Quasi-perfect linear codes from singular plane cubics

Massimo Giulietti[1]

Abstract. We present some recently obtained constructions of quasi-perfect linear codes with small density arising from plane cubic curves defined over finite fields.

1 Introduction

Galois Geometry, that is the theory of combinatorial objects embedded in projective spaces over finite fields, is well known to be rich of nice algebraic, combinatorial and group theoretic aspects that have also found wide and relevant applications in Coding Theory and Cryptography; see *e.g.* the monography [5]. In this context an important role is played by plane arcs and their generalizations - especially complete caps, saturating sets and arcs in higher dimensions - since their code theoretic counterparts are distinguished types of error-correcting and covering linear codes. In this extended abstract we present some recent results on small complete caps and quasi-perfect linear codes, obtained in few joint works with N. Anbar, D. Bartoli and I. Platoni, mostly unpublished.

Let $\mathbb{F}_q$ be the finite field with q elements and let $\mathbf{C}$ be an $[n,k,d]_q$-code, *i.e.*, a q-ary linear code of length n, dimension k and minimum distance d. The covering radius of $\mathbf{C}$ is the minimum integer $R(\mathbf{C})$ such that for any vector $\mathbf{v} \in \mathbb{F}_q^n$ there exists $\mathbf{x} \in C$ with $d(\mathbf{v},\mathbf{x}) \leq R(\mathbf{C})$. An $[n,k,d]_q$-code with covering radius R is denoted by $[n,k,d]_q R$. Let t be the integer part of $(d-1)/2$. Clearly, $R(\mathbf{C}) \geq t$ holds and when equality is attained the code $\mathbf{C}$ is said to be perfect. As there are only finitely many classes of linear perfect codes, of particular interest are those codes $\mathbf{C}$ with $R(\mathbf{C}) = t+1$, called quasi-perfect codes. One of the parameters characterizing the covering quality of an $[n,k,d]_q R$-code $\mathbf{C}$ is its covering density $\mu(\mathbf{C})$, introduced in [3] as the average number of codewords at distance less than or equal to R from a vector in $\mathbb{F}_q^n$. The covering

[1] Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Italia. Email: giuliet@dmi.unipg.it

J. Nešetřil et al. (eds.), *The Seventh European Conference on Combinatorics, Graph Theory and Applications*

density $\mu(\mathbf{C})$ is always greater than or equal to 1, and equality holds precisely when $\mathbf{C}$ is perfect. Among codes with the same codimension s and covering radius R, the shortest ones have the best covering density. This explains why the problem of determining the minimal length n for which there exists an $[n, n-s, d]_q R$-code with given s, q, d and R, has been broadly investigated. Throughout, such minimal length will be denoted as $l(s, R, q)_d$.

Here we will restrict our attention to codes with covering radius $R = 2$ and $d = 4$, *i.e.* quasi-perfect linear codes that are both 1-error correcting and 3-error detecting. Interestingly, such codes have a nice geometrical counterpart: the columns of a parity check matrix of an $[n, n-s, 4]_q 2$-code can be considered as points of a complete cap of size n in the finite projective space $PG(s-1, q)$. In particular, $l(s, 2, q)_4$ coincides with the minimum size of a complete cap in $PG(s-1, q)$. This makes it possible to use methods from both Galois Geometries and Algebraic Geometry in order to investigate covering-radius-2 codes with small density. Here, we are going to discuss some recently obtained upper bounds on the minimum size of a complete cap which are valid for arbitrarily large values of q. The key tool is the construction of complete caps in higher dimensional spaces from singular plane cubic curves defined over $\mathbb{F}_q$.

2 Complete caps from bicovering arcs

An n-cap in an (affine or projective) Galois space over $\mathbb{F}_q$ is a set of n points no three of which are collinear. An n-cap is said to be complete if it is not contained in an $(n+1)$-cap. A plane n-cap is also called an n-arc. Let $t\,(AG\,(N, q))$ be the size of the smallest complete cap in the Galois affine space $AG(N, q)$ of dimension N over $\mathbb{F}_q$. Since the affine space $AG(N, q)$ is embedded in the projective space $PG(N, q)$, a complete cap in $AG(N, q)$ can be viewed as a cap in $PG(N, q)$, whose completeness can be achieved by adding some extra-points at the hyperplane at infinity. Therefore, the following relation holds.

Proposition 2.1. *Let $M(N, q)$ denote the maximal size of a complete cap in $PG(N-1, q)$. Then*

$$l(N+1, 2, q)_4 \leq t(AG(N, q)) + M(N, q).$$

In particular, $l(5, 2, q)_4 \leq t(AG(4, q)) + q^2 + 1$.

The trivial lower bound for $t(AG(N, q))$ is $\sqrt{2}q^{\frac{N-1}{2}}$. General constructions of complete caps whose size is close to this lower bound are only known for q even and N odd. When N is even, complete caps of size

of the same order of magnitude as $cq^{N/2}$, with c a constant independent of q, are known to exist for both the odd and the even order case.

