The 2-blocking number and the upper chromatic number of $\mathrm{PG}(2, q)$

Tamás Héger
Joint work with **Gábor Bacsó and Tamás Szőnyi**

Eötvös Loránd University
Budapest

September 18, 2012

The problem

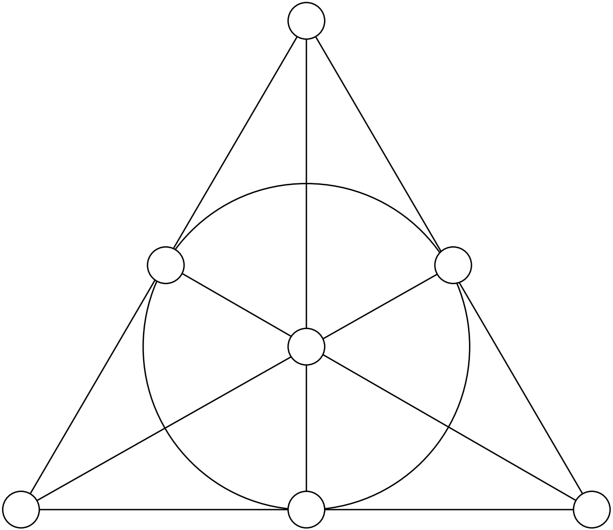
Color the vertices of a hypergraph $\mathcal{H}$.

A hyperedge is *rainbow*, if its vertices have pairwise distinct colors.

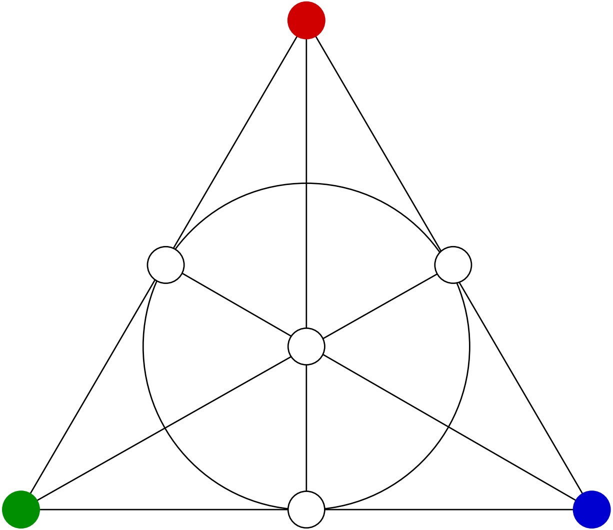
The upper chromatic number of $\mathcal{H}$, $\bar{\chi}(\mathcal{H})$: the maximum number of colors that can be used without creating a rainbow hyperedge.

Determining $\bar{\chi}(\Pi_q)$ and $\bar{\chi}(\mathrm{PG}(2,q))$ has been of interest since the mid-1990s.

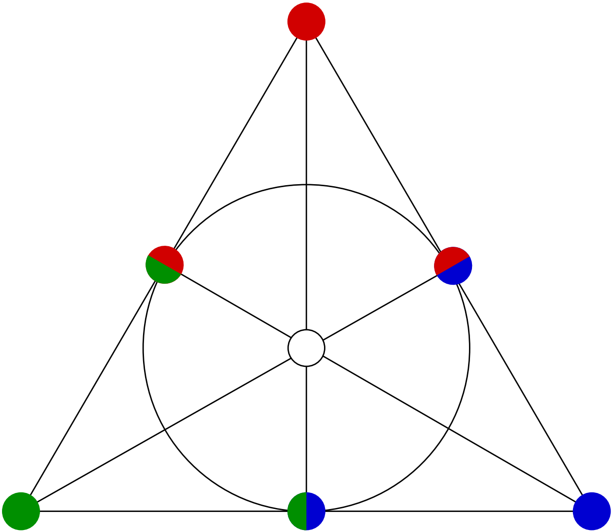
Example: $\bar{\chi}(\mathrm{PG}(2,2)) = 3$



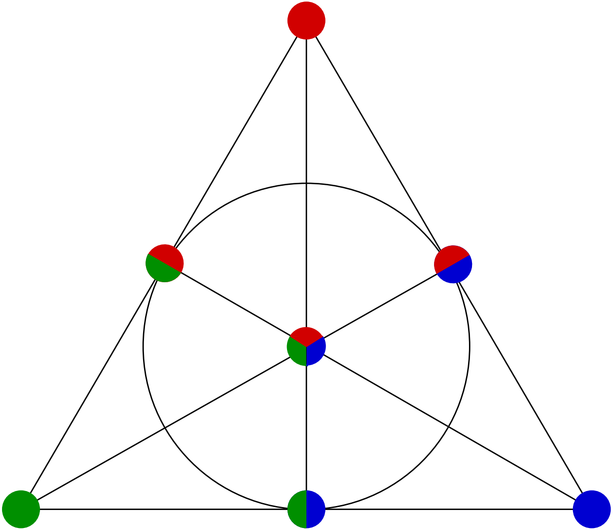
Example: $\bar{\chi}(\mathrm{PG}(2,2)) = 3$



