# On Saturating Sets in Small Projective Geometries 

Alexander A. Davydov and Patric R. J. Östergård


#### Abstract

A set of points, $S \subseteq P G(r, q)$, is said to be $\varrho$-saturating if, for any point $x \in P G(r, q)$, there exist $\varrho+1$ points in $S$ that generate a subspace in which $x$ lies. The cardinality of a smallest possible set $S$ with this property is denoted by $k(r, q, \varrho)$. We give a short survey of what is known about $k(r, q, 1)$ and present new results for $k(r, q, 2)$ for small values of $r$ and $q$. One construction presented proves that $k(5, q, 2) \leq 3 q+1$ for $q=2, q \geq 4$. We further give an upper bound on $k\left(\varrho+1, p^{m}, \varrho\right)$. (C) 2000 Academic Press


## 1. Introduction

We denote the Galois field of $q$ elements by $G F(q)$ (so $q$ is a prime or a prime power), and let $G F(q)^{*}=G F(q) \backslash\{0\}$. We say that a set of points, $S \subseteq P G(r, q)$, is $\varrho$-saturating if, for any point $x \in P G(r, q)$, there exist $\varrho+1$ points in $S$ that generate a subspace in which $x$ lies. The cardinality of a smallest possible set $S$ with this property is denoted by $k(r, q, \varrho)$.

The term saturated was to our knowledge coined by Ughi in [22] and used therein for the points in $S$. This term has later been used, for example, in [6, 16]. In [19], however, the points in $P G(r, q) \backslash S$ are said to be saturated, and as we find this definition more natural, we adopt it here (so the points in $S$ are saturating).
Exact values of $k(r, q, \varrho)$ are only known for the smallest parameters; in other cases, we can try to construct $\varrho$-saturating sets to find upper bounds on this function. If $\varrho=0$, we clearly have to include all points of $P G(r, q)$ to get a saturating set. Hence

$$
k(r, q, 0)=|P G(r, q)|=\left(q^{r+1}-1\right) /(q-1) .
$$

For $\varrho>0$, the problem of determining values of (or good bounds on) $k(r, q, \varrho)$ is highly non-trivial. In Section 2, some known results on $k(r, q, 1)$ are surveyed. Several of these results were obtained in the context of coding theory. In fact, $\varrho$-saturating sets in projective geometry correspond to linear codes with covering radius $R=\varrho+1$ in coding theory. See $[6,16]$ for further details regarding this correspondence.
In Section 3, we consider $k(r, q, 2)$ for $r<5$. In Section 4, we give a construction that proves $k(5, q, 2) \leq 3 q+1$ for $q=2, q \geq 4$. Finally, in Section 5, best known upper bounds on $k(r, q, 2)$ are tabulated for $r=3,4,5$ and $q \leq 16$. Some of these bounds are obtained using a computer.

## 2. On 1-Saturating Sets

The function $k(r, q, 1)$ has been fairly intensively studied, in particular, in the framework of linear codes with covering radius 2 ; see, for example, [4-11].
Trivially $k(1, q, 1)=2$ (take any two distinct points in $P G(1, q))$. The following theorem gives an upper bound on $k(2, q, 1)$ for all $q \geq 8$ [13, p. 59].

Theorem 1. For $q \geq 8, k(2, q, 1) \leq\lfloor q / 2+2\rfloor$.
This bound comes from constructions of complete caps (or complete arcs), which have the additional requirement that no three of the points be collinear. Work has been done on finding
upper bounds on the smallest size of complete caps in $P G(2, q)$ that are asymptotically better than $q / 2$. Such work has, for example, led to bounds of asymptotic size $q / 3[1,17,21,23]$, $q / 4$ [17], and $2 q^{9 / 10}$ [21]; all these bounds, however, only hold for special values of $q$.

For 1-saturated sets, Ughi [22, Example B] obtained a bound of order $3 q^{1 / 2}$, and this result was slightly improved in [6, Theorem 5.2]:

Theorem 2. For $p \geq 2, k\left(2, p^{2}, 1\right) \leq 3 p-1$.
The construction in [22, Example B] can, for example, be generalized as follows to obtain families of 1-saturating sets in $P G(2, q)$ of size asymptotically $2 q^{(m-1) / m}$ when $m \geq 3$.

