*Fifteenth International Workshop on Algebraic and Combinatorial Coding Theory*
*June 18-24, 2016, Albena, Bulgaria* *pp. 129-132*

# A new $(37, 3)$-arc in PG(2,23)[1]

Rumen Daskalov daskalov@tugab.bg
Mladen Manev ml.manev@gmail.com
Department of Mathematics, Technical University of Gabrovo, 5300 Gabrovo, BULGARIA

**Abstract.** An $(n, r)$-arc is a set of $n$ points of a projective plane such that some $r$, but no $r+1$ of them, are collinear. The maximum size of an $(n, r)$-arc in PG(2,q) is denoted by $m_r(2, q)$. It follows from [9] and [6] that $m_3(2, 23) \geq 36$. In this paper we establish that $m_3(2, 23) \geq 37$.

## 1 Introduction

Let GF$(q)$ denote the Galois field of $q$ elements and V$(3, q)$ be the vector space of row vectors of length three with entries in GF$(q)$. Let PG$(2, q)$ be the corresponding projective plane. The *points* $(x_1, x_2, x_3)$ of PG$(2, q)$ are the 1-dimensional subspaces of V$(3, q)$. Subspaces of dimension two are called *lines*. The number of points and the number of lines in PG$(2, q)$ is $q^2 + q + 1$. There are $q + 1$ points on every line and $q + 1$ lines through every point.

**Definition 1.** *An $(n, r)$-arc is a set of $n$ points of a projective plane such that some $r$, but no $r + 1$ of them, are collinear.*

**Definition 2.** *An $(l, t)$-blocking set $S$ in PG$(2, q)$ is a set of $l$ points such that every line of PG$(2, q)$ intersects $S$ in at least $t$ points, and there is a line intersecting $S$ in exactly $t$ points.*

An $(n, r)$-arc is the complement of a $(q^2 + q + 1 - n, q + 1 - r)$-blocking set in a projective plane and conversely.

**Definition 3.** *Let $M$ be a set of points in any plane. An $i$-secant is a line meeting $M$ in exactly $i$ points. Define $\tau_i$ as the number of $i$-secants to a set $M$.*

In terms of $\tau_i$ the definitions of an $(n, r)$-arc and an $(l, t)$-blocking set become the following: An $(n, r)$-arc is a set of $n$ points of a projective plane for which $\tau_i \geq 0$ for $i < r$, $\tau_r > 0$ and $\tau_i = 0$ when $i > r$. An $(l, t)$-blocking set is a set of $l$ points of a projective plane for which $\tau_i = 0$ for $i < t$, $\tau_t > 0$ and $\tau_i \geq 0$ when $i > t$.

[1] This work was partially supported by the Ministry of Education and Science under contract in TU-Gabrovo.

A survey of $(n, r)$-arcs with the best known results was presented in [8]. After this publication many improvements were obtained in [4], [5] and [3]. Summarizing these improvements, Ball and Hirschfeld [2] presented a new table with bounds on $m_r(2, q)$ for $q \leq 19$. It follows from these tables that the exact values of $m_r(2, q)$ are known only for $q \leq 9$. A survey of the new improvements in recent years can be found in the online table for $m_r(2, q),\ q \leq 19$, maintained by S. Ball [1]. New results and tables with lower and upper bounds on $m_r(2, q)$ for $q = 23$, and $q = 25, 27$ are presented in [6] and [7] respectively.

## 2 Quasi-Cyclic Codes

Let GF(q) denote the Galois field of $q$ elements and let V(n,q) denote the vector space of all ordered $n$-tuples over GF(q). The Hamming weight of a vector $x$, denoted by $wt(x)$, is the number of nonzero entries in $x$. A linear code $C$ of length $n$ and dimension $k$ over GF(q) is a $k$-dimensional subspace of V(n,q). Such a code is called $[n, k, d]_q$ code if its minimum Hamming distance is $d$. For linear codes, the minimum distance is equal to the smallest of the weights of the nonzero codewords. A $k \times n$ matrix $G$ having as rows the vectors of a basis of a linear code $C$ is called a generator matrix for $C$.

A code $C$ is said to be $p$-QC if a cyclic shift of any codeword by $p$ positions results in another codeword. Suppose that $C$ is a $p$-QC $[pm, k]$ code $(m \geq k)$. It is convenient to take the co-ordinate places of $C$ in the following order

$$\begin{array}{l} 1, p+1, 2p+1, \ldots, (m-1)p+1, \\ 2, p+2, \ldots, (m-1)p+2, \\ p, 2p, \ldots, mp. \end{array}$$

Then $C$ will be generated by a matrix of the form

$$[B_1, B_2, \ldots, B_p]$$

where each $B_i$ is a circulant matrix, i.e. a matrix of the form

$$B = \begin{bmatrix} b_0 & b_1 & b_2 & \cdots & b_{m-1} \\ b_{m-1} & b_0 & b_1 & \cdots & b_{m-2} \\ b_{m-2} & b_{m-1} & b_0 & \cdots & b_{m-3} \\ \vdots & \vdots & \vdots & & \vdots \\ b_1 & b_2 & b_3 & \cdots & b_0 \end{bmatrix}$$

If the row vector $(b_0 b_1 \cdots b_{m-1})$ is identified with the polynomial $d(x) = b_0 + b_1 x + ... + b_{m-1} x^{m-1}$, then we may write

$$B = \begin{bmatrix} d(x) \\ xd(x) \\ x^2d(x) \\ \vdots \\ x^{m-1}d(x) \end{bmatrix}$$

where each polynomial is reduced modulo $x^m - 1$.

