Perfect hash families from transversal designs

Jeff H. Dinitz

Department of Mathematics
University of Vermont
Burlington, VT, 05405
U.S.A.

Alan C.H. Ling

Department of Computer Science
University of Vermont
Burlington, VT, 05405
U.S.A.

Douglas R. Stinson*

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

Abstract

In this paper, we investigate some interesting connections between transversal designs and perfect hash families. We introduce a class of transversal designs which can be used to obtain certain perfect hash families. We then give a few constructions of such transversal designs, which yield new perfect hash families.

1 Introduction and definitions

Let n, q, t, and s be positive integers and suppose (to avoid trivialities) that $n > q \geq t \geq 2$. Let V be a set of cardinality n and let W be a set of cardinality q. We say that a function $f : V \to W$ *separates* a subset X of V if f is an injection when restricted

---

to X. An (n, q, t)-*perfect hash family* of *size* s is a collection $\mathcal{F} = \{f_1, f_2, \ldots, f_s\}$ of functions from V to W with property that for all sets $X \subseteq V$ such that $|X| = t$, at least one of the functions $f_1, f_2, \ldots, f_s$ separates X. The notation $\mathrm{PHF}(s; n, q, t)$ is used for an (n, q, t)-perfect hash family of size s. A perfect hash family is *optimal* if s is as small as possible, given n, q, t.

Perfect hash families can be characterized as arrays satisfying certain properties. The following elementary result is well-known.

Theorem 1.1. *A $PHF(s; n, q, t)$ is equivalent to an s by n array A of elements from a q-set F, such that, for any t columns of A, there exists a row of A, say r, such that the entries in the t given columns of row r of A are distinct.*

Proof. Let $\mathcal{F} = \{f_1, f_2, \ldots, f_s\}$ be the s functions in the $\mathrm{PHF}(s; n, q, t)$. Construct an array A whose rows are indexed by the functions $f_1, f_2, \ldots, f_s$ and whose columns are indexed by the elements of V. Then define $A(f_i, v) = f_i(v)$ for all f_i and for all $v \in V$. It is clear that A satisfies the stated properties.

Conversely, if we start with an array A satisfying the stated properties, then we can construct a family of functions $\mathcal{F}$ that comprise a $\mathrm{PHF}(s; n, q, t)$. This is done by reversing the previous construction. $\qquad\square$

Given a $\mathrm{PHF}(s; n, q, t)$, say $\mathcal{F}$, we define the *array representation* of $\mathcal{F}$ to be the array A defined in the proof of Theorem 1.1.

Perfect hash families have been studied for over twenty years; see Mehlhorn [9] for some basic results. There has been some recent interest in combinatorial constructions for perfect hash families. See, for example, Atici *et al* [1], Barwick and Jackson [2, 3], Barwick, Jackson and Quinn [4], Blackburn [6], Blackburn and Wild [7], Stinson, Wei and Zhu [11] and Wang and Xing [12].

In [6], Blackburn proved the following.

Theorem 1.2. *A $PHF(6; p^2, p, 4)$ exists for all prime numbers $p \geq 11$, $p \neq 13$.*

Recently, this result was generalized from primes to prime powers by Barwick, Jackson and Quinn in [4].

Theorem 1.3. [4] *A $PHF(6; p^2, p, 4)$ exists for all prime powers $p \geq 11$, $p \neq 13$.*

In this paper, we give some constructions for $\mathrm{PHF}(6; n^2, n, 4)$ when n is not necessarily a prime power.

2   Transversal designs and perfect hash families

A *transversal design* $\mathrm{TD}(k, n)$ is a triple $(X, \mathcal{G}, \mathcal{B})$ in which the following properties are satisfied:

1. X is a set of kn elements called *points*,

2. $\mathcal{G}$ is a partition of X into k n-subsets of points called *groups*,

3. $\mathcal{B}$ is a set of n^2 k-subsets of points called *blocks*, and

4. every pair of points from different groups is contained in a unique block.

In a transversal design $\mathrm{TD}(k, n)$, a 4-block configuration is called a *Pasch configuration* if

1. the four blocks intersect pairwise in six distinct points, and

2. the six points defined by the pairwise intersection of the four blocks occur in six different groups of the transversal design.

