Thai Journal of Mathematics : 401-412
Special Issue : Annual Meeting in Mathematics 2019

http://thaijmath.in.cmu.ac.th
Online ISSN 1686-0209

Improved Bounds on the Size of Separating Hash Families of Short Length

Penying Rochanakul[1]

Research Center in Mathematics and Applied Mathematics,
Department of Mathematics, Faculty of Science,
Chiang Mai University, Chiang Mai 50200, Thailand.
e-mail : Penying.Rochanakul@cmu.ac.th

Abstract : In this paper, we present some new upper bounds on the size of separating hash families of type $\{w_1, w_2\}$ of short length, where the length N is not exceeding $2w_2$. A new proof for tight bounds on the size of separating hash families of type $\{1, w\}$ is also given.

Keywords : separating hash families; frameproof codes.
2010 Mathematics Subject Classification : 05D99; 94B25.

1 Introduction

Let X and Y be two finite sets. Let f be a function mapping from X to Y. Let A and $B \subseteq X$. We say f *separates* A and B when$f(A) \cap f(B) = \phi$. A *hash family* $\mathcal{F}$ is a family of functions $\{f_i : X \to Y, i \in \{1, 2, ..., N\}\}$, for some positive integer N. Let n, m and t be positive integers and let $w_1, w_2, ..., w_t$ be positive integers in non-decreasing order.

Definition 1.1. Let X and Y be two finite sets such that $|X| = n$ and $|Y| = m$. Let $\mathcal{F}$ be a family of functions $\{f_i : X \to Y, i \in \{1, 2, ..., N\}\}$, for some positive integer N. Then $\mathcal{F}$ is an $(N; n, m, \{w_1, w_2, ..., w_t\})-$*separating hash family*, or an SHF$(N; n, m, \{w_1, w_2, ..., w_t\})$ if for any pairwise disjoint $C_1, C_2, ..., C_t \subseteq X$ such that $|C_j| \leq w_j, j \in \{1, 2, ..., t\}$, there exists $i \in \{1, 2, ..., N\}$ such that f_i separates $C_1, C_2, ..., C_t \subseteq X$.

This work was supported by Chiang Mai University, Chiang Mai, Thailand.
[1]Corresponding author.

For any $\mathrm{SHF}(N; n, m, \{w_1, w_2, ..., w_t\})$, we refer to n, N and $\{w_1, w_2, ..., w_t\}$ as its *size*, *length* and *type*, respectively.

We avoid the trivial case by letting $m \geq 2$ and $t \geq 2$.

Here are some known results on the bounds of separating hash families.

Theorem 1.2. ([1, Theorem 1])
If there exists an $\mathrm{SHF}(N; n, m, \{w_1, w_2, ..., w_t\})$*, then*

$$n \leq (w_1 w_2 + u - w_1 - w_2) m^{\lceil \frac{N}{u-1} \rceil} \tag{1.1}$$

where $u = \sum_i w_i$*.*

Theorem 1.3. ([2, Theorem 6])
If there exists an $\mathrm{SHF}(N; n, m, \{w_1, w_2, ..., w_t\})$*, then*

$$n \leq (u-1) m^{\lceil \frac{N}{u-1} \rceil} \tag{1.2}$$

where $u = \sum_i w_i$*.*

The following theorem is the best previously known result on the upper bound of separating hash families of type $\{1, w\}$. The theorem is originally in frameproof codes language.

Theorem 1.4. ([3, Corollary 12])
If there exists an $\mathrm{SHF}(N; n, m, \{1, w\})$*, then*

$$n \leq \left(\frac{N}{N - (r-1)\lceil \frac{N}{w} \rceil} \right) m^{\lceil \frac{N}{w} \rceil} + O\left(m^{\lceil \frac{N}{w} \rceil - 1} \right),$$

where r is a unique positive integer in $\{1, 2, ..., w\}$ such that $r \equiv N \bmod w$.

In the following sections we state our new bounds and compare them with the known results. Section 3 is dedicated to separating hash families of type $\{1, w\}$. The improved bounds for separating hash families of type $\{w_1, w_2\}$ are presented in Section 4.

