ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 14 (2008) 1–13

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Geometric constructions of optimal linear perfect hash families ☆

S.G. Barwick *, Wen-Ai Jackson

School of Pure Mathematics, University of Adelaide, Adelaide 5005, Australia

Received 5 August 2004; revised 6 September 2006

Available online 13 November 2007

Communicated by Gary L. Mullen

Abstract

A linear (q^d, q, t)-perfect hash family of size s in a vector space V of order q^d over a field F of order q consists of a sequence $\phi_1, \ldots, \phi_s$ of linear functions from V to F with the following property: for all t subsets $X \subseteq V$ there exists $i \in \{1, \ldots, s\}$ such that ϕ_i is injective when restricted to F. A linear (q^d, q, t)-perfect hash family of minimal size $d(t-1)$ is said to be optimal. In this paper we use projective geometry techniques to completely determine the values of q for which optimal linear $(q^3, q, 3)$-perfect hash families exist and give constructions in these cases. We also give constructions of optimal linear $(q^2, q, 5)$-perfect hash families.

Keywords: Projective planes; Linear perfect hash families

1. Introduction to perfect hash families

Perfect hash families were introduced by Mehlhorn [11] in 1984 as part of compiler design. In the last few years, perfect hash families have proved useful in a large variety of applications, in particular, there have been a number of recent applications to cryptography. For example, to threshold cryptography (see Blackburn, Burmester, Desmedt and Wild [8] and Blackburn [6]), to broadcast encryption (see Fiat and Naor [10]). They have also been used to improve explicit

☆ This work was supported by the Australian Research Council.

* Corresponding author.

E-mail address: sbarwick@maths.adelaide.edu.au (S.G. Barwick).

1071-5797/$ – see front matter

doi:10.1016/j.ffa.2007.09.003

constructions of secure frameproof codes, key distribution patterns, group testing algorithms, cover free families and separating systems (see Stinson, van Trung and Wei [12]).

Let s, t, n, q be positive integers and let V be a set of size n and let F be a set of size q. A function $\phi: V \to F$ *separates* a subset X of V if ϕ is an injection when restricted to X. An (n, q, t)*-perfect hash family* of *size* s is a set $S = \{\phi_1, \ldots, \phi_s\}$ of s functions from V to F with the property that for all t-subsets $X \subseteq V$, at least one of $\phi_1, \ldots, \phi_s$ separates X.

We say that S is a *linear* perfect hash family if F can be identified with a finite field GF(q) and V can be identified with a vector space over GF(q) in such a way that S is a set of linear functions under this identification. Thus in the linear case, q is a prime power and $n = q^d$ for some integer $d \geqslant 2$. This paper deals with linear perfect hash families and throughout we use q to denote a prime power. Linear perfect hash families also have a geometric interpretation which is described in Section 2.1.

Blackburn and Wild [9] showed that if $d \geqslant 2$ and $t \geqslant 2$ then a linear (q^d, q, t)-perfect hash family S has size $|S| \geqslant d(t-1)$. If $|S| = d(t-1)$ then S is called *optimal*. Blackburn and Wild give conditions on the existence of optimal linear perfect hash families and show that an optimal linear (q^d, q, t)-perfect hash family S exists if $q \geqslant (\frac{1}{2}t(t-1))^{d(t-1)}$.

Perfect hash families are hard to construct. There are few known constructions of optimal linear perfect hash families. Blackburn and Wild give a general construction of an optimal linear perfect hash family which works for q much larger than their bound and of a certain form, namely $q = q_0^{\alpha_1\alpha_2\cdots\alpha_{d(t-2)}}$ where q_0 is any prime power and $\alpha_i \geqslant d$ for $1 \leqslant i \leqslant d(t-2)$. Blackburn [7] gives a construction of optimal linear $(p^2, p, 4)$-perfect hash families where p is a prime, $p = 11$ or $p \geqslant 17$. Wang and Xing [13] construct linear perfect hash families but their constructions are not optimal. In [3] the authors use geometric techniques to show that optimal $(q^2, q, 4)$-linear perfect hash families exist if $q = 11$ or $q \geqslant 17$ and constructions are given for each such q. The techniques used in the paper are geometric. In [1,2], recursive algorithms for constructing perfect hash families are given. These algorithms need as input perfect hash families with small parameters. This gives some motivation for constructing small perfect hash families.

In this paper we completely determine the values of (prime power) q for which optimal linear $(q^3, q, 3)$-perfect hash families exist, and provide constructions for all values of q where they do exist. We also find a surprising relation between these and optimal linear $(q^2, q, 4)$-perfect hash families. We also consider the case $d = 2, t = 5$ and give constructions of optimal linear $(q^2, q, 5)$-perfect hash families.

2. Optimal linear $(q^3, q, 3)$-perfect hash families

2.1. Geometric interpretation

Linear (q^d, q, t)-perfect hash families have a geometric interpretation described in [9]. We detail this interpretation for the case $d = 3$, $t = 3$. For more details on projective geometry, see [5]. We can identify the elements of V with the points of the affine geometry AG$(3, q)$ of dimension 3 over GF(q). For any linear function $\phi: V \to$ GF(q) and any element $\gamma \in$ GF(q) the elements $v \in V$ with $\phi(v) = \gamma$ correspond to points in a plane of AG$(3, q)$ and so ϕ corresponds to a parallel class of planes. The function ϕ *separates* a set $\mathcal{K}$ of 3 points of AG(d, q) if each point in $\mathcal{K}$ lies in a different plane in the parallel class corresponding to ϕ. We can extend AG$(3, q)$ to a projective space PG$(3, q)$ be adding π_∞, a plane at infinity. The parallel planes of AG$(3, q)$ corresponding to ϕ all contain a line ℓ_ϕ of π_∞, and conversely, each line of π_∞ determines a parallel class of planes. Hence we may identify ϕ with the line ℓ_ϕ. Note that for $\lambda \in \mathrm{GF}(q)$, ϕ and $\lambda\phi$ are identified with the same line ℓ_ϕ.

So a linear $(q^3, q, 3)$-perfect hash family $S = \{\phi_1, \ldots, \phi_k\}$ corresponds to a set $\mathcal{S} = \{\ell_{\phi_1}, \ldots, \ell_{\phi_k}\}$ of k lines of π_∞. The property that S is a perfect hash family means that given a set $\mathcal{K}$ of 3 points in $\mathrm{AG}(3, q)$, there exists at least one i $(1 \leqslant i \leqslant k)$ such that each of the planes through ℓ_{ϕ_i} contain at most one point of $\mathcal{K}$. Two points of $\mathrm{AG}(3, q)$ belong to different planes of the parallel class through ℓ_{ϕ_j} if and only if the projective line joining them meets π_∞ in a point that is not in ℓ_{ϕ_j}. The *shadow* of a set $\mathcal{K} = \{P_1, P_2, P_3\}$ of 3 distinct points of $\mathrm{AG}(3, q)$ is the set of three points $\mathcal{X} = \{P_i P_j \cap \pi_\infty, 1 \leqslant i < j \leqslant 3\}$ in π_∞. Note that if P_1, P_2, P_3 are collinear, then the three points in $\mathcal{X}$ coincide, otherwise, the three points in $\mathcal{X}$ are distinct and collinear. Thus $S = \{\phi_1, \ldots, \phi_k\}$ is a linear $(q^3, q, 3)$-perfect hash family if for any 3-set $\mathcal{K}$ in $\mathrm{AG}(3, q)$, there is at least one line of $\mathcal{S}$ disjoint from the shadow of $\mathcal{K}$. As noted in [9], if $\mathcal{S}$ is optimal, then it is a necessary condition that the lines in $\mathcal{S}$ form a dual arc of π_∞, that is, no three lines in $\mathcal{S}$ are concurrent (or equivalently, no 3 functions in the perfect hash family are dependent).

