Research Article

New Bounds on 2-Frameproof Codes of Length 4

Penying Rochanakul

Research Center in Mathematics and Applied Mathematics, Department of Mathematics, Faculty of Science,
Chiang Mai University, Chiang Mai 50200, Thailand

Correspondence should be addressed to Penying Rochanakul; penying.rochanakul@cmu.ac.th

Received 30 August 2019; Revised 21 November 2019; Accepted 6 December 2019; Published 23 January 2020

Academic Editor: Aloys Krieg

Copyright © 2020 Penying Rochanakul. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Frameproof codes were first introduced by Boneh and Shaw in 1998 in the context of digital fingerprinting to protect copyrighted materials. These digital fingerprints are generally denoted as codewords in Q^n , where Q is an alphabet of size q and n is a positive integer. A 2-frameproof code is a code C such that any 2 codewords in C cannot form a new codeword under a particular rule. Thus, no pair of users can frame a user who is not a member of the coalition. This paper concentrates on the upper bound for the size of a q -ary 2-frameproof code of length 4. Our new upper bound shows that $|C| \leq 2q^2 - 2q + 1$ when q is odd and $q > 10$.

1. Introduction

In order to protect a digital content, a distributor marks each copy with a codeword. This marking discourages users from releasing an unauthorized copy, since a mark allows the distributor to detect any unauthorized copy and trace it back to the user. However, a coalition of users may detect some of the marks, namely, the ones where their copies differ. Thus, they can forge a new copy by changing these marks arbitrarily. To prevent a coalition of users from “framing” a user outside the coalition, Boneh and Shaw [1] defined the concept of frameproof codes. A w -frameproof code has the property that no coalition of at most w users can frame a user not in the coalition. Frameproof codes are defined as follows.

Let q and n be positive integers. Let Q be a set of size q , and let $C \subseteq Q^n$ be a set of words of length n over the alphabet Q . Each codeword $x \in C$ can be represented as $x = (x_1, x_2, \dots, x_n)$, where $x_i \in Q$ for all $i \in \{1, 2, \dots, n\}$. The set of descendants of $X \subseteq C$, $\text{desc}(X)$, is defined as

$$\text{desc}(X) = \{c \in Q^n : c_i = x_i \text{ for some } x \in X\}. \quad (1)$$

Definition 1. Let w be an integer such that $w \geq 2$. A w -frameproof code is a subset $C \subseteq Q^n$ such that for all $X \subseteq C$ with $|X| \leq w$, we have that $\text{desc}(X) \cap C = X$.

Example 1. Let $C = \{(0, 0, 0, 0), (0, 1, 2, 2), (0, 2, 1, 2), (0, 2, 2, 1), (1, 1, 1, 1), (1, 2, 0, 0), (1, 0, 0, 2), (1, 0, 2, 0), (2, 2, 2, 2), (2, 0, 1, 1), (2, 1, 0, 1), (2, 1, 1, 0)\}$. Then, C is a 3-ary 2-frameproof code of length 4.

As the number of codewords in the code corresponds to the number of authorized users in the digital copyright protection system, one of the classical question regarding frameproof codes is what is the largest cardinality $M_{n,w}(q)$ of a w -frameproof code of length n over an alphabet of size q ? This paper concentrates on the special case when $w = 2$, $n = 4$, and q is large.

There has been extensive study on the upper bound and lower bound on the size of frameproof codes [2–11]. Some of those are in separating hash families’ language [3, 6, 10, 11]. Previous bounds are restated as follows.

Theorem 1 (see [2]). Let q , n , and w be positive integers such that $q \geq 2$ and $2 \leq n \leq w$. Then,

$$M_{n,w}(q) = n(q - 1). \quad (2)$$

Theorem 2 (see [2]). Let n be a positive even integer such that $n \geq 4$. Let m be a prime power such that $m \geq n + 1$. Let $q = m^2 + 1$. There exists a q -ary 2-frameproof code of length n of size

$$2(q - 1)^{n/2} (1 - 1/(2\sqrt{q - 1})). \quad (3)$$

Theorem 3 (see [4]). *There exists a q -ary w -frameproof code of length $w + 2$ of size*

$$\frac{w+2}{w}(q-1)^2 + 1, \quad (4)$$

for all odd q , when $w = 2$, and for all $q \equiv 4 \pmod{6}$, when $w = 3$.

