Explicit Constructions for Perfect Hash Families

Sosina Martirosyan
University of Houston-Clear Lake
2700 Bay Area Blvd.,
Houston, TX, 77058, U.S.A.
Martirosyan@uhcl.edu

Tran van Trung
Institut für Experimentelle Mathematik,
Universität Duisburg-Essen
Ellernstrasse 29, 45326 Essen, Germany
trung@iem.uni-due.de

Abstract

Let k, v, t be integers such that $k \geq v \geq t \geq 2$. A perfect hash family $\mathsf{PHF}(N; k, v, t)$ can be defined as an $N \times k$ array with entries from a set of v symbols such that every $N \times t$ subarray contains at least one row having distinct symbols. Perfect hash families have been studied by over 20 years and they find a wide range of applications in computer sciences and in cryptography. In this paper we focus on explicit constructions for perfect hash families using combinatorial methods. We present many recursive constructions which result in a large number of improved parameters for perfect hash families. The paper also includes extensive tables for parameters with $t = 3, 4, 5, 6$ of newly constructed perfect hash families.

Keywords: Perfect hash family, combinatorial method, explicit construction.

1 Introduction

Let h be a function from a set A to a set B. We say that h *separates* a subset $T \subseteq A$ if h is injective when restricted to T. Let k, v, t be integers such that $k \geq v \geq t \geq 2$. Suppose $|A| = k$ and $|B| = v$. A set $\mathcal{H}$ of functions from A to B with $|\mathcal{H}| = N$ is an $(N; k, v, t)$-*perfect hash family* if for all $T \subseteq A$ with $|T| = t$, there exists at least one $h \in \mathcal{H}$ such that h separates T. We use the notation $\mathsf{PHF}(N; k, v, t)$ for an $(N; k, v, t)$-perfect hash family. A $\mathsf{PHF}(N; k, v, t)$ can be depicted as $N \times k$ array 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 value $h_i(j)$. Thus, a $\mathsf{PHF}(N; k, v, t)$ is equivalent to an $N \times k$ array with entries from a set of v symbols such that every $N \times t$ subarray contains at least one row having distinct symbols.

Let $\mathsf{PHFN}(k, v, t)$ denote the smallest value N for which a $\mathsf{PHF}(N; k, v, t)$ exists. We call $\mathsf{PHFN}(k, v, t)$ the *perfect hash family number*.

Perfect hash families were first used by Mehlhorn [20] in compiler design for efficient information storage and retrieval and they have been intensively studied by computer scientists for over 20 years. Recently, perfect hash families have found increasingly applications in cryptography, for instance, in threshold cryptography [4, 5], in broadcast encryption [13], in multicast re-keying schemes [21], in secure frameproof codes, key distribution patterns, group testing algorithms etc. [22], in parent property codes [25]. And more recently, they have been used in constructions for covering arrays [9], [16], [17], [11]

For given parameters k, v, t it is not difficult to construct a perfect hash family, if the number N of functions does not have to be small. However, regarding the efficieny in practical use of PHFs it is most desirable that N should be as small as possible. The problem is therefore to minimize N. A perfect hash family with the smallest possible number of functions, i.e. a $\mathsf{PHF}(N; k, v, t)$ with $N = \mathsf{PHFN}(k, v, t)$, is called *optimal*. Necessary conditions for the existence of a perfect hash family can be found in [19], [14], [15], [7], where probabilistic methods are used to obtain sufficient conditions as well. In fact, for fixed v and t the value of $\mathsf{PHFN}(k, v, t)$ is proved to be $\Theta(\log k)$. However, the proof is not constructive and finding explicit constructions of PHFs having such asymptotical values for N appears to be a challenge.

Efforts have been put into searching for explicit constructions of perfect hash families. Consequently, various methods and techniques have been found and developed for this purpose, see for instance [1], [2], [8], [4], [6], [3], [17], [23], [24], [25].

In a recent paper [27] Walker II and Colbourn review the known explicit constructions for PHFs and present many new explicit constructions. The paper also contains large tables for PHFs for a wide range of parameters. Specially, the first comprehensive tables of known parameters for PHFs created by Walker II at `http://www.phftables.com` are very useful for comparing the strength of the known and new constructions. For a brief survey of perfect hash families the reader is also referred to [10].

In this paper we focus on explicit constructions for PHFs using combinatorial methods - mainly recursive in nature. Surprisingly, the results from our constructions improve a great deal of known parameters for PHFs. Several of the constructions generalize those in [27] as well.

2 Some Results about Explicit Constructions

In this section we briefly summarize some known results of PHF constructions. For further information about known results for perfect hash families the reader is referred to [27].

Theorem 2.1 $\mathsf{PHFN}(k, v, 2) = \lceil \log_v k \rceil$.

A simple direct construction yields an optimal class of PHFs.

Theorem 2.2 (First-N Construction) *[27] For $s \geq 1$ and $m \geq 2$, $\mathsf{PHFN}(ms+m, ms+1, 2s+1) = s+1$.*

The first interesting recursive construction of "Roux-type" for PHFs is given by Walker and Colbourn.

Theorem 2.3 *[27] $\mathsf{PHFN}(k\ell, v, t) \leq \mathsf{PHFN}(k, v, t) + \mathsf{PHFN}(k, \lfloor v/\ell \rfloor, t-1)$ whenever $\ell(t-1) \leq v$.*

Theorem 2.4 *[27] For $t \geq 3$, $\mathsf{PHFN}(k+1, v, t) \leq \mathsf{PHFN}(k, v, t) + \mathsf{PHFN}(k-1, v-2, t-2)$.*

The next basic construction, called *symbol increase*, is very simple, however useful.

Theorem 2.5 $\mathsf{PHFN}(k+1, v+1, t) \leq \mathsf{PHFN}(k, v, t)$

3 The First Construction

Although the following recursive construction is simple, perfect hash families produced by this construction improve many known results. Also it is worth noting that the Walker-Colbourn first-N construction can be derived from this construction.

Let A_1 be a $\mathsf{PHF}(N_1; k_1, v_1, t_1)$ and A_2 be a $\mathsf{PHF}(N_2; k_2, v_2, t_2)$ with $k_1 > t_1$, $k_2 > t_2$ and $t_1 \leq t_2$. Let $v = \max\{v_1 + k_2, v_2 + k_1\}$. We construct a $\mathsf{PHF}(N_1 + N_2; k_1 + k_2, v, t_1 + t_2 + 1)$.

1. Assume $v = \max\{v_1 + k_2, v_2 + k_1\} = v_1 + k_2$. Let V_1 be the symbol set of A_1 and W_2 a symbol set of size k_2 such that $V_1 \cap W_2 = \emptyset$. Define $V := V_1 \cup W_2$. Let B_2 denote an $N_1 \times k_2$ array, in which each row is a copy of set W_2. Let $V_2 \subseteq V$ be the symbol set of A_2 and let $W_1 \subseteq V$ be a subset of size k_1 such that $V_2 \cap W_1 = \emptyset$. Let B_1 be an $N_2 \times k_1$ array, in which each row is a copy of set W_1. Denote C_1 the $N_1 \times (k_1 + k_2)$ array formed by horizontally juxtaposing A_1 and B_2. Denote C_2 the $N_2 \times (k_1 + k_2)$ array obtained by horizontally juxtaposing B_1 and A_2. Define C to be an $(N_1 + N_2) \times (k_1 + k_2)$ array formed by vertically juxtaposing C_1 and C_2. We prove that C is a $\mathsf{PHF}(N_1 + N_2; k_1 + k_2, v, t_1 + t_2 + 1)$.

Let I_1 resp. I_2 be the set of k_1 first columns resp. k_2 last columns of C. Let T be any set of $t_1 + t_2 + 1$ columns of C.

If $|T \cap I_1| \geq t_1 + 1$, then there is a row in C_2 having distinct symbols in the columns of T.

If $|T \cap I_1| \leq t_1$, then there is a row in C_1 having distinct symbols in the columns of T. Hence C is a perfect hash family.

2. The case $v = \max\{v_1 + k_2, v_2 + k_1\} = v_2 + k_1$ can be proved similarly. In this case denote V_2 the symbol set of A_2 and W_1 a symbol set of size k_1 such that $V_2 \cap W_1 = \emptyset$. Define $V := V_2 \cup W_1$. Denote B_1 an $N_2 \times k_1$ array, in which each row is a copy of symbol set W_1. Let $V_1 \subseteq V$ be the symbol set of A_1 and let $W_2 \subseteq V$ be a subset of size k_2 such that $V_1 \cap W_2 = \emptyset$. Now if C is formed from A_1, A_2, B_1 and B_2 as in the previous case, then we can prove similarly that C is a $\mathsf{PHF}(N_1 + N_2; k_1 + k_2, v, t_1 + t_2 + 1)$.

Thus we have the following theorem.

Theorem 3.1 *For $1 \leq t_1 \leq t_2$, $t_1 < k_1$ and $t_2 < k_2$ we have*

$$\mathsf{PHFN}(k_1 + k_2, v, t_1 + t_2 + 1) \leq \mathsf{PHFN}(k_1, v_1, t_1) + \mathsf{PHFN}(k_2, v_2, t_2),$$

where $v = \max\{k_1 + v_2, k_2 + v_1\}$.

