International Journal of Mathematics and
Computer Science, **16**(2021), no. 4, 1575–1581

The Non-existence of $[1864, 3, 1828]_{53}$ Linear Code by Combinatorial Technique

Nada Yassen Kasm Yahya[1], **Emad Bakr Al-Zangana**[2]

[1]Department of Mathematics
College of Education for Pure Science
University of Mosul
Mosul, Iraq

[2]Department of Mathematics
College of Science
Mustansiriyah University,
Baghdad, Iraq

email: drnadaqasim3@uomosul.edu.iq,
e.b.abdulkareem@uomustansiriyah.edu.iq

(Received April 15, 2021, Accepted May 17, 2021)

Abstract

An arc and a blocking set are both geometrical objects linked with linear codes. In this paper, we use relations among these objects to prove the non-existence of linear codes over F_{53} of lengths $s = (t-1)p + t - (p+1)/2, (p+3)/2 < t < p$ and minimum Hamming distance $d = s - t$ with dimension three. As a special case, no linear code of length 1864 exists. In addition, we determine the upper bounds of $m_t(2, 53)$.

1 Introduction

For a prime number p and a positive integer h, let $GF(q) = F_q, q = p^h$ be the Galois field of order q and let $V(n+1, q) = F_q^{n+1}$ denote the vector space of

Key words and phrases: Arc, Bocking set, Linear code, Projective geometry.
AMS (MOS) Subject Classifications: 14N05, 51N15, 51N35.
ISSN 1814-0432, 2021, http://ijmcs.future-in-tech.net

dimension $n+1$ over F_q. A Hamming distance between two distinct vectors x, y in F_q^n is the number of positions in which x and y differ. A linear code $\mathcal{L}$ with parameters $[n, k, d]$ over F_q, denoted by $[n, k, d]_q$, is a subspace of F_q^n of length n, dimension k and minimum distance $d(\mathcal{L})$ which is equal to the minimum Hamming distance among its non-zero codewords. Researchers working in linear coding attempted to make one of the parameters n, k, d ideal. In other words, they tried to decide whether a given linear code is good, the information rate $k^* = k/n$ and the relative distance $d^* = d/n$, should be large enough; that is, the length is small enough with respect to dimension and distance. A code that achieves one of k^* and d^* values is called optimal. More basic properties of linear codes can be found in [1].

Let $PG(2, q)$ be the finite projective plane over F_q. The following geometrical objects are needed [2].

Definition 1.1. *An $(s;t)$-arc A is a subset of $PG(2, q)$ with cardinality s such that no line meets A in $t+1$ points but there are some lines that meet A in t points. If no $(s+1;t)$-arc contains A, then it is called complete. The largest cardinal of an arc of degree t is denoted by $m_t(n, q)$. A line with respect to an arc in a plane is called i-secant if it intersects the arc in i points. The overall number of i-secants is denoted by T_i.*

Definition 1.2. *An $\imath$-fold blocking k-set B in a projective plane is a set of k points such that each line contains at least $\imath$ points of B and some line contains exactly $\imath$ points of B. Such a block set will be denoted by $\{\imath, k\}$-blocking set.*

Clearly, an $(s;t)$-arc, S in a projective plane over F_q gives an $\imath$-fold blocking k-set, H in the same plane with $t+i = q+1$ and $s+k = q^2+q+1$ such that $S = \mathcal{H}^c$ (complement of $\mathcal{H}$). Generally, the link between an $(s;t)$-arc, S in $PG(k-1, q)$ and linear code $\mathcal{L}$ of length s over F_q is given as follows:

Theorem 1.3. *[3] An $(s;t)$-arc, S in $PG(k-1, q)$ exist if and only if a linear code $\mathcal{L}$, $[n, k, n-t]_q$ exist with condition that any pair of columns of generator matrix is projectively distinct.*

In this paper, the three terms arc, blocking set and linear code are linked together.

