Perfect Hash Families with Few Functions

Simon R. Blackburn*
Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX
United Kingdom

May 3, 2000

Abstract

An $(s; n, q, t)$*-perfect hash family* is a set of functions $\phi_1, \phi_2, \ldots, \phi_s$ from a set V of cardinality n to a set F of cardinality q with the property that every t-subset of V is injectively mapped into F by at least one of the functions ϕ_i.

The paper shows that the maximum value $n_{s,t}(q)$ that n can take for fixed s and t has a leading term that is linear in q if and only if $t > s$. Moreover, for any s and t such that $t > s$, the paper shows how to calculate the coefficient of this linear leading term; this coefficient is explicitly calculated in some cases. As part of this process, new classes of good perfect hash families are constructed.

1 Introduction

Let ϕ be a function from a set V to a set F. We say that ϕ *separates* a set $X \subseteq V$ if ϕ is injective when restricted to X.

Let $\phi_1, \phi_2, \ldots, \phi_s : V \to F$. Suppose V has cardinality n and F has cardinality q. Let t be an integer such that $2 \leq t \leq q$. We say that $\phi_1, \phi_2, \ldots, \phi_s$

*The author is an E.P.S.R.C. Advanced Fellow

is an $(s;n,q,t)$-*perfect hash family* if for all $X \subseteq V$ such that $|X| = t$, there exists $i \in \{1, 2, \ldots, s\}$ such that ϕ_i separates X.

Perfect hash families were first used by Mehlhorn [13] to prove a theoretical result in compiler design. They have continued to find new applications — in cryptography (see Blackburn [4], Blackburn, Burmester, Desmedt and Wild [6], Fiat and Naor [9], Safavi-Naini and Wang [15], Staddon, Stinson and Wei [16] and Stinson, van Trung, Wei [17]) in circuit design (see Newman and Wigderson [14]) and to reducing the random input of an algorithm (see Alon and Naor [2]). They have been studied as combinatorial objects by Alon [1], Atici, Magliveras, Stinson and Wei [3], Blackburn [5], Blackburn and Wild [7], Fredman and Komlós [10], Körner and Marton [11], Martirosyan and Martirosyan [12] and Stinson, Wei and Zhu [18].

Perfect hash families may also be regarded as sets of partitions. We say that a partition π of a set V *separates* a subset $X \subseteq V$ if distinct elements of X lie in distinct parts of π. Let $\pi_1, \pi_2, \ldots, \pi_s$ be a sequence of partitions of a set V. We say that $\pi_1, \pi_2, \ldots, \pi_s$ form an $(s;n,q,t)$-*perfect hash family* if $|V| = n$, if each partition π_i has at most q parts and if for all $X \subseteq V$ such that $|X| = t$, there exists $i \in \{1, 2, \ldots, s\}$ such that π_i separates X. The 'partition' and 'function' definitions are equivalent: given a set of partitions, we may construct appropriate functions by labelling the parts of each partition π_i with distinct elements of F, and then defining ϕ_i to map $x \in V$ to the label of the part of π_i containing x. In the reverse direction, we define $x, y \in V$ to be in the same part of π_i if and only if $\phi_i(x) = \phi_i(y)$. We will use the partition representation of a perfect hash family throughout this paper.

When s, q and t are fixed, what is the largest value $n_{s,t}(q)$ of n such that an $(s;n,q,t)$-perfect hash family exists? In particular, we are interested in the case when $t > s$, so there are few partitions when compared to the value of t. This is a natural class of parameters to consider, as there is an upper bound on n that is linear in q if and only if $t > s$, as we shall prove in Section 2. In fact, when $t > s$ the leading term of $n_{s,t}(q)$ is linear in q. We will show how to calculate the coefficient of this leading term. As a byproduct of this process, we construct several new classes of good perfect hash families. These constructions are better than the perfect hash families that are shown to exist by probabilistic methods, and than the explicit constructions from error correcting codes due to Alon [1].

Martirosyan and Martirosyan [12] recently observed that $n \leq q$ whenever

$t \geq 2s$. (This bound is clearly tight: it is met by a 'trivial' perfect hash family with a partition whose parts are all singletons.) They also showed that $n \leq \frac{s}{s-1}(q-1)$ when $t = 2s-1$, and proved by construction that this bound is attained when $\frac{s}{s-1}$ is an integer. The constructions in this paper include the Martirosyan–Martirosyan construction as a special case.

The paper is organised as follows. In Section 2, we construct a class of perfect hash families that are basic building blocks in our constructions, and we show that the parameters we are considering are precisely those where there is an upper bound on n that is linear in q. In Section 3, we provide new constructions for perfect hash families. We introduce a method involving linear programming to prove linear upper bounds on n, and we use the building blocks of Section 2 to show that these bounds are tight. Finally, in Section 4 we simplify the linear programming method and explicitly derive the coefficient of the linear leading term in several special cases.

2 A Linear Upper Bound

We aim to show that the parameters we are considering are precisely those where there is an upper bound on n that is linear in q. We will use the following collection of partitions in our proof — this collection will be used as a basic building block in all the constructions in this paper.

Proposition 1 *Let k and a be positive integers. Let A be a set of cardinality a. Define $V = A^k$. Define partitions $\pi_1, \pi_2, \ldots, \pi_k$ by defining $(a_1, a_2, \ldots, a_k)$ and $(a'_1, a'_2, \ldots, a'_k)$ to lie in the same part of π_i if and only if $a_j = a'_j$ for all $j \in \{1, 2, \ldots, k\} \setminus \{i\}$. Let t be a positive integer and let $X \subseteq V$ be such that $|X| = t$. Then X is separated by at least $k - (t-1)$ of the partitions $\pi_1, \pi_2, \ldots, \pi_k$.*

Proof: Suppose, for a contradiction, that $X \subseteq V$ is such that $|X| = t$, but X fails to be separated by t partitions. Without loss of generality, assume that these partitions are $\pi_1, \pi_2, \ldots, \pi_t$. We define a graph G with coloured edges as follows (we allow G to have multiple edges). The vertex set of G is X. For each $i \in \{1, 2, \ldots, t\}$, we choose one pair of distinct vertices $x, y \in X$ that lie in the same part of π_i and add an edge of colour i between x and y. Note that an edge of colour i between $x, y \in V$ implies that x and y differ in their ith position and no other. Now, G has t vertices and t edges, and so G

contains a cycle $x_1, x_2, \ldots, x_c$, where $x_1 = x_c$. Let the edge between x_1 and x_2 be coloured j. Then x_1 and x_2 differ in position j. Moreover, since each colour occurs once in the graph, for all $i \in \{2, 3, \ldots, c-1\}$ we have that x_i and x_{i+1} agree in their jth position. But this implies that the jth position of x_1 differs from the jth position of x_c. Since $x_1 = x_c$, we have our required contradiction.$\Box$

Corollary 1 *The partitions $\pi_1, \pi_2, \ldots, \pi_k$ defined in Proposition 1 form a $(k; a^k, a^{k-1}, k)$-perfect hash family.*

Proof: Clearly, each partition π_i has a^{k-1} parts. Moreover, by Proposition 1, every subset X of V is size k is separated by at least $k-(k-1)$ of the partitions $\pi_1, \pi_2, \ldots, \pi_k$.$\Box$

[We remark that this construction in the case when $k=2$ was known to Mehlhorn [13], and the case when $k=3$ is a construction of Blackburn [5, Theorem 3].]