A $\mathrm{TD}(k, n)$ is called *anti-Pasch* if no set of four blocks forms a Pasch configuration.

Remark: The anti-Pasch property has been extensively studied in the context of Steiner triple systems (see for example, [8]). Here we are considering a similar property for transversal designs.

We will prove an interesting connection between anti-Pasch $\mathrm{TD}(6, n)$ and $\mathrm{PHF}(6; n^2, n, 4)$. This result is stated in terms of orthogonal arrays, which we define now. An *orthogonal array* $\mathrm{OA}(k, n)$ is a k by n^2 array, say A, of elements chosen from an n-set Y, such that, for every two rows of A, say r_1 and r_2, it holds that

$$\{(A(r_1, c), A(r_2, c)) : 1 \leq c \leq n^2\} = Y \times Y.$$

It is well-known that a $\mathrm{TD}(k, n)$ is equivalent to an $\mathrm{OA}(k, n)$. Every $\mathrm{TD}(k, n)$ has a natural *orthogonal array representation* obtained as follows. Let $(X, \mathcal{G}, \mathcal{B})$ be a $\mathrm{TD}(k, n)$. Let Y be an n-set, and for $1 \leq i \leq k$ let $\phi_i : G_i \rightarrow Y$ be a bijection. Let the blocks in $\mathcal{B}$ be named B_j, $1 \leq j \leq n^2$. Now construct a k by n^2 array A, where $A(i, j) = \phi_i(B_j \cap G_i)$ for all i, j. It is easy to see that A is an $\mathrm{OA}(k, n)$; we say that A is an orthogonal array that *corresponds* to the transversal design $(X, \mathcal{G}, \mathcal{B})$.

The following theorem provides a connection between transversal designs and perfect hash families.

Theorem 2.1. *Suppose* $(X, \mathcal{G}, \mathcal{A})$ *is a* $\mathrm{TD}(6, n)$ *and let* A *be the corresponding* $\mathrm{OA}(6, n)$. *Then* A *is the array representation of a* $\mathrm{PHF}(6; n^2, n, 4)$ *if and only if* $(X, \mathcal{G}, \mathcal{A})$ *is an anti-Pasch* $\mathrm{TD}(6, n)$.

Proof. Suppose that $(X, \mathcal{G}, \mathcal{A})$ is not anti-Pasch, and let $B_1, B_2, B_3, B_4 \in \mathcal{B}$ be four blocks that form a Pasch configuration. Consider the four corresponding columns in A. In each of the six rows of A, there is a repeated element within these four columns (from property 2 of a Pasch configuration). Therefore A is not the array representation of a $\mathrm{PHF}(6; n^2, n, 4)$.

Conversely, suppose that A is not the array representation of a $\mathrm{PHF}(6; n^2, n, 4)$. Let i, j, k, ℓ be four columns of A for which the perfect hash property is violated.

Therefore, for every row r of A, there is a repeated element in row r within the four given columns. For any 2-subset of the four columns i, j, k, ℓ, there can be at most one row containing a repeated element in the two given columns, because A is an $\mathrm{OA}(6, n)$. Therefore the four blocks in $(X, \mathcal{G}, \mathcal{A})$ correponding to the four rows i, j, k, ℓ form a Pasch configuration, and $(X, \mathcal{G}, \mathcal{A})$ is not anti-Pasch. $\qquad\square$

It can be checked that the constructions for all the $\mathrm{PHF}(6; n^2, n, 4)$ in Theorems 1.2 and 1.3 in fact produce orthogonal arrays $\mathrm{OA}(6, n)$. Hence, by Theorem 2.1, they also yield anti-Pasch $\mathrm{TD}(6, n)$. So, we have the following:

Theorem 2.2. *For all prime powers $p \geq 11$, $p \neq 13$, there is an anti-Pasch $TD(6, p)$.*

In the remainder of this paper, we present constructions for anti-Pasch $\mathrm{TD}(6, n)$ when n is not a prime power.

3 Constructions

We begin with a direct product construction. In this construction and elsewhere, we denote $I_m = \{1, \ldots, m\}$ for a positive integer m.