2 Separating Hash Families Type $\{1, w\}$

2.1 Case of length equals $1 \bmod w$

In [4], Trung stated and proved the tight bounds for separating hash families of type $\{1, w\}$, when the length $N \equiv 1 \bmod w$. Here we present our alternate proof.

Theorem 2.1. *Let m, n, w and N be positive integers where $m > w \geq 2$, $n \geq 2$ and $N \equiv 1 \bmod w$. If there exists an* $\mathrm{SHF}(N; n, m, \{1, w\})$*, then*

$$n \leq m^{\lceil \frac{N}{w} \rceil}.$$

To make it easier for us to generate the proof for Theorem 2.1, it is necessary that we introduce some additional terms and notation, including definition and a relevant theorem of a combinatorial object.

Let $\mathcal{F} = \{f_i : X \to Y, i \in \{1,2,...,N\}\}$ be an SHF$(N; n, m, \{w_1, w_2\})$. For any $x \in X$, any $i \in \{1,2,...,N\}$, and any $I \subseteq \{1,2,...,N\}$, let $x_i = f_i(x)$, and let $x_I = (f_j(x))_{j \in I}$. We say x is *unique* under I if $|\{z \in X : z_I = x_I\}| = 1$, and we say x is *non-unique* under I when $|\{z \in X : z_I = x_I\}| > 1$.

For any $I \subseteq \{1,2,...,N\}$, let $U_I = \{x \in X : x \text{ is unique under } I\}$.

Definition 2.2. A family $\mathcal{S}$ of subsets of a set is *t-colliding* if $\mathcal{S}$ does not contain t pairwise disjoint subsets.

Theorem 2.3 ([3], Theorem 11)**.** *Let t, k and ℓ be positive integers such that $\ell \geq tk$. Let $\mathcal{S}$ be a t-colliding family of subsets of $\{1,2,...,\ell\}$, where $|S| = k$ for all $S \in \mathcal{S}$. Then*

$$|\mathcal{S}| \leq \binom{\ell}{k}\frac{(t-1)k}{\ell}.$$

Proof of Theorem 2.1. Let $\mathcal{F} = \{f_1, f_2, ..., f_{wh+1} : X \to Y\}$ be an SHF$(wh+1; n, m, \{1, w\})$. Assume for contradiction that $n \geq m^{h+1} + 1$.

For any $i \in \{1,2,...,wh+1\}$, let $\mathcal{I}_i$ be the set of all i-subsets of $\{1,2,...,wh+1\}$. For any $I \in \mathcal{I}_{h+1}$, there are at most m^{h+1} possible $(h+1)$-tuples for x_I. Thus, there are at least $\left\lceil \frac{m^{h+1}+1}{m^{h+1}} \right\rceil = 2$ elements $x, x' \in X$ with $x_I = x'_I$, by the pigeonhole principle.

Let $I_{max} \in \mathcal{I}_{h+1}$ maximize the number of $x \in X$ where $x \notin U_{I_{max}}$.
Let $s = |X \backslash U_{I_{max}}|$. It follows from the previous paragraph that $s \geq 2$.

Claim. There exits $J \in \mathcal{I}_h$ such that $J \cap I_{max} = \emptyset$ and at least $\frac{s}{w-1}$ elements $x \in X \backslash U_{I_{max}}$ are unique under J.

Once we are confident that the claim is true the rest of the proof follows naturally. To justify the claim, we define $\mathcal{J}_x$, for each $x \in X \backslash U_{I_{max}}$, to be the set of all h-subsets I' of $\{1,2,...,wh+1\} \backslash I_{max}$ such that $x \notin U_{I'}$. Then $\mathcal{J}_x$ must be a $(w-1)$-colliding family.