The polynomials

$$d_1(x), \quad d_2(x), \quad \ldots \quad , d_p(x),$$

associated in this way with a $QC$ code, are called *defining polynomials* of $C$. Taking the polynomials $ax^l d_i(x)$ instead of $d_i(x)$ we make a cyclic shift of the columns of $B_i$ and multiply them by a nonzero element of the field. This leads to a generator matrix of an equivalent code. So, the defining polynomials of a $QC$-code can be chosen from a fixed set of representatives of the equivalence classes of polynomials of degree less than $m$ under the following relation:

$$c_i(x) \approx c_j(x) \iff c_i(x) \equiv ax^l c_j(x) \mod (x^m - 1)$$

## 3 The new arc

The new arc is constructed in the following way:

1. We generated all 185 inequivalent defining polynomials for 3-dimensional QC codes over GF(23) (see [10], [11]).
2. Using these polynomials and a method, presented in [11], we constructed more than 2500 $[36, 3, 33]_{23}$ QC codes.
3. For each of these codes the respective $(36, 3)$-arc in PG(2,23) was generated.
4. Afterwards we tried to enlarge each of those arcs.
5. Some of them were successfully enlarged to new $(37, 3)$-arcs in PG(2,23).

**Theorem 1.** *There exist a* $(37, 3)$*-arc in* PG(2,23)*.*

*Proof.*

The set of points (0,1,4), (0,1,15), (0,1,17), (1,0,6), (1,0,19), (1,0,20), (1,1,1), (1,1,2), (1,1,4), (1,2,1), (1,3,22), (1,4,0), (1,4,1), (1,4,11), (1,6,6), (1,8,11), (1,8,22), (1,10,3), (1,12,9), (1,12,12), (1,12,19), (1,14,22), (1,15,0), (1,15,2), (1,15,8), (1,17,0), (1,17,20), (1,18,2), (1,18,5), (1,18,9), (1,20,3), (1,20,6), (1,21,7), (1,21,15), (1,22,9), (1,22,15), (1,22,20) forms a (37,3)-arc in PG(2,23) with secant distribution

$$\tau_0 = 151, \tau_1 = 96, \tau_2 = 126, \tau_3 = 180.$$

□

## References

[1] S. Ball, Three-dimensional linear codes, Online table, `http://www-ma4.upc.edu/~simeon/`.

[2] S. Ball, J. W. P. Hirschfeld, Bounds on $(n, r)$-arcs and their applications to linear codes, *Finite Fields and Their Applications*, **11**, 326–336, 2005.

[3] M. Braun, A. Kohnert, A. Wassermann, Construction of $(n, r)$-arcs in PG(2, q), *Innov. Incid. Geometry*, **1**, 133–141, 2005.

[4] R. Daskalov, On the existence and the nonexistence of some $(k, r)$-arcs in PG(2, 17), *in Proc. of Ninth International Workshop on Algebraic and Combinatorial Coding Theory*, 19-25 June, 2004, Kranevo, Bulgaria, 95–100.

[5] R. Daskalov, E. Metodieva, New $(k, r)$-arcs in $PG(2, 17)$ and the related optimal linear codes, *Mathematica Balkanica*, New series, **18**, 121–127, 2004.

[6] R. Daskalov, E. Metodieva, New (n,r)-arcs in PG(2, 17), PG(2, 19), and PG(2, 23), *Problemi Peredachi Informatsii*, **47**, no. 3, (2011), 3–9. English translation: *Problems of Information Transmission*, **47**, no. 3, 217–223, 2011.

[7] R.Daskalov, E.Metodieva, Improved bounds on $m_r(2, q)$ $q$ = 19,25, 27, Hindawi Publishing Corporation, *Journal of Discrete Mathematics*, Volume 2013, Article ID 628952, 7 pages, http://dx.doi.org/10.1155/2013/628952.

[8] J. W. P. Hirschfeld, L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001, *Finite Geometries*, Developments in Mathematics, Kluwer, Boston, 201–246, 2001.

[9] A. Kohnert, Arcs in the projective planes, Online tables, `www.algorithm.uni-bayreuth.de/en/research/Coding_Theory/PG_arc_table/index.html`.

[10] E. Metodieva, N. Daskalova, "Generating Generalized Necklaces and New Quasi-Cyclic Codes", (preprint).

[11] V. Venkaiah, T.A.Gulliver, "Quasi-cyclic codes over $F_{13}$ and enumerating of defininings polynomials", *Journal Discrete Algorithms*, vol. 16, (2012), 249–257.