Discrete Mathematics 341 (2018) 2627–2638

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Constructions and bounds for separating hash families

Xiaolei Niu, Haitao Cao *

Institute of Mathematics, Nanjing Normal University, Nanjing 210023, China

ARTICLE INFO

Article history:
Received 17 September 2017
Received in revised form 25 April 2018
Accepted 11 June 2018

Keywords:
Hash family
Separating hash family
Strong separating hash family
Hypergraph

ABSTRACT

In this paper, we present a new construction for strong separating hash families by using hypergraphs and obtain some optimal separating hash families. We also improve some previously known bounds of separating hash families.

1. Introduction

Let X and Y be two finite sets of sizes n and m respectively. An $(N; n, m)$-*hash family* $\mathcal{F}$ is a family of functions from X to Y with $|\mathcal{F}| = N$. For all pairwise disjoint subsets $C_1, C_2, \ldots, C_t \subseteq X$, if there exists some f such that $f(C_i) \cap f(C_j) = \emptyset$ for all $1 \leq i < j \leq t$. Then $C_1, C_2, \ldots, C_t$ are *separable* in $\mathcal{F}$, and the function f is said to *separate* the sets $C_1, C_2, \ldots, C_t$.

Given positive integers $w_1, w_2, \ldots, w_t$, we say $\mathcal{F}$ is a $\{w_1, w_2, \ldots, w_t\}$-*separating hash family*, denoted by SHF$(N; n, m, \{w_1, w_2, \ldots, w_t\})$, if for all pairwise disjoint subsets $C_1, C_2, \ldots, C_t \subseteq X$ with $|C_i| = w_i$ for $i = 1, 2, \ldots, t$, there exists some $f \in \mathcal{F}$ which separates $C_1, C_2, \ldots, C_t$. The parameter multiset $\{w_1, w_2, \ldots, w_t\}$ is called the *type* of $\mathcal{F}$. For the sake of brevity, we use SHF to denote separating hash family, and we also use $\{w_1^{q_1}, w_2^{q_2}, \ldots, w_t^{q_t}\}$ to denote the multiset in which there are exactly q_i copies of w_i and $w_i < w_j$ for $1 \leq i < j \leq t$. Further, w^1 will be written as w. An SHF$(N; n, m, \{1^q, w\})$ with $w \geq 2$ is also called a *strong separating hash family*.

Separating hash families were first introduced by Stinson, Trung and Wei [24]. It can be used to construct frameproof codes, secure frameproof codes and parent-identifying codes, see [7,20,23,24]. Most results of the known papers on separating hash families are focused on their bounds and constructions, see [1–6,10–14,22,25,26].

Given an SHF$(N; n, m, \{w_1, w_2, \ldots, w_t\})$, we construct an $N \times n$ matrix $A = (a_{i,j})$ having entries on a set of m elements such that $a_{i,j} = f_i(x_j)$ where $f_1, f_2, \ldots, f_N$ are some fixed ordering of the functions in $\mathcal{F}$ and $x_1, \ldots, x_n$ are elements of X. This matrix is called the *representation matrix* of the SHF. For all disjoint sets of columns $C_1, C_2, \ldots, C_t$ of A with $|C_i| = w_i$, $1 \leq i \leq t$, there exists at least one row r of A such that $\{a_{r,x} : x \in C_i\} \cap \{a_{r,y} : y \in C_j\} = \emptyset$ holds for all $1 \leq i < j \leq t$. We say the row r separates the sets $C_1, C_2, \ldots, C_t$. An SHF$(N; n, m, \{w_1, w_2, \ldots, w_t\})$ is called *optimal* if n is maximum for given $N, m, w_1, w_2, \ldots, w_t$ or if N is minimum for given $n, m, w_1, w_2, \ldots, w_t$.

In the literature optimal results for separating hash families are quite rare. In this paper, we present a new construction for strong separating hash families by using hypergraphs and obtain some optimal separating hash families. It is easy to see that a separating hash family with type $\{w_1, w_2, \ldots, w_t\}$ can also be viewed as a separating hash family with type $\{w_1 + w_2 + \cdots + w_s, w_{s+1} + w_{s+2} + \cdots + w_t\}$ for any s, $1 \leq s \leq t - 1$. So an upper bound type $\{w_1, w_2\}$ will induce an upper bound for the general case. Thus it is valuable to study the bound of separating hash families with type $\{w_1, w_2\}$.

* Corresponding author.
E-mail address: caohaitao@njnu.edu.cn (H. Cao).

https://doi.org/10.1016/j.disc.2018.06.018
0012-365X/

This paper is organized as follows. In the next section, we present a new construction for strong separating hash families by using hypergraphs and present some optimal strong separating hash families. In Section 3 we construct an optimal SHF(4; 10, 4, {2, 2}) and use it to improve the known upper bound for an SHF($2w$; n, m, $\{w, w\}$). In Section 4 we improve the known upper bound for an SHF($w_1 + w_2$; n, m, $\{w_1, w_2\}$) and use it to improve the known upper bound for an SHF($\sum_{i=1}^{t} w_i$; n, m, $\{w_1, w_2, \ldots, w_t\}$). Section 5 contains some concluding remarks and comparison of bounds for SHF.

2. A new construction for strong separating hash family

In this section, we will use hypergraphs to present a new construction for strong separating hash families. A *hypergraph* is a pair $H = (V, E)$, where V is a finite set whose elements are called vertices and E is a family of subsets of V, called edges. It is k-uniform if each of its edges contains precisely k vertices.