For 2-frameproof codes of length 4, Theorem 3 only gives lower bound for odd q . For even q , we first use only $q - 1$ symbols to construct a $(q - 1)$ -ary 2-frameproof code of size $2(q - 2)^2 + 1$. Then, add a codeword $(\alpha, \alpha, \alpha, \alpha)$ to the code, where α is the unused symbol. Thus, the following result on the lower bound of $M_{4,2}(q)$ is obtained.

Corollary 1 (see [4]). *For any positive integer q ,*

$$M_{4,2}(q) \geq \begin{cases} 2(q-1)^2 + 1, & \text{when } q \text{ is odd,} \\ 2(q-2)^2 + 2, & \text{when } q \text{ is even.} \end{cases} \quad (5)$$

In 2003, Blackburn proved the following upper bound of w -frameproof codes.

Theorem 4 (see [2]). *For any positive integers q , n , and $w \geq 2$, if C is a q -ary w -frameproof code of length n , then*

$$|C| \leq \max\{q^{n/w}, r(q^{n/w} - 1) + (w - r)(q^{n/w} - 1)\}, \quad (6)$$

where r is a unique integer in $\{0, 1, 2, \dots, w - 1\}$ such that $r = n \bmod w$.

When $n = 4$ and $w = 2$, the following result on the upper bound of $M_{4,2}(q)$ is obtained.

Corollary 2. *For any positive integer q ,*

$$M_{4,2}(q) \leq 2q^2 - 2. \quad (7)$$

Much later on, in 2019, Cheng et al. proved the following theorem, which is the best previously known result on the upper bound of 2-frameproof code of length 4.

Theorem 5 (see [5]). *For any positive integer $q > 48$, if C is a q -ary 2-frameproof code of length 4, then*

$$|C| \leq 2q^2 - 2q + 7. \quad (8)$$

Our result is the improved version of Theorem 5. We aim to prove the following theorem.

Theorem 6. *For any odd positive integer $q > 10$, if C is a q -ary 2-frameproof code of length 4, then*

$$|C| \leq 2q^2 - 2q + 1. \quad (9)$$

We analyze the combinatorial structure of a code, setting up an optimization problem, deriving some constraints, and solving this optimization problem to obtain Theorem 6. The gap between the lower bound of odd and even q in Corollary 1 is the

key motivation for proving the main result. The rest of this paper is ordered as follows. In Section 2, the essential notations are defined. Necessary conditions of a q -ary 2-frameproof code of length 4 are also stated. In Section 3, the proof of Theorem 6 is provided. We conclude the result in the last section.

2. Preliminaries

In this section, we define some notations and state relating lemmas that are useful for proving the main theorem.

Let $[4] = \{1, 2, 3, 4\}$. For $x = (x_1, x_2, x_3, x_4) \in C$, for $i \in [4]$, and for any non-empty set $I \subseteq [4]$,

- (i) let $f_i(x) = x_i$
- (ii) let $f_i(X) = \{x_i : x \in X\}$, for any $X \subseteq C$
- (iii) let $f_I(x) = (f_j(x))_{j \in I}$
- (iv) let $f_I(X) = \{f_I(x) : x \in X\}$, for any $X \subseteq C$

We say x is *unique* under I if $|\{z \in C : f_I(z) = f_I(x)\}| = 1$, and we say x is *nonunique* under I when $|\{z \in C : f_I(z) = f_I(x)\}| > 1$.

For any $I \subseteq [4]$, let $U_I = \{x \in C : x \text{ is unique under } I\}$ and $V_I = \{x \in C : x \text{ nonunique under } I\}$.

Remark. It is easy to see that for any nonempty subsets $I, J \subset [4]$, the following conditions hold:

- (i) $U_I \cap V_I = \emptyset$
- (ii) $C = U_I \cup V_I$
- (iii) $U_I \subseteq U_J$, for any $I \subseteq J \subseteq [4]$

Lemma 1. *Let C be a q -ary 2-frameproof code of length 4. For any $x = (x_1, x_2, x_3, x_4) \in C$ and any nonempty subset $I \subset [4]$, if $x \in V_I$, then $x \in U_{I'}$, where $I' = [4] \setminus I$.*

Proof. Let $x \in V_I$. Then, there exists $y \in C \setminus \{x\}$ such that $f_I(x) = f_I(y)$.

Assume $x \notin U_{I'}$. Then, $x \in V_{I'}$. Thus, there exists $z \in C \setminus \{x\}$ such that $f_{I'}(x) = f_{I'}(z)$. Hence, $x \in \text{desc}(\{y, z\})$. This contradicts the 2-frameproof property of C .