Theorem 1 *Let s and t be positive integers such that $t \geq 2$. For any positive integer q, let $n_{s,t}(q)$ be the largest integer n such that an $(s; n, q, t)$-perfect hash family exists. Then $n_{s,t}(q) = O(q)$ if and only if $t > s$.*

Proof: When $s = t$, the $(s; q^{s/(s-1)}, q, s)$-perfect hash families constructed in Corollary 1 show that $n_{s,s}(q) \neq O(q)$. An $(s; n, q, t)$-perfect hash family is a $(s; n, q, t')$-perfect hash family for all $t' \leq t$; in particular, the constructions in Corollary 1 are $(s; q^{s/(s-1)}, q, t)$-perfect hash families for any t such that $2 \leq t \leq s$. Thus $n_{s,t}(q) \neq O(q)$ whenever $t \leq s$. To prove the theorem, it remains to show that $n_{s,t}(q) = O(q)$ whenever $t > s$.

Suppose that $\pi_1, \pi_2, \ldots, \pi_s$ form a $(s; n, q, t)$-perfect hash family, and suppose that $t > s$. For all $i \in \{1, 2, \ldots, s\}$, define $R_i \subseteq V$ by

$$R_i = \{x \in V : \text{ the part of } \pi_i \text{ containing } x \text{ contains at least two elements}\}.$$

Note that $|V \setminus R_i| \leq q$, since every element not in R_i lies in a part of π_i consisting of a single element, and π_i has at most q parts. (If $n > q$, so R_i is non-empty, $|V \setminus R_i| \leq q-1$.)

We show that $\cap_{i=1}^{s} R_i = \emptyset$. Suppose, for a contradiction, that $x \in \cap_{i=1}^{s} R_i$. Let $x_1, x_2, \ldots, x_s \in V \setminus \{x\}$ be such that x and x_i are distinct and lie in the same part of π_i (such x_i exist by our choice of x). Define X to be any set of size t containing $\{x, x_1, x_2, \ldots, x_s\}$; such a set exists since $t > s$. But X is not separated by any of $\pi_1, \pi_2, \ldots, \pi_s$, since x and x_i are distinct elements of X that lie in the same part of π_i. This contradicts the perfect hash family property, and so $\cap_{i=1}^{s} R_i = \emptyset$.

But now $V = \cup_{i=1}^{s}(V \setminus R_i)$ and so $n = |V| \leq \sum_{i=1}^{s}(|V \setminus R_i|) \leq sq$. Hence $n_{s,t}(q) = O(q)$ when $t > s$, as required.□

3 Some Constructions

This section constructs new classes of perfect hash families, and then shows that $\lim_{q\to\infty}(n_{s,t}(q))/q$ exists and that computing this limit can be reduced to a collection of linear programming problems.

The constructions in this section are all variations of the $(3; 3a^2, a^2+2a, 4)$-perfect hash family defined as follows. We imagine the elements of the set V as the disjoint union of three $a \times a$ squares C_1, C_2, C_3 (arranged in a horizontal line, see Figure 1). We describe the partitions π_1, π_2 and π_3 as follows. Elements in distinct squares are never in the same part of π_i. All the elements of C_1 are in parts of size 1 with respect to π_1; the square C_2 is partitioned into rows and the square C_3 into columns. The partitions π_2 and π_3 are similar, except the role of the squares changes cyclically. So π_2 divides C_2 into its individual elements, C_3 into rows and C_1 into columns. Similarly, π_3 divides C_3 into its individual elements, C_1 into rows and C_2 into columns.

Since each partition π_i clearly has $a^2 + 2a$ parts, to show that π_1, π_2, π_3 form a $(3; 3a^2, a^2 + 2a, 4)$-perfect hash family it suffices to show that every 4-subset of V is separated by at least one of the partitions.

Note that every pair of points in distinct squares is separated by every partition π_i. Moreover, if $x, y \in C_i$ are distinct, then $\{x, y\}$ is separated by at least two partitions — the partition π_i that divides C_i into individual elements, and at least one of the two remaining partitions, depending on whether x and y are in distinct rows of C_i or distinct columns of C_i.

Let X be a 4-subset of V. The intersection of X with C_1, C_2 and C_3 partitions X into 3 parts. The possibilities for the orders of these parts are $4,0,0$; $3,1,0$; $2,1,1$ and $2,2,0$. If one of the first three possibilities occurs, then X is separated by π_i, where C_i is the square containing the most elements of X. Suppose the last case occurs, and let C_i and C_j have non-trivial intersection with X. Now, $C_i \cap X$ is separated by at least two of

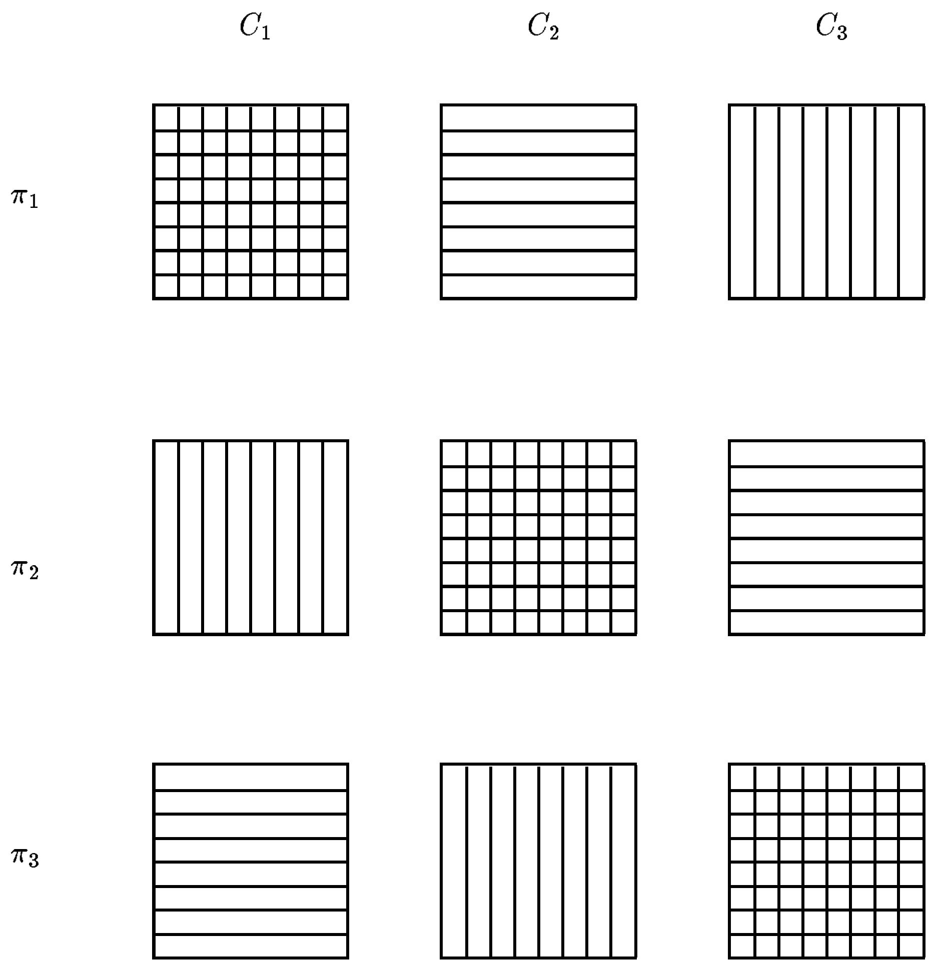

Figure 1: A $(3; 3a^2, a^2 + 2a, 4)$-perfect hash family

the three partitions, as is $C_j \cap X$. So there is a partition π_k that separates $C_i \cap X$ and $C_j \cap X$. But this partition separates X, since no element of $C_i \cap X$ can be in the same part of π_k as an element of $C_j \cap X$. Thus every 4-subset is separated, and we have a perfect hash family as required.

