Journal of Combinatorial Theory, Series A 118 (2011) 1129–1135

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Bounds for separating hash families

Marjan Bazrafshan, Tran van Trung

Institut für Experimentelle Mathematik, Universität Duisburg–Essen, Ellernstrasse 29, 45326 Essen, Germany

ARTICLE INFO

Article history:
Received 17 May 2010
Available online 17 November 2010

Keywords:
Separating hash family
Perfect hash family
Frameproof code
w-IPP code

ABSTRACT

This paper aims to present new upper bounds on the size of separating hash families. These bounds improve previously known bounds for separating hash families.

1. Introduction

Let h be a function from a set A to a set B and let $C_1, C_2, \dots, C_t \subseteq A$ be t pairwise disjoint subsets. We say that h *separates* $C_1, C_2, \dots, C_t$ if $h(C_1), h(C_2), \dots, h(C_t)$ are pairwise disjoint. Let $|A| = n$ and $|B| = m$. We call a set $\mathcal{H}$ of N functions from A to B an $(N; n, m)$-*hash family*. We say that $\mathcal{H}$ is *an* $(N; n, m, \{w_1, w_2, \dots, w_t\})$ *separating hash family*, and we shall also write as an SHF$(N; n, m, \{w_1, w_2, \dots, w_t\})$, if for all pairwise disjoint subsets $C_1, C_2, \dots, C_t \subseteq A$ with $|C_i| = w_i$, for $i = 1, 2, \dots, t$, there exists at least one function $h \in \mathcal{H}$ that separates $C_1, C_2, \dots, C_t$. The multiset $\{w_1, w_2, \dots, w_t\}$ is the *type* of the separating hash family. Obviously, we have $2 \leqslant t \leqslant m$ and $\sum_{i=1}^{t} w_i \leqslant n$. Separating hash family with $t = 2$ was introduced in [13] and the general case in [16]. It is worth remarking that various well-known combinatorial objects may be viewed as special cases of separating hash families. For example, if $w_1 = w_2 = \cdots = w_t = 1$, an SHF$(N; n, m, \{1, 1, \dots, 1\})$ is called a *perfect hash family* which is usually denoted by PHF$(N; n, m, t)$. Perfect hash families have been studied extensively, see for instance, [1,3,5,9,10,12,18]. A w-*frameproof code* is a separating hash family of type $\{1, w\}$ [4,6,11] and a w-*secure frameproof code* is a separating hash family of type $\{w, w\}$ [13]. Further, a w-*IPP code* (code with identifiable parent property) [7,11,17], is necessarily a PHF with $t = w + 1$ and an SHF of type $\{w, w\}$.

An SHF$(N; n, m, \{w_1, w_2, \dots, w_t\})$ can be depicted as an $N \times n$ array $\mathcal{A}$ in which the columns are labeled by the elements of A, the rows by the functions $h_i \in \mathcal{H}$ and the (i, j)-entry of the array is the

E-mail addresses: marjan@iem.uni-due.de (M. Bazrafshan), trung@iem.uni-due.de (T. van Trung).

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2010.11.006

value $h_i(j)$. Thus, an $\mathsf{SHF}(N; n, m, \{w_1, w_2, \ldots, w_t\})$ is equivalent to an $N \times n$ array with entries from a set of m symbols such that for all disjoint sets of columns $C_1, C_2, \ldots, C_t$ of $\mathcal{A}$ with $|C_i| = w_i$, for $i = 1, 2, \ldots, t$, there exists at least one row r of $\mathcal{A}$ such that

$$\left\{\mathcal{A}(r, x)\colon\ x \in C_i\right\} \cap \left\{\mathcal{A}(r, y)\colon\ y \in C_j\right\} = \emptyset,$$

for all $i \neq j$. We call $\mathcal{A}$ the *array representation* or *matrix representation* of the hash family.

In general, for given N, m, $\{w_1, w_2, \ldots, w_t\}$ we want to maximize n. The determination of bounds for n has been subject of much research recently [2,8,11,14–16].

The best known upper bounds on n for separating hash families of type $\{w_1, w_2\}$ are the following.

Theorem 1. *(See [5,11].) Suppose there exists an* $\mathsf{SHF}(N; n, m, \{1, w\})$ *with* $w \geqslant 2$*. Then* $n \leqslant w(m^{\lceil \frac{N}{w} \rceil} - 1)$.

Theorem 2. *(See [16].) Suppose there is an* $\mathsf{SHF}(N; n, m, \{2, 2\})$*. Then* $n \leqslant 4m^{\lceil \frac{N}{3} \rceil} - 3$.

For the special case $\{w_1, w_2, w_3\} = \{1, 1, 2\}$ we have the following strong bound.

Theorem 3. *(See [16].) Suppose there is an* $\mathsf{SHF}(N; n, m, \{1, 1, 2\})$*. Then* $n \leqslant 3m^{\lceil \frac{N}{3} \rceil} + 2 - 2\sqrt{3m^{\lceil \frac{N}{3} \rceil} + 1}$.

A general bound for SHF of type $\{w_1, \ldots, w_t\}$ has been obtained by Stinson and Zaverucha in [14]. In [2] Blackburn, Etzion, Stinson and Zaverucha introduce a new method to establish a significant bound for SHF of type $\{w_1, \ldots, w_t\}$, which considerably improves the bound in [14], when $w_i \geqslant 2$ for all $i = 1, \ldots, t$. We record this bound for SHF of type $\{w_1, \ldots, w_t\}$ in the following theorem.

Theorem 4. *(See [2].) Suppose an* $\mathsf{SHF}(N; n, m, \{w_1, \ldots, w_t\})$ *exists. Let* $u = \sum_{i=1}^{t} w_i$*. Then*

$$n \leqslant \gamma m^{\lceil \frac{N}{(u-1)} \rceil},$$

where $\gamma = (w_1 w_2 + u - w_1 - w_2)$*, and* w_1 *and* w_2 *are the smallest two of the integers* w_i*.*

Note that the constant γ in Theorem 4 depends on $w_1, w_2, \ldots, w_t$. If we take $\gamma = \binom{u}{2}$ for the theorem, we obtain a bound derived from the graph theoretical method [2], and if we take $\gamma = 2(u - w_1)w_1 - w_1$, where w_1 is the smallest of the integers w_i, we have the bound in [14].

It should be noted that there exist further bounds for type $\{w_1, w_2\}$ and for general type $\{w_1, w_2, \ldots, w_t\}$ [14,15]. However as those bounds have been improved by the bound of Theorem 4, they are not included here.

To date, Theorem 4 presents the best known bound for SHF of general type $\{w_1, \ldots, w_t\}$.

In this paper we present new strong bounds for SHF which improve the Blackburn–Etzion–Stinson–Zaverucha bound of Theorem 4.

2. Bounds for SHF of type $\{w_1, \ldots, w_t\}$

We aim to prove the following results.

Theorem 5. *Suppose there exists an* $\mathsf{SHF}(N; n, m, \{w_1, w_2\})$*. Let* $u = w_1 + w_2$*. Then*

$$n \leqslant (u-1)m^{\lceil \frac{N}{(u-1)} \rceil}.$$

Theorem 6. *Let* $t \geqslant 3$ *be an integer. Suppose there exists an* $\mathsf{SHF}(N; n, m, \{w_1, w_2, \ldots, w_t\})$*. Let* $u = \sum_{i=1}^{t} w_i$*. Then*

$$n \leqslant (u-1)(m-1)^{\lceil \frac{N}{(u-1)} \rceil} + 1.$$