The Use of 7-Blocking Sets in Galois Geometries

Nada Yassen Kasm Yahya
Department of Mathematics, College of Education
University of Mosul, Mosul-Iraq

ABSTRACT

The lower bounds for the size of \( \mu \)-blocking sets where \( \mu = 7 \) is unknown except for \( \mu \leq 6 \). In this work we finding lower bounds for the size of 7-blocking set we obtain three main results about it in Galois geometries. These bounds are proved in the case \( q \) is square, which are the following results theorems.

1. Introduction:

Évariste Galois (French pronunciation: [evaʁist ɡalwa]) (25 October 1811 – 31 May 1832) was a French mathematician born in Bourg-la-Reine. While still in his teens, he was able to determine a necessary and sufficient condition for a polynomial to be solvable by radicals, thereby solving a long-standing problem. His work laid the foundations for Galois theory and group theory, two major branches of abstract algebra, and the subfield of Galois connections. He was the first to use the word "group" (French: group) as a technical term in mathematics to represent a group of permutations. A radical Republican during the monarchy of Louis Philippe in France, he died from wounds suffered in a duel under questionable circumstances [Ball, 2009] at the age of twenty. In my dissertation, \( p \) always denotes an arbitrary prime and \( q = p^n (n \geq 1) \) always denotes an arbitrary prime power (that can also be a prime). \( GF(q) \) denotes the finite field with \( q \) elements, and \( F \) can denote an arbitrary field (or also a Euclidean ring) [Bertrand, 1899], [Caroline, 2008], [Dupuy, 1896], [Rigatelli, 1996], [Verdier, 2003].

Galois geometry is geometry over a finite field (a "Galois" field), particularly algebraic geometry and analytic geometry; it is a branch of finite geometry. Objects of study include vector spaces (and affine spaces) and projective spaces over finite fields. More narrowly, a Galois geometry may be defined as a projective space over a finite field. Algebraic geometry is a branch of mathematics which combines techniques of abstract algebra, especially commutative algebra, with the language and the problems of geometry. It occupies a central place in modern mathematics and has multiple conceptual connections with such diverse fields as complex analysis, topology and number theory. Initially a study of polynomial equations in many variables, the subject of algebraic geometry starts where equation solving leaves off, and it becomes at least as important to understand the totality of solutions of a system of equations, as to find some solution; this leads into some of the deepest waters in the whole of mathematics, both conceptually and in terms of technique [Dembowski, 1968], [Hirschfeld, 1979], [Hirschfeld, 1991], [Landjev and Storme, 1996], [Segre, 1976].
In this paper, PG(d, q) denotes the projective Galois geometry of dimension d over the finite field GF(q), when one identifies the vector lines of V(N+1, q) as being the points of PG(N, q). These finite projective spaces PG(N, q) are also called Galois geometries [Hirschfeld, 1979], [Hirschfeld, 1991].

A μ-blocking set in a projective plane is a set S of points with the property that each line contains at least μ points of S. A 1-blocking set is known as a blocking set and is defined with the extra condition that it should contain no line. If μ = 2 or 3 such sets are known as double or triple blocking sets respectively [Ball, 2009], [Hirschfeld, 1979], [Storme, 2010].

Non-trivial μ-blocking set B in PG(2,q) does not contain a line, and q + r(q) + 1 = size of smallest non-trivial blocking set in PG(2,q), r(q) = (q+1)/2 for q > 2 prime, r(q) = q^2/3 for q cube power [Storme, 2010]. From now on, we will consider non-trivial 7-blocking sets only. In PG(2,q), q is square a non-trivial μ-blocking set B of size q + \sqrt{q} + 1 is called a Baer subplane with the property that every line joining two points of B contain precisely \sqrt{q} + 1 points of B, and this line called Baer subline. The field GF(q) \cup \{\infty\} can be identified with the projective line PG(1,q). It contains the Baer subline GF(\sqrt{q} ) \cup \{\infty\} [Hirschfeld, 1979].

2. μ-Blocking Sets in PG(2,q)

In this section we review the known results containing important information about the possible sizes of μ-blocking sets in PG(2;q) which we shall use subsequently. Suppose that 2 ≤ μ ≤ q.

Proposition (2.1) [Ball, 2009]: If B is a proper subset of the points of PG(2;q) and it is a μ-blocking set then |B| ≥ μ(q + 1).

Proof: Let P ∈ PG(2;q) \setminus B be a point not in the blocking set. There are q + 1 lines through P and each line contains at least μ points of B (and these points are distinct).

