Lecture 1: A conjecture by van Lint & MacWilliams and its confirmation by Blokhuis

Sergey Goryainov
(Hebei Normal University)

Lectorium on Algebraic Graph Theory

Mathematical Center in Akademgorodok,
Novosibirsk, Russia

April 11, 2023

Affine planes

An affine plane is a system of points and lines that satisfy the following axioms:

- Any two distinct points lie on a unique line.
- Given any line and any point not on that line there is a unique line which contains the point and does not meet the given line. (Playfair's axiom)
- There exist three non-collinear points (points not on a single line).

In an affine plane, two lines are called parallel if they are equal or disjoint. Using this definition, Playfair's axiom above can be replaced by:

- Given a point and a line, there is a unique line which contains the point and is parallel to the line.

The familiar Euclidean plane is an affine plane. In this lecture we are interested in finite affine planes (that is, affine planes having finitely many points).

Properties of finite affine planes

If the number of points in an affine plane is finite, then if one line of the plane contains n points then:

- each line contains n points,
- each point is contained in $n + 1$ lines,
- there are n^2 points in all, and
- there is a total of $n^2 + n$ lines.

The number n is called the order of the affine plane.

Affine plane $AG(2, q)$

Let q be a prime power and W be a 2-dimensional vector space over the finite fields $GF(q)$.

Then the set of all cosets of 0-dimensional and 1-dimensional subspaces of W, ordered by inclusion, forms an affine plane of order q, denoted by $AG(2, q)$.

Identification of the elements of $GF(q^2)$ and the points of $AG(2,q)$

Let $F = GF(q^2)$. Then F can be viewed in a canonical way as a two-dimensional vector space over $GF(q)$, or, as the affine plane $AG(2,q)$.

Each nonzero element uniquely defines a line through 0 and can be viewed as a slope of this line.

Basic properties of finite fields

Let F be a finite field.

- If F has characteristic 2, then each element of the multiplicative group F^* is a square.
- If F has an odd characteristic, then the multiplicative group F^* has an even number of elements, and exactly a half of them are squares.

Let F be a finite field of an odd order r. Then the field F is known to be the splitting field for the polynomial

$$z^r - r = z(z^{\frac{r-1}{2}} - 1)(z^{\frac{r-1}{2}} + 1).$$

Moreover, each square from F^* is a root of

$$z^{\frac{r-1}{2}} - 1,$$

and each non-square from F^* is a root of

$$z^{\frac{r-1}{2}} + 1.$$

Lines in $AG(2,q)$

Let $F = GF(q^2)$, where q is an odd prime power.

Let d be a non-square in F^*. Consider the polynomial $g(z) = z^2 - d$, which is irreducible over $GF(q)$.

Let α be a root of f. Then we have

$$F = \{x + y\alpha \mid x, y \in GF(q)\}.$$

Under the indentification, a line in $AG(2,q)$ can be written as

$$\{x_1 + y_1\alpha + c(x + y\alpha) \mid c \in GF(q)\},$$

where $x + y\alpha$ is a slope.

Quadratic and non-quadratic lines in $AG(2,q)$

Let $F = GF(q^2)$, where q is an odd prime power.

The lines of the plane $AG(2,q)$ are q-subsets with the property that the difference of two elements is either always a square, or always a non-square, depending only on the slope of the line.

Thus the lines are partitioned into two classes, S and N (for square and non-square type). Through each point of $AG(2,q)$ there pass $\frac{q+1}{2}$ lines of S and $\frac{q+1}{2}$ lines of N.

Hence on an arbitrary line l of S not passing through 0, there are $\frac{q+1}{2}$ non-squares (indeed, the line parallel to l containing 0 is also in S; consider the lines connecting 0 with a point of l; note that $\frac{q-1}{2}$ of them lie in S and $\frac{q+1}{2}$ of them lie in N; the latter ones intersect l in $\frac{q+1}{2}$ points, which are non-squares).

van Lint & MacWilliams conjecture

In 1978, van Lint and MacWilliams conjectured that the only q-subset X if $GF(q^2)$, with the properties $0, 1 \in X$ and $x - y$ is a square for all $x, y \in X$, is the set $GF(q)$.

Currently, this conjecture has been proved in several ways, but the first proof is due to Blokhuis. In this lecture, we discuss the Blokhuis' proof in detail.

A general statement in terms of special sets

Let $X \subset F$ be a set of points such that all differences are squares. Call such a set special. Then aX is also special if a is a square (and "anti-special" if a is a non-square), and $X + a$ is special for all a. We will consider special q-sets containing 0.

Theorem (Blokhuis, 1984)

Let X be a special q-set. Then X is a line in S.

It is easy to see that this theorem confirms the van Lint & MacWilliams conjecture.

Furthermore, if $0 \in X$ let $X_0 := X \setminus \{0\}$.