For convenience, we set up some parameters. Let $h_1 = |V_{\{2,3,4\}}|$, $h_2 = |V_{\{1,3,4\}}|$, $h_3 = |V_{\{1,2,4\}}|$, and $h_4 = |V_{\{1,2,3\}}|$. Without loss of generality, we assume $h_1 \geq h_2 \geq h_3 \geq h_4$.

Consider

$$\begin{aligned} C &= U_{\{1,2,3\}} \cup V_{\{1,2,3\}} \\ &= (U_{\{1,2,3\}} \cap C) \cup V_{\{1,2,3\}} \\ &= (U_{\{1,2,3\}} \cap (U_{\{3,4\}} \cup V_{\{3,4\}})) \cup V_{\{1,2,3\}} \\ &= (U_{\{1,2,3\}} \cap U_{\{3,4\}}) \cup (U_{\{1,2,3\}} \cap V_{\{3,4\}}) \cup V_{\{1,2,3\}}. \end{aligned} \quad (10)$$

From Lemma 1, we can see that $V_{\{3,4\}} \subseteq U_{\{1,2\}} \subseteq U_{\{1,2,3\}}$. Therefore, $U_{\{1,2,3\}} \cap V_{\{3,4\}} = V_{\{3,4\}}$. Since $U_{\{1,2,3\}} \cap U_{\{3,4\}}$, $V_{\{3,4\}}$, and $V_{\{1,2,3\}}$ are all pairwise disjoint, we have

$$|C| = |U_{\{1,2,3\}} \cap U_{\{3,4\}}| + |V_{\{3,4\}}| + h_4. \quad (11)$$

Hence, we can deduce upper bound of C from the upper bounds of $|U_{\{1,2,3\}} \cap U_{\{3,4\}}|$, $|V_{\{3,4\}}|$, and $|V_{\{1,2,3\}}|$. The

following sections are dedicated to the upper bounds of $|U_{\{1,2,3\}} \cap U_{\{3,4\}}|$, $|V_{\{3,4\}}|$, and $|V_{\{1,2,3\}}|$. $\square$

2.1. Upper Bound of $|U_{\{1,2,3\}} \cap U_{\{3,4\}}|$. This section gives the upper bound of the first component of equation (11).

Lemma 2. Suppose C is a q -ary 2-frameproof code of length 4. Then,

$$|U_{\{1,2,3\}} \cap U_{\{3,4\}}| \leq q^2 - qh_4 - |f_{\{3,4\}}(V_{\{3,4\}})|. \quad (12)$$

Proof. Assume $x \in U_{\{1,2,3\}}$. Then, we have that $x \in U_{\{1,2,3\}}$ and thus $f_4(x) \notin f_4(V_{\{1,2,3\}})$. Clearly, there are at most $q(q - h_4)$ choices of $f_{\{3,4\}}(x)$. Thus,

$$|f_{\{3,4\}}(U_{\{1,2,3\}} \cap U_{\{3,4\}})| + |f_{\{3,4\}}(U_{\{1,2,3\}} \cap V_{\{3,4\}})| \leq q^2 - qh_4. \quad (13)$$

From the definition of $U_{\{3,4\}}$, all x in $U_{\{3,4\}}$ has different values of $f_{\{3,4\}}(x)$. This makes $|f_{\{3,4\}}(U_{\{1,2,3\}} \cap U_{\{3,4\}})| = |U_{\{1,2,3\}} \cap U_{\{3,4\}}|$. So,

$$|U_{\{1,2,3\}} \cap U_{\{3,4\}}| + |f_{\{3,4\}}(U_{\{1,2,3\}} \cap V_{\{3,4\}})| \leq q^2 - qh_4. \quad (14)$$

Since $U_{\{1,2,3\}} \cap V_{\{3,4\}} = V_{\{3,4\}}$, then $|f_{\{3,4\}}(U_{\{1,2,3\}} \cap V_{\{3,4\}})| = |f_{\{3,4\}}(V_{\{3,4\}})|$. Therefore,

$$|U_{\{1,2,3\}} \cap U_{\{3,4\}}| \leq q^2 - qh_4 - |f_{\{3,4\}}(V_{\{3,4\}})|, \quad (15)$$

as required.