The elements of a perfect hash family are lines in $\pi_\infty \cong \mathrm{PG}(2, q)$, so we work with homogeneous coordinates in $\mathrm{PG}(2, q)$. A point of $\mathrm{PG}(2, q)$ has homogeneous coordinates (x_0, x_1, x_2) where $(x_0, x_1, x_2) \equiv \rho(x_0, x_1, x_2)$ for any $\rho \in \mathrm{GF}(q) \setminus \{0\}$. A line of $\mathrm{PG}(2, q)$ is the set of points (x_0, x_1, x_2) satisfying a homogeneous equation $ax_0 + bx_1 + cx_2 = 0$, we usually refer to a line using its homogeneous coordinates $[a, b, c]$.

Note that the line $\ell_\phi = [a, b, c]$ in π_∞ corresponds to the linear function $\phi: V \to \mathrm{GF}(q)$ where $\phi(x, y, z) = ax + by + cz$. This is because $\phi(x_1, y_1, z_1) = \phi(x_2, y_2, z_2)$ if and only if $\phi(x_1 - x_2, y_1 - y_2, z_1 - z_2) = 0$. This happens if and only if the line joining the two points $(x_1, y_1, z_1, 1)$ and $(x_2, y_2, z_2, 1)$ in $\mathrm{AG}(3, q)$ meets π_∞ in a point of the line $[a, b, c]$.

2.2. Constructions

In this section we completely determine the existence of optimal linear $(q^3, q, 3)$-perfect hash families and provide constructions in the cases where they exist. Note that by definition of a linear perfect hash family, q must be a prime power.

An optimal linear $(q^3, q, 3)$-perfect hash family $\mathcal{S}$ has size $d(t - 1) = 6$. Thus $\mathcal{S}$ consists of 6 lines in $\pi_\infty \cong \mathrm{PG}(2, q)$ such that given any 3-set $\mathcal{K}$ in $\mathrm{AG}(3, q)$ at least one of the lines in $\mathcal{S}$ is disjoint from the shadow of $\mathcal{K}$. Without loss of generality, we only consider 3-sets $\mathcal{K}$ consisting of three distinct non-collinear points. Thus the shadow of $\mathcal{K}$ consists of a set $\mathcal{X}$ of three distinct collinear points in π_∞. Conversely, it is easy to see that given any set $\mathcal{X}$ of three distinct collinear points in π_∞, there exists a 3-set in $\mathrm{AG}(2, q)$ whose shadow is $\mathcal{X}$. Thus we want to find a set $\mathcal{S}$ of 6 lines in $\mathrm{PG}(2, q)$ such that given any set $\mathcal{X}$ of three collinear points, at least one of the lines of $\mathcal{S}$ is disjoint from $\mathcal{X}$.

We now verify that the 6 lines $\{\ell_{\phi_1}, \ell_{\phi_2}, \ell_{\phi_3}, \ell_{\phi_4}, \ell_{\phi_5}, \ell_{\phi_6}\}$ in $\mathcal{S}$ must form a dual arc. Suppose not, so suppose that $\ell_{\phi_1}, \ell_{\phi_2}, \ell_{\phi_3}$ meet in a point P. Let $Q = \ell_{\phi_4} \cap \ell_{\phi_5}$ and let $R = PQ \cap \ell_{\phi_6}$. Then $\{P, Q, R\}$ is a set of 3 collinear points contained in $\{\ell_{\phi_1}, \ldots, \ell_{\phi_6}\}$ and so $\mathcal{S}$ is not a perfect hash family.

Given a set $\mathcal{S}$ of 6 lines, we can partition $\mathcal{S}$ into 3 pairs of 2 lines, and each pair of lines meets in a point. So each partition of $\mathcal{S}$ gives us 3 points. If these 3 points are collinear, then we can find a set $\mathcal{K}$ whose shadow consists of these 3 points and so $\mathcal{S}$ is not a perfect hash family. Thus we are looking for a set $\mathcal{S}$ where for any such partition, the 3 points are not collinear.

In order to construct such sets $\mathcal{S}$, we found it easier to work with the dual object. That is, such a perfect hash family corresponds to a set $\mathcal{S}$ of 6 points (on an arc) that do not lie on 3 concurrent

Table 1
The 10 bisecants of $\mathcal{S}'$

$[0, 1, 0]$	$[1, -1, 0]$	$[a, -1, 0]$	$[0, a, -1]$	$[a, -a-1, 1]$
$[ab, -a-b, 1]$	$[0, 1, -1]$	$[b, -1, 0]$	$[0, b, -1]$	$[b, -b-1, 1]$

lines. To check this condition, we look at all the sets of 3 lines partitioning the 6 points and we require them to be non-concurrent.

Suppose we start with 5 points $\mathcal{S}'$ that form an arc, we count the number of conditions that a 6th point must satisfy in order to complete $\mathcal{S}'$ to a perfect hash family. First note that the 6th point and $\mathcal{S}'$ must form an arc, so the 6th point cannot lie on any of the $\binom{5}{2} = 10$ bisecants of $\mathcal{S}'$ (that is, lines joining 2 points of $\mathcal{S}'$). We show that there are another 15 lines that the 6th point cannot lie on. Let $\mathcal{S}' = \{P_1, P_2, P_3, P_4, P_5\}$, then for example, the 6th point cannot lie on the line joining $P_1P_2 \cap P_3P_4$ and P_5. We need to count the number of ways that we can form such a line. First pick a point X from $\mathcal{S}'$ ($X = P_5$ in the above example), there are 5 ways to do this. Then partition the remaining 4 points in $\mathcal{S}'$ into 2 pairs and consider the lines ℓ, m joining them, there are 3 ways to do this. As above, the 6th point cannot lie on the line through $\ell \cap m$ and X. Thus $5 \times 3 = 15$ lines are eliminated.

We now coordinatise the plane so that we can find these 15 eliminated lines and the 10 bisecants of $\mathcal{S}'$. We do all our calculations in $\pi_\infty \cong \mathrm{PG}(2, q)$. We use the fact that in $\mathrm{PG}(2, q)$, any 5-arc (5 points, no three collinear) lies on a unique conic. Further, any conic of $\mathrm{PG}(2, q)$ is equivalent to the conic $\mathcal{C} = \{(0, 0, 1)\} \cup \{(1, \alpha, \alpha^2)\colon \alpha \in \mathrm{GF}(q)\}$. Since our 5 points in $\mathcal{S}'$ must lie on an arc, without loss of generality we can assume that $\mathcal{S}' = \{(0, 0, 1), (1, 0, 0), (1, 1, 1), (1, a, a^2), (1, b, b^2)\}$ for some distinct $a, b \in \mathrm{GF}(q)$, $a, b \neq 0, 1$.