Construction 2.1. *Let $V = \{x_1, x_2, \ldots, x_n\}$ and $E = \{B_1, B_2, \ldots, B_N\}$, where B_i is an m-subset of V, $1 \le i \le N$. If $G = (V, E)$ is an m-uniform hypergraph with the property that any l vertices are contained in exactly one edge, then there exists an SHF(N; n, $m+1$, $\{1^{w_1}, w_2\}$) for all positive integers w_1 and w_2 satisfying $w_1 \le l$ and $w_1 + w_2 \le n$.*

Proof. Let $B_i = \{y_{i,1}, y_{i,2}, \ldots, y_{i,m}\}$, $1 \le i \le N$. Define an $N \times n$ matrix $A = (a_{i,j})$ by

$$a_{i,j} = \begin{cases} b, & \text{if } x_j = y_{i,b} \\ 0, & \text{otherwise.} \end{cases}$$

Now we prove A is a representation matrix of an SHF(N; n, $m+1$, $\{1^{w_1}, w_2\}$). Let $\mathcal{C} = \{c_1, c_2, \ldots, c_n\}$ denote the column set of A. Let $C_1, C_2, \ldots, C_{w_1}, C_{w_1+1}$ be pairwise disjoint subsets of $\mathcal{C}$ such that $C_i = \{c_{s_i}\}$ for $i = 1, 2, \ldots, w_1$ and $|C_{w_1+1}| = w_2 \le n - w_1$. Then $|C_1 \cup C_2 \cup \cdots \cup C_{w_1}| = w_1 \le l$, $C_{w_1+1} \subset \mathcal{C} \setminus \{c_{s_1}, c_{s_2}, \ldots, c_{s_{w_1}}\}$.

Since $G = (V, E)$ is an m-uniform hypergraph with the property that any l vertices are contained in exactly one edge, we can find an edge $B_t \in E$ such that $\{x_{s_1}, x_{s_2}, \ldots, x_{s_{w_1}}\} \subset B_t$. Let $B_t = \{x_{s_1}, x_{s_2}, \ldots, x_{s_{w_1}}, x_{s_{w_1+1}}, \ldots, x_{s_m}\}$. Then $\{a_{t,s_1}, a_{t,s_2}, \ldots, a_{t,s_m}\} = \{1, 2, \ldots, m\}$ and $a_{t,j} = 0$ for any $j \in \{1, 2, \ldots, n\} \setminus \{s_1, s_2, \ldots, s_m\}$. Thus, $\{a_{t,k} : c_k \in C_i\} \cap \{a_{t,k} : c_k \in C_j\} = \emptyset$ holds for all $1 \le i < j \le w_1 + 1$. Therefore, the tth row of A can separate $C_1, C_2, \ldots, C_{w_1+1}$. □

Example 2.2. Let $V = \mathbb{Z}_7$ and $E = \{\{i, i+1, i+3\} : i \in \mathbb{Z}_7\}$. We can obtain the following representation matrix of an SHF(7; 7, 4, $\{1^2, 5\}$) by Construction 2.1.

1	2	0	3	0	0	0
0	1	2	0	3	0	0
0	0	1	2	0	3	0
0	0	0	1	2	0	3
3	0	0	0	1	2	0
0	3	0	0	0	1	2
2	0	3	0	0	0	1

For our results, we need the following conclusion on m-uniform hypergraphs.

Lemma 2.3 ([15–17])**.** *1. For any $3 \le m \le 5$, there exists an m-uniform hypergraph $G = (V, E)$ with the property that any two vertices are contained in exactly one edge, where $|V| = n$ satisfying $n \equiv 1, m \pmod{m^2 - m}$, and $|E| = \frac{n(n-1)}{m(m-1)}$.*

2. For any $n \equiv 2, 4 \pmod 6$, there exists a 4-uniform hypergraph with n vertices and $\frac{n(n-1)(n-2)}{24}$ edges such that any three vertices are contained in exactly one edge.

3. For any prime power m and integer $l \ge 2$, there exists an $(m+1)$-uniform hypergraph $G = (V, E)$ with the property that any three vertices are contained in exactly one edge, where $|V| = n$ satisfying $n = m^l + 1$, and $|E| = \frac{\binom{n}{3}}{\binom{m+1}{3}}$.

By Construction 2.1 and Lemma 2.3 we have the following theorem.

Theorem 2.4. *1. Let $3 \le m \le 5$, $n \equiv 1, m \pmod{m^2 - m}$, $n > m$, and $N = \frac{n(n-1)}{m(m-1)}$. Then there is an SHF($N$; n, $m+1$, $\{1^2, n-2\}$).*

2. Let $n \equiv 2, 4 \pmod 6$, $n \ge 8$ and $N = \frac{n(n-1)(n-2)}{24}$. Then there is an SHF($N$; n, 5, $\{1^3, n-3\}$).

3. Let $n = m^l + 1$, where m is a prime power and $l \ge 2$. Let $N = \frac{\binom{n}{3}}{\binom{m+1}{3}}$. Then there is an SHF($N$; n, $m+2$, $\{1^3, n-3\}$).

Now we have obtained some new strong separating hash families from Theorem 2.4. We continue to show that these results from Theorem 2.4 are all tight by discussing the lower bound of N for an SHF(N; $w_1 + w_2$, m, $\{1^{w_1}, w_2\}$). When $w_1 + w_2 \le m$, it is easy to see that $N \ge 1$. So this case is trivial and we only need to deal with the case $w_1 + w_2 > m$.

Lemma 2.5. *If there is an SHF(N; $w_1 + w_2$, m, $\{1^{w_1}, w_2\}$) with $w_1 + w_2 > m$, then $N \ge \frac{\binom{w_1+w_2}{w_1}}{\binom{m-1}{w_1}}$.*