We use this lemma to find constraints on the upper bound of $|V_{\{i,j,k\}}|$. Then, after Section 2.3, we eliminate the term qh_4 before proving the main theorem. $\square$

2.2. Upper Bound of $|V_{\{3,4\}}|$. This section gives the upper bound of the second component of equation (11). It gives the same results as [5]. We put it here for completeness. We find an upper bound of $|V_{\{3,4\}}|$ by counting elements in $f_{\{1,2,3\}}(C)$.

Lemma 3. Suppose C is a q -ary 2-frameproof code of length 4. Then,

$$|V_{\{3,4\}}| \leq q^2 - \frac{|U_{\{1,2,3\}} \cap U_{\{3,4\}}|}{q} - (h_1 + h_2)(q - 1) + h_1h_2. \quad (16)$$

Proof. Assume $x \in U_{\{1,2,3\}} \cap V_{\{3,4\}}$. Then, x is nonunique under $\{3, 4\}$. Therefore, x must be unique under $\{1, 2\}$. Thus, when $c \neq f_3(x)$, the triple $(f_1(x), f_2(x), c)$ is a forbidden value in $f_{\{1,2,3\}}(C)$. We say x contributes at least $q - 1$ forbidden values in $f_{\{1,2,3\}}(C)$. And hence we can eliminate

$$|V_{\{3,4\}}|(q - 1), \quad (17)$$

values from $f_{\{1,2,3\}}(C)$.

Here, we reduce the size of $f_{\{1,2,3\}}(C)$ further. Let $h_1 = |U_{\{1,2,3\}} \cap V_{\{2,3,4\}}| = |V_{\{2,3,4\}}|$ and $h_2 = |U_{\{1,2,3\}} \cap V_{\{1,3,4\}}| =$

$|V_{\{1,3,4\}}|$. Assume $x \in V_{\{2,3,4\}}$. Then, x must be an element of $U_{\{1\}}$. Therefore, x must be unique under $\{1\}$. Thus, when $(b, c) \neq f_{\{2,3\}}(x)$, the triple $(f_1(x), b, c)$ is a forbidden values in $f_{\{1,2,3\}}(C)$. We say x contributes at least $q^2 - 1$ forbidden values in $f_{\{1,2,3\}}(C)$. To sum up, $V_{\{2,3,4\}}$ contributes at least

$$h_1(q^2 - 1), \quad (18)$$

forbidden values in $f_{\{1,2,3\}}(C)$. Similarly, $V_{\{1,3,4\}}$ contributes at least

$$h_2(q^2 - 1), \quad (19)$$

forbidden values in $f_{\{1,2,3\}}(C)$. However, the triple in the form of $(f_1(x), f_2(y), c)$, where $x \in V_{\{2,3,4\}}$, $y \in V_{\{1,3,4\}}$, and $c \in Q$ will be counted twice. Thus, together, $V_{\{2,3,4\}}$ and $V_{\{1,3,4\}}$ eliminate

$$(h_1 + h_2)(q^2 - 1) - h_1h_2q, \quad (20)$$

values from $f_{\{1,2,3\}}(C)$.

Furthermore, $V_{\{2,3,4\}}$ and $V_{\{1,3,4\}}$ are subsets of $V_{\{3,4\}}$. This makes $(h_1 + h_2)(q - 1)$ forbidden values counted twice in equations (17) and (20). Thus, we obtain at least

$$|V_{\{3,4\}}|(q - 1) + (h_1 + h_2)q(q - 1) - h_1h_2q, \quad (21)$$

different forbidden values in $f_{\{1,2,3\}}(C)$ from this step.

Hence,

$$|f_{\{1,2,3\}}(C)| \leq q^3 - |V_{\{3,4\}}|(q - 1) - (h_1 + h_2)q(q - 1) + h_1h_2q. \quad (22)$$

Since $(U_{\{1,2,3\}} \cap U_{\{3,4\}})$ and $V_{\{3,4\}}$ form a partition of $U_{\{1,2,3\}}$, we have

$$|f_{\{1,2,3\}}(U_{\{1,2,3\}})| = |V_{\{3,4\}}| + |f_{\{1,2,3\}}(U_{\{1,2,3\}} \cap U_{\{3,4\}})|. \quad (23)$$