It is straightforward to calculate the coordinates of the 10 bisecants of $\mathcal{S}'$, they are given in Table 1.

We now calculate the coordinates of the 15 eliminated lines. To find the first eliminated line, let ℓ be the line joining $(1, 1, 1)$ and $(1, b, b^2)$ and let m be the line joining $(1, 0, 0)$ and $(1, a, a^2)$. The line ℓ has coordinates $[b, -b-1, 1]$ and m has coordinates $[0, -a, 1]$, and the point $A = \ell \cap m$ has coordinates $A = (a-b-1, -b, -ab)$. Finally we need to find the line joining A and $X = (0, 0, 1)$; this line has coordinates $[b, a-b-1, 0]$. This corresponds to the first row in Table 2. We do this for all 15 cases, and the 15 eliminated lines obtained are detailed in Table 2.

To construct a perfect hash family, we need to add a 6th point P_6 to $\mathcal{S}'$ which does not lie on any of these 15 eliminated lines and such that $\mathcal{S}' \cup P_6$ is an arc (that is, P_6 does not lie on any of the 10 bisecants of $\mathcal{S}'$). We first consider the case where P_6 lies on the same conic as the points in $\mathcal{S}'$, that is $P_6 = (1, x, x^2)$ for some $x \in \mathrm{GF}(q)$, $x \neq \infty, 0, 1, a, b$, and so $\mathcal{S}' \cup P_6$ is an arc (so P_6 does not lie on any of the 10 bisecants of $\mathcal{S}'$). The condition that P_6 does not lie on the first eliminated line $[b, a-b-1, 0]$ means that $x \neq \frac{b}{a-b-1}$. In total we obtain 15 conditions from the 15 eliminated lines, these are listed in Table 3.

We note that these are exactly the same 15 conditions obtained in [3] for the case $d = 2$, $t = 4$. For example, the first condition here means that P_6 cannot be $(1, \frac{b}{a-b-1}, (\frac{b}{a-b-1})^2)$. This corresponds to point $T2$ in [3] where the excluded point is $(1, \frac{b}{a-b-1}, 0)$. Note that if $a-b-1 = 0$, then using the homogeneity of the coordinates, the above condition becomes $P_6 \neq (0, 0, 1)$ (this corresponds to the case $T2 = (0, 1, 0)$ in [3]). Thus we can use the constructions obtained there for this case. We give the constructions in the next theorem; we have dualised back, so we list the 6 lines in $\pi_\infty \cong \mathrm{PG}(2, q)$ that form the perfect hash family.

Table 2
The 15 eliminated lines

	X	$\ell \cap m$	Eliminated line
1	(0,0,1)	$(a-b-1,-b,-ab)$	$[b,a-b-1,0]$
2	(0,0,1)	$(1-a-b,-ab,-ab)$	$[ab,1-a-b,0]$
3	(0,0,1)	$(-b+a+1,a,ab)$	$[-a,-b+a+1,0]$
4	(1,0,0)	$(1,a,ab+a-b)$	$[0,-ab-a+b,a]$
5	(1,0,0)	$(1,b,ab+b-a)$	$[0,-ab-b+a,b]$
6	(1,0,0)	$(-1,-1,-a-b+ab)$	$[0,a+b-ab,-1]$
7	(1,1,1)	$(1,b,ab)$	$[b-ab,-1+ab,1-b]$
8	(1,1,1)	$(1,a,ab)$	$[a-ab,-1+ab,1-a]$
9	(1,1,1)	$(1,0,-ab)$	$[-ab,ab+1,-1]$
10	$(1,a,a^2)$	$(1,1,b)$	$[ab-a^2,a^2-b,1-a]$
11	$(1,a,a^2)$	$(-1,0,b)$	$[-ab,b+a^2,-a]$
12	$(1,a,a^2)$	$(1,b,b)$	$[ab-a^2b,a^2-b,b-a]$
13	$(1,b,b^2)$	$(1,1,a)$	$[ab-b^2,b^2-a,1-b]$
14	$(1,b,b^2)$	$(-1,0,a)$	$[-ab,a+b^2,-b]$
15	$(1,b,b^2)$	$(1,a,a)$	$[ab-b^2a,b^2-a,a-b]$

Table 3
The 15 conditions when P_6 is on the conic

	Eliminated line coordinates	Condition
1	$[-b,-a+b+1,0]$	$x \neq \frac{b}{-a+b+1}$
2	$[ab,1-a-b,0]$	$x \neq \frac{-ab}{1-a-b}$
3	$[-a,-b+a+1,0]$	$x \neq \frac{a}{a-b+1}$
4	$[0,-ab-a+b,a]$	$x \neq \frac{ab+a-b}{a}$
5	$[0,-ab-b+a,b]$	$x \neq \frac{ab+b-a}{b}$
6	$[0,a+b-ab,-1]$	$x \neq a+b-ab$
7	$[b-ab,-1+ab,1-b]$	$x \neq \frac{ab-b}{b-1}$
8	$[a-ab,-1+ab,1-a]$	$x \neq \frac{ab-a}{a-1}$
9	$[-ab,ab+1,-1]$	$x \neq ab$
10	$[ab-a^2,a^2-b,1-a]$	$x \neq \frac{a-b}{a-1}$
11	$[-ab,b+a^2,-a]$	$x \neq \frac{b}{a}$
12	$[ab-a^2b,a^2-b,b-a]$	$x \neq \frac{b-ab}{b-a}$
13	$[ab-b^2,b^2-a,1-b]$	$x \neq \frac{b-a}{b-1}$
14	$[-ab,a+b^2,-b]$	$x \neq \frac{a}{b}$
15	$[ab-b^2a,b^2-a,a-b]$	$x \neq \frac{a-ab}{a-b}$

Theorem 2.1. *Optimal linear $(q^3,q,3)$-perfect hash families exist for prime powers $q=11$, $q>13$. The following are examples for each such q.*

(A) *Let $q=p^h$, where $p=11$ or p is a prime greater than 13. Then $\{[0,0,1], [1,0,0], [1,1,1], [1,2,2^2], [1,3,3^2], [1,5,5^2]\}$ is a linear $(q^3,q,3)$-perfect hash family.*