Assume that $\mathcal{J}_x$ is not a $(w-1)$-colliding family. Then there exist pairwise disjoint sets $J_1, J_2, ..., J_{w-1}$ in $\mathcal{J}_x$ such that

$$\bigcup_{i=1}^{w-1} J_i = \{1,2,...,wh+1\} \backslash I_{max}.$$

Since $x \in X \backslash U_{I_{max}}$, there exists an element $z \in X \backslash U_{I_{max}}$ such that $z \neq x$ and $z_{I_{max}} = x_{I_{max}}$. For each $i \in \{1,2,...,w-1\}$, let z^i be an element of $X \backslash \{x\}$ such that $z^i_{J_i} = x_{J_i}$. This makes $f(\{x\}) \cap f(\{z, z^1, z^2, ..., z^{w-1}\}) \neq \emptyset$ for all $f \in \mathcal{F}$, contradicting to the SHF$(wh+1; n, m, \{1, w\})$ property of $\mathcal{F}$.

We have that $\mathcal{J}_x$ is a $(w-1)$-colliding family. By Theorem 2.3, $|\mathcal{J}_x| \leq \binom{(w-1)h}{h}\frac{w-2}{w-1}$.

Note that there are $\binom{(w-1)h}{h}$ different h-subsets of $\{1,2,...,wh+1\}\backslash I_{max}$. Therefore the number of h-subsets I of $\{1,2,...,wh+1\}\backslash I_{max}$ that $x \in U_I$ is

$$\binom{(w-1)h}{h} - |\mathcal{J}_x| \geq \binom{(w-1)h}{h} - \binom{(w-1)h}{h}\frac{w-2}{w-1} = \binom{(w-1)h}{h}\frac{1}{w-1}.$$

This establishes our claim.

Now we consider $U_{I_{max}}$. The number of h-tuples of the form x_J when $x \in U_{I_{max}}$ is at most $m^h - \dfrac{s}{w-1}$ by our choice of J. Let the exact number of h-tuples be η, where $\eta \leq m^h - \dfrac{s}{w-1}$. Let $X_1, \ldots, X_\eta$ denote the partition of $U_{I_{max}}$ under x_J.

Let $j \in \{1,2,...,wh+1\}\backslash J$ be fixed, and define $I_0 \in \mathcal{I}_{h+1}$ by $I_0 = J \cup \{j\}$. Observe that there are at most m symbols occur in the j^{th} coordinate. Hence each X_i contributes at least $|X_i| - m$ non-unique $(h+1)$-tuples under I_0.

Therefore, the number of $x \in X$ that are non-unique under I_0 is at least

$$\begin{aligned}
|X\backslash U_{I_0}| &\geq \sum_{h=1}^{\eta}(|X_i| - m) \\
&= \sum_{h=1}^{\eta}|X_i| - \sum_{h=1}^{\eta} m \\
&= |U_{I_{max}}| - \eta m \\
&\geq (m^{h+1} + 1 - s) - \left(m^h - \frac{s}{w-1}\right)m \\
&= 1 + s(\frac{m}{w-1} - 1) \\
&> s.
\end{aligned}$$

Since $m \geq 2(w-1)$, which contradicts our choice of I_{max}.

Thus, $n \leq m^{h+1}$ as required. □

2.2 Case of length between w and $2w$

In this section, we focus on improving the previously known bounds for separating hash families of type $\{1, w\}$, when the length N satisfies $w < N \leq 2w$. We will first compare the previously known results. Then state and prove the new bounds. Our bound is as least as good as the previously known bounds. Moreover, it is tight for the case of $N = w + 2$ as constructed by orthogonal arrays in [5].

Let m, n, w be positive integers greater than 1 and let r be an integer such that $0 < r \leq w$. Then $w < w + r \leq 2w$. From Theorems 1.3 and 1.4, we can derive the two following results on the upper bound of separating hash families.

Corollary 2.4. *Let m, n, w and r be positive integers where $m > w \geq 2$, $n \geq 2$ and $0 < r \leq w$. If there exists an* $\mathrm{SHF}(w+r; n, m, \{1, w\})$, *then*

$$n \leq wm^2.$$

Corollary 2.5. *Let m, n, w and r be positive integers where $m > w \geq 2$, $n \geq 2$ and $0 < r \leq w$. If there exists an* $\mathrm{SHF}(w+r; n, m, \{1, w\})$, *then*

$$n \leq \gamma m^2 + O(m),$$

where $\gamma = \frac{w+r}{w-r+2}$.

Note that $1 \leq \gamma \leq w$, which equality occurs only when $r = 1$ and $r = w$. Hence the leading term in Corollary 2.5 is better than the leading term in Corollary 2.4.

