On Compression Functions over Small Groups with Applications to Cryptography

Koji Nuida

1 Institute of Mathematics for Industry (IMI), Kyushu University
2 National Institute of Advanced Industrial Science and Technology (AIST)

Abstract

In the area of cryptography, fully homomorphic encryption (FHE) enables any entity to perform arbitrary computation on encrypted data without decrypting the ciphertexts. An ongoing group-theoretic approach to construct FHE schemes uses a certain “compression” function $F(x)$ implemented by group operators on a given finite group $G$ (i.e., it is given by a sequence of elements of $G$ and variable $x$), which satisfies that $F(1) = 1$ and $F(\sigma) = F(\sigma^2) = \sigma$ where $\sigma \in G$ is some element of order three. The previous work gave an example of such $F$ over $G = S_5$ by just a heuristic approach. In this paper, we systematically study the possibilities of such $F$. We construct a shortest possible $F$ over smaller group $G = A_5$, and prove that no such $F$ exists over other groups $G$ of order up to $60 = |A_5|$.

2010 Mathematics Subject Classification: 20D60, 94A60
Keywords: Function over groups; alternating groups; fully homomorphic encryption

1 Introduction

1.1 Background and Problem Statement

Let $G$ be a group. A sequence consisting of elements of $G$ and variables can be regarded as a function over $G$ implemented by group operators on $G$ only. For example, by putting $F(x, y) = g_1 xyg_2x$ with $g_1, g_2 \in G$, we have $F(h_1, h_2) = g_1 h_1 h_2 g_2 h_1 \in G$ for $h_1, h_2 \in G$. The aim of this paper is to investigate existence and inexistence of such a kind of functions over a given group $G$ satisfying a certain condition.

Such a kind of functions over groups have appeared in the literature of cryptography. Our study in this paper is also motivated by cryptography, as explained below. In the area of cryptography, an encryption scheme is a method to protect some data, called plaintexts, from an eavesdropping adversary in a way that a plaintext is converted (encrypted) into a ciphertext and only an authorized entity having a decryption key can decrypt the ciphertext to recover the plaintext (hence an adversary without the decryption key cannot see the plaintext even if the adversary obtains a ciphertext). A special kind of encryption schemes, called homomorphic encryption schemes, enable an entity to perform “computation on encrypted data”, that is, given ciphertexts $c_1, \ldots, c_\ell$ with corresponding (unknown) plaintexts $m_1, \ldots, m_\ell$, an entity can generate a ciphertext for plaintext $\varphi(m_1, \ldots, m_\ell)$ without decrypting the ciphertexts, where $\varphi$ denotes a possible operator on plaintexts. In particular, fully homomorphic encryption (FHE) schemes can perform such operators on ciphertexts corresponding to an arbitrary operator $\varphi$ on plaintexts. After the first construction of an FHE scheme by Gentry in 2009 [2], FHE schemes have been actively studied in the area of cryptography, from not only theoretical viewpoints but also practical viewpoints related to e.g., privacy protection in personal data analysis.

Besides the only successful approach to construction of FHE schemes at the present using “ciphertexts with noise”, there is another ongoing approach from group theory. Such an approach was firstly proposed by...
Ostrovsky and Skeith III [4] and later re-formulated by the author in a recent paper [3]. In this approach, each bit in \{0,1\} is encoded as an element of a given finite group \(G\), and operators on bits are realized by functions implemented on \(G\) (in the sense of the first paragraph) through the encoding. More precisely, we take two distinct elements \(\sigma_0\) and \(\sigma_1\) of \(G\). If we want to realize, for example, \(\text{AND}\) function for two bits as a function \(F_{\text{AND}}(x_1, x_2)\) implemented on \(G\), we find such a function satisfying that \(F_{\text{AND}}(\sigma_0, \sigma_0) = F_{\text{AND}}(\sigma_0, \sigma_1) = F_{\text{AND}}(\sigma_1, \sigma_0) = \sigma_0\) and \(F_{\text{AND}}(\sigma_1, \sigma_1) = \sigma_1\). Now if we have a homomorphic encryption scheme for the set of plaintexts \(G\) that can perform group operators on \(G\) in encrypted form, then we will be able to perform computation of the function \(F_{\text{AND}}\) over ciphertexts, which results in computation of \(\text{AND}\) operator in encrypted form through the encoding of bits \(b \mapsto \sigma_b\). Based on this strategy, the problem of constructing FHE schemes is reduced to the problem of constructing such functions on \(G\) corresponding to a functionally complete set of bit operators (e.g., \{\text{NAND}, \text{NOT}, \text{AND}, \text{OR}, \text{XOR}\}) and the problem of constructing a homomorphic encryption scheme that can perform group operators on \(G\). This paper focuses on the former of these two problems.

For such functions on groups, the paper [4] proved the existence of a function realizing \(\text{NAND}\) operator over any finite non-Abelian simple group by utilizing the properties of commutators. On the other hand, in [3], a different approach called “approximate-then-adjust” method was proposed. In this approach, a target function is constructed by composition of a two-variable inner function \(F^{\text{in}}(x_1, x_2)\) followed by a one-variable outer function \(F^{\text{out}}(g)\). For example, for the case of \(\text{OR}\) operator, we take an element \(\sigma \in G\) of order three, set \(\sigma_0 := 1\) and \(\sigma := \sigma\), and simply set \(F^{\text{in}}_{\text{OR}}(x_1, x_2) := x_1 x_2\). Now the three values \(F^{\text{in}}_{\text{OR}}(\sigma_0, \sigma_0) = \sigma_0, F^{\text{in}}_{\text{OR}}(\sigma_0, \sigma_1) = \sigma_1, \text{and } F^{\text{in}}_{\text{OR}}(\sigma_1, \sigma_0) = \sigma_1\) correctly correspond to \(\text{OR}\) operator, while the remaining value \(F^{\text{in}}_{\text{OR}}(\sigma_1, \sigma_1) = \sigma^2\) is not correct. Then an outer function \(F^{\text{out}}\) satisfying that \(F^{\text{out}}(1) = 1\) and \(F^{\text{out}}(\sigma) = F^{\text{out}}(\sigma^2) = \sigma\) can adjust the incorrect value (i.e., \(F^{\text{out}}(F^{\text{in}}_{\text{OR}}(\sigma_1, \sigma_1)) = F^{\text{out}}(\sigma^2) = \sigma_1\)) while keeping the other correct values. The same outer function \(F^{\text{out}}\) can also be used to realize some other bit operators; e.g., \(\text{NAND}\) with \(F^{\text{in}}_{\text{NAND}}(x_1, x_2) = x_1^{-1} x_2^{-1} \sigma^2\) and \(\text{XOR}\) with \(F^{\text{in}}_{\text{XOR}}(x_1, x_2) = x_1^{-1} x_2\). Hence the problem is reduced to construct such a function \(F^{\text{out}}\) satisfying that \(F^{\text{out}}(1) = 1\) and \(F^{\text{out}}(\sigma) = F^{\text{out}}(\sigma^2) = \sigma\). In [3], by setting \(G = S_5\) and \(\sigma = (1 2 3)\), the following example of the function \(F^{\text{out}}\) was given:

\[
F^{\text{out}}(y) = (1 5)(2 3 4) \cdot y \cdot (2 3 4) \cdot y \cdot (3 4) \cdot y^2 \cdot (2 3)(4 5) \cdot y \cdot (2 3 4) \cdot y \cdot (3 4) \cdot y^2 \cdot (1 4 2 5) .
\] (1)

However, this function was found by a heuristic argument, and no systematic approach to find such a function was given in [3]. The aim of this paper is to execute a systematic study for possibilities of such functions, possibly over smaller groups and having shorter expressions than the example above.

1.2 Our Contributions

In this paper, we systematically study the possibilities of functions \(F\) implemented on various groups \(G\) satisfying the aforementioned conditions \(F(1) = 1\) and \(F(\sigma) = F(\sigma^2) = \sigma\) where \(\sigma\) is some element of \(G\) of order three. In comparison to the known function in Eq. (1) where \(G = S_5\), our function given in this paper is constructed over smaller group \(G = A_5\), and is shorter than Eq. (1) (namely, our function involves the variable only four times). See Section 3 for the concrete function. Moreover, we prove that such a function does not exist over any other group \(G\) of order up to 60 = |\(A_5\)| (see Theorem 4 in Section 4), and that any such function over \(A_5\) must involve the variable at least four times (see Theorem 4 in Section 5). By these results, our function in this paper is in some sense the smallest possible construction. We also show that such a function cannot be constructed over a fairly large class of finite groups including Abelian groups and dihedral groups (see Theorem 5 in Section 4).

2 Definitions and Basic Observations

In this paper, we let \(G\) be a finite group with unit element denoted by 1.

**Definition 1.** For an integer \(\ell \geq 1\), we define a group function of size \(\ell\) over \(G\) to be a sequence over \(G \sqcup \{x\}\) of the form \(F(x) = g_0 x^{e_1} g_1 x^{e_2} \cdots g_{\ell-1} x^{e_{\ell-1}} g_\ell\) where \(g_i \in G, e_i \geq 1,\) and \(x^{e_i}\) is an abbreviation of \(xx \cdots x\) (\(e_i\) letters). We define the substitution of \(h \in G\) into \(F\) to be \(F(h) := g_0 h^{e_1} g_1 h^{e_2} \cdots g_{\ell-1} h^{e_{\ell-1}} g_\ell \in G\).
Owing to the motivation explained in Section 1, we focus on group functions $F(x)$ satisfying the following “compression” condition:

(*) For some $\sigma \in G$ of order three, we have $F(1) = 1$ and $F(\sigma) = F(\sigma^2) = \sigma$.

Note that, as the element $\sigma$ in (*) satisfies $\sigma^3 = 1$, we may assume without loss of generality that the exponents of $x$ in $F$ satisfy $e_i \in \{1, 2\}$.

In order to investigate (in)existence of such group functions, the following lemma is useful.

**Lemma 1.** Let $\sigma \in G$ be of order three, and let $\ell \geq 1$. Then the following conditions are equivalent:

1. There exists a group function $F$ of size $\ell$ over $G$ satisfying that $F(1) = 1$ and $F(\sigma) = F(\sigma^2) = \sigma$.

2. There exist elements $\tau_1, \ldots, \tau_\ell \in G$ conjugate to $\sigma$ in $G$ and exponents $e_1, \ldots, e_\ell \geq 1$ satisfying that $\tau_1^{e_1} \cdots \tau_\ell^{e_\ell} = \tau_1^{2e_1} \cdots \tau_\ell^{2e_\ell} = \sigma$.

**Proof.** First, we assume Condition 1 and show that Condition 2 holds. By putting $h_i := g_0g_1 \cdots g_i$ for $0 \leq i \leq \ell$, we have $g_i = h_{i-1}^{-1}h_i$ for $1 \leq i \leq \ell$ and

$$F(\nu) = h_0\nu^{e_1}h_0^{-1}h_1\nu^{e_2}h_1^{-1} \cdots h_{\ell-1}\nu^{e_\ell}h_{\ell-1}^{-1} \cdot h_\ell$$

for $\nu \in G$.

Now the condition $F(1) = 1$ implies $h_\ell = 1$. By putting $\tau_i := h_{i-1}^{-1}\sigma h_{i-1}^{-1}$ for $1 \leq i \leq \ell$ which is conjugate to $\sigma$, the condition $F(\sigma) = \sigma$ implies $\tau_1^{e_1} \cdots \tau_\ell^{e_\ell} = \sigma$, and the condition $F(\sigma^2) = \sigma$ implies $\tau_1^{2e_1} \cdots \tau_\ell^{2e_\ell} = \sigma$. Hence Condition 2 holds.

