Journal of Statistical Planning and Inference 95 (2001) 167–173

journal of statistical planning and inference

www.elsevier.com/locate/jspi

Recursive constructions of complete caps[☆]

Alexander A. Davydov[a], Patric R.J. Östergård[b, *]

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

[b] *Department of Computer Science and Engineering, Helsinki University of Technology, P.O. Box 5400, 02015 HUT Finland*

Dedicated to S.S. Shrikhande

Abstract

We present three constructions of complete caps in PG(d,q), q odd, where complete caps in a projective space of smaller dimension are involved. We thereby obtain new series of upper bounds on $n_2(d,q)$, the smallest number of points in a complete cap in PG(d,q). The constructions show that for $k \geqslant 0$, $n_2(k+1,3) \leqslant 2n_2(k,3)$; $n_2(4k+2,q) \leqslant q^{2k+1} + n_2(2k,q)$ for $q \geqslant 5$ an odd prime power; and $n_2(4k+2,q) \leqslant q^{2k+1} - (q+1) + n_2(2k,q) + n_2(2,q)$ for $q \geqslant 9$ an odd prime power. © 2001 Elsevier Science B.V. All rights reserved.

MSC: 51E22

Keywords: Complete cap; Finite field; Projective geometry

1. Introduction

Let q be a prime power. We denote the finite field of order q by F_q and let $F_q^* = F_q \backslash \{0\}$. Complete caps in PG$(d,q)$, the projective space of dimension d over F_q, have a long history in projective geometry (Hirschfeld, 1979). A *cap K* is a set of points no three of which are collinear, and it is *complete* if every point not in K is on a bisecant of K. The minimum number of points in a complete cap in PG(d,q) is denoted by $n_2(d,q)$.

Little is known about small complete caps for large dimensions. Recently, however, Pambianco and Storme (1996) were able to obtain constructions that give infinite families of complete caps for $q \geqslant 4$ even. They prove that for $k \geqslant 1$,

$$n_2(2k,q) \leqslant q^k + 3(q^{k-1} + q^{k-2} + \cdots + q) + 2, \tag{1}$$

$$n_2(2k+1,q) \leqslant 3(q^k + q^{k-1} + \cdots + q) + 2. \tag{2}$$

[☆] This work was supported by the Academy of Finland.

[*] Corresponding author.

E-mail address: pat@ultra.hut.fi (P.R.J. Östergård).

PII: S0378-3758(00)00286-X

These families of complete caps are obtained by starting from complete caps in $\mathrm{PG}(1,q)$ and $\mathrm{PG}(2,q)$ and recursively building up the whole family. This recursion is not general in the sense that it can only be applied to other, smaller complete caps of this family. Earlier Gabidulin et al. (1991) had obtained families of binary complete caps giving (for $k \geqslant 4$) the bounds

$$n_2(2k,2) \leqslant 23 \cdot 2^{k-3} - 3, \tag{3}$$

$$n_2(2k+1,2) \leqslant 30 \cdot 2^{k-3} - 3. \tag{4}$$

With a field of even characteristic, (1)–(4) give upper bounds on $n_2(d,q)$ for all dimensions $d \geqslant 8$. Less is known about small complete caps when the characteristic is odd. The published results are restricted to some exact values and bounds for small parameters; see Hirschfeld and Storme (1998); Östergård (to appear); Pambianco and Storme (1996); and references therein.

In this paper, we increase the knowledge about complete caps in spaces of odd characteristic by presenting three recursive constructions. These constructions have the property that they use complete caps that are not required to have any special properties.

The three new constructions are considered in Sections 2, 3, and 4, respectively. A construction for $q=3$ is given in Section 2, and a construction for $q \geqslant 5$ odd, $d \equiv 2 \pmod 4$, is given in Section 3. In Section 4, a slight improvement on the construction in Section 3 is obtained for $q \geqslant 9$ odd.

2. Ternary complete caps

The construction to be presented in this section has emerged from results on constructing caps in Mukhopadhyay (1978) and linear covering codes in Davydov (1996) and Östergård (1999).

Let K' be a complete cap in $\mathrm{PG}(k,3)$ and let $K_1 = \{(0,a) \mid a \in K'\} \cup \{(1,a) \mid a \in K'\}$.

Theorem 1. *K_1 is a complete cap in* $\mathrm{PG}(k+1,3)$.