The proof will be established in a series of lemmas. Assume $0 \in X$ (if not then a translation will do).

A polynomial criterion for a q-set with 0 to be a line (I)

Let $f_X(t) := \prod_{x \in X_0} (t - x)$.

Lemma 1

Let X be a q-set in $GF(q^2)$ containing 0*. The set X is a line if and only if*

$$f_X(t) = t^{q-1} + \prod_{x \in X_0} x.$$

Proof.

($\Rightarrow$) A line through 0 looks like $\{ia \mid i \in GF(q)\}$ for some non-zero element $a \in GF(q^2)$.

Given a non-zero element $j \in GF(q)$, consider

$$f_X(ja) = (ja)^{q-1} + \prod_{i \in GF(q)^*} ia = a^{q-1} + a^{q-1} \prod_{i \in GF(q)^*} i =$$

$$= a^{q-1} - a^{q-1} = 0.$$

A polynomial criterion for a q-set with 0 to be a line (II)

Thus, the $q-1$ elements of $X_0 = \{ia \mid i \in GF(q)^*\}$ are roots of the polynomial $t^{q-1} + \prod_{x \in X_0} x$. In means that

$$t^{q-1} + \prod_{x \in X_0} x = \prod_{x \in X_0} (t-x) = f_X(t).$$

$(\Leftarrow)$ Suppose

$$f_X(t) = \prod_{x \in X_0} (t-x) = t^{q-1} + \prod_{x \in X_0} x$$

holds. For any $y_1, y_2 \in X_0$, we have

$$0 = f_X(y_1) = (y_1)^{q-1} + \prod_{x \in X_0} x$$

and

$$0 = f_X(y_2) = (y_2)^{q-1} + \prod_{x \in X_0} x.$$

A polynomial criterion for a q-set with 0 to be a line (III)

It implies that, for any $y_1, y_2 \in X$, we have $(y_1)^{q-1} = (y_2)^{q-1}$ and, consequently, $(y_1^{-1} y_2)^{q-1} = 1$.

This means that $y_1^{-1} y_2 \in GF(q)^*$.

Thus, there exists $i \in GF(q)^*$ such that $y_2 = i y_1$. It implies that $X_0 = \{i y_1 \mid i \in GF(q)^*\}$. $\square$

kth elementary symmetric function of the set X

Let $\sigma_k(X)$ denote the kth elementary symmetric function of the (finite) set X, that is,

$$\prod_{x\in X}(1+xt)=\sum_{k=0}^{|X|}\sigma_k(X)t^k.$$

In other words, $\sigma_k(X)$ denotes the sum of all k-products of elements from X.

Since

$$f_X(t)=\prod_{x\in X_0}(t-x)=t^{q-1}-\sigma_1(X_0)t^{q-2}+\sigma_2(X_0)t^{q-3}-\dots$$

$$-\sigma_{q-2}(X_0)t+\sigma_{q-1}(X_0)=\sum_{k=0}^{q-1}(-1)^k\sigma_k(X_0)t^{q-1-k},$$

it suffices to show that $\sigma_k(X_0)=0$ if $0<k<q-1$.

Reduction to a half of the symmetric functions

Lemma 2

Let $X_0 \cup \{0\}$ be an arbitrary special q-set. To show that $\sigma_k(X_0) = 0$ for $0 < k < q-1$, it suffices to prove that $\sigma_k(X_0) = 0$ for $0 < k \leq \frac{q-1}{2}$.

Proof.

First prove that, $X_0^{-1} \cup \{0\}$ is a special q-set. Let $x_1, x_2 \in X_0$ be two arbitrary distinct elements. Then x_1^{-1}, x_2^{-1} represent arbitrary elements in $X_0^{(-1)}$. We have $x_1^{-1} - x_2^{-1} = x_1^{-1}x_2^{-1}(x_2 - x_1)$. Since x_1^{-1}, x_2^{-1} and $(x_2 - x_1)$ are squares, the set $X_0^{-1} \cup \{0\}$ is a special q-set.

By the assumption of the lemma, we have that $\sigma_k(X_0) = 0$ and $\sigma_k(X_0^{(-1)}) = 0$ for $0 < k \leq \frac{q-1}{2}$.

Since

$$\sigma_{q-1-k}(X_0) = \sigma_k(X_0^{(-1)}) \cdot \prod_{x \in X_0} x,$$

we conclude that $\sigma_k(X_0) = 0$ for $\frac{q-1}{2} < k < q-1$. $\square$

A decomposition of the set of non-squares

Let A be a set of $\frac{q+1}{2}$ non-squares such that $a-b$ is a square for $a, b \in A$ (an example of such a set is the collection of non-squares on a line in S, not through the origin). Call such a set extra-special.