Theorem 3.1. *If there exists an anti-Pasch $TD(6, n)$ and an anti-Pasch $TD(6, m)$, then there exists an anti-Pasch $TD(6, mn)$.*

Proof. Let $(I_m \times I_6, \{I_m \times \{i\} : i \in I_6\}, \mathcal{B})$ be an anti-Pasch $\mathrm{TD}(6, m)$ and let $(I_n \times I_6, \{I_n \times \{i\} : i \in I_6\}, \mathcal{C})$ be an anti-Pasch $\mathrm{TD}(6, n)$. We construct an anti-Pasch $\mathrm{TD}(6, mn)$, namely, $(X = I_m \times I_n \times I_6, \{I_m \times I_n \times \{i\} : i \in I_6\}, \mathcal{D})$, where the blocks are formed as follows. For $B \in \mathcal{B}, C \in \mathcal{C}$ define

$$D_{B,C} = \{(b, c, i) : (b, i) \in B, (c, i) \in C\}.$$

Then define

$$\mathcal{D} = \{D_{B,C} : B \in \mathcal{B}, C \in \mathcal{C}\}.$$

This is just the standard direct product construction for transversal designs.

Now, suppose there exists a Pasch configuration in this $\mathrm{TD}(6, mn)$, consisting of blocks D_{B_1,C_1}, D_{B_2,C_2}, D_{B_3,C_3}, D_{B_4,C_4}.

Suppose that two of the B_i's are identical, say $B_1 = B_2$. The block D_{B_3,C_3} must intersect both of D_{B_1,C_1} and D_{B_2,C_2}, which can happen only if $B_3 = B_1$. Similarly, we also have $B_4 = B_1$, so all four B_i's are identical. But then C_1, C_2, C_3, C_4 forms a Pasch configuration in the $\mathrm{TD}(6, n)$, which is a contradiction.

In a similar fashion, if two of the C_j's are identical, then B_1, B_2, B_3, B_4 forms a Pasch configuration in the $\mathrm{TD}(6, m)$, which is again a contradiction.

Finally, if all the B_i's are different and all the C_j's are different, then B_1, B_2, B_3, B_4 and C_1, C_2, C_3, C_4 are both Pasch configurations in the respective transversal designs. $\qquad\square$

Our next construction is a simplified Wilson-type construction. For use in this construction, we now obtain some anti-Pasch $TD(7, p)$, where p is prime. Suppose p is a prime, and let $a_1, a_2, \ldots, a_7$ be distinct elements in $\mathbb{Z}_p$, $p \geq 7$. Construct a $TD(7, p)$ on point set $\mathbb{Z}_p \times I_7$, with groups $\mathbb{Z}_p \times \{i\}$ for $i \in I_k$ and blocks

$$\{(m + na_1, 1), (m + na_2, 2), \ldots, (m + na_7, 7)\},$$

for all $m, n \in \mathbb{Z}_p$. It is easy to check that this is indeed a $TD(7, p)$ under the stated hypotheses.

We next investigate conditons on the a_i's which guarantee that the resulting $TD(7, p)$ will be anti-Pasch. Suppose there is a Pasch configuration in which the six points of intersection occur in the first six groups.

Each block is uniquely defined by an ordered pair (m, n). Suppose that the four blocks in the Pasch configutration are defined by the pairs (m_1, n_1), (m_2, n_2), (m_3, n_3) and (m_4, n_4). By permuting the a_i's, we can assume that

$$m_1 + a_1 n_1 = m_2 + a_1 n_2$$
$$m_1 + a_2 n_1 = m_3 + a_2 n_3$$
$$m_1 + a_3 n_1 = m_4 + a_3 n_4$$
$$m_2 + a_4 n_2 = m_3 + a_4 n_4$$
$$m_2 + a_5 n_2 = m_4 + a_5 n_4$$
$$m_3 + a_6 n_3 = m_4 + a_6 n_4$$

Simple computation yields

$$\begin{pmatrix} a_1 - a_4 & a_4 - a_2 & 0 \\ a_1 - a_5 & 0 & a_5 - a_3 \\ 0 & a_2 - a_6 & a_6 - a_3 \end{pmatrix} \begin{pmatrix} n_2 - n_1 \\ n_3 - n_1 \\ n_4 - n_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \qquad (1)$$

Let M denote the 3×3 matrix in Equation (1) above. Suppose that $\det M \not\equiv 0 \bmod p$. Then the only solution to Equation (1) has $n_1 = n_2 = n_3 = n_4$. It then follows that $m_1 = m_2 = m_3 = m_4$, which means that we do not have four different blocks. Hence, the assumed Pasch configuration cannot occur in the transversal design.