Proof. We first show that K_1 is a cap. Clearly, all points in K_1 are different. For three $(i=1,2,3)$ different points (h_i,k_i), $h_i \in \{0,1\}$, $k_i \in K'$, in K_1 to be collinear, a necessary condition is that $s_1k_1+s_2k_2+s_3k_3=0$ $(s_i \in F_3^*)$, which is impossible since at most two of the k_is coincide and K' is a cap. Hence K_1 is a cap.

We now show that K_1 is complete. Take any nonzero point (a,b), $a \in \{0,1\}$, $b \in F_3^{k+1}$. Since K' is a complete cap, we can express a nonzero b as $b = sp+tq$ for two points $p,q \in K'$ $(p \neq q)$, where $s,t \in F_3$ are not both zero. Without loss of generality, it suffices to consider the following cases for expressing a point (a,b) as a linear combination of at most two points in K_1:

$a=0$: $\quad s(0,p)+t(0,q)$;

$a=1,\ b=0$: $\quad (1,c)+2(0,c)$ for any $c \in K'$;

$$\begin{array}{ll}
a=1,\ s=1,\ t=0: & (1,p);\\
a=1,\ s=2,\ t=0: & (1,p)+(0,p);\\
a=1,\ s=1,2,\ t=1: & s(0,p)+(1,q);\\
a=1,\ s=2,\ t=2: & 2(1,p)+2(1,q). \qquad \square
\end{array}$$

Corollary 1. *For $k \geqslant 0$, $n_2(k+1,3) \leqslant 2n_2(k,3)$.*

By using Theorem 1 repeatedly, starting from an initial, small complete cap, only the first few complete caps are good in the following sense. Following Pambianco and Storme (1996), we can calculate how many bisecants a point not in the complete cap belongs to on average. Direct calculations reveal that this parameter tends to infinity when the construction is applied repeatedly and the dimension tends to infinity.

Applied to the result $n_2(5,3) \leqslant 22$ from Pambianco and Storme (1996) (also obtained in Baicheva and Velikova (1997,1998)), Corollary 1 gives that $n_2(6,3) \leqslant 44$ (the upper bound in Pambianco and Storme (1996) is 55). The bound $n_2(5,3) \leqslant 22$ actually follows by applying Corollary 1 to $n_2(4,3) = 11$ (which comes from the ternary Golay code).

3. Complete caps for $q \geqslant 5$ odd

Let $V_1 = \{(1,\omega,\omega^2) \mid \omega \in F_{q^{2k+1}}\}$ and $V_2 = \{(0,0,v) \mid v \in K'\}$, where $q \geqslant 5$ is an odd prime power, $k \geqslant 0$, and K' is a complete cap in $\mathrm{PG}(2k,q)$. (Here and in the rest of the paper, we mainly consider triples in $F_q F_{q^m} F_{q^m}$, where the elements in F_{q^m} can be mapped to m-element vectors over F_q and vice versa.) We shall now prove that $K_2 = V_1 \cup V_2$ is a complete cap. (In the proof, QR stands for quadratic residue and QNR for quadratic nonresidue.)

Theorem 2. *K_2 is a complete cap in* $\mathrm{PG}(4k+2,q)$.

Proof. We first show that K_2 is a cap. First of all, no three points in V_1 are collinear, and no two points in V_1 together with one point in V_2 are collinear, since the determinants (the first matrix is a Vandermonde matrix)

$$\begin{vmatrix} 1 & 1 & 1 \\ \omega_1 & \omega_2 & \omega_3 \\ \omega_1^2 & \omega_2^2 & \omega_3^2 \end{vmatrix} = (\omega_2-\omega_1)(\omega_3-\omega_1)(\omega_3-\omega_2),$$

$$\begin{vmatrix} 1 & 1 & 0 \\ \omega_1 & \omega_2 & 0 \\ \omega_1^2 & \omega_2^2 & v \end{vmatrix} = v(\omega_2-\omega_1)$$

are nonzero when the points are distinct. Specifically, any three such points are linearly independent with coefficients from $F_{q^{2k+1}}$ and then also with coefficients from F_q. Since K' is a complete cap, no three points in V_2 are collinear. Finally, no bisecant of V_2 contains a point with a nonzero first coordinate.