(B) *Let* $q = r^i$, $r \geqslant 4$, $i \geqslant 2$. *Let* $\{0, 1, a, b\} \subseteq \mathrm{GF}(r)$ *and let* $\alpha \in \mathrm{GF}(r^i) \setminus \mathrm{GF}(r)$. *Then* $\{[0,0,1], [1,0,0], [1,1,1], [1,a,a^2], [1,b,b^2], [1,\alpha,\alpha^2]\}$ *is a linear* $(q^3, q, 3)$*-perfect hash family.*
(C) *Let* $q = 2^h$, $h \geqslant 5$, *and let* α *be a generator of* $\mathrm{GF}(2^h)$. *Then* $\{[0,0,1], [1,0,0], [1,1,1], [1,\alpha,\alpha^2], [1,\alpha^2,\alpha^4], [1,\alpha^4,\alpha^8]\}$ *is a linear* $(q^3, q, 3)$*-perfect hash family.*
(D) *Let* $q = 3^h$, $h \geqslant 3$, *and let* α *be a generator of* $\mathrm{GF}(3^h)$. *Then* $\{[0,0,1], [1,0,0], [1,1,1], [1,\alpha,\alpha^2], [1,\alpha^2,\alpha^4], [1,\alpha^4,\alpha^8]\}$ *is a linear* $(q^3, q, 3)$*-perfect hash family.* (*For* $h = 3$ *and* $h \geqslant 5$, α *can be any generator, but for* $h = 4$, α *must be chosen carefully.*)

Proof. This follows directly from the constructions in [3]. □

We note that it is difficult to explain geometrically why the conditions for the cases $d = 2$, $t = 4$ and $d = 3$, $t = 3$ are the same. However, if we look at perfect hash families as sequences (using the model described in [9]) then it is possible to explain this surprising relation. The reader should consult [4] for a detailed description of the sequence model of perfect hash families, and an explanation of the relationship between these two cases.

To investigate the existence of optimal linear $(q^3, q, 3)$-perfect hash families for the remaining values of q, we need to consider the case when the 6th point P_6 is not on the same conic as the points in $\mathcal{S}'$. So we need to find a point P_6 which does not lie on any of the 15 eliminated lines in Table 2 and such that $\mathcal{S}' \cup P_6$ forms an arc (that is P_6 does not lie on any of the 10 bisecants of $\mathcal{S}'$ given in Table 1). There are two forms that the coordinates for P_6 can take, either $P_6 = (1, x, y)$ for some $x, y \in \mathrm{GF}(q)$ or $P_6 = (0, 1, z)$ for some $z \in \mathrm{GF}(q)$. To construct a perfect hash family, we need to find a point P_6 that does not lie on any of the 25 lines in Tables 1 and 2. We can construct a perfect hash family when $q = 13$ by considering a point P_6 of the form $P_6 = (1, x, y)$. The 25 eliminated lines give us 25 conditions on x and y. By checking all these 25 conditions, we can find a construction that works for $q = 13$, namely when $a = 2, b = 3, x = 4, y = 7$.

Theorem 2.2. *There exists an optimal linear* $(q^3, q, 3)$*-perfect hash family when* $q = 13$. *The following is an example*: $\{[0,0,1], [1,0,0], [1,1,1], [1,2,2^2], [1,3,3^2], [1,4,7]\}$.

The cases $q < 11$ need to be checked individually, and it can be shown that if $q = 2, 3, 4, 5, 7, 8, 9$, then given any 5-set $\mathcal{S}' = \{(0,0,1), (1,0,0), (1,1,1), (1,a,a^2), (1,b,b^2)\}$, for $a, b \in \mathrm{GF}(q)$, every point of $\mathrm{PG}(2, q)$ lies on at least one of the 25 eliminated lines listed in Tables 1 and 2. Thus, there are no optimal linear perfect hash families for these values of q. In summary, we have proved the following existence result.

Theorem 2.3. *Optimal linear* $(q^3, q, 3)$*-perfect hash families exist if and only if* q *is a prime power and* $q \geqslant 11$.

3. Optimal linear $(q^2, q, 5)$-perfect hash families

A linear (q^2, q, t)-perfect hash family has a geometric representation in the projective plane. We can identify the elements of V with points in $\mathrm{AG}(2, q)$ and a linear function $\phi\colon V \to \mathrm{GF}(q)$ corresponds to a point P_ϕ on ℓ_∞. Let $\mathcal{K}$ be a set of t points in $\mathrm{AG}(2, q)$. The $\binom{t}{2}$ lines determined by a pair of points of $\mathcal{K}$ meet ℓ_∞ in $\binom{t}{2}$ (not necessarily distinct) points on ℓ_∞ called the *shadow* of $\mathcal{K}$. If P_ϕ is not in the shadow of $\mathcal{K}$, then all the lines through P_ϕ meet $\mathcal{K}$ in at most one point, so ϕ separates $\mathcal{K}$. A set $\mathcal{S} = \{P_{\phi_1}, \dots, P_{\phi_k}\}$ of k points of ℓ_∞ is a linear (q^2, q, t)-perfect hash family if for all sets $\mathcal{K}$ of t points in $\mathrm{AG}(2,q)$, at least one point of $\mathcal{S}$ is not contained in the shadow of $\mathcal{K}$.

In this section we give constructions of optimal linear $(q^2,q,5)$-perfect hash families for q much smaller than the known bound. We use a subfield construction and first review the known subfield constructions of linear (q^2,q,t)-perfect hash families.

3.1. *Known subfield constructions of (q^2,q,t)-perfect hash families*

An optimal linear $(q^2,q,4)$-perfect hash family has size $d(t-1)=6$, and so consists of 6 points on the line at infinity. In [3], it is shown that they exist for $q=11$ and all prime powers $q>13$, and constructions are given for all values of q where they exist. One of the key constructions is the following subfield construction.

Theorem 3.1 *(Subfield Construction [3]). Let $q=r^i$, $r\geqslant 4, i\geqslant 2$. Let $\{0,1,a,b\}\subseteq \mathrm{GF}(r)$ be distinct and let $\alpha\in \mathrm{GF}(r^i)\setminus \mathrm{GF}(r)$. Then $\{(0,1,0),\ (1,0,0),\ (1,1,0),\ (1,a,0),\ (1,b,0),\ (1,\alpha,0)\}$ is a linear $(q^2,q,4)$-perfect hash family.*

Geometrically, this corresponds to the following subplane construction. We can naturally embed $\mathrm{PG}(2,r)$ as a subplane of $\mathrm{PG}(2,r^i)$. Any subset $\mathcal{S}$ of ℓ_∞ that has 5 distinct points in $\mathrm{PG}(2,r)$ and one point in $\mathrm{PG}(2,r^i)\setminus\mathrm{PG}(2,r)$ is a $(q^2,q,4)$-perfect hash family. This can be proved by showing that if $\mathcal{K}$ is *any* set of 4 points in $\mathrm{AG}(2,r^i)$ whose shadow contains 5 points in $\mathrm{PG}(2,r)$, then we can find a collineation that fixes ℓ_∞ and maps $\mathcal{K}$ to 4 points in $\mathrm{AG}(2,r)$. Thus the entire shadow of $\mathcal{K}$ is contained in $\mathrm{PG}(2,r)$ and the given set $\mathcal{S}$ is not contained in the shadow of $\mathcal{K}$, and so is a perfect hash family.

