AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **67(2)** (2017), Pages 294–303

A tight bound on the size of certain separating hash families

Chuan Guo* Douglas R. Stinson †

David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, N2L 3G1
Canada

Abstract

In this paper, we present a new lower bound on the size of separating hash families of type $\{w_1^{q-1}, w_2\}$ where $w_1 < w_2$. Our result extends the paper by Guo, Stinson and Tran on binary frameproof codes [*Des. Codes Crypto.* 77 (2015), 301–319]. This bound compares well against known general bounds, and is especially useful when trying to bound the size of strong separating hash families. We also show that our new bound is tight by constructing hash families that meet the new bound with equality.

1 Introduction

Let X, Y be finite sets of size n and q, respectively. Let $\mathcal{F}$ be a family of functions from X to Y with $|\mathcal{F}| = N$. Given positive integers $w_1, w_2, \ldots, w_t$, we say that $\mathcal{F}$ is a $\{w_1, w_2, \ldots, w_t\}$-*separating hash family*, denoted $\mathsf{SHF}(N; n, q, \{w_1, w_2, \ldots, w_t\})$, if for every choice of subsets $X_1, X_2, \ldots, X_t \subseteq X$ with $|X_i| = w_i$ for $i = 1, \ldots, t$ and $X_i \cap X_j = \emptyset$ for $i \neq j$, there exists some $f \in \mathcal{F}$ such that $f(X_i) \cap f(X_j) = \emptyset$ for $i \neq j$. Such f is said to *separate* the sets $X_1, \ldots, X_t$. The parameter multiset $\{w_1, w_2, \ldots, w_t\}$ is called the *type* of the SHF.

The notion of separating hash families was introduced by Stinson et al. in [9]. It is a generalization of many other combinatorial structures such as perfect hash families [6], frameproof codes [4], and secure frameproof codes [8]. We would like to study bounds on the size of separating hash families when given the other parameters.

It is often useful to represent separating hash families in matrix form. When given an $\mathsf{SHF}(N; n, q, \{w_1, w_2, \ldots, w_t\})$, construct an $N \times n$ q-ary matrix A with $A(i, j) = f_i(x_j)$ where $f_1, \ldots, f_N$ is some fixed ordering of the functions in $\mathcal{F}$ and

* C. Guo's research is supported by NSERC CGS-M scholarship.
† D. Stinson's research is supported by NSERC discovery grant 203114-11.

$x_1, \ldots, x_n$ is some fixed ordering of the elements of X. This matrix is called the *representation matrix* of $\mathcal{F}$. Specializing our definition of an SHF to this form, the equivalent property for when a matrix is the representation matrix of an SHF is as follows.

Theorem 1.1. *An $N \times n$ q-ary matrix A is the representation matrix of an* $\mathsf{SHF}(N; n, q, \{w_1, w_2, \ldots, w_t\})$ *if and only if, for every choice of t column sets $C_1, \ldots, C_t$ in A where $C_i \cap C_j = \emptyset$ for $i \neq j$ and $|C_i| = w_i$ for $i = 1, \ldots, t$, there exists a row r such that $A(r, c_i) \neq A(r, c_j)$ whenever $c_i \in C_i$ and $c_j \in C_j$ where $i \neq j$.*

A list of t column sets $(C_1, \ldots, C_t)$, as specified in Theorem 1.1, will be termed a *column set t-tuple.*

We will only consider SHFs with $\sum_i w_i \leq n$ and $q \geq t$ in order to avoid vacuous cases. The following properties regarding SHFs with different parameter sets $\{w_1, \ldots, w_t\}$ are easy to prove.

Theorem 1.2. *Let $\mathcal{F}$ be an* $\mathsf{SHF}(N; n, q, \{w_1, w_2, \ldots, w_t\})$ *with $\sum_i w_i \leq n$ and $q \geq t$.*

(i) If $w'_1 \leq w_1$ then $\mathcal{F}$ is also an $\mathsf{SHF}(N; n, q, \{w'_1, w_2, \ldots, w_t\})$.