All the constructions of this section share many features with the construction of Figure 1. We will partition V into parts C_i and each of our partitions π_j will be a refinement of this partition. Moreover, restricting our partitions to C_i we find that a partition either has all parts of cardinality 1 or may be regarded as one of the partitions in the perfect hash family constructed in Section 2. A more complicated example is shown in Figure 2. In this example, we divide V into 7 parts. If the number of elements in C_1, C_2, C_3, C_4 and C_5 is chosen to be approximately $\frac{1}{5}q$, $\frac{1}{5}q$, $\frac{2}{5}q$, $\frac{2}{5}q$ and $\frac{3}{5}q$ respectively, then it is possible to check that the partitions form a $(5; n, q, 7)$-perfect hash family where n is approximately $\frac{9}{5}q$.

We will now define a class of linear programming problems, and we will go on to show the relationship between perfect hash families and these problems.

Let $\Gamma \subseteq \mathcal{P}(s)$ be a collection of subsets of $\{1, 2, \ldots, s\}$. We define the constant c_Γ to be the maximum value of $\sum_{S \in \Gamma} z_S$ where the variables z_S are real variables subject to the conditions that

$$z_S \geq 0 \tag{1}$$

for all $S \in \Gamma$ and

$$\sum_{j \notin S \in \Gamma} z_S \leq 1 \tag{2}$$

for all $j \in \{1, 2, \ldots, s\}$.

We say that $\{1, 2, \ldots, s\}$ has a *d set Γ-covering* if there exist subsets $S_1, S_2, \ldots, S_d \in \Gamma$ (not necessarily distinct) such that $\cup_{i=1}^{d} S_i = \{1, 2, \ldots, s\}$. Define $\mathcal{C}_d(s)$ to be the set of all $\Gamma \subseteq \mathcal{P}(s)$ such that $\{1, 2, \ldots, s\}$ has no d set Γ-covering, and define

$$c_{s,d} = \max_{\Gamma \in \mathcal{C}_d(s)} c_\Gamma.$$

We claim that for all positive integers s and d, $\lim_{q \to \infty}(n_{s,s+d}(q))/q = c_{s,d}$. Once we have proved this claim, we will have reduced the determination of the coefficient in the leading term of $n_{s,s+d}(q)$ to a collection of linear programming problems.

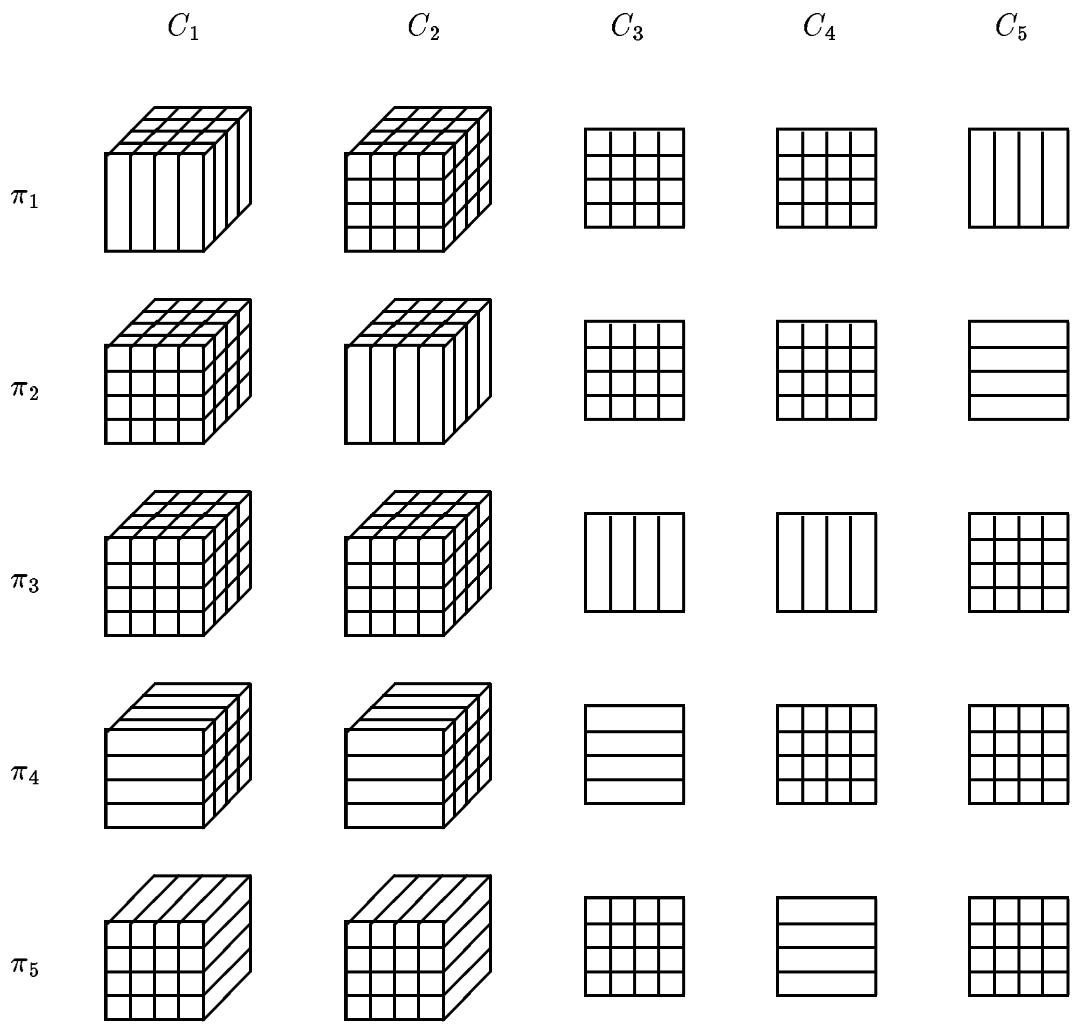

Figure 2: A more complicated construction

Theorem 2 *Let $\pi_1, \pi_2 \ldots, \pi_s$ be a $(s; n, q, s+d)$-perfect hash family, where $n > q$ and d is positive. Then, defining $c_{s,d}$ as above, $n/q \leq c_{s,d}$.*

Proof: For all $i \in \{1, 2, \ldots, s\}$, let $R_i \subseteq V$ be the set defined (just as in Section 2) by

$$R_i = \{x \in V : \text{ the part of } \pi_i \text{ containing } x \text{ contains at least two elements}\}.$$

As in Section 2, we have that $|V \setminus R_i| \leq q$. Define a collection $\Gamma \subseteq \mathcal{P}(s)$ of subsets of $\{1, 2, \ldots, s\}$ by

$$\Gamma = \{S \subseteq \{1, 2, \ldots, s\} : \cap_{i \in S} R_i \neq \emptyset\}.$$

We show that $\{1, 2, \ldots, s\}$ does not have a d set Γ-covering. Suppose, for a contradiction, that subsets $S_1, S_2, \ldots, S_d \in \Gamma$ have the property that $\cup_{i=1}^d S_i = \{1, 2, \ldots, s\}$. For all $i \in \{1, 2, \ldots, d\}$, let $x_i \in V$ be such that $x_i \in \cap_{j \in S_i} R_j$; such an element exists by definition of Γ. For all $k \in \{1, 2, \ldots, s\}$, there exists $i_k \in \{1, 2, \ldots, d\}$ such that $k \in S_{i_k}$, since $S_1, S_2, \ldots, S_d$ is an d-covering. Now, $x_{i_k} \in \cap_{j \in S_{i_k}} R_j \subseteq R_k$ and so there exists $y_k \in V \setminus \{x_{i_k}\}$ that is in the same part of π_k as x_{i_k}. Let X be a subset of V of cardinality $s+d$ containing $\{x_1, x_2, \ldots, x_d, y_1, y_2, \ldots, y_s\}$. Now, none of the partitions $\pi_1, \pi_2, \ldots, \pi_s$ separates X, since x_{i_k} and y_k are in the same part of π_k and are distinct. This contradicts the perfect hash family property of $\pi_1, \pi_2, \ldots, \pi_s$. Hence $\{1, 2, \ldots, s\}$ does not have a d set Γ-covering and so $\Gamma \in \mathcal{C}_d(s)$.