THEOREM 3. For $p \geq 2$ and $m \geq 2, k\left(2, p^{m}, 1\right) \leq 2 p^{m-1}+p$.

Proof. An element in $G F\left(q=p^{m}\right)$ can be expressed as

$$
\begin{equation*}
A=a_{m-1} \alpha^{m-1}+\cdots+a_{1} \alpha+a_{0} \tag{1}
\end{equation*}
$$

where $\alpha$ is a primitive element of $G F(q)$ and $a_{i} \in G F(p), 0 \leq i \leq m-1$. The 1-saturating set is given by the columns of the matrix

$$
\mathbf{H}=\left[\begin{array}{ccc|ccc|ccc|ccc}
1 & 0 & 0 & 1 & \cdots & 1 & 1 & \cdots & 1 & 0 & \cdots & 0  \tag{2}\\
0 & 1 & 0 & \xi_{1} & \cdots & \xi_{p^{m-1}-1} & 0 & \cdots & 0 & 1 & \cdots & 1 \\
0 & 0 & 1 & 0 & \cdots & 0 & \xi_{1} & \cdots & \xi_{p^{m-1}-1} & e_{1} & \cdots & e_{p-1}
\end{array}\right]
$$

where $\left\{e_{1}, e_{2}, \ldots, e_{p-1}\right\}=G F(p)^{*}$, and $\left\{\xi_{1}, \xi_{2}, \ldots, \xi_{p^{m-1}-1}\right\}=E \subset G F(q)^{*}$ consists of all non-zero elements of the form (1) with $a_{m-1}=0$.

We shall now show that any point can be obtained as a linear combination of at most two columns of $\mathbf{H}$. For points with a 0 in a coordinate, we can use (at most) two of the first three columns of $\mathbf{H}$. So, we just need to show that a column

$$
\left[\begin{array}{c}
1 \\
A=a_{m-1} \alpha^{m-1}+\cdots+a_{1} \alpha+a_{0} \\
B=b_{m-1} \alpha^{m-1}+\cdots+b_{1} \alpha+b_{0}
\end{array}\right]
$$

can be obtained as a linear combination of two columns of $\mathbf{H}$. If $a_{m-1}=0$ or $b_{m-1}=0$, then we take $(1, A, 0)+B(0,0,1)$ or $(1,0, B)+A(0,1,0)$, respectively. If $a_{m-1} \neq 0$ and $b_{m-1} \neq$ 0 , then we have $b_{m-1}=k a_{m-1}$ where $k \in G F(p)$, and we take $(1,0, B-k A)+A(0,1, k)$. Note that $B-k A \in E \cup\{0\}$.

If $m=2$, then we obtain three independent lines in a Baer subplane of $P G\left(2, p^{2}\right)$ as in [22, Example B].
A further generalization of this result will be given later. For small $q$, better values can often be obtained by determining the exact value or by constructively finding a good upper bound (often by computer search); see [18] and [19, Table 1]. In all but one case, $k(2,4,1)=5$, the exact value of or the best known upper bound on $k(2, q, 1)$ is attained by a complete cap.

For $r=3$, we have the following result [6, Theorem 5.1], which was earlier proved in [3] for even $q$.

THEOREM 4. For $q \geq 4, k(3, q, 1) \leq 2 q+1$.

## 3. On 2-Saturating Sets

Values of $k(r, q, 2)$ for small $r$ have previously been considered for $q=2$ and $q=3$; see [2, 5, 6, 12].
In this section, we consider 2-saturating sets with $r<5$. For $r=2$, we can take any three points that are not collinear and find $k(2, q, 2)=3$.
Before we proceed, we present an elementary bound. This well-known bound comes from the direct sum construction in coding theory. Special cases of this result are proved in [22, (12) and Lemma 10].

THEOREM 5. $k\left(r+r^{\prime}+1, q, \varrho+\varrho^{\prime}+1\right) \leq k(r, q, \varrho)+k\left(r^{\prime}, q, \varrho^{\prime}\right)$.
We can often improve on the bounds obtained using Theorem 5, but it turns out that it gives a few best known bounds for small $r$ and $q$ with $\varrho=2$ (using $k(0, q, 0)=1, k(1, q, 0)=q+1$, and bounds on $k(r, q, 1)$ ).
We shall now give a generalization of Theorem 3, which gives $\varrho$-saturating sets in $P G(\varrho+$ $\left.1, p^{m}\right)$.
THEOREM 6. For $p \geq 2$ and $m \geq \varrho+1, k\left(\varrho+1, p^{m}, \varrho\right) \leq(p-1)\binom{\varrho+1}{2}+p^{m-\varrho}$ $(\varrho+1)+1$.