Remark 3.1 It should be noted that the construction in Theorem 3.1 may use PHFs with $t = 1$. Naturally, the definition of PHFs can include the case $t = 1$. However, this case is trivial, as a $\mathsf{PHF}(1; k, v, 1)$ can always be constructed.

When A_1 and A_2 have the same parameter $\mathsf{PHF}(N; k, v, t)$, Theorem 3.1 provides the following result.

Corollary 3.2 *For $k > t$,*

$$\mathsf{PHFN}(2k, v + k, 2t + 1) \leq 2\mathsf{PHFN}(k, v, t).$$

Now we show that the first-N construction can be obtained from the construction in Theorem 3.1.

Corollary 3.3 *For $s \geq 1$ and $m \geq 2$ there is a*

$$\mathsf{PHF}(s+1; sm+m, sm+1, 2s+1).$$

Proof. Using Theorem 3.1 we construct a $\mathsf{PHFN}(s+1; sm+m, sm+1, 2s+1)$ for every $s \geq 1$ and $m \geq 2$. This can be done recursively as follows. Let A_1 be a $\mathsf{PHF}(1; m, 1, 1)$. Using Corollary 3.2 we obtain a perfect hash family A_3 having parameter $\mathsf{PHF}(1+1; m+m, m+1, 2+1)$. Applying Theorem 3.1 to the pair A_1 and A_3 produces a $\mathsf{PHF}(2+1; 2m+m, 2m+1, 2.2+1)$ A_5. The pair A_1 and A_5 forms a $\mathsf{PHF}(3+1; 3m+m, 3m+1, 2.3+1)$ A_7. Hence the corollary follows by continuing this process. □

Here are some examples of PHFs obtained from Theorem 3.1. Using a $\mathsf{PHF}(2; 9, 3, 2)$ and a $\mathsf{PHF}(4; 9, 3, 3)$ as ingredients yields a $\mathsf{PHF}(6; 18, 12, 6)$. Using a $\mathsf{PHF}(1; 11, 1, 1)$ and a $\mathsf{PHF}(4; 19, 9, 4)$ produces $\mathsf{PHF}(5; 30, 20, 6)$.

4 The Second Construction

Let v be a prime power and $t \geq 3$ an integer with $v > \binom{t}{2} - 1$. Let

A be a $\mathsf{PHF}(N_1; k, v, t)$,

$\mathsf{B} = (b_{ij})$ be a $\mathsf{PHF}(N_2; k, v, t-1)$ and

$\mathsf{C} = (c_{ij})$ be a $(\binom{t}{2} - 1) \times v$-array, obtained by taking any $(\binom{t}{2} - 1)$ non-zero rows of the multiplication table of the finite field $\mathbb{F}_v$. The entries of arrays A and B will be considered as elements of $\mathbb{F}_v$.

We make use of the following two properties of the array C in our construction.

(P_1) : Giving any two columns j_1, j_2, the set of $N_3 := \binom{t}{2} - 1$ differences $\{c_{1j_1} - c_{1j_2}, c_{2j_1} - c_{2j_2}, \ldots, c_{N_3 j_1} - c_{N_3 j_2}\}$ are pairwise distinct, where the differences are computed modulo v.

(P_2) : The entries in each row of C are pairwise distinct.

Let D be an $(N_1 + (\binom{t}{2} - 1).N_2 + 1) \times vk$-array, which is formed by vertically juxtaposition of three arrays D_1, D_2 and D_3.

D_1 is an $N_1 \times vk$ array consisting of v copies of A placed side by side.

D_2 is a $(\binom{t}{2} - 1).N_2 \times vk$ array is the "Kronecker addition" of C and B, denoted $\mathsf{D}_2 = \mathsf{C} \oplus \mathsf{B}$. The array D_2 is obtained by replacing each of its entry c_{rs} with a $N_2 \times k$ array $c_{rs} + B := \{c_{rs} + b_{ij} : i = 1, \ldots, N_2;\ j = 1, \ldots, k\}$

D_3 is an $1 \times vk$ array obtained by placing side by side v distinct blocks of size k, where each block contains one element of $\mathbb{F}_v$ repeated k times.

We prove that D is a $\mathsf{PHF}(N_1 + (\binom{t}{2} - 1).N_2 + 1; vk, v, t)$.

Partition the columns of D into v blocks of k columns each; denote these blocks $I_1, I_2, \ldots, I_v$ (i.e. I_1 is the first k columns, I_2 the next k columns, and so on). Let T be a set of t columns of D. There are 3 main cases.

(1) $|T \cap I_j| = t$, i.e. $T \subseteq I_j$;

(2) $|T \cap I_j| \leq 1$ for all $j = 1, \ldots, v$;

(3) There is a block I_j such that $2 \leq |T \cap I_j| < t$.

In case (1) the columns of T restricted to D_1 arise from t distinct columns of A. Hence T is separated in D_1. In case (2) the columns of T are in t different blocks I_j's, therefore T is separated in D_3.

The most involved case is case (3). This case implies that the columns of T are distributed in at least 2 and at most $(t-1)$ blocks I_j's. We show that T is separated by D_2.

To explain the proof that T is separated in case (3) for any $t \geq 3$, we first look at an example with $t = 4$. Here, without loss of generality, we need to consider the following distributions of the columns of T.

(a) $|T \cap I_1| = 3$, $|T \cap I_2| = 1$;

(b) $|T \cap I_1| = |T \cap I_2| = 2$;

(c) $|T \cap I_1| = 2$, $|T \cap I_2| = |T \cap I_3| = 1$.

Now consider these 3 cases.

(a) $|T \cap I_1| = 3$, $|T \cap I_2| = 1$.

Let $T_1 = T \cap I_1 = \{t_1, t_2, t_3\}$, $T_2 = T \cap I_2 = \{t_4\}$. If $t_4 \pmod{k} \neq t_1, t_2, t_3$, then the columns of T restricted to D_1 arise from 4 distinct columns of A, hence T is separated in D_1. Assume that $t_4 \pmod{k} = t_1$. Now as B is a $\mathsf{PHF}(N_2; k, v, 3)$ we have a row having symbols a, b, c which separates T_1 in B. Hence in D_2 we have 4 rows having the following symbols in columns t_1, t_2, t_3, t_4:

$$\begin{array}{llll} a+c_{i1} & b+c_{i1} & c+c_{i1} & a+c_{i2} \\ a+c_{j1} & b+c_{j1} & c+c_{j1} & a+c_{j2} \\ a+c_{h1} & b+c_{h1} & c+c_{h1} & a+c_{h2} \\ a+c_{\ell 1} & b+c_{\ell 1} & c+c_{\ell 1} & a+c_{\ell 2} \end{array}$$

Property (P_1) says that $c_{x1} - c_{x2} \neq c_{y1} - c_{y2}$ for $x, y = i, j, h, \ell$ with $x \neq y$. It follows that there is a row $r \in \{i, j, h, \ell\}$ such that $a + c_{r2} \neq a + c_{r1},\ b + c_{r1},\ c + c_{r1}$. Moreover, as $a + c_{r1}$, $b + c_{r1}$, $c + c_{r1}$ are distinct, the symbols $a + c_{r2}$, $a + c_{r1}$, $b + c_{r1}$, $c + c_{r1}$ in row r separate T in D_2.

(b) $|T \cap I_1| = |T \cap I_2| = 2$.

Let $T_1 = T \cap I_1 = \{t_1, t_2\}$, $T_2 = T \cap I_2 = \{t_3, t_4\}$. If $t_3, t_4 \pmod{k} \neq t_1, t_2$, then T is separated in D_1. Assume that $t_3 \pmod{k} = t_1$ and $t_4 \pmod{k} \neq t_2$. Again there are 4 rows in D_2 with the following symbols in columns t_1, t_2, t_3, t_4:

$$\begin{array}{llll} a+c_{i1} & b+c_{i1} & a+c_{i2} & c+c_{i2} \\ a+c_{j1} & b+c_{j1} & a+c_{j2} & c+c_{j2} \\ a+c_{h1} & b+c_{h1} & a+c_{h2} & c+c_{h2} \\ a+c_{\ell 1} & b+c_{\ell 1} & a+c_{\ell 2} & c+c_{\ell 2} \end{array}$$

where a, b, c are distinct. At least one of these 4 rows must separate T. In fact, if the first row does not separate T, then we may assume $a + c_{i2} = b + c_{i1}$; it follows from (P_1) that $a + c_{u2} \neq b + c_{u1}$, $u = j, h, \ell$. Now if the second row and the third row both do not separate T, then we may assume $c + c_{j2} = b + c_{j1}$ and $c + c_{h2} = a + c_{h1}$. Again (P_1) implies that $c + c_{\ell 2} \neq b + c_{\ell 1}$ and $c + c_{\ell 2} \neq a + c_{\ell 1}$, therefore $a + c_{\ell 1}, b + c_{\ell 1}, a + c_{\ell 2}, c + c_{\ell 2}$ are pairwise distinct (note that $a + c_{\ell 2} \neq c + c_{\ell 2}$ as $a \neq c$). Thus the fourth row separates T. The case $t_3 \pmod{k} = t_1$ and $t_4 \pmod{k} = t_2$ can be treated in a similar manner.