For every $S \in \Gamma$, define the non-negative real number z_S by

$$z_S = \frac{1}{q} \left| \{x \in V : x \in R_i \text{ if and only if } i \in S\} \right|.$$

[In the example of Figure 1 we find that $d = 1$, $R_1 = C_2 \cup C_3$, $R_2 = C_1 \cup C_3$, $R_3 = C_1 \cup C_2$. Since $R_1 \cap R_2 \cap R_3 = \emptyset$ but any R_i and R_j intersect non-trivially, Γ consists of every proper subset of $\{1, 2, 3\}$. Every element of V is contained in precisely two subsets R_i, and so $z_S = 0$ whenever $|S| \leq 1$. When $|S| = 2$, it is not difficult to check that $z_s = \frac{a^2}{a^2+2a}$ (for example, $z_{\{1,2\}} = \frac{|C_3|}{q}$) and so z_S approaches 1 from below as $q \to \infty$ whenever $|S| = 2$.]

Clearly the real numbers z_S satisfy (1). For any $j \in \{1, 2, \ldots, s\}$,

$$\begin{aligned} q &\geq |V \setminus R_j| \\ &= \left| \cup_{j \notin S \in \Gamma} \{x \in V : x \in R_i \text{ if and only if } i \in S\} \right| \end{aligned}$$

$$
\begin{aligned}
&= \sum_{j \notin S \in \Gamma} |\{x \in V : x \in R_i \text{ if and only if } i \in S\}| \\
&\quad \text{(as the sets in the union are disjoint)} \\
&= (\sum_{j \notin S \in \Gamma} z_S) q.
\end{aligned}
$$

Hence (2) holds. This implies that $\sum_{S \in \Gamma} z_S \leq c_\Gamma \leq c_{s,d}$.

Now,

$$
\begin{aligned}
n &= |V| = |\cup_{S \in \Gamma} \{x \in V : x \in R_i \text{ if and only if } i \in S\}| \\
&= \sum_{S \in \Gamma} |\{x \in V : x \in R_i \text{ if and only if } i \in S\}| \\
&\quad \text{(as the sets in the union are disjoint)} \\
&= (\sum_{S \in \Gamma} z_S) q \\
&\leq c_{s,d} q.
\end{aligned}
$$

Hence $n/q \leq c_{s,d}$ as required. $\Box$

Theorem 2 shows that $c_{s,d}$ provides an upper bound for $\lim_{q \to \infty}(n_{s,s+d}(q))/q$. The next theorem shows that this limit exists and that the bound is tight by constructing a good class of perfect hash families.

Theorem 3 *Let s and d be positive integers. Let $\Gamma \subseteq \mathcal{C}_d(s)$. Let $\{z_S : S \in \Gamma\}$ be a set of real numbers satisfying (1) and (2). Let m be the largest cardinality of a set in Γ, and let $c = \sum_{S \in \Gamma} z_S$. Then there exists a constant c' such that an $(s; n, q, s+d)$-perfect hash family exists with $n \geq cq - c'q^{(m-1)/m}$ for all sufficiently large q.*

Proof: Let q be a positive integer. When q is sufficiently large, we construct an $(s; n, q, s+d)$-perfect hash family as follows.

Define $p = \lfloor q - |\Gamma| q^{(m-1)/m} \rfloor$. Assume that q is large enough so that p is positive.

Let $S \in \Gamma$. Define $a_S = \left\lfloor (z_S p)^{1/|S|} \right\rfloor$, and let A_S be a set of cardinality a_S. Define $C_S = (A_S)^{|S|}$. Note that $z_S p \geq |C_S| \geq z_S p - f$, where $f = O(p^{(|S|-1)/|S|})$. Hence, since $q = p + O(q^{(m-1)/m})$, we find that $|C_S| \geq z_S q - f'$, where $f' = O(q^{(m-1)/m})$.

We define V to be the disjoint union $V = \cup_{S \in \Gamma} C_S$ and define $n = |V|$. By our lower bound on $|C_S|$, there exists a constant c' such that $n \geq cq - c'q^{(m-1)/m}$ for all sufficiently large q.

We define partitions $\pi_1, \pi_2, \dots \pi_s$ as follows. We define each partition so that $x \in C_S$ and $y \in C_{S'}$ lie in distinct parts of π_i whenever $S \neq S'$. If $i \notin S$, we let π_i restrict to equality on C_S. If $i \in S$ we define π_i restricted to C_S by the rule that $x, y \in C_S$ lie in the same part of π_i if they only disagree in their jth components, where $|\{1, 2, \dots, i\} \cap S| = j$. Now, π_i has at most $z_S p$ parts on C_S when $i \notin S$ and has at most $p^{(|S|-1)/|S|}$ parts on C_S when $i \in S$. Hence, since (2) is satisfied, the number of parts of π_i is at most

$$\begin{aligned}\sum_{i \in S \in \Gamma} p^{(|S|-1)/|S|} + \sum_{i \notin S \in \Gamma} z_S p &\leq |\Gamma| p^{(m-1)/m} + p \\ &\leq |\Gamma| q^{(m-1)/m} + p \\ &= q.\end{aligned}$$

The theorem will follow if we show that this set of partitions form a $(s; n, q, s+d)$-perfect hash family. We must show that every set X contained in V such that $|X| = s + d$ is separated by at least one of the partitions $\pi_1, \pi_2, \dots, \pi_s$.

Suppose that X is a subset of V such that $|X| = s + d$. Define, for all $S \in \Gamma$, the set X_S by $X_S = X \cap C_S$. Note that a partition π_i separates X if and only if it separates X_S for all $S \in \Gamma$ such that $X_S \neq \emptyset$. Suppose that at most d of the sets X_S are non-empty. So there exist $S_1, S_2, \dots S_d \in \Gamma$ such that $X_S \neq \emptyset$ implies that $S \in \{S_1, S_2, \dots S_d\}$. Since $\Gamma \in \mathcal{C}_d(s)$, we have that $\{1, 2, \dots, s\}$ does not have a d set Γ-covering, and so there exists $k \in \{1, 2, \dots, s\}$ such that $k \notin S_1 \cup S_2 \cup \dots \cup S_d$. But then π_k acts as equality when restricted to any of $C_{S_1}, C_{S_2}, \dots, C_{S_d}$, and so π_k separates all of the sets X_S. Hence we may assume that X_S is non-empty for more than d choices of S.