Next we prove the completeness of K_2. A point $(a,b,c)\in F_qF_{q^{2k+1}}F_{q^{2k+1}}$ can be expressed in the following way as a linear combination with coefficients from F_q^* of at most two points in $V_1\cup V_2$ (note that $-1\in F_q^*$):

$a=b=0$:	Follows as V_2 is a complete cap in $\mathrm{PG}(2k,q)$;
$a=0,\ b\neq 0$:	$(1,u,u^2)-(1,v,v^2)$ with $u,v=(c\pm b^2)/2b$;
$a=1,\ c-b^2=0$:	$(1,b,b^2)$;
$a=1,\ c-b^2\neq 0$:	$(1-t)(1,u,u^2)+t(1,v,v^2)$ with $v=b+\sqrt{\frac{1-t}{t}(c-b^2)}$, $u=(b-tv)/(1-t)$, where $t\in F_q^*\backslash\{1\}$ such that $(1-t)/t$ and $(c-b^2)$ are both QRs or both QNRs.

Any one of the two possible values of the square root may be taken. In the last case, t has to be chosen based on whether $(c-b^2)$ is a QR or a QNR. For different $t\in F_q^*\backslash\{1\}$, we get different values of $(1-t)/t$, which are all in F_q^*. Now, since half of the elements in F_q^* are QRs (and the other half are QNRs) in $F_{q^{2k+1}}$ (Davydov and Östergård, 1999, Theorem 3), a feasible value of t can always be found if $q\geqslant 5$.

The cap in $\mathrm{PG}(4k+2,q)$ is explicitly obtained by mapping elements over $F_{q^{2k+1}}$ to $(2k+1)$-tuples over F_q. □

Also Theorem 2 has emerged from recent results in coding theory, cf. Davydov and Östergård (1999). Note that with $k=0$ we get the *oval* of $q+1$ points in the projective plane $\mathrm{PG}(2,q)$, $q\geqslant 5$ odd.

Corollary 2. *Let $q\geqslant 5$ be an odd prime power and $k\geqslant 0$. Then*

$$n_2(4k+2,q)\leqslant q^{2k+1}+n_2(2k,q).$$

The bound in Corollary 2 can be compared with that from (1) for even q, which after a parameter substitution reads $n_2(4k+2,q)\leqslant q^{2k+1}+3q^{2k}+\cdots$. We can also calculate the average number of bisecants through the points that are not in the complete cap. For the series of complete caps obtained by applying Theorem 2 repeatedly, starting from any complete cap in $\mathrm{PG}(d,q)$, d even, this average tends to

$$\frac{q}{2}-1+\frac{1}{2q}$$

as the dimension tends to infinity (for these series, the expression in Corollary 2 has $n_2(2k,q)\in O(q^k)$).

4. Complete caps for $q\geqslant 9$ odd

We shall now see how the construction presented in the previous section can be slightly improved for $q\geqslant 9$. Let $V_1=\{(1,\omega,\omega^2)\mid \omega\in F_{q^{2k+1}}\backslash F_q\}$, $V_2=\{(0,0,v)\mid v\in K'\}$ where K' is a complete cap in $\mathrm{PG}(2k,q)$, and $V_3=\{(a,b,c)\in F_qF_{q^{2k+1}}F_{q^{2k+1}}\mid b,c\in F_q\}$ such that when the points of V_3 are treated as points in F_q^3 these form a complete cap in PG$(2,q)$. Furthermore, we require that $(0,0,1)\in F_qF_{q^{2k+1}}F_{q^{2k+1}}$ is contained in both V_2 and V_3 (if necessary, projective transformations are applied to obtain sets that fulfill this requirement). Finally, let $K_3=V_1\cup V_2\cup V_3$.

Theorem 3. K_3 *is a complete cap in* PG$(4k+2,q)$.

Proof. We first prove that we have a cap. The proof of Theorem 2 can be used partially, since we have reduced V_1 and added a set of points V_3. It is thus sufficient to consider the following cases. Any point $(a,b,c)\in F_qF_{q^{2k+1}}F_{q^{2k+1}}$ lying on a bisecant of $V_2\cup V_3$ will have $b\in F_q$, so the point cannot be in V_1. Since $(0,0,1)\in V_2\cap V_3$ and V_2 and V_3 are complete caps with given parameters, it follows that no linear combination of two points from one set will be in the other set.