Conversely, we assume Condition 2 and show that Condition 1 holds. As $\tau_i$ is conjugate to $\sigma$, we can write $\tau_i = h_{i-1}^{-1}\sigma h_{i-1}^{-1}$ for some $h_{i-1} \in G$. Now for each $m \in \{1, 2\}$, the condition $\tau_i^{me_1} \cdots \tau_\ell^{me_\ell} = \sigma$ implies $h_0(\sigma^m)^{e_1}h_0^{-1}h_1(\sigma^m)^{e_2}h_1^{-1} \cdots h_{\ell-1}(\sigma^m)^{e_\ell}h_{\ell-1}^{-1} = \sigma$. Therefore, the group function

$$F(x) := h_0x^{e_1}h_0^{-1}h_1x^{e_2} \cdots h_{\ell-2}^{-1}h_{\ell-1}x^{e_\ell}h_{\ell-1}^{-1}$$

satisfies Condition 1 as desired. Hence the claim holds.

We have the following consequence of Lemma 1.

**Proposition 1.** There does not exist a group function of size at most two over any finite group $G$ satisfying Condition (*).

**Proof.** For the case of size one, assume for the contrary that $\tau_1$ and $e_1$ satisfy the equivalent condition in Lemma 1. Then the equality $\tau_1^{e_1} = \tau_1^{2e_1}$ implies $\tau_1^{e_1} = 1$, which contradicts the equality $\tau_1^{e_1} = \sigma$. Hence the claim holds for this case.

For the case of size two, assume for the contrary that $\tau_1, \tau_2$ and $e_1, e_2$ satisfy the equivalent condition in Lemma 1. Then the equality $\tau_1^{e_1}\tau_2^{e_2} = \tau_1^{2e_1}\tau_2^{2e_2}$ implies $\tau_1^{e_1}\tau_2^{e_2} = 1$, which contradicts the equality $\tau_1^{e_1}\tau_2^{e_2} = \sigma$. Hence the claim holds.

### 3 On Normal Subgroups and Quotients

In this section, we investigate some reductions of the search for group functions with desired property to smaller cases of normal subgroups and quotient groups. We start with the following easy lemma.

**Lemma 2.** Let $G'$ be another finite group and $\varphi: G \to G'$ a group homomorphism. Suppose that $\sigma$ and a group function $F$ of size $\ell$ over $G$ are as in Condition (*) and satisfy $\varphi(\sigma) \neq 1$. Then there exists a group function of size $\ell$ over $G'$ satisfying Condition (*).

**Proof.** First we note that $\varphi(\sigma)$ also has order three by the hypothesis. We write $F(x) = g_0x^{e_1} \cdots g_{\ell-1}x^{e_\ell}g_\ell$, and put $\overline{F}(x) := \varphi(g_0)x^{e_1} \cdots \varphi(g_{\ell-1})x^{e_\ell}\varphi(g_\ell)$. Then we have $\overline{F}(\varphi(\tau)) = \varphi(F(\tau))$ for any $\tau \in G$. Therefore the element $\varphi(\sigma)$ and the function $\overline{F}$ satisfy Condition (*) with respect to $G'$. Hence the claim holds.
Then we have the following consequences of Lemma 2.

**Corollary 1.** Suppose that $G$ is decomposed as $G = H_1 \times H_2$. If there exists a group function of size $\ell$ over $G$ satisfying Condition (\textit{*}), then for some $k \in \{1, 2\}$, there exists a group function of size $\ell$ over $H_k$ satisfying Condition (\textit{*}).

**Proof.** This follows from Lemma 2 and the fact that for any element $\sigma \in G$ of order three, we have $\pi_k(\sigma) \neq 1$ for some $k \in \{1, 2\}$ where $\pi_k: G \to H_k$ is the projection. □

**Corollary 2.** Let $H$ be a normal subgroup of $G$. If $|H| \equiv 0 \pmod{3}$ and there exists a group function of size $\ell$ over $G$ satisfying Condition (\textit{*}), then there exists a group function of size $\ell$ over $G/H$ satisfying Condition (\textit{*}).

**Proof.** For the element $\sigma$ of order three as in Condition (\textit{*}), we have $\sigma \not\in H$ by the hypothesis $|H| \equiv 0 \pmod{3}$. Hence the claim follows from Lemma 2 applied to the natural projection $G \to G/H$. □

We also have the following property.

**Proposition 2.** Let $H$ be a normal subgroup of $G$. Suppose that an element $\sigma \in H$ and a group function $F$ of size $\ell$ over $G$ are as in Condition (\textit{*}) and satisfy that $G = HZ_G(\sigma)$ where $Z_G(\sigma)$ denotes the centralizer of $\sigma$ in $G$. Then there exists a group function of size $\ell$ over $H$ satisfying Condition (\textit{*}).

**Proof.** Let $\tau_1, \ldots, \tau_\ell$ and $e_1, \ldots, e_\ell$ be as in the equivalent condition of Lemma 1. For each $i$, write $\tau_i = u_is_i^{-1}$ with $u_i \in G$. Now by the hypothesis that $H \triangleleft G$ and $G = HZ_G(\sigma)$, we can write $u_i$ as $u_i = h_i z_i$ with $h_i \in H$ and $z_i \in Z_G(\sigma)$. Then we have $\tau_i = h_i z_i \sigma z_i^{-1} h_i^{-1} = h_i \sigma h_i^{-1}$, that is, $\tau_i$ is an element of $H$ conjugate to $\sigma$ in $H$. Therefore, those $\tau_i$ and $e_i$ satisfy the equivalent condition of Lemma 1 with respect to $H$ as well. Hence the claim holds. □

### 4 On the Inexistence over Some Class of Groups

In this section, we show inexistence of group functions with desired property over some class of groups. A fundamental lemma for our argument here is the following.

**Lemma 3.** Suppose that $\sigma \in G$ is of order three and we have $\nu_1 \nu_2 = \nu_2 \nu_1$ for any elements $\nu_1, \nu_2 \in G$ conjugate to $\sigma$. Then there does not exist a group function $F$ over $G$ satisfying that $F(1) = 1$ and $F(\sigma) = F(\sigma^2) = \sigma$.

**Proof.** Assume for the contrary that the equivalent condition in Lemma 1 is satisfied. By the hypothesis, all the elements $\tau_1, \ldots, \tau_\ell$ commute with each other. Therefore we have $\tau_1^{\nu_1} \cdots \tau_\ell^{\nu_1} = (\tau_1^{e_1} \cdots \tau_\ell^{e_1})^2$. Now the equality $\tau_1^{e_1} \cdots \tau_\ell^{e_1} = \tau_1^{e_2} \cdots \tau_\ell^{e_2}$ implies $\tau_1^{e_1} \cdots \tau_\ell^{e_1} = 1$, contradicting the equality $\tau_1^{e_1} \cdots \tau_\ell^{e_1} = \sigma$. Hence the claim holds. □

Now the following result is immediately deduced from Lemma 3.