Proof. We consider points in $P G\left(\varrho+1, p^{m}\right)$ as $(\varrho+2)$-tuples over $G F\left(p^{m}\right)$ with homogeneous coordinates, and express an element in $G F\left(q=p^{m}\right)$ as $A=a_{m-1} \alpha^{m-1}+\cdots+a_{1} \alpha+a_{0}$ ( $\alpha$ is a primitive element in $G F\left(p^{m}\right)$ ). The set $E \subset G F\left(p^{m}\right)^{*}$ consists of all non-zero elements with $a_{m-1}, a_{m-2}, \ldots, a_{m-\varrho}=0$.
We shall now prove that the following points make up a $\varrho$-saturating set: all points with one non-zero coordinate (that is, with weight one), and all points with two non-zero coordinates where the second non-zero coordinate is in $G F(p)$ if the first coordinate is zero and in $E$ otherwise (that is, points of the form $\left(0, \ldots, 0,1,0, \ldots, 0, e \in G F(p)^{*}, 0, \ldots, 0\right)$ and $(1,0, \ldots, 0, \xi \in E, 0, \ldots, 0)$ ). The total number of such points clearly coincides with the upper bound in the theorem.
It is not difficult to see that the requirement of being $\varrho$-saturating is fulfilled if we consider a point which has zero coordinates or which has, in any but the first coordinate, coordinate values in $E$. (We then take a linear combination of points of weight one and possibly-with coefficient 1—a point with a one in the first coordinate and an element from $E$ in some other coordinate.) Hence, we need only consider points

$$
\left[\begin{array}{c}
1 \\
A_{1}=a_{1, m-1} \alpha^{m-1}+\cdots+a_{1,1} \alpha+a_{1,0} \\
\vdots \\
A_{\varrho+1}=a_{\varrho+1, m-1} \alpha^{m-1}+\cdots+a_{\varrho+1,1} \alpha+a_{\varrho+1,0}
\end{array}\right]
$$

with $a_{i, j} \in G F(p)$ where, for all $i$, at least one of $a_{i, m-1}, a_{i, m-2}, \ldots, a_{i, m-\varrho}$ is non-zero.
We now write $A_{i}=B_{i} \alpha^{m-\varrho}+a_{i, m-\varrho-1} \alpha^{m-\varrho-1}+\cdots+a_{i, 0}$. The polynomials $B_{i}$ are of the form $B_{i}=b_{i, \varrho-1} \alpha^{\varrho-1}+\cdots+b_{i, 0}$, where $b_{i, j}=a_{i, j+m-\varrho} \in G F(p)$. We then have $\varrho+1$ polynomials $B_{i}$, which we can consider to be in a vector space with $\varrho$ coordinates in $G F(p)$. These polynomials must then be linearly dependent with coefficients from $\operatorname{GF}(p)$. Then there exists a $B_{i}$ that can be expressed as a linear combination of the other polynomials. Without loss of generality, due to symmetry of the points in our saturating set, we may assume that we can write

$$
B_{\varrho+1}=\sum_{i=1}^{\varrho} k_{i} B_{i}
$$

with $k_{i} \in G F(p)$. Note that the elements $A_{i}-B_{i} \alpha^{m-\varrho} \in E \cup\{0\}$. Our proof is now completed by the fact that $\left(1, A_{1}, A_{2}, \ldots, A_{\varrho+1}\right)=\left(1,0, \ldots, 0, A_{\varrho+1}-k_{1} A_{1}-k_{2} A_{2}-\cdots-k_{\varrho} A_{\varrho}\right)+$ $A_{1}\left(0,1,0, \ldots, 0, k_{1}\right)+A_{2}\left(0,0,1,0, \ldots, 0, k_{2}\right)+\cdots+A_{\varrho}\left(0, \ldots, 0,1, k_{\varrho}\right)$.