(ii) If $w'_1 = w_1 + w_2$ then $\mathcal{F}$ is also an $\mathsf{SHF}(N; n, q, \{w'_1, w_3, \ldots, w_t\})$.

We now present some known results on general separating hash families.

Theorem 1.3 ([3])**.** *If there exists an* $\mathsf{SHF}(N; n, q, \{w_1, \ldots, w_t\})$ *with $w_1, w_2 \leq w_i$ for $i = 3, \ldots, t$, then*

$$n \leq \gamma q^{\lceil \frac{N}{u-1} \rceil},$$

where $u = \sum_i w_i$ and $\gamma = (w_1 w_2 + u - w_1 - w_2)$.

Theorem 1.4 ([1])**.** *If there exists an* $\mathsf{SHF}(N; n, q, \{w_1, \ldots, w_t\})$, *then*

$$n \leq (u-1) q^{\lceil \frac{N}{u-1} \rceil},$$

where $u = \sum_i w_i$.

Theorem 1.5 ([2])**.** *If there exists an* $\mathsf{SHF}(N; n, q, \{w_1, \ldots, w_t\})$ *with $t \geq 3$ and $u = \sum_i w_i \geq 4$, then*

$$n \leq (u-1) q^{\lceil \frac{N}{u-1} \rceil} + 2 - 2\sqrt{3 q^{\lceil \frac{N}{u-1} \rceil} + 1}.$$

In the remainder of this paper, we will present a construction and a new bound on the size of an SHF of the type $\{w_1^{q-1}, w_2\}$, where w_1^{q-1} denotes the multiset consisting of $q-1$ copies of w_1 and $w_1 < w_2$. Using Theorem 1.2, one can extend this result to bounds for more general types of SHF, such as strong separating hash families [7].

2 A construction for SHF of type $\{w_1^{q-1}, w_2\}$

We first give a construction for SHF of type $\{w_1^{q-1}, w_2\}$.

Construction 2.1. *Fix positive integers n, q, w_1, w_2 with $w_2 + (q-1)w_1 \leq n$. Let $\mathcal{S} =$*

$$\{(C_1, \ldots, C_{q-1}) : C_i \subseteq \{1, \ldots, n\} \text{ with } |C_i| = w_1 \text{ for all } i \text{ and } C_i \cap C_j = \emptyset \text{ if } i \neq j\},$$

and let $\mathcal{T} =$

$$\{(C_1, \ldots, C_{q-1}) \in \mathcal{S} : c_1 < c_2 < \ldots < c_{q-1} \text{ where } c_i \text{ is the smallest element of } C_i\}.$$

Now for $(C_1, \ldots, C_{q-1}) \in \mathcal{T}$, let $r_{(C_1,\ldots,C_{q-1})}$ be the vector

$$r_{(C_1,\ldots,C_{q-1})}(i) = \begin{cases} j & \text{if } i \in C_j \\ 0 & \text{otherwise.} \end{cases}$$

Let A be the matrix that contains all rows $r_{(C_1,\ldots,C_{q-1})}$ for every $(C_1, \ldots, C_{q-1}) \in \mathcal{T}$.

Theorem 2.1. *The matrix A from Construction 2.1 is an $\mathsf{SHF}(N; n, q, \{w_1^{q-1}, w_2\})$ where*

$$N = \frac{1}{(q-1)!}\binom{n}{w_1}\binom{n-w_1}{w_1}\cdots\binom{n-(q-2)w_1}{w_1}.$$

Proof. Let $C_0, \ldots, C_{q-1}$ be pairwise disjoint subsets of $\{1, \ldots, n\}$ such that $|C_0| = w_2$ and $|C_i| = w_1$ for $i = 1, \ldots, q-1$. By construction, there exists a unique permutation π over $\{1, \ldots, q-1\}$ such that the $(q-1)$-tuple $(C_{\pi(1)}, \ldots, C_{\pi(q-1)})$ is contained in $\mathcal{T}$. The column set q-tuple is separated by the row $r_{(C_{\pi(1)},\ldots,C_{\pi(q-1)})}$ in A. Thus A is the representation matrix of an SHF of type $\{w_1^{q-1}, w_2\}$.

