

# Bounds for Complete Arcs in PG$(3, q)$ and Covering Codes of Radius 3, Codimension 4, Under a Certain Probabilistic Conjecture

Alexander A. Davydov[1(✉)], Stefano Marcugini[2], and Fernanda Pambianco[2]

[1] Institute for Information Transmission Problems (Kharkevich Institute), Russian Academy of Sciences, Moscow, Russia
adav@iitp.ru

[2] Department of Mathematics and Computer Science, Perugia University, Perugia, Italy
{stefano.marcugini,fernanda.pambianco}@unipg.it

**Abstract.** Let $t(N, q)$ be the smallest size of a complete arc in the $N$-dimensional projective space PG$(N, q)$ over the Galois field of order $q$. The $d$-length function $\ell_q(r, R, d)$ is the smallest length of a $q$-ary linear code of codimension (redundancy) $r$, covering radius $R$, and minimum distance $d$; in particular, $\ell_q(4, 3, 5)$ is the smallest length $n$ of an $[n, n-4, 5]_q 3$ quasi-perfect MDS code. By the definitions, $\ell_q(4, 3, 5) = t(3, q)$. In this paper, a step-by-step construction of complete arcs in PG$(3, q)$ is considered. It is proved that uncovered points are uniformly distributed in the space. A natural conjecture on quantitative estimations of the construction is presented. Under this conjecture, new upper bounds on $t(3, q)$ are obtained, in particular, $t(3, q) < 2.93\sqrt[3]{q \ln q}$.

**Keywords:** Arcs in projective spaces · Covering codes · The $d$-length function

## 1 Introduction

Let $\mathbb{F}_q$ be the Galois field with $q$ elements. Denote by $\mathbb{F}_q^n$ the $n$-dimensional vector space over $\mathbb{F}_q$. Let PG$(N, q)$ be the $N$-dimensional projective space over $\mathbb{F}_q$. For

The research of A. A. Davydov was done at IITP RAS and supported by the Russian Government (Contract No. 14.W03.31.0019). The research of S. Marcugini and F. Pambianco was supported in part by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INDAM) and by University of Perugia (Project: Curve, codici e configurazioni di punti, Base Research Fund 2018). This work has been carried out using computing resources of the federal collective usage center Complex for Simulation and Data Processing for Mega-science Facilities at NRC "Kurchatov Institute", http://ckp.nrcki.ru/.

© Springer Nature Switzerland AG 2020
O. Gervasi et al. (Eds.): ICCSA 2020, LNCS 12249, pp. 107–122, 2020.
https://doi.org/10.1007/978-3-030-58799-4_8

an introduction to projective spaces over finite fields and connections between the projective geometry and covering codes, see [10,14,16–22].

An $n$-arc in $\mathrm{PG}(N,q)$ with $n > N+1$ is a set of $n$ points such that no $N+1$ points belong to the same hyperplane of $\mathrm{PG}(N,q)$. An $n$-arc is complete if it is not contained in an $(n+1)$-arc.

Let $t(N,q)$ be *the smallest size of a complete arc in* $\mathrm{PG}(N,q)$. The value of $t(N,q)$ is an important open problem. The spectrum of possible sizes of complete arcs is one of the essential tasks in study of projective spaces.

Denote by $[n, n-r, d]_q R$ a $q$-ary linear code of length $n$, codimension (redundancy) $r$, minimum distance $d$, and covering radius $R$. The covering radius of a linear code of length $n$ is the least integer $R$ such that the space $\mathbb{F}_q^n$ is covered by spheres of radius $R$ centered at the codewords. For an introduction to coverings of vector Hamming spaces over finite fields, see [7,8,10].

The covering density of an $[n, n-r, d]_q R$-code is the ratio of the total volume of all $q^{n-r}$ spheres of radius $R$ centered at the codewords to the volume of the space $\mathbb{F}_q^n$. The covering quality of a code is better if its covering density is smaller. Codes providing a convenient covering density are called *covering codes* [4,5,7,8,10–14,16,22,23]. Covering codes are applied, e.g. to data compression, decoding errors and erasures, football pools, write-once memories [8]. For fixed $q$, $r$, $R$, the covering density of an $[n, n-r, d]_q R$ code decreases with decreasing $n$.

Let *the length function* $\ell_q(r,R)$ be the smallest length of a $q$-ary linear code of codimension (redundancy) $r$ and covering radius $R$ [7,8]. Let *the d-length function* $\ell_q(r,R,d)$ be the smallest length of a $q$-ary linear code of codimension $r$, covering radius $R$, and minimum distance $d$ [5,6,11]. We have $\ell_q(r,R) \le \ell_q(r,R,d)$.

Columns of a parity check matrix of an $[n, n-N-1, N+2]_q N$ maximum distance separable (MDS) code can be considered as points (in homogeneous coordinates) of a complete $n$-arc in $\mathrm{PG}(N,q)$ [4–6,10,14,16,18,20,22]. If $N = 2, 3$ these codes are quasi-perfect. Arcs and linear MDS codes are equivalent objects. We have $\ell_q(N+1,N) \le \ell_q(N+1,N,N+2) = t(N,q),\ \ell_q(4,3,5) = t(3,q)$.

The value of $\ell_q(N+1,N,N+2)$ is an open important problem studied insufficiently, see e.g. [6, Introduction], [15, Remark 1].

This paper is devoted to upper bounds on $t(3,q)$ that are also upper bounds on the smallest length $\ell_q(4,3,5)$ of an $[n, n-4, 5]_q 3$ quasi-perfect MDS code.

The known results on $t(N,q)$ and $\ell_q(N+1,N,N+2)$, $N \ge 2$, can be found in [1–6,13,26], see also the references therein. In [1–4], the case $N = 2$ is considered. In [6,26], algebraic constructions for $N \ge 3$ are proposed. Computer search results for $N = 3, 4$ are given in [4,5,13].

In this paper, under a natural probabilistic conjecture, we obtain new upper bounds on $t(3,q)$. The new bounds are better than the known ones. In particular, the smallest known complete arcs obtained by algebraic constructions have size of order $\simeq q^{3/4}$ [6,26] while the bounds of this paper for $N = 3$ are of order $\simeq (q \ln q)^{1/3}$. Also, in this paper, the computer search is made in a more wide region of $q$ than in [4,5,13]; many results of these papers are improved.

Some results of this paper were briefly presented in [11]. Unfortunately, in [11], some inaccuracies are present in the proof of the main result. In this

paper, we *correct the inaccuracies of* [11]; for this we introduce a new tool called "implicit bound", see Sect. 2 (including Remark 1) and Sect. 6. Also, in comparison with [11], in this paper we decrease the constant (2.93 instead of 3) before $\sqrt[3]{q \ln q}$ and increase the range of $q$ values in computer search. This is essential for the initial part of the combined bound on $t(3, q)$ in Theorem 6.

The paper is organized as follows. In Sect. 2, the main results are presented. In Sect. 3, an iterative step-by-step construction of complete arcs is considered. In Sect. 4, it is proved that uncovered points are uniformly distributed in the space. In Sect. 5, Conjecture 2 on quantitative estimations of the construction is presented. Under this conjecture, new upper bounds (implicit and explicit) on $t(3, q)$ are obtained in Sect. 6. In Sect. 7, we give upper bounds based on computer search. In Sect. 8, a combined bound based on the bounds in the previous sections is presented. In Sect. 9, we summarize the results obtained.

