ON THE (WEAK) CYLINDER CONJECTURE

Finite Geometry Workshop Szeged 2017

April 29, 2017

jan@debeule.eu

VUB VRIJE UNIVERSITEIT BRUSSEL

THREE MUSKETEERS IN PÉCS, 2016

THE STATEMENT

Conjecture (S. Ball 2008)

Let q be prime. Let U be a set of q^2 points of $\mathrm{AG}(3,q)$ such that for every hyperplane π of $\mathrm{AG}(3,q)$

$$|U \cap \pi| \equiv 0 \pmod{q}.$$

Then U is the set of points of q parallel lines.

THE STATEMENT

Conjecture (S. Ball 2008)

Let q be prime. Let U be a set of q^2 points of $\mathrm{AG}(3,q)$ such that for every hyperplane π of $\mathrm{AG}(3,q)$

$$|U \cap \pi| \equiv 0 \pmod{q}.$$

Then U is the set of points of q parallel lines.

Definition

A *cylinder* in $\mathrm{AG}(3,q)$ is the set of points of q parallel lines.

RICH AND EMPTY PLANES

Let U be a set of points of $\mathrm{AG}(3, q)$ satisfying the conditions of the cylinder conjecture.

Definition

Call a plane *rich* if it contains more than q points of U. Call a plane *empty* if it contains no points of U.

COMBINATORIAL OBSERVATIONS

Definition

Let π be a plane of $\mathrm{AG}(3, q)$. Let $n_\pi := |\pi \cap U|$ and when $|\pi \cap U| \neq 0$, call $\frac{n_\pi}{q} - 1$ the *excess of* π.

COMBINATORIAL OBSERVATIONS

Definition

Let π be a plane of $\mathrm{AG}(3, q)$. Let $n_\pi := |\pi \cap U|$ and when $|\pi \cap U| \neq 0$, call $\frac{n_\pi}{q} - 1$ the *excess of* π.

Lemma

Let l be a line meeting U in $k > 0$ points. Then the sum of the excess of the $q + 1$ planes on l equals $k - 1$.

Corollary

There exists rich planes and empty planes.

COMBINATORIAL OBSERVATIONS

Definition

Let π be a plane of $\mathrm{AG}(3, q)$. Let $n_\pi := |\pi \cap U|$ and when $|\pi \cap U| \neq 0$, call $\frac{n_\pi}{q} - 1$ the *excess of* π.

Lemma

Let l be a line meeting U in $k > 0$ points. Then the sum of the excess of the $q + 1$ planes on l equals $k - 1$.

Corollary

There exists rich planes and empty planes.

Corollary

If there is only one rich plane π, then U is the set of points of π.

COMBINATORIAL OBSERVATIONS

Lemma

The cylinder conjecture is true for $q = 3$.

COMBINATORIAL OBSERVATIONS

Lemma

The cylinder conjecture is true for $q = 3$.

Conjecture

The cylinder conjecture is true for $q = 5$.

STATEMENT

Conjecture (S. Ball 2008)

Let q be prime. Let U be a set of q^2 points of $\mathrm{AG}(3,q)$ and let N be the set of non-determined directions. If $|N| \geq p$, then U is the set of points of a cylinder.

INTERSECTION NUMBERS

Lemma

Let q be prime. Let U be a set of q^2 points of $\mathrm{AG}(3,q)$ and let N be the set of non-determined directions. If $|N| \geq q$, then for every plane π of $\mathrm{AG}(2,q)$