For an arbitrary values n, k and d, it is not necessarily an $[n, k, d]_q$ code exists. The research aims to prove that there are no linear codes of dimension three and lengths take values in the interval $[1486, 2728]$ over F_{53}. As an example, no linear code exists with parameters $[1864, 3, 1828]$ over F_{53}. Also, we find a new upper bound to $m_t(2, 53)$, $29 \le t \le 52$. Our technique is combinatorial and relies on the theorems given in Section 2.

Several researchers have studied the non-existence of some $(s; t)$-arcs in the plane and many others have shown interest in finding new linear codes through arcs in the projective space. In [4], for $q = 19, 23, 43$, Alabdullah proved the non-existence for some $(s; t)$-arcs and new upper bounds (lower bounds) of complete $(s; t)$-arcs for certain finite fields were presented. In [5], the non-existence of an additive quatemary code with parameters $[15, 5, 9]$ was proved. In [6], Cheon proved the non-existence of a special code, called Griesmer code, with special parameters. In addition, Ball [7] studied the lower bounds by using blocking sets in the plane. In [8] and [9], the authors used a reverse technique to construct complete $(s; t)$-arcs in $PG(2, q)$, which gave new linear codes. In [10, 11], Al-Zangana used the action property of groups on the points of the plane to construct new arcs and then gave new codes over finite fields of specific orders. There were many other studies that show the existence and non-existence of coding for specific parameters linked with graph theory; for instance, Mollard [12] showed the existence of perfect codes from subgraphs, called cubes .

2 Preliminaries

In this section, the fundamental theory behind our research is given.

Theorem 2.1. *([13]) Let* $\mathcal{U}$ *be* $\imath$*-blocking set in* $PG(2, p)$, $p \ge 5$ *a prime.*
i. *If* $\imath < p/2$, *then* $|\mathcal{U}| \ge (p + 1)(\imath + 1)/2$. **ii.** *If* $\imath > p/2$, *then* $|\mathcal{U}| \ge (\imath + 1)q$.

Theorem 2.2. *([13]) Let* $\mathcal{U}$ *be an PG(2,p)* $\imath$*-blocking set that contains a line.*
If $(\imath - 1, p) = 1$, *then* $|\mathcal{U}| \le p(\imath + 1)$.

Theorem 2.3. *([13]) Let* $\mathcal{U}$ *be an* $\{k, \imath\}$*-blocking set in* $PG(2, p)$ *with* p *prime.*

- **i.** *If* $\imath < p/2$ *and* $p \ge 5$, *then* $k \ge \imath(p + 1) + (p + 1)/2$.
- **ii.** *If* $k = \imath(p + 1) + (p + 1)/2$, *then:*
  - **1-** *There are* $(p + 3)/2$ *lines across any point* $\mathcal{U}$ *that are not* $\imath$*-secants.*
  - **2-** *There are* $(p - 1)/2$ *lines that are* $\imath$*-secants across each point of* $\mathcal{U}$.
  - **3-** *The overall numbers of* $\imath$*-secants is* $\mu = k(p - 1)/(2\imath)$

Theorem 2.4. *([14]) For an arc of degree t in $PG(2,p)$ with p prime, if $t \geq (p+3)/2$, then $m_t(2,p) \geq (t-1)p + t - (p+1)/2$.*

Theorem 2.5. *([2]) For any $(s;t)$-arc in $PG(2,q)$, the following conditions are fulfilled:*

$$\sum_{j=0}^{t} \mathrm{T}_j = q^2 + q + 1 \tag{2.1}$$

$$\sum_{j=1}^{t} j\mathrm{T}_j = s\,(q+1) \tag{2.2}$$

$$\sum_{j=2}^{t} \frac{1}{2} j\,(j-1)\,\mathrm{T}_j = \frac{1}{2} s(s-1) \tag{2.3}$$

3 Non-existence of [1864,3,1828] codes

It is known that the total number of points (lines) of the plane $PG(2,q)$ is q^2+q+1, each line has $(q+1)$ points and there are $(q+1)$ lines through a point. So, the number of points (lines) of $PG(2,53)$ is 2863 and each line has 20 points such that 20 lines pass through each point.