Clearly A has n columns and $|\mathcal{T}|$ rows. For any $(C_1, \ldots, C_{q-1}) \in \mathcal{T}$, every permutation π over $\{1, \ldots, q-1\}$ gives a unique element $(C_{\pi(1)}, \ldots, C_{\pi(q-1)}) \in \mathcal{S}$. Since there are

$$\binom{n}{w_1}\binom{n-w_1}{w_1}\cdots\binom{n-(q-2)w_1}{w_1}$$

elements in $\mathcal{S}$, we have that

$$|\mathcal{T}| = \frac{1}{(q-1)!}\binom{n}{w_1}\binom{n-w_1}{w_1}\cdots\binom{n-(q-2)w_1}{w_1},$$

as desired. □

3 A bound for the SHF of type $\{w_1^{q-1}, w_2\}$

In this section, for a certain range of values n, we prove a lower bound on N for existence of an $\mathsf{SHF}(N; n, q, \{w_1^{q-1}, w_2\})$. Whenever it is applicable, this lower bound is tight, in view of Theorem 2.1.

Our bound is in fact a generalization of Theorem 2.2.3 in [5], which we provide here for reference.

Theorem 3.1 ([5]). *Let w, N be positive integers such that $w \geq 3$ and $w+1 \leq N \leq 2w+1$. Suppose there exists an $\mathsf{SHF}(N; n, 2, \{1, w\})$. Then $n \leq N$.*

We will extend the idea of the proof of Theorem 2.2.3 in [5] by counting the total number of column set q-tuples separated in an SHF versus the number of column set q-tuples separated by a single row in the SHF. We can then give a lower bound on the number of rows required by dividing these two quantities. The following definition will be used throughout this section.

Definition 3.1. *Let $x \in Q^n$ where $Q = \{0, 1, \ldots, q-1\}$. We say that x is of* weight *$(i_1, i_2, \ldots, i_{q-1})$ if the number of entries equal to k in x is exactly i_k, for each $k = 1, \ldots, q-1$. The number of entries equal to 0 is thus $i_0 = n - \sum_{k=1}^{q-1} i_k$.*

The next definition gives a simplified notation for counting the number of column set q-tuples separated by a row of weight $(i_1, i_2, \ldots, i_{q-1})$. The correctness of this fact will be proven in Lemma 3.2.

Definition 3.2. *Let w_1, w_2 be positive integers with $w_1 < w_2$. For integers $i_0, i_1, \ldots, i_{q-1}$ with $i_0 \geq w_2$, $i_k \geq w_1$ for $k = 1, \ldots, q-1$ and $n \geq \sum_{k=0}^{q-1} i_k$, define*

$$T^{(q-1)}_{w_1,w_2,n}(i_1, \ldots, i_{q-1}) = \binom{i_1}{w_1}\binom{i_2}{w_1}\cdots\binom{i_{q-1}}{w_1}\binom{n - \sum_{k=1}^{q-1} i_k}{w_2}.$$

Lemma 3.2. *Let w_1, w_2 be positive integers with $w_1 < w_2$. For integers $i_0, i_1, \ldots, i_{q-1}$ with $i_0 \geq w_2$, $w_1 \leq i_k < w_2$ for $k = 1, \ldots, q-1$ and $n \geq \sum_{k=0}^{q-1} i_k$, the number of column set q-tuples separated by a row of weight $(i_1, \ldots, i_{q-1})$ is*

$$Z = (q-1)!\, T^{(q-1)}_{w_1,w_2,n}(i_1, \ldots, i_{q-1}).$$

Proof. Since $w_1 \leq i_k < w_2$ for $k = 1, \ldots, q-1$, it is clear that a row r of weight $(i_1, \ldots, i_{q-1})$ only separates column set q-tuples of the form $(C_0, \ldots, C_{q-1})$ with $|C_k| = w_1$ for $k = 1, \ldots, q-1$ and $|C_0| = w_2$. The columns in C_0 correspond to entries in r that are equal to 0. The columns in C_k for $k = 1, \ldots, q-1$ correspond to distinct entries in r that are equal to $1, \ldots, q-1$. There are $(q-1)!$ permutations of the set $\{1, \ldots, q-1\}$, thus the total number of columns set q-tuples separated by r is

$$\begin{aligned} Z &= (q-1)!\binom{i_0}{w_2}\binom{i_1}{w_1}\binom{i_2}{w_1}\cdots\binom{i_{q-1}}{w_1} \\ &= (q-1)!\, T^{(q-1)}_{w_1,w_2,n}(i_1, \ldots, i_{q-1}). \end{aligned}$$