## 2 The Main Results

The main results of the paper are given by Theorem 1 based on the results of Sects. 6–8, see Examples 1, 2, 3, Lemma 3, and Theorems 2, 4, 5, 6.

**Theorem 1** (***the main results***). *Let $t(3, q)$ be the smallest size of a complete arc in* PG$(3, q)$. *Let $\ell_q(4, 3)$ be the smallest length of a $q$-ary linear code of codimension (redundancy)* 4 *and covering radius* 3. *Let $\ell_q(4, 3, 5)$ be the smallest length of a $q$-ary linear code of codimension (redundancy)* 4, *covering radius* 3, *and minimum distance 5 (it is a quasi-perfect MDS code).*

**(i)** *The following upper "computer" bounds are provided by complete arcs obtained with the help of computer search:*

$$\ell_q(4,3) \le \ell_q(4,3,5) = t(3,q) < \begin{cases} 2.61\sqrt[3]{q \ln q} & \text{for } 13 \le q \le 4373 \\ 2.65\sqrt[3]{q \ln q} & \text{for } 4373 < q \le 7057 \end{cases}.$$

**(ii)** *The following upper "implicit" and "explicit" bounds hold under Conjecture 2:*

$$\ell_q(4,3) \le \ell_q(4,3,5) = t(3,q) < \begin{cases} 2.72\sqrt[3]{q \ln q} & \text{for } 7057 < q < 71143 \\ 2\sqrt[3]{3q \ln q} + 4 < 2.926\sqrt[3]{q \ln q} & \text{for } q \ge 71143 \end{cases}.$$

**(iii)** *The following upper "combined" bound holds under Conjecture 2; it is an union of the bounds* (i) *and* (ii)*:*

$$\ell_q(4,3) \le \ell_q(4,3,5) = t(3,q) < 2.93\sqrt[3]{q \ln q} \quad \text{for } q \ge 11 \text{ and } q = 4, 8.$$

Our observations and the results of [4,5] allow us to conjecture the following.

*Conjecture 1.* The upper bound

$$\ell_q(4,3) \le \ell_q(4,3,5) = t(3,q) < 2.93\sqrt[3]{q \ln q}$$

holds for all $q \ge 11$ without any extra conditions and conjectures.

*Remark 1.* In [11, Abstract, Ths. 6, 20], the final upper bound $3\sqrt[3]{\ln q}\cdot q^{(r-3)/3}$, $r=3t+1\ge 4$, is correct, but its multistep proof contains inaccuracies in the first stage connected with $\mathrm{PG}(3,q)$ and codimension (redundancy) $r=4$.

In particular, it can be checked that in Proof of [11, Th. 12] for $r=4$, the value $w=\left\lfloor 2\sqrt[3]{q+4}\sqrt[3]{\ln(q^3+q^2+q)}+1\right\rfloor$ satisfies inequality $q-1\ge(w-2)(w-3)$ [11, eq. (12)] if and only if $q\ge 71119$. Therefore, see [11, Cor. 13, eq. (4)], the bound $\ell_q(4,3)\le\ell_q(4,3,5)<2\sqrt[3]{3(q+4)\ln(q+1)}+4$ also holds only for $q\ge 71119$. However, in [11] this fact is not noted and the mentioned bound is used for $q>4973$, see [11, Fig. 1, Lem. 14].

In this paper, we prove the bound $\ell_q(4,3)\le\ell_q(4,3,5)=t(3,q)\le 2\sqrt[3]{3q\ln q}+4$ using inequality $q-13\ge(w-2)(w-3)$ with $w=2\sqrt[3]{3q\ln q}+2$, see (11), (19), (20). We show that this inequality holds if and only if $q\ge 71143$. To solve the problem we *introduce an implicit bound*, see Sect. 6.1. The implicit bound is given iteratively by (6)–(9); we calculated it by computer for each $q<71143$. As the result, we avoided the inaccuracies in the proofs of the upper bounds under Conjecture 2.

## 3 A Step-By-Step Process to Construct a Complete Arc

In $\mathrm{PG}(3,q)$, we construct a complete arc with the help of a greedy iterative step-by-step algorithm (*Algorithm* for short) which, in each step adds one new point to the arc. The added point provides the maximal possible (for the given step) number of new covered points.

If a point of $\mathrm{PG}(3,q)$ lies on a plane through three non-collinear points of an arc, we say that *the point is covered by the arc*. Clearly, all the points of the arc and the points of $\mathrm{PG}(3,q)$ lying on a bisecant line of the arc are covered.

The space $\mathrm{PG}(N,q)$ contains $\theta_{N,q}=\frac{q^{N+1}-1}{q-1}$ points.

Assume that after the $w$-th step of Algorithm, we obtain a $w$-arc that does not cover exactly $U_w$ points. We denote by $\mathbf{S}(U_w)$ the set of all $w$-arcs in $\mathrm{PG}(3,q)$ each of which does not cover exactly $U_w$ points. The group of collineations $P\Gamma L(4,q)$ preserves $\mathbf{S}(U_w)$.

*Remark 2.* To increase the volume of $\mathbf{S}(U_w)$ we could include in $\mathbf{S}(U_w)$ all $w$-arcs in $\mathrm{PG}(3,q)$ each of which does not cover $\le U_w$ points. This does not change estimates below, but some reflections could become more complicated.

The $(w+1)$-st step of Algorithm starts from a $w$-arc $\mathcal{K}_w\in\mathbf{S}(U_w)$ chosen from $\mathbf{S}(U_w)$ in a random manner. Every arc of $\mathbf{S}(U_w)$ can be chosen with the probability $\frac{1}{\#\mathbf{S}(U_w)}$. This means that we consider the set $\mathbf{S}(U_w)$ as an ensemble of random objects with the uniform probability distribution.

Let $\mathcal{U}(\mathcal{K})$ be the set of the points of $\mathrm{PG}(3,q)$ that are not covered by an arc $\mathcal{K}$. Evidently, $\#\mathcal{U}(\mathcal{K}_w)=U_w$. Let $\mathcal{K}_w$ consist of $w$ points $A_1,A_2,\dots,A_w$. Let $A_{w+1}\in\mathcal{U}(\mathcal{K}_w)$ be the point that is included into the arc in the $(w+1)$-st step.

*Remark 3.* In future, we introduce point subsets with the notation of the form $\mathcal{M}_w(A_{w+1})$. Any uncovered point may be added to $\mathcal{K}_w$. So, there exist $U_w$ distinct subsets $\mathcal{M}_w(A_{w+1})$. When a particular point $A_{w+1}$ is not relevant, we may use the notation $\mathcal{M}_w$. The same concerns the quantities $\Delta_w(A_{w+1})$ and $\Delta_w$.