If $m=\varrho+1$, then the $\varrho$-saturating set in the construction in Theorem 6 consists of $(\varrho+1)(\varrho+2) / 2$ lines in the subgeometry $P G(\varrho+1, p)$. A further generalization of this approach, using planes, etc. in subgeometries seems possible.
Given a field $G F\left(p^{r}\right)$, where $p$ is a prime, we get the best bound by finding the smallest factor in $r$ that is greater than or equal to $\varrho+1$ and letting this be the value of $m$ when Theorem 6 is applied. For example, $k\left(3, p^{6}, 2\right)=k\left(3,\left(p^{2}\right)^{3}, 2\right) \leq 6 p^{2}-2$.

## 4. An Infinite Family with $r=5$

In this section we shall give a construction that shows that $k(5, q, 2) \leq 3 q+1$ for $q \neq 3$. The construction can be seen as taking, with slight modifications, two ovals and one line in this projective space. It can further be seen as a generalization of the (oval plus line) construction giving Theorem 4. The points of the constructions are columns of the following matrix (of size $(3 q+1) \times 6)$ :

$$
\mathbf{H}=\left[\begin{array}{ccc|c|ccc|cccc|c}
1 & \cdots & 1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0  \tag{3}\\
a_{1} & \cdots & a_{q} & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & 0 \\
a_{1}^{2} & \cdots & a_{q}^{2} & 0 & 1 & \cdots & 1 & 0 & \cdots & 0 & 0 & 0 \\
0 & \cdots & 0 & 0 & a_{2} & \cdots & a_{q} & 1 & \cdots & 1 & 0 & 0 \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & a_{2} & \cdots & a_{q} & 0 & 1 \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & a_{2}^{2} & \cdots & a_{q}^{2} & 1 & 0
\end{array}\right]=\left[\mathbf{h}_{1} \cdots \mathbf{h}_{3 q+1}\right],
$$

where $\left\{a_{1}=0, \ldots, a_{q}\right\}=G F(q)$. We can also present the points in the following isomorphic way, thereby observing a symmetry that will later be useful (coordinates of each point $\mathbf{h}_{2 q+2}, \ldots, \mathbf{h}_{3 q-1}$ are divided by $a_{i}^{2}$ ):

$$
\mathbf{H}^{\prime}=\left[\begin{array}{ccc|c|ccc|ccc|c}
1 & \cdots & 1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0  \tag{4}\\
a_{1} & \cdots & a_{q} & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\
a_{1}^{2} & \cdots & a_{q}^{2} & 0 & 1 & \cdots & 1 & 0 & \cdots & 0 & 0 \\
0 & \cdots & 0 & 0 & a_{2} & \cdots & a_{q} & a_{1}^{2} & \cdots & a_{q}^{2} & 0 \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & a_{1} & \cdots & a_{2} & 1 \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & \cdots & 1 & 0
\end{array}\right]=\left[\mathbf{h}_{1}^{\prime} \cdots \mathbf{h}_{3 q+1}^{\prime}\right] .
$$

As the points $\mathbf{h}_{q+2}, \ldots, \mathbf{h}_{2 q}$ further can be given with a 1 in the fourth position, we clearly have a symmetry given by the permutation

$$
\begin{equation*}
(16)(25)(34) \tag{5}
\end{equation*}
$$

on the coordinates. We will now prove that every point of $P G(5, q)$ is a linear combination of at most three columns of $\mathbf{H}$ and hence that the set is 2 -saturating.
We use the following notations for the points: $C^{*}=\left\{\mathbf{h}_{1}, \ldots, \mathbf{h}_{q+1}\right\}, D^{*}=\left\{\mathbf{h}_{1}, \ldots, \mathbf{h}_{q}\right\}$, $L^{*}=\left\{\mathbf{h}_{q+2}, \ldots, \mathbf{h}_{2 q}\right\}$.
The points $(0,0,1,0,0,0)$ and $(0,0,0,1,0,0)$ are called $A_{1}$ and $A_{2}$, respectively. We let $C=C^{*} \cup\left\{A_{1}\right\}$ and $D=D^{*} \cup\left\{A_{1}\right\}$, so $C$ is a hyperoval if $q$ is even, and $D$ is an oval if $q$ is odd [14, Ch. 8].
The following notations are used for spaces. The projective plane $(a, b, c, 0,0,0)$ is called $\pi$, the line $(0,0, a, b, 0,0)$ is called $L$, and the three-dimensional space $(a, b, c, d, 0,0)$ is called $V$.