Theorem (2.2) [Blokhuis, 1994]: Let B be a μ-blocking set with respect to lines in PG(2;p) where p is an arbitrary prime. If 2 ≤ μ ≤ q then |B| ≥ μp + μ + \min \left\{ \frac{p + 1}{2}, p - μ \right\}

Theorem (2.3) [Ball, 2009]: Let B be a μ-blocking set in PG(2;q). If B contains no line then it has at least μq + \sqrt{\mu q} + 1 points.

Theorem (2.4) [Blokhuis, 2007]: Let B be a μ-blocking set in PG(2;p), p > 3 prime.

1. If μ ≤ p/2 then |B| ≥ (μ + 1/2)(p + 1).
2. If μ > p/2 then |B| ≥ (μ + 1)p.

Theorem (2.5) [Ball, 2009]: Let B be a μ-blocking set in PG(2;q), where μ < min(q^{1/6}, q^{1/4}/2), if d ≥ 2, p > 3, q = p^d then |B| ≥ μ(q + \sqrt{q} + 1)

Theorem (2.6) [Ball, 2009]: Let B be a μ-blocking set in PG(2;q), where μ < min(q^{1/3}, q^{1/6}, q^{1/4}/2), if d ≥ 2, p > 3, q = p^d then |B| ≥ μ(q + \sqrt{q} + 1)