(c) $|T \cap I_1| = 2$, $|T \cap I_2| = |T \cap I_3| = 1$.

Let $T_1 = T \cap I_1 = \{t_1, t_2\}$, $T_2 = T \cap I_2 = \{t_3\}$ and $T_3 = T \cap I_3 = \{t_4\}$. There are 5 subcases that need to be considered:

(c1) $t_3 \equiv t_4 \pmod{k}$ and $t_3, t_4 \pmod{k} \neq t_1, t_2$,

(c2) $t_3 \equiv t_4 \pmod{k}$ and $t_3, t_4 \pmod{k} = t_1$,

(c3) $t_3 \not\equiv t_4 \pmod{k}$, $t_3 \pmod{k} = t_1$ and $t_4 \pmod{k} = t_2$

(c4) $t_3 \not\equiv t_4 \pmod{k}$, $t_3 \pmod{k} = t_1$ and $t_4 \pmod{k} \neq t_2$

(c5) $t_3 \not\equiv t_4 \pmod{k}$, $t_3 \pmod{k} \neq t_1$ and $t_4 \pmod{k} \neq t_2$.

As a demonstration we show that T is separated in case (c4). Now there are 5 rows in D_2 with the following symbols in columns t_1, t_2, t_3, t_4:

$$\begin{array}{cccc} a+c_{i1} & b+c_{i1} & a+c_{i2} & c+c_{i3} \\ a+c_{j1} & b+c_{j1} & a+c_{j2} & c+c_{j3} \\ a+c_{h1} & b+c_{h1} & a+c_{h2} & c+c_{h3} \\ a+c_{\ell 1} & b+c_{\ell 1} & a+c_{\ell 2} & c+c_{\ell 3} \\ a+c_{m1} & b+c_{m1} & a+c_{m2} & c+c_{m3} \end{array}$$

with (a, b, c) distinct. If the first 4 rows do not separate T, then w.l.o.g. we may assume that

$$a + c_{i2} = b + c_{i1},$$
$$c + c_{j3} = a + c_{j1},$$
$$c + c_{h3} = b + c_{h1},$$
$$c + c_{\ell 3} = a + c_{\ell 2}.$$

It follows from (P_1) and (P_2) that $c + c_{m3} \neq a + c_{m2}, a + c_{m1}, b + c_{m1}$ and that $a + c_{m2}, a + c_{m1}, b + c_{m1}$ are distinct. Hence the fifth row separates T. By a similar proof we see that D_2 separates T in cases (c1), (c2) and (c3) as well. Finally, D_1 separates T in case (c5).

From the example for $t = 4$, it is clear that if t is large, the number of different distributions of the columns of T among the blocks I_j's become very large. However, to deal with case (3) it is not necessary to deal with all the possible distributions of the columns of T separately. The proof for case $t = 4$ above shows that we only need the properties (P_1), (P_2) and the fact that B is a $\mathsf{PHF}(N_2; k, v, t-1)$ and C has $\binom{t}{2} - 1$ rows.

This can be seen as follows: The t columns of $T = \{t_1, t_2, \ldots, t_t\}$ are distributed among at most $(t-1)$ the blocks I_j's and there is a block, say I_1, with $2 \leq |T \cap I_1| < t$. W.l.o.g. we may assume that the columns of T are distributed among blocks $I_1, I_2, \ldots, I_{t-1}$. If these columns (modulo k) are all distinct, then D_1 separates T. Assume that this is not the case. Then the set $T^* := \{t_1 \bmod k, t_2 \bmod k, \ldots, t_t \bmod k\}$ has s distinct elements with $s \leq t-1$. Thus the columns of T^* restricted to D_2 arise $s \leq t-1$ distinct columns of B. So, there is a row r in B having s distinct elements $b_1, b_2, \ldots, b_s$ in the columns T^*. As D_2 is the Kronecker addition of C and B, the $\binom{t}{2} - 1$ rows in D_2 corresponding to this row r and columns of T form a $(\binom{t}{2} - 1) \times t$ sub-array Q. Since $2 \leq |T \cap I_1| < t$, there are at least two columns t_1 and t_2 in $T \cap I_1$ such that the entries in column t_1 and t_2 of each row of Q are distinct. Using properties (P_1) and (P_2) for C we see that in the worst case at most $\binom{t-2}{2} + 2(t-2) - 1$ rows of Q cannot separate T. This is because there are at least two columns t_i and t_j of T such that $t_i = t_j \bmod k$ and each row u of Q has already distinct entries $b_i + c_{uh_i}$, $b_i + c_{uh_j}$ in columns t_i and t_j. Now, since $\binom{t-2}{2} + 2(t-2) - 1 < \binom{t}{2} - 1$, there is at least one row of Q separating T.

Thus we have the following result.

Theorem 4.1 *Let v be a prime power and let $t \geq 3$ be an integer such that $\binom{t}{2} - 1 < v$. Suppose that there exist a $\mathsf{PHF}(N_1; k, v, t)$ and a $\mathsf{PHF}(N_2; k, v, t-1)$. Then there exists a $\mathsf{PHF}(N_1 + (\binom{t}{2} - 1)N_2 + 1; vk, v, t)$.*

Here are some examples of PHFs constructed from Theorem 4.1. Using a $\mathsf{PHF}(6; 22, 7, 4)$ and a $\mathsf{PHF}(3; 22, 7, 3)$ we obtain a $\mathsf{PHF}(22; 154, 7, 4)$. A $\mathsf{PHF}(6; 27, 13, 5)$ and $\mathsf{PHF}(4; 27, 13, 4)$

together produce a $\mathsf{PHF}(43; 531, 13, 5)$. A $\mathsf{PHF}(79; 1058, 23, 6)$ is obtained from a $\mathsf{PHF}(8; 46, 23, 6)$ and a $\mathsf{PHF}(5; 46, 23, 5)$.

5 The second extended construction

An observation shows that the second construction can be modified for the case when v is not a prime power.

Let v be a composite number and w be a prime power such that $w < v$. Let $t \geq 3$ an integer such that $\binom{t}{2} - 1 < w$. Assume that the following exist

A, a $\mathsf{PHF}(N_1; k, v, t)$,

$\mathsf{B} = (b_{ij})$, a $\mathsf{PHF}(N_2; k, w, t-1)$ and

$\mathsf{C} = (c_{ij})$, a $(\binom{t}{2} - 1) \times w$-array, obtained by taking any $(\binom{t}{2} - 1)$ non-zero rows of the multiplication table of the finite field $\mathbb{F}_w$. The elements of $\mathbb{F}_w$ are the symbol set for B and we will consider $\mathbb{F}_w$ as a subset of the symbol set for A.

As for the second construction we define an array D be an $(N_1 + (\binom{t}{2} - 1).N_2 + 1) \times wk$-array, which is formed by vertically juxtaposition of three arrays D_1, D_2 and D_3.

D_1 is an $N_1 \times wk$ array consisting of w copies of A placed side by side.

D_2 is an $(\binom{t}{2} - 1).N_2 \times wk$ array, which is the "Kronecker addition" of C and B, denoted $\mathsf{D}_2 = \mathsf{C} \oplus \mathsf{B}$. The array D_2 is obtained by replacing each of its entry c_{rs} with a $N_2 \times k$ array $c_{rs} + B := \{c_{rs} + b_{ij} : i = 1, \ldots, N_2;\ j = 1, \ldots, k\}$

D_3 is an $1 \times wk$ array obtained by placing side by side w distinct blocks of size k, where each block contains one element of $\mathbb{F}_w$ repeated k times.

Now, with a similar argumentation as for the second construction we see that D is a $\mathsf{PHF}(N_1 + (\binom{t}{2} - 1).N_2 + 1; wk, v, t)$.

Theorem 5.1 *Let v be an integer and let w be a prime power with $w \leq v$. Let $t \geq 3$ be an integer such that $\binom{t}{2} - 1 < w$. Suppose that there exist a $\mathsf{PHF}(N_1; k, v, t)$ and a $\mathsf{PHF}(N_2; k, w, t-1)$. Then there exists a $\mathsf{PHF}(N_1 + (\binom{t}{2} - 1)N_2 + 1; wk, v, t)$.*

Theorem 5.1 produces, for instance, a $\mathsf{PHF}(27; 1331, 12, 4)$ from a $\mathsf{PHF}(6; 121, 12, 4)$ and a $\mathsf{PHF}(4; 121, 11, 3)$. Also a $\mathsf{PHF}(66; 1599, 14, 5)$ is constructed from a $\mathsf{PHF}(11; 123, 14, 5)$ and a $\mathsf{PHF}(6; 123, 13, 4)$.

6 General Constructions

In this section we generalize the results of the last two constructions. We first begin with a definition of a new combinatorial object.

Definition 6.1 *A $\mathsf{PPPHF}(N; k, v, s, r)$ is a $N \times k$ array if its any $N \times r$ subarray, B, has a subset of s rows for which the properties P_1 and P_2 are satisfied.*

Let C be the $s \times r$ subarray of B containing the subset of s rows.

(P_1) : Giving any two columns j_1, j_2 of C, the set of s differences $\{c_{1j_1} - c_{1j_2}, c_{2j_1} - c_{2j_2}, \ldots, c_{sj_1} - c_{sj_2}\}$ are pairwise distinct, where the differences are computed modulo v.