□

Using Lemma 3.2, we would like to determine the maximum number of column set q-tuples separated by a row of weight $(i_1, \ldots, i_{q-1})$. The following lemma shows that this maximum is achieved when $i_1 = \cdots = i_{q-1} = w_1$.

Lemma 3.3. *Let w_1, w_2 be positive integers such that $w_1 < w_2$, and let q, n be positive integers with $q \geq 2$ and*

$$w_2 + (q-1)w_1 \leq n \leq w_2 + (q-1)w_1 + \frac{w_2}{w_1} - 1.$$

Then for every $k = 1, \ldots, q-1$, we have

$$T^{(q-1)}_{w_1,w_2,n}(i_1, \ldots, i_{q-1}) > T^{(q-1)}_{w_1,w_2,n}(i_1, \ldots, i_{k-1}, i_k + 1, i_{k+1}, \ldots, i_{q-1}).$$

In particular, $T^{(q-1)}_{w_1,w_2,n}$ obtains its global maximum at $(w_1, \ldots, w_1)$ over the domain of integers $(i_1, \ldots, i_{q-1})$ for which $T^{(q-1)}_{w_1,w_2,n}$ is defined.

Proof.

$$\begin{aligned}
&T^{(q-1)}_{w_1,w_2,n}(i_1, \ldots, i_{q-1}) > T^{(q-1)}_{w_1,w_2,n}(i_1, \ldots, i_{k-1}, i_k + 1, i_{k+1}, \ldots, i_{q-1}) \\
\Leftrightarrow\ &\binom{i_k}{w_1}\binom{n - \sum_{l=1}^{q-1} i_l}{w_2} > \binom{i_k + 1}{w_1}\binom{n - \sum_{l=1}^{q-1} i_l - 1}{w_2} \\
\Leftrightarrow\ &\frac{i_k - w_1 + 1}{i_k + 1} > \frac{n - \sum_{l=1}^{q-1} i_l - w_2}{n - \sum_{l=1}^{q-1} i_l}.
\end{aligned}$$

Letting $I = \sum_{l=1}^{q-1} i_l$ and rearranging the inequality gives

$$\begin{aligned}
&(i_k + 1 - w_1)(n - I) > (n - I - w_2)(i_k + 1) \\
\Leftrightarrow\ &-w_1(n - I) > -w_2(i_k + 1) \\
\Leftrightarrow\ &n\frac{w_1}{w_2} < i_k + 1 + \frac{w_1}{w_2}I \\
\Leftrightarrow\ &n < i_k\frac{w_2}{w_1} + I + \frac{w_2}{w_1}
\end{aligned}$$

where the last inequality holds by the assumption $n < w_2 + (q-1)w_1 + \frac{w_2}{w_1}$ since $w_1 \leq i_k$ and $(q-1)w_1 \leq I$. ∎

Before we prove the main theorem, we need a final lemma that corresponds to a special case.

Lemma 3.4. *Let q, w be positive integers with $q \geq 3$ and $w \geq 2$. Let $n = 2w + q - 2$. Then*

$$(q-1)!\, T^{(q-1)}_{1,w,n}(1, \ldots, 1) > 2(q-2)!\, T^{(q-1)}_{1,w,n}(1, \ldots, 1, w).$$

Proof. Expanding the desired inequality gives

$$\begin{aligned}
&(q-1)!\binom{1}{1}^{q-1}\binom{n-q+1}{w} > 2(q-2)!\binom{1}{1}^{q-2}\binom{w}{1}\binom{w}{w} \\
\Leftrightarrow\ &(q-1)\binom{2w-1}{w} > 2w.
\end{aligned}$$