The next theorem is our new result. Notice that the term $O(m)$ is eliminated from the bounds in Theorem 2.5.

Theorem 2.6. *Let m, n, w and r be positive integers where $m > w \geq 2$, $n \geq 2$ and $0 < r \leq w$. If there exists an* $\mathrm{SHF}(w+r; n, m, \{1, w\})$, *then*

$$n \leq \gamma m^2,$$

where $\gamma = \frac{w+r}{w-r+2}$.

Recall the notions of x_i, x_I and U_I from Section 3. Inspired by the proof of Theorem 1.4 in [3], we generate the proof as follows.

Proof of Theorem 2.6. Let $\mathcal{F} = \{f_1, f_2, ..., f_{w+r} : X \to Y\}$ be an $\mathrm{SHF}(w + r; n, m, \{1, w\})$.

Let $S_1, S_2, ..., S_w$ be pairwise disjoint subsets of $\{1, 2, ..., w+r\}$, where cardinality of S_i is 2 for $i \leq r$ and 1 otherwise. It is not difficult to see that $S_1 \cup S_2 \cup ... \cup S_w = \{1, 2, ..., w+r\}$ since S_i are pairwise disjoint and $\sum_{i=1}^{w} |S_i| = 2r + 1(w-r) = w+r$.

Moreover, it can be seen from the following contradiction that $U_{S_1} \cup U_{S_2} \cup ... \cup U_{S_w} = X$.

Assume for a contradiction that $U_{S_1} \cup U_{S_2} \cup ... \cup U_{S_w} \neq X$. Then, there exists $x \in X \setminus (U_{S_1} \cup U_{S_2} \cup ... \cup U_{S_w})$. Hence $x \notin U_{S_i}$ for all $i \in \{1, 2, ..., w\}$. Therefore, for every $i \in \{1, 2, ..., w\}$, there exists $y^i \in X \setminus \{x\}$ such that $f_j(y^i) = f_j(x)$ for all $j \in S_i$, i.e., none of function f_j, $j \in S_i$ can separate x and y^i. Let $C_1 = \{x\}$, $C_2 = \{y^1, ..., y^w\}$. We have $|C_1| \leq 1, |C_2| \leq w$ and C_1, C_2 are disjoint. Since $S_1 \cup S_2 \cup ... \cup S_w = \{1, 2, ..., w+r\}$, none of function $f_j \in \mathcal{F}$ can separate C_1 and C_2, contradicts the $\mathrm{SHF}(w + r; n, m, \{1, w\})$ property of $\mathcal{F}$. Therefore, $U_{S_1} \cup U_{S_2} \cup ... \cup U_{S_w} = X$.

Let $W = \bigcup_{\substack{S \subseteq \{1,2,...,w+r\},\\ |S|=1}} U_S$ and let $Z = X \setminus W$. For any $I \subseteq \{1, 2, ..., w+r\}$, define $\Gamma_I = U_I \cap Z$.

For any choice of $S_1, ..., S_w$, whenever $i \geq r+1$, we have that $\Gamma_{S_i} = U_{S_i} \cap Z = \emptyset$ and

$$\begin{aligned}\Gamma_{S_1} \cup \Gamma_{S_2} \cup ... \cup \Gamma_{S_r} &= (U_{S_1} \cap Z) \cup (U_{S_2} \cap Z) \cup ... \cup (U_{S_r} \cap Z)\\ &= (U_{S_1} \cap Z) \cup (U_{S_2} \cap Z) \cup ... \cup (U_{S_w} \cap Z)\\ &= X \cap Z\\ &= Z. \end{aligned} \tag{2.1}$$

Since $|U_{\{i\}}| \leq m$ for all $i \in \{1, 2, ..., w+r\}$ and by the definition of Z and W, we have

$$\begin{aligned}|Z| &= |X \backslash W|\\ &\geq |X| - (|U_{\{1\}}| + |U_{\{2\}}| + ... + |U_{\{w+r\}}|)\\ &= n - \sum_{i \in \{1,2,...,w+r\}} |U_{\{i\}}|. \end{aligned} \tag{2.2}$$