**Corollary 3.** Suppose that $G$ satisfies the following condition:

(C) All the elements of order three in the group commute with each other.

Then there does not exist a group function over $G$ satisfying Condition (\textit{*}).

Easy examples of the groups $G$ satisfying Condition (C) include Abelian groups. In order to extend the result to more general groups, we use the following lemma.

**Lemma 4.** Suppose that $G$ has a normal series $1 \triangleleft G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G$ satisfying that $|G|/|G_n| \equiv 0 \pmod{3}$. Then any element of order three in $G$ is involved in $G_n$. 

4
Proof. First note that as \(|G|/|G_1| \not\equiv 0 \pmod{3}\) and \(|G_1|/|G_n| \not\equiv 0 \pmod{3}\) by the hypothesis, the claim for a general \(n\) follows recursively from the claim for \(n = 1\). Therefore it suffices to show the claim for \(n = 1\). Take a Sylow 3-subgroup \(P\) of \(G_1\). Then by the hypothesis \(|G|/|G_1| \not\equiv 0 \pmod{3}\), \(P\) is also a Sylow 3-subgroup of \(G\). Now for any \(\nu \in G\) of order three, by Sylow’s Theorem, \(\nu\) is involved in some Sylow 3-subgroup \(P'\) of \(G\), and \(P'\) is conjugate to \(P\). As \(P \leq G_1 \triangleleft G\), this implies \(P' \leq G_1\), therefore we have \(\nu \in G_1\), as desired. Hence the claim holds.

Now we have the following result.

Theorem 1. Suppose that \(G\) has a normal series \(1 \triangleleft G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G = G\) \((n \geq 1)\) satisfying that \(|G|/|G_{n-1}| \not\equiv 0 \pmod{3}\), \(|G_n| \not\equiv 0 \pmod{3}\), and \(|G_{n-1}/G_n|\) satisfies Condition (C). Then there does not exist a group function over \(G\) satisfying Condition (*)

Proof. Assume for the contrary that \(\sigma, \tau_1, \ldots, \tau_\ell\), and \(e_1, \ldots, e_\ell\) satisfy the equivalent condition in Lemma 3. By Lemma 4 applied to the normal series \(1 \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G\), we have \(\sigma, \tau_1, \ldots, \tau_\ell \in G_{n-1}\). Moreover, by the hypothesis \(|G_n| \not\equiv 0 \pmod{3}\), we have \(\sigma, \tau_1, \ldots, \tau_\ell \not\in G_n\). Let \(\pi: G_{n-1} \to G_{n-1}/G_n\) be the natural projection. Then the argument above implies \(\pi(\sigma), \pi(\tau_1), \ldots, \pi(\tau_\ell) \neq 1\), therefore \(\pi(\sigma), \pi(\tau_1), \ldots, \pi(\tau_\ell)\) are of order three. Now the equality \(\sigma = \tau_1^e_1 \cdots \tau_\ell^e_\ell = \tau_1^{2e_1} \cdots \tau_\ell^{2e_\ell}\) implies

\[
\pi(\sigma) = \pi(\tau_1)^{e_1} \cdots \pi(\tau_\ell)^{e_\ell} = \pi(\tau_1)^{2e_1} \cdots \pi(\tau_\ell)^{2e_\ell} .
\]  

Moreover, by Condition (C) for \(G_{n-1}/G_n\), all of \(\pi(\tau_1), \ldots, \pi(\tau_\ell)\) commute with each other. Therefore we have \(\pi(\tau_1)^{2e_1} \cdots \pi(\tau_\ell)^{2e_\ell} = (\pi(\tau_1)^{e_1} \cdots \pi(\tau_\ell)^{e_\ell})^2\). Now the latter equality in Eq. (2) implies \(\pi(\tau_1)^{e_1} \cdots \pi(\tau_\ell)^{e_\ell} = 1\), contradicting the former equality in Eq. (2) as \(\pi(\sigma) \neq 1\). Hence the former part of the claim holds. Now the latter part of the claim follows by putting \(n = 1\) and \(G_1 = 1\) when \(G\) is Abelian, and by putting \(n = 2, G_1\) to be the cyclic normal subgroup of \(G\) of index two, and \(G_2 = 1\) when \(G\) is a dihedral group. Hence the claim holds.

5 Compressions over Symmetric Groups

In this section, we show that a group function over symmetric group \(S_n\) for \(n \leq 4\) with the desired property does not exist, and on the other hand, construct such a group function over alternating group \(A_5\) of smaller size (four) than the existing construction (of size six) over \(S_5\) in [3].

First we give the following results on the inexistence of such group functions.

Theorem 2. Let \(G = S_n\) with \(n \leq 4\). Then there does not exist a group function \(F\) over \(G\) satisfying Condition (*).

Proof. The claim for \(S_1\) and \(S_2\) is obvious, as neither \(S_1\) nor \(S_2\) has an element of order three. The claim for \(S_3\) follows from Theorem 1 and the fact that \(S_3\) is isomorphic to the dihedral group of order six.

For the case of \(S_4\), note that \(S_4\) has a normal subgroup \(H := \{1, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)\}\) and \(S_4/H \cong S_3\). Now as \(|H| = 4 \not\equiv 0 \pmod{3}\), Corollary 2 implies that if there were a group function over \(S_4\) satisfying Condition (*), then there would be a group function over \(S_3\) satisfying Condition (*), which contradicts the result in the previous paragraph. Hence the claim for \(S_4\) holds, concluding the proof.

Theorem 3. There does not exist a group function of size at most three over \(S_5\) satisfying Condition (*).