One can check that $\binom{2w-1}{w} > w$ for $w \geq 2$, and the proof follows since $q - 1 \geq 2$. ∎

Theorem 3.5. *Let w_1, w_2 be positive integers with $w_1 < w_2$, and let q, n be positive integers with $q \geq 2$ and*

$$w_2 + (q-1)w_1 \leq n \leq w_2 + (q-1)w_1 + \frac{w_2}{w_1} - 1. \tag{3.1}$$

If there exists an $\mathsf{SHF}(N; n, q, \{w_1^{q-1}, w_2\})$ then

$$N \geq \frac{1}{(q-1)!}\binom{n}{w_1}\binom{n-w_1}{w_1}\cdots\binom{n-(q-2)w_1}{w_1}.$$

Proof. Let A be the representation matrix of an $\mathsf{SHF}(N; n, q, \{w_1^{q-1}, w_2\})$. For any row r of A and $k \in \{0, 1, \ldots, q-1\}$, let i_k be the number of occurrences of symbol k in row r. By permuting the alphabet on row r if necessary, we may assume without loss of generality that $i_1 \leq i_2 \leq \ldots \leq i_{q-1} \leq i_0$. Furthermore, we may assume that $i_1 \geq w_1$ and $i_0 \geq w_2$, since otherwise r cannot separate any column set q-tuple $(C_0, C_1, \ldots, C_{q-1})$ with $|C_k| = w_1$ for $1 \leq k \leq q-1$ and $|C_0| = w_2$ and we may remove r from the matrix. Observe that

$$\begin{aligned} i_{q-1} &= n - i_0 - \sum_{k=1}^{q-2} i_k \\ &\leq n - w_2 - (q-2)w_1 \\ &\leq w_1 + \frac{w_2}{w_1} - 1 && \text{from (3.1)} \\ &\leq w_1 + (w_2 - w_1) \\ &= w_2. \end{aligned}$$

We consider the following two cases.

(i) $i_{q-1} = w_2$. The above inequalities must all be equalities, so we have $w_1 = 1$, $i_k = 1$ for $k = 1, \ldots, q-2$, $i_0 = w_2$ and

$$n = w_2 + (q-1)w_1 + \frac{w_2}{w_1} - 1 = 2w_2 + q - 2.$$

Let $w = w_2$. We only need to consider the case $q \geq 3$ since $q = 2$ is covered by Theorem 3.1. The number of column set q-tuples separated by r is exactly $2(q-2)!\ T^{(q-1)}_{1,w,n}(1, \ldots, 1, w)$, which is less than the number of column set q-tuples separated by a row of weight $(w_1, \ldots, w_1) = (1, \ldots, 1)$ by Lemma 3.2 and Lemma 3.4.

(ii) $i_{q-1} < w_2$: By Lemma 3.2, the number of column set q-tuples separated by r is

$$Z = (q-1)!\ T^{(q-1)}_{w_1,w_2,n}(i_1, \ldots, i_{q-1}).$$

The number of column set q-tuples separated by a row of weight $(w_1, \ldots, w_1)$ is greater than Z by Lemma 3.3 unless $i_k = w_1$ for $k = 1, \ldots, q-1$.

In either case, the number of column set q-tuples separated by r is maximized only when the row is of weight $(w_1, \ldots, w_1)$. The total number of column set q-tuples that need to be separated is

$$T = \binom{n}{w_1}\binom{n-w_1}{w_1}\cdots\binom{n-(q-2)w_1}{w_1}\binom{n-(q-1)w_1}{w_2}.$$

Thus

$$\begin{aligned} N &\geq \frac{T}{(q-1)!\, T^{(q-1)}_{w_1,w_2,n}(w_1,\ldots,w_1)} \\ &= \frac{1}{(q-1)!}\binom{n}{w_1}\binom{n-w_1}{w_1}\cdots\binom{n-(q-2)w_1}{w_1}. \end{aligned}$$

□

The following result is an immediate consequence of Theorems 2.1 and 3.5.

