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

Clearly, an $(s; t)$-arc, $S$ in a projective plane over $F_q$ gives an $i$-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 \( m_t(2, 53), 29 \leq t \leq 52 \). 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 quaternary 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 properties 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 codes 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 \( U \) be an \( (s, ı) \)-blocking set in \( PG(2, p) \), \( p \geq 5 \) a prime.

i. If \( ı < p/2 \), then \(|U| \geq (p+1)(ı+1)/2\).

ii. If \( ı > p/2 \), then \(|U| \geq (ı+1)q\).

**Theorem 2.2. ([13])** Let \( U \) be an \( PG(2, p) \) \( (s, ı) \)-blocking set that contains a line.

If \((ı−1, p) = 1\), then \(|U| \leq p(ı+1)\).

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

i. If \( ı < p/2 \) and \( p \geq 5 \), then \( k \geq ı(p+1) + (p+1)/2\).

ii. If \( k = ı(p+1) + (p+1)/2 \), then:

1. There are \((p+3)/2\) lines across any point \( U \) that are not \( ı \)-secants.

2. There are \((p−1)/2\) lines that are \( ı \)-secants across each point of \( U \).

3. The overall numbers of \( ı \)-secants is \( \mu = k(p−1)/(2ı) \).
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:

\begin{align*}
\sum_{j=0}^{t} T_j &= q^2 + q + 1 \quad (2.1) \\
\sum_{j=1}^{t} j T_j &= s(q + 1) \quad (2.2) \\
\sum_{j=2}^{t} \frac{1}{2} j (j - 1) T_j &= \frac{1}{2} s(s - 1) \quad (2.3)
\end{align*}

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 $i$ in Theorem 2.3(ii)(3) that make $\mu$ 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, $U = S^c$ 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 $U$ is at least 1337. Theorem 2.3(ii) shows that, there are 28 lines through each point of $U$ not on 25-secants, while there are 26 lines that are 25-secants to $U$. Thus, the parameter $\mu$ 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.
The Non-existence of $[1864, 3, 1828]_{53}$ Linear Code...

Table 1: $s$ and $t$ values making $\mu$ non-integer.

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

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

Table 2: $s$ and $t$ values making $\mu$ integer.

<table>
<thead>
<tr>
<th>$t$</th>
<th>36</th>
<th>41</th>
<th>45</th>
<th>48</th>
<th>51</th>
<th>52</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s$</td>
<td>1864</td>
<td>2134</td>
<td>2350</td>
<td>2512</td>
<td>2674</td>
<td>2728</td>
</tr>
<tr>
<td>$\mu$</td>
<td>1443</td>
<td>1458</td>
<td>1482</td>
<td>1521</td>
<td>1638</td>
<td>1755</td>
</tr>
</tbody>
</table>

Proof. Let $K$ be an arc of degree 36 and cardinality 1864. Then the set $B = K^c$ is formed $\{999, 18\}$-blocking set. By Theorem 2.3.(ii)(3), the total number of 18-secants, $\mu$ is $1443$. Let $\ell^*$ be a line with longest intersection with $K$. Put $|K \cap \ell^*| = r$, $18 \leq r \leq 53$. 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 $\ell^*$ 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, $\ell_j$ with $\ell^*$. Put $i = 45 - r$. The following inequality holds:

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

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 $T_{18}$

<table>
<thead>
<tr>
<th>$r$</th>
<th>45</th>
<th>44</th>
<th>43</th>
<th>42</th>
<th>41</th>
<th>40</th>
<th>39</th>
<th>38</th>
<th>37</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i$</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>$T_{18} \geq$</td>
<td>1647</td>
<td>1664</td>
<td>1679</td>
<td>1692</td>
<td>1703</td>
<td>1712</td>
<td>1719</td>
<td>1724</td>
<td>1727</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$r$</th>
<th>27</th>
<th>26</th>
<th>25</th>
<th>24</th>
<th>23</th>
<th>22</th>
<th>21</th>
<th>20</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i$</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
</tr>
<tr>
<td>$T_{18} \geq$</td>
<td>1647</td>
<td>1628</td>
<td>1607</td>
<td>1584</td>
<td>1559</td>
<td>1532</td>
<td>1503</td>
<td>1472</td>
<td>1443</td>
</tr>
</tbody>
</table>

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.

\[\square\]

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 $m_t(2,53) \leq$.

<table>
<thead>
<tr>
<th>$t$</th>
<th>$\hat{m}$</th>
<th>$t$</th>
<th>$\hat{m}$</th>
<th>$t$</th>
<th>$\hat{m}$</th>
<th>$t$</th>
<th>$\hat{m}$</th>
<th>$t$</th>
<th>$\hat{m}$</th>
<th>$t$</th>
<th>$\hat{m}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>1485</td>
<td>30</td>
<td>1539</td>
<td>31</td>
<td>1593</td>
<td>32</td>
<td>1647</td>
<td>33</td>
<td>1701</td>
<td>34</td>
<td>1755</td>
</tr>
<tr>
<td>35</td>
<td>1809</td>
<td>36</td>
<td>1863</td>
<td>37</td>
<td>1917</td>
<td>38</td>
<td>1971</td>
<td>39</td>
<td>2025</td>
<td>40</td>
<td>2079</td>
</tr>
<tr>
<td>41</td>
<td>2133</td>
<td>42</td>
<td>2187</td>
<td>43</td>
<td>2241</td>
<td>44</td>
<td>2295</td>
<td>45</td>
<td>2349</td>
<td>46</td>
<td>2403</td>
</tr>
<tr>
<td>47</td>
<td>2457</td>
<td>48</td>
<td>2511</td>
<td>49</td>
<td>2565</td>
<td>50</td>
<td>2619</td>
<td>51</td>
<td>2673</td>
<td>52</td>
<td>2727</td>
</tr>
</tbody>
</table>
The Non-existence of [1864, 3, 1828]_53 Linear Code...

References