We call a *bundle* $\mathcal{B}(A_{w+1})$ the set of $\binom{w}{2}$ planes through $A_{w+1}$ and two distinct points of $\mathcal{K}_w$. Let $\pi_{i,j}$, $1 \le i < j \le w$, be the plane through $A_i, A_j, A_{w+1}$. We denote by $\overline{A_iA_j}$ the line through $A_i, A_j$. We consider the set of the points

$$\mathcal{C}_w(A_{w+1}) = \mathcal{B}(A_{w+1}) \setminus \left( \{A_{w+1}\} \cup \bigcup_{1 \le i < j \le w} \overline{A_iA_j} \right) \tag{1}$$

where $\overline{A_iA_j}$ is a bisecant of $\mathcal{K}_w$. The points on the bisecants are covered by $\mathcal{K}_w$; also, $A_{w+1}$ is a new covered point. All the points in $\mathcal{C}_w(A_{w+1})$ are *candidates to be new covered points in the* $(w+1)$*-st step.* We denote

$$\Omega_w = \binom{w}{2}\left(\theta_{2,q} - 3q - \binom{w-2}{2}(q-2)\right) + \frac{1}{2}\binom{w}{2}\binom{w-2}{2}(q-2) \tag{2}$$
$$+ w(q-1) = \binom{w}{2}(q-1)^2 + w(q-1) - 3\binom{w}{4}(q-2).$$

**Lemma 1.** *For the set of candidates* $\mathcal{C}_w$ *we have* $\#\mathcal{C}_w \ge \Omega_w$.

*Proof.* In $\pi_{i,j}$, a part of points is common with other planes. In (2), we subtract from $\theta_{2,q}$ the volume of these parts. For fixed $i, j$, there are $\binom{w-2}{2}$ cases when $\{i,j\} \cap \{k,m\} = \emptyset$ and $\pi_{i,j}$ intersects $\pi_{k,m}$. An intersection line contains $A_{w+1}$ and it is skew to $\mathcal{K}_w$. Also, $\pi_{i,j} \cap \pi_{k,m}$ meets $\overline{A_iA_j}$ in a point $P \notin \{A_i, A_j\}$ and $\overline{A_kA_m}$ in $P' \notin \{A_k, A_m\}$. The points $P$ and $P'$ are covered by $\mathcal{K}_w$. Thus, we should subtract 3 from the cardinality $q+1$ of a line. As a result, we have the term $-\binom{w-2}{2}(q-2)$. In principle, for $\{i,j\} \cap \{k,m\} = \emptyset$ and $\{n,p\} \cap \{i,j,k,m\} = \emptyset$, intersection lines $\pi_{i,j} \cap \pi_{k,m}$ and $\pi_{i,j} \cap \pi_{n,p}$ can be the same. But for simplicity, in the estimate of $\#\mathcal{C}_w$, we put that all the intersection lines are distinct.

The term $-3q$ corresponds to the triangle with the vertices $A_i, A_j, A_{w+1}$.

On the other hand, at least one time, the subtracted values should be included in $\#\mathcal{C}_w$. Therefore, we add $\frac{1}{2}\binom{w}{2}\binom{w-2}{2}(q-2)$ where $\frac{1}{2}$ takes into account that every line $\pi_{i,j} \cap \pi_{k,m}$ is contained at least in two planes of $\mathcal{B}(A_{w+1})$. The addition $w(q-1)$ corresponds to $w$ sets $\overline{A_iA_{w+1}} \setminus \{A_i, A_{w+1}\}$, $i = 1, \ldots, w$. □

Let $\Delta_w(A_{w+1})$ be the number of new covered points in the $(w+1)$-st step;

$$\Delta_w(A_{w+1}) = \#\mathcal{U}(\mathcal{K}_w) - \#\mathcal{U}(\mathcal{K}_w \cup \{A_{w+1}\}) = \#\{\mathcal{C}_w(A_{w+1}) \cap \mathcal{U}(\mathcal{K}_w)\}. \tag{3}$$

We consider continuous approximations of the discrete functions $\#\mathcal{U}(\mathcal{K}_w)$, $\Delta_w(A_{w+1})$, $\#\mathcal{U}(\mathcal{K}_w \cup \{A_{w+1}\})$, and other ones keeping the same notations.

## 4 The Uniform Distribution of Uncovered Points

For a point $H \in \mathrm{PG}(3,q)$, let $n_w(H)$ be the number of arcs of $\mathbf{S}(U_w)$ that do not cover it. Each point $H$ is considered as a random object that is not covered by a randomly chosen $w$-arc $\mathcal{K}_w$ with the probability $p_w(H) = \frac{n_w(H)}{\#\mathbf{S}(U_w)}$.

**Lemma 2.** *The value $n_w(H)$ and the probability $p_w(H)$ are the same for all points $H \in \mathrm{PG}(3,q)$. They can be considered, respectively, as $n_w$ and*

$$p_w = \frac{n_w}{\#\mathbf{S}(U_w)}.$$

*Proof.* We denote $\mathbf{K}_w(H)$ the subset of $w$-arcs in $\mathbf{S}(U_w)$ that do not cover $H$. By the definition, $n_w(H) = \#\mathbf{K}_w(H)$. Let $H_i$ and $H_j$ be two points of $\mathrm{PG}(3,q)$. In $P\Gamma L(4,q)$, let $\Psi(H_i,H_j)$ be a collineation transforming $H_i$ to $H_j$. Evidently, $\Psi(H_i,H_j)$ embeds $\mathbf{K}_w(H_i)$ in $\mathbf{K}_w(H_j)$, while $\Psi(H_j,H_i)$ embeds $\mathbf{K}_w(H_j)$ in $\mathbf{K}_w(H_i)$. Thus, we have $\#\mathbf{K}_w(H_i) \le \#\mathbf{K}_w(H_j)$ and $\#\mathbf{K}_w(H_j) \le \#\mathbf{K}_w(H_i)$, whence $\#\mathbf{K}_w(H_i) = \#\mathbf{K}_w(H_j)$, i.e. $n_w(H_i) = n_w(H_j)$. □

We have proved that *uncovered points are uniformly distributed in the space* and the probability to be uncovered is independent of a point. Therefore, for a randomly chosen $w$-arc $\mathcal{K}_w \in \mathbf{S}(U_w)$, the fraction $\#\mathcal{U}_w(\mathcal{K}_w)/\theta_{3,q}$ of uncovered points of $\mathrm{PG}(3,q)$ is equal to the probability $p_w$ that a point of $\mathrm{PG}(3,q)$ is not covered. Thus,

$$p_w = \frac{\#\mathcal{U}_w(\mathcal{K}_w)}{\theta_{3,q}} = \frac{\mathcal{U}_w}{\theta_{3,q}}. \tag{4}$$

Note that by Lemma 2, the multiset consisting of all points that are not covered by all arcs of $\mathbf{S}(U_w)$ has cardinality $n_w\theta_{3,q}$. This cardinality can also be written as $U_w \cdot \#\mathbf{S}(U_w)$. Thus, $n_w\theta_{3,q} = U_w \cdot \#\mathbf{S}(U_w)$ and we have

$$\frac{n_w}{\#\mathbf{S}(U_w)} = \frac{U_w}{\theta_{3,q}}.$$

We obtained another explanation of the equality (4).