Corollary 3.6. *Let w_1, w_2 be positive integers with $w_1 < w_2$, and let q, n be positive integers with $q \geq 2$ and*

$$w_2 + (q-1)w_1 \leq n \leq w_2 + (q-1)w_1 + \frac{w_2}{w_1} - 1.$$

Then the minimum value of N such that there exists an $\mathsf{SHF}(N; n, q, \{w_1^{q-1}, w_2\})$ is

$$N = \frac{1}{(q-1)!}\binom{n}{w_1}\binom{n-w_1}{w_1}\cdots\binom{n-(q-2)w_1}{w_1}.$$

4 Applications

Theorem 3.5 is particularly useful for studying the combinatorial objects known as strong separating hash families (denoted SSHF), introduced by Sarkar and Stinson in [7]. They are equivalent to an SHF of type $\{1^{t_1}, t_2\}$ for some positive integers t_1, t_2. We can give a strong bound for the code length of SSHFs as a corollary.

Corollary 4.1. *Let n, t_1, t_2 be positive integers with $t_1 \geq q-1$ and $t_1 + t_2 \leq n \leq 2(t_1+t_2) - q$. Suppose there exists an $\mathsf{SHF}(N; n, q, \{1^{t_1}, t_2\})$. Then*

$$N \geq \binom{n}{q-1}.$$

Proof. By Theorem 1.2, an $\mathsf{SHF}(N; n, q, \{1^{t_1}, t_2\})$ is also an $\mathsf{SHF}(N; n, q, \{1^{q-1}, t_1 + t_2 - q + 1\})$. Applying Theorem 3.5, if $t_1 + t_2 \leq n \leq 2(t_1 + t_2) - q$, then we have

$$N \geq \frac{1}{(q-1)!} n(n-1)\ldots,(n-q+2),$$

as desired. □

Example 4.1. *Let $q = 3$, $t_1 = 4$ and $t_2 = 3$. Suppose there exists an* $\mathsf{SHF}(N; 11, 3, \{1, 1, 1, 1, 3\})$ *(Corollary 4.1 applies to $n = 7, 8, 9, 10$ as well). Then $N \geq \binom{11}{2} = 55$. In other words, for $N \leq 54$, we have that $n \leq 10$.*

Compare this with known results: Theorem 1.3 and Theorem 1.4 both give the bound $n \leq 6(3^9) = 118098$ for $N = 54$; Theorem 1.5 gives the bound

$$n \leq 6(3^9) + 2 - 2\sqrt{3(3^9) + 1} < 118023$$

for $N = 54$.

Finally, Table 1 (overleaf) lists various parameter choices for q, w_1, w_2 and compares the bound in Theorem 3.5 to some known bounds for general SHFs. The symbol Ω means the computed bound is above the Java `double` maximum value of $(2 - 2^{-52})2^{1023}$.

5 Conclusion

We have presented a new bound in Theorem 3.5 for SHF of type $\{w_1^{q-1}, w_2\}$. As an application, we derived a bound in Corollary 4.1 for SSHFs that compares well against known general bounds. One can also choose other types of SHFs and apply Theorem 3.5 to obtain competitive bounds, since Table 4 demonstrates a large gap between our result and best known general bounds.

There is an inherent difficulty of generalizing Theorem 3.5 to other types. For example, if we relax the type of the SHF to $\{w_1^{q-2}, w_2, w_3\}$ where $w_1 < w_2 < w_3$, then a row of weight $(w_1, \ldots, w_1, w_2, w_2)$ could separate the column set consisting of w_2 columns in multiple ways. This difficulty is even more prevalent when the type set $\{w_1, \ldots, w_t\}$ consists of a large number of different values. It would be interesting to develop a counting method that can overcome this difficulty. Another extension of our result could be in the direction of allowing the type multiset $\{w_1, \ldots, w_t\}$ to contain more elements than q, i.e., $t > q$. Making progress in either direction would allow us to derive more powerful bounds for general SHFs.