Next, we improve our upper bound of $\mathrm{SHF}(w+r; n, m, \{1, w\})$ through the upper bound on $|Z|$ by double counting the elements of the following set K:

$$K = \{(x, S) : x \in \Gamma_S, S \subseteq \{1, 2, ..., w+r\} \text{ of cardinality } 2\}.$$

For any $x \in Z$, let $\mathcal{J}_x$ be defined by

$$\mathcal{J}_x = \{S \subset \{1, 2, ..., w+r\} : |S| = 2 \text{ and } x \notin \Gamma_S\}.$$

Once x is fixed, there are $\binom{w+r}{2} - |\mathcal{J}_x|$ choices for S such that $(x, S) \in K$.

$\mathcal{J}_x$ is r-colliding since if there exist pairwise disjoint subsets $S_1, S_2, ..., S_r \in \mathcal{J}_x$, then $x \notin \Gamma_{S_1} \cup \Gamma_{S_2} \cup ... \cup \Gamma_{S_r}$. This implies $x \notin Z$ by (2.1), contradicts our choice of x. Hence, $\mathcal{J}_x$ is r-colliding. Therefore, by Theorem 2.3,

$$|\mathcal{J}_x| \leq \binom{w+r}{2} \frac{2(r-1)}{w+r}. \tag{2.3}$$

Therefore,

$$
\begin{aligned}
|K| &= \sum_{x\in Z}\left(\binom{w+r}{2} - |\mathcal{J}_x|\right)\\
&\geq \sum_{x\in Z}\left(\binom{w+r}{2} - \binom{w+r}{2}\frac{2(r-1)}{w+r}\right) \text{ by (2.3)}\\
&= |Z|\left(\binom{w+r}{2} - \binom{w+r}{2}\frac{2(r-1)}{w+r}\right)\\
&\geq \left(n - \sum_{i\in\{1,2,\ldots,w+r\}}|U_{\{i\}}|\right)\left(\binom{w+r}{2} - \binom{w+r}{2}\frac{2(r-1)}{w+r}\right) \text{ by (2.2)}\\
&= \frac{\binom{w+r}{2}}{\gamma}\left(n - \sum_{i\in\{1,2,\ldots,w+r\}}|U_{\{i\}}|\right).
\end{aligned}
$$

Hence, we have

$$
|K| \geq \frac{\binom{w+r}{2}}{\gamma}\left(n - \sum_{i\in\{1,2,\ldots,w+r\}}|U_{\{i\}}|\right). \tag{2.4}
$$

On the other hand, for any fixed S, there are $|\Gamma_S|$ choices for x such that $(x, S) \in K$. Let $S = \{i, j\}$, we have

$$
\begin{aligned}
\Gamma_S &= U_S \cap Z\\
&= U_S \backslash W\\
&\subseteq U_S \backslash (U_{\{i\}} \cup U_{\{j\}}).
\end{aligned}
$$

Hence, for any x in Γ_S, x is unique under S, but non-unique under $\{i\}$ and $\{j\}$. The combination of functions f_i and f_j can give up to m^2 different images $(f_i(x), f_j(x))$ for element $x \in X$. However, each unique symbol a of $f_i(x)$ and each unique symbol b of $f_j(x)$ rules out m different images $(f_i(x), f_j(x))$ from elements of Γ_S. The image (a, b) is counted twice. Hence there are at most

$$
m^2 - m(|U_{\{i\}}| + |U_{\{j\}}|) + |U_{\{i\}}||U_{\{j\}}|
$$

different images $(f_i(x), f_j(x))$ for element $x \in \Gamma_S$.