TABLE 1.

| Upper bounds on $k(r, q, 2)$ for $3 \leq r \leq 5$ and $q \leq 16$. |  |  |  |  |  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| $r \backslash q$ | 2 | 3 | 4 | 5 | 7 | 8 | 9 | 11 | 13 | 16 |
| 3 | 5. ${ }^{\text {d }}$ | $5 .{ }^{e}$ | 5. ${ }^{\text {b }}$ | 6. ${ }^{\text {b }}$ | 7. ${ }^{\text {a }}$ | 7. ${ }^{\text {a }}$ | 7. ${ }^{\text {a }}$ | $8^{a}$ | $8^{c}$ | $9^{c}$ |
| 4 | $6 .{ }^{d}$ | $8 .{ }^{e}$ | $9^{c}$ | $10^{c}$ | $13^{c}$ | $15^{a}$ | $16^{a}$ | $19^{a}$ | $22^{a}$ | $26^{a}$ |
| 5 | 7. ${ }^{d}$ | $11^{e}$ | $13^{f}$ | $16^{f}$ | $22^{f}$ | $25^{f}$ | $28^{f}$ | $34^{f}$ | $40^{f}$ | $49^{f}$ |

Table 2.
Explicitly listed saturating sets.

```
k(3,13,2) \leq 8: {(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,9,8,2), (1,3,10,11),(1,1,10,5), (1,2,1,0)}
k(3,16,2) \leq 9: {(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1),(1,0,5,5),(1,4,4,15),(1,9,9,8),(1,13,12,14),
(1,12,1,3)}
k(4,4,2) \leq 9: {(1,0,0,0,0),(0,1,0,0,0),(0,0,1,0,0),(0,0,0,1,0),(0,0,0,0,1),(1,3,2,2,0),(1,1,0,3,2),
(1,1,2,1,2), (0,1,3,0,3)}
k(4,5,2) \leq 10:{(1,0,0,0,0),(0,1,0,0,0),(0,0,1,0,0),(0,0,0,1,0),(0,0,0,0,1),(1,1,0,1,3),(1,0,3,1,4),
(1,4,2,4,3), (0,1,1,0,3), (1,1,3,3,2)}
k(4,7,2) \leq 13: {(1,0,0,0,0),(0,1,0,0,0),(0,0,1,0,0),(0,0,0,1,0),(0,0,0,0,1),(0,1,1,1,6),(1,1,1,1,1),
(1,0,1,4,4),(0,1,3,0,2),(1,5,6,4,5),(1,1,5,2,6), (1,3,3,6,2), (1,3,4,5,6)}
```

THEOREM 7. The sets given by (3) and (4) are 2 -saturating for $q \geq 4$.
Proof. We shall show that any point $Z=\left(z_{1}, z_{2}, z_{3}, z_{4}, z_{5}, z_{6}\right)$ can be expressed as a linear combination of at most three columns of (3) or (4). Taking the symmetry (5) into account, we need to consider four cases.
Case 1. $Z \in L: z_{1}=z_{2}=z_{5}=z_{6}=0$. These points are on the line $L$ and such a point can be expressed as a linear combination of any two distinct points on the line, that is, using at most two columns in $L^{*}$.

Case 2. $Z \in \pi: z_{4}=z_{5}=z_{6}=0$. We consider the cases $q$ even and $q$ odd separately. Let $q$ be even. Then the hyperoval $C$ has no unisecants and every point of $\pi \backslash C$ lies on $q / 2+1$ bisecants of this hyperoval [14, Section 8.1]. Hence every point of $\pi \backslash C$ lies on $q / 2$ bisecants of the point set $C^{*}$. Such bisecants exist when $q / 2 \geq 1$, that is, $q \geq 2$.
Now let $q$ be odd. Then every point of the oval $D$ has one unisecant and every point of $\pi \backslash D$ lies on at least $(q-1) / 2$ bisecants of this oval [14, Table 8.2]. Hence every point of $\pi \backslash D$ lies on at least $(q-3) / 2$ bisecants of the point set $D^{*}$. Such bisecants exist when $(q-3) / 2 \geq 1$, that is, $q \geq 5$.
Since, according to Case 1 , the point $A_{1}$ can also be expressed as a linear combination of two points in $L^{*}$, every point of $\pi$ is a linear combination of at most two points of $H$.