(P_2) : *The entries in each row of* C *are pairwise distinct.*

Lemma 6.1 *For any integer* s *and any prime power* v, $v > s$, *if a* $\mathsf{PHF}(N; k, v, r)$ *exists then a* $\mathsf{PPPHF}(sN; k, v, s, r)$ *exists.*

Proof. Let E be a $\mathsf{PHF}(N; k, v, r)$ and $\mathsf{D} = (d_{ij})$ be a $s \times v$-array, obtained by taking any s non-zero rows of the multiplication table of the finite field $\mathbb{F}_v$. Note that D is a $\mathsf{PPPHF}(s; k, v, s, v)$. Also note that $r \leq v$(this is because a $\mathsf{PHF}(N; k, v, r)$ exists). Denote v columns of D by $\mathsf{D}_1, \mathsf{D}_2, \cdots, \mathsf{D}_v$. The array A is obtained by replacing the symbols of E with columns of D (i.e. symbol 0 is replaced with D_1, symbol 1 with D_2 and so on.) It is left to show that A is a $\mathsf{PPPHF}(sN; k, v, s, r)$.

Let B be any $sN \times r$ subarray of A. Since E is a $\mathsf{PHF}(N; k, v, r)$, B has a $s \times r$ subarray C the columns of which are r distinct columns of D. Hence A is a $\mathsf{PPPHF}(sN; k, v, s, r)$ by definition. □

The following theorem is a generalization of Theorem 5.1.

Theorem 6.2 *Let* v *be an integer and let* w *be a prime power with* $w \leq v$. *Let* $t \geq 3$ *be an integer such that* $\binom{t}{2} - 1 < w$. *Suppose that there exist* $\mathsf{PHF}(N_1; k, v, t)$, $\mathsf{PHF}(N_2; l, v, t)$, $\mathsf{PHF}(N_3; k, w, t-1)$ *and* $\mathsf{PPPHF}(N_4; l, w, \binom{t}{2} - 1, t-1)$. *Then there exists a* $\mathsf{PHF}(N_1 + N_2 + N_3N_4; lk, v, t)$.

Proof. Let A be a $\mathsf{PHF}(N_1; k, v, t)$, B be a $\mathsf{PHF}(N_2; l, v, t)$

$\mathsf{C} = (c_{ij})$ be a $\mathsf{PHF}(N_3; k, w, t-1)$ and

$\mathsf{F} = (f_{ij})$ be a $\mathsf{PPPHF}(N_4; l, w, \binom{t}{2} - 1, t-1)$. The entries of arrays C and F will be considered as elements of $\mathbb{F}_w$. Let D be an $(N_1 + N_2 + N_3N_4) \times lk$-array, which is formed by vertically juxtaposition of three arrays D_1, D_2 and D_3.

D_1 is an $N_1 \times lk$ array consisting of l copies of A placed side by side.

D_2 is an $N_2 \times lk$ array repeating first columns of B k times, and then second column of B k times and so on.

D_3 is a $N_3N_4 \times lk$ array, which is the "Kronecker addition" of F and C, denoted $\mathsf{D}_3 = \mathsf{F} \oplus \mathsf{C}$. The array D_3 is obtained by replacing each entry f_{rs} of F with a $N_3 \times k$ array $f_{rs} + C := \{f_{rs} + c_{ij} : i = 1, \ldots, N_3;\ j = 1, \ldots, k\}$

The proof that D is a $\mathsf{PHF}(N_1 + N_2 + N_3N_4; lk, v, t)$ is similar to the proof of the second construction. □

Next corollary is obtained from Lemma 6.1 and Theorem 6.2.

Corollary 6.3 *Let* v *be an integer and let* w *be a prime power with* $w \leq v$. *Let* $t \geq 3$ *be an integer such that* $\binom{t}{2} - 1 < w$. *Suppose that there exist* $\mathsf{PHF}(N_1; k, v, t)$, $\mathsf{PHF}(N_2; l, v, t)$, $\mathsf{PHF}(N_3; k, w, t-1)$ *and* $\mathsf{PHF}(N_4; l, w, t-1)$. *Then there exists a* $\mathsf{PHF}(N_1 + N_2 + (\binom{t}{2} - 1)N_3N_4; lk, v, t)$.

Definition 6.2 *A* $\mathsf{PHF}((N_1, N_2); k, v, (t, s))$ *is a* $\mathsf{PHF}(N_1 + N_2; k, v, t)$ *such that* N_2 *rows of it form a* $\mathsf{PHF}(N_2; k, v, s)$ *where* $s < t$.

If a $\mathsf{PHF}(N_1 + N_2 + N_3N_4; k, v, 3)$ is obtained from the construction in the Theorem 6.2, then it can be shown that a $\mathsf{PHF}((N_1 + N_2, N_3N_4); k, v, (3, 2))$ and a $\mathsf{PHF}((N_3N_4, N_1 + N_2), k, v, (3, 2))$ exist.

Lemma 6.4 *For any prime power v and any integer i, $0 \le i \le \frac{v}{3}$, there exists a* $\mathsf{PHF}((2i, i+1); v^{i+1}, v, (3,2))$.

Proof. For any prime power v and any integer $0 \le i \le \frac{v}{3}$ a $\mathsf{PHF}(3i+1; v^{i+1}, v, 3)$ can be constructed using Bush's construction for orthogonal arrays. Note that any set of $i+1$ rows of this PHF is a $\mathsf{PHF}(i+1; v^{i+1}, v, 2)$. □

When $t = 4$, for some parameter values the following theorem gives stronger results than Theorem 5.1.

Theorem 6.5 *Let v be an integer and let w be a prime power with $5 < w \le v$. Suppose that there exist* $\mathsf{PHF}(N_1; k, v, 4)$ *and* $\mathsf{PHF}((N_2, N_3); k, w, (3,2))$. *Then there exists a* $\mathsf{PHF}(N_1 + 4N_2 + 5N_3 + 1, wk, v, 4)$.

Proof. Let A be a $\mathsf{PHF}(N_1; k, v, 4)$,

$\mathsf{B} = (b_{ij})$ be a $\mathsf{PHF}((N_2, N_3); k, w, (3,2))$ and

$\mathsf{C} = (c_{ij})$ be a $4 \times w$-array, obtained by taking any 4 non-zero rows of the multiplication table of the finite field $\mathbb{F}_w$. The elements of $\mathbb{F}_w$ are the symbol set for B and we will consider $\mathbb{F}_w$ as a subset of the symbol set for A.

Let B', a $\mathsf{PHF}(N_3; k, w, 2)$ obtained from B by removing its N_2 rows. And let C' be $1 \times w$-array containing any non-zero rows of the multiplication table of the finite field $\mathbb{F}_w$ not used in C.

We define an array D be an $(N_1 + 4N_2 + 5N_3 + 1) \times wk$-array, which is formed by vertically juxtaposition of four arrays D_1, D_2, D_3 and D_4.

D_1 is an $N_1 \times wk$ array consisting of w copies of A placed side by side.

D_2 is an $4(N_2 + N_3) \times wk$ array consisting of the "Kronecker addition" of C and B, denoted $\mathsf{D}_2 = \mathsf{C} \oplus \mathsf{B}$. The array D_2 is obtained by replacing each of entry c_{rs} of C with a $(N_2 + N_3) \times k$ array $c_{rs} + B := \{c_{rs} + b_{ij} : i = 1, \ldots, (N_2 + N_3);\ j = 1, \ldots, k\}$.

D_3 is an $N_3 \times wk$ array, which is the "Kronecker addition" of C' and B'.

D_4 is an $1 \times wk$ array obtained by placing side by side w distinct blocks of size k, where each block contains one element of $\mathbb{F}_w$ repeated k times.

With a similar argumentation as for the second construction we see that D is a $\mathsf{PHF}(N_1 + 4N_2 + 5N_3 + 1; wk, v, t)$.

In other words, considering all possible cases as it is done in the second construction for $t = 4$, we notice that the only case for which it is required to have 5 rows in C is the case where B does not need to be a 3-PHF. In this case, a part of B that is a 2-PHF can be used. The remaining cases to be covered B have to be a 3-PHF and C needs to have only 4 rows not 5. □

Theorem 6.6 *For any prime power v and for any integer i, $0 \le i \le \frac{v}{6}$, there exists a* $\mathsf{PHF}(19i + 7; v^{i+2}, v, 4)$

Proof. There exists a $\mathsf{PHF}(6i + 1; v^{i+1}, v, 4)$, (Reed-Solomon code or orthogonal array of index 1), for any integer i, $0 \le i \le \frac{v}{6}$. From Lemma 6.4 there exists a $\mathsf{PHF}((2i, i+1); v^{i+1}, v, (3,2))$. Hence a $\mathsf{PHF}(19i + 7; v^{i+2}, v, 4)$ can be obtained by applying Theorem 6.5 with $w = v$. □

Theorem 6.6, for instance, provides a $\mathsf{PHF}(26; 7^3, 7, 4)$ and a $\mathsf{PHF}(26; 9^3, 9, 4)$.

Note also that using symbol increasing on $\mathsf{PHF}(26; 729, 9, 4)$ we get $\mathsf{PHF}(26; 730, 10, 4)$.