Proof. Owing to Proposition 1 it suffices to consider the case of size three. Assume for the contrary that \(\sigma, \tau_1, \tau_2, \tau_3\) and \(e_1, e_2, e_3\) satisfy the equivalent condition in Lemma 3. We may assume that \(e_1, e_2, e_3 \in \{1, 2\}\), as those elements \(\tau_\ell\) have order three. Then the equality \(\tau_1^{e_1} \tau_2^{e_2} \tau_3^{e_3} = \tau_1^{2e_1} \tau_2^{2e_2} \tau_3^{2e_3}\) implies \(\tau_2^{-e_2} \tau_1^{e_1} \tau_2^{2e_2} = \tau_3^{-e_3}\), or equivalently \(\tau_2^{-e_2} \tau_1^{e_1} \tau_2^{e_2} = \tau_3^{-e_3} \tau_2^{-e_2}\). The left-hand side is conjugate to \(\tau_1^{e_1}\) and hence to \(\sigma^{e_1}\) as well, therefore it is a cyclic permutation of length three (note that any element in \(S_3\) of order three is a cyclic permutation of length three). Moreover, both \(\nu_1 := \tau_3^{-e_3}\) and \(\nu_2 := \tau_2^{-e_2}\) are also cyclic permutations.
of length three by a similar reason. As the underlying group is \( S_5 \), we may write \( \nu_1 = (a \ b \ c) \) and \( \nu_2 = (a \ c \ b) \) where \( a, b, c \) are all different and \( a, c \) are all different.

If \( \{b_1, b_2\} \cap \{c_1, c_2\} \neq \emptyset \), then there is a subgroup \( H \) of \( S_5 \) satisfying that \( H \cong S_4 \) and \( \nu_1, \nu_2 \in H \). Now the equality \( \tau_2^{-e_2} \tau_1^{-e_1} \tau_2^{e_2} = \tau_3^{-e_3} \tau_2^{-e_2} \) implies \( \tau_1^{e_1} = \nu_2^{-1} \nu_1 \nu_2^2 \in H \). Hence \( \tau_i = (\tau_i^{e_i}) \in H \) for each \( i \in \{1, 2, 3\} \) (recall that \( e_i \in \{1, 2\} \) and \( \tau_i \) is of order three). Moreover, the equality \( \tau_1^{e_1} \tau_2^{e_2} \tau_3^{e_3} = \sigma \) implies \( \sigma \in H \), and as all of \( \sigma, \tau_1, \tau_2, \tau_3 \) are elements of \( H \cong S_4 \) of order three, those elements are conjugate in \( H \) to each other. Hence by Lemma 4 there is a group function over \( H \cong S_4 \) satisfying Condition (*) , contradicting Theorem 2.

From now, we consider the other case where \( \{b_1, b_2\} \cap \{c_1, c_2\} = \emptyset \). Now \( \nu_1 \nu_2 \) has to be a cyclic permutation of length three as mentioned above, while \( \nu_1 \nu_2 (c_2) = \nu_1 (a) = b_1, \nu_1 \nu_2 (b_1) = \nu_1 (b_1) = b_2 \), and \( \nu_1 \nu_2 (b_2) = \nu_1 (b_2) = c_1 \neq c_2 \). This is a contradiction. Hence the claim holds.

On the other hand, we give an observation towards constructing a group function over \( A_5 \) with the desired property. Here we give a proof of the following known fact for the sake of completeness.

**Lemma 5.** Let \( n \geq 5 \). Then any two cyclic permutations of length three are conjugate in \( A_n \).

**Proof.** Let \( \sigma, \tau \in A_n \) be cyclic permutations of length three. First we show that \( \sigma \) is conjugate in \( A_n \) to either \( \tau \) or \( \tau^2 \). Now \( \tau \) is conjugate to \( \sigma \) in \( S_n \), say \( u \tau u^{-1} = \sigma \) with \( u \in S_n \). The current claim holds when \( u \in A_n \); we consider the other case \( u \not\in A_n \) from now. Let \( \tau = (a \ b \ c) \). By the properties \( u \not\in A_n, (a \ b) \not\in A_n, \) and \( |S_n : A_n| = 2 \), we have \( v := u(a \ b) \in A_n \) and \( u = v(a \ b) \). Now \( \sigma = u \tau u^{-1} = v(a \ b) \tau (a \ b) v^{-1} \) and \( (a \ b) \tau (a \ b) = (a \ c \ b) = \tau^2 \); therefore \( \sigma = \tau^2 v^{-1} \). Hence the current claim holds.

Now it suffices to show that \( \tau \) is conjugate to \( \tau^2 \) in \( A_n \). For \( \tau = (1 \ 2 \ 3) \) this follows from the equality \((1 \ 2)(4 \ 5) \cdot (1 \ 2 \ 3) \cdot (1 \ 2)(4 \ 5) = (1 \ 3 \ 2) \); and for the other \( \tau \) this also follows by symmetry. Hence the claim holds.

**Corollary 4.** If there exists a group function of size \( \ell \) over \( S_5 \) satisfying Condition (*), then there exists a group function of size \( \ell \) over \( A_5 \) satisfying Condition (*).

**Proof.** By the hypothesis, some cyclic permutations \( \sigma, \tau_1, \ldots, \tau_\ell \in S_5 \) of length three and some \( e_1, \ldots, e_\ell \) satisfy the equivalent condition in Lemma 4. Now each \( \tau_i \) is conjugate to \( \sigma \) in \( A_5 \) by Lemma 5; therefore those elements satisfy the condition with respect to \( A_5 \) as well. Hence the claim holds.

Now our strategy to search for group functions over \( A_5 \) satisfying Condition (*) is as follows. We fix \( \sigma = (1 \ 2 \ 3) \). Observe that if \( \sigma, \tau_1, \ldots, \tau_\ell \) and \( e_1, \ldots, e_\ell \) satisfy the equivalent condition in Lemma 4 with respect to \( A_5 \), then the elements \( \sigma, \tau_1^{e_1}, \ldots, \tau_\ell^{e_\ell} \) and the exponents \( 1, \ldots, \ell \) also satisfy the condition (owing to Lemma 5). Hence it suffices to fix all the exponents to be 1’s. Now we search over all the choices of cyclic permutations \( \tau_1, \ldots, \tau_\ell \) of length three, starting from the smallest possible case \( \ell = 4 \), to obtain a desired group function. Following this strategy, a computer search using SageMath found e.g., \( \ell = 4, \tau_1 = (2 \ 4 \ 5), \tau_2 = (1 \ 5 \ 4), \tau_3 = (3 \ 4 \ 5), \) and \( \tau_4 = (2 \ 5 \ 4) \) that satisfy that \( \tau_1 \tau_2 \tau_3 \tau_4 = \sigma \) and \( \tau_1^2 \tau_2^2 \tau_3^2 \tau_4^2 = \sigma \).