Now, we have

$$\begin{aligned}
|K| &= \sum_{\substack{S\subseteq\{1,2,\ldots,w+r\},\\ |S|=2}} |\Gamma_S| \\
&\leq \sum_{\substack{S\subseteq\{1,2,\ldots,w+r\}\\ |S|=2}} (m^2 - m(|U_{\{i\}}| + |U_{\{j\}}|) + |U_{\{i\}}||U_{\{j\}}|) \\
&= \frac{1}{2}\sum_{\substack{i,j\in\{1,2,\ldots,w+r\}\\ i\neq j}} (m^2 - m(|U_{\{i\}}| + |U_{\{j\}}|) + |U_{\{i\}}||U_{\{j\}}|) \\
&= \binom{w+r}{2}m^2 - (w+r-1)m \sum_{i\in\{1,2,\ldots,w+r\}} |U_{\{i\}}| + \frac{1}{2}\sum_{\substack{i,j\in\{1,2,\ldots,w+r\}\\ i\neq j}} |U_{\{i\}}||U_{\{j\}}|.
\end{aligned}$$

So,

$$|K| \leq \binom{w+r}{2}m^2 - (w+r-1)m \sum_{i\in\{1,2,\ldots,w+r\}} |U_{\{i\}}| + \frac{1}{2}\sum_{\substack{i,j\in\{1,2,\ldots,w+r\}\\ i\neq j}} |U_{\{i\}}||U_{\{j\}}|. \tag{2.5}$$

From (2.4) and (2.5), we have

$$\begin{aligned}
&\frac{\binom{w+r}{2}}{\gamma}\left(n - \sum_{i\in\{1,2,\ldots,w+r\}} |U_{\{i\}}|\right) \\
&\quad \leq \binom{w+r}{2}m^2 - (w+r-1)m \sum_{i\in\{1,2,\ldots,w+r\}} |U_{\{i\}}| + \frac{1}{2}\sum_{\substack{i,j\in\{1,2,\ldots,w+r\}\\ i\neq j}} |U_{\{i\}}||U_{\{j\}}|.
\end{aligned}$$

Therefore,

$$n \leq \gamma m^2 - \left(\left(\frac{(w+r-1)\gamma m}{\binom{w+r}{2}} - 1\right)\sum_{i\in\{1,2,\ldots,w+r\}} |U_{\{i\}}| - \frac{\gamma}{2\binom{w+r}{2}}\sum_{\substack{i,j\in\{1,2,\ldots,w+r\}\\ i\neq j}} |U_{\{i\}}||U_{\{j\}}|\right).$$

If we can show that

$$\left(\frac{(w+r-1)\gamma m}{\binom{w+r}{2}} - 1\right)\sum_{i\in\{1,2,\ldots,w+r\}} |U_{\{i\}}| - \frac{\gamma}{2\binom{w+r}{2}}\sum_{\substack{i,j\in\{1,2,\ldots,w+r\}\\ i\neq j}} |U_{\{i\}}||U_{\{j\}}| \geq 0,$$

then $n \leq \gamma m^2 - 0 = \gamma m^2$, and the theorem follows.

Consider

$$\left(\frac{(w+r-1)\gamma m}{\binom{w+r}{2}}-1\right)\sum_{i\in\{1,2,\dots,w+r\}}|U_{\{i\}}|-\frac{\gamma}{2\binom{w+r}{2}}\sum_{\substack{i,j\in\{1,2,\dots,w+r\}\\ i\neq j}}|U_{\{i\}}||U_{\{j\}}|$$

$$=\left(\frac{2m}{w-r+2}-1\right)\sum_{i\in\{1,2,\dots,w+r\}}|U_{\{i\}}|$$
$$-\frac{1}{(w-r+2)(w+r-1)}\sum_{\substack{i,j\in\{1,2,\dots,w+r\}\\ i\neq j}}|U_{\{i\}}||U_{\{j\}}|$$
$$\geq\left(\frac{2m}{w-r+2}-1\right)\sum_{i\in\{1,2,\dots,w+r\}}|U_{\{i\}}|$$
$$-\frac{1}{(w-r+2)(w+r-1)}\sum_{\substack{i,j\in\{1,2,\dots,w+r\}\\ i\neq j}}|U_{\{i\}}|m$$
$$=\left(\frac{2m}{w-r+2}-1\right)\sum_{i\in\{1,2,\dots,w+r\}}|U_{\{i\}}|$$
$$-\frac{m}{(w-r+2)}\sum_{i\in\{1,2,\dots,w+r\}}|U_{\{i\}}|$$
$$=\frac{m-w+r-2}{w-r+2}\sum_{i\in\{1,2,\dots,w+r\}}|U_{\{i\}}|$$
$$\geq\frac{(w+1)-w+1-2}{w-r+2}\sum_{i\in\{1,2,\dots,w+r\}}|U_{\{i\}}|$$
$$=0.$$