7 Two Further Constructions

We study two further recursive constructions.

The first construction is a generalization of the construction given in Theorem 2.4 by Walker and Colbourn, in which the number of columns k is increased by one. The next theorem shows that it is possible to increase k by more than one column.

Theorem 7.1 *For $t \geq 3$, and for any integer $2 \leq x \leq v-t+2$,* $\mathsf{PHFN}(k+x-1, v, t) \leq \mathsf{PHFN}(k, v, t) + \mathsf{PHFN}(k-1, v-x, t-2)$

Proof. Let x be any fixed integer $2 \leq x \leq v-t+2$. Suppose there exist a $\mathsf{PHF}(N_1; k, v, t)$ A and a $\mathsf{PHF}(N_2; k-1, v-x, t-2)$ B. Let the symbol set of A be $\{m_1, m_2, \cdots, m_v\}$ and and the symbol set of B be $\{m_1, m_2, \cdots, m_{v-x}\}$. We produce a perfect hash family $\mathsf{PHF}(N'; k+x-1, v, t)$ C where $N' = N_1 + N_2$. C is formed by vertically juxtaposing arrays C_1 of size $N_1 \times (k+x-1)$ and C_2 $N_2 \times (k+x-1)$.

In row r and column c of C_1 place the entry in cell (r, c) of A if $c \leq k$ and the entry in cell (r, k) of A if $k < c \leq k+x-1$.

In row r and column c of C_2 place the entry in cell (r, c) of B if $c \leq k-1$. For $i = 0, \ldots, x-1$ in the column $k+i$ place the symbol $m_{v-x+i+1}$. These are the symbols of A that are not used in B.

We show that C is a perfect hash family. Consider t columns of C. If this set of columns includes at most one of last x columns then when restricted to C_1 they arise from t distinct columns of A and hence at least one row has distinct symbols.

It remains to check the cases when, for a fixed j such that $0 \leq j \leq t-3$, the $t-j-2$ columns are selected from the first $k-1$ columns and $j+2$ columns are selected from the remaining columns. The $t-j-2$ columns when restricted to C_2 arise from $t-j-2$ distinct columns of B. Hence at least one row r has distinct symbols in these columns. In the row r and the remaining $j+2$ columns the entries are distinct symbols that are not used in B. Hence the row r has distinct entries in the set of t columns. □

Some examples of $\mathsf{PHF}(k, 5, 4)$ constructed from Theorem 7.1 are $\mathsf{PHF}(34; 66, 5, 4)$, $\mathsf{PHF}(57; 173, 5, 4)$, and $\mathsf{PHF}(75, 363, 5, 4)$.

A large number of new parameters for PHFs obtained from Theorem 7.1 has been included in the tables at `http://www.phftables.com` under the source: *column increase x*.

Another approach to study perfect hash families is that for fixed N, v and t find the largest k for which a $\mathsf{PHF}(N; k, v, t)$ exists. The following simple recursive construction is using a known perfect hash family to construct a perfect hash family with one less row. As a result perfect hash families with improved parameters are obtained.

Theorem 7.2 (row decrease) *Suppose there exists a* $\mathsf{PHF}(N; k, v, t)$. *Then there exists a* $\mathsf{PHF}(N-1; \lceil \frac{k(t-1)}{v} \rceil, v, t)$.

Proof. Let A be a $\mathsf{PHF}(N; k, v, t)$. Suppose the symbol i, $0 \leq i \leq v-1$ appears x_i times in the jth row of A. So $x_0 + x_1 + \cdots + x_{(v-1)} = k$. Without loss of generality suppose $x_0 \geq x_1 \geq \cdots \geq x_{(v-1)}$. Note that the symbols could be simply renamed otherwise.

Let $k' = x_0 + x_1 + \cdots + x_{(t-2)}$. Let B be an $N \times k'$ subarray of A obtained by deleting the columns of A that have the symbols $x_{(t-1)}, x_{(t)}, \cdots, x_{(v-1)}$ in row j. B is a $\mathsf{PHF}(N; k', v, t)$

as deleting a column from a perfect hash family we get a perfect hash family of the same strength. Note that we may even get less symbols after this step. Now remove the row j from B to get an $(N-1)\times k'$ array C. C is a $\mathsf{PHF}(N-1;k',v,t)$ as the row j deleted from B contains at most $t-1$ distinct symbols.

From $x_0 \geq x_1 \geq \cdots \geq x_{(v-1)}$ it follows that $x_0 + x_1 + \cdots + x_{(v-1)} \leq v\frac{x_0+x_1+\cdots+x_{(t-2)}}{t-1}$. So $k' \geq \frac{k(t-1)}{v}$ and hence a $\mathsf{PHF}(N-1;\lceil\frac{k(t-1)}{v}\rceil,v,t)$ exists. □

Here are some PHF parameters provided by using row decrease construction of Theorem 7.2: $\mathsf{PHF}(27;2048,4,3)$, $\mathsf{PHF}(90;1320,5,4)$, and $\mathsf{PHF}(65;70,11,5)$.

Remark 7.1 Note that by using the construction given in the proof of Theorem 7.2 we can construct perfect hash families having more columns than the bound $\lceil\frac{k(t-1)}{v}\rceil$ given in the theorem. In fact, $\lceil\frac{k(t-1)}{v}\rceil$ is a lower bound on number of columns of a PHF obtained by this construction method.

A large number of new PHF parameters obtained from Theorem 7.2 has been presented at `http://www.phftables.com` under the source: *row decrease.*

8 Tables for newly constructed PHFs

In this section we present tables of parameters for PHFs with relatively small values of v and with $t = 3,4,5,6$ produced by the methods in this paper. To our knowledge the newly constructed PHFs are the best known. For creating the tables we intensively use the beneficial existence tables for PHFs of Walker II at `http://www.phftables.com` to obtain most of the ingredients. The remaining part of ingredients is taken from our tables.

Ingredients	New PHF
$\mathsf{PHF}(2;22,5,2)$ & $\mathsf{PHF}(2;22,5,2)$	$\mathsf{PHF}(4;44,27,5)$
$\mathsf{PHF}(2;25,5,2)$ & $\mathsf{PHF}(2;25,5,2)$	$\mathsf{PHF}(4;50,30,5)$
$\mathsf{PHF}(2;9,3,2)$ & $\mathsf{PHF}(4;9,3,3)$	$\mathsf{PHF}(6;18,12,6)$
$\mathsf{PHF}(2;11,4,2)$ & $\mathsf{PHF}(4;11,4,3)$	$\mathsf{PHF}(6;22,15,6)$
$\mathsf{PHF}(2;15,4,2)$ & $\mathsf{PHF}(4;15,4,3)$	$\mathsf{PHF}(6;30,19,6)$
$\mathsf{PHF}(2;16,4,2)$ & $\mathsf{PHF}(3;18,6,3)$	$\mathsf{PHF}(5;34,22,6)$
$\mathsf{PHF}(2;20,5,2)$ & $\mathsf{PHF}(3;22,7,3)$	$\mathsf{PHF}(5;42,27,6)$
$\mathsf{PHF}(1;15,1,1)$ & $\mathsf{PHF}(4;23,9,4)$	$\mathsf{PHF}(5;38,24,6)$
$\mathsf{PHF}(1;8,1,1)$ & $\mathsf{PHF}(5;13,6,4)$	$\mathsf{PHF}(6;21,14,6)$
$\mathsf{PHF}(1;14,1,1)$ & $\mathsf{PHF}(4;22,9,4)$	$\mathsf{PHF}(5;36,23,6)$
$\mathsf{PHF}(1;12,1,1)$ & $\mathsf{PHF}(4;20,9,4)$	$\mathsf{PHF}(5;32,21,6)$
$\mathsf{PHF}(1;11,1,1)$ & $\mathsf{PHF}(4;19,9,4)$	$\mathsf{PHF}(5;30,20,6)$
$\mathsf{PHF}(1;10,1,1)$ & $\mathsf{PHF}(4;18,9,4)$	$\mathsf{PHF}(5;28,19,6)$
$\mathsf{PHF}(1;9,1,1)$ & $\mathsf{PHF}(4;17,9,4)$	$\mathsf{PHF}(5;26,18,6)$
$\mathsf{PHF}(1;16,1,1)$ & $\mathsf{PHF}(4;25,10,4)$	$\mathsf{PHF}(5;41,26,6)$
$\mathsf{PHF}(1;15,1,1)$ & $\mathsf{PHF}(4;24,10,4)$	$\mathsf{PHF}(5;39,25,6)$
$\mathsf{PHF}(2;21,5,2)$ & $\mathsf{PHF}(2;21,5,2)$	$\mathsf{PHF}(4;42,26,5)$
$\mathsf{PHF}(1;16,1,1)$ & $\mathsf{PHF}(4;28,13,4)$	$\mathsf{PHF}(5;44,29,6)$
$\mathsf{PHF}(2;23,5,2)$ & $\mathsf{PHF}(3;26,8,3)$	$\mathsf{PHF}(5;51,31,6)$