By the relations \( \tau_i = u_i \sigma u_i^{-1} \) (for \( i \in \{1, \ldots, 4\} \)) with \( u_1 = (1 \ 2 \ 4 \ 3 \ 5) \in A_5, u_2 = (1 \ 5 \ 2 \ 4 \ 3) \in A_5, u_3 = (1 \ 3 \ 5 \ 2 \ 4) \in A_5, u_4 = (1 \ 2 \ 5 \ 3 \ 4) \in A_5, \) we get

\[
F(x) := u_1 x u_1^{-1} u_2 x u_2^{-1} u_3 x u_3^{-1} u_4 x u_4^{-1}
\]

\[
= (1 \ 2 \ 4 \ 3 \ 5) \cdot x \cdot (1 \ 3 \ 5) \cdot x \cdot (1 \ 4 \ 3) \cdot x \cdot (1 \ 5) \cdot x \cdot (1 \ 2 \ 5 \ 3 \ 4)
\]

to satisfy Condition (*) over \( A_5 \) with \( \sigma = (1 \ 2 \ 3) \), as desired.

### 6 The Case of Groups of Order up to 60

In this section, we prove the following result.

**Theorem 4.** Suppose that \( |G| \leq 60 \) and \( G \not\cong A_5 \). Then there does not exist a group function over \( G \) satisfying Condition (*).

6
Table 1: Numbers of non-isomorphic non-Abelian groups of order \( n \leq 60 \) with \( n \equiv 0 \pmod{3} \)

| Order \( n \) | 6 | 12 | 18 | 21 | 24 | 27 | 30 | 36 | 39 | 42 | 48 | 54 | 57 | 60 |
|-------------|---|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Number      | 1 | 3  | 3  | 1  | 12 | 2  | 3  | 10 | 1  | 5  | 47 | 12 | 1  | 11 |

Towards the proof of Theorem 4, we prepare the following lemma.

**Lemma 6.** Suppose that \( G \) has a normal subgroup \( H \) satisfying Condition (C). If there exists a group function of size \( \ell \) over \( G \) satisfying Condition (*), then there exists a group function of size \( \ell \) over \( G/H \) satisfying Condition (*).

**Proof.** Let \( \sigma \) and a group function \( F \) over \( G \) be as in the hypothesis. If \( \sigma \not\in H \), then Lemma 2 applied to the natural projection \( G \to G/H \) implies the claim. Therefore it suffices to deduce a contradiction by assuming that \( \sigma \in H \). Now as \( H \triangleleft G \), any element of \( G \) conjugate to \( \sigma \) is involved in \( H \). By Condition (C) for \( H \), all elements of \( G \) conjugate to \( \sigma \) commute with each other. Therefore Lemma 3 deduces a contradiction, as desired. Hence the claim holds.

**Corollary 5.** Suppose that \( G \) is the semidirect product \( G = H_1 \rtimes H_2 \) and the center \( Z(H_1) \) of \( H_1 \) is non-trivial. Then we have \( Z(H_1) \triangleleft G \), and if there exists a group function of size \( \ell \) over \( G \) satisfying Condition (*), then there exists a group function of size \( \ell \) over \( G/Z(H_1) \) satisfying Condition (*).

**Proof.** First, as \( Z(H_1) \) is preserved by any group automorphism on \( H_1 \), the group action on \( H_1 \) by \( H_2 \) also preserves \( Z(H_1) \). Therefore we have \( Z(H_1) \triangleleft G \). Now the claim follows from Lemma 6, as the Abelian group \( Z(H_1) \) satisfies Condition (C).}

We start the proof of Theorem 4. The basic strategy is a recursive argument with respect to the order \( n \) of \( G \). First note that no solution (a group function satisfying Condition (*)) exists if either \( n \not\equiv 0 \pmod{3} \) (as now \( G \) has no elements of order three) or \( G \) is Abelian (by Theorem 1). Due to this fact, it suffices to consider the choices of \( n \equiv 0 \pmod{3} \) for which there exists a non-Abelian group of order \( n \). Table 1 shows the numbers of non-isomorphic non-Abelian groups of order \( n \leq 60 \) with \( n \equiv 0 \pmod{3} \), quoted from the sequence A060689 of [5]. Moreover, if \( G \) is directly decomposable, i.e., \( G \) can be written as the direct product of two non-trivial groups, then Corollary 1 enables us to reduce the argument to the cases of smaller \( n \). Therefore, we can immediately exclude directly decomposable groups \( G \) from our argument.

From now, we perform case-by-case arguments for each possible order \( n \) of \( G \), by using the list of groups of small orders in [1]. Here \( C_N \) denotes the cyclic group of order \( N \), \( D_N \) denotes the dihedral group of order \( N \), and the symbol ‘\( \rtimes \)’ is used only for the case that the corresponding group action is non-trivial (i.e., it is not the direct product).

**Case** \( n = 6 \). Now the unique possibility of \( G \) is \( S_3 \), where no solution exists by Theorem 2.

**Case** \( n = 12 \). Now the three possibilities are \( D_{12}, A_4 \), and \( C_3 \rtimes C_4 \), where no solution exists by Theorem 1, Theorem 2, and Theorem 1 (with normal series \( 1 \triangleleft 1 \triangleleft C_3 \triangleleft G \)), respectively.

**Case** \( n = 18 \). Besides one directly decomposable case \( C_3 \rtimes S_3 \), there are two possibilities \( D_{18} \) and \( (C_3 \rtimes C_3) \rtimes C_2 \). Now no solution exists by Theorem 1.