The following properties of a Baer subline will be used as well [Hirschfeld, 1979]:

```
1-the intersection of dual Baer subline with line is a Baer subline.
2-two Baer subline intersect in at most two points.
3-if one has two points and two dual Baer subline through these points so that the line joining the two points belongs to both Baer subline, then the intersection of the lines of these Baer sublines contain a Baer subplane.

3. Lower Bounds of The Size of 7-Bloking Sets
The object of this section is to obtain good lower bounds for the size of a 7-blocking sets in PG(2,q),q is square. Using the results in the previous section we are now able to prove the following .

Lemma(3.1):
Let B be 7-blocking set of size k in PG(2,q);|B|=k ,if L is an i-secant to B ,then k≥i+7q
Proof: Let P be a point in L\B , since every another line through P containing at least 7 points of B then |B|≥ 7(q+1-1) +i then k≥i+7q.

Theorem(3.2):
Let B be a 7-blocking set in PG(2,q),q is square (\sqrt{q} >7 ),such that through each of its points there are \sqrt{q} +1 lines containing at least \sqrt{q} +7 points of B and forming a dual Baer subline ,then |B|≥7q +2\sqrt{q} +7.

Proof:
Calling the line meeting B in at least \sqrt{q} +7 points long line if two long lines meet outside B ,then |B|≥2(\sqrt{q} +7)+7(q+1-2)= 7q +2\sqrt{q} +7 .If every two long lines meet in B, let L be a long line and P ∈ B not on L.
The long line through P containing a dual Baer subline and meet L in Baer subline ,let Q be a point on this Baer subline ,consider long lines through a point of 7-secant to Q these long lines meet L in another Baer subline not containing Q ,since two Baer subline meet in at most two points ,so L has at least 2(\sqrt{q} +1) -2=2\sqrt{q} points.
So every long line has at least 2\sqrt{q} points of B. Hence 
|B|≥1+(\sqrt{q} +1)(2\sqrt{q} -1)+6(q +1-(\sqrt{q} +1)) =8q -5\sqrt{q}
Since 8q-5\sqrt{q} >7q +2\sqrt{q} +7 ,for \sqrt{q} >7 then |B|≥ 7q +2\sqrt{q} +7.

Lemma(3.3):
for \sqrt{q} >33,q is square let B be a 7-blocking set in PG(2,q),having through every point at least \sqrt{q} +1lines , containing at least \sqrt{q} +7points of B and forming a dual then |B|≥7q +3\sqrt{q} +7points.

Proof:
Let B behave fewer than 7q +3\sqrt{q} +7.points call lines meeting B in at least \sqrt{q} +7points long lines ,take 21 points on long line L then at least 21(\sqrt{q} (\sqrt{q} +6 )points of B\L lying on the long lines through these 21 points with
multiplicity since $B \setminus L$ containing less than \((7q + 3\sqrt{q} + 7) - (\sqrt{q} + 7) = 7q + 2\sqrt{q}\) of points, so there exists more than \(21\sqrt{q} (\sqrt{q} + 6) - 3(7q + 2\sqrt{q}) = 120\sqrt{q}\) of points on four or more long lines through 21 points (with multiplicity).

Let $P_1$ be a point of $B \setminus L$ joined to at least four of these 21 points on $L$ by long line. Let $S_i$ be the point of $L$ at which the long line through $P_i$ meet $L$, the set $S_i$ has most \(\sqrt{q} + 2\) points other wise $P_i$ lies on at least \(\sqrt{q} + 3\) long lines. So that $B$ contains at least \(1 + (\sqrt{q} + 3)(\sqrt{q} + 6) + 6(q - \sqrt{q} - 2) = 1 + q + 9\sqrt{q} + 18 + 6q - 6\sqrt{q} - 12 = 7q + 3\sqrt{q} + 7\)

The bound obtained (since $B$ has fewer than \((7q + 3\sqrt{q} + 7)\).

By assumption $b_i$ contains a baer subline $b_i$, since there exists 120 \(\sqrt{q}\) points in $B \setminus L$ (with multiplicity) meeting four of the 21 points.

There exist 120 \(\sqrt{q}\) points the corresponding $b_i$ of which meet at least three of the 21 points. There exists $P_1, P_2$ correspond to $b_1, b_2$ of which meet at least 3 points, since two a baer subline meet at least two points, $b_1 \equiv b_2$.

If 3 long lines meet in $P \notin B$ then $B$ has at least \(3(\sqrt{q} + 7) + 7(q - 2) = 7q + 3\sqrt{q} + 7\). There exists no 3 long lines meet outside $B$, so there exists at most two long lines meet outside. The long lines through $P_1, P_2$ meet $L$ in at most one point outside $B$ and the point lies on the long line joining $P_1, P_2$. Let $S$ be the set of points of $L \cap B$ at which $b_1 \equiv b_2$ meet $L \cap B$, then $S$ has \(q + 1\) points.

So there are \(\binom{21}{3} = 1330\) different sets of three points of these 21 points. There exists $P_1, P_2$ correspond to $b_1, b_2$ of which meet at least 3 points, since two a baer subline meet at least two points, $b_1 \equiv b_2$.

