Proof of a conjecture of Metsch

Zsuzsa Weiner and Tamás Szőnyi *

July 30, 2014

Abstract

In this paper we prove a conjecture of Metsch about the maximum number of lines intersecting a pointset in PG(2, q), presented at the conference ”Combinatorics 2002”. As a consequence, we give a short proof of the famous Jamison, Brouwer-Schrijver bound on the size of the smallest affine blocking set in AG(2, q).

1 Introduction

At the conference “Combinatorics 2002”, Klaus Metsch presented the following conjecture.

Conjecture 1.1. Let B be a point set in PG(2, q). Pick a point P not from B and assume that through P there pass exactly r lines meeting B (that is containing at least 1 point of B). Then the total number of lines meeting B is at most $1 + rq + (|B| - r)(q + 1 - r)$.

In this paper, we prove the above conjecture to be true, see Theorem 4.1. Klaus Metsch used this theorem to give lower bound on the number of s-spaces missing a given point set in PG(n, q), see [9]. Later, this latter theorem was used to determine the chromatic number of the q-Kneser graphs, see [3].

A blocking set in a projective or affine plane is a set of points intersecting each line of the plane. An m-fold blocking set is a blocking set intersecting

*The authors were partially supported by K 81310 and NK 67867 grants. The second author was also supported by ERC Grant 227701 DISCRETECONT.
each line in at least \( m \) points. In Section 4, we will show that Theorem 4.1 is stronger than the famous Jamison, Brouwer and Schrijver result on the size of the smallest affine blocking set in \( \text{AG}(2,q) \). As a consequence, the theorem also yields Bruen’s lower bound on the minimal number of points of an \( m \)-fold blocking set.

2 A bound on the degree of the greatest common divisor

In this section, we recall results from [10] and [11], where a condition is given which guarantees that the greatest common divisor of two given polynomials has a prescribed degree. Then we refine these results by introducing a variable for the degree of the second polynomial.

**Result 2.1.** Let \( u(X) = u_0 X^n + u_1 X^{n-1} + \ldots \ (u_0 \neq 0) \) be a polynomial of degree \( n \) and \( v(X) = v_0 X^{n-1} + v_1 X^{n-2} + \ldots \) be a polynomial of degree at most \( n-1 \). Denote by \( R_k \) the following \( 2k \times 2k \) matrix:

\[
R_k = \begin{pmatrix}
    u_0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\
    u_1 & u_0 & 0 & \ldots & 0 & v_0 & 0 & \ldots & 0 \\
    u_2 & u_1 & u_0 & \ldots & 0 & v_1 & v_0 & \ldots & 0 \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
    u_{k-1} & u_{k-2} & u_{k-3} & \ldots & u_0 & v_{k-2} & v_{k-3} & \ldots & v_0 \\
    u_k & u_{k-1} & u_{k-2} & \ldots & u_1 & v_{k-1} & v_{k-2} & \ldots & v_0 \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
    u_{2k-1} & \ldots & \ldots & u_k & v_{2k-2} & v_{2k-3} & \ldots & v_{k-1}
\end{pmatrix}
\]

where \( u_j, j > n \) or \( j < 0 \) and \( v_i, i > n - 1 \) or \( i < 0 \) are defined to be zero.

If the degree of the greatest common divisor of \( u \) and \( v \) is \( n - k \), then the determinant of \( R_k \) is non-zero. When the degree of the greatest common divisor is greater than \( n - k \), then \( \det R_k = 0 \).

Note that \( \det R_k \) plays a very similar role to the resultant. Actually, deleting the first row and the first column of \( R_k \) we get back a submatrix of the resultant; for \( n = k \) it is just the resultant of the two polynomials.
The advantage now is that when the greatest common divisor of the two polynomials has large degree, then the matrix \( R_k \) is small.

**Result 2.2.** Suppose that the polynomials \( u(X, Y) = \sum_{i=0}^{n} u_i(Y)X^{n-i} \) and \( v(X, Y) = \sum_{i=0}^{n-i} v_i(Y)X^{n-1-i} \), satisfy \( \deg u_i(Y) \leq i \) and \( \deg v_i(Y) \leq i \), and \( u_0 \neq 0 \). Then the following holds.

1. The determinant of \( R_k(Y) \) in Result 2.1 has \( Y \)-degree at most \( k(k-1) \).

2. For \( Y = y' \), let \( n - (k - h) \) be the degree of the greatest common divisor of \( u(X, y') \) and \( v(X, y') \). Assume that \( h \) is non-negative and construct the matrix \( R_k(Y) \) of Result 2.1. Then \( (Y - y')^h \) divides \( \det R_k(Y) \).