The construction of optimal linear perfect hash families given by Blackburn and Wild in [9] is also a subfield/subplane construction. In the case $d=2$, the geometric interpretation of their construction is as follows. Suppose we have a chain of subfields $F_0<F_1<\cdots<F_{2(t-2)}$ such that $|F_{2(t-2)}|=q$ and $[F_i:F_{i-1}]\geqslant 2$. Then in $\mathrm{PG}(2,F_{2(t-2)})=\mathrm{PG}(2,q)$, we have a chain of subplanes $\mathrm{PG}(2,F_0),\mathrm{PG}(2,F_1),\ldots,\mathrm{PG}(2,q)$. We can form an optimal linear (q^d,q,t)-perfect hash family by taking one point on the line at infinity from each of the subplanes (that is, one point of ℓ_∞ from $\mathrm{PG}(2,F_0)$, one point of ℓ_∞ from $\mathrm{PG}(2,F_1)\setminus\mathrm{PG}(2,F_0)$ and so on). Hence this construction needs a large q of a certain form.

In practice, a smaller subfield construction works as the example with $t=4$ shows above. We show here how to optimize the subfield construction for the case $t=5$ and so obtain constructions for much smaller q than previously known. We first note that an optimal linear $(q^2,q,5)$-perfect hash family has size $d(t-1)=8$. Blackburn and Wild [9] proved that they exist if $q>10^8$, further, they gave the above subfield construction. By improving this construction, we have examples for much smaller q.

3.2. *Subfield constructions of $(q^2,q,5)$-perfect hash families*

Before describing our constructions, we prove the following result about the structure of optimal linear $(q^2,q,5)$-perfect hash families.

Lemma 3.2. *If $\mathcal{S}$ is an optimal linear $(q^2,q,5)$-perfect hash family, then any subset of 6 points of $\mathcal{S}$ is an optimal linear $(q^2,q,4)$-perfect hash family.*

Proof. Let $\mathcal{S}$ be a set of 8 points on ℓ_∞ such that at least one 6-subset $\mathcal{S}'$ of $\mathcal{S}$ is not a $(q^2, q, 4)$-perfect hash family. We show that there is a set of 5 points in $\mathrm{AG}(2, q)$ whose shadow contains $\mathcal{S}$ and so $\mathcal{S}$ is not a perfect hash family. If $\mathcal{S}'$ is not a $(q^2, q, 4)$-perfect hash family, then there exists a set $\mathcal{K}'$ of 4 points in $\mathrm{AG}(2, q)$ whose shadow contains $\mathcal{S}'$. Let $\{X_1, X_2\} = \mathcal{S} \setminus \mathcal{S}'$ and $K_1, K_2 \in \mathcal{K}$, then $K_5 = X_1K_1 \cap X_2K_2$ is a point of $\mathrm{AG}(2, q)$ and the shadow of $\mathcal{K} = \mathcal{K}' \cup K_5$ contains $\mathcal{S}$, thus $\mathcal{S}$ is not a perfect hash family. □

We describe two subfield constructions of optimal linear $(q^2, q, 5)$-perfect hash families. Note that for simplicity we state these constructions using field extensions of degree 2. However, they are valid for any extension of degree $\geqslant 2$.

Construction 1. *Let $q = r^4$, r a prime power. Let $a, b, c \in \mathrm{GF}(r)$ such that in $\mathrm{PG}(2, r)$, the 6 points $(0, 1, 0), (1, 0, 0), (1, 1, 0), (1, a, 0), (1, b, 0), (1, c, 0)$ form a $(r^2, r, 4)$-perfect hash family. Let $\alpha \in \mathrm{GF}(r^2) \setminus \mathrm{GF}(r)$ and $\beta \in \mathrm{GF}(r^4) \setminus \mathrm{GF}(r^2)$, then the following 8 points on ℓ_∞ in $\mathrm{PG}(2, r^4)$ form a $(q^2, q, 5)$-perfect hash family*:

$$(0, 1, 0), \quad (1, 0, 0), \quad (1, 1, 0), \quad (1, a, 0), \quad (1, b, 0), \quad (1, c, 0), \quad (1, \alpha, 0), \quad (1, \beta, 0).$$

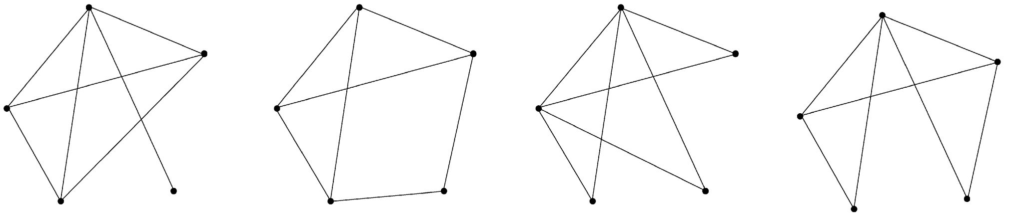
Construction 2. *Let $q = r^2$, r a prime power. Let $a, b, c, d \in \mathrm{GF}(r)$ and suppose the seven points $(0, 1, 0)$, $(1, 0, 0)$, $(1, 1, 0)$, $(1, a, 0)$, $(1, b, 0)$, $(1, c, 0)$, $(1, d, 0)$ on ℓ_∞ in $\mathrm{PG}(2, r)$ are such that any 6 of them forms a linear $(r^2, r, 4)$-perfect hash family. Let $\alpha \in \mathrm{GF}(r^2) \setminus \mathrm{GF}(r)$. Then the following 8 points on ℓ_∞ in $\mathrm{PG}(2, r^2)$ form a $(q^2, q, 5)$-perfect hash family:*

$$(0, 1, 0), \quad (1, 0, 0), \quad (1, 1, 0), \quad (1, a, 0), \quad (1, b, 0), \quad (1, c, 0), \quad (1, d, 0), \quad (1, \alpha, 0).$$

Before proving these constructions work, we provide a geometric description of them using subplanes. To use Construction 1, we naturally embed $\mathrm{PG}(2, r)$ in $\mathrm{PG}(2, r^2)$ in $\mathrm{PG}(2, r^4)$ (all with the same line at infinity ℓ_∞). Let $\mathcal{S}$ be a set of 8 points on ℓ_∞ satisfying the following: $\mathcal{S}$ consists of 6 points in $\mathrm{PG}(2, r)$ that form a $(q^2, q, 4)$-perfect hash family; one point of $\mathrm{PG}(2, r^2) \setminus \mathrm{PG}(2, r)$; and one point of $\mathrm{PG}(2, r^4) \setminus \mathrm{PG}(2, r^2)$. Then $\mathcal{S}$ is a $(q^2, q, 5)$-perfect hash family. To use Construction 2, we naturally embed $\mathrm{PG}(2, r)$ in $\mathrm{PG}(2, r^2)$ (with the common line at infinity ℓ_∞). Let $\mathcal{S}'$ be a set of 7 points of $\ell_\infty \cap \mathrm{PG}(2, r)$ such that any 6 of them is a $(q^2, q, 4)$-perfect hash family. Then $\mathcal{S}'$ together with any point of ℓ_∞ in $\mathrm{PG}(2, r^2) \setminus \mathrm{PG}(2, r)$ is a $(q^2, q, 5)$-perfect hash family.