Table 1: PHFs constructed from Theorem 3.1

Ingredients	New PHF
PHF(4; 12, 7, 4) & PHF(2; 12, 7, 3)	PHF(15; 84, 7, 4)
PHF(5; 18, 7, 4) & PHF(3; 18, 7, 3)	PHF(21; 126, 7, 4)
PHF(6; 22, 7, 4) & PHF(3; 22, 7, 3)	PHF(22; 154, 7, 4)
PHF(14; 70, 7, 4) & PHF(5; 70, 7, 3)	PHF(40; 490, 7, 4)
PHF(13; 63, 7, 4) & PHF(5; 63, 7, 3)	PHF(39; 441, 7, 4)
PHF(3; 12, 8, 4) & PHF(2; 12, 8, 3)	PHF(14; 96, 8, 4)
PHF(4; 14, 8, 4) & PHF(2; 14, 8, 3)	PHF(15; 112, 8, 4)
PHF(5; 21, 8, 4) & PHF(3; 21, 8, 3)	PHF(21; 168, 8, 4)
PHF(6; 27, 8, 4) & PHF(3; 27, 8, 3)	PHF(22; 216, 8, 4)
PHF(7; 32, 8, 4) & PHF(3; 32, 8, 3)	PHF(23; 256, 8, 4)
PHF(10; 67, 8, 4) & PHF(5; 67, 8, 3)	PHF(36; 536, 8, 4)
PHF(14; 88, 8, 4) & PHF(5; 88, 8, 3)	PHF(40; 704, 8, 4)
PHF(3; 13, 9, 4) & PHF(2; 13, 9, 3)	PHF(14; 117, 9, 4)
PHF(4; 16, 9, 4) & PHF(2; 16, 9, 3)	PHF(15; 144, 9, 4)
PHF(4; 23, 9, 4) & PHF(3; 23, 9, 3)	PHF(20; 207, 9, 4)
PHF(5; 27, 9, 4) & PHF(3; 27, 9, 3)	PHF(21; 243, 9, 4)
PHF(6; 33, 9, 4) & PHF(3; 33, 9, 3)	PHF(22; 297, 9, 4)
PHF(7; 36, 9, 4) & PHF(3; 36, 9, 3)	PHF(23; 324, 9, 4)
PHF(6; 49, 11, 4) & PHF(3; 49, 11, 3)	PHF(22; 539, 11, 4)
PHF(6; 121, 11, 4) & PHF(4; 121, 11, 3)	PHF(27; 1331, 11, 4)

Ingredients	New PHF
PHF(3; 15, 11, 5) & PHF(3; 15, 11, 4)	PHF(31; 165, 11, 5)
PHF(4; 16, 11, 5) & PHF(3; 16, 11, 4)	PHF(32; 176, 11, 5)
PHF(5; 17, 11, 5) & PHF(3; 17, 11, 4)	PHF(33; 187, 11, 5)
PHF(6; 22, 11, 5) & PHF(4; 22, 11, 4)	PHF(43; 242, 11, 5)
PHF(8; 26, 11, 5) & PHF(4; 26, 11, 4)	PHF(45; 286, 11, 5)
PHF(11; 121, 11, 5) & PHF(6; 121, 11, 4)	PHF(66; 1331, 11, 5)
PHF(3; 18, 13, 5) & PHF(3; 18, 13, 4)	PHF(31; 234, 13, 5)
PHF(4; 20, 13, 5) & PHF(3; 20, 13, 4)	PHF(32; 260, 13, 5)
PHF(6; 27, 13, 5) & PHF(4; 27, 13, 4)	PHF(43; 531, 13, 5)
PHF(7; 28, 13, 5) & PHF(4; 28, 13, 4)	PHF(44; 364, 13, 5)
PHF(11; 123, 13, 5) & PHF(6; 123, 13, 4)	PHF(66; 1599, 13, 5)
PHF(11; 169, 13, 5) & PHF(7; 169, 13, 4)	PHF(75; 2197, 13, 5)
PHF(3; 22, 16, 5) & PHF(3; 22, 16, 4)	PHF(31; 352, 16, 5)
PHF(6; 35, 16, 5) & PHF(4; 35, 16, 4)	PHF(43; 560, 16, 5)
PHF(7; 41, 16, 5) & PHF(4; 41, 16, 4)	PHF(44; 656, 16, 5)
PHF(8; 50, 16, 5) & PHF(5; 50, 16, 4)	PHF(54; 800, 16, 5)
PHF(11; 256, 16, 5) & PHF(7; 256, 16, 4)	PHF(75; 4096, 16, 5)
PHF(7; 43, 17, 5) & PHF(4; 43, 17, 4)	PHF(44; 731, 17, 5)
PHF(3; 27, 19, 5) & PHF(3; 27, 19, 4)	PHF(31; 513, 19, 5)
PHF(8; 55, 19, 5) & PHF(4; 55, 19, 4)	PHF(46; 1045, 19, 5)

Ingredients	New PHF
$\mathsf{PHF}(16;256,16,6)$ & $\mathsf{PHF}(11;256,16,5)$	$\mathsf{PHF}(171;4096,16,6)$
$\mathsf{PHF}(8;33,17,6)$ & $\mathsf{PHF}(5;33,17,5)$	$\mathsf{PHF}(79;561,17,6)$
$\mathsf{PHF}(16;289,17,6)$ & $\mathsf{PHF}(11;289,17,5)$	$\mathsf{PHF}(171;4913,17,6)$
$\mathsf{PHF}(8;38,19,6)$ & $\mathsf{PHF}(5;38,19,5)$	$\mathsf{PHF}(79;722,19,6)$
$\mathsf{PHF}(16;361,19,6)$ & $\mathsf{PHF}(11;361,19,5)$	$\mathsf{PHF}(171;6859,19,6)$
$\mathsf{PHF}(5;33,23,6)$ & $\mathsf{PHF}(3;33,23,5)$	$\mathsf{PHF}(48;759,23,6)$
$\mathsf{PHF}(6;38,23,6)$ & $\mathsf{PHF}(4;38,23,5)$	$\mathsf{PHF}(63;874,23,6)$
$\mathsf{PHF}(8;46,23,6)$ & $\mathsf{PHF}(5;46,23,5)$	$\mathsf{PHF}(79;1058,23,6)$
$\mathsf{PHF}(4;35,25,6)$ & $\mathsf{PHF}(3;35,25,5)$	$\mathsf{PHF}(47;875,23,6)$
$\mathsf{PHF}(5;36,25,6)$ & $\mathsf{PHF}(3;36,25,5)$	$\mathsf{PHF}(48;900,23,6)$
$\mathsf{PHF}(6;49,25,6)$ & $\mathsf{PHF}(5;49,25,5)$	$\mathsf{PHF}(77;1225,25,6)$
$\mathsf{PHF}(7;50,25,6)$ & $\mathsf{PHF}(5;50,25,5)$	$\mathsf{PHF}(78;1250,25,6)$
$\mathsf{PHF}(4;37,27,6)$ & $\mathsf{PHF}(3;37,27,5)$	$\mathsf{PHF}(47;999,27,6)$
$\mathsf{PHF}(5;39,27,6)$ & $\mathsf{PHF}(3;39,27,5)$	$\mathsf{PHF}(48;1053,27,6)$
$\mathsf{PHF}(6;44,27,6)$ & $\mathsf{PHF}(4;44,27,5)$	$\mathsf{PHF}(63;1188,27,6)$
$\mathsf{PHF}(11;69,27,6)$ & $\mathsf{PHF}(5;69,27,5)$	$\mathsf{PHF}(82;1863,27,6)$
$\mathsf{PHF}(4;41,29,6)$ & $\mathsf{PHF}(3;41,29,5)$	$\mathsf{PHF}(47;1189,29,6)$
$\mathsf{PHF}(5;42,29,6)$ & $\mathsf{PHF}(3;42,29,5)$	$\mathsf{PHF}(48;1218,29,6)$
$\mathsf{PHF}(6;49,29,6)$ & $\mathsf{PHF}(4;49,29,5)$	$\mathsf{PHF}(63;1421,29,6)$
$\mathsf{PHF}(11;71,29,6)$ & $\mathsf{PHF}(5;71,29,5)$	$\mathsf{PHF}(72;2059,29,6)$