Consider a sequence of $h$ random and independent 0/1 trials each of which yields 1 with the probability $p_w$. The number $s_w(h)$ of ones in this sequens is the random variable with *binomial probability distribution* and the expected value

$$\mathbf{E}[s_w(h)] = hp_w = h\frac{U_w}{\theta_{3,q}}. \tag{5}$$

*Remark 4.* We can consider the *hypergeometric probability distribution*, which describes the probability of $s'_w(h)$ successes in $h$ random and independent draws without replacement from a finite population of size $\theta_{3,q}$ containing exactly $U_w$ successes. The expected value of $s'_w(h)$ again is

$$\mathbf{E}[s'_w(h)] = h\frac{U_w}{\theta_{3,q}} = \mathbf{E}[s_w(h)].$$

Note also that the average number of uncovered points among $h$ points of PG$(3,q)$ calculated over all $\binom{\theta_{3,q}}{h}$ combinations of $h$ points is

$$\frac{1}{\binom{\theta_{3,q}}{h}}\sum_{i=1}^{h} i\binom{\theta_{3,q}-U_w}{h-i}\binom{U_w}{i} = \frac{U_w}{\binom{\theta_{3,q}}{h}}\sum_{i=1}^{h}\binom{\theta_{3,q}-U_w}{h-i}\binom{U_w-1}{i-1}$$
$$= \frac{U_w\binom{\theta_{3,q}-1}{h-1}}{\binom{\theta_{3,q}}{h}} = h\frac{U_w}{\theta_{3,q}} = \mathbf{E}[s_w(h)].$$

We denote by $\mathbf{E}_{w,q}$ the expected value of the number of uncovered points among $\Omega_w$ randomly taken points in PG$(3,q)$, under the condition that the events to be uncovered are independent. By Lemma 2 and (2), (4), (5), we have

$$\mathbf{E}_{w,q} = \mathbf{E}[s_w(\Omega_w)] = \Omega_w p_w = \Omega_w\frac{U_w}{\theta_{3,q}}\,.$$

## 5 The Main Conjecture

The points-candidates of the set (1) cannot be considered as random and independent as they belong to the same bundle $\mathcal{B}(A_{w+1})$. Therefore, in general, $\mathbf{E}[\Delta_w] \neq \mathbf{E}_{w,q}$ where $\mathbf{E}[\Delta_w]$ is the expected value of $\Delta_w$ defined in (3).

However, there are *many random aspects of the process*. We note e.g. the relative positions and intersections of planes in distinct bundles and planes through three points of a current arc. Remind also that the starting arc $\mathcal{K}_w$ is taken from $\mathbf{S}(U_w)$ randomly. If $q$ and, hence, the number $U_w$ of distinct bundles and the volume of the ensemble $\mathbf{S}(U_w)$ are relatively large then the random aspects noted are especially essential. Therefore, with a large probability, the variance of the random variable $\Delta_w$ implies the existence of bundles providing $\Delta_w(A_{w+1}) > \mathbf{E}[\Delta_w]$ and, moreover, $\Delta_w(A_{w+1}) \geq \mathbf{E}_{w,q}$. By above, Conjecture 2 seems to be reasonable and founded.

*Conjecture 2* (**the main conjecture**)**.** For $q$ large enough, in every $(w+1)$-st step of the step-by-step process in PG$(3,q)$ considered in Sect. 3, there exists a $w$-arc $\mathcal{K}_w \in \mathbf{S}(U_w)$ such that one can find an uncovered point $A_{w+1}$ providing the inequality

$$\Delta_w(A_{w+1}) \geq \mathbf{E}_{w,q} = \Omega_w\frac{U_w}{\theta_{3,q}}\,.$$

*Remark 5.* We could do a "milder" conjecture of the form

$$\Delta_w(A_{w+1}) \geq \frac{\mathbf{E}_{w,q}}{D},\ D \geq 1 \text{ is a constant independent of } q,$$

cf. [9, Conjecture 3.3]. This inequality is more easy to achieve than the inequality of Conjecture 2. On the other hand, the new conjecture would give the extra multiplier $\sqrt[3]{D}$ in upper bounds (20). Also, the proofs become more complicated as $D$ is not limited from above.

## 6 Upper Bounds on $t(3,q)$ Under Conjecture 2

We always have at least one new covered point in the $(w+1)$-st step; it is $A_{w+1}$. Therefore, $\Delta_w(A_{w+1}) \ge 1$. Also, $\Delta_w(A_{w+1})$ should be integer. By Conjecture 2,

$$\Delta_w(A_{w+1}) \ge \left\lceil \max\left\{1, \Omega_w \frac{U_w}{\theta_{3,q}}\right\}\right\rceil$$

hence, by (3),

$$\begin{aligned} &\#\mathcal{U}_{w+1} = \#\mathcal{U}(\mathcal{K}_w \cup \{A_{w+1}\}) = \#\mathcal{U}(\mathcal{K}_w) - \Delta_w(A_{w+1}) \\ &\le U_w - \left\lceil \max\left\{1, \Omega_w \frac{U_w}{\theta_{3,q}}\right\}\right\rceil. \end{aligned} \tag{6}$$

In future, we put in $\mathcal{K}_3$ three non-collinear points. Therefore,

$$\#\mathcal{U}_3(\mathcal{K}_3) = \theta_{3,q} - \theta_{2,q} = q^3. \tag{7}$$

### 6.1 An Implicit Upper Bound $A(w_0, U_{w_0})$

Assume that there exists a $w_0$-arc $\mathcal{K}_{w_0} \subset \mathrm{PG}(3,q)$ that does not cover exactly $U_{w_0}$ points of $\mathrm{PG}(3,q)$. Starting from the values $w_0$ and $U_{w_0}$, one can iteratively apply relation (6) and obtain eventually $\#\mathcal{U}_{w+1} \le 1$ for some $w$, say $w^*$. Obviously, $w^*$ depends on $w_0$ and $U_{w_0}$, i.e. we have a function $w^*(w_0, U_{w_0})$. The obtained complete arc has size $k$, where

$$k = w^*(w_0, U_{w_0}) + 2 \text{ under condition } \#\mathcal{U}(\mathcal{K}_{w^*(w_0,U_{w_0})} \cup \{A_{w^*(w_0,U_{w_0})+1}\}) \le 1. \tag{8}$$

We call the value $w^*(w_0, U_{w_0}) + 2$ an *implicit upper bound* $A(w_0, U_{w_0})$. In other words, the following theorem holds.

**Theorem 2 (implicit bound).** *Let the values $w_0$, $U_{w_0}$, and $w^*(w_0, U_{w_0})$ be defined and calculated as above including (8). Then, under Conjecture 2, the following upper bound holds:*

$$t(3,q) \le w^*(w_0, U_{w_0}) + 2 := A(w_0, U_{w_0}). \tag{9}$$

In future, we use the implicit bound $A(3,q^3)$ based on (7)–(9).

*Example 1.* The implicit bound $A(3,q^3)$ divided by $\sqrt[3]{q \ln q}$ (i.e. the value $(w^*(3,q^3)+2)/\sqrt[3]{q \ln q}$) is shown by the top curve in Figs. 1 and 2, for $q \le 7057$, and by the middle curve in Fig. 3, for $7057 < q < 71143$.