Proof of Constructions. By Theorem 3.1, Construction 1 contains the 7 points $(0, 1, 0)$, $(1, 0, 0)$, $(1, 1, 0)$, $(1, a, 0)$, $(1, b, 0)$, $(1, c, 0)$, $(1, \alpha, 0)$ in $\mathrm{PG}(2, r^2)$ such that any 6 are a $(r^2, r, 4)$-perfect hash family. Hence, Construction 1 is a special case of Construction 2, so we only need to prove Construction 2.

Geometrically, we argue that if 5 points in $\mathrm{AG}(2, q)$ have a shadow that contains a set $\mathcal{S}'$ of 7 points of ℓ_∞ in $\mathrm{PG}(2, r)$, then all points of the shadow are in $\mathrm{PG}(2, r)$. Let $\mathcal{K}$ be a set of 5 points in $\mathrm{AG}(2, q)$ whose shadow contains $\mathcal{S}'$ a set of 7 points of ℓ_∞ in $\mathrm{PG}(2, r)$. We consider the case where the shadow of $\mathcal{K}$ has 10 points on ℓ_∞ (the cases where the shadow of $\mathcal{K}$ has less than 10 points are proved similarly). Hence there are 10 2-secants of $\mathcal{K}$ that meet ℓ_∞ in distinct points. Those 2-secants which contain a point of $\mathcal{S}'$ are called $\mathcal{S}'$*-secants*, so $\mathcal{K}$ has 7 $\mathcal{S}'$-secants. Each point of $\mathcal{K}$ lies on 1, 2, 3 or 4 $\mathcal{S}'$-secants, and it is easy to see that there are only 4 ways to distribute the $\mathcal{S}'$-secants among the points of $\mathcal{K}$. These four cases are illustrated as graphs



A B C D

Fig. 1. The 4 cases for the $\mathcal{S}'$-secants.

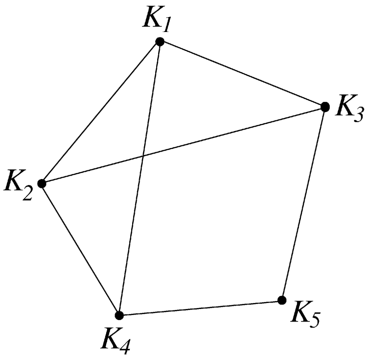


Fig. 2. The $\mathcal{S}'$-secants for case B.

in Fig. 1 where the vertices are the points of $\mathcal{K}$ and the edges are the $\mathcal{S}'$-secants. For example, case A has one point of $\mathcal{K}$ lying on 4 $\mathcal{S}'$-secants, three points of $\mathcal{K}$ lying on 3 $\mathcal{S}'$-secants and one point of $\mathcal{K}$ lying on 1 $\mathcal{S}'$-secants.

We first note that case A cannot occur, since then the four points of $\mathcal{K}$ that lie on 3 or 4 $\mathcal{S}'$-secants form a 4 arc whose shadow of 6 points is contained in $\mathcal{S}'$, and so $\mathcal{S}'$ contains a set of 6 points that is not a $(r^2, r, 4)$-perfect hash family, a contradiction.

Consider case B, we note that there is only one way to draw a graph consisting of 5 vertices, such that 4 of the vertices lie on 3 edges, and the remaining vertex lies on 2 edges. Thus up to isomorphism, there is only one configuration in this case. Without loss of generality, we can label the points of $\mathcal{K}$ so that K_1, K_2, K_3, K_4 each lie on 3 $\mathcal{S}'$-secants and K_5 lies on 2 $\mathcal{S}'$-secants and such that K_1K_2 is an $\mathcal{S}'$-secant. Figure 2 shows the 5 points and the lines in the figure indicate the $\mathcal{S}'$-secants.

Now, the translation group of $\mathrm{AG}(2,q)$ consisting of the automorphisms of $\mathrm{AG}(2,q)$ fixing pointwise the line at infinity is transitive on the points of $\mathrm{AG}(2,q)$ and for any point of $\mathrm{AG}(2,q)$, the stabilizer of that point is transitive on the points of the (fixed) lines through it. Hence we can find a collineation that fixes ℓ_∞ pointwise and maps K_1 and K_2 to points in $\mathrm{AG}(2,r)$. It is now easy to check that all the points of $\mathcal{K}$ must be in $\mathrm{AG}(2,r)$. For example, $K_1, K_2 \in \mathrm{AG}(2,q)$, and K_2K_4 and K_1K_4 are both $\mathcal{S}'$-secants, hence they are both lines of $\mathrm{AG}(2,r)$, and so their intersection K_4 must be in $\mathrm{AG}(2,r)$. Similarly, $K_3, K_5 \in \mathrm{AG}(2,r)$. So $\mathcal{K} \subset \mathrm{AG}(2,r)$, and hence all of the points of the shadow of $\mathcal{K}$ are in $\mathrm{AG}(2,r)$ and so $\mathcal{S}$ cannot contain the shadow of $\mathcal{K}$. Cases C and D are similar. $\square$

Now we want to determine the values of q for which perfect hash families arise from these constructions. We prove the following existence results, and the proof describes the construction of a perfect hash family for each q where it exists.

Theorem 3.3.

(1) *There exists an optimal linear* $(q^2, q, 5)$*-perfect hash family if* $q = r^4$*, where* r *is a prime power satisfying* $r = 11$ *or* $r > 13$.
(2) *There exists an optimal linear* $(q^2, q, 5)$*-perfect hash family if* $q = r^2$*, where* r *is a prime power satisfying* $\operatorname{char} \mathrm{GF}(r) \geqslant 31$.

Proof of part (1). We use Construction 1 for part (1), and so we need an optimal linear $(r^2, r, 4)$-perfect hash family. In [3] it is shown these exist for all prime powers r where $r = 11$ or $r > 13$. Further, constructions are provided for each value of r where they exist. Hence we can use these construction with Construction 1 to obtain optimal linear $(q^2, q, 5)$-perfect hash family if $q = r^4$, $r = 11$ or $r > 13$. Note that the smallest value there exists for is $q = 11^4 = 14{,}641$. □

The proof of part (2) uses Construction 2 and is lengthy; it is proved in the next subsection. Note that the smallest example of a $(q^2, q, 5)$-perfect hash family in this case is for $q = 31^2 = 961$. This is much smaller q than the known existence bound of 10^8.

3.3. *Proof of Theorem 3.3(2)*

To prove Theorem 3.3(2), we need to show that if $r \geqslant 31$, then there exists a set of 7 points of ℓ_∞ in $\mathrm{PG}(2, r)$ such that any 6 of them forms a linear $(r^2, r, 4)$-perfect hash family. We call such a family of 7 points a *suitable* family.

We give an easy counting argument using the results from [3] that show a suitable family will exist if $r > 96$. Let $\mathcal{S}$ be a set of 6 points on ℓ_∞ that form a $(r^2, r, 4)$-perfect hash family. A subset $\mathcal{S}'$ of 5 of these points eliminates 15 points that cannot be added to $\mathcal{S}'$ to form a perfect hash family [3]. So in total, there are $\binom{6}{5} \times 15 = 90$ points eliminated. So if $q > 6 + 90 = 96$ then there will be a point P on ℓ_∞ such that $\mathcal{S} \cup P$ is a set of 7 points such that any 6 form a $(r^2, r, 4)$-perfect hash family.