In [11], Result 2.2 (2) was proved for three variable polynomials where the coefficients \( v_i \) and \( u_i \) were homogeneous polynomials. A similar argument yields that the above result holds for two variable inhomogeneous polynomials.

### 2.1 A new parameter

In this section we will assume that the polynomial \( v \) has degree at most \( n-m \), \( m \geq 1 \), and we will see how we can refine the above results by using this new parameter. Hence we assume that \( v(X, Y) = v'_0(Y)X^{n-m} + v'_1(Y)X^{n-m-1} + \cdots \), where \( \deg v'_i(Y) \leq i \). Of course, the polynomial \( v \) can still be written in the form of the previous section, that is \( v = 0X^n + 0X^{n-1} + \cdots + 0X^{n-m+1} + v'_0(Y)X^{n-m} + \cdots \). With this in mind, Result 2.1 and Result 2.2 will obviously still hold. The main difference now, is that we have stronger conditions on the degrees of the \( v_i \)-s. More precisely, instead of \( \deg v_i \leq i \), we have that \( v_i = v'_{i-(m-1)} \), when \( i \geq m-1 \) and so \( \deg v_i \leq i - (m-1) \), when \( i \geq m-1 \); otherwise \( v_i = 0 \). Note that in each term of the determinant \( R_k(Y) \), there are \( k \) \( v_i \)-s, and since now the bound on the degree of each \( v_i \) dropped by \((m-1)\) (or \( v_i \) is zero), the degree of each term in the determinant will drop by \( k(m-1) \). Hence the bound in Result 2.2 will be \( k(m-1) \) less.

**Result 2.3.** Suppose that the polynomials \( u(X, Y) = \sum_{i=0}^{n} u_i(Y)X^{n-i} \) and \( v(X, Y) = \sum_{i=0}^{n-m} v_i(Y)X^{n-m-i} \), \( m > 0 \), satisfy \( \deg u_i(Y) \leq i \) and \( \deg v'_i(Y) \leq i \), and \( u_0 \neq 0 \). Then the determinant of \( R_k(Y) \) in Result 2.1 has \( Y \)-degree at most \( k(k-m) \), when \( k \geq m \) and it is zero otherwise.
As in [10] and [11], Result 2.2 and Result 2.3 have a very important corollary, which will be crucial in the remaining part of this paper.

**Corollary 2.4.** Using the notation of Result 2.3, assume that there exists a value \( y \), so that the degree of the greatest common divisor of \( u(X, y) \) and \( v(X, y) \) is \( n - k \). Denote by \( n_h \), the number of values \( y' \) for which \( \deg(\gcd(u(X, y'), v(X, y'))) = n - (k - h) \), \( h > 0 \).

Then

\[
\sum_{h=1}^{k-1} h n_h \leq \deg(\det\mathcal{R}_k(Y)) \leq k(k - m).
\]

### 3 The Rédei polynomial

Let \( \ell_\infty \) be the line at infinity in \( \text{PG}(2, q) \) and let \( U = \{(a_i, b_i) : i = 1, \ldots, n\} \) be a set of points in \( \text{PG}(2, q) \setminus \ell_\infty \). Then the **Rédei polynomial** of \( U \) is the following polynomial in two variables:

\[
H(X, Y) = \prod_{i=1}^{n} (X + a_i Y - b_i) = \sum_{j=0}^{n} h_j(Y) X^{n-j}.
\]

Note that \( h_j(Y) \) is a polynomial of degree at most \( j \). It is not difficult to see that this polynomial encodes the intersection numbers of \( U \) and the affine lines.

**Lemma 3.1.** For a fixed \( y \in \text{GF}(q) \), the element \( x \in \text{GF}(q) \) is an \( r \)-fold root of \( H(X, y) \) if and only if the line with equation \( Y = yX + x \) intersects \( U \) in exactly \( r \) points. Similarly, for a fixed \( x \in \text{GF}(q) \), the element \( y \in \text{GF}(q) \) is an \( r \)-fold root of \( H(x, Y) \) if and only if the line with equation \( Y = yX + x \) intersects \( U \) in exactly \( r \) points.

### 4 How many lines can meet a point set?

Now we prove a conjecture of Metsch presented at the conference “Combinatorics 2002”, see [8]. The proof is an immediate consequence of Corollary 2.4. It can also be found in [12].