The only more complicated case is that of proving that no point in V_3 is on a bisecant of V_1. We first see when an arbitrary point $(0,b,c)\in F_qF_{q^{2k+1}}F_{q^{2k+1}}$, $b\neq 0$, can be obtained as a linear combination of two points from V_1. For $t\in F_q^*$ and $u,v\in F_{q^{2k+1}}$ we want to solve

$$t(1,u,u^2)-t(1,v,v^2)=(0,b,c) \tag{5}$$

and get the solution

$$u=\frac{b}{2t}+\frac{c}{2b},\quad v=-\frac{b}{2t}+\frac{c}{2b}. \tag{6}$$

Hence, if $b,t\in F_q^*$ and $c\in F_q$, then both u and v lie in the subfield F_q, and neither $(1,u,u^2)$ nor $(1,v,v^2)$ is in V_1.

The case with an arbitrary point $(1,b,c)\in F_qF_{q^{2k+1}}F_{q^{2k+1}}$ is similar. Now for $t\in F_q^*\backslash\{1\}$ and $u,v\in F_{q^{2k+1}}$ we get the equation

$$(1-t)(1,u,u^2)+t(1,v,v^2)=(1,b,c) \tag{7}$$

which has the solution (cf. the proof of Theorem 2)

$$v=b+\sqrt{\frac{1-t}{t}(c-b^2)},\quad u=\frac{b-tv}{1-t}, \tag{8}$$

where $(1-t)/t$ and $(c-b^2)$ are both QRs or both QNRs. Also in this case, if $b,c\in F_q$, we get that both u and v are in F_q (from Davydov and Östergård (1999), Theorem 3 we know that in the field $F_{q^{2k+1}}$ a square root of a square element in the subfield F_q is always in F_q).

We turn to the question of completeness, and consider an arbitrary point $(a,b,c)\in F_qF_{q^{2k+1}}F_{q^{2k+1}}$. We consider the cases $a=0$ and $a=1$ separately, starting with $a=0$. If $b=0$, then we are done as V_2 is a complete cap in PG$(2k,q)$. If $b,c\in F_q$, then we use the fact that V_3 is a complete cap in PG$(2,q)$. If $b\in F_q^*$ and $c\notin F_q$, then it follows from (6) that $u,v\notin F_q$, and we have a solution of (5) with points from V_1. Hence we are left with the case $b\notin F_q$, for which we will find a solution of the form (5).

Let u',v' and u'',v'' be the two solutions (6) corresponding to the distinct values t' and t'', respectively, of the parameter t. Note that t and $-t$ give the same solution of

(5) with the values of u and v in (6) interchanged. Now we have that

$$u' - u'' = \frac{b}{2}\left(\frac{1}{t'} - \frac{1}{t''}\right),$$

$$v' - v'' = -\frac{b}{2}\left(\frac{1}{t'} - \frac{1}{t''}\right).$$

Since $t', t'' \in F_q^*$ and $b \in F_{q^{2k+1}} \backslash F_q$, these differences are in $F_{q^{2k+1}} \backslash F_q$, so if $u' \in F_q$ then $u'' \in F_{q^{2k+1}} \backslash F_q$, and if $u'' \in F_q$ then $u' \in F_{q^{2k+1}} \backslash F_q$ (and similarly for v' and v''). Hence for at most one value of t we have $u \in F_q$ ($v \in F_q$). So for all but at most one pair of values of t, $\{t, -t\}$, we have that $u, v \in F_{q^{2k+1}} \backslash F_q$, and a required solution always exists when $(q-1)/2 - 1 \geqslant 1$, that is, $q \geqslant 5$.

We finally consider $a = 1$, that is, we consider an arbitrary point $(1, b, c) \in F_q F_{q^{2k+1}} F_{q^{2k+1}}$. If $b, c \in F_q$, then we use the fact that V_3 is a complete cap in PG$(2, q)$. If $b \in F_q$ and $c \notin F_q$, then it follows from (8) that $u, v \notin F_q$, and we have a solution of (7) with points from V_1; the same holds for $b \notin F_q$ and $(c - b^2) \in F_q^*$. The case $c - b^2 = 0$ with $b \in F_{q^{2k+1}} \backslash F_q$ is taken care of by a single point $(1, b, b^2) \in V_1$.

