}(\sigma_1, \sigma_0) = \sigma_0$, $F_{\mathrm{AND}}(\sigma_1, \sigma_1) = \sigma_1$

(3) Construct HE for plaintext space G; i.e., hom. eval. of multiplication $\cdot_G$ is possible

An Ongoing Approach to FHE

(1) Encode bit b into an element σ_b of a group G

(2) For each fundamental bit operation, implement it as a group function on G

- E.g., $F_{\mathrm{AND}}(\sigma_{b_1}, \sigma_{b_2}) = \sigma_{\mathrm{AND}(b_1,b_2)}$, i.e., $F_{\mathrm{AND}}(\sigma_0, \sigma_0) = F_{\mathrm{AND}}(\sigma_0, \sigma_1)$ $= F_{\mathrm{AND}}(\sigma_1, \sigma_0) = \sigma_0$, $F_{\mathrm{AND}}(\sigma_1, \sigma_1) = \sigma_1$

(3) Construct HE for plaintext space G; i.e., hom. eval. of multiplication $\cdot_G$ is possible

- $\rightsquigarrow$ By defining $\mathrm{Enc}'(b_i) := [[\sigma_{b_i}]]$, e.g., $\mathrm{Eval}'(\mathrm{AND}; [[b_1]]', [[b_2]]')$ $:= \mathrm{Eval}(F_{\mathrm{AND}}; [[\sigma_{b_1}]], [[\sigma_{b_2}]])$ $= [[\sigma_{\mathrm{AND}(b_1,b_2)}]] = [[\mathrm{AND}(b_1, b_2)]]'$

An Ongoing Approach to FHE

- Thus constructing FHE is reduced to (2) & (3)
  - where (3) is the most difficult (unsolved)

An Ongoing Approach to FHE

- Thus constructing FHE is reduced to (2) & (3)
  - where (3) is the most difficult (unsolved)
- [Grigoriev & Ponomarenko, 2004] firstly mentioned such an approach
  - where (2) uses [Barrington et al., 1990]

An Ongoing Approach to FHE

- Thus constructing FHE is reduced to (2) & (3)
  - where (3) is the most difficult (unsolved)
- [Grigoriev & Ponomarenko, 2004] firstly mentioned such an approach
  - where (2) uses [Barrington et al., 1990]
- [Ostrovsky & Skeith III, 2008] re-invented
  - where (2) uses commutators in simple groups

An Ongoing Approach to FHE

- Thus constructing FHE is reduced to (2) & (3)
  - where (3) is the most difficult (unsolved)
- [Grigoriev & Ponomarenko, 2004] firstly mentioned such an approach
  - where (2) uses [Barrington et al., 1990]
- [Ostrovsky & Skeith III, 2008] re-invented
  - where (2) uses commutators in simple groups
- [N., 2021] formalized a similar approach
  - Preprint in 2014

Step (2) in [N., 2021]

- Called "approximate-then-adjust" method

Step (2) in [N., 2021]

- Called "approximate-then-adjust" method
- E.g., when $\sigma_0 := 1 \in G$ and $\sigma_1 := \sigma$, OR is approximated by multiplication $\sigma_{b_1}\sigma_{b_2}$

Step (2) in [N., 2021]

- Called "approximate-then-adjust" method
- E.g., when $\sigma_0 := 1 \in G$ and $\sigma_1 := \sigma$, OR is approximated by multiplication $\sigma_{b_1}\sigma_{b_2}$
  - $\sigma_0\sigma_0 = 1 = \sigma_0 = \sigma_{\mathrm{OR}(0,0)}$
  - $\sigma_0\sigma_1 = \sigma = \sigma_1 = \sigma_{\mathrm{OR}(0,1)}$
  - $\sigma_1\sigma_0 = \sigma = \sigma_1 = \sigma_{\mathrm{OR}(1,0)}$
  - But $\sigma_1\sigma_1 = \sigma^2 \neq \sigma_1 = \sigma_{\mathrm{OR}(1,1)}$

Step (2) in [N., 2021]

- Called "approximate-then-adjust" method
- E.g., when $\sigma_0 := 1 \in G$ and $\sigma_1 := \sigma$, OR is approximated by multiplication $\sigma_{b_1}\sigma_{b_2}$
  - $\sigma_0\sigma_0 = 1 = \sigma_0 = \sigma_{\mathrm{OR}(0,0)}$
  - $\sigma_0\sigma_1 = \sigma = \sigma_1 = \sigma_{\mathrm{OR}(0,1)}$
  - $\sigma_1\sigma_0 = \sigma = \sigma_1 = \sigma_{\mathrm{OR}(1,0)}$
  - But $\sigma_1\sigma_1 = \sigma^2 \neq \sigma_1 = \sigma_{\mathrm{OR}(1,1)}$
- The incorrect result σ^2 should be adjusted to σ while keeping 1 and σ unchanged
  - by a group function F s.t. $F(1) = 1$ and $F(\sigma) = F(\sigma^2) = \sigma$

Step (2) in [N., 2021]

- When $\sigma_1 = \sigma$ has order 3, the same function F can adjust the incorrect results of the followings (taken from [N., arXiv 2022]):
  - OR: $\sigma_{b_1}\sigma_{b_2}$
  - NAND (NOT AND): $\sigma\sigma_{b_1}\sigma_{b_2}$
  - XOR: ${\sigma_{b_1}}^2\sigma_{b_2}$
  - EQ (=): $\sigma^2\sigma_{b_1}\sigma_{b_2}$
  - 3-NEQ (NOT $b_1 = b_2 = b_3$): $\sigma_{b_1}\sigma_{b_2}\sigma_{b_3}$

- For the "compression" function F s.t. $F(1) = 1$ and $F(\sigma) = F(\sigma^2) = \sigma$, the following function on $G = S_5$ was found by a heuristic approach where $\sigma := (1\ 2\ 3)$:

$$F(x) = (1\ 5)(2\ 3\ 4)x(2\ 3\ 4)x(3\ 4)x^2(2\ 3)(4\ 5) \\ \cdot x(2\ 3\ 4)x(3\ 4)x^2(1\ 4\ 2\ 5)$$

Step (2) in [N., 2021]