Small complete caps in dimensions $N \equiv 0 \pmod 4$ can be obtained from plane arcs via the product method for caps: let $q' = q^{\frac{N-2}{2}}$ and fix a basis of $\mathbb{F}_{q'}$ as a linear space over $\mathbb{F}_q$; identify points in $AG(N,q)$ with vectors of $\mathbb{F}_{q'} \times \mathbb{F}_{q'} \times \mathbb{F}_q \times \mathbb{F}_q$; for an arc A in $AG(2,q)$, let

$$K_A = \{(\alpha, \alpha^2, u, v) \in AG(N,q) \mid \alpha \in \mathbb{F}_{q'}, (u,v) \in A\};$$

then the set K_A is a cap in $AG(N,q)$. For q odd, the completeness of the cap K_A depends on the bicovering properties of A in $AG(2,q)$; see Theorem 2.3 below. According to Segre [6], given three pairwise distinct points P, P_1, P_2 on a line ℓ in $AG(2,q)$, P is external or internal to the segment P_1P_2 depending on whether $(x-x_1)(x-x_2)$ is a non-zero square or a non-square in $\mathbb{F}_q$, where x, x_1 and x_2 are the coordinates of P, P_1 and P_2 with respect to any affine frame of ℓ.

Definition 2.2. Let A be a complete arc in $AG(2,q)$. A point $P \in AG(2,q) \setminus A$ is said to be bicovered with respect to A if there exist $P_1, P_2, P_3, P_4 \in A$ such that P is both external to the segment P_1P_2 and internal to the segment P_3P_4. If every $P \in AG(2,q) \setminus A$ is bicovered by A, then A is said to be a bicovering arc.

Theorem 2.3 ([4]). *Let A be a bicovering n-arc in $AG(2,q)$; then K_A is a complete cap in $AG(N,q)$.*

3 Small complete caps from cubic curves

From now on we assume that the characteristic of $\mathbb{F}_q$ is $p > 3$. Let $\mathcal{X}$ be an irreducible plane cubic curve defined over $\mathbb{F}_q$, and consider the set G of the non-singular $\mathbb{F}_q$-rational points of $\mathcal{X}$. As it is well known, for any point O of G it is possible to give a group structure to G, by defining a binary operation $\boxplus$ in such a way that $(G, \boxplus)$ is an abelian group with neutral element $O \in G$. The point O is usually chosen as an inflection point. One of the main properties of this operation is that three distinct points in G are collinear if and only if their sum is the neutral element in G. Then it is easy to see that for a subgroup H of G of index m, with $(3,m) = 1$, and a point P in $G \setminus H$, the coset $K = H \boxplus P$ is an arc.

In order to investigate the covering properties of such an arc, we recall a general method, due to Segre and Lombardo-Radice, that uses Hasse-Weil's Theorem to prove the completeness of arcs contained in conic or cubic curves. This method is based on the following idea for proving that the secants of K cover a generic point P off the curve $\mathcal{X}$: (1) write K in an algebraically parametrized form; in the case of cubic curves $\mathcal{X}$, this

can be easily done when $\mathcal{X}$ is singular; (2) construct an algebraic curve $\mathcal{C}_P$, defined over $\mathbb{F}_q$, describing the collinearity of two points of K and P; (3) show that $\mathcal{C}_P$ is absolutely irreducible or has at least an absolutely irreducible component defined over $\mathbb{F}_q$; (4) apply the Hasse-Weil bound to guarantee the existence of a suitable $\mathbb{F}_q$-rational point of $\mathcal{C}_P$ (or of its irreducible component): this is sufficient to deduce the collinearity between P and two points in K. Finally, in order to obtain the completeness, it might be necessary to extend the arc K with some points on $\mathcal{X}$.

By Theorem 2.3, bicovering arcs in affine planes are a powerfool tool to construct small complete caps in $AG(N,q)$ with q odd and $N \equiv 0 \pmod 4$. However, to establish whether a complete arc is bicovering can be a difficult task. So far, three different types of irreducible plane cubic curves have been investigated in order to prove the bicovering properties of the associated arcs: non-singular, cuspidal and nodal. The non-singular (or elliptic) case was investigated in [1].

Theorem 3.1 ([1]). *Let q be odd, and let m be a prime divisor of $q-1$, with $7 < m < \frac{1}{8}\sqrt[4]{q}$. Assume that the cyclic group of order m admits a maximal-3-independent subset of size s. Then for any positive integer $N \equiv 0 \pmod 4$,*

$$t(AG(N,q)) \le s \cdot q^{\frac{N-2}{2}} \cdot \left(\left\lfloor \frac{q - 2\sqrt{q} + 1}{m} \right\rfloor + 31 \right). \tag{3.1}$$

It has been noticed in [7] that in the cyclic group of order m there exists a maximal 3-independent subset of size $s \le (m+1)/3$. For specific values of m, the upper bound on $t(AG(N,q))$ can be improved, as there exist maximal-3-independent subsets of the cyclic group of order m of size significantly less than $m/3$ (see [1, Table 1]).