The values of k and $\imath$ in Theorem 2.3.(ii)(3) that make μ non-integer are given in the following theorem.

Theorem 3.1. *There exists no $[s,3,s-t]_{53}$ codes with parameters s and t given in Table 1.*

Proof. The $(s;29)$-arc, S, in $PG(2,53)$ with $s = m_{29}(2,53)$ corresponds to the 25-blocking set, $\mathcal{U} = S^c$ set with the largest size. From Theorem 2.4, $|S| \geq 1486$. Since $25 < 53/2$, by Theorem 2.1, the cardinality of the set $\mathcal{U}$ is at least 1337. Theorem 2.3(ii) shows that, there are 28 lines through each point of $\mathcal{U}$ not on 25-secants, while there are 26 lines that are 25-secants to $\mathcal{U}$. Thus, the parameter μ in Theorem 2.3(ii) is not an integer. This means that there exists no $\{1377, 25\}$-blocking set in $PG(2,53)$ and, hence, no $(1486;29)$-arc exists; that is, $m_{29}(2,53) \leq 1486$. Therefore, no $[1486,3,1457]_{53}$ code exists.
The same process shows that the desired for the other values in Table 1. $\square$

Table 1: s and t values making μ non-integer.

t	29	30	31	32	33	34
s	1486	1540	1594	1648	1702	1756
μ	35802/25	5733/4	32994/23	15795/11	10062/7	14391/10
t	35	37	38	39	40	42
s	1810	1918	1972	2026	2080	2188
μ	27378/19	24570/17	11583/8	7254/5	10179/7	2925/2
t	43	44	46	47	49	50
s	2242	2296	2404	2458	2566	2620
μ	16146/11	7371/5	5967/4	10530/7		

Theorem 3.2. *There exists no* $[s, 3, s-t]_{53}$ *codes for values* s *and* t *in Table 2 that make the parameter* μ *an integer.*

Table 2: s and t values making μ integer.

t	36	41	45	48	51	52
s	1864	2134	2350	2512	2674	2728
μ	1443	1458	1482	1521	1638	1755

Proof. Let K be an arc of degree 36 and cardinality 1864. Then the set $\mathcal{B} = K^c$ is formed $\{999, 18\}$-blocking set. By Theorem 2.3.(ii)(3), the total number of 18-secants, μ is 1443. Let ℓ^* be a line with longest intersection with K. Put $|K \bigcap \ell^*| = r$, $18 \leq r \leq 53$. Now we will prove by contradiction that no such block set exists for all integers r in the interval between 18 and 53.

Let $r = 53$. Then K contains a line properly. From Theorem 2.2, it follows that $|K| \geq 1007$, which is a contradiction.

Let $45 < r < 52$. For any point Q on ℓ^* out of K, consider the lines through Q. So, $1000 \leq 18 \times 53 + r \leq |K|$. This leads to a contradiction.

Let $20 \leq r \leq 45$. Consider the intersection of 18-secants, ℓ_j with ℓ^*. Put $i = 45 - r$. The following inequality holds:

$$\mathrm{T}_{18} \geq 26r + (54 - r)(53 - i) \tag{3.4}$$

Substituting the values of r and i in (3.4) as shown in Table 3 give a contradiction in each case.

Table 3: Values of T_{18}

r	45	44	43	42	41	40	39	38	37
i	0	1	2	3	4	5	6	7	8
$T_{18} \geq$	1647	1664	1679	1692	1703	1712	1719	1724	1727
r	36	35	34	33	32	31	30	29	28
i	9	10	11	12	13	14	15	16	17
$T_{18} \geq$	1728	1727	1724	1719	1712	1703	1692	1679	1664
r	27	26	25	24	23	22	21	20	
i	18	19	20	21	22	23	24	25	
$T_{18} \geq$	1647	1628	1607	1584	11559	1532	1503	1472	