q	w_1	w_2	$N \leq$	implies $n \leq$			
				Theorem 3.5	Theorem 1.3	Theorem 1.4	Theorem 1.5
3	1	2	9	4	243	243	213
3	1	3	20	6	2916	2916	2824
3	1	4	35	8	32805	32805	32526
3	1	5	54	10	354294	354294	353454
3	1	6	77	12	3720087	3720087	3717563
3	2	3	104	6	3.09×10^{9}	2.32×10^{9}	2.32×10^{9}
3	2	4	377	8	5.81×10^{26}	4.07×10^{26}	4.07×10^{26}
3	2	5	629	9	5.91×10^{38}	3.94×10^{38}	3.94×10^{38}
3	2	6	1484	11	7.43×10^{79}	4.77×10^{79}	4.77×10^{79}
3	3	4	2099	9	6.64×10^{112}	3.98×10^{112}	3.98×10^{112}
3	3	5	4619	10	4.84×10^{221}	2.69×10^{221}	2.69×10^{221}
3	3	6	17159	12	Ω	Ω	Ω
4	1	2	19	5	4096	4096	3987
4	1	3	54	7	2.09×10^{7}	2.09×10^{7}	2.09×10^{7}
4	1	4	118	9	6.59×10^{12}	6.59×10^{12}	6.59×10^{12}
4	1	5	219	11	1.29×10^{20}	1.29×10^{20}	1.29×10^{20}
4	1	6	362	13	3.96×10^{28}	3.96×10^{28}	3.96×10^{28}
4	2	3	1259	8	1.33×10^{96}	1.06×10^{96}	1.06×10^{96}
4	2	4	6929	10	Ω	Ω	Ω
4	2	5	13859	11	Ω	Ω	Ω
4	2	6	45044	13	Ω	Ω	Ω
4	3	4	200199	12	Ω	Ω	Ω
4	3	5	560559	13	Ω	Ω	Ω
4	3	6	3203199	15	Ω	Ω	Ω
5	1	2	33	6	390625	390625	389658
5	1	3	125	8	2.86×10^{15}	2.86×10^{15}	2.86×10^{15}
5	1	4	329	10	2.48×10^{34}	2.48×10^{34}	2.48×10^{34}
5	1	5	714	12	6.46×10^{63}	6.46×10^{63}	6.46×10^{63}
5	1	6	1364	14	1.57×10^{107}	1.57×10^{107}	1.57×10^{107}
5	2	3	17324	10	Ω	Ω	Ω
5	2	4	135134	12	Ω	Ω	Ω
5	2	5	315314	13	Ω	Ω	Ω
5	2	6	1351349	15	Ω	Ω	Ω
5	3	4	28027999	15	Ω	Ω	Ω
5	3	5	95295198	16	Ω	Ω	Ω
5	3	6	775975199	18	Ω	Ω	Ω

Table 1: Comparison of Bounds for $\mathsf{SHF}(N; n, q, \{w_1^{q-1}, w_2\})$

References

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

[2] M. Bazrafshan and Tran van Trung, Improved bounds for separating hash families, *Des. Codes Crypto.* (2013), 369–382.

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

[4] D. Boneh and J. Shaw, Collusion-free fingerprinting for digital data, *IEEE Trans. Inform. Theory* **44** (1998), 1897–1905.

[5] C. Guo, D. R. Stinson and Tran van Trung, On tight bounds for binary frameproof codes, *Des. Codes Crypto.* 77 (2015), 301–319.

[6] K. Mehlhorn, On the program size of perfect and universal hash functions, *Proc. 23rd Annual Symp. Foundations of Comp. Sci.* (1982), 170–175.

[7] P. Sarkar and D. R. Stinson, Frameproof and IPP codes, Progress in Cryptology — Indocrypt 2001, *Lec. Notes Comp. Sci.*, Springer, **2247** (2001), 117–126.

[8] D. R. Stinson, Tran van Trung and R. Wei, Secure frameproof codes, key distribution patterns, group testing algorithms and related structures, *J. Statist. Plann. Inference* **86** (2000), 595–617.

[9] D. R. Stinson, R. Wei and K. Chen, On generalized separating hash families, *J. Combin. Theory Ser. A* **115** (2008), 105–120.

(Received 19 Sep 2015; revised 12 Jan 2016)