If 3 long lines meet in $P \notin B$ then $B$ has at least \(3(\sqrt{q} + 7) + 7(q - 2) = 7q + 3\sqrt{q} + 7\). There exists no 3 long lines meet outside $B$, so there exists at most two long lines meet outside. The long lines through $P_1, P_2$ meet $L$ in at most one point outside $B$ and the point lies on the long line joining $P_1, P_2$. Let $S$ be the set of points of $L \cap B$ at which $b_1 \equiv b_2$ meet $L \cap B$, then $S$ has \(q + 1\) points.

So there are \(\binom{21}{3} = 1330\) different sets of three points of these 21 points. There exists $P_1, P_2$ correspond to $b_1, b_2$ of which meet at least 3 points, since two a baer subline meet at least two points, $b_1 \equiv b_2$.

If 3 long lines meet in $P \notin B$ then $B$ has at least \(3(\sqrt{q} + 7) + 7(q - 2) = 7q + 3\sqrt{q} + 7\). There exists no 3 long lines meet outside $B$, so there exists at most two long lines meet outside. The long lines through $P_1, P_2$ meet $L$ in at most one point outside $B$ and the point lies on the long line joining $P_1, P_2$. Let $S$ be the set of points of $L \cap B$ at which $b_1 \equiv b_2$ meet $L \cap B$, then $S$ has \(q + 1\) points.

So there are \(\binom{21}{3} = 1330\) different sets of three points of these 21 points. There exists $P_1, P_2$ correspond to $b_1, b_2$ of which meet at least 3 points, since two a baer subline meet at least two points, $b_1 \equiv b_2$.

If 3 long lines meet in $P \notin B$ then $B$ has at least \(3(\sqrt{q} + 7) + 7(q - 2) = 7q + 3\sqrt{q} + 7\). There exists no 3 long lines meet outside $B$, so there exists at most two long lines meet outside. The long lines through $P_1, P_2$ meet $L$ in at most one point outside $B$ and the point lies on the long line joining $P_1, P_2$. Let $S$ be the set of points of $L \cap B$ at which $b_1 \equiv b_2$ meet $L \cap B$, then $S$ has \(q + 1\) points.

So there are \(\binom{21}{3} = 1330\) different sets of three points of these 21 points. There exists $P_1, P_2$ correspond to $b_1, b_2$ of which meet at least 3 points, since two a baer subline meet at least two points, $b_1 \equiv b_2$.

If 3 long lines meet in $P \notin B$ then $B$ has at least \(3(\sqrt{q} + 7) + 7(q - 2) = 7q + 3\sqrt{q} + 7\). There exists no 3 long lines meet outside $B$, so there exists at most two long lines meet outside. The long lines through $P_1, P_2$ meet $L$ in at most one point outside $B$ and the point lies on the long line joining $P_1, P_2$. Let $S$ be the set of points of $L \cap B$ at which $b_1 \equiv b_2$ meet $L \cap B$, then $S$ has \(q + 1\) points.

So there are \(\binom{21}{3} = 1330\) different sets of three points of these 21 points. There exists $P_1, P_2$ correspond to $b_1, b_2$ of which meet at least 3 points, since two a baer subline meet at least two points, $b_1 \equiv b_2$.

If 3 long lines meet in $P \notin B$ then $B$ has at least \(3(\sqrt{q} + 7) + 7(q - 2) = 7q + 3\sqrt{q} + 7\). There exists no 3 long lines meet outside $B$, so there exists at most two long lines meet outside. The long lines through $P_1, P_2$ meet $L$ in at most one point outside $B$ and the point lies on the long line joining $P_1, P_2$. Let $S$ be the set of points of $L \cap B$ at which $b_1 \equiv b_2$ meet $L \cap B$, then $S$ has \(q + 1\) points.

So there are \(\binom{21}{3} = 1330\) different sets of three points of these 21 points. There exists $P_1, P_2$ correspond to $b_1, b_2$ of which meet at least 3 points, since two a baer subline meet at least two points, $b_1 \equiv b_2$.
least $\sqrt{q} + 8$ points of $B$. So $|B| \geq 1 + (\sqrt{q} + 1)(\sqrt{q} + 7) + 6(q - \sqrt{q}) = 7q + 2\sqrt{q} + 8$, that is also contradicts the number of points of $B$. Hence $|B| \geq 7q + 3\sqrt{q} + 7$, for $\sqrt{q} > 33$.

**Theorem (3.4):**
(for $\sqrt{q} > 33$, $q$ is square).
Let $B$ be a 7-blocking set in PG(2, $q$), such that each of its points is one of the following:

1. the meet of a secant of length $2\sqrt{q} + 7$ or more and $\sqrt{q}$-secant each of length at least $\sqrt{q} + 7$;
2. the meet of two $i$-secant of length $2\sqrt{q} + 7$ or more and $\sqrt{q}$-2 secant each of length at least $\sqrt{q} + 7$;
3. the meet of at least $\sqrt{q} + 1$ lines that meet $B$ in at least $\sqrt{q} + 7$ points and contain each dual Baer subline then $|B| \geq 7q + 3\sqrt{q} + 7$.