The bound $A(3,q^3)$ is obtained by computer by iteratively applying (6). By these computations, in the range $7 \le q \le 61$, the bound $A(3,q^3)$ tends to increase with the minimal value $A(3,q^3) \sim 3.34\sqrt[3]{q \ln q}$ for $q = 7$ and the maximal value $A(3,q^3) \sim 7.46\sqrt[3]{q \ln q}$ for $q = 61$; in the range $61 \le q \le 7057$, $A(3,q^3)$ tends to decrease with the minimal value $A(3,q^3) \sim 2.68\sqrt[3]{q \ln q}$ for $q = 5471$, see Figs. 1 and 2. In the range $7057 < q < 71143$, the bound $A(3,q^3)$ tends to decrease with the maximal value $A(3,q^3) \sim 2.72\sqrt[3]{q \ln q}$ for $q = 7129$ and the minimal value $A(3,q^3) \sim 2.62\sqrt[3]{q \ln q}$ for $q = 59863$, see Fig. 3.

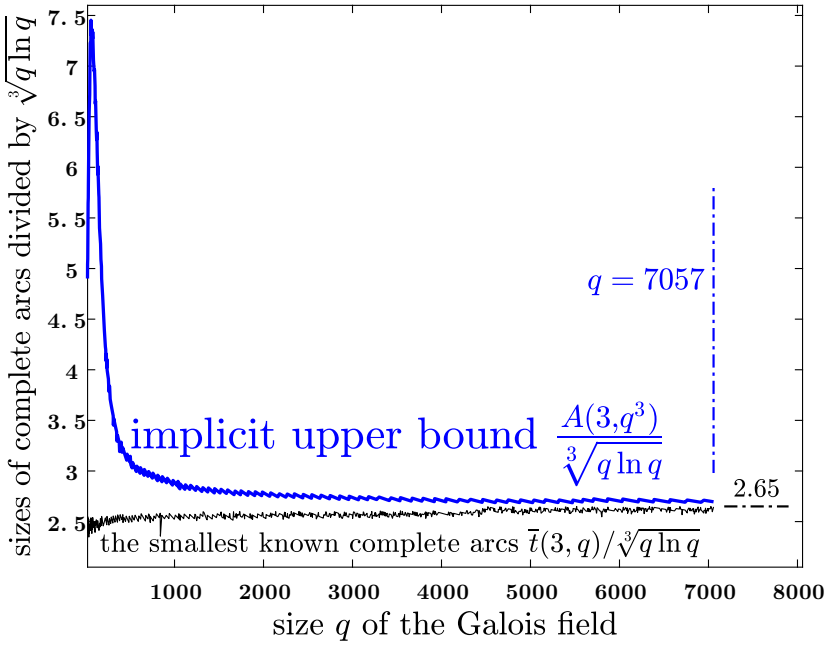


**Fig. 1.** Implicit upper bound $A(3, q^3)$ on the smallest size of a complete arc in PG$(3, q)$ (*top curve*) vs the smallest known sizes $\overline{t}(3, q)$ of complete arcs in PG$(3, q)$, $q \le 7057$ (*bottom curve*). The bound and the sizes are divided by $\sqrt[3]{q \ln q}$; $\frac{\overline{t}(3,q)}{\sqrt[3]{q \ln q}} < 2.65$

**Lemma 3.** **(i)** *In the range* $7 \le q \le 7057$*, we have* $A(3, q^3) > 2.68\sqrt[3]{q \ln q}$.

**(ii)** *In the range* $7057 < q < 71143$*, we have* $A(3, q^3) < 2.72\sqrt[3]{q \ln q}$.

*Proof.* The assertions are obtained by computer search using (6)–(9). □

### 6.2 An Explicit Upper Bound

By (2) and (6), we have

$$\#\mathcal{U}_{w+1} = \#\mathcal{U}(\mathcal{K}_w \cup \{A_{w+1}\}) = \#\mathcal{U}(\mathcal{K}_w) - \Delta_w(A_{w+1}) \le U_w\left(1 - \frac{\Omega_w}{\theta_{3,q}}\right) \quad (10)$$

$$= U_w\left(1 - \frac{4(w-1)(q-1)^2 + 8(q-1) - (w-1)(w-2)(w-3)(q-2)}{8\theta_{3,q}}w\right)$$

$$< U_w\left(1 - (4(w-1)(q-1) + 8 - (w-1)(w-2)(w-3))\frac{w(q-1)}{8\theta_{3,q}}\right)$$

$$< U_w\left(1 - (4(q-1) - (w-2)(w-3))\frac{w(w-1)(q-1)}{8\theta_{3,q}}\right).$$

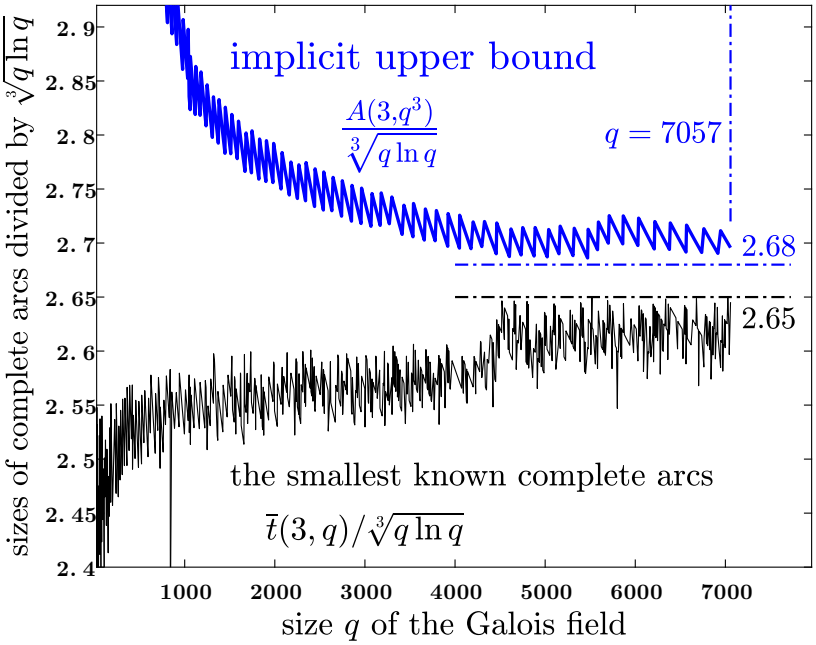


**Fig. 2.** Implicit upper bound $A(3, q^3)$ (*top curve*) vs the smallest known sizes $\bar{t}(3, q)$ of complete arcs (*bottom curve*) (in another scale than in Fig. 1). The bounds and the sizes are divided by $\sqrt[3]{q \ln q}$; $\frac{\bar{t}(3,q)}{\sqrt[3]{q \ln q}} < 2.65$, $\frac{A(3,q^3)}{\sqrt[3]{q \ln q}} > 2.68$

Assume that

$$q - 13 \geq (w-2)(w-3). \tag{11}$$

Under the condition (11) and by (10), we have

$$\begin{aligned} \#\mathcal{U}(\mathcal{K}_w \cup \{A_{w+1}\}) &< U_w \left(1 - \frac{3w(w-1)(q-1)(q+3)}{8(q^3+q^2+q+1)}\right) \\ &= U_w \left(1 - \frac{3w(w-1)}{8\left(q - \frac{q^2-4q-1}{q^2+2q-3}\right)}\right) < U_w \left(1 - \frac{3(w^2-w)}{8q}\right). \end{aligned} \tag{12}$$