Lemma 3

Let A be any extra-special set and X be a special q-set containing 0. *Then $A \cdot X_0 = \{ax \mid a \in A, x \in X_0\}$ is the set of all non-squares in F.*

Proof.

Obviously, $A \cdot X_0$ contains only non-squares. Since there are $\frac{q^2-1}{2}$ products ax involved, it remains to show that all are different. Suppose $a_1x_1 = a_2x_2$ $(a_1, a_2 \in A,\ x_1, x_2 \in X)$. Then $a_1x_1 - a_2x_1 = a_2x_2 - a_2x_1$ and $(a_1 - a_2)x_1 = a_2(x_2 - x_1)$. The element $(a_1 - a_2)x_1$ is square. The element $a_2(x_2 - x_1)$ is either non-square or $x_1 = x_2$, but then $a_1 = a_2$. □

Using the decomposition

For an element $a \in A$, put

$$f_{X,a}(t) = \prod_{x \in X_0} (t - ax)$$

Lemma 4

For an extra-special set A and a special q-set X, the equality

$$\prod_{a \in A} f_{X,a}(t) = t^{\frac{q^2-1}{2}} + 1$$

holds.

Proof.

We have

$$\prod_{a \in A} f_{X,a}(t) = \prod_{\substack{a \in A \\ x \in X_0}} (t - ax) = \prod_{\substack{n \in F \\ n \in \not\square}} (t - n) = t^{\frac{q^2-1}{2}} + 1.$$

Main lemma (I)

Lemma 5

Let $X_0 \cup 0$ be an arbitrary special q-set. Then $\sigma_k(X_0) = 0$ for $0 < k \leq \frac{q-1}{2}$ holds.

Proof.

Let $m \leq \frac{q-1}{2}$ be the smallest positive integer with the property $\sigma_m(X_0) \neq 0$ (if there is no such m, we are done).
Then

$$f_{X,a}(t) = t^{q-1} + (-1)^m a^m \sigma_m(X_0) t^{q-1-m} + \text{terms of lower degree.}$$

As a consequence:

$$\prod_{a \in A} f_{X,a}(t) = t^{\frac{q^2-1}{2}} + (-1)^m (\sum_{a \in A} a^m) \sigma_m(X_0) t^{\frac{q^2-1}{2} - m} +$$

$$+ \text{terms of lower degree.}$$

Main lemma (II)

Since

$$\prod_{a\in A} f_{X,a}(t) = t^{\frac{q^2-1}{2}} + 1$$

and $\sigma_m(X_0) \neq 0$, it follows that

$$\sum_{a\in A} a^m = 0$$

for all extra-special sets A.

For an extra-special set A and an integer s, put

$$A^{(s)} = \{a^s \mid a \in A\}.$$

Main lemma (III)

Let us show that, for an extra-special set A, the sets $A^{(-1)}$ and A^q are extra-special. Take arbitrary $a_1, a_2 \in A$. It means that a_1, a_2 are non-squares and $a_1 - a_2$ is a square. Note that $a_1^{-1}, a_2^{-1}, a_1^q, a_2^q$ are non-squares. Then $a_1^{-1} - a_2^{-1} = (a_1 a_2)^{-1}(a_2 - a_1)$ is a square, and $A^{(-1)}$ is extra-special. Also, $a_1^q - a_2^q = (a_1 - a_2)^q$ is a square, which means that A^q is extra-special. Hence, $A^{(-q)}$ is extra-special and we have:

$$\sum_{a \in A} a^{-qm} = 0 \text{ for all extra-special sets } A.$$

Since, for any non-square a, the equality $a^{\frac{q^2-1}{2}} = -1$ holds, we finally have

$$\sum_{a \in A} a^{\frac{q^2-1}{2} - qm} = 0 \text{ for all extra-special sets } A.$$

Main lemma (IV)

Let $t \in GF(q^2) \setminus GF(q)$ and take $A = \{t+i \mid i \in GF(q), t+i \in \not\square\}$. Then

$$0 = 2 \sum_{\substack{i \in GF(q) \\ t+i \in \not\square}} (t+i)^{\frac{q^2-1}{2}-qm} =$$

$$= \sum_{\substack{i \in GF(q) \\ t+i \in \not\square}} (t+i)^{\frac{q^2-1}{2}-qm} + \sum_{\substack{i \in GF(q) \\ t+i \in \not\square}} (t+i)^{\frac{q^2-1}{2}-qm} =$$

$$= (\sum_{\substack{i \in GF(q) \\ t+i \in \not\square}} (t+i)^{\frac{q^2-1}{2}-qm} + \sum_{\substack{i \in GF(q) \\ t+i \in \square}} (t+i)^{\frac{q^2-1}{2}-qm})+$$

$$+(\sum_{\substack{i \in GF(q) \\ t+i \in \not\square}} (t+i)^{\frac{q^2-1}{2}-qm} - \sum_{\substack{i \in GF(q) \\ t+i \in \square}} (t+i)^{\frac{q^2-1}{2}-qm}) =$$