**Proof:**
Call the secant of length $2\sqrt{q} + 7$ or more a long line and call the secant of length $\sqrt{q} + 7$ long line and call this point of type 3 is special point. If every point of $B$ is of type 3, then by lemma (3.3) $|B| \geq 7q + 3\sqrt{q} + 7$, now assume that $\lambda$ is the number of very long lines and assume $\lambda$ is non-zero and hence $B$ has at least $2\sqrt{q} + 7 + 7q = 7q + 2\sqrt{q} + 7$ points.
Assume $B$ has points fewer than $7q + 3\sqrt{q} + 7$ that implies, very long line meet long lines and other very long line in $B$ because if they meet in point meet not in the $B$, $|B| \geq 7q + 3\sqrt{q} + 7$.

Assume every very long line has exactly $2\sqrt{q} + 7$ points, there exists at least $7q + 2\sqrt{q} + 7 - (2\sqrt{q} + 7) \lambda + \lambda(\lambda - 1)/2$ special point.
Consider $L$ to be a very long line and $P$ be a special points $P \not\in L$, the long lines through $P$ meet $L \cap B$ in a set containing a Baer subline.
$\forall Q$ in this Baer subline $\exists$ in another Baer subline in $L \cap B$ not containing $Q$. This is since, there is a special point on $7$-secant through $Q$ so the long lines through $Q$ containing at most $\sqrt{q}(\sqrt{q} + 6 - 3/2)$ special point, and this always less than the total number of special point, so $L \cap B$ split into two disjoint dual Baer subline and 5 points or $L$ has at least $3\sqrt{q} - 3$, because very long lines has at least $2\sqrt{q} + 7$.
Assume $L$ split into two dual Baer subline and 5 points take $Q1$ point of type 1 and $Q2$ point of type 2 in separate Baer subline in $L \cap B$. If every point of type 1 $\lambda = 1$, if every point is of type 2, then $\lambda = 2\sqrt{q} + 8$ and take two points $Q1,Q2$ of type 2. The long line through $Q1$ containing at most $\sqrt{q}(\sqrt{q} + 6 - (3-1)/2)$ special points.

The long line through $Q2$ meet at most $(\sqrt{q} - 2)(\sqrt{q} + 7 - 3/2)$ special point, the number of special point joined $Q1,Q2$ by 7-secant is $7q + 2\sqrt{q} + 7 - (2\sqrt{q} + 7)\lambda + \lambda(\lambda - 1)/2 - \sqrt{q}(\sqrt{q} + 6 - (3-1)/2 - (\sqrt{q} - 2)(\sqrt{q} + 7 - 3/2)$
$= 1/2\lambda^2 - 1/2(17 + 2\sqrt{q})\lambda^2 + 5\lambda - 19/2\sqrt{q} + 21/8(17 + 2\sqrt{q})^2 > 0$. 

1233
Similarly if every point is of type 1, then \( b = 1 \), and take the two points \( Q_1, Q_2 \) of type 1.

\[
7q + 2\sqrt{q} + 7 - (2\sqrt{q} + 7)3 + 3(3 - 1)/2 - 2\sqrt{q} (\sqrt{q} + 6 - (3 - 1)/2)
\]

\[
= 7q + 2\sqrt{q} + 7 - 2\sqrt{q} - 7 + 0 - 2q - 12\sqrt{q}
\]

\[
= 5q - 12\sqrt{q} > 0 \text{ (for } \sqrt{q} > 33) \]

Similarly for \( b = 2 \), we have

\[
7q + 2\sqrt{q} + 7 - (2\sqrt{q} + 7)3 + 3(3 - 1)/2 - 2(\sqrt{q} - 2)(\sqrt{q} + 7 - 3/2)
\]

\[
= 5q - 19\sqrt{q} - 9
\]

Which is positive (for \( \sqrt{q} > 33 \)) \( L \) contains \( 3\sqrt{q} - 3 \) special point. \( \exists \) a very long line with more than \( 2\sqrt{q} + 7 \) points, this implies there are at least

\[
(2\sqrt{q} + 8)(\sqrt{q} - 2)
\]

\[
= (2\sqrt{q} + 8)\sqrt{q} - 2(2\sqrt{q} + 8)
\]

\[
= (2\sqrt{q} + 8)\sqrt{q} - 23
\]

Because \( b = 2\sqrt{q} + 8 \) long lines meet at most \( \sqrt{q} + 2 \) in a point otherwise.

\[
|B| \geq 1 + (\sqrt{q} + 3)(\sqrt{q} + 6) + 6(q + 1 - \sqrt{q} - 3)
\]

\[
= 7q + 3\sqrt{q} + 7
\]

If a long line has \( \sqrt{q} + 7 \) points then it meet at most:

\[
(\sqrt{q} + 7)(\sqrt{q} + 1) + (q + 1 - (\sqrt{q} + 7)) - 23
\]

\[
= q + 8\sqrt{q} + 7q + 1 - \sqrt{q} - 7 - 23
\]

\[
= 2q + 8\sqrt{q} - \sqrt{q} + 1 - 23
\]

\[
= (2\sqrt{q} + 8)\sqrt{q} - \sqrt{q} + 1 - 23
\]

Long lines. Every long line has at least \( \sqrt{q} + 8 \) points. The number of points through \( Q_1 \) is at least

\[
1 + 2\sqrt{q} + 7 + \sqrt{q}(\sqrt{q} + 7) + 6(q - \sqrt{q})
\]

\[
= 1 + 2\sqrt{q} + 7 + q + 7\sqrt{q} + 6q - 6\sqrt{q}
\]

\[
= 7q + 3\sqrt{q} + 8
\]

The number of points through \( Q_2 \)

\[
1 + 2(\sqrt{q} + 7) + (\sqrt{q} - 2)(\sqrt{q} + 7) + q + 1 - 2(\sqrt{q} - 2)
\]

\[
= 1 + 4\sqrt{q} + 14 + q + 5\sqrt{q} - 14 + 6q + 6 - 6\sqrt{q}
\]

\[
= 7q + 3\sqrt{q} + 7
\]

Therefore \( |B| \geq 7q + 3\sqrt{q} + 7 \).
References
Ahmad, Ch.A. (2006), Lower Bounds of t-Blocking sets in PG(2,q)and the Existence of minimal Blocking sets of size 16 and 17 in PG(2,9), M.Sc. Thesis ,University of Mosul.
AL-Taee ,R.S.D. (2011), Anon PGL(3,q)and non PΓL(3,q)k-arcs in PG(2,32)and Lower Bounds of 5-blocking set, M.Sc. Thesis ,University of Mosul.
Storme ,L. (2010),"The use of blocking sets in Galois geometries and related research areas", Ghent University, Dept. of Mathematics , Krijgslaan 281 - S22, 9000 Ghent,Belgium Bangalore, August 31, pp.1-62.

1235