Starting from (7) and using (12) iteratively, we obtain

$$\#\mathcal{U}_{w+1} \leq q^3 f_q(w) \tag{13}$$

where

$$f_q(w) = \prod_{i=3}^{w} \left(1 - \frac{3(i^2-i)}{8q}\right). \tag{14}$$

We are finishing the step-by-step process when $\#\mathcal{U}_{w+1} \leq 1$. The size $k$ of an obtained complete arc $\mathcal{K}_k$ is as follows:

$$k = w + 2 \text{ under condition } \#\mathcal{U}_{w+1} \leq 1. \tag{15}$$

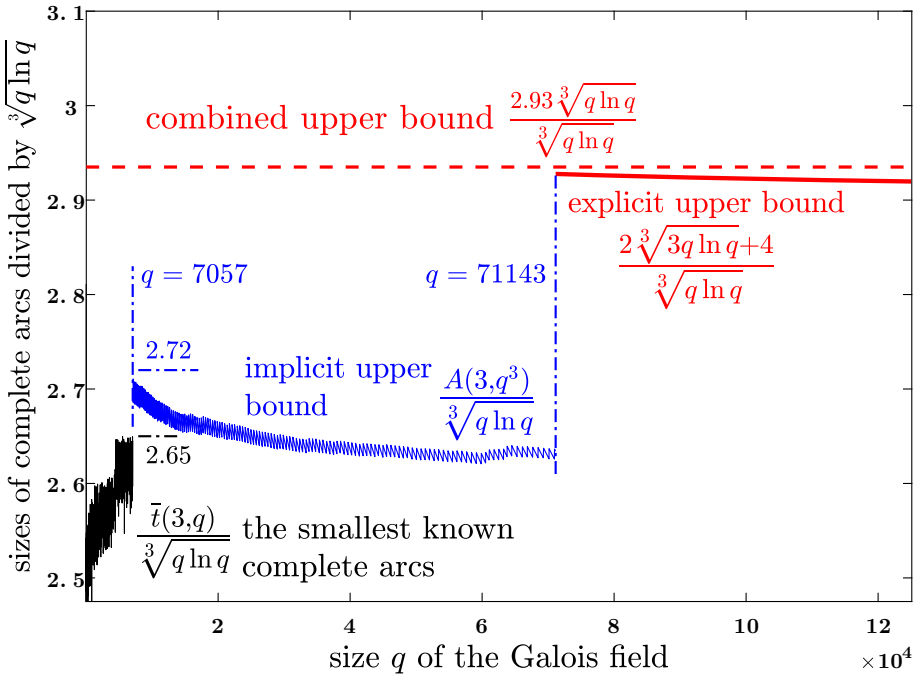


**Fig. 3.** Upper bounds on the smallest size of a complete arc in PG$(3, q)$ and the smallest known sizes of complete arcs in PG$(3, q)$, $q \le 125003$. Explicit upper bound $2\sqrt[3]{3q \ln q}+4$, $71143 \le q \le 125003$ (*the right-hand solid curve*); implicit upper bound $A(3, q^3)$, $7057 < q < 71143$ (*the middle curve*); combined upper bound $2.93\sqrt[3]{q \ln q}$ (*the top dashed line* $y = 2.93$); the smallest known sizes $\bar{t}(3, q)$ of complete arcs in PG$(3, q)$, $q \le 7057$ (*the left-hand curve*). The bounds and the sizes are divided by $\sqrt[3]{q \ln q}$; $\frac{\bar{t}(3,q)}{\sqrt[3]{q \ln q}} < 2.65$, $\frac{A(3,q^3)}{\sqrt[3]{q \ln q}} < 2.72$, $\frac{2\sqrt[3]{3q \ln q}+4}{\sqrt[3]{q \ln q}} < 2.93$, $\frac{2.93\sqrt[3]{q \ln q}}{\sqrt[3]{q \ln q}} = 2.93$

**Theorem 3 (the basic inequality).** *Let* $f_q(w)$ *be as in* (14). *Under Conjecture 2, in* $PG(3, q)$ *the following holds:*

$$t(3, q) \le w + 2 \tag{16}$$

*where the value* $w$ *satisfies the "basic" inequality*

$$f_q(w) \le q^{-3}. \tag{17}$$

*Proof.* By (13), to provide the inequality $\#\mathcal{U}_{w+1} \le 1$ it is sufficient to find $w$ such that $q^3 f_q(w) \le 1$. Now (16) follows from (15). □

We find an upper bound on the smallest possible solution of inequality (17). By the Taylor series of $e^{-\alpha}$, we have

$$1 - \alpha < e^{-\alpha} \text{ for } \alpha \ne 0. \tag{18}$$

**Lemma 4.** *The value*

$$w \geq 2\sqrt[3]{3q\ln q} + 2 \tag{19}$$

*satisfies the basic inequality* (17).

*Proof.* By (14),(18), we have

$$f_q(w) = \prod_{i=3}^{w}\left(1 - \frac{3(i^2-i)}{8q}\right) < e^{-\Upsilon(w)}$$

where

$$\Upsilon(w) = \sum_{i=3}^{w}\frac{3(i^2-i)}{8q} = \frac{3}{8q}\left(-2 + \sum_{i=1}^{w}(i^2-i)\right)$$
$$= \frac{3}{8q}\left(-2 + \frac{w(w+1)(2w+1)}{6} - \frac{w(w+1)}{2}\right) = \frac{w(w^2-1)-6}{8q} > \frac{(w-1)^3}{8q}$$

whence $f_q(w) =< e^{-(w-1)^3/8q}$. Thus, to provide (17) it is sufficient to find $w$ such that $e^{-(w-1)^3/8q} \leq q^{-3}$ whence $(w-1)^3 \geq 8q\ln q^3$ and $w \geq \sqrt[3]{3q\ln q} + 1$. As $w$ should be an integer, in (19) one is added. □

**Lemma 5.** *The value* $w = 2\sqrt[3]{3q\ln q} + 2$ *of* (19) *satisfies the condition* (11) *if and only if* $q \geq 71143$.

*Proof.* The assertion can be checked directly by computer. □

**Theorem 4** ***(explicit bound).*** *Under Conjecture 2, in* $PG(3,q)$ *we have*

$$t(3,q) \leq 2\sqrt[3]{3q\ln q} + 4 < 2.926\sqrt[3]{q\ln q}, \quad q \geq 71143. \tag{20}$$

*Proof.* The assertion follows from (16), (19) and Lemma 5. Note also that $2\sqrt[3]{3q\ln q} + 4 = \sqrt[3]{q\ln q}\left(2\sqrt[3]{3} + \frac{4}{\sqrt[3]{q\ln q}}\right)$. □

*Example 2.* For $71143 \leq q \leq 125003$, the explicit bound (20) divided by $\sqrt[3]{q\ln q}$ (i.e. the value $\frac{2\sqrt[3]{3q\ln q}+4}{\sqrt[3]{q\ln q}}$) is shown by the right-hand solid curve in Fig. 3.