We want to construct suitable families, so we start with a particular $(r^2, r, 4)$-perfect hash family and calculate these 90 points. We consider the following set of six points $\mathcal{S} = \{(0, 1, 0), (1, 0, 0), (1, 1, 0), (1, 2, 0), (1, 3, 0), (1, 5, 0)\}$ of ℓ_∞. This set is a $(r^2, r, 4)$-perfect hash family for $r = 11$ and r any prime power $r > 13$ as shown in [3]. We want to find a seventh point on ℓ_∞ to add to $\mathcal{S}$ to make a suitable family (that is, so that every six points form a perfect hash family). There are 6 cases to consider, for example, the first case considers the 5 points $\mathcal{S}'_1 = \{(1, 0, 0), (1, 1, 0), (1, 2, 0), (1, 3, 0), (1, 5, 0)\} = \mathcal{S} \setminus \{(0, 1, 0)\}$ and finds the 15 points of ℓ_∞ that cannot be added to $\mathcal{S}'_1$ to form a perfect hash family. We use the results from [3] to find the coordinates of these 15 points. We obtain in total 90 points we cannot use. Table 4 lists the 6 cases and the resulting 15 points in each case. The 6 cases in the table are $\mathcal{S}'_1 = \mathcal{S} \setminus \{(0, 1, 0)\}$, $\mathcal{S}'_2 = \mathcal{S} \setminus \{(1, 5, 0)\}$, $\mathcal{S}'_3 = \mathcal{S} \setminus \{(1, 3, 0)\}$, $\mathcal{S}'_4 = \mathcal{S} \setminus \{(1, 2, 0)\}$, $\mathcal{S}'_5 = \mathcal{S} \setminus \{(1, 1, 0)\}$, $\mathcal{S}'_6 = \mathcal{S} \setminus \{(1, 0, 0)\}$.

If we assume that the underlying field has characteristic larger than 7, then we can divide these homogeneous point coordinates by any of $-1, 2, 3, 7$. This reduces these 90 points to the following set of points which we have divided into 8 subcases in Table 5. Note that by casual

Table 4
The 90 forbidden points

	$\mathcal{S}_1'$	$\mathcal{S}_2'$	$\mathcal{S}_3'$	$\mathcal{S}_4'$	$\mathcal{S}_5'$	$\mathcal{S}_6'$
T1	$(1, 11, 0)$	$(0, 1, 0)$	$(-2, 2, 0)$	$(-1, 3, 0)$	$(0, 1, 0)$	$(-1, 1, 0)$
T2	$(7, 19, 0)$	$(2, 3, 0)$	$(4, 5, 0)$	$(3, 5, 0)$	$(4, 10, 0)$	$(3, 7, 0)$
T3	$(13, 29, 0)$	$(4, 6, 0)$	$(6, 10, 0)$	$(7, 15, 0)$	$(6, 15, 0)$	$(5, 13, 0)$
T4	$(6, 24, 0)$	$(3, 7, 0)$	$(5, 13, 0)$	$(5, 17, 0)$	$(5, 19, 0)$	$(4, 14, 0)$
T5	$(6, 20, 0)$	$(2, 5, 0)$	$(2, 7, 0)$	$(3, 13, 0)$	$(3, 11, 0)$	$(2, 8, 0)$
T6	$(9, 15, 0)$	$(1, -1, 0)$	$(1, -3, 0)$	$(1, -7, 0)$	$(2, 1, 0)$	$(1, -1, 0)$
T7	$(5, 9, 0)$	$(2, 3, 0)$	$(4, 5, 0)$	$(4, 10, 0)$	$(3, 5, 0)$	$(3, 7, 0)$
T8	$(-1, 5, 0)$	$(1, 4, 0)$	$(1, 8, 0)$	$(2, 12, 0)$	$(1, 9, 0)$	$(1, 7, 0)$
T9	$(8, 4, 0)$	$(1, -3, 0)$	$(3, -5, 0)$	$(2, -10, 0)$	$(2, -5, 0)$	$(2, -2, 0)$
T10	$(2, -4, 0)$	$(-1, -4, 0)$	$(-3, -8, 0)$	$(-2, -12, 0)$	$(-2, -9, 0)$	$(-2, -8, 0)$
T11	$(-7, -5, 0)$	$(-1, 1, 0)$	$(-1, 3, 0)$	$(-2, 2, 0)$	$(-1, 4, 0)$	$(-1, 1, 0)$
T12	$(-7, -9, 0)$	$(-2, -1, 0)$	$(-4, -3, 0)$	$(-4, -2, 0)$	$(-3, -4, 0)$	$(-3, -5, 0)$
T13	$(1, -15, 0)$	$(-1, -6, 0)$	$(-1, -10, 0)$	$(-1, -15, 0)$	$(-2, -15, 0)$	$(-1, -9, 0)$
T14	$(-8, -20, 0)$	$(-2, -3, 0)$	$(-2, -5, 0)$	$(-3, -5, 0)$	$(-3, -10, 0)$	$(-2, -6, 0)$
T15	$(-14, -24, 0)$	$(-3, -2, 0)$	$(-5, -2, 0)$	$(-5, -3, 0)$	$(-5, -6, 0)$	$(-4, -6, 0)$

Table 5
The 8 subcases

Case	
1	$(0, 1, 0)$
2	$(1, 1, 0)$, $(1, 4, 0)$, $(1, 6, 0)$, $(1, 7, 0)$, $(1, 8, 0)$, $(1, 9, 0)$, $(1, 10, 0)$, $(1, 11, 0)$, $(1, 15, 0)$
	$(1, -1, 0)$, $(1, -2, 0)$, $(1, -3, 0)$, $(1, -4, 0)$, $(1, -5, 0)$, $(1, -7, 0)$, $(1, -15, 0)$
3	$(2, -5, 0)$, $(2, 1, 0)$, $(2, 3, 0)$, $(2, 5, 0)$, $(2, 7, 0)$, $(2, 9, 0)$, $(2, 15, 0)$
4	$(3, -5, 0)$, $(3, 2, 0)$, $(3, 4, 0)$, $(3, 5, 0)$, $(3, 7, 0)$, $(3, 8, 0)$, $(3, 10, 0)$, $(3, 11, 0)$, $(3, 13, 0)$
5	$(4, 3, 0)$, $(4, 5, 0)$
6	$(5, 2, 0)$, $(5, 3, 0)$, $(5, 6, 0)$, $(5, 9, 0)$, $(5, 13, 0)$, $(5, 17, 0)$, $(5, 19, 0)$
7	$(7, 5, 0)$, $(7, 9, 0)$, $(7, 12, 0)$, $(7, 15, 0)$, $(7, 19, 0)$
8	$(13, 29, 0)$

inspection of the table, we can see that the points $(1, 4, 0)$, $(1, 6, 0)$, $(1, 7, 0)$, $(1, 8, 0)$, $(1, 9, 0)$, $(1, 10, 0)$, $(1, 11, 0)$, $(1, 15, 0)$ can never be added to our set $\mathcal{S}$ to make a suitable family.