$$|\pi \cap U| \equiv 0 \pmod{q}.$$

INTERSECTION NUMBERS

$$U = \{(a_i, b_i, c_i, 1) | i = 1, \ldots, q^2\}.$$

INTERSECTION NUMBERS

$$U = \{(a_i, b_i, c_i, 1) | i = 1, \ldots, q^2\}.$$

$$\pi_\infty : W = 0$$

INTERSECTION NUMBERS

$$U = \{(a_i, b_i, c_i, 1) | i = 1, \ldots, q^2\}.$$

$$\pi_\infty : W = 0$$

$$\pi[x, z, y, w] : xX + yY + zZ + wW = 0$$

INTERSECTION NUMBERS

$$U = \{(a_i, b_i, c_i, 1) | i = 1, \ldots, q^2\}.$$

$$\pi_\infty : W = 0$$

$$\pi[x, z, y, w] : xX + yY + zZ + wW = 0$$

$$l[x, y, z] : xX + yY + zZ = W = 0$$

INTERSECTION NUMBERS

$$R(X, Y, Z, W) := \prod_{i=1}^{q^2} (a_i X + b_i Y + c_i Z + W).$$

INTERSECTION NUMBERS

$$R(X, Y, Z, W) := \prod_{i=1}^{q^2} (a_i X + b_i Y + c_i Z + W).$$

$$R(x, y, z, w) = 0 \iff \pi[x, y, z, w] \text{ contains } (a_i, b_i, c_i, 1).$$

INTERSECTION NUMBERS

$$R(X,Y,Z,W) := \prod_{i=1}^{q^2}(a_iX + b_iY + c_iZ + W).$$

$$R(x,y,z,w) = 0 \iff \pi[x,y,z,w] \text{ contains } (a_i,b_i,c_i,1).$$

$$R(X,Y,Z,W) = W^{q^2} + \sum_{j=1}^{q^2}\sigma_j(X,Y,Z)W^{q^2-j}.$$

INTERSECTION NUMBERS

$$R(X,Y,Z,W) = W^{q^2} + \sum_{j=1}^{q^2} \sigma_j(X,Y,Z) W^{q^2-j}\,.$$

INTERSECTION NUMBERS

$$R(X,Y,Z,W) = W^{q^2} + \sum_{j=1}^{q^2} \sigma_j(X,Y,Z) W^{q^2-j}\,.$$

$$S_j(X,Y,Z) := \sum_{i=1}^{q^2} (a_i X + b_i Y + c_i Z)^j\,,$$

$$k\sigma_k(X,Y,Z) = \sum_{i=1}^{k} (-1)^{i-1} S_i(X,Y,Z)\sigma_{k-i}(X,Y,Z).$$

INTERSECTION NUMBERS

Lemma

The polynomials $\sigma_i(X, Y, Z) = 0 = S_i(X, Y, Z)$, $i = 1 \dots q - 1$.

INTERSECTION NUMBERS

Lemma

The polynomials $\sigma_i(X, Y, Z) = 0 = S_i(X, Y, Z)$, $i = 1 \dots q - 1$.

$$G(X, Y, Z, W) := \sum_{i=1}^{q^2} (a_i X + b_i Y + c_i Z + W)^{q-1}$$

INTERSECTION NUMBERS

Lemma

The polynomials $\sigma_i(X, Y, Z) = 0 = S_i(X, Y, Z)$, $i = 1 \dots q - 1$.

$$G(X, Y, Z, W) := \sum_{i=1}^{q^2} (a_i X + b_i Y + c_i Z + W)^{q-1}$$

$$G(X, Y, Z, W) = \sum_{i=1}^{q^2} \sum_{j=0}^{q-1} \binom{p-1}{j} (a_i X + b_i Y + c_i Z)^j W^{p-1-j}.$$

INTERSECTION NUMBERS

Lemma

The polynomials $\sigma_i(X, Y, Z) = 0 = S_i(X, Y, Z)$, $i = 1 \dots q - 1$.

$$G(X, Y, Z, W) := \sum_{i=1}^{q^2} (a_i X + b_i Y + c_i Z + W)^{q-1}$$

$$G(X, Y, Z, W) = \sum_{i=1}^{q^2} \sum_{j=0}^{q-1} \binom{p-1}{j} (a_i X + b_i Y + c_i Z)^j W^{p-1-j}.$$

$$G(X, Y, Z, W) = \sum_{j=0}^{p-1} \binom{p-1}{j} S_j(X, Y, Z) W^{p-1-j}.$$

BACK TO THE WEAK CYLINDER CONJECTURE

Corollary

Every plane $\pi[x, y, z, w]$ *meets* U *in* $0 \pmod{q}$ *points.*

BACK TO THE WEAK CYLINDER CONJECTURE

Corollary

Every plane $\pi[x, y, z, w]$ *meets* U *in* $0 \pmod{q}$ *points.*

Theorem (Ball, Govaerts, Storme 2006)

If the set N *of non-determined directions contains a conic, then* U *is the set of points of a plane not meeting* N*.*

THE WEAKER CYLINDER CONJECTURE

We assume that at least $q+1$ directions are not determined, then $\sigma_q(X,Y,Z)=0$.

AN EXAMPLE

q odd, $S = \{(x, x^{\frac{q+1}{2}} | x \in \mathbb{F}_q\}$, this set determines $\frac{q+3}{2}$ points.

SOME NICE POLYNOMIALS

Lemma

The polynomials $\sigma_i(X, Y, Z) = 0$, $i = 1 \dots q$.

SOME NICE POLYNOMIALS

Lemma

The polynomials $\sigma_i(X, Y, Z) = 0$, $i = 1 \dots q$.

Lemma

$$R \cdot (G - d) = (X^q - X)\frac{\partial R}{\partial X} + (Y^q - Y)\frac{\partial R}{\partial Y} + (Z^q - Z)\frac{\partial R}{\partial Z} + (W^q - W)\frac{\partial R}{\partial W}.$$

Lemma

$$d \cdot R = X\frac{\partial R}{\partial X} + Y\frac{\partial R}{\partial Y} + Z\frac{\partial R}{\partial Z} + W\frac{\partial R}{\partial W}.$$

SOME NICE POLYNOMIALS

Lemma

The polynomials $\sigma_i(X, Y, Z) = 0$, $i = 1 \dots q$.