From equations (22) and (23), we have

$$\begin{aligned} |V_{\{3,4\}}| + |f_{\{1,2,3\}}(U_{\{1,2,3\}} \cap U_{\{3,4\}})| &\leq |f_{\{1,2,3\}}(C)| \\ &\leq q^3 - |V_{\{3,4\}}|(q - 1) - (h_1 + h_2)q(q - 1) + h_1h_2q. \end{aligned} \quad (24)$$

Thus,

$$|V_{\{3,4\}}| \leq q^2 - \frac{|U_{\{1,2,3\}} \cap U_{\{3,4\}}|}{q} - (h_1 + h_2)(q - 1) + h_1h_2. \quad (25)$$

We use this lemma to find constraints on the upper bound of $|V_{\{i,j,k\}}|$ in the next section. $\square$

2.3. Upper Bound of $|V_{\{i,j,k\}}|$. This section aim to eliminate the third component of equation (11). Recall that we define $h_1 = |V_{\{2,3,4\}}|$, $h_2 = |V_{\{1,3,4\}}|$, $h_3 = |V_{\{1,2,4\}}|$, and $h_4 = |V_{\{1,2,3\}}|$.

Lemma 4. Suppose C is a q -ary 2-frameproof code of length 4 such that $q \geq 3$.

If $h_1 \geq h_2 \geq h_3 \geq h_4$, then $h_2 = h_3 = h_4 = 0$ and $h_1 \in \{0, 2, 3\}$.

Proof. From equation (11), Lemma 2 and Lemma 3, we have

$$\begin{aligned}
|C| &= |U_{\{1,2,3\}} \cap U_{\{3,4\}}| + |V_{\{3,4\}}| + h_4 \\
&\leq |U_{\{1,2,3\}} \cap U_{\{3,4\}}| + \left(q^2 - \frac{|U_{\{1,2,3\}} \cap U_{\{3,4\}}|}{q} \right. \\
&\quad \left. - (h_1 + h_2)(q-1) + h_1 h_2 + h_4 \right) \\
&= |U_{\{1,2,3\}} \cap U_{\{3,4\}}| \left(1 - \frac{1}{q} \right) + q^2 \\
&\quad - (h_1 + h_2)(q-1) + h_1 h_2 + h_4 \\
&\leq \left(q^2 - q h_4 - |f_{\{3,4\}}(V_{\{3,4\}})| \right) \left(1 - \frac{1}{q} \right) + q^2 \quad (26) \\
&\quad - (h_1 + h_2)(q-1) + h_1 h_2 + h_4 \\
&= 2q^2 - q - h_4(q-2) - |f_{\{3,4\}}(V_{\{3,4\}})| \left(1 - \frac{1}{q} \right) \\
&\quad - (h_1 + h_2)(q-1) + h_1 h_2 \\
&\leq 2q^2 - q - |f_{\{3,4\}}(V_{\{3,4\}})| \left(1 - \frac{1}{q} \right) \\
&\quad - (h_1 + h_2)(q-1) + h_1 h_2.
\end{aligned}$$

From Corollary 1, we have that there always exists a q -ary 2-FP code of size $2(q-1)^2 + 1$ for any positive odd integer q . So, we have

$$\begin{aligned}
2(q-1)^2 + 1 &\leq |C| \leq 2q^2 - q - |f_{\{3,4\}}(V_{\{3,4\}})| \left(1 - \frac{1}{q} \right) \\
&\quad - (h_1 + h_2)(q-1) + h_1 h_2 \\
&\leq 2q^2 - q - (h_1 + h_2)(q-1) + h_1 h_2, \quad (27)
\end{aligned}$$

which can be rewritten as

$$3(q-1) \geq (h_1 + h_2)(q-1) - h_1 h_2. \quad (28)$$

Note that if $h_1 = q$ or $h_2 = q$, there are at most q codewords in C . We then only consider the case $0 \leq h_1$ and $h_2 \leq q-1$. We have

$$3(q-1) \geq (h_1 + h_2)(q-1) - (q-1)h_2 \geq h_1(q-1). \quad (29)$$

Hence,

$$0 \leq h_2 \leq h_1 \leq 3. \quad (30)$$

Substitute in equation (28), we obtain

$$3(q-1) \geq (h_1 + h_2)(q-1) - 9. \quad (31)$$

Thus,

$$0 \leq h_1 + h_2 \leq 3, \quad (32)$$

when $q > 10$.