**Case** \( n = 21, 39, \text{ or } 57 \). Now the unique possibilities of \( G \) for each case are \( C_7 \rtimes C_3, C_{13} \rtimes C_3 \), and \( C_{19} \rtimes C_3 \), respectively. For each of them, Corollary 2 reduces the argument to the case of smaller quotient group \( C_3 \).
Case $n = 24$. Among the 12 possibilities of $G$ shown in the list [1], there are six directly decomposable ones; $C_4 \times S_3$, $C_2 \times (C_3 \times C_4)$, $C_2 \times A_4$, $C_2 \times C_2 \times S_3$, $C_3 \times D_8$, and $C_3 \times Q_8$ where $Q_8$ denotes the quaternion group. The remaining six possibilities are $D_{24}$, $C_3 \times C_8$, $C_3 \times Q_8$, $(C_2 \times C_6) \rtimes C_2$, $S_4$, and the special linear group $SL_2(F_6)$. Except for the last one, no solution exists by Theorem 1 for the first four cases and by Theorem 2 for the fifth case, respectively. For the last case of $SL_2(F_3)$, it has a normal subgroup $H := \{ \pm I \}$ of order two, therefore Corollary 2 reduces the argument to the case of smaller group $G/H$.

Case $n = 27$. Now the two possibilities are $C_9 \rtimes C_3$ and $(C_3 \times C_3) \rtimes C_3$. For both cases, Lemma 6 with $H = C_9$ or $C_3 \times C_3$ reduces the argument to the case of smaller quotient group $C_3$.

Case $n = 30$. Besides two directly decomposable cases $C_3 \times D_{10}$ and $C_5 \times S_6$, there is one possibility $D_{30}$.

No solution exists by Theorem 1.

Case $n = 36$. Among the 10 possibilities of $G$ shown in the list [1], there are five directly decomposable ones; $C_2 \times ((C_3 \times C_3) \rtimes C_2)$, $C_3 \times A_4$, $C_3 \times (C_3 \times C_4)$, $C_6 \times S_4$, and $S_3 \times S_3$. The remaining five possibilities are $D_{36}$, $C_3 \rtimes C_4$, $(C_2 \times C_2) \rtimes C_9$, and $(C_3 \times C_3) \rtimes C_4$ (with two choices of group actions). For the third case, Corollary 2 reduces the argument to smaller quotient group $C_9$. For the remaining four cases, no solution exists by Theorem 1.

Case $n = 42$. Besides three directly decomposable cases $C_2 \times (C_7 \times C_3)$, $C_3 \times D_{14}$, and $C_7 \times S_3$, there are two possibilities $D_{42}$ and $(C_7 \times C_3) \rtimes C_2$. For the first case, no solution exists by Theorem 1. For the second case, no solution exists by Theorem 1 with normal series $1 \vartriangleleft C_7 \vartriangleleft C_7 \rtimes C_3 \vartriangleleft G$.

Case $n = 48$. Tables 2 and 3 give a list of non-isomorphic groups of order 48 quoted from [1], including five Abelian groups (IDs 2, 20, 23, 44, 52) and 47 non-Abelian groups. Among the 47 non-Abelian cases, 24 of them are directly decomposable. Moreover, for most of the remaining 23 cases, a direct application of Theorem 1 implies that no solution exists over the group. For example, for $G = C_3 \times C_{16}$ (ID 1) we take a normal series $1 \vartriangleleft 1 \vartriangleleft C_3 \vartriangleleft G$; for $G = (C_3 \times D_8) \rtimes C_2$ (ID 15) we take a normal series $1 \vartriangleleft D_8 \vartriangleleft C_3 \times D_8 \vartriangleleft G$; for $G = (C_2 \times (C_3 \times C_4)) \rtimes C_2$ (ID 19) we take a normal series $1 \vartriangleleft 1 \vartriangleleft C_3 \vartriangleleft C_3 \vartriangleleft C_3 \times C_3 \vartriangleleft C_2 \times (C_3 \times C_4) \vartriangleleft G$; and for $G = (C_4 \times S_3) \rtimes C_2$ (ID 41) we take a normal series $1 \vartriangleleft C_4 \vartriangleleft C_4 \times S_3 \vartriangleleft G$ (note that $S_3$ satisfies Condition (C)). Now we have the following four remaining cases from the table.

Subcase $G = [SL_2(F_3) \rtimes C_2]$ (ID 28). This group $G$ is the binary octahedral group $\langle a, b, c \mid a^4 = b^3 = c^2 = abc \rangle$. As $z := a^4 = b^3 = c^2$ is a non-trivial element in the center, we have $Z(G) \neq 1$. Now Corollary 5 reduces the argument to smaller quotient group $G/Z(G)$.

Subcase $G = GL_2(F_3)$ (ID 29). As the general linear group $GL_2(F_3)$ has a normal subgroup $H = \{ \pm I \}$ of order two, Corollary 2 reduces the argument to smaller quotient group $G/H$.

Subcase $G = A_4 \rtimes C_4$ (ID 30). Assume for the contrary that $\sigma, \tau_1, \ldots, \tau_t$ and $e_1, \ldots, e_t$ satisfy the equivalent condition in Lemma 1. Then Lemma 4 implies $\sigma, \tau_1, \ldots, \tau_t \in A_4$. Now as all elements of order three are conjugate to each other in $S_4$, the existence of such $\sigma, \tau_1, \ldots, \tau_t$ implies (by Lemma 1) that there exists a group function over $S_4$ satisfying Condition (*). This contradicts Theorem 2. Hence no solution exists in this case.

Subcase $G = SL_2(F_3) \rtimes C_2$ (ID 33). Recall that $SL_2(F_3)$ has nontrivial center, as $-I \in Z(SL_2(F_3))$. Now Corollary 5 reduces the argument to smaller quotient group $G/Z(SL_2(F_3))$.

This completes the argument for the case $n = 48$.  