Case 3. $Z \in V: z_{5}=z_{6}=0$. All points in $V$ can be expressed as a linear combination of at most two points in $C^{*} \cup L^{*} \cup\left\{A_{2}\right\}$ [6, Theorem 5.1]. Moreover, from Case 1 it follows that $A_{2}$ can be obtained as a linear combination of two points in $L^{*}$, so every point in $V$ is a linear combination of at most three columns of $\mathbf{H}$.

Case 4. $Z \notin V$ and $Z \notin V$ after applying (5): $z_{1}=1$ or $z_{1}=0, z_{2}=1$, and not both $z_{5}=z_{6}=0$. Then there is a column $\mathbf{h}_{i}$ in $C^{*}$ of the form $\left(z_{1}, z_{2}, x, 0,0,0\right)$. If $x=z_{3}$, then we use the result from Case 2 to express the point $\left(0,0,0, z_{4}, z_{5}, z_{6}\right)$ as a linear combination of at most two columns of $\mathbf{H}$.

TABLE 3.

| $\overline{q \backslash k}$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 4 | - | 2 | 1 |  |  |  |  |  |  |  |  |  |  |  |  |
| 16 | - | 12 | 9 | 4 | 3 | 10 | 8 | 13 | 6 | 2 | 5 | 14 | 1 | 7 | 11 |

Also, due to the symmetry, there is a column $\mathbf{h}_{j}$ with $2 q+1 \leq j \leq 3 q+1$ of the form $a^{-1}\left(0,0,0, y, z_{5}, z_{6}\right)$, and the case is settled if $y=z_{4}$.
If $x \neq z_{3}$ and $y \neq z_{4}$, then we get $Z=\mathbf{h}_{i}+a \mathbf{h}_{j}+\left(z_{3}-x\right)\left(0,0,1,\left(z_{4}-y\right) /\left(z_{3}-x\right), 0,0\right)$. This completes the final case and the whole proof.

It is interesting to see that the construction also works for $q=2$ (with a slightly altered proof), and then gives a set corresponding to $k(5,2,2)=7$. In coding theoretic terms, this is a so-called perfect code.
By $k(1, q, 1)=q+1$ and Theorems 4 and 5 , we find that $k(5, q, 2) \leq 3 q+2$. The current construction gives a slight improvement (by 1) on this size.
Attempts were made to find smaller 2-saturating sets than those given by Theorem 7 using a computer, but without success. This indicates that, at least for small values of $q$, the construction is effective.

## 5. A TABLE

The best known bounds on $k(r, q, 2)$ for $q \leq 16$ are displayed in Table 1. A period indicates an exact value. All these follow from the so-called sphere covering bound in coding theory, except for the cases $k(3,5,2)=6, k(3,7,2)=7, k(3,8,2)=7, k(3,9,2)=7$, and $k(4,3,2)=8$, which have been proved by Penttila [20]. Bounds can sometimes be obtained in several ways, but we have restricted the keys to one construction or reference.
Several of the bounds in Table 1 were found by computer search. The saturating sets found in this way are explicitly listed in Table 2 . We used a stochastic search method called tabu search, and applied this to our problem as described in [15].

In listing the sets, we use the following convention for the field elements. If $q$ is a prime field, the elements are $G F(q)=\{0,1, \ldots, q-1\}$ and we operate on these modulo $q$. In the case of an extension field, we denote $G F(q)=\left\{0,1=\alpha^{0}, 2=\alpha^{1}, \ldots, q-1=\alpha^{q-2}\right\}$, where $\alpha$ is a primitive element. This defines multiplication. Addition is defined using Zech logarithms. The Zech logarithm is the function $Z(k)$ for which $\alpha^{Z(k)}=1+\alpha^{k}$. The Zech logarithms for the extension fields used can be found in Table 3. A dash denotes $1+\alpha^{k}=0$. The primitive polynomials used to generate the fields are $x^{2}+x+1$ for $q=4$ and $x^{4}+x^{3}+1$ for $q=16$.