The case of a cubic with a cuspidal rational singularity and a rational inflection point is the object of the preprint [2].

Theorem 3.2 ([2]). *Let $q = p^h$ with $p > 3$ a prime, $h > 8$. Let $N \equiv 0 \pmod 4$, $N \ge 4$. Let t_h be the integer in $\{1, \ldots, 4\}$ such that $t_h \equiv h \pmod 4$. Assume that $p^{t_h} > 144$. Then*

$$t(AG(N,q)) \le 2pq^{\frac{N}{2} - \frac{1}{8}}.$$

We now present some new results on cubics with both a rational node and a rational inflection point, which for infinite q's improve both Theorems 3.1 and 3.2.

Theorem 3.3. *Let m be an odd divisor of $q-1$ such that $(3,m) = 1$ and*

$$q + 1 - (12m^2 - 8m + 2)\sqrt{q} \ge 8m^2 + 8m + 1. \tag{3.2}$$

Assume that the cyclic group of order m admits a maximal 3-independent subset of size s. Then there exists a bicovering arc in $AG(2,q)$ of size $\frac{s(q-1)}{m}$ contained in the cubic curve with equation $XY = (X-1)^3$.

Theorem 3.3 can be used together with Theorem 2.3 in order to construct small complete caps in affine spaces. Note that (3.2) holds whenever $m \leq \frac{\sqrt[4]{q}}{3.5}$.

Corollary 3.4. *Let m be an odd divisor of $q-1$ such that $(3,m)=1$ and $m \leq \frac{\sqrt[4]{q}}{3.5}$. Assume that the cyclic group of order m admits a maximal 3-independent subset of size s. Then for $N \equiv 0 \pmod 4$, $N \geq 4$,*

$$t(AG(N,q)) \leq \frac{s(q-1)}{m} q^{\frac{N-2}{2}}.$$

In the case where a group $\mathcal{G}$ is the direct product of two groups $\mathcal{G}_1 \times \mathcal{G}_2$ of order at least 4, neither of which elementary 3-abelian, there exists a maximal 3-independent subset of $\mathcal{G}$ of size less than or equal to $(\#\mathcal{G}_1) + (\#\mathcal{G}_2)$. Then the following holds.

Theorem 3.5. *Let m be an odd divisor of $q-1$ such that $(3,m)=1$ and $m \leq \frac{\sqrt[4]{q}}{3.5}$. Assume that $m = m_1 m_2$ with $(m_1, m_2) = 1$ and $m_1, m_2 \geq 4$. Then for $N \equiv 0 \pmod 4$, $N \geq 4$*

$$t(AG(N,q)) \leq \frac{(m_1+m_2)(q-1)}{m_1 m_2} q^{\frac{N-2}{2}}$$

Corollary 3.6. *Let $q = \bar{q}^8$ for an odd prime power $\bar{q}$. Let $m = (\bar{q}^2-1)/(2^h 3^k)$, where $2^h \geq 4$ is the highest power of 2 which divides $\bar{q}^2-1$, and similarly $3^k \geq 3$ is the highest power of 3 which divides $\bar{q}^2-1$. Then for $N \equiv 0 \pmod 4$, $N \geq 4$*

$$t(AG(N,q)) \leq (2^{h_2} + 2^{h_1} 3^k) q^{\frac{N}{2} - \frac{1}{8}}.$$

with $h_1 + h_2 = h$.

Results on complete arcs contained in cubics with an isolated double point have not appeared in the literature so far. This case is currently under investigation by the authors of [2].

References

[1] N. Anbar and M. Giulietti, *Bicovering arcs and complete caps from elliptic curves*, J. Algebraic Combin., published online 25/10/2012, DOI: 10.1007/s10801-012-0407-8.

[2] N. ANBAR, D. BARTOLI, M. GIULIETTI and I. PLATONI, *Small complete caps from singular cubics*, preprint.

[3] G. D. COHEN, A. C. LOBSTEIN and N. J. A. SLOANE, *Further results on the covering radius of codes*, IEEE Trans. Inform. Theory **32** (5) (1986), 680–694.

[4] M. GIULIETTI, *Small complete caps in Galois affine spaces*, J. Algebraic Combin. **25** (2) (2007), 149–168.

[5] J. W. P. HIRSCHFELD, "Projective Geometries over Finite Fields", Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, second edition, 1998.

[6] B. SEGRE, *Proprietà elementari relative ai segmenti ed alle coniche sopra un campo qualsiasi ed una congettura di Seppo Ilkka per il caso dei campi di Galois*, Ann. Mat. Pura Appl. (4) **96** (1972), 289–337.

[7] J. F. VOLOCH, *On the completeness of certain plane arcs. II*, European J. Combin. **11** (5) (1990), 491–496.