8
Table 2: List of groups of order 48 (part I). In “Expression”, e.g., “C16” means $C_{16}$; ‘x’ denotes direct product; and ‘:’ denotes semidirect product. “Reason” indicates the reason why no solution exists.

| GAP4 ID | Expression       | Reason   |
|---------|------------------|----------|
| 1       | $[C3 : C16]$     | Theorem 1|
| 2       | $[C48]$          | Abelian  |
| 3       | $[(C4 \times C4) : C3]$ | Theorem 1|
| 4       | $[C8 \times S3]$ | Decomposable |
| 5       | $[C24 : C2]$     | Theorem 1|
| 6       | $[C24 : C2]$     | Theorem 1|
| 7       | $[D48]$          | Theorem 1|
| 8       | $[C3 : Q16]$     | Theorem 1|
| 9       | $[C2 \times (C3 : C8)]$ | Decomposable |
| 10      | $[(C3 : C8) : C2]$ | Theorem 1|
| 11      | $[C4 \times (C3 : C4)]$ | Decomposable |
| 12      | $[(C3 : C4) : C4]$ | Theorem 1|
| 13      | $[C12 : C4]$     | Theorem 1|
| 14      | $[(C12 \times C2) : C2]$ | Theorem 1|
| 15      | $[(C3 \times D8) : C2]$ | Theorem 1|
| 16      | $[(C3 \times C8) : C2]$ | Theorem 1|
| 17      | $[(C3 \times Q8) : C2]$ | Theorem 1|
| 18      | $[C3 : Q16]$     | Theorem 1|
| 19      | $[(C2 \times (C3 : C4)) : C2]$ | Theorem 1|
| 20      | $[C12 \times C4]$ | Abelian |
| 21      | $[C3 \times ((C4 \times C2) : C2)]$ | Decomposable |
| 22      | $[C3 \times (C4 : C4)]$ | Decomposable |
| 23      | $[C24 \times C2]$ | Abelian |
| 24      | $[C3 \times (C8 : C2)]$ | Decomposable |
| 25      | $[C3 \times D16]$ | Decomposable |
| 26      | $[C3 \times QD16]$ | Decomposable |

Case $n = 54$. Among the 12 possibilities of $G$ shown in the list [1], there are six directly decomposable ones: $C_2 \times ((C_3 \times C_3) \times C_3)$, $C_2 \times (C_9 \times C_3)$, $C_3 \times D_{18}$, $C_3 \times C_3 \times S_3$, $C_3 \times ((C_3 \times C_3) \times C_2)$, and $C_9 \times S_3$. The remaining six possibilities are $D_{54}$, $(C_9 \times C_3) \rtimes C_2$, $(C_3 \times C_3 \times C_3) \rtimes C_2$, $(C_3 \times C_3) \rtimes C_2$ (with two group actions), and $(C_9 \times C_3) \rtimes C_2$. For the first three cases, no solution exists by Theorem 1. For the remaining possibilities $G = H \rtimes C_2$ where $H = (C_3 \times C_3) \rtimes C_3$ or $H = C_9 \rtimes C_3$, we note that an argument using the conjugacy class equation implies that the group $H$ of order $27 = 3^3$ has non-trivial center. Now Corollary 5 reduces the argument to smaller quotient group $G/Z(H)$.

Case $n = 60$. Among the 10 possibilities of $G$ except $G \simeq A_5$ shown in the list [1], there are seven directly decomposable ones: $C_3 \times (C_5 \times C_4)$ (with two group actions), $C_5 \times (C_3 \times C_4)$, $C_5 \times A_4$, $C_6 \times D_{10}$, $S_3 \times D_{10}$, and $S_3 \times C_{10}$. For the remaining three possibilities $C_{15} \rtimes C_4$ (with two group actions) and $D_{60}$, no solution exists by Theorem 1.

This completes the proof of Theorem 4.

Acknowledgements. This work was supported by JSPS KAKENHI Grant Number 19H01804.
Table 3: List of groups of order 48 (part II). In “Expression”, e.g., “C16” means $C_{16}$; ‘x’ denotes direct product; and ‘:’ denotes semidirect product. “Reason” indicates the reason why no solution exists.

| GAP4 ID | Expression | Reason |
|---------|------------|--------|
| 27      | [C3 x Q16]| Decomposable |
| 28      | [C2 . S4 = SL(2,3) . C2]| (In the text) |
| 29      | [GL(2,3)]| (In the text) |
| 30      | [A4 : C4]| (In the text) |
| 31      | [C4 x A4]| Decomposable |
| 32      | [C2 x SL(2,3)]| Decomposable |
| 33      | [SL(2,3) : C2]| (In the text) |
| 34      | [C2 x (C3 : Q8)]| Decomposable |
| 35      | [C2 x C4 x S3]| Decomposable |
| 36      | [C2 x D24]| Decomposable |
| 37      | [(C12 x C2) : C2]| Theorem 1 |
| 38      | [D8 x S3]| Decomposable |
| 39      | [(C2 x (C3 : C4)) : C2]| Theorem 1 |
| 40      | [Q8 x S3]| Decomposable |
| 41      | [(C4 x S3) : C2]| Theorem 1 |
| 42      | [C2 x C2 x (C3 : C4)]| Decomposable |
| 43      | [C2 x ((C6 x C2) : C2)]| Decomposable |
| 44      | [C12 x C2 x C2]| Abelian |
| 45      | [C6 x D8]| Decomposable |
| 46      | [C6 x Q8]| Decomposable |
| 47      | [C3 x ((C4 x C2) : C2)]| Decomposable |
| 48      | [C2 x S4]| Decomposable |
| 49      | [C2 x C2 x A4]| Decomposable |
| 50      | [(C2 x C2 x C2 x C2) : C3]| Theorem 1 |
| 51      | [C2 x C2 x C2 x S3]| Decomposable |
| 52      | [C6 x C2 x C2 x C2]| Abelian |

References

[1] B. Allombert and I. Schein, List of Groups of Orders 1–143, in: A Database of Galois Polynomials, \url{http://pari.math.u-bordeaux.fr/galpol/}, accessed on November 19, 2021

[2] C. Gentry, Fully Homomorphic Encryption Using Ideal Lattices, in: Proceedings of STOC 2009, pp.169–178, 2009

[3] 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

[4] R. Ostrovsky, W. E. Skeith III, Communication Complexity in Algebraic Two-Party Protocols, in: Proceedings of CRYPTO 2008, Springer LNCS vol.5157, pp.379–396, 2008

[5] The On-Line Encyclopedia of Integer Sequences, \url{http://oeis.org/}, accessed on November 19, 2021