**Theorem 4.1.** Let \( B \) be a point set in \( \text{PG}(2, q) \). Pick a point \( P \) not from \( B \) and assume that through \( P \) there pass exactly \( r \) lines meeting \( B \) (that is
containing at least 1 point of \( B \)). Then the total number of lines meeting \( B \) is at most \( 1 + rq + (|B| - r)(q + 1 - r) \).

Before the proof, observe that there are point sets for which the given bound is sharp. Assume that \( r - 1 \) is the order of a subplane \( \pi \) in \( \text{PG}(2, q) \) and let \( B \) be the proper subset of \( \pi \) containing \( r \) collinear points. Since \( B \) blocks all the lines of \( \pi \), the number of lines meeting \( B \) is \((|r - 1|^2 + (r - 1) + 1) + |B|(q + 1 - r)\). The first part is the number of lines in \( \pi \), the second counts the lines through the points of \( B \) which does not contain a line of \( \pi \). Choose \( P \) to be in \( \pi \setminus B \), hence the number of lines through \( P \) meeting \( B \) is \( r \) and so the bound in the Theorem 4.1 is sharp. Note that the following well-known result of Jamison [7] and Brouwer and Schrijver [4] is a consequence of the statement of Theorem 4.1.

**Result 4.2.** (Jamison, Brouwer and Schrijver) A blocking set in \( \text{AG}(2, q) \) contains at least \( 2q - 1 \) points.

**Proof.** Assume to the contrary that there is a blocking set \( B \) in \( \text{AG}(2, q) \), of size \( |B| \leq 2q - 2 \). Embed \( \text{AG}(2, q) \) into \( \text{PG}(2, q) \) and let \( P \) be an ideal point. Now the value \( r \) in Theorem 4.1 is \( q \) and so the total number of lines meeting \( B \) is at most \( 1 + q^2 + (|B| - q)(q + 1 - q) \leq q^2 + q - 1 \); which is a contradiction, since \( B \) blocks all the \( q^2 + q \) affine lines.

There are blocking sets of size less than \( 2q - 1 \) in certain non-Desarguesian affine planes of order \( q \), see [6]. This shows that Theorem 4.1 cannot be true for arbitrary projective planes.

For the proof of Theorem 4.1 the following lemma is crucial.

**Lemma 4.3.** Let \( \ell_\infty \) be the line at infinity in \( \text{PG}(2, q) \) and let \( S \) be a point set in \( \text{PG}(2, q) \setminus \ell_\infty \). Assume that \( |S| \neq q \) and suppose that through the ideal point \( (y) \) there pass \( t \) affine lines meeting \( S \). Denote by \( n_{t+h} \) the number of ideal points, not including \( (\infty) \), through that there pass exactly \( t + h \) affine lines meeting \( S \). Then \( \sum_{h=1}^{q-1} hn_{t+h} \leq (|S| - t)(q - t) \).

**Proof.** For the points of \( S \) write \( \{(a_i, b_i)\} \) and consider the Rédei polynomial of \( S \), that is \( H(X, Y) = \prod_{i=1}^{|S|} (X + a_i Y - b_i) = \sum_{j=0}^{|S|} h_j(Y)X^{|S|-j} \). Recall that \( \deg h_j \leq j \). It follows from Lemma 3.1, that \( \deg_X \gcd(H(X, y), (X^q - X)) = t \).

For the polynomials \( H \) and \( X^q - X \) and for the value \( k = \max(\deg_X H, q) - t \), construct the matrix \( R_k(Y) \) introduced in Result 2.1. The result now follows from Corollary 2.4. \( \square \)
Proof of Theorem 4.1: For the line at infinity $\ell_\infty$ choose an $m$-secant of $B$ passing through $P$, where $m > 0$. Note that now the line at infinity meets $B$, hence through $P$ there pass $(r-1)$ affine lines containing at least 1 point from $B$. Let $(\infty) \in B$ and again denote by $n_{(r-1)+h}$ the number of ideal points, not including $(\infty)$, through which there pass exactly $(r-1)+h$ affine lines meeting $B$. Let us sum up the number of affine lines meeting $B$ through the ideal points, in total we get at most $qm + [(q+1-m)(r-1) + \sum_{h=1}^{q-(r-1)} h n_{(r-1)+h}]$; where the first part corresponds to the points of $\ell_\infty \cap B$, the second to the points of $\ell_\infty \setminus B$. When $|B \setminus \ell_\infty| \neq q$, then the result follows from Lemma 4.3 immediately.