This completes the proof. □

3 Separating Hash Families Type $\{w_1, w_2\}$

In this section, we state new improved bounds for SHF$(N; n, m, \{w_1, w_2\})$ when $w_1 + w_2 - 1 < N \leq 2w_2$. The bound is as follows:

Theorem 3.1. *Let m, n, N be positive integers greater than 1. Let w_1, w_2 be positive integers such that $1 \leq w_1 \leq w_2$.*

If there exists an SHF$(N; n, m, \{w_1, w_2\})$ *where $w_1 + w_2 \leq N \leq 2w_2$, then*

$$n \leq \gamma m^2,$$

where $\gamma = \frac{N-2(w_1-1)}{2w_2-N+2}$.

We are now stating the next lemma as a key stepping stone to obtaining our result.

Lemma 3.2. *Let m, n be positive integers where $n \geq m^2$, and let w_1, w_2 be positive integers in non-decreasing order such that $w_1+w_2 < m$. If there exists an* $\mathrm{SHF}(N+2s; n, m, \{w_1+s, w_2+s\})$*, then there exists an* $\mathrm{SHF}(N; n, m, \{w_1, w_2\})$.

Proof. We first show that if there exists an $\mathrm{SHF}(N+2; n, m, \{w_1+1, w_2+1\})$, then there exists an $\mathrm{SHF}(N; n, m, \{w_1, w_2\})$. The theorem can be obtained from recursively repeating the result.

Let $\mathcal{F} = \{f_1, f_2, ..., f_{N+2} : X \to Y\}$ be an $\mathrm{SHF}(N+2; n, m, \{w_1+1, w_2+1\})$. Assume for a contradiction that there is no $\mathrm{SHF}(N; n, m, \{w_1, w_2\})$.

Let $\mathcal{F}' = \mathcal{F} \backslash \{f_1, f_2\}$. By our assumption, there is no $\mathrm{SHF}(N; n, m, \{w_1, w_2\})$. Hence there exist two disjoint subsets C_1, C_2 of X that $|C_1| \leq w_1$, $|C_2| \leq w_2$ and none of the functions $f \in \mathcal{F}'$ can separate C_1 and C_2.

Claim. If there is no $\mathrm{SHF}(N; n, m, \{w_1, w_2\})$, then there exist two distinct elements $x \in X \backslash C_1$ and $y \in X \backslash (C_2 \cup \{x\})$, such that $C_1' = C_1 \cup \{x\}$ and $C_2' = C_2 \cup \{y\}$ cannot be separated by f_1 and f_2.

Once the claim is justified, we can observe that $|C_1'| \leq w_1+1$, $|C_2'| \leq w_2+1$ and none of the functions $f \in \mathcal{F}$ can separate C_1' and C_2', which contradicts the $\mathrm{SHF}(N+2; n, m, \{w_1+1, w_2+1\})$ of $\mathcal{F}$. Hence, there exists an $\mathrm{SHF}(N; n, m, \{w_1, w_2\})$ and the theorem follows.

If both of the two statements below are true, our claim follows.

1. There exists an element $x \in X \backslash C_1$ such that $f_1(x) \in f_1(C_2)$. So f_1 cannot separate $C_1 \cup \{x\}$ and C_2.
2. There exists an element $y \in X \backslash (C_1 \cup \{x\})$ such that $f_2(y) \in f_2(C_1)$. So f_2 cannot separate C_1 and $C_2 \cup \{y\}$.