For $S \in \Gamma$, define $t_S = |X_S|$, so $\sum_{S \in \Gamma} t_S = s + d$ and at least $d + 1$ of the integers t_S are non-zero. For any $S \in \Gamma$ the set X_S is separated by all partitions π_i where $i \notin S$. Moreover, when $t_S > 0$, Proposition 1 shows that at most $t_S - 1$ of the remaining partitions fail to separate X_S. Hence the number of partitions that fail to separate X is at most

$$\begin{aligned}\sum_{\{S \in \Gamma : t_S > 0\}} (t_S - 1) &\leq \left(\sum_{\{S \in \Gamma : t_S > 0\}} t_S \right) - (d+1) \\ &\leq \left(\sum_{S \in \Gamma} t_S\right) - (d+1) \\ &= s + d - (d+1) = s - 1 < s.\end{aligned}$$

So there is at least one partition that separates X in this case, and so the theorem is proved.□

Theorem 4 *Let s and d be fixed positive integers, and define $c_{s,d}$ as above. Then $\lim_{q\to\infty} n_{s,s+d}/q$ exists and*

$$\lim_{q\to\infty} n_{s,s+d}/q = c_{s,d}.$$

Moreover, $c_{s,d}$ is a rational number.

Proof: The upper bound is provided by Theorem 2. To establish the lower bound, let $\Gamma \subseteq \mathcal{C}_d(s)$ be such that $c_\Gamma = c_{s,d}$, and let $\{z_S : S \in \Gamma\}$ satisfy (1) and (2) and have the property that $\sum_{S\in\Gamma} z_s = c_{s,d}$. Theorem 3 now implies that there exists a collection of $(s; n(q), q, s+d)$-perfect hash families for all sufficiently large q such that $n(q)/q \to c_{s,d}$ as $q \to \infty$.

Finally, $c_{s,d}$ is a rational number as it is derived from a finite collection of linear programming problems with integer coefficients. □

4 Explicit Calculation of the Leading Term

In this section, we compute the constants $c_{s,d}$ defined at the end of the previous section in several cases. In particular, we derive the values of $c_{s,d}$ given in Table 1. We finish the section with some brief remarks on the asymptotic properties of the constants $c_{s,d}$.

Lemma 1 *Let $\Gamma \subseteq \mathcal{P}(s)$ have the property that $\cup_{S\in\Gamma} S$ is strictly contained in $\{1, 2, \ldots, s\}$. Then $c_\Gamma \leq 1$.*

Proof: Let $i \in \{1, 2, \ldots, s\}$ be such that $i \notin \cup_{S\in\Gamma} S$. Then since $i \notin S$ for all $S \in \Gamma$, the corresponding inequality (2) becomes $\sum_{S\in\Gamma} z_S \leq 1$.□

Proposition 2 *For all positive integers s, we have $c_{s,1} = s$. When s and d are positive integers such that $d \geq s$, we have $c_{s,d} = 1$.*

Proof: The proof of Theorem 1 shows that an $(s; n, q, s+1)$-perfect hash family cannot have $n > sq$. Hence $c_{s,1} \leq s$. To show that $c_{s,1} \geq s$, consider the set Γ consisting of the subsets of $\{1, 2, \ldots, s\}$ of cardinality $s-1$. Since

		d					
		1	2	3	4	5	6
	1	1	1	1	1	1	1
	2	2	1	1	1	1	1
s	3	3	3/2	1	1	1	1
	4	4	5/3	4/3	1	1	1
	5	5	9/5	7/5	5/4	1	1
	6	6	2	3/2	9/7	6/5	1

Table 1: $c_{s,d}$ for $1 \leq s, d \leq 6$

all these sets are proper, $\Gamma \in \mathcal{C}_1(s)$. For any $i \in \{1, 2, \ldots, s\}$ there is a unique set $\{1, 2, \ldots, s\} \setminus \{i\} \in \Gamma$ that does not contain i, and so the inequalities (2) become $z_S \leq 1$ for all $S \in \Gamma$. Thus setting $z_S = 1$ for all $S \in \Gamma$ we find that the inequalities (1) and (2) are satisfied and $\sum_{S \in \Gamma} z_S = s$. This shows that $c_{s,1} = s$, as required. The construction corresponding to Γ in the case $s = 3$ is shown in Figure 1.

Clearly, $c_{s,d} \geq 1$ for any positive integers s and d (as any set of partitions that includes equality is an $(s; q, q, s+d)$-perfect hash family). Suppose that $d \geq s$. Let $\Gamma \in \mathcal{C}_d(s)$. If $\cup_{S \in \Gamma} S = \{1, 2, \ldots, s\}$, then $\{1, 2, \ldots, s\}$ has an s set Γ-covering (for each $i \in \{1, 2, \ldots, s\}$ choose a set S_i containing i; then $S_1, S_2, \ldots, S_s$ is a Γ-covering). Hence, since $d \geq s$, any $\Gamma \in \mathcal{C}_d(s)$ must have the property that $\cup_{S \in \Gamma} S \neq \{1, 2, \ldots, s\}$. But in this case, Lemma 1 implies that $c_\Gamma \leq 1$, and so the lemma is proved. Here is another way of seeing this last result: If we have an $(s; n, q, s+d)$-perfect hash family $\pi_1, \pi_2, \ldots, \pi_s$ with $n > q$ then for all $i \in \{1, 2, \ldots, s\}$ there exist distinct elements $x_i, y_i \in V$ contained in the same part of π_i. But then $\{x_i, y_i : 1 \leq i \leq s\}$ is a set of cardinality at most $2s$ that is not separated by any partition in the perfect hash family. Since $2s \leq s + d$, this is a contradiction and so $n \leq q$. Thus $c_{s,d} = 1$. $\square$

Let $\Gamma \subseteq \mathcal{C}_d(s)$, and suppose that there exist $S_1, S_2 \in \Gamma$ such that $S_1 \subset S_2$. Define $\Gamma' = \Gamma \setminus \{S_1\}$. Since $\{1, 2, \ldots, s\}$ has a d set Γ-covering if and only if $\{1, 2, \ldots, s\}$ has a d set Γ'-covering, we find that $\Gamma' \in \mathcal{C}_d(s)$. The maximum value c_Γ of $\sum_{S \in \Gamma} z_S$ may be obtained in the subregion produced by imposing the extra condition that $z_{S_1} = 0$ — for we may increment z_{S_2} by the value of

z_{S_1} and then set $z_{S_1} = 0$ without changing the sum we are trying to maximise or violating the conditions (1) and (2). This implies that $c_{\Gamma'} \geq c_\Gamma$. (It is not difficult to see that in fact $c_{\Gamma'} = c_\Gamma$.) We may repeat this process, removing any subset that is contained in another, until we obtain $\Gamma'' \in \mathcal{C}_d(s)$ such that $c_{\Gamma''} \geq c_\Gamma$ and that consists of incomparable sets (so $S_1, S_2 \in \Gamma''$ with $S_1 \subseteq S_2$ implies that $S_1 = S_2$).

Hence we may restrict ourselves to the case when Γ consists of incomparable subsets.

Lemma 2 *Let d and s be integers such that $d, s \geq 2$. Then*

$$c_{s,d} \geq \max\{c_{s,d+1}, c_{s-1,d}, 2 - (1/c_{s-1,d-1})\}.$$

Because of this lemma, we say that a set $\Gamma \in \mathcal{C}_d(s)$ is (s,d)-*interesting* if Γ consists of incomparable subsets and

$$c_\Gamma > \max\{c_{s,d+1}, c_{s-1,d}, 2 - (1/c_{s-1,d-1})\}.$$

Since the values of s and d are always clear by context, we omit them and merely refer to a collection of subsets as being interesting.

Proof: Since every $(s; n, q, s+d+1)$-perfect hash family is an $(s; n, q, s+d)$-perfect hash family, it is clear that $c_{s,d} \geq c_{s,d+1}$. (Another way of seeing this is to observe that if $\{1, 2, \ldots, s\}$ has no $d+1$ set Γ-covering then it has no d set Γ-covering.)