In order to show that the $TD(7, p)$ is anti-Pasch, we need to compute 6! determinants for each of the $\binom{7}{6}$ 6-subsets of $\{a_1, \ldots, a_7\}$. If all 7! of these determinants are non-zero modulo p, then we have an anti-Pasch $TD(7, p)$. We record some computational results in Table 1. The entries in the first column are values of $a_1, \ldots, a_7$. The entries in the second column are all the primes p such that $p \geq 50$ and at least one of the relevant determinants is zero modulo p.

From this table, it is clear that, for any prime $p > 50$, there exists at least one 7-set of a_i's such that the 720 determinants are non-zero modulo p. Hence, the $TD(7, p)$ constructed by using the corresponding a_i's is anti-Pasch. We record this result in the following theorem.

$a_1, a_2, \ldots, a_7$	primes $p \geq 50$ except
$1, 2, 3, 4, 8, 13, 15$	$53, 59, 61, 67, 71, 97, 103, 127, 131, 139, 163, 223, 191, 467,$
	$593, 397, 167, 811$
$1, 2, 3, 4, 8, 11, 13$	$53, 59, 71, 79, 97, 107, 109, 113, 151, 227$
$1, 2, 3, 4, 8, 13, 19$	$53, 59, 61, 71, 79, 83, 89, 103, 113, 131, 631, 349, 661, 197,$
	$239, 263, 191$
$1, 3, 5, 7, 9, 13, 19$	$61, 73, 79$

Table 1: Possible exceptions for anti-Pasch $\mathrm{TD}(7, p)$, p prime

Theorem 3.2. *If p is a prime and $p \geq 50$, then there exists an anti-Pasch $\mathrm{TD}(7, p)$.*

We next explore a Wilson-type construction.

Theorem 3.3. *Suppose there exists an anti-Pasch $\mathrm{TD}(7, n)$, an anti-Pasch $\mathrm{TD}(6, m)$ and an anti-Pasch $\mathrm{TD}(6, m+1)$. Then there exists an anti-Pasch $\mathrm{TD}(6, mn+1)$.*

Proof. Assume the groups of the $\mathrm{TD}(7, n)$ are $I_n \times \{i\}$ for $i \in I_7$, the groups of the $\mathrm{TD}(6, m)$ are $I_m \times \{i\}$ for $i \in I_6$ and the groups of the $\mathrm{TD}(6, m+1)$ are $(I_m \cup \{\infty\}) \times \{i\}$ for $i \in I_6$. We further assume that, in the $\mathrm{TD}(6, m+1)$, there is a block of the form $\{(\infty, 1), (\infty, 2), \ldots, (\infty, 6)\}$. We will construct a $\mathrm{TD}(6, mn+1)$ that has groups $((I_n \times I_m) \cup \{\infty\}) \times \{i\}$ for $i \in I_6$. The blocks of the $\mathrm{TD}(6, mn+1)$ are defined as follows:

type 1 blocks

For every block in the $\mathrm{TD}(7, n)$ that does not contain the point $(1, 7)$ (say the block is $\{(a_1, 1), (a_2, 2), \ldots, (a_7, 7)\}$ with $a_7 \neq 1$) construct m^2 blocks of the form

$$\{(a_1, b_1, 1), (a_2, b_2, 2), \ldots, (a_6, b_6, 6)\},$$

where $\{(b_1, 1), (b_2, 2), \ldots, (b_6, 6)\}$ is a block in the $\mathrm{TD}(6, m)$.

type 2 blocks

For every block in the $\mathrm{TD}(7, n)$ that contains the point $(1, 7)$ (say the block is $\{(a_1, 1), (a_2, 2), \ldots, (1, 7)\}$), construct $(m+1)^2 - 1$ blocks of the form

$$\{(a_1, b_1, 1), (a_2, b_2, 2), \ldots, (a_6, b_6, 6)\},$$

where $\{(b_1, 1), (b_2, 2), \ldots, (b_6, 6)\}$ is a block in the $\mathrm{TD}(6, m+1)$ other than $\{(\infty, 1), (\infty, 2), \ldots, (\infty, 6)\}$.

type 3 blocks

Finally, include the block $\{(\infty, 1), (\infty, 2), \ldots, (\infty, 6)\}$ in the $\mathrm{TD}(6, mn+1)$.