Lemma

$$R \cdot (G - d) = (X^q - X)\frac{\partial R}{\partial X} + (Y^q - Y)\frac{\partial R}{\partial Y} + (Z^q - Z)\frac{\partial R}{\partial Z} + (W^q - W)\frac{\partial R}{\partial W}.$$

Lemma

$$d \cdot R = X\frac{\partial R}{\partial X} + Y\frac{\partial R}{\partial Y} + Z\frac{\partial R}{\partial Z} + W\frac{\partial R}{\partial W}.$$

Corollary

$$G \cdot R = X^q\frac{\partial R}{\partial X} + Y^q\frac{\partial R}{\partial Y} + Z^q\frac{\partial R}{\partial Z} + W^q\frac{\partial R}{\partial W}$$

THE WEAKER CYLINDER CONJECTURE

Lemma

Under the assumptions for the set U, the following polynomial identities hold.

$$\sigma_k(Y,Z,W) \equiv 0\,, k = lq+1 \ldots (l+1)q-l, l = 0 \ldots q-1\,,$$

$$(-j+1)\sigma_{j+q-1}(Y,Z,W) + (Y^q\frac{\partial \sigma_j}{\partial Y} + Z^q\frac{\partial \sigma_j}{\partial Z} + W^q\frac{\partial \sigma_j}{\partial W}) \equiv 0\,,$$

$$j = q+1 \ldots q^2-q\,,$$

$$Y^q\frac{\partial \sigma_j}{\partial Y} + Z^q\frac{\partial \sigma_j}{\partial Z} + W^q\frac{\partial \sigma_j}{\partial W} \equiv 0\,, j = q^2-q+1 \ldots q^2\,.$$

INTERSECTIONS WITH LINES

- Consider the planes $\pi_s := \pi[s, 1, 0, \alpha]$ and $\pi_t := \pi[t, 0, 1, -\beta]$
- Define $l_{s,t} := \pi_s \cap \pi_t$, this is a line through $(1, -s, -t, 0)$.
- $R_{s,t}(Y, Z, W) := R(sY + tZ, Y, Z, W)$ "describes" the intersection of U with lines.

INTERSECTIONS WITH LINES

- Consider the planes $\pi_s := \pi[s, 1, 0, \alpha]$ and $\pi_t := \pi[t, 0, 1, -\beta]$
- Define $l_{s,t} := \pi_s \cap \pi_t$, this is a line through $(1, -s, -t, 0)$.
- $R_{s,t}(Y, Z, W) := R(sY + tZ, Y, Z, W)$ "describes" the intersection of U with lines.

$$G_{s,t}(Y, Z, W) := G(sY + tZ, Y, Z, W)$$

idea: try to prove that for a fixed (s, t) the polynomial $R_{s,t}(Y, Z, W)$ is a qth power.

PROJECTING FROM APEX

- Empty planes: $\pi[1,0,0,0]$ and $\pi[0,1,0,0]$, intersection point at infinity: apex $a = (0,0,1,0)$.
- Projection from a on a plane not through a.

multiset

$$U' = \{(a_i, b_i) | i = 1 \dots q^2\}$$

Define $w(x,y) : \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{N}$ as the number of times that $(x,y) \in U'$.

PROPERTIES OF THE WEIGHT FUNCTION

- $w(x,0) = 0$ for all $x \in \mathbb{F}_q$, $w(0,y) = 0$ for all $y \in \mathbb{F}_q$.
- Let $a, b \in \mathbb{F}_q$, then $\sum_{x \in \mathbb{F}_q} w(x, ax+b) \equiv 0 \pmod{q}$.
- $\sum_{x,y \in \mathbb{F}_q} w(x,y) \leq q^2$.

PROPERTIES OF THE WEIGHT FUNCTION

- $w(x,0) = 0$ for all $x \in \mathbb{F}_q$, $w(0,y) = 0$ for all $y \in \mathbb{F}_q$.
- Let $a, b \in \mathbb{F}_q$, then $\sum_{x \in \mathbb{F}_q} w(x, ax+b) \equiv 0 \pmod{q}$.
- $\sum_{x,y \in \mathbb{F}_q} w(x,y) \leq q^2$.

If a full line on a is contained in U, we can delete it, properties above remain unchanged, and furthermore

- $w(x,y) < p$ for all $x, y \in \mathbb{F}_q$

Lemma

$\sum_{x,y \in \mathbb{F}_q} w(x,y) x^k y^l = 0$, *for all* k, l *such that* $k + l \leq q$.

A COMPUTATIONAL APPROACH

Lemma

There exists no polynomial $w(X, Y)$ as described for $q \leq 13$.

BIBLIOGRAPHY

Simeon Ball and Michel Lavrauw.
How to use Rédei polynomials in higher dimensional spaces.
Matematiche (Catania), 59(1-2):39–52 (2006), 2004.

Simeon Ball and Michel Lavrauw.
On the graph of a function in two variables over a finite field.
J. Algebraic Combin., 23(3):243–253, 2006.

Simeon Ball.
On the graph of a function in many variables over a finite field.
Des. Codes Cryptogr., 47(1-3):159–164, 2008.