Since an $(s-1; n, q, s+d)$-perfect hash family may be extended to a $(s; n, q, s+d)$-perfect hash family by adding any partition, it is clear that $c_{s,d} \geq c_{s-1,d}$. (Another way of seeing this is to observe that any incomparable $\Gamma \in \mathcal{C}_d(s-1)$ gives rise to an incomparable $\overline{\Gamma} \in \mathcal{C}_d(s)$ by adding s to each set $S \in \Gamma$. Moreover, the inequalities (1) and (2) associated with $\overline{\Gamma}$ are the same as those corresponding to Γ, with the addition of the trivial inequality $0 \leq 1$.)

Let $\Gamma \in \mathcal{C}_{d-1}(s-1)$ consist of incomparable subsets, and suppose that $c_\Gamma = c_{s-1,d-1}$. Let $\{a_S \in \mathbb{R} : S \in \Gamma\}$ have the property that when $z_S = a_S$ for all $S \in \Gamma$, we have $\sum_{S \in \Gamma} z_S = c_{s-1,d-1}$ and (1) and (2) are satisfied. Let $\overline{\Gamma} = \Gamma \cup \{s\}$. Then $\overline{\Gamma}$ is a set of incomparable subsets of $\{1, 2, \ldots, s\}$. Any d set $\overline{\Gamma}$-covering of $\{1, 2, \ldots, s\}$ must consist of $\{s\}$ and a $d-1$ set Γ-covering of $\{1, 2, \ldots, s-1\}$, and so $\{1, 2, \ldots, s\}$ does not have a d set $\overline{\Gamma}$-covering.

Moreover, the inequalities (2) may be written

$$\begin{aligned}\left(\sum_{i\notin S\in\Gamma} z_S\right) + z_{\{s\}} &\le 1 \text{ for } i \in \{1,2,\ldots,s-1\} \text{ and}\\ \sum_{S\in\Gamma} z_S &\le 1.\end{aligned}$$

Setting $z_S = a_S/c_{s-1,d-1}$ for all $S \in \Gamma$ and setting $z_{\{s\}} = 1 - 1/c_{s-1,d-1}$ we find that the above inequalities are satisfied and $\sum_{S\in\overline{\Gamma}} z_S = 2 - 1/c_{s-1,d-1}$. So $c_{s,d} \ge 2 - 1/c_{s-1,d-1}$ as required.□

Lemma 3 *Let s and d be such that $s, d \ge 2$. Let $\Gamma \in \mathcal{C}_d(s)$ be interesting.*

(i) *We have $\cap_{S\in\Gamma} S = \emptyset$.*

(ii) *For all $i \in \{1,2,\ldots,s\}$, there are at least two sets $S \in \Gamma$ such that $i \in S$. In particular, $|S| \ge 2$ for all $S \in \Gamma$.*

(iii) *There is a subset $\Gamma' \subseteq \Gamma$ such that $c_{\Gamma'} = c_\Gamma$, $\Gamma' \in \mathcal{C}_d(s)$, $|\Gamma'| \le s$ and Γ' is interesting.*

(iv) *For any integer k such that $1 \le k \le d$, the union of any k subsets in Γ has cardinality at most $s - d + k - 1$. In particular, $|S| \le s - d$ for all $S \in \Gamma$.*

Proof: Suppose that $\cap_{S\in\Gamma} S \ne \emptyset$. Without loss of generality, assume that $s \in \cap_{S\in\Gamma} S$. Define the set Γ' of subsets of $\{1,2,\ldots,s-1\}$ by $\Gamma' = \{S \setminus \{s\} : S \in \Gamma\}$. The fact that $\{1,2,\ldots,s\}$ has no d set Γ-cover implies that $\{1,2,\ldots,s-1\}$ has no d set Γ'-cover and so $\Gamma' \in \mathcal{C}_d(s-1)$. There is a one-to-one correspondence between the members of Γ and the members of Γ'. Moreover, the inequalities (1) and (2) also correspond in a one-to-one manner, except Γ has the additional trivial relation $0 \le 1$ arising from considering the point s. Hence $c_\Gamma = c_{\Gamma'} \le c_{s-1,d}$ and so Γ is not interesting. This proves part (i).

Every $i \in \{1,2,\ldots,s\}$ is contained in at least one member of Γ by Lemma 1 and the fact that Γ is interesting. Suppose that there exists $i \in \{1,2,\ldots,s\}$ that is contained in precisely one member of Γ. Without loss of generality, we may assume that $i = s$. Define $\overline{\Gamma} = \{S \cup \{s\} : S \in \Gamma\}$.

A $(d-1)$ set $\overline{\Gamma}$-covering of $\{1,2,\ldots,s\}$ gives rise to a d set Γ-covering of $\{1,2,\ldots,s\}$ by adding the element of Γ containing s to the covering. Hence $\overline{\Gamma} \in \mathcal{C}_{d-1}(s)$. Since the sets in Γ are incomparable, there is a one-to-one correspondence between the sets in Γ and the sets in $\overline{\Gamma}$. Since every member of Γ corresponds to a member of $\overline{\Gamma}$ that contains it, the inequalities (2) are no stronger for $\overline{\Gamma}$ and so $c_\Gamma \leq c_{\overline{\Gamma}}$. But Part (i) shows that $\overline{\Gamma}$ is not interesting, and so Γ is not interesting. This contradiction shows that every $i \in \{1,2,\ldots,s\}$ is contained in at least two members of Γ. Since Γ consists of incomparable sets, $\emptyset \notin \Gamma$ (for otherwise Γ would contain no other sets, and so every $i \in \{1,2,\ldots,s\}$ would not be contained in any set $S \in \Gamma$). Moreover, if $\{i\} \in \Gamma$ for some $i \in \{1,2,\ldots,s\}$ then i is contained in no other set $S \in \Gamma$ (for then $\{i\}, S \in \Gamma$ would be comparable). Hence $|S| \geq 2$ for all $S \in \Gamma$.

We claim that whenever $|\Gamma| > s$, there exists $\Gamma' \in \mathcal{C}_d(s)$ such that $\Gamma' \subseteq \Gamma$, $|\Gamma'| = |\Gamma| - 1$ and $c_{\Gamma'} = c_\Gamma$; this will establish Part (iii) of the lemma. The maximum value of $\sum_{S\in\Gamma} z_S$ subject to (1) and (2) must occur at a basic feasible solution, i.e. at a vertex of the convex polytope obtained by imposing $|\Gamma|$ of the conditions (1) and (2) as equalities. At most s of these equalities can correspond to the inequalities (2), and so when $|\Gamma| > s$ we impose at least one condition of the form $z_S = 0$ (corresponding to an inequality of the form (1)) and still achieve the maximum value $c_{s,t}$. But in this case, defining $\Gamma' \in \mathcal{C}_d(s)$ by $\Gamma' = \Gamma \setminus \{S\}$ we have that $c_{\Gamma'} = c_\Gamma$. This establishes our claim.

Finally, we prove Part (iv) of the lemma. By Lemma 1, $\cup_{S\in\Gamma} S = \{1,2,\ldots,s\}$. Suppose for a contradiction that Γ contains subsets $S_1, S_2, \ldots S_k$ such that $\cup_{i=1}^k S_i$ has cardinality $s-d+k$ or more. There are at most $d-k$ elements of $\{1,2,\ldots,s\}$ that are not in $\cup_{i=1}^k S_i$. Since every element of $\{1,2,\ldots,s\}$ is contained in at least one member of Γ, there exist $S_{k+1}, S_{k+2}, \ldots, S_d \in \Gamma$ such that $\cup_{i=k+1}^d S_i$ contains every element not in $\cup_{i=1}^k S_i$. But now $S_1, S_2, \ldots, S_d$ is a d set Γ-covering of $\{1,2,\ldots,s\}$. This contradiction establishes Part (iv) of the lemma. $\Box$

Proposition 3 *Let s be an integer such that $s \geq 2$. Then $c_{s,s-1} = s/(s-1)$*

Proof: Let $\Gamma \in \mathcal{C}_{s-1}(s)$. Suppose that Γ is interesting. Then Lemma 3 (iv) implies that $|S| \leq 1$ for all $S \in \Gamma$ and Lemma 3 (ii) implies that $|S| \geq 2$ for all $S \in \Gamma$. Since Γ is non-empty, this is a contradiction. So no member of $\mathcal{C}_{s-1}(s)$ is interesting.