Since it is impossible to have a single codeword in C , that is, nonunique under $\{i, j, k\}$, then $h_\ell \neq 1$ for all $\ell \in [4]$. Therefore, if $h_1 \neq 0$, then $h_1 \geq 2$. Thus, with the maximal of h_1 , we have $h_2 = h_3 = h_4 = 0$. Furthermore, there are only 3 possible cases for h_1 , which are $h_1 = 3$, $h_1 = 2$, and $h_1 = 0$. $\square$

Remark. Note that the condition $q > 10$ can be removed by substituting corresponding values into equations (28) and (32) repeatedly until a contradiction is reached.

3. Main Results

In this section, we aim to prove Theorem 6, which is the main theorem.

By applying the condition $h_2 = h_3 = h_4 = 0$ from Lemma 4 to equations (11) and (26), we obtain new equations:

$$|C| = |U_{\{1,2,3\}} \cap U_{\{3,4\}}| + |V_{\{3,4\}}|, \quad (33)$$

$$|C| \leq 2q^2 - q - |f_{\{3,4\}}(V_{\{3,4\}})| \left(1 - \frac{1}{q} \right) - h_1(q-1). \quad (34)$$

We also obtain the following corollary from Lemma 2.

Corollary 3. Suppose C is a q -ary 2-frameproof code of length 4. Then,

$$|U_{\{1,2,3\}} \cap U_{\{3,4\}}| \leq q^2 - |f_{\{3,4\}}(V_{\{3,4\}})|. \quad (35)$$

Using equations (33) and (34) and Corollary 3, we now prove Theorem 6.

Proof of the Theorem 6. Here, $|f_{\{3,4\}}(V_{\{3,4\}})|$ is the number of different order pairs $(f_3(x), f_4(x))$, where x is nonunique in the last two positions. If we remove all codewords in $V_{\{2,3,4\}}$ from C , then h_1 symbols from $f_1(V_{\{2,3,4\}})$ are also eliminated from the first position of the remaining codewords. The condition $h_2 = 0$ implies $V_{\{1,3,4\}} = \emptyset$. Thus, each order pair in $f_{\{3,4\}}(V_{\{3,4\}})$ is used at most $q - h_1$ times in the last two positions of remaining codewords. Thus,

$$|V_{\{3,4\}}| - h_1 \leq (q - h_1) |f_{\{3,4\}}(V_{\{3,4\}})| \quad (36)$$

So, by equations (33) and (36) and Corollary 3, we have

$$\begin{aligned}
|C| &= |U_{\{1,2,3\}} \cap U_{\{3,4\}}| + |V_{\{3,4\}}| \\
&= |U_{\{1,2,3\}} \cap U_{\{3,4\}}| + (|V_{\{3,4\}}| - h_1) + h_1 \\
&\leq \left(q^2 - |f_{\{3,4\}}(V_{\{3,4\}})| \right) + (q - h_1) |f_{\{3,4\}}(V_{\{3,4\}})| + h_1. \quad (37)
\end{aligned}$$

Thus, by Corollary 1,

$$2(q-1)^2 + 1 \leq |C| \leq q^2 + (q-1-h_1) |f_{\{3,4\}}(V_{\{3,4\}})| + h_1. \quad (38)$$

Hence,

$$\begin{aligned}
|f_{\{3,4\}}(V_{\{3,4\}})| &\geq \frac{1}{q-1-h_1} (2(q-1)^2 + 1 - q^2 - h_1) \\
&= \begin{cases} q, & \text{for } h_1 = 3, \\ q-1 - \frac{2}{q-3}, & \text{for } h_1 = 2, \\ q-3, & \text{for } h_1 = 0, \end{cases} \quad (39) \\
&\geq q-3.
\end{aligned}$$

However, when $q-3 \leq |f_{\{3,4\}}(V_{\{3,4\}})| \leq q-2$, we have $|C| = |U_{\{1,2,3\}} \cap U_{\{3,4\}}| + |V_{\{3,4\}}| \leq |U_{\{1,2,3\}} \cap U_{\{3,4\}}| + q|f_{\{3,4\}}(V_{\{3,4\}})| \leq q^2 - (q-3) + q(q-2) < 2q^2 - 2q$. Thus, we only have yet to consider the case that $|f_{\{3,4\}}(V_{\{3,4\}})| \geq q-1$.