We still have to consider the case $b \in F_{q^{2k+1}} \backslash F_q$, $c - b^2 \in F_{q^{2k+1}} \backslash F_q$. Let u', v' and u'', v'' be two solutions of (7) corresponding to the values t' and t'', respectively, of the parameter t. Now t and $1 - t$ give the same solution of (7) with the values of u and v in (8) interchanged. We have that

$$(v' - v'')^2 = (c - b^2)\left(\frac{1-t'}{t'} - 2\sqrt{\frac{(1-t')(1-t'')}{t't''}} + \frac{1-t''}{t''}\right).$$

Since $t', t'' \in F_q^* \backslash \{1\}$ and $c - b^2 \in F_{q^{2k+1}} \backslash F_q$, we get that $(v' - v'')^2 \in F_{q^{2k+1}} \backslash F_q$. If $v' \in F_q$, then $v'' \in F_{q^{2k+1}} \backslash F_q$, and if $v'' \in F_q$, then $v' \in F_{q^{2k+1}} \backslash F_q$ (and similarly for u' and u'' using (8) or the comment above regarding solutions with the values of u and v interchanged). Thus at most one value of t gives $v \in F_q$ ($u \in F_q$). We also have to take into account that $(1-t)/t$ must be either QR or QNR depending on the residue of $c - b^2$ (note that for $t' = 1 - t$, $(1 - t')/t' = t/(1 - t)$). There are now $(q-1)/2$ sets $\{t, 1-t\}$ for $t \in F_q^* \backslash \{1\}$, one of which consists of only one element (for $t = \frac{1}{2}$; then $(1-t)/t = 1$ is a QR). For $\lfloor (q-1)/4 \rfloor$ sets, $(1-t)/t$ is a QNR and for $\lceil (q-1)/4 \rceil$ sets, $(1-t)/t$ is a QR. To complete the proof, a required solution exists when $\lfloor (q-1)/4 \rfloor - 1 \geqslant 1$, that is, when $q \geqslant 9$. □

Corollary 3. *Let $q \geqslant 9$ be an odd prime power and $k \geqslant 0$. Then $n_2(4k+2, q) \leqslant q^{2k+1} - (q+1) + n_2(2k, q) + n_2(2, q)$.*

Note that for q odd, from Hirschfeld (1983) we have the bound $n_2(2, q) \leqslant (q+3)/2$, so for $q \geqslant 9$ the result in Corollary 3 is indeed an improvement on that in Corollary 2.

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.

References

Baicheva, T.S., Velikova, E.D., 1997. Covering radii of ternary linear codes of small dimensions and codimensions. IEEE Trans. Inform. Theory 43, 2057–2061.

Baicheva, T.S., Velikova, E.D., 1998. Covering radii of ternary linear codes of small dimensions and codimensions. IEEE Trans. Inform. Theory 44, 2032 (E).

Davydov, A.A., 1996. On nonbinary linear codes with covering radius two. Proceedings of the Fifth International Workshop on Algebraic and Combinatorial Coding Theory. Unicorn, Shumen, Bulgaria, pp. 105–110.

Davydov, A.A., Östergård, P.R.J., 1999. New linear codes with covering radius 2 and odd basis. Designs Codes Cryptogr. 16, 29–39.

Gabidulin, E.M., Davydov, A.A., Tombak, L.M., 1991. Linear codes with covering radius 2 and other new covering codes. IEEE Trans. Inform. Theory 37, 219–224.

Hirschfeld, J.W.P., 1979. Projective Geometries over Finite Fields. Clarendon, Oxford, 2nd Edition, 1998.

Hirschfeld, J.W.P., 1983. Maximum sets in finite projective spaces. In: Lloyd, E.K. (Ed.), Surveys in Combinatorics, London Mathematical Society Lecture Note Series, Vol. 82. Cambridge University Press, Cambridge, pp. 55–76.

Hirschfeld, J.W.P., Storme, L., 1998. The packing problem in statistics, coding theory and finite projective spaces. J. Statist. Plann. Inference 72, 355–380.

Mukhopadhyay, A.C., 1978. Lower bounds on $m_t(r,s)$. J. Combin. Theory. Ser. A 25, 1–13.

Östergård, P.R.J., 1999. New constructions for q-ary covering codes. Ars Combin. 52, 51–63.

Östergård, P.R.J. Computer search for small complete caps. J. Geom., to appear.

Pambianco, F., Storme, L., 1996. Small complete caps in spaces of even characteristic. J. Combin. Theory Ser. A 75, 70–84.