## 7 The Smallest Known Complete Arcs in $PG(3,q)$

Let $\bar{t}(3,q)$ be the *smallest* ***known*** *size of a complete arc in* $\mathrm{PG}(3,q)$.

Obviously, $t(3,q) \leq \bar{t}(3,q)$. The smallest known complete arcs in $PG(3,q)$ are obtained in [4,5] and in this paper by computer search with the help of two types of algorithms. They both build an arc iteratively, step-by-step. Algorithms of these types are considered in [2,3,5], see also the references therein.

***Algorithms with Fixed Order of Points*** **(FOP)**
We fix an order on points of $\mathrm{PG}(3,q)$ as $A_1, A_2, \ldots, A_{\theta_{3,q}}$ where $A_1, A_2, A_3$ are non-collinear. The set $S^{(1)} = \{A_1, A_2, A_3\}$ is the start of the search. On the $j$-th

step we obtain the set $S^{(j)}$. To obtain $S^{(j+1)}$, we add to $S^{(j)}$ the first point in the fixed order, which is not covered by $S^{(j)}$.

A point $A_i \in \mathrm{PG}(3,q)$ in homogeneous coordinates is written as $A_i = (x_0^{(i)}, x_1^{(i)}, x_2^{(i)}, x_3^{(i)})$, $x_u^{(i)} \in \mathbb{F}_q$. The number $i$ of $A_i$ is assigned by two ways. In the *lexicographical* order we put $i = \sum_{u=0}^{3} x_u^{(i)} q^{3-u}$. In the *inverse lexicographical* order we have $i = \theta_{3,q} - \sum_{u=0}^{3} x_u^{(i)} q^{3-u}$.

Let $q$ *be prime.* Then *for an algorithm with fixed order of points, the size of a complete arc and the point list of the arc depend on* $q$ *only.*

We use "FOP algorithm" with the lexicographical order of points and "2FOP algorithm" where both the lexicographical and the inverse lexicographical orders of points are applied and the best result is taken.

One can consider the algorithm with fixed order of points as a version of the recursive $g$-parity check matrix algorithm for greedy codes [24, Sect. 7].

***Randomized Greedy Algorithms***

We use the so-called *d-Rand-Greedy algorithm.* In every step, the $d$-Rand-Greedy algorithm considers a few randomly chosen points that are not covered in the previous steps. The chosen point providing the most number of new covered points is included to the current arc. This gives smaller complete arcs than algorithms FOP, but takes greater computer time.

The smallest known complete arcs in $PG(3,q)$, $q \le 7057$, are obtained by computer search in [4,5] and in this paper. These arcs provide the following.

**Theorem 5.** ***(computer bound).*** *In* $\mathrm{PG}(3,q)$*, the following upper bounds hold:*

$$t(3,q) \le \overline{t}(3,q) \le \begin{cases} 2.61\sqrt[3]{q \ln q} & \text{for } 13 \le q \le 4373 \\ 2.65\sqrt[3]{q \ln q} & \text{for } 4373 < q \le 7057 \end{cases}.$$

*Proof.* The needed complete arcs are obtained by computer search. To construct arcs, for $q \le 4451$ the $d$-Rand-Greedy algorithm is used. For $4451 < q \le 7057$, the FOP and 2FOP algorithms are applied, in preference, but for $q = 4489, 4679, 4877, 4889, 4913, 5801, 6653$, we used the $d$-Rand-Greedy algorithm. For $q = 841$, the complete 42-arc of [25] is taken. □

*Example 3.* The sizes $\overline{t}(3,q)$ of the smallest known complete arcs in $PG(3,q)$, $q \le 7057$, divided by $\sqrt[3]{q \ln q}$, are shown by the bottom curves in Figs. 1, 2, 3 and 4.

## 8 A Combined Upper Bound

We join the upper bounds of the previous sections.

**Theorem 6** (***combined bound***)**.** *Under Conjecture 2, in* $\mathrm{PG}(3,q)$*, the following upper bound holds:*

$$\ell_q(4,3) \le \ell_q(4,3,5) = t(3,q) < 2.93\sqrt[3]{q \ln q} \quad \text{for } q \ge 11 \text{ and } q = 4, 8. \tag{21}$$

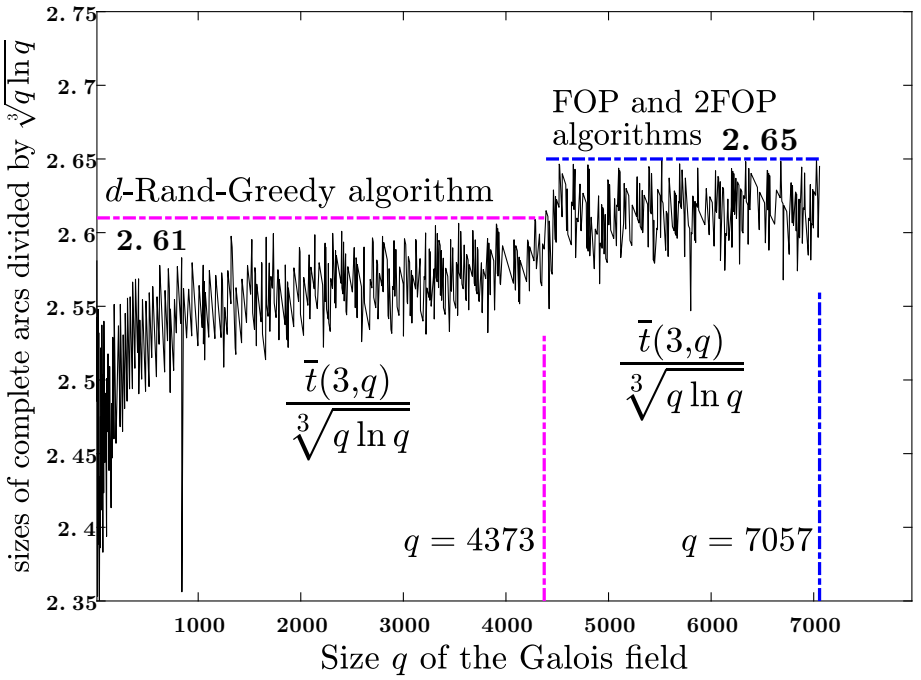


**Fig. 4.** The smallest **known** sizes $\overline{t}(3, q)$ of complete arcs in PG$(3, q)$ divided by $\sqrt[3]{q \ln q}$

*Proof.* We use the results of Examples 1, 2, 3, Lemma 3, and Theorems 2, 4, 5; see also Figures 1–4. In particular, Fig. 3 illustrates that the combined bound (21) is provided by the smallest known complete arcs for $13 \le q \le 7057$, by the implicit bound for $7057 < q < 71143$, and by the explicit bound for $q \ge 71143$. Finally, for $q = 4, 8, 11$ we take convenient arcs from [5,13]. □

## 9 Conclusion

We consider the upper bounds on the smallest size $t(3, q)$ of a complete arc in the projective space PG$(3, q)$. This size is equal to the smallest length of an $[n, n-4, 5]_q 3$ quasi-perfect MDS code. We analyse the working mechanism of a step-by-step greedy algorithm constructing a complete arc. It is proved that uncovered points are uniformly distributed in the space. A natural conjecture on an estimate of the number of new covered points in every step of the algorithm is presented. Under this conjecture, new upper bounds on t(3,q) are obtained. The initial part of the bounds is based on computer search, see Theorem 1.