Substitute $|f_{\{3,4\}}(V_{\{3,4\}})| \geq q-1$ in (34), we obtain

$$\begin{aligned}
|C| &\leq 2q^2 - q - |f_{\{3,4\}}(V_{\{3,4\}})| \left(1 - \frac{1}{q}\right) - h_1(q-1) \\
&\leq 2q^2 - q - (q-1) \left(1 - \frac{1}{q}\right) \quad (40) \\
&= 2q^2 - 2q + 2 - \frac{1}{q}.
\end{aligned}$$

Since $|C|$ must be an integer, $|C| \leq 2q^2 - 2q + 1$ as required.

We show that $|C| \leq 2q^2 - 2q + 1$ for odd $q > 10$. Thus, $2q^2 - 4q + 3 \leq M_{4,2}(q) \leq 2q^2 - 2q + 1$.

Example 1 gives a 3-ary 2-frameproof of size $12 = 2q^2 - 2q$ for $q = 3$, which is very close to the obtained upper bound. However, things could be different for larger q .

Consider h_1 from the proof of Theorem 6. Notice that for $h_1 \geq 2$, $|f_{\{3,4\}}(V_{\{3,4\}})|$ must be an integer. We can conclude that $|f_{\{3,4\}}(V_{\{3,4\}})| \geq q-1$ for $h_1 = 2$. Hence, for $h_1 \geq 2$, we have $|C| \leq 2q^2 - 4q + 4 - 1/q$. This implies $|C| \leq 2q^2 - 4q + 3$ which is equal to the lower bound. Thus, this could also be investigated further whether it is possible to push the upper bound down to $2q^2 - 4q + 3$ when $h_1 = 0$.

4. Conclusion

In this paper, we investigate the bounds of 2-frameproof codes with length 4 by observing the structure of a code. The improvement of the upper bound for the case of odd q is derived from the difference between the known lower bound of odd and even q . The paper shows that $|C| \leq 2q^2 - 2q + 1$ in the case when q is odd and $q > 10$. Then, if q is large, $2q^2 - 4q + 3 \leq M_{4,2}(q) \leq 2q^2 - 2q + 1$ when q is odd and $2q^2 - 8q + 10 \leq M_{4,2}(q) \leq 2q^2 - 2q + 7$ when q is even. Example 1, for $q = 3$, suggests that the upper bound might be tighter than the lower bound; however, the case of larger q is yet to be determined.

Data Availability

No data were used to support this study since all proofs are included in the manuscript.

Conflicts of Interest

The author declares that there are no conflicts of interest.

Acknowledgments

This research was supported by Chiang Mai University.

References

- [1] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1897–1905, 1998.
- [2] S. R. Blackburn, "Frameproof codes," *SIAM Journal on Discrete Mathematics*, vol. 16, no. 3, pp. 499–510, 2003.
- [3] S. R. Blackburn, T. Etzion, D. R. Stinson, and G. M. Zaverucha, "A bound on the size of separating hash families," *Journal of Combinatorial Theory, Series A*, vol. 115, no. 7, pp. 1246–1256, 2008.
- [4] Y. M. Chee and X. Zhang, "Improved constructions of frameproof codes," *IEEE Transactions on Information Theory*, vol. 58, no. 8, pp. 5449–5453, 2012.
- [5] M. Cheng, J. Jiang, and Q. Wang, "Improved bounds on 2-frameproof codes with length 4," *Designs, Codes and Cryptography*, vol. 87, no. 1, pp. 97–106, 2019.
- [6] M. Bazrafshan and T. van Trung, "Bounds for separating hash families," *Journal of Combinatorial Theory, Series A*, vol. 118, no. 3, pp. 1129–1135, 2011.
- [7] A. Kathuria, S. Batra, and S. K. Arora, "A class of 2-FP codes," *Journal of Information and Optimization Sciences*, vol. 38, no. 8, pp. 1311–1324, 2017.
- [8] C. Shangguan, X. Wang, G. Ge, and Y. Miao, "New bounds for frameproof codes," *IEEE Transactions on Information Theory*, vol. 63, no. 11, pp. 7247–7252, 2017.
- [9] J. N. Staddon, D. R. Stinson, and R. Ruizhong Wei, "Combinatorial properties of frameproof and traceability codes," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1042–1049, 2001.
- [10] D. R. Stinson, R. Wei, and K. Chen, "On generalized separating hash families," *Journal of Combinatorial Theory, Series A*, vol. 115, no. 1, pp. 105–120, 2008.
- [11] T. van Trung, "A tight bound for frameproof codes viewed in terms of separating hash families," *Designs, Codes and Cryptography*, vol. 72, no. 3, pp. 713–718, 2014.