Now assume that for each line $\ell$ through $P$, for which $\ell$ contains at least 1 point of $B$, $|B \setminus \ell| = q$ holds. This means that each line through $P$, which intersects $B$, contains the same number of points from $B$. Then either each line through $P$ contains exactly 1 point of $B$, hence $r = q + 1$ and so the bound in Theorem 4.1 gives $1 + q + q^2$ (which is just the total number of lines of PG(2, $q$)), or it follows that $|B| \geq 2r$. Note that in the latter case $r < q + 1$, hence there is a line $\ell'$ through $P$ so that it is skew to $B$. Since now $|B| \geq 2r$, choosing $\ell'$ to be the line at infinity, Lemma 4.3 gives that the total number of lines meeting $B$ is at most $(q+1)r + (|B| - r)(q-r)$, which (since now $|B| \geq 2r$) is a stronger bound than what we have in the theorem.

4.1 Another immediate corollary

An $m$-fold blocking set in AG(2, $q$) is a set of points intersecting each line in at least $m$ points. For $m = 1$, we have already seen the surprising result by Jamison, Brouwer and Schrijver, see Result 4.2. Bruen [5] proved the following lower bound on the size of an $m$-fold blocking set.

Result 4.4. (Bruen) The size of an $m$-fold blocking set in AG(2, $q$) is at least $(m+1)q - m$.

Blokhuis ([2]) improved on the above result by showing that an $m$-fold blocking set $S$ in AG(2, $q$), where $(m, q) = 1$, has at least $(m+1)q - 1$ points. Later Ball ([1]) extended this result to arbitrary $m$; he showed that if $e(m)$ is the maximal exponent such that $p^{e(m)}|m$, then $|S| \geq (m+1)q - p^{e(m)}$.

In this subsection we show that Corollary 2.4 immediately implies Result 4.4.
Proof of Result 4.4. Assume to the contrary that there exists an affine $m$-fold (not necessarily minimal) blocking set $B$ of size $(m+1)q - m - 1$. Let $\ell$ be an $(m+k)$-secant, $k \geq 0$, where $|B| - (m+k) \neq qm$. Such a line $\ell$ can be chosen, since counting the points of $B$ on the lines through a point of $B$ and on the lines through an affine point not in $B$ shows that the intersection numbers of $B$ with lines take at least two different values. Change the coordinate system, so that $\ell$ is the line at infinity and $(\infty) \in B$. Now $B$ contains at least $m$ points from each line, except from the ‘old’ line at infinity that is skew to $B$. Denote this line by $\ell'$ and by $(y')$ the ideal point of it in this new coordinate system. Let $U = B \setminus \ell = \{(a_i, b_i)\}_i$ and consider the Rédei polynomial of $U$, that is $H(X, Y) = \prod_{i=1}^{|B|-(m+k)} (X + a_iY - b_i) = \sum_{j=0}^{|B|-(m+k)} h_j(Y)X^{|B|-(m+k)-j}$. By Lemma 3.1, $\deg_X \gcd(H(X,y'),(X^q-X)^m) = m(q-1)$ and for any $(y') \in \ell \setminus (B \cup (y'))$, $\deg_X \gcd(H(X,y'),(X^q-X)^m) = mq$. For the polynomial $H$ and $(X^q-X)^m$ and for the value $s = \max(\deg_X H, qm) - m(q-1)$, construct the matrix $R_s$ introduced in Section 2. By Result 2.1, the determinant of this matrix is not zero. Furthermore, similarly as in the proof of Lemma 4.3, one can show that $\deg(\det R_s) \leq m(q-m-k-1)$. To obtain a contradiction, we apply Corollary 2.4. For the $y$ value in the corollary, we choose $y'$, for the polynomial $u$ we choose the polynomial $H$, and for $v$ the polynomial $(X^q-X)^m$. Above we saw, that for every value $y'$ not in $B$, $h$ in the corollary will be $m$ and there are $(q-m-k)$ of such values. So Corollary 2.4 says that $m(q-m-k) \leq \deg(\det R_s)$, which contradicts our previous upper bound on $\deg(\det R_s)$. \hfill \Box

References


Authors address:
Tamás Szönyi, Zsuzsa Weiner
Department of Computer Science, Eötvös Loránd University,
H-1117 Budapest, Pázmány Péter sétány 1/C, HUNGARY
e-mail: szonyi@cs.elte.hu, weiner@cs.elte.hu

Tamás Szönyi
Computer and Automation Research Institute of the Hungarian Academy of Sciences
H-1111 Budapest, Lágymányosi út 11, HUNGARY

Zsuzsa Weiner
Prezi.com
H-1075 Budapest, Károly krt. 9., HUNGARY
e-mail: zsuzsa.weiner@prezi.com