If the first statement is not true, any symbol in $f_1(C_2)$ is not the image of an element outside C_1 and C_2 under f_1. Therefore, under f_1 there are at most $m-1$ symbols left for elements in $X \backslash (C_1 \cup C_2)$ and at most

$$\min\{m(m-1), |X \backslash (C_1 \cup C_2)|\}$$

distinct ordered pairs $(f_1(c), f_2(c))$ for an element c in $X \backslash (C_1 \cup C_2)$.
Since $\left\lceil \frac{|X \backslash (C_1 \cup C_2)|}{m(m-1)} \right\rceil = \left\lceil \frac{n-|C_1|-|C_2|}{m(m-1)} \right\rceil \geq \left\lceil \frac{n-(w_1+w_2)}{m^2-m} \right\rceil \geq \left\lceil \frac{n-(m-1)}{m^2-m} \right\rceil \geq \left\lceil \frac{m^2-m+1}{m^2-m} \right\rceil \geq 2$, by the pigeonhole principle, there are at least 2 elements x and y in $X \backslash (C_1 \cup C_2)$ such that $(f_1(x), f_2(x)) = (f_1(y), f_2(y))$.

Let $C_1' = C_1 \cup \{x\}$ and $C_2' = C_2 \cup \{y\}$, then C_1' and C_2' cannot be separated by f_1 and f_2. Thus, the claim holds when statement 1 is false. Similarly, the claim holds when statement 2 is false. Therefore, there exists an $\mathrm{SHF}(N; n, m, \{w_1, w_2\})$. With a little help of an inductive step on s, we obtain the theorem. □

Proof of Theorem 3.1. Let $\mathcal{F}$ be an SHF$(N; n, m, \{w_1, w_2\})$ where $w_1 + w_2 \leq N \leq 2w_2$. By substituting s in Lemma 3.2 with $w_1 - 1$, there exists an SHF$(N'; n, m, \{1, w\})$ where $N' = N - 2(w_1 - 1)$ and $w = w_2 - (w_1 - 1)$.

Let $r = N' - w = N - (w_1 + w_2 - 1)$. So we have $0 < r \leq w$. Therefore,

$$n \leq \gamma m^2,$$

where $\gamma = \dfrac{w + r}{w - r + 2} = \dfrac{N'}{N' - 2r + 2} = \dfrac{N - 2(w_1 - 1)}{2w_2 - N + 2}$. □

When $w_1 = 1$, the Theorem 3.1 gives the same bound as in Theorem 2.6. Hence Theorem 3.1 is the generalised version of Theorem 2.6. Since $N \geq w_1 + w_2$, we have $N - 2(w_1 - 1) \geq 2w_2 - N + 2$. Hence $\gamma \geq 1$ and $\gamma = 1$ only when $N = w_1 + w_2$. Moreover, $\gamma \leq w_1 + w_2 - 1$ and it reaches equality only when $w_1 = 1$ and $N = 2(w_1 + w_2 - 1) = 2w_2$. Theorem 1.3 gives $n \leq (w_1 + w_2 - 1)m^2$. Hence, our leading term is better than any previously known bounds.

4 Discussion

The bounds in Theorems 2.6 and 3.1 improve the bounds for separating hash families type $\{w_1, w_2\}$ of length $N \leq 2w_2$. The improved bounds are tight in the case of SHF$(N; n, m, \{1, w\})$, both when $N = 1 \bmod w$ and $N = w + 2$. Moreover, when $w_1 + w_2 \leq N \leq 2w_2$ we reduce the leading term γ from $w_1 + w_2 - 1$ to $\frac{N-2(w_1-1)}{2w_2-N+2}$.

Acknowledgement : This work was supported by Chiang Mai University, Chiang Mai, Thailand.

References

[1] S.R. Blackburn, T. Etzion, D.R. Stinson, G.M. Zaverucha, A bound on the size of separating hash families, J. Combin. Theory Ser. A 115 (2008) 1246–1256.

[2] M. Bazrafshan, T. van Trung, Bounds for separating hash families, J. Combin. Theory Ser. A 118 (2011) 1129–1135.

[3] S.R. Blackburn, Frameproof codes, SIAM J. Discrete Math. 16 (2003) 499–510.

[4] T. van Trung, A tight bound for frameproof codes viewed in terms of separating hash families, Des. Codes Cryptography 72 (3) (2014) 713–718.

[5] Y.M. Chee, X. Zhang, Improved constructions of frameproof codes, IEEE Transactions on Information Theory, 58 (2012) 5449–5453.

(Received 18 June 2019)
(Accepted 24 December 2019)

Thai J. Math. Online @ http://thaijmath.in.cmu.ac.th