- For the "compression" function F s.t. $F(1) = 1$ and $F(\sigma) = F(\sigma^2) = \sigma$, the following function on $G = S_5$ was found by a heuristic approach where $\sigma := (1\ 2\ 3)$:

$$F(x) = (1\ 5)(2\ 3\ 4)x(2\ 3\ 4)x(3\ 4)x^2(2\ 3)(4\ 5) \cdot x(2\ 3\ 4)x(3\ 4)x^2(1\ 4\ 2\ 5)$$

- **Question: More systematic approach?**
  - More efficient construction?
  - (Im)possibility on smaller groups, e.g., S_4? (Step (3) might be easier)

Remark on Step (3)

- HE over a group G will be obtained when $\exists$ surj. group hom. $\varphi\colon \widetilde{G} \to G$ s.t.
  - preimage of $g \in G$ can be efficiently sampled (encryption),
  - computation of φ (decryption) is efficient when a secret key sk is given, but is hard when sk is not given

Remark on Step (3)

- HE over a group G will be obtained when $\exists$ surj. group hom. $\varphi\colon \widetilde{G} \to G$ s.t.
  - preimage of $g \in G$ can be efficiently sampled (encryption),
  - computation of φ (decryption) is efficient when a secret key sk is given, but is hard when sk is not given
- Candidate over any finite G was given in [Grigoriev & Ponomarenko, 2004] but broken by [Choi et al., 2007]
  - Even if it were not broken, the HE is not compact ($\widetilde{G}$ is an **infinite** group)

Contents

- Re-formulating existence of such a function by existence of solutions for certain equations
- $\nexists$, when G is a finite solvable group (including Abelian groups and S_n, $n \leq 4$)
- If $\exists$ on S_5, then $\exists$ on A_5 ($\therefore$ no advantage of considering S_5)
- Shortest possible expression on A_5

Re-formulation of Problem

Definition 1

A compression function of **type** $(\sigma; (\mu_i, \rho_i)_{i=1}^{L})$, **size** ℓ, and **exponent** $(e_1, e_2, \dots, e_\ell)$ is a group function of the form

$$F(x) = g_0 x^{e_1} g_1 x^{e_2} \cdots g_{\ell-1} x^{e_\ell} g_\ell$$

s.t. $F(\sigma^{\mu_i}) = \rho_i \ (\forall i)$.

Re-formulation of Problem

Definition 1

A compression function of **type** $(\sigma; (\mu_i, \rho_i)_{i=1}^{L})$, **size** ℓ, and **exponent** $(e_1, e_2, \dots, e_\ell)$ is a group function of the form

$$F(x) = g_0 x^{e_1} g_1 x^{e_2} \cdots g_{\ell-1} x^{e_\ell} g_\ell$$

s.t. $F(\sigma^{\mu_i}) = \rho_i \ (\forall i)$.

- Here we only consider "normalized" types w/ $(\mu_1, \rho_1) = (0, 1)$ (i.e., $F(1) = 1$)
- Our target function is normalized of type $(\sigma; (0,1), (1,\sigma), (2,\sigma))$ s.t. $\mathrm{ord}(\sigma) = 3$

Lemma 2

$\exists F$ of (normalized) type $(\sigma; (\mu_i, \rho_i)_{i=1}^{L})$, size ℓ, and exponent $(e_1, \dots, e_\ell)$ over a group G $\iff$ the equations

$$y_1^{\mu_i e_1} y_2^{\mu_i e_2} \cdots y_\ell^{\mu_i e_\ell} = \rho_i \quad (i = 2, \dots, L)$$

*have a solution $(\tau_1, \dots, \tau_\ell) \in G^\ell$ w/ the **conjugacy condition**: $\forall i$, τ_i is conjugate to σ in G.*

Lemma 2

$\exists F$ of (normalized) type $(\sigma; (\mu_i, \rho_i)_{i=1}^{L})$, size ℓ, and exponent $(e_1, \dots, e_\ell)$ over a group G
$\iff$ the equations

$$y_1^{\mu_i e_1} y_2^{\mu_i e_2} \cdots y_\ell^{\mu_i e_\ell} = \rho_i \quad (i = 2, \dots, L)$$

have a solution $(\tau_1, \dots, \tau_\ell) \in G^\ell$ w/ the ***conjugacy condition****: $\forall i$, τ_i is conjugate to σ in G.*

Corollary 3

$\exists$ our target function $\iff$ the equations $y_1^{e_1} \cdots y_\ell^{e_\ell} = \sigma$ and $y_1^{2e_1} \cdots y_\ell^{2e_\ell} = \sigma$ have a solution w/ the conjugacy condition.

(Proof)

$$F(\sigma^{\mu_i}) = g_0 \sigma^{\mu_i e_1} g_1 \cdots g_{\ell-1} \sigma^{\mu_i e_\ell} g_\ell$$

(Proof)

$$F(\sigma^{\mu_i}) = g_0 \sigma^{\mu_i e_1} g_1 \cdots g_{\ell-1} \sigma^{\mu_i e_\ell} g_\ell$$

$$= (g_0 \sigma^{\mu_i e_1} {g_0}^{-1}) \cdot (g_0 g_1 \sigma^{\mu_i e_2} (g_0 g_1)^{-1})$$

$$\cdots (g_0 g_1 \cdots g_{\ell-1} \sigma^{\mu_i e_\ell} (g_0 g_1 \cdots g_{\ell-1})^{-1}) \cdot g_0 g_1 \cdots g_\ell$$

Re-formulation of Problem

(Proof)

$$
\begin{aligned}
F(\sigma^{\mu_i}) &= g_0 \sigma^{\mu_i e_1} g_1 \cdots g_{\ell-1} \sigma^{\mu_i e_\ell} g_\ell \\
&= (g_0 \sigma^{\mu_i e_1} {g_0}^{-1}) \cdot (g_0 g_1 \sigma^{\mu_i e_2} (g_0 g_1)^{-1}) \\
&\quad \cdots (g_0 g_1 \cdots g_{\ell-1} \sigma^{\mu_i e_\ell} (g_0 g_1 \cdots g_{\ell-1})^{-1}) \cdot g_0 g_1 \cdots g_\ell \\
&= (g_0 \sigma {g_0}^{-1})^{\mu_i e_1} \cdot (g_0 g_1 \sigma (g_0 g_1)^{-1})^{\mu_i e_2} \\
&\quad \cdots (g_0 g_1 \cdots g_{\ell-1} \sigma (g_0 g_1 \cdots g_{\ell-1})^{-1})^{\mu_i e_\ell} \cdot g_0 g_1 \cdots g_\ell
\end{aligned}
$$