Main lemma (V)

$$= \sum_{i \in GF(q)} (t+i)^{\frac{q^2-1}{2} - qm} -$$

$$-(\sum_{\substack{i \in GF(q) \\ t+i \in \not\square}} (t+i)^{\frac{q^2-1}{2}} (t+i)^{\frac{q^2-1}{2} - qm} + \sum_{\substack{i \in GF(q) \\ t+i \in \square}} (t+i)^{\frac{q^2-1}{2}} (t+i)^{\frac{q^2-1}{2} - qm}) =$$

$$= \sum_{i \in GF(q)} (t+i)^{\frac{q^2-1}{2} - qm} - (\sum_{\substack{i \in GF(q) \\ t+i \in \not\square}} (t+i)^{q^2-1-qm} + \sum_{\substack{i \in GF(q) \\ t+i \in \square}} (t+i)^{q^2-1-qm}) =$$

$$= \sum_{i \in GF(q)} (t+i)^{\frac{q^2-1}{2} - qm} - \sum_{i \in GF(q)} (t+i)^{q^2-1-qm}.$$

Main lemma (VI)

Put

$$F(t) := \sum_{i \in GF(q)} (t+i)^{\frac{q^2-1}{2}-qm} - \sum_{i \in GF(q)} (t+i)^{q^2-1-qm}.$$

The polynomial $F(t)$ vanishes for all $t \in GF(q^2) \setminus GF(q)$. Since $F(t)$ has degree less than $q^2 - q$, it is identically zero.

Main lemma (VII)

Consider the coefficient of t^{q^2-qm-q} in $F(t)$. Since

$$q^2 - qm - q > \frac{q^2-1}{2} - qm,$$

$$q^2 - q > \frac{q^2-1}{2},$$

$$q(q-1) > \frac{(q-1)(q+1)}{2},$$

$$q > \frac{q+1}{2},$$

$$2q > q+1,$$

$$q > 1,$$

we only need to consider the term $\sum_{i \in GF(q)} (t+i)^{q^2-1-qm}$ of $F(t)$.

Main lemma (VIII)

We apply the binomial theorem

$$(x+y)^n = x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \ldots + \binom{n}{n-1} x y^{n-1} + y^n$$

to $(t+i)^{q^2-1-qm}$ and then sum up by i; this gives

$$\binom{q^2-qm-1}{q^2-qm-q} \sum_{i \in GF(q)} i^{q-1} = 0.$$

Main lemma (IX)

Note that

$$\sum_{i \in GF(q)} i^{q-1} = q - 1 \equiv -1 \pmod{p},$$

where p is the characteristic of $GF(q)$. To have a contradiction, it suffices to show that $\binom{q^2-qm-1}{q^2-qm-q} \not\equiv 0 \pmod{p}$. We have

$$\binom{q^2-qm-1}{q^2-qm-q} = \frac{(q^2-qm-1)!}{(q^2-qm-q)! \cdot (q-1)!} =$$

$$= \frac{(q^2-qm-1)(q^2-qm-2)\dots(q^2-qm-(q-1))}{1 \cdot 2 \cdot \ldots \cdot (q-1)} =$$

$$= \prod_{j=1}^{q-1} \frac{q^2-qm-j}{j}.$$

Main lemma (X)

Let us show that

$$\frac{q^2 - qm - j}{j} \equiv -1 \pmod{p}.$$

If p does not divide j, it is clear that

$$\frac{q^2 - qm - j}{j} \equiv -1 \pmod{p}.$$

Consider the case when p does divide j. Let $j = p^s r$ for some positive integers s and r, where p does not divide r. Then

$$\frac{q^2 - qm - j}{j} = \frac{q^2 - qm}{p^s r} - 1 \equiv -1 \pmod{p}.$$

Main lemma (XI)

Let us show that p divides $\frac{q^2-qm}{p^s r} = \frac{q(q-m)}{p^s r}$. Let $q = p^n$ for some positive integer n. Then we have

$$\frac{q(q-m)}{p^s r} = \frac{p^{n-s}(q-m)}{r}.$$

It suffices to show that $n - s \geq 1$. We have

$$p^n = q > j = p^s r,$$

$$p^{n-s} > r \geq 1,$$

which means that $n - s > 0$. □

Concluding remarks

In this lecture we have considered the Blokhuis proof of van Lint & MacWilliams conjecture.

In the next lecture we will discuss why the quadratic lines in $AG(2, q)$ can be viewed as canonical cliques in the Paley graph $P(q^2)$, and the Blokhuis' result can be viewed as establishing strict EKR-property for Paley graphs of square order.

Thank you for your attention!