It is easy to see that this is just the standard Wilson construction for transveral designs (see [13]), where we give a weight of one to one point in the last group (and a weight of zero to all other points in this group). Observe that every block in the

TD$(7, n)$ gives rise to a sub-TD$(6, m)$ (from type 1 blocks) or a sub-TD$(6, m + 1)$ (from blocks of types 2 and 3) in the TD$(6, mn + 1)$. These sub-TDs are isomorphic to the TD$(6, m)$ or TD$(6, m + 1)$ (respectively) which are hypothesized to exist in the statement of the theorem.

We now prove that the TD$(6, mn + 1)$ is anti-Pasch. Suppose there exists a Pasch configuration in the TD$(6, mn + 1)$. First, assume that one of the blocks in the Pasch configuration is $\{(\infty, 1), (\infty, 2), \ldots, (\infty, 6)\}$. Then the other three blocks come from blocks in the TD$(7, n)$ that contain the point $(0, 7)$. These three blocks have no other point of intersection, and it follows that we cannot have a Pasch configuration in this case. Therefore, we can assume that all blocks in the Pasch configuration are of type 1 or type 2.

Next, if two of the four blocks in the Pasch configuration come from the same sub-TD, then all four blocks must come from the same sub-TD. This means that there is a Pasch configuration in the TD$(6, m)$ or in the TD$(6, m + 1)$, which is a contradiction. Therefore, we can assume that the four blocks in the Pasch configuration are in four different sub-TDs. We split the argument into cases.

Case 1: Suppose that the Pasch configuration does not contain any point of the form (∞, i). Since all four blocks are from different sub-TDs, we a can restrict them to the set $I_n \times I_6$ by ignoring their second coordinates. The result is a Pasch configuration in the TD$(6, n)$, which is a contradication.

Case 2: Suppose that the Pasch configuration contains exactly one point of the form (∞, i). Then the two blocks in the Pasch configuration that intersect at the point (∞, i) must originate from two distinct blocks in the TD$(7, n)$ containing the point $(1, 7)$. The remaining two blocks must correspond to another two blocks in the TD$(7, n)$. These four blocks form a Pasch configuration in the TD$(7, n)$ that includes the point $(1, 7)$, contradicting the assumption that the TD$(7, n)$ is anti-Pasch.

Case 3: Suppose the Pasch configuration contains exactly two points of the form (∞, i), say (∞, i) and (∞, j). The two blocks in the Pasch configuration that intersect at (∞, i) must come from two different blocks in the TD$(7, n)$ that contain the point $(1, 7)$. Similarly, two blocks in the Pasch configuration that intersect at (∞, j) must come from two other blocks in the TD$(7, n)$ that contain the point $(1, 7)$. These four blocks in the TD$(7, n)$ have no other point of intersection, and it follows that we cannot have a Pasch configuration in this case.

Case 4: If the Pasch configuration contains more than two points of the form (∞, i) then it must contain the block $\{(\infty, 1), (\infty, 2), \ldots, (\infty, 6)\}$. We already showed that this is impossible.

□

$mn+1$	n	m
849	53	16
945	59	16
1137	71	16
1169	73	16
1265	79	16
1329	83	16
1617	101	16
1644	53	31
1713	107	16
1745	109	16
1830	59	31
1892	61	31
1937	121	16

Table 2: New examples of anti-Pasch TD$(6, mn + 1)$ constructed using Theorem 3.3

We construct anti-Pasch TD$(6, mn + 1)$ for several orders using Theorem 3.3, where the required anti-Pasch TD$(7, n)$ come from Lemma 3.2 and anti-Pasch TD$(6, m)$ and anti-Pasch TD$(6, m + 1)$ come from Theorem 2.2. These constructions are summarized in Table 2. Note that in each of these cases $mn + 1$ is not a prime power, and hence these orders were all previously unknown.