Re-formulation of Problem

(Proof)

$$F(\sigma^{\mu_i}) = g_0\sigma^{\mu_i e_1} g_1 \cdots g_{\ell-1}\sigma^{\mu_i e_\ell} g_\ell$$

$$= (g_0\sigma^{\mu_i e_1}{g_0}^{-1}) \cdot (g_0 g_1 \sigma^{\mu_i e_2}(g_0 g_1)^{-1})$$

$$\cdots (g_0 g_1 \cdots g_{\ell-1}\sigma^{\mu_i e_\ell}(g_0 g_1 \cdots g_{\ell-1})^{-1}) \cdot g_0 g_1 \cdots g_\ell$$

$$= (g_0 \sigma {g_0}^{-1})^{\mu_i e_1} \cdot (g_0 g_1 \sigma (g_0 g_1)^{-1})^{\mu_i e_2}$$

$$\cdots (g_0 g_1 \cdots g_{\ell-1} \sigma (g_0 g_1 \cdots g_{\ell-1})^{-1})^{\mu_i e_\ell} \cdot g_0 g_1 \cdots g_\ell$$

$$= (g_0 \sigma {g_0}^{-1})^{\mu_i e_1} \cdot (g_0 g_1 \sigma (g_0 g_1)^{-1})^{\mu_i e_2}$$

$$\cdots (g_0 g_1 \cdots g_{\ell-1} \sigma (g_0 g_1 \cdots g_{\ell-1})^{-1})^{\mu_i e_\ell} \ (\because F(1) = 1)$$

(Proof)

$$F(\sigma^{\mu_i}) = g_0\sigma^{\mu_i e_1} g_1 \cdots g_{\ell-1}\sigma^{\mu_i e_\ell} g_\ell$$

$$= (g_0\sigma^{\mu_i e_1} {g_0}^{-1}) \cdot (g_0 g_1 \sigma^{\mu_i e_2} (g_0 g_1)^{-1})$$
$$\cdots (g_0 g_1 \cdots g_{\ell-1}\sigma^{\mu_i e_\ell}(g_0 g_1 \cdots g_{\ell-1})^{-1}) \cdot g_0 g_1 \cdots g_\ell$$

$$= (g_0\sigma {g_0}^{-1})^{\mu_i e_1} \cdot (g_0 g_1 \sigma (g_0 g_1)^{-1})^{\mu_i e_2}$$
$$\cdots (g_0 g_1 \cdots g_{\ell-1}\sigma(g_0 g_1 \cdots g_{\ell-1})^{-1})^{\mu_i e_\ell} \cdot g_0 g_1 \cdots g_\ell$$

$$= (g_0\sigma {g_0}^{-1})^{\mu_i e_1} \cdot (g_0 g_1 \sigma (g_0 g_1)^{-1})^{\mu_i e_2}$$
$$\cdots (g_0 g_1 \cdots g_{\ell-1}\sigma(g_0 g_1 \cdots g_{\ell-1})^{-1})^{\mu_i e_\ell} \; (\because F(1) = 1)$$

Then $\tau_j := g_0 g_1 \cdots g_{j-1}\sigma(g_0 g_1 \cdots g_{j-1})^{-1}$. □

Abelian or Size 2 Cases

Lemma 4

If $\exists i_1 \neq i_2$ *s.t.* $\rho_{i_1} = \rho_{i_2} \neq 1$ *and* $\mu_{i_2} = \mu_{i_1} + 1$ *(e.g., our target function), then* $\nexists$ *solution* $(\tau_1, \ldots, \tau_\ell)$ *s.t.* $\tau_1, \ldots, \tau_{\ell-1}$ *commute or* $\tau_2, \ldots, \tau_\ell$ *commute.*

Note: Here conj. cond. is not concerned.

Lemma 4

If $\exists i_1 \neq i_2$ *s.t.* $\rho_{i_1} = \rho_{i_2} \neq 1$ *and* $\mu_{i_2} = \mu_{i_1} + 1$ *(e.g., our target function), then* $\nexists$ *solution* $(\tau_1, \ldots, \tau_\ell)$ *s.t.* $\tau_1, \ldots, \tau_{\ell-1}$ *commute or* $\tau_2, \ldots, \tau_\ell$ *commute.*

Note: Here conj. cond. is not concerned.

(Proof) When $\tau_1, \ldots, \tau_{\ell-1}$ commute,

Abelian or Size 2 Cases

Lemma 4

If $\exists i_1 \neq i_2$ *s.t.* $\rho_{i_1} = \rho_{i_2} \neq 1$ *and* $\mu_{i_2} = \mu_{i_1} + 1$ *(e.g., our target function), then* $\nexists$ *solution* $(\tau_1, \dots, \tau_\ell)$ *s.t.* $\tau_1, \dots, \tau_{\ell-1}$ *commute or* $\tau_2, \dots, \tau_\ell$ *commute.*

Note: Here conj. cond. is not concerned.

(Proof) When $\tau_1, \dots, \tau_{\ell-1}$ commute,

$$\left({\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}}\right)^{\mu_{i_1}} {\tau_\ell}^{e_\ell \mu_{i_1}} = \rho_{i_1}$$
$$= \rho_{i_2} = \left({\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}}\right)^{\mu_{i_2}} {\tau_\ell}^{e_\ell \mu_{i_2}} \quad .$$

Lemma 4

If $\exists i_1 \neq i_2$ s.t. $\rho_{i_1} = \rho_{i_2} \neq 1$ and $\mu_{i_2} = \mu_{i_1} + 1$ (e.g., our target function), then $\nexists$ solution $(\tau_1, \dots, \tau_\ell)$ s.t. $\tau_1, \dots, \tau_{\ell-1}$ commute or $\tau_2, \dots, \tau_\ell$ commute.

Note: Here conj. cond. is not concerned.