## Acknowledgements

This work was carried out while the first author was visiting Helsinki University of Technology. He gratefully acknowledges the Academy of Finland and Helsinki University of Technology for hospitality during this visit. This work was supported by the Academy of Finland.

## REFERENCES

1. V. Abatangelo, A class of complete $((q+8) / 3)-\operatorname{arcs}$ in $P G\left(2,2^{h}\right)(h \geq 6$ even $)$, Ars Comb., 16 (1983), 103-111.
2. T. S. Baicheva and E. D. Velikova, Covering radii of ternary linear codes of small dimensions and codimensions, IEEE Trans. Inf. Theory, 43 (1997), 2057-2061; and 44 (1998), 2032.
3. R. A. Brualdi, V. S. Pless and R. M. Wilson, Short codes with a given covering radius, IEEE Trans. Inf. Theory, 35 (1989), 99-109.
4. J. C. Cock and P. R. J. Östergård, Ternary covering codes derived from BCH codes, J. Comb. Theory, Ser. A, 80 (1997), 283-289.
5. G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, Covering Codes, North-Holland, Amsterdam, The Netherlands, 1997.
6. A. A. Davydov, Constructions and families of covering codes and saturated sets of points in projective geometry, IEEE Trans. Inf. Theory, 41 (1995), 2071-2080.
7. A. A. Davydov, Constructions and families of nonbinary linear codes with covering radius 2, IEEE Trans. Inf. Theory, 45 (1999), 1679-1686.
8. A. A. Davydov and A. Y. Drozhzhina-Labinskaya, Constructions, families, and tables of binary linear covering codes, IEEE Trans. Inf. Theory, 40 (1994), 1270-1279.
9. A. A. Davydov and P. R. J. Östergård, New linear codes with covering radius 2 and odd basis, Des. Codes Cryptogr., 16 (1999), 29-39.
10. A. A. Davydov and P. R. J. Östergård, New quaternary linear codes with covering radius 2, Finite Fields Appl., 6 (2000), 164-174.
11. E. M. Gabidulin, A. A. Davydov and L. M. Tombak, Linear codes with covering radius 2 and other new covering codes, IEEE Trans. Inf. Theory, 37 (1991), 219-224.
12. R. L. Graham and N. J. A. Sloane, On the covering radius of codes, IEEE Trans. Inf. Theory, $\mathbf{3 1}$ (1985), 385-401.
13. J. W. P. Hirschfeld, Maximum sets in finite projective spaces, in: Surveys in Combinatorics, L.M.S. Lecture Notes, 82, E. K. Lloyd (ed.), Cambridge University Press, Cambridge, UK, 1983, pp. 5576.
14. J. W. P. Hirschfeld, Projective Geometries over Finite Fields, 2nd edn, Clarendon Press, Oxford, UK, 1998.
15. I. S. Honkala and P. R. J. Östergård, Code design, in: Local Search in Combinatorial Optimization, E. Aarts and J. K. Lenstra (eds), Wiley, New York, 1997, pp. 441-456.
16. H. Janwa, Some optimal codes from algebraic geometry and their covering radii, Europ. J. Combinatorics, 11 (1990), 249-266.
17. G. Korchmáros, New examples of complete $k$-arcs in $P G(2, q)$, Europ. J. Combinatorics, 4 (1983), 329-334.
18. P. R. J. Östergård, Computer search for small complete caps, J. Geom., to appear.
19. F. Pambianco and L. Storme, Small complete caps in spaces of even characteristic, J. Comb. Theory, Ser. A, 75 (1996), 70-84.
20. T. Penttila, personal communication.
21. T. Szőnyi, Small complete arcs in Galois planes, Geom. Ded., 18 (1985), 161-172.
22. E. Ughi, Saturated configurations of points in projective Galois spaces, Europ. J. Combinatorics, 8 (1987), 325-334.
23. J. F. Voloch, On the completeness of certain plane arcs II, Europ. J. Combinatorics, 11 (1990), 491-496.

Institute for Information Transmission Problems,
Russian Academy of Sciences,
Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 101447

Russia
AND
Patric R. J. Östergård
Department of Computer Science and Engineering,
Helsinki University of Technology,
P.O. Box 5400, 02015 HUT, Finland