When $s = 2$, we have already established that $s_{2,1} = 2$. When $s > 2$ and the proposition holds for all smaller values of s,

$$c_{s,s-1} = \max\{1, 1, 2 - (s-2)/(s-1)\} = s/(s-1),$$

since no Γ is interesting. The proposition now follows by induction on s. $\square$

We remark that the collection of perfect hash families implicit in this proposition is exactly the collection constructed by Martirosyan and Martirosyan [12].

Proposition 4 *Let s be an integer such that $s \geq 3$. Then $c_{s,s-2} = (2s-3)/(2s-5)$.*

Proof: Proposition 2 establishes the result when $s = 3$. By Lemma 2, $c_{s,s-2} \geq 2 - 1/c_{s-1,s-3}$. Using this inequality in an inductive argument on s establishes that $c_{s,s-2} \geq (2s-3)/(2s-5)$.

Suppose, for a contradiction, that $\Gamma \in \mathcal{C}_{s-2}(s)$ consists of incomparable sets and has the property that $c_\Gamma > (2s-3)/(2s-5)$. Lemma 2 and Proposition 3 combine to show that Γ must be interesting.

By Lemma 3 (ii) and (iv), $|S| = 2$ for all $S \in \Gamma$. So we may identify Γ with a graph G on s vertices.

Now, G has no vertex of degree 0 or 1, as this would contradict the fact that Γ is interesting by Lemma 1 and Lemma 3 (ii) respectively. Lemma 3 (iv) implies that no two subsets of cardinality 2 in Γ are disjoint, and so G contains no pair of disjoint edges. The only graph satisfying all these properties is a triangle on 3 vertices. But we are assuming that $s > 3$, and so we have our required contradiction.$\square$

Proposition 5 *Let s be an integer such that $s \geq 4$. Then*

$$c_{s,s-3} = \begin{cases} 4 & \textit{if } s = 4, \\ 9/5 & \textit{if } s = 5 \textit{ and} \\ (s-3)/(s-4) & \textit{if } s \geq 6. \end{cases}$$

Proof: Proposition 2 proves the proposition when $s = 4$. We now consider the case when $s = 5$. Let $\Gamma \in \mathcal{C}_2(5)$ be such that $c_\Gamma = c_{5,2}$. Suppose that Γ is interesting. By Lemma 3 (iii), we may assume that Γ consists of at most 5 subsets. Lemma 3 (ii) and (iv) imply that $|S| \in \{2, 3\}$ for all $S \in \Gamma$ and any two 3-subsets in Γ must intersect in 2 points.

Suppose Γ contains no 3-subsets. As in the previous proposition, the graph G associated with Γ has 5 vertices, at most 5 edges and contains no vertices of degree 0 or 1. Hence G must be a 5-cycle. It is easy to check that $c_\Gamma = 5/3$ in this case.

Suppose Γ contains a 3-set; without loss of generality, we may assume that $\{1,2,3\} \in \Gamma$. No set $S \in \Gamma$ contains $\{4,5\}$, as then $S, \{1,2,3\}$ would cover $\{1,2,3,4,5\}$. Every point is contained in at least 2 members of Γ, by Lemma 3 (ii). Hence there must be four more sets in Γ; precisely two sets contain 4 and precisely two sets contain 5.

Suppose Γ contains no other 3-sets. Without loss of generality, we may assume that the two members of Γ containing 4 are $\{1,4\}$ and $\{2,4\}$. The remaining two members of Γ contain 5, and since 3 must be contained in at least two members of Γ, we must have $\{3,5\} \in \Gamma$. Without loss of generality, we may assume the final member to be $\{2,5\}$. In summary, if Γ is interesting and contains only one 3-subset, we may assume that

$$\Gamma = \{\{1,2,3\},\{1,4\},\{2,4\},\{2,5\},\{3,5\}\}.$$

It is not difficult to calculate that $c_\Gamma = 7/4 < 9/5$ in this case, the maximum of the associated linear programming problem being achieved when

$$\begin{aligned} z_{\{1,2,3\}} &= 1/4, \\ z_{\{1,4\}} = z_{\{3,5\}} &= 1/2, \\ z_{\{2,4\}} = z_{\{2,5\}} &= 1/4. \end{aligned}$$

Suppose Γ contains a second 3-set; so without loss of generality $\{1,2,4\} \in \Gamma$. In this case, neither of the two members $S_1, S_2 \in \Gamma$ containing 5 can contain 3 (as otherwise we would have a covering $\{1,2,4\}, S_i$ of $\{1,2,3,4,5\}$ for some i). Hence $S_1, S_2 \subseteq \{1,2,5\}$. These sets are incomparable and both contain 5, so they must be $\{1,5\}$ and $\{2,5\}$. The remaining subset $S \in \Gamma$ contains $\{3,4\}$, as 3 and 4 must each be contained in at least two members of Γ; moreover $5 \notin S$. But $\{1,3,4\}, \{2,3,4\} \notin \Gamma$ as otherwise we would have a 2 set Γ-covering of $\{1,2,3,4,5\}$. So $S = \{3,4\}$. To summarise, if Γ contains two 3-sets, we may assume without loss of generality that

$$\Gamma = \{\{1,2,3\},\{1,2,4\},\{3,4\},\{1,5\},\{2,5\}\}.$$

It is not difficult to show that $c_\Gamma = 9/5$; the maximum of the associated linear programming problem occurs when:

$$\begin{aligned} z_{\{1,2,3\}} = z_{\{1,2,4\}} &= 1/5, \\ z_{\{3,4\}} &= 3/5, \\ z_{\{1,5\}} = z_{\{2,5\}} &= 2/5. \end{aligned}$$

This example shows that $c_\Gamma \geq 9/5$. Moreover, we have shown that if Γ is interesting then $c_\Gamma \leq 9/5$. Since the uninteresting case has $c_\Gamma \leq \max\{5/3, 7/5, 2-1/4\} < 9/5$, we have shown that $c_{5,2} = 9/5$. (The perfect hash family in Figure 2 is a realisation of this case.)

Now suppose that $s \geq 6$ and Γ is interesting. As before, Γ consists of incomparable 2-sets and 3-sets. Suppose Γ contains a 3-set S. Since the union of any two member of Γ has cardinality at most 4, no member of Γ contains two points not in S. Now, there are at most $s-1$ subsets in $\Gamma \setminus \{S\}$, and so a point outside S is contained in at most $(s-1)/(s-3)$ members of Γ on average. Since $s \geq 6$, this average is less than 2, and so there exists a point contained in at most one member of Γ, contradicting the fact that Γ is interesting. So Γ contains only 2-sets.

The graph G associated with Γ has s vertices, at most s edges and no vertices of degree 0 or 1. So G is a union of disjoint cycles. Moreover, Lemma 3 (iv) implies that there cannot be three disjoint edges in G. This implies that $s = 6$ and G consists of two disjoint triangles. In this case, we may assume without loss of generality that

$$\Gamma = \{\{1,2\},\{2,3\},\{1,3\},\{4,5\},\{4,6\},\{5,6\}\}.$$

Then $c_\Gamma = 3/2$, which is achieved by setting $z_S = 1/4$ for all $S \in \Gamma$.