Suppose the characteristic of the underlying field is p, we show that for most p, we can add the point $(1, 12, 0)$ to make a suitable family.

Theorem 3.4. *The set* $\{(0, 1, 0), (1, 0, 0), (1, 1, 0), (1, 2, 0), (1, 3, 0), (1, 5, 0), (1, 12, 0)\}$ *is a suitable family for* $p = 37$ *and* $p \geqslant 53$ (*except* $p = 79$).

Proof. To add the point $(1, 12, 0)$ to the set $\mathcal{S} = \{(0, 1, 0), (1, 0, 0), (1, 1, 0), (1, 2, 0), (1, 3, 0), (1, 5, 0)\}$ to make a suitable family, we need to show that the point $(1, 12, 0)$ is never equivalent mod p to any of the points listed in cases 1–8 in Table 5.

In case 1, $(0, 1, 0)$ is never $(1, 12, 0)$. For case 2, $(1, 12, 0) = (1, -1, 0)$ if and only if $12 \equiv -1 \bmod p$, if and only if $p = 13$ (as p is prime). We repeat this process for all the points in this case and get the following forbidden values of p: 2, 3, 7, 11, 13, 17, 19, 23. For case 3, $(1, 12, 0) = (2, 24, 0)$. For the first point, we have $(2, 24, 0) = (2, -5, 0)$ if and only if $24 \equiv -5 \bmod p$, if and only if $p = 29$. Repeating this gives the following forbidden values: 3, 5, 17, 19, 23, 29. The forbidden values for case 4 are 2, 5, 7, 13, 17, 23, 29, 31, 41. For case 5 we get 3, 5, 43; for case 6 we get 2, 3, 13, 19, 29, 41, 43, 47; for case 7 we get 2, 3, 5, 23, 79 and for case 8 we get 11, 29. Thus, the forbidden values of p are $p = 79$ and $p \leqslant 47$, except $p = 37$. □

Using a similar technique, we find a suitable family for the remaining characteristics $p \geqslant 31$.

Theorem 3.5.

(1) $\{(0,1,0), (1,0,0), (1,1,0), (1,2,0), (1,3,0), (1,5,0), (1,16,0)\}$ *is a suitable family for* $p = 47, 79$.
(2) $\{(0,1,0), (1,0,0), (1,1,0), (1,2,0), (1,3,0), (1,5,0), (1,20,0)\}$ *is a suitable family for* $p = 41, 43$.
(3) $\{(0,1,0), (1,0,0), (1,1,0), (1,2,0), (1,3,0), (1,5,0), (1,21,0)\}$ *is a suitable family for* $p = 31$.

We note that computer tests have shown that there are no suitable families containing $\{(0,1,0), (1,0,0), (1,1,0), (1,2,0), (1,3,0), (1,5,0)\}$ for $p < 31$. However, it may be possible to construct suitable families for smaller characteristic p by taking a different set of 6 initial points. We chose these 6 points to work with as they are a linear $(q^2, q, 4)$-perfect hash family for a large set of q: namely all $q = p^h$, $p \geqslant 11$, $p \neq 13$.

Proof of Theorem 3.3(2). By Theorems 3.4 and 3.5, there exists a suitable family for all prime power $r = p^h$, p prime, $p \geqslant 31$. That is, there exists a set of 7 points on ℓ_∞ in $\mathrm{PG}(2, q)$ such that any 6 of them form a $(r^2, r, 4)$-perfect hash family. Hence we can use Construction 2 to construct a $(q^2, q, 5)$-perfect hash family for all $q = r^2$, where r is a prime power satisfying $\mathrm{char}\,\mathrm{GF}(r) \geqslant 31$. □

4. Conclusion

In this article, we used geometric techniques to investigate the existence of and to construct optimal linear (q^d, q, t)-perfect hash families. We completely answered the question of existence in the case $d = 3$, $t = 3$, and provided constructions for all q where they exist. We also gave constructions for the case $d = 2$, $t = 5$ for much smaller q than previously known, and much smaller than the known existence bound. In [3], the case $d = 2$, $t = 4$ is solved using similar techniques. It seems likely that larger values of d and t will not be accessible by these geometric techniques as the number of conditions to calculate quickly grows large. A general technique for constructing perfect hash families with small parameters would be useful. Motivation is provided by articles such as [1,2] which give algorithms that use perfect hash families with small parameters to construct other perfect hash families.

We note that in each case we studied, optimal linear perfect hash families exist for much smaller q than current bounds indicate, so a natural question is: can the bounds in [9] be improved?

References

[1] M. Atici, S.S. Magliveras, D.R. Stinson, W.-D. Wei, Some recursive constructions for perfect hash families, J. Combin. Des. 4 (1996) 353–363.
[2] M. Atici, D.R. Stinson, W.-D. Wei, A new practical algorithm for the construction of a perfect hash function, J. Combin. Math. Combin. Comput. 35 (2000) 127–145.

[3] S.G. Barwick, W.-A. Jackson, C.T. Quinn, Optimal linear perfect hash families with small parameters, J. Combin. Des. 12 (2004) 311–324.
[4] S.G. Barwick, W.-A. Jackson, A sequence approach to linear perfect hash families, Des. Codes Cryptogr., in press.
[5] A. Beutelspacher, U. Rosenbaum, Projective Geometry: From Foundations to Applications, Cambridge Univ. Press, 1998.
[6] S.R. Blackburn, Combinatorics and threshold cryptography, in: Combinatorial Designs and Their Applications, in: CRC Res. Notes in Math., vol. 403, CRC Press, 1999, pp. 49–70.
[7] S.R. Blackburn, Perfect hash families: Probabilistic methods and explicit constructions, J. Combin. Theory Ser. A 92 (2000) 54–60.
[8] S.R. Blackburn, M. Burmester, Y. Desmedt, P.R. Wild, Efficient multiplicative sharing schemes, in: Advances in Cryptology—EUROCRYPT'96, in: Lecture Notes in Comput. Sci., vol. 1070, Springer, 1996, pp. 107–118.
[9] S.R. Blackburn, P.R. Wild, Optimal linear perfect hash families, J. Combin. Theory Ser. A 83 (1998) 233–250.
[10] A. Fiat, M. Naor, Broadcast encryption, in: Advances in Cryptology—CRYPTO'93, in: Lecture Notes in Comput. Sci., vol. 773, Springer, 1994, pp. 480–491.
[11] K. Mehlhorn, Data Structures and Algorithms 1: Sorting and Searching, Springer, 1984.
[12] D.R. Stinson, T. van Trung, R. Wei, Secure frameproof codes, key distribution patterns, group testing algorithms and related structures, J. Statist. Plann. Inference 86 (2000) 595–617.
[13] H. Wang, C. Xing, Explicit constructions of perfect hash families from algebraic curves over finite fields, J. Combin. Theory Ser. A 93 (2001) 112–124.