Table 2: PHFs constructed using Theorem 4.1

Ingredients	New PHF
$\mathsf{PHF}(3;16,10,4)$ & $\mathsf{PHF}(2;16,9,3)$	$\mathsf{PHF}(14;144,10,4)$
$\mathsf{PHF}(5;30,10,4)$ & $\mathsf{PHF}(3;30,9,3)$	$\mathsf{PHF}(21;270,10,4)$
$\mathsf{PHF}(6;36,10,4)$ & $\mathsf{PHF}(3;36,9,3)$	$\mathsf{PHF}(22;324,10,4)$
$\mathsf{PHF}(3;20,12,4)$ & $\mathsf{PHF}(2;20,11,3)$	$\mathsf{PHF}(14;220,12,4)$
$\mathsf{PHF}(6;49,12,4)$ & $\mathsf{PHF}(3;49,11,3)$	$\mathsf{PHF}(22;539,12,4)$
$\mathsf{PHF}(6;121,12,4)$ & $\mathsf{PHF}(4;121,11,3)$	$\mathsf{PHF}(27;1331,12,4)$
$\mathsf{PHF}(3;16,12,5)$ & $\mathsf{PHF}(3;16,11,4)$	$\mathsf{PHF}(31;176,12,5)$
$\mathsf{PHF}(8;31,12,5)$ & $\mathsf{PHF}(5;31,11,4)$	$\mathsf{PHF}(54;341,12,5)$
$\mathsf{PHF}(11;121,12,5)$ & $\mathsf{PHF}(6;121,11,4)$	$\mathsf{PHF}(66;1331,12,5)$
$\mathsf{PHF}(3;19,14,5)$ & $\mathsf{PHF}(3;19,13,4)$	$\mathsf{PHF}(31;209,14,5)$
$\mathsf{PHF}(4;21,14,5)$ & $\mathsf{PHF}(3;21,13,4)$	$\mathsf{PHF}(32;273,14,5)$
$\mathsf{PHF}(8;42,14,5)$ & $\mathsf{PHF}(5;42,13,4)$	$\mathsf{PHF}(54;546,14,5)$
$\mathsf{PHF}(11;123,14,5)$ & $\mathsf{PHF}(6;123,13,4)$	$\mathsf{PHF}(66;1599,14,5)$
$\mathsf{PHF}(11;169,14,5)$ & $\mathsf{PHF}(7;169,13,4)$	$\mathsf{PHF}(75;2197,14,5)$
$\mathsf{PHF}(3;21,15,5)$ & $\mathsf{PHF}(3;21,13,4)$	$\mathsf{PHF}(31;273,15,5)$
$\mathsf{PHF}(8;43,15,5)$ & $\mathsf{PHF}(5;43,13,4)$	$\mathsf{PHF}(54;559,15,5)$
$\mathsf{PHF}(11;123,15,5)$ & $\mathsf{PHF}(6;123,13,4)$	$\mathsf{PHF}(66;1599,15,5)$
$\mathsf{PHF}(11;169,15,5)$ & $\mathsf{PHF}(7;169,13,4)$	$\mathsf{PHF}(75;2197,15,5)$
$\mathsf{PHF}(3;28,20,5)$ & $\mathsf{PHF}(3;28,19,4)$	$\mathsf{PHF}(31;532,20,5)$
$\mathsf{PHF}(4;32,20,5)$ & $\mathsf{PHF}(3;32,19,4)$	$\mathsf{PHF}(32;608,20,5)$
$\mathsf{PHF}(8;55,20,5)$ & $\mathsf{PHF}(4;55,19,4)$	$\mathsf{PHF}(45;1045,20,5)$
$\mathsf{PHF}(3;30,21,5)$ & $\mathsf{PHF}(3;30,19,4)$	$\mathsf{PHF}(31;570,21,5)$
$\mathsf{PHF}(4;33,21,5)$ & $\mathsf{PHF}(3;33,19,4)$	$\mathsf{PHF}(32;627,21,5)$
$\mathsf{PHF}(7;55,21,5)$ & $\mathsf{PHF}(4;55,19,4)$	$\mathsf{PHF}(44;1045,21,5)$

Ingredients	New PHF
$\mathsf{PHF}(7;34,18,6)$ & $\mathsf{PHF}(5;34,17,5)$	$\mathsf{PHF}(78;578,18,6)$
$\mathsf{PHF}(9;39,18,6)$ & $\mathsf{PHF}(6;39,17,5)$	$\mathsf{PHF}(94;663,18,6)$
$\mathsf{PHF}(16;289,18,6)$ & $\mathsf{PHF}(11;289,17,5)$	$\mathsf{PHF}(171;4913,18,6)$
$\mathsf{PHF}(5;30,20,6)$ & $\mathsf{PHF}(4;30,19,5)$	$\mathsf{PHF}(62;570,20,6)$
$\mathsf{PHF}(6;31,20,6)$ & $\mathsf{PHF}(4;31,19,5)$	$\mathsf{PHF}(63;589,20,6)$
$\mathsf{PHF}(16;361,20,6)$ & $\mathsf{PHF}(11;361,19,5)$	$\mathsf{PHF}(171;6859,20,6)$
$\mathsf{PHF}(16;361,21,6)$ & $\mathsf{PHF}(11;361,19,5)$	$\mathsf{PHF}(171;6859,21,6)$
$\mathsf{PHF}(16;361,22,6)$ & $\mathsf{PHF}(11;361,19,5)$	$\mathsf{PHF}(171;6859,22,6)$
$\mathsf{PHF}(4;33,24,6)$ & $\mathsf{PHF}(3;33,23,5)$	$\mathsf{PHF}(47;759,24,6)$
$\mathsf{PHF}(6;38,24,6)$ & $\mathsf{PHF}(4;38,23,5)$	$\mathsf{PHF}(63;874,24,6)$
$\mathsf{PHF}(4;36,26,6)$ & $\mathsf{PHF}(3;36,25,5)$	$\mathsf{PHF}(47;900,26,6)$
$\mathsf{PHF}(5;40,26,6)$ & $\mathsf{PHF}(4;40,25,5)$	$\mathsf{PHF}(62;1000,26,6)$
$\mathsf{PHF}(6;41,26,6)$ & $\mathsf{PHF}(4;41,25,5)$	$\mathsf{PHF}(63;1025,26,6)$
$\mathsf{PHF}(4;39,28,6)$ & $\mathsf{PHF}(3;39,27,5)$	$\mathsf{PHF}(47;1053,28,6)$
$\mathsf{PHF}(10;68,28,6)$ & $\mathsf{PHF}(5;68,27,5)$	$\mathsf{PHF}(81;1836,28,6)$
$\mathsf{PHF}(11;69,28,6)$ & $\mathsf{PHF}(5;69,27,5)$	$\mathsf{PHF}(82;1863,28,6)$
$\mathsf{PHF}(4;42,30,6)$ & $\mathsf{PHF}(3;42,29,5)$	$\mathsf{PHF}(47;1218,30,6)$
$\mathsf{PHF}(4;49,30,6)$ & $\mathsf{PHF}(4;49,29,5)$	$\mathsf{PHF}(61;1421,30,6)$
$\mathsf{PHF}(9;71,30,6)$ & $\mathsf{PHF}(5;71,29,5)$	$\mathsf{PHF}(80;2059,30,6)$

Table 3: PHFs constructed using Theorem 5.1

new PHF
PHF$(26; 7^3 = 343, 7, 4)$
PHF$(26; 9^3 = 729, 9, 4)$
PHF$(26; 8^3 = 512, 8, 4)$
PHF$(26; 11^3 = 1331, 11, 4)$
PHF$(45; 13^4 = 28561, 13, 4)$
PHF$(45; 16^4 = 65536, 16, 4)$

Table 4: PHFs constructed using Theorem 6.6

PHF(11; 10,4,4)	PHF(54; 66,4,4)	PHF(27; 51,5,4)
PHF(34; 66,5,4)	PHF(57; 173,5,4)	PHF(81; 365,5,4)
PHF(103; 2201,5,4)	PHF(111; 2202,5,4)	PHF(115; 2203,5,4)
PHF(156; 6861,5,4)	PHF(165; 6862,5,4)	PHF(169; 6863,5,4)
PHF(178; 6864,5,4)	PHF(226; 130323,5,4)	PHF(237; 130324,5,4)
PHF(243; 130325,5,4)	PHF(254; 130326,5,4)	PHF(260; 130327,5,4)
PHF(21; 12,5,5)	PHF(382; 173,5,5)	PHF(958; 731,5,5)
PHF(83; 62,6,5)	PHF(111; 123,6,5)	PHF(145; 171,6,5)
PHF(169; 173,6,5)	PHF(235; 291,6,5)	PHF(280; 363,6,5)
PHF(300; 364,6,5)	PHF(307; 365,6,5)	PHF(327; 366,6,5)
PHF(358; 531,6,5)	PHF(39; 13,6,6)	PHF(53; 14,6,6)
PHF(666; 66,6,6)	PHF(714; 67,6,6)	PHF(768; 68,6,6)
PHF(1616; 291,6,6)	PHF(1972; 363,6,6)	PHF(2278; 365,6,6)
PHF(2688; 531,6,6)	PHF(284; 66,7,6)	PHF(298; 67,7,6)
PHF(332; 68,7,6)	PHF(352; 69,7,6)	PHF(408; 71,7,6)
PHF(664; 291,7,6)	PHF(8734; 262148,7,6)	PHF(9000; 262149,7,6)