(Proof) When $\tau_1, \dots, \tau_{\ell-1}$ commute,

$$\left({\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}}\right)^{\mu_{i_1}} {\tau_\ell}^{e_\ell \mu_{i_1}} = \rho_{i_1}$$
$$= \rho_{i_2} = \left({\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}}\right)^{\mu_{i_2}} {\tau_\ell}^{e_\ell \mu_{i_2}} \quad .$$

$\therefore {\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}} = {\tau_\ell}^{-e_\ell}$ ($\because \mu_{i_2} = \mu_{i_1} + 1$).

Lemma 4

If $\exists i_1 \neq i_2$ s.t. $\rho_{i_1} = \rho_{i_2} \neq 1$ and $\mu_{i_2} = \mu_{i_1} + 1$ (e.g., our target function), then $\nexists$ solution $(\tau_1, \dots, \tau_\ell)$ s.t. $\tau_1, \dots, \tau_{\ell-1}$ commute or $\tau_2, \dots, \tau_\ell$ commute.

Note: Here conj. cond. is not concerned.

(Proof) When $\tau_1, \dots, \tau_{\ell-1}$ commute,

$$\left({\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}}\right)^{\mu_{i_1}} {\tau_\ell}^{e_\ell \mu_{i_1}} = \rho_{i_1} = \rho_{i_2} = \left({\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}}\right)^{\mu_{i_2}} {\tau_\ell}^{e_\ell \mu_{i_2}} .$$

$\therefore {\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}} = {\tau_\ell}^{-e_\ell}$ ($\because \mu_{i_2} = \mu_{i_1} + 1$).

$\therefore \left({\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}}\right)^{\mu_{i_1}} = {\tau_\ell}^{-\mu_{i_1} e_\ell}$.

Lemma 4

If $\exists i_1 \neq i_2$ s.t. $\rho_{i_1} = \rho_{i_2} \neq 1$ and $\mu_{i_2} = \mu_{i_1} + 1$ (e.g., our target function), then $\nexists$ solution $(\tau_1, \dots, \tau_\ell)$ s.t. $\tau_1, \dots, \tau_{\ell-1}$ commute or $\tau_2, \dots, \tau_\ell$ commute.

Note: Here conj. cond. is not concerned.

(Proof) When $\tau_1, \dots, \tau_{\ell-1}$ commute,

$$({\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}})^{\mu_{i_1}} {\tau_\ell}^{e_\ell \mu_{i_1}} = \rho_{i_1} = \rho_{i_2} = ({\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}})^{\mu_{i_2}} {\tau_\ell}^{e_\ell \mu_{i_2}} .$$

$\therefore {\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}} = {\tau_\ell}^{-e_\ell}$ ($\because \mu_{i_2} = \mu_{i_1} + 1$).

$\therefore ({\tau_1}^{e_1} \cdots {\tau_{\ell-1}}^{e_{\ell-1}})^{\mu_{i_1}} = {\tau_\ell}^{-\mu_{i_1} e_\ell}$.

$\therefore \rho_{i_1} = 1$. Contradiction. □

Abelian or Size 2 Cases

Remark: Lemma 4 (and some of the following results) can be slightly generalized.

Remark: Lemma 4 (and some of the following results) can be slightly generalized.

Corollary 5

If $\exists i_1 \neq i_2$ *s.t.* $\rho_{i_1} = \rho_{i_2} \neq 1$ *and* $\mu_{i_2} = \mu_{i_1} + 1$ *(e.g., our target function), then* $\nexists$ F *of size* ≤ 2*.*

Corollary 6

If $\exists i_1 \neq i_2$ *s.t.* $\rho_{i_1} = \rho_{i_2} \neq 1$ *and* $\mu_{i_2} = \mu_{i_1} + 1$ *(e.g., our target function), then* $\nexists$ F *over Abelian groups.*

(Proof) The commutativity condition in Lemma 4 is trivially satisfied in these cases. □

Lemma 7

If

- $\exists i_1 \neq i_2$ *s.t.* $\rho_{i_1} = \rho_{i_2} = \sigma$ *and* $\mu_{i_2} = \mu_{i_1} + 1$ *(e.g., our target function),*
- $\exists N \lhd H \leq G$ *s.t.* $\sigma \in H \setminus N$ *and*

(C1) *any element of* G *conjugate to* σ *belongs to* H*,*

(C2) *if* $\nu_1, \nu_2 \in H$ *and* $\mathrm{ord}(\nu_1) = \mathrm{ord}(\nu_2) = \mathrm{ord}(\sigma)$, *then* $\overline{\nu_1 \nu_2} = \overline{\nu_2 \nu_1}$ *where* $\bar{\cdot} \colon H \to H/N$ *is the natural projection,*

then $\nexists F$.

(Proof) $\overline{\sigma} = \overline{\rho_{i_1}} \neq 1$.

(Proof) $\overline{\sigma} = \overline{\rho_{i_1}} \neq 1$.
If $\exists$ solution $(\tau_1, \dots, \tau_\ell)$, this is also a solution over H s.t. $\mathrm{ord}(\tau_j) = \mathrm{ord}(\sigma)$ by the conjugacy condition and (C1).

(Proof) $\overline{\sigma} = \overline{\rho_{i_1}} \neq 1$.
If $\exists$ solution $(\tau_1, \dots, \tau_\ell)$, this is also a solution over H s.t. $\mathrm{ord}(\tau_j) = \mathrm{ord}(\sigma)$ by the conjugacy condition and (C1).
$\therefore$ $(\overline{\tau_1}, \dots, \overline{\tau_\ell})$ is a solution over H/N (w/ $\overline{\rho_i}$ instead of ρ_i), while all $\overline{\tau_j}$ commute by (C2).

(Proof) $\overline{\sigma} = \overline{\rho_{i_1}} \neq 1$.
If $\exists$ solution $(\tau_1, \ldots, \tau_\ell)$, this is also a solution over H s.t. $\mathrm{ord}(\tau_j) = \mathrm{ord}(\sigma)$ by the conjugacy condition and (C1).
$\therefore$ $(\overline{\tau_1}, \ldots, \overline{\tau_\ell})$ is a solution over H/N (w/ $\overline{\rho_i}$ instead of ρ_i), while all $\overline{\tau_j}$ commute by (C2).
Such a solution is denied by Lemma 4.
Contradiction. $\square$

Theorem 8

If $\exists i_1 \neq i_2$ *s.t.* $\rho_{i_1} = \rho_{i_2} = \sigma \neq 1$ *and* $\mu_{i_2} = \mu_{i_1} + 1$ *(e.g., our target function), and* G *is finite and solvable, then* $\nexists F$.