Let $r = 18$ or $r = 19$. The equations (2.1), (2.2) and (2.3) in Theorem 2.5 give the following system:

$$\begin{pmatrix} 1 & 1 \\ 118 & 19 \\ 306 & 342 \end{pmatrix} \begin{pmatrix} T_{18} \\ \\ T_{19} \end{pmatrix} = \begin{pmatrix} 2864 \\ 53946 \\ 997002 \end{pmatrix}.$$

This system has no solution. Thus, there is no $\{999, 18\}$-blocking set and hence, no $(1864; 36)$-arc is exists; that is, $m_t(2, 53) \leq 1863$. Therefore, $[1864, 3, 1828]_{53}$ code does not exist.
The remaining cases are proved similarly. □

4 Conclusion

When $p = 53$, the combinatorial technique that we used and the relations among arc, blocking set and linear code show that with respect to linear code there are no linear codes of dimension three over F_p for certain values of lengths $s = (t-1)p + t - (p+1)/2, (p+3)/2 < t < p$, and minimum Hamming distance $d = s - t$. Also, the upper bounds of $m_t(2, p)$ are given below. Let $\hat{m}$ refer to $m_t(2, 53) \leq$.

t	$\hat{m}$	t	$\hat{m}$	t	$\hat{m}$	t	$\hat{m}$	t	$\hat{m}$	t	$\hat{m}$
29	1485	30	1539	31	1593	32	1647	33	1701	34	1755
35	1809	36	1863	37	1917	38	1971	39	2025	40	2079
41	2133	42	2187	43	2241	44	2295	45	2349	46	2403
47	2457	48	2511	49	2565	50	2619	51	2673	52	2727

References

[1] S. Ball, A Course in Algebraic Error-Correcting Codes, Birkhauser, Springer Nature Switzerland AG, 2020.

[2] G. Kiss, T. Szonyi, Finite Geometries, 1^{st} Edition, Chapman and Hall/CRC, 2020.

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

[4] S. Alabdullah, Classification of Arcs in Finite Geometry and Applications to Operational Research, Ph.D. Thesis, University of Sussex, UK, 2018.

[5] J. Bierbrauer, D. Bartoli, G. Faina, S. Marcugini, F. Pambianco, The nonexistence of an additive quatemary $[15, 5, 9]$-code, Finite Fields and Their Applications, **36**, (2015), 29–40.

[6] E. J. Cheon, The non-existence of Griesmer codes with parameters close to codes of Belov type, Designs, codes and Cryptography, **61**, no. 2, (2011), 131–139.

[7] S. Ball, On the size of triple blocking set in $PG(2, q)$, European J. Combin., **17**, (1998), 427–435.

[8] A. E. M. Sulaimaan, N. Y. Kasm Yahya, The Reverse construction of complete (k, n)-arcs in three dimensional projective space $PG(3, 4)$, Journal of Physics: Conference Series, **1591**, (2020).

[9] A. E. M. Sulaimaan, N. Y. Kasm Yahya, The Reverse construction of complete (k, n)-arcs in $PG(2, q)$ where $q = 2, 4, 8$ related with linear codes, Journal of Physics: Conference Series, **1591**, (2020).

[10] E. B. Al-Zangana, S. A. Joudah, Action of groups on the projective plane over the field $GF(41)$, Journal of Pysics: Conference Series, **1003**, (2018), 012059.

[11] E. B. Al-Zangana, E. A. shehab, Certain types of linear codes over the finite field of order twenty-five, Iraqi Journal of Science, **62**, no. 11, Accepted on January 2021, to appear.

[12] M. Mollard, The existence of perfect codes in a family of generalized Fibonacci cubes, Information Processing Letters, Elsevier, **140**, (2018), 1–3.

[13] R. N. Daskalov, On the existence and the nonexistence of some $(k; r)$-arcs in $PG(2, 17)$, In Proceedings of Ninth International Worksop on Algebraic and Combinatorial Coding Theory, Kranevo, Bulgaria, (2004), 95–100.

[14] S. Ball, On Sets of Points in Finite Planes, Ph.D. Thesis, University of Sussex, UK, 1994.