Table 5: Some PHFs constructed using Theorem 7.1

PHF(26; 324,3,3)	PHF(27; 486,3,3)	PHF(39; 972,3,3)
PHF(48; 2731,3,3)	PHF(55; 4573,3,3)	PHF(59; 9762,3,3)
PHF(68; 29128,3,3)	PHF(69; 43691,3,3)	PHF(79; 86881,3,3)
PHF(87; 157464,3,3)	PHF(88; 236196,3,3)	PHF(89; 354294,3,3)
PHF(27; 2048,4,3)	PHF(38; 16384,4,3)	PHF(39; 32768,4,3)
PHF(50; 262144,4,3)	PHF(51; 524288,4,3)	PHF(27; 6250,5,3)
PHF(34; 20262,5,3)	PHF(38; 62500,5,3)	PHF(39; 156250,5,3)
PHF(27; 10924,6,3)	PHF(38; 473286,6,3)	PHF(19; 4184,7,3)
PHF(27; 33614,7,3)	PHF(38; 707468,7,3)	PHF(19; 7141,8,3)
PHF(25; 92824,8,3)	PHF(6; 162,9,3)	PHF(19; 14564,9,3)
PHF(25; 233017,9,3)	PHF(19; 16705,10,3)	PHF(25; 283972,10,3)
PHF(6; 242,11,3)	PHF(9; 2662,11,3)	PHF(25; 450200,11,3)
PHF(40; 36,4,4)	PHF(41; 48,4,4)	PHF(71; 91,4,4)
PHF(119; 217,4,4)	PHF(167; 397,4,4)	PHF(191; 696,4,4)
PHF(192; 927,4,4)	PHF(193; 1236,4,4)	PHF(194; 1648,4,4)
PHF(245; 2304,4,4)	PHF(246; 3072,4,4)	PHF(298; 5145,4,4)
PHF(363; 9126,4,4)	PHF(431; 23196,4,4)	PHF(432; 30927,4,4)
PHF(433; 41235,4,4)	PHF(434; 54980,4,4)	PHF(435; 73306,4,4)
PHF(436; 97741,4,4)	PHF(530; 157411,4,4)	PHF(531; 209881,4,4)
PHF(569; 292969,4,4)	PHF(607; 398581,4,4)	PHF(59; 174,5,4)
PHF(89; 792,5,4)	PHF(90; 1320,5,4)	PHF(129; 2948,5,4)
PHF(181; 7301,5,4)	PHF(206; 28150,5,4)	PHF(207; 46916,5,4)
PHF(208; 78193,5,4)	PHF(265; 167906,5,4)	PHF(64; 1099,6,4)
PHF(131; 32581,6,4)	PHF(132; 65161,6,4)	PHF(170; 139921,6,4)
PHF(40; 407,7,4)	PHF(41; 948,7,4)	PHF(88; 9261,7,4)
PHF(89; 21609,7,4)	PHF(90; 50421,7,4)	PHF(125; 151263,7,4)
PHF(130; 453789,7,4)	PHF(131; 1058841,7,4)	PHF(132; 2470629,7,4)
PHF(41; 1397,8,4)	PHF(89; 36864,8,4)	PHF(90; 98304,8,4)
PHF(75; 93281,9,4)	PHF(75; 117188,10,4)	PHF(5; 33,11,4)
PHF(35; 2567,11,4)	PHF(173; 63,5,5)	PHF(174; 78,5,5)
PHF(175; 97,5,5)	PHF(285; 136,5,5)	PHF(428; 205,5,5)
PHF(747; 424,5,5)	PHF(1209; 1096,5,5)	PHF(1359; 1693,5,5)
PHF(1421; 2553,5,5)	PHF(1422; 3191,5,5)	PHF(1423; 3988,5,5)
PHF(1424; 4985,5,5)	PHF(1425; 6231,5,5)	PHF(1426; 7788,5,5)
PHF(1427; 9734,5,5)	PHF(1553; 12500,5,5)	PHF(1721; 15747,5,5)
PHF(2309; 40523,5,5)	PHF(2540; 55137,5,5)	PHF(2819; 95332,5,5)
PHF(2905; 123955,5,5)	PHF(2906; 154943,5,5)	PHF(2907; 193678,5,5)
PHF(2908; 242097,5,5)	PHF(2909; 302621,5,5)	PHF(2910; 378276,5,5)
PHF(2911; 472844,5,5)	PHF(2912; 591054,5,5)	PHF(2913; 738817,5,5)
PHF(87; 81,6,5)	PHF(626; 2404,6,5)	PHF(627; 3606,6,5)
PHF(628; 5408,6,5)	PHF(629; 8112,6,5)	PHF(1007; 33769,6,5)
PHF(1267; 182424,6,5)	PHF(1268; 273636,6,5)	PHF(1269; 410454,6,5)
PHF(1270; 615681,6,5)	PHF(65; 70,7,5)	PHF(375; 2271,7,5)
PHF(376; 3974,7,5)	PHF(377; 6953,7,5)	PHF(772; 172320,7,5)
PHF(773; 301559,7,5)	PHF(774; 527727,7,5)	PHF(250; 3042,8,5)
PHF(251; 6084,8,5)	PHF(525; 262144,8,5)	PHF(526; 524288,8,5)
PHF(208; 3087,9,5)	PHF(209; 6945,9,5)	PHF(401; 207127,9,5)
PHF(402; 466034,9,5)	PHF(167; 4868,10,5)	PHF(308; 147764,10,5)
PHF(309; 369409,10,5)	PHF(10; 44,11,5)	PHF(120; 5324,11,5)

Table 6: Some PHFs constructed using Theorem 7.2.

9 Conclusions

The construction of perfect hash families is a challenging problem. We have presented many recursive constructions for perfect hash families using combinatorial methods. The new constructions turn out very useful as they produce a great many new perfect hash families for large t. A number of our constructions generalize some recent results. A remarkable fact of combinatorial methods is that they often allow to construct good perfect hash families not only for the case, where v is a prime power, but also for the non-prime power case. We believe that combinatorial methods are powerful and they are worthy of further investigations. The extensive tables included for newly constructed parameters once more bear evidence of the strength of these methods.

References

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

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

[3] S. G. Barwick and Wen-Ai Jackson A sequence approach to linear perfect hash families, preprint.

[4] S. R. Blackburn, "Combinatorics and threshold cryptography", Combinatorial designs and their applications, Chapman and Hall Research Notes in Mathematics **403** (1999), 49–70.

[5] S. R. Blackburn. M. Burmester, Y. Desmedt and P. R. Wild, Efficient multiplicative sharing schemes, Advances in Cryptology-Eurocrypt'96, *Lecture Notes in Computer Science* **1070** (1996), 107–118.

[6] S. R. Blackburn, Perfect hash families: probabilistic methods and explicit constructions, *J Combin. Theory A* **92** (2000), 54–60.

[7] S. R. Blackburn, P. R. Wild, Optimal linear perfect hash families, *J. Combin. Theory A*, **83** (1998), 233–250.

[8] E. F. Brickell, A problem in broacast encryption, 5th Vermont Summer Workshop on Combinatorics and Graph Theory, June 1991.

[9] M. Chateauneuf and D. L. Kreher, On the State of Strength-Three Covering Arrays, *J Combin Designs* **10** (2002), 217–238.

[10] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs*, 2nd Edition Chapman & Hall/CRC, 2007.

[11] C. J. Colbourn, S. S. Martirosyan, Tran van Trung, and R. A. Walker II, Roux-type constructions for covering arrays of strengths three and four, *Des. Codes Cryptography* **41** (2006), 333–57.

[12] Z. J. Czech, G. Havas, and B. S. Majewski, Perfect hashing, *Theor. Comp. Sci.* **182** (1994), 1–143.

[13] A. Fiat and M. Naor, Broadcast encryption, Advances in Cryptology-Crypto'93, *Lecture Notes in Computer Science* **773** (1994), 480–491.

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

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

[16] S. S. Martirosyan and Tran van Trung, On t-covering arrays, *Des. Codes Cryptography* **32** (2004), 323–339.

[17] S. Martirosyan and S. S. Martirosyan, New upper bounds on the cardinality of k-separated set of perfect hash family and a near optimal construction for it. *Transactions of IPIA of NAN RA & YSU* "Mathematical Problems in Computer Science" XXI (2000), 104–115.

[18] S. S. Martirosyan, Perfect Hash Families, Identifiable Parent Property Codes and Covering arrays, Ph.D. Thesis, Instiute for Experimental Mathematics, Universität Duisburg-Essen, Germany, October 2003.

[19] K. Mehlhorn, On the program size of perfect and universal hash functions, *Proceedings of the 23rd IEEE Symposium on Foundation of Computer Science (FOCS'82)* (1982), 170 – 175.

[20] K. Mehlhorn, Data structures and algorithm 1: Sorting and Searching, Springer-Verlag, Berlin, 1984.

[21] R. Safavi-Naini, Y. Wang, Sequential traitor tracing, Advances in Cryptology-Crypto'00, *Lecture Notes in Computer Science* **1880** (2000), 316–332.

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

[23] D. R. Stinson, R. Wei, and L. Zhu, New constructions for perfect hash families and related structures using combinatorial designs and codes, *J. Combin. Designs* **8** (2000), 189–200.

[24] D. Tonien and R. Safavi-Naini, Recursive constructions of secure codes and hash families using difference function families, *J. Combin. Theory A*, **113** (2006), 664–674.

[25] Tran van Trung and S. S. Martirosyan, New constructions for IPP codes, *Des. Codes Cryptography* **35** (2005), 227–239.

[26] R. A. Walker II and C. J. Colbourn, Perfect hash families: constructions and existence, *J. Math. Cryptology*, **1** (2007), 125–150.

[27] R. A. Walker II, Covering arrays and perfect hash families, Ph.D. thesis, Department of Computer Science, Arizona State University, USA, December 2005.

[28] R. A. Walker II, PHF Tables: `http://www.phftables.com`

[29] H. Wang and C. Xing, Explicit constructions of perfect hash families from algebraic curves over finite fields, *J. Combin. Theory A* **93** (2001), 112–124.