## References


1. Bartoli, D., Davydov, A.A., Faina, G., Kreshchuk, A.A., Marcugini, S., Pambianco, F.: Upper bounds on the smallest sizes of a complete arc in PG(2, q) under certain probabilistic conjectures. Probl. Inf. Transm. **50**(4), 320–339 (2014). https://doi.org/10.1134/S0032946014040036
2. Bartoli, D., Davydov, A.A., Faina, G., Kreshchuk, A.A., Marcugini, S., Pambianco, F.: Upper bounds on the smallest size of a complete arc in a finite Desarguesian projective plane based on computer search. J. Geom. **107**(1), 89–117 (2016). https://doi.org/10.1007/s00022-015-0277-z
3. Bartoli, D., Davydov, A.A., Faina, G., Kreshchuk, A.A., Marcugini, S., Pambianco, F.: Tables, bounds and graphics of sizes of complete arcs in the plane PG(2, q) for all $q \leq 321007$ and sporadic $q$ in [323761 . . . 430007] obtained by an algorithm with fixed order of points (FOP). arXiv:1404.0469 [math.CO] (2018)
4. Bartoli, D., Davydov, A.A., Giulietti, M., Marcugini, S., Pambianco, F.: New bounds for linear codes of covering radii 2 and 3. Crypt. Commun. **11**(5), 903–920 (2018). https://doi.org/10.1007/s12095-018-0335-0
5. Bartoli, D., Davydov, A.A., Marcugini, S., Pambianco, F.: Tables, bounds and graphics of short linear codes with covering radius 3 and codimension 4 and 5. arXiv:1712.07078 [cs IT] (2020)
6. Bartoli, D., Giulietti, M., Platoni, I.: On the covering radius of MDS codes. IEEE Trans. Inf. Theory **61**(2), 801–811 (2015). https://doi.org/10.1109/TIT.2014.2385084
7. Brualdi, R.A., Litsyn, S., Pless, V.: Covering radius. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, vol. 1, pp. 755–826. Elsevier, Amsterdam (1998)
8. Cohen, G., Honkala, I., Litsyn, S., Lobstein, A.: Covering Codes, North-Holland Mathematical Library, vol. 54. Elsevier, Amsterdam (1997)
9. Davydov, A.A., Faina, G., Marcugini, S., Pambianco, F.: Upper bounds on the smallest size of a complete cap in PG(N, q), $N \geq 3$, under a certain probabilistic conjecture. Australas. J. Combin. **72**(3), 516–535 (2018)
10. Davydov, A.A., Giulietti, M., Marcugini, S., Pambianco, F.: Linear nonbinary covering codes and saturating sets in projective spaces. Adv. Math. Commun. **5**(1), 119–147 (2011). https://doi.org/10.3934/amc.2011.5.119
11. Davydov, A.A., Marcugini, S., Pambianco, F.: New bounds for linear codes of covering radius 3 and 2-saturating sets in projective spaces. In: Proceedings of the 2019 XVI International Symposium Problems of Redundancy in Information and Control Systems (REDUNDANCY), pp. 47–52. IEEE Xplore, Moscow, Russia, October 2019 (2020). https://doi.org/10.1109/REDUNDANCY48165.2019.9003348
12. Davydov, A.A., Östergård, P.R.J.: Linear codes with covering radius $R = 2, 3$ and codimension $tR$. IEEE Trans. Inform. Theory **47**(1), 416–421 (2001). https://doi.org/10.1109/18.904551
13. Davydov, A.A., Östergård, P.R.J.: Linear codes with covering radius 3. Des. Codes Crypt. **54**(3), 253–271 (2010). https://doi.org/10.1007/s10623-009-9322-y
14. Etzion, T., Storme, L.: Galois geometries and coding theory. Des. Codes Crypt. **78**(1), 311–350 (2015). https://doi.org/10.1007/s10623-015-0156-5
15. Gabidulin, E.M., Kløve, T.: The Newton radius of MDS codes. In: Proceedings of the IEEE Information Theory Workshop (ITW 1998), pp. 50–51. IEEE Xplore, Killarney, Ireland, June 1998 (2002). https://doi.org/10.1109/ITW.1998.706367

16. Giulietti, M.: The geometry of covering codes: small complete caps and saturating sets in Galois spaces. In: Blackburn, S.R., Holloway, R., Wildon, M. (eds.) Surveys in Combinatorics 2013, London Math. Society Lecture Note Series, vol. 409, pp. 51–90. Cambridge University Press, Cambridge (2013). https://doi.org/10.1017/CBO9781139506748.003
17. Hirschfeld, J.W.P.: Finite Projective Spaces of Three Dimensions. Oxford University Press, Oxford (1985)
18. Hirschfeld, J.W.P.: Projective Geometries Over Finite Fields. Oxford Mathematical Monographs, 2nd edn. Clarendon Press, Oxford (1998)
19. Hirschfeld, J.W.P., Storme, L.: The packing problem in statistics, coding theory and finite projective spaces: update 2001. In: Blokhuis, A., Hirschfeld, J.W.P., Jungnickel, D., Thas, J.A. (eds.) Finite Geometries, Developments of Mathematics, Proceedings of the Fourth Isle of Thorns Conference, Chelwood Gate, vol. 3, pp. 201–246. Kluwer Academic, Boston (2001). https://doi.org/10.1007/978-1-4613-0283-4_13
20. Hirschfeld, J.W.P., Thas, J.A.: Open problems in finite projective spaces. Finite Fields Appl. **32**, 44–81 (2015). https://doi.org/10.1016/j.ffa.2014.10.006
21. Klein, A., Storme, L.: Applications of finite geometry in coding theory and cryptography. In: Crnković, D., Tonchev, V. (eds.) Security, Coding Theory and Related Combinatorics, NATO Science for Peace and Security, Series - D: Information and Communication Security, vol. 29, pp. 38–58. IOS Press (2011). https://doi.org/10.3233/978-1-60750-663-8-38
22. Landjev, I., Storme, L.: Galois geometry and coding theory. In: De. Beule, J., Storme, L. (eds.) Current Research Topics in Galois geometry, chap. 8, pp. 187–214. NOVA Academic, New York (2011)
23. Lobstein, A.: Covering radius, an online bibliography (2019). https://www.lri.fr/~lobstein/bib-a-jour.pdf. Accessed 18 Jun 2020
24. Pless, V.S.: Coding constructions. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory, vol. 1, pp. 141–176. Elsevier, Amsterdam (1998)
25. Sonnino, A.: Transitive PSL$(2, 7)$-invariant 42-arcs in 3-dimensional projective spaces. Des. Codes Crypt. **72**(2), 455–463 (2014). https://doi.org/10.1007/s10623-012-9778-z
26. Storme, L.: Small arcs in projective spaces. J. Geom. **58**(1–2), 179–191 (1997). https://doi.org/10.1007/BF01222939