Theorem 8

If $\exists i_1 \neq i_2$ *s.t.* $\rho_{i_1} = \rho_{i_2} = \sigma \neq 1$ *and* $\mu_{i_2} = \mu_{i_1} + 1$ *(e.g., our target function), and* G *is finite and solvable, then* $\nexists F$.

(Proof) Let $G = G^{(0)} > G^{(1)} > \cdots > G^{(n)} = 1$ $(G^{(k)} = [G^{(k-1)}, G^{(k-1)}])$ be the derived series of G. Note that $G^{(k)} \lhd G$.

Theorem 8

If $\exists i_1 \neq i_2$ s.t. $\rho_{i_1} = \rho_{i_2} = \sigma \neq 1$ and $\mu_{i_2} = \mu_{i_1} + 1$ (e.g., our target function), and G is finite and solvable, then $\nexists F$.

(Proof) Let $G = G^{(0)} > G^{(1)} > \cdots > G^{(n)} = 1$ $(G^{(k)} = [G^{(k-1)}, G^{(k-1)}])$ be the derived series of G.
Note that $G^{(k)} \lhd G$.
As $\sigma \neq 1$, $\exists k < n$ s.t. $\sigma \in G^{(k)} \setminus G^{(k+1)}$.

Theorem 8

If $\exists i_1 \neq i_2$ s.t. $\rho_{i_1} = \rho_{i_2} = \sigma \neq 1$ and $\mu_{i_2} = \mu_{i_1} + 1$ (e.g., our target function), and G is finite and solvable, then $\nexists F$.

(Proof) Let $G = G^{(0)} > G^{(1)} > \cdots > G^{(n)} = 1$ $(G^{(k)} = [G^{(k-1)}, G^{(k-1)}])$ be the derived series of G.
Note that $G^{(k)} \lhd G$.
As $\sigma \neq 1$, $\exists k < n$ s.t. $\sigma \in G^{(k)} \setminus G^{(k+1)}$.
Then for Lemma 7 with $H := G^{(k)}$ and $N := G^{(k+1)}$, (C1) holds as $G^{(k)} \lhd G$, and (C2) holds as $G^{(k)}/G^{(k+1)}$ is Abelian, so Lemma 7 works. □

No Advantage to Consider S_n

Lemma 9

If $\exists N \lhd G$ *s.t.* $\sigma \in N$ *and* $G = NZ_G(\sigma)$ *(*$Z_G(\sigma)$*: centralizer of* σ*), and if* $\exists$ *solution over* G *w/ conj. cond., then* $\exists$ *solution over* N *w/ conj. cond.*

No Advantage to Consider S_n

Lemma 9

If $\exists N \triangleleft G$ *s.t.* $\sigma \in N$ *and* $G = NZ_G(\sigma)$ *(*$Z_G(\sigma)$*: centralizer of* σ*), and if* $\exists$ *solution over* G *w/ conj. cond., then* $\exists$ *solution over* N *w/ conj. cond.*

(Proof) For solution $(\tau_1, \dots, \tau_\ell)$ over G, write $\tau_i = u_i \sigma {u_i}^{-1}$.

No Advantage to Consider S_n

Lemma 9

If $\exists N \lhd G$ s.t. $\sigma \in N$ and $G = NZ_G(\sigma)$ ($Z_G(\sigma)$: centralizer of σ), and if $\exists$ solution over G w/ conj. cond., then $\exists$ solution over N w/ conj. cond.

(Proof) For solution $(\tau_1, \dots, \tau_\ell)$ over G, write $\tau_i = u_i \sigma {u_i}^{-1}$. Write $u_i = h_i z_i$, $h_i \in N$, $z_i \in Z_G(\sigma)$.

No Advantage to Consider S_n

Lemma 9

If $\exists N \triangleleft G$ s.t. $\sigma \in N$ and $G = NZ_G(\sigma)$ ($Z_G(\sigma)$: centralizer of σ), and if $\exists$ solution over G w/ conj. cond., then $\exists$ solution over N w/ conj. cond.

(Proof) For solution $(\tau_1, \ldots, \tau_\ell)$ over G, write $\tau_i = u_i \sigma {u_i}^{-1}$. Write $u_i = h_i z_i$, $h_i \in N$, $z_i \in Z_G(\sigma)$. Then $\tau_i = h_i z_i \sigma {z_i}^{-1} {h_i}^{-1} = h_i \sigma {h_i}^{-1} \in N$.

Lemma 9

If $\exists N \lhd G$ s.t. $\sigma \in N$ and $G = NZ_G(\sigma)$ ($Z_G(\sigma)$: centralizer of σ), and if $\exists$ solution over G w/ conj. cond., then $\exists$ solution over N w/ conj. cond.

(Proof) For solution $(\tau_1, \dots, \tau_\ell)$ over G, write $\tau_i = u_i \sigma {u_i}^{-1}$. Write $u_i = h_i z_i$, $h_i \in N$, $z_i \in Z_G(\sigma)$. Then $\tau_i = h_i z_i \sigma {z_i}^{-1} {h_i}^{-1} = h_i \sigma {h_i}^{-1} \in N$.
$\therefore$ $(\tau_1, \dots, \tau_\ell)$ is a solution over N w/ conj. cond. □

Corollary 10

Let $n \geq 5$ *and* $\sigma = (1\ 2\ 3) \in A_n$. *If* $\exists$ *our target function over* S_n, *then* $\exists$ *our target function over* A_n.

No Advantage to Consider S_n

Corollary 10

Let $n \geq 5$ and $\sigma = (1\ 2\ 3) \in A_n$. If $\exists$ our target function over S_n, then $\exists$ our target function over A_n.

(Proof) As $A_n \lhd S_n$, $[S_n : A_n] = 2$, and $(4\ 5) \in Z_{S_n}(\sigma) \setminus A_n$, we have $S_n = A_n Z_{S_n}(\sigma)$. Apply Lemma 9. $\square$

No Advantage to Consider S_n

Corollary 10

Let $n \geq 5$ and $\sigma = (1\ 2\ 3) \in A_n$. If $\exists$ our target function over S_n, then $\exists$ our target function over A_n.