4   A construction using anti-Pasch pairwise balanced designs

Let K be a subset of positive integers. A *pairwise balanced design* PBD(v, K) is a pair $(X, \mathcal{B})$ where X is a finite set of v *points* and $\mathcal{B}$ is a family of subsets of X (called *blocks*) such that $|B| \in K$ for every $B \in \mathcal{B}$, and every pair of distinct points occurs in exactly one block in $\mathcal{B}$. A PBD(v, K) is *anti-Pasch* if no set of four blocks in the design pairwise intersect in six distinct points.

An anti-Pasch TD$(6, n)$ is *idempotent* if the anti-Pasch TD$(6, n)$ contains a set of n pairwise disjoint blocks. It is easy to observe that every anti-Pasch TD$(6, n)$ that we have used and constructed in this paper is idempotent. The next construction uses anti-Pasch PBD(v, K) and idempotent, anti-Pasch TD$(6, k)$ to construct idempotent anti-Pasch TD$(6, v)$.

Theorem 4.1. *If there exists an anti-Pasch PBD(v, K), and, for every $k \in K$, there exists an idempotent, anti-Pasch TD$(6, k)$, then there exists an idempotent anti-Pasch TD$(6, v)$.*

Proof. We apply the standard Bose-Shrikhande-Parker PBD construction for idempotent transversal designs. Suppose A_1, A_2, A_3, A_4 are four blocks in a Pasch configuration in the constructed anti-Pasch TD$(6, v)$. If two of the four blocks are from the

same transversal design $TD(6, k)$, then all four blocks come from the same transversal design, and hence the $TD(6, v)$ contains a Pasch configuration. However, if all four blocks come from different transversal designs, then there is a Pasch configuration in the $PBD(v, K)$. $\square$

One way to obtain anti-Pasch $PBD(v, K)$ is by deleting points from an anti-Pasch BIBD. Anti-Pasch BIBDs can be constructed from finite geometries. The following result in [10] is obtained from the unital in $PG(2, q^2)$ whenever q is a prime power.

Theorem 4.2. [10] *There exists a anti-Pasch BIBD*$(q^3 + 1, q + 1, 1)$ *whenever q is a prime power.*

If we delete a block from an anti-Pasch BIBD$(q^3 + 1, q + 1, 1)$, then we get an anti-Pasch PBD$(q^3 - q, \{q, q + 1\})$. Applying Theorems 4.2, 4.1 and 2.2, we have the following result.

Theorem 4.3. *Suppose q and $q + 1$ are both prime powers, where $q \geq 16$. Then there is an anti-Pasch $TD(6, q^3 - q)$.*

As an example, if we let $q = 16$, then we get an anti-Pasch $TD(6, 15 \times 16 \times 17)$.

References

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

[2] S.G. Barwick and W.-A. Jackson, A sequence approach to constructing perfect hash families, Cryptology ePrint Archive: Report 2005/465, http://eprint.iacr.org/2005/465

[3] S.G. Barwick and W.-A. Jackson, Geometric constructions of optimal linear perfect hash families, Cryptology ePrint Archive: Report 2006/002, http://eprint.iacr.org/2006/002

[4] S.G. Barwick, W.-A. Jackson and C.T. Quinn, Optimal linear perfect hash families with small parameters, *J. Combin. Des.* **12** (2004), 311–324.

[5] T. Beth, D. Jungnickel and H. Lenz, *Design Theory, Second Edition*, Cambridge University Press, 1999.

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

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

[8] M.J. Grannell, T.S. Griggs and C.A.Whitehead, The resolution of the anti-Pasch conjecture, *J. Combin. Des.* **8** (2000), 300–309.

[9] K. Mehlhorn, *Data Structures and Algorithms 1: Sorting and Searching*, Springer-Verlag, 1984.

[10] M.E. O'Nan, Automorphisms of unitary block designs, *J. Algebra* **20** (1972), 495–511.

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

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

[13] R.M. Wilson, Concerning the number of mutually orthogonal Latin squares, *Discrete Math.* **9** (1974), 181–198.