When $s = 6$, an uninteresting collection of subsets Γ has

$$c_\Gamma \leq \max\{7/5, 9/7, 2-5/9\} < 3/2,$$

and so $c_{6,3} = 3/2$. When $s > 6$, there are no interesting choices for Γ and so we may prove by induction on s that

$$\begin{aligned} c_{s,s-3} &= \max\{(2s-3)/(2s-5), (2s-5)/(2s-7), 2-(s-5)/(s-4)\} \\ &= (s-3)/(s-4). \end{aligned}$$

This establishes the proposition. $\Box$

Proposition 6 *We have* $c_{6,2} = 2$.

Proof: Let Γ be the subset of $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ given by

$$\Gamma = \{\{(x,y),(x+1,y),(x,y+1)\} : x \in \mathbb{Z}/3\mathbb{Z}, y \in \mathbb{Z}/2\mathbb{Z}\}$$

It is easy to check that $\Gamma \in \mathcal{C}_2(6)$ (since every pair of subsets in Γ intersects non-trivially), and that every element of $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ is contained in exactly 3 members of Γ (since the group $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ acts regularly on the subsets in Γ). Setting $z_S = 1/3$ for all $S \in \Gamma$, we find that (1) and (2) are satisfied and $\sum_{S\in\Gamma} z_S = 2$.

Let $\Gamma \in \mathcal{C}_2(6)$ be such that $c_\Gamma > 2$ and consists of incomparable subsets; in particular, Γ is interesting. We may assume that there are at most 6 subsets in Γ. By Lemma 3 (ii) and (iv), Γ consists of 2-sets, 3-sets and 4-sets. Suppose there exist $x, y \in \{1,2,3,4,5,6\}$ such that $x \neq y$ and such that $\{x,y\}$ is not contained in any member of Γ. Then

$$\sum_{S\in\Gamma} z_S \leq \sum_{x\notin S\in\Gamma} z_S + \sum_{y\notin S\in\Gamma} z_S \leq 1 + 1 \leq 2,$$

by (2). Hence $c_\Gamma \leq 2$, which is a contradiction. Hence every pair of elements from $\{1,2,3,4,5,6\}$ is contained in some member of Γ. In particular, Γ does not contain a 4-set, as this set together with a subset in Γ containing its complement would produce a 2 set Γ-covering.

Let $S \in \Gamma$. Then z_S occurs three times in the inequalities (2) if $|S| = 3$ and four times if $|S| = 2$. If we sum all the inequalities (2), we find that

$$4(\sum_{S\in\Gamma,|S|=2} z_S) + 3(\sum_{S\in\Gamma,|S|=3} z_S) \leq 6.$$

Hence $3(\sum_{S\in\Gamma} z_S) \leq 6$ and so $c_\Gamma \leq 2$. This contradiction shows that $c_{6,2} = 2$, as required. □

Finally, we make some remarks on the asymptotics of the table entries. Firstly, it is possible to show that $c_{s,s-k} \to 1$ as $s \to \infty$ with k fixed. This can be shown by proving that there exist no interesting sets Γ when s is sufficiently large. Secondly, $c_{s,d} \to \infty$ as $s \to \infty$ with d fixed. Indeed, suppose $s = k^d$ for some integer k and identify $\{1,2,\ldots,s\}$ with $(\mathbb{Z}/k\mathbb{Z})^d$ in some way. Take Γ to consist of all images under the natural action of $(\mathbb{Z}/k\mathbb{Z})^d$ of the subset $(\{0,1,2\ldots,k-2\})^d$. Setting $z_S = 1/(k^d - (k-1)^d)$ for all $S \in \Gamma$ we find that $c_\Gamma \geq k^d/(k^d - (k-1)^d)$. Hence $c_{s,d}$ grows at least as fast as $s^{1/d}$.

Acknowledgements Many thanks to Peter Wild for his careful reading of an earlier manuscript, and to Andrew Sheer for help with linear programming terminology.

References

[1] N. Alon, Explicit construction of exponential sized families of k-independent sets, Discrete Math. 58 (1986) 191-193.

[2] N. Alon and M. Naor, Derandomization, witnesses for Boolean matrix multiplication and construction of perfect hash functions, Algorithmica 16 (1996) 434-449.

[3] M. Atici, S.S. Magliveras, D.R. Stinson and W.-D. Wei, Some recursive constructions for perfect hash families, J. Comb. Designs 4 (1996) 353-363.

[4] S.R. Blackburn, Combinatorics and threshold cryptography, in: F.C. Holroyd, K.A.S. Quinn, C. Rowley and B.S. Webb eds, Combinatorial designs and their applications, Chapman & Hall/CRC Research Notes in Mathematics 403 (CRC Press, London, 1999) 49-70.

[5] S.R. Blackburn, Perfect hash families: probabilistic methods and explicit constructions, J. Comb. Theory, Series A, to appear.

[6] S.R. Blackburn, M. Burmester, Y. Desmedt and P.R. Wild, Efficient multiplicative sharing schemes, in: U. Maurer ed., Advances in Cryptology — EUROCRYPT '96, Lecture Notes in Computer Science 1070 (Springer, Berlin, 1996) 107-118.

[7] S.R. Blackburn and P.R. Wild, Optimal linear perfect hash families, J. Comb. Theory, Series A 83 (1998) 233-250.

[8] Z.J. Czech, G. Havas and B.S. Majewski, Perfect hashing, Theoretical Computer Science 182 (1997) 1-143.

[9] A. Fiat and M. Naor, Broadcast encryption, in: D.R. Stinson ed., Advances in Cryptology — CRYPTO '93, Lecture Notes in Computer Science 773 (Springer, Berlin, 1994) 480-491.

[10] M.L. Fredman and J. Komlós, On the size of separating systems and families of perfect hash functions, SIAM J. Alg. Disc. Methods 5 (1984) 61-68.

[11] J. Körner and Marton, New bounds for perfect hashing via information theory, Europ. J. Combinatorics 9 (1988) 523-530.

[12] S. Martirosyan and S. Martirosyan, New upper bound on the cardinality of a k-separated set or perfect hash family and a near optimal construction for it, Proceedings of the International Seminar on Coding Theory dedicated to 70th anniversary of Prof. R.R. Varshamov, Thakadzor, Armenia, 2-6 October 1997.

[13] K. Mehlhorn, Data Structures and Algorithms 1: Sorting and Searching (Springer-Verlag, Berlin, 1984).

[14] I. Newman and A. Wigderson, Lower bounds on formula size of Boolean functions using hypergraph entropy, SIAM J. Disc. Math. 8 (1995) 536-542.

[15] R. Safavi-Naini and H. Wang, Broadcast authentication in group communication, in: K.Y. Lam, E. Okamoto, C. Xing eds, Advances in Cryptology — ASIACRYPT '99, Lecture Notes in Computer Science 1716 (Springer, Berlin, 1999) 399-411.

[16] J.N. Staddon, D.R. Stinson and R. Wei, Combinatorial properties of frameproof and traceability codes, *preprint.*

[17] D.R. Stinson, T. van Trung and R. Wei, Secure frameproof codes, key distribution patterns, group testing algorithms and related structures, J. Statist. Plan. Infer., to appear.

[18] D.R. Stinson, R. Wei and L. Zhu, New constructions for perfect hash families and related structures using combinatorial designs, *preprint.*