(Proof) As $A_n \triangleleft S_n$, $[S_n : A_n] = 2$, and $(4\ 5) \in Z_{S_n}(\sigma) \setminus A_n$, we have $S_n = A_n Z_{S_n}(\sigma)$. Apply Lemma 9. □

By this corollary and Theorem 8, we consider A_5 instead of S_5 as the underlying group.

Theorem 11

Let $\sigma = (1\ 2\ 3)$. Then $\nexists$ our target function F of size 3 over A_5.

Theorem 11

Let $\sigma = (1\ 2\ 3)$. Then $\nexists$ our target function F of size 3 over A_5.

(Proof) Assume $\exists F$ of exponent (e_1, e_2, e_3), $e_i \in \{1, 2\}$.
Let (τ_1, τ_2, τ_3) be the corresponding solution for the equations.

Theorem 11

Let $\sigma = (1\ 2\ 3)$. Then $\nexists$ our target function F of size 3 over A_5.

(Proof) Assume $\exists F$ of exponent (e_1, e_2, e_3), $e_i \in \{1, 2\}$.
Let (τ_1, τ_2, τ_3) be the corresponding solution for the equations.
As $F(\sigma) = F(\sigma^2) = \sigma$, we have
${\tau_1}^{e_1}{\tau_2}^{e_2}{\tau_3}^{e_3} = \sigma = {\tau_1}^{2e_1}{\tau_2}^{2e_2}{\tau_3}^{2e_3}$.

Theorem 11

Let $\sigma = (1\ 2\ 3)$. Then $\nexists$ our target function F of size 3 over A_5.

(Proof) Assume $\exists F$ of exponent (e_1, e_2, e_3), $e_i \in \{1, 2\}$.
Let (τ_1, τ_2, τ_3) be the corresponding solution for the equations.
As $F(\sigma) = F(\sigma^2) = \sigma$, we have
${\tau_1}^{e_1}{\tau_2}^{e_2}{\tau_3}^{e_3} = \sigma = {\tau_1}^{2e_1}{\tau_2}^{2e_2}{\tau_3}^{2e_3}$.
$\therefore\ {\tau_2}^{-e_2}{\tau_1}^{e_1}{\tau_2}^{e_2} = {\tau_3}^{-e_3}{\tau_2}^{-e_2}$.

Case of Size 3 over A_5

$$\nu_2 {\tau_1}^{e_1} {\nu_2}^{-1} = \nu_1 \nu_2 ,\ \nu_1 := {\tau_3}^{-e_3} ,\ \nu_2 := {\tau_2}^{-e_2} .$$

Case of Size 3 over A_5

${\nu_2}{\tau_1}^{e_1}{\nu_2}^{-1} = \nu_1\nu_2$, $\nu_1 := {\tau_3}^{-e_3}$, $\nu_2 := {\tau_2}^{-e_2}$.
$\therefore$ $\nu_1\nu_2 \sim_{\mathrm{conj}} {\tau_1}^{e_1} \sim_{\mathrm{conj}} \sigma^{e_1}$, $\nu_1 \sim_{\mathrm{conj}} \sigma^{-e_3}$,
$\nu_2 \sim_{\mathrm{conj}} \sigma^{-e_2}$ are cyclic permutations of length 3.

$\nu_2 {\tau_1}^{e_1} {\nu_2}^{-1} = \nu_1 \nu_2$, $\nu_1 := {\tau_3}^{-e_3}$, $\nu_2 := {\tau_2}^{-e_2}$.
$\therefore \nu_1 \nu_2 \sim_{\mathrm{conj}} {\tau_1}^{e_1} \sim_{\mathrm{conj}} \sigma^{e_1}$, $\nu_1 \sim_{\mathrm{conj}} \sigma^{-e_3}$,
$\nu_2 \sim_{\mathrm{conj}} \sigma^{-e_2}$ are cyclic permutations of length 3.
Write $\nu_1 = (a\ b_1\ b_2)$, $\nu_2 = (a\ c_1\ c_2)$.

${\nu_2}{\tau_1}^{e_1}{\nu_2}^{-1} = \nu_1\nu_2$, $\nu_1 := {\tau_3}^{-e_3}$, $\nu_2 := {\tau_2}^{-e_2}$.

$\therefore \nu_1\nu_2 \sim_{\mathrm{conj}} {\tau_1}^{e_1} \sim_{\mathrm{conj}} \sigma^{e_1}$, $\nu_1 \sim_{\mathrm{conj}} \sigma^{-e_3}$,
$\nu_2 \sim_{\mathrm{conj}} \sigma^{-e_2}$ are cyclic permutations of length 3.

Write $\nu_1 = (a\ b_1\ b_2)$, $\nu_2 = (a\ c_1\ c_2)$.

(I) When $\{b_1, b_2\} \cap \{c_1, c_2\} \neq \emptyset$:

${\nu_2}{\tau_1}^{e_1}{\nu_2}^{-1} = \nu_1\nu_2$, $\nu_1 := {\tau_3}^{-e_3}$, $\nu_2 := {\tau_2}^{-e_2}$.
$\therefore$ $\nu_1\nu_2 \sim_{\mathrm{conj}} {\tau_1}^{e_1} \sim_{\mathrm{conj}} \sigma^{e_1}$, $\nu_1 \sim_{\mathrm{conj}} \sigma^{-e_3}$,
$\nu_2 \sim_{\mathrm{conj}} \sigma^{-e_2}$ are cyclic permutations of length 3.
Write $\nu_1 = (a\ b_1\ b_2)$, $\nu_2 = (a\ c_1\ c_2)$.

(I) When $\{b_1, b_2\} \cap \{c_1, c_2\} \neq \emptyset$:
$\exists H \leq S_5$ s.t. $\nu_1, \nu_2 \in H \simeq S_4$.

$\nu_2 {\tau_1}^{e_1} {\nu_2}^{-1} = \nu_1 \nu_2$, $\nu_1 := {\tau_3}^{-e_3}$, $\nu_2 := {\tau_2}^{-e_2}$.
$\therefore$ $\nu_1 \nu_2 \sim_{\mathrm{conj}} {\tau_1}^{e_1} \sim_{\mathrm{conj}} \sigma^{e_1}$, $\nu_1 \sim_{\mathrm{conj}} \sigma^{-e_3}$,
$\nu_2 \sim_{\mathrm{conj}} \sigma^{-e_2}$ are cyclic permutations of length 3.
Write $\nu_1 = (a\ b_1\ b_2)$, $\nu_2 = (a\ c_1\ c_2)$.

(I) When $\{b_1, b_2\} \cap \{c_1, c_2\} \neq \emptyset$:
$\exists H \leq S_5$ s.t. $\nu_1, \nu_2 \in H \simeq S_4$.
$\therefore$ ${\tau_1}^{e_1} = {\nu_2}^{-1} \nu_1 {\nu_2}^2 \in H$.

$\nu_2{\tau_1}^{e_1}{\nu_2}^{-1} = \nu_1\nu_2$, $\nu_1 := {\tau_3}^{-e_3}$, $\nu_2 := {\tau_2}^{-e_2}$.
$\therefore \nu_1\nu_2 \sim_{\mathrm{conj}} {\tau_1}^{e_1} \sim_{\mathrm{conj}} \sigma^{e_1}$, $\nu_1 \sim_{\mathrm{conj}} \sigma^{-e_3}$,
$\nu_2 \sim_{\mathrm{conj}} \sigma^{-e_2}$ are cyclic permutations of length 3.
Write $\nu_1 = (a\ b_1\ b_2)$, $\nu_2 = (a\ c_1\ c_2)$.

(I) When $\{b_1, b_2\} \cap \{c_1, c_2\} \neq \emptyset$:
$\exists H \leq S_5$ s.t. $\nu_1, \nu_2 \in H \simeq S_4$.
$\therefore {\tau_1}^{e_1} = {\nu_2}^{-1}\nu_1{\nu_2}^2 \in H$.
As $\tau_1 \in \langle {\tau_1}^{e_1} \rangle$, $\tau_2 \in \langle \nu_2 \rangle$, $\tau_3 \in \langle \nu_1 \rangle$, we have
$\tau_1, \tau_2, \tau_3 \in H$ and $\sigma = \tau_1\tau_2\tau_3 \in H$.

Case of Size 3 over A_5

$\nu_2 {\tau_1}^{e_1} {\nu_2}^{-1} = \nu_1 \nu_2$, $\nu_1 := {\tau_3}^{-e_3}$, $\nu_2 := {\tau_2}^{-e_2}$.
$\therefore$ $\nu_1 \nu_2 \sim_{\mathrm{conj}} {\tau_1}^{e_1} \sim_{\mathrm{conj}} \sigma^{e_1}$, $\nu_1 \sim_{\mathrm{conj}} \sigma^{-e_3}$,
$\nu_2 \sim_{\mathrm{conj}} \sigma^{-e_2}$ are cyclic permutations of length 3.
Write $\nu_1 = (a\ b_1\ b_2)$, $\nu_2 = (a\ c_1\ c_2)$.

(I) When $\{b_1, b_2\} \cap \{c_1, c_2\} \neq \emptyset$:
$\exists H \leq S_5$ s.t. $\nu_1, \nu_2 \in H \simeq S_4$.
$\therefore$ ${\tau_1}^{e_1} = {\nu_2}^{-1} \nu_1 {\nu_2}^2 \in H$.
As $\tau_1 \in \langle {\tau_1}^{e_1} \rangle$, $\tau_2 \in \langle \nu_2 \rangle$, $\tau_3 \in \langle \nu_1 \rangle$, we have
$\tau_1, \tau_2, \tau_3 \in H$ and $\sigma = \tau_1 \tau_2 \tau_3 \in H$.
They are in $H \simeq S_4$ and have order 3, so they are conjugate to σ in H.

$\nu_2 {\tau_1}^{e_1} {\nu_2}^{-1} = \nu_1 \nu_2$, $\nu_1 := {\tau_3}^{-e_3}$, $\nu_2 := {\tau_2}^{-e_2}$.
$\therefore$ $\nu_1 \nu_2 \sim_{\text{conj}} {\tau_1}^{e_1} \sim_{\text{conj}} \sigma^{e_1}$, $\nu_1 \sim_{\text{conj}} \sigma^{-e_3}$,
$\nu_2 \sim_{\text{conj}} \sigma^{-e_2}$ are cyclic permutations of length 3.
Write $\nu_1 = (a\ b_1\ b_2)$, $\nu_2 = (a\ c_1\ c_2)$.

(I) When $\{b_1, b_2\} \cap \{c_1, c_2\} \neq \emptyset$:
$\exists H \leq S_5$ s.t. $\nu_1, \nu_2 \in H \simeq S_4$.
$\therefore$ ${\tau_1}^{e_1} = {\nu_2}^{-1} \nu_1 {\nu_2}^2 \in H$.
As $\tau_1 \in \langle {\tau_1}^{e_1} \rangle$, $\tau_2 \in \langle \nu_2 \rangle$, $\tau_3 \in \langle \nu_1 \rangle$, we have
$\tau_1, \tau_2, \tau_3 \in H$ and $\sigma = \tau_1 \tau_2 \tau_3 \in H$.
They are in $H \simeq S_4$ and have order 3, so they are conjugate to σ in H.
$\therefore$ $\exists$ solution over $H \simeq S_4$, contradicting Theorem 8.

$\nu_2 {\tau_1}^{e_1} {\nu_2}^{-1} = \nu_1 \nu_2$, $\nu_1 := {\tau_3}^{-e_3}$, $\nu_2 := {\tau_2}^{-e_2}$.
Write $\nu_1 = (a\ b_1\ b_2)$, $\nu_2 = (a\ c_1\ c_2)$.

(II) When $\{b_1, b_2\} = \{c_1, c_2\} \neq \emptyset$:

${\nu_2 \tau_1}^{e_1} {\nu_2}^{-1} = \nu_1 \nu_2$, $\nu_1 := {\tau_3}^{-e_3}$, $\nu_2 := {\tau_2}^{-e_2}$.
Write $\nu_1 = (a\ b_1\ b_2)$, $\nu_2 = (a\ c_1\ c_2)$.

(II) When $\{b_1, b_2\} = \{c_1, c_2\} \neq \emptyset$:
Now $\nu_1 \nu_2(c_2) = b_1$, $\nu_1 \nu_2(b_1) = b_2$, $\nu_1 \nu_2(b_2) = a \neq c_2$, so $\nu_1 \nu_2$ cannot be a cyclic permutation of length 3. Contradiction. □

$\nu_2 {\tau_1}^{e_1} {\nu_2}^{-1} = \nu_1 \nu_2$, $\nu_1 := {\tau_3}^{-e_3}$, $\nu_2 := {\tau_2}^{-e_2}$.
Write $\nu_1 = (a\ b_1\ b_2)$, $\nu_2 = (a\ c_1\ c_2)$.

(II) When $\{b_1, b_2\} = \{c_1, c_2\} \neq \emptyset$:
Now $\nu_1 \nu_2(c_2) = b_1$, $\nu_1 \nu_2(b_1) = b_2$, $\nu_1 \nu_2(b_2) = a \neq c_2$, so $\nu_1 \nu_2$ cannot be a cyclic permutation of length 3. Contradiction. □

By this theorem and Corollary 5, the smallest possible size of our target function over A_5 is 4.

Lemma 12

Any two cyclic permutations ρ, ν of length 3 are conjugate in A_5.

(Proof) Take a transposition $\tau \in S_5$ s.t. $\rho\tau = \tau\rho$. For $\nu = u\rho u^{-1}$ with $u \in S_5$, $\nu = (u\tau)\rho(u\tau)^{-1}$, and either u or $u\tau$ is in A_5 as $[S_5 : A_5] = 2$. $\square$

Corollary 13

Let $\sigma = (1\ 2\ 3)$. *If* $\exists$ *our target function of size* ℓ *and exponent* $(e_1, \ldots, e_\ell)$ *over* A_5 *s.t.* $e_i \in \{1, 2\}$, *then* $\exists$ *our target function of size* ℓ *and exponent* $(1, 1, \ldots, 1)$ *over* A_5.

Corollary 13

Let $\sigma = (1\ 2\ 3)$. If $\exists$ our target function of size ℓ and exponent $(e_1, \dots, e_\ell)$ over A_5 s.t. $e_i \in \{1, 2\}$, then $\exists$ our target function of size ℓ and exponent $(1, 1, \dots, 1)$ over A_5.

(Proof) As ${\tau_i}^{e_i} \sim_{\mathrm{conj}} \tau_i$ by Lemma 12, $({\tau_1}^{e_1}, \dots, {\tau_\ell}^{e_\ell})$ is a solution of the equations corresponding to exponent $(1, 1, \dots, 1)$. □

A Smallest Solution

We search (by SageMath) for a solution of the equations over A_5 corresponding to our target function of size 4 (cf. Corollary 5 and Theorem 11) and exponent $(1, 1, 1, 1)$ (cf. Corollary 13), where $\sigma = (1\ 2\ 3)$:

$$\tau_1 \tau_2 \tau_3 \tau_4 = {\tau_1}^2 {\tau_2}^2 {\tau_3}^2 {\tau_4}^2 = (1\ 2\ 3) \enspace .$$

We found

$$\tau_1 := (2\ 4\ 5) \, , \, \tau_2 := (1\ 5\ 4) \enspace ,$$
$$\tau_3 := (3\ 4\ 5) \, , \, \tau_4 := (2\ 5\ 4) \enspace .$$

Moreover,

$$\tau_1 = (1\ 2\ 4\ 3\ 5)\sigma(1\ 2\ 4\ 3\ 5)^{-1} \ ,$$
$$\tau_2 = (1\ 5\ 2\ 4\ 3)\sigma(1\ 5\ 2\ 4\ 3)^{-1} \ ,$$
$$\tau_3 = (1\ 3\ 5\ 2\ 4)\sigma(1\ 3\ 5\ 2\ 4)^{-1} \ ,$$
$$\tau_4 = (1\ 2\ 5\ 3\ 4)\sigma(1\ 2\ 5\ 3\ 4)^{-1} \ .$$

Then by following the proof of Lemma 2, we obtain

$$F(x) := (1\ 2\ 4\ 3\ 5)x(1\ 3\ 5)x \cdot (1\ 4\ 3)x(1\ 5)(2\ 3)x(1\ 4\ 3\ 5\ 2) \ ,$$

simpler than the previously known F (of size 6 and exponent $(1, 1, 2, 1, 1, 2)$).

Future Work

- (Im)possibility of our target function over other groups
- Construction of compact HE over a finite non-solvable group G (hopefully $G = A_5$)

References

- [Barrington et al., 1990] D. A. M. Barrington, H. Straubing, D. Thérien: Non-Uniform Automata over Groups, Information and Computation, 1990
- [Choi et al., 2007] S.-J. Choi, S. R. Blackburn, P. R. Wild: Cryptanalysis of a Homomorphic Public-Key Cryptosystem over a Finite Group, Journal of Mathematical Cryptology, vol.1, pp.351–358, 2007
- [van Dijk et al., 2010] M. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan: Fully Homomorphic Encryption over the Integers, EUROCRYPT 2010

References

- [Gentry, 2009] C. Gentry: Fully homomorphic encryption using ideal lattices, STOC 2009
- [Grigoriev & Ponomarenko, 2004] D. Grigoriev, I. Ponomarenko: Homomorphic Public-Key Cryptosystems over Groups and Rings, in: Complexity of Computations and Proofs, Quaderni di Matematica 13, Dept. of Mathematics, Seconda Università di Napoli, Caserta, 2004, pp.305–325

References

- [N., 2021] K. Nuida: Towards Constructing Fully Homomorphic Encryption without Ciphertext Noise from Group Theory, in: International Symposium on Mathematics, Quantum Theory, and Cryptography, Mathematics for Industry book series vol.33, Springer, pp.57–78, 2021
- [N., arXiv 2022] K. Nuida: On Compression Functions over Groups with Applications to Homomorphic Encryption, arXiv:2208.02468
- [Ostrovsky & Skeith III, 2008] R. Ostrovsky, W. E. Skeith III: Communication Complexity in Algebraic Two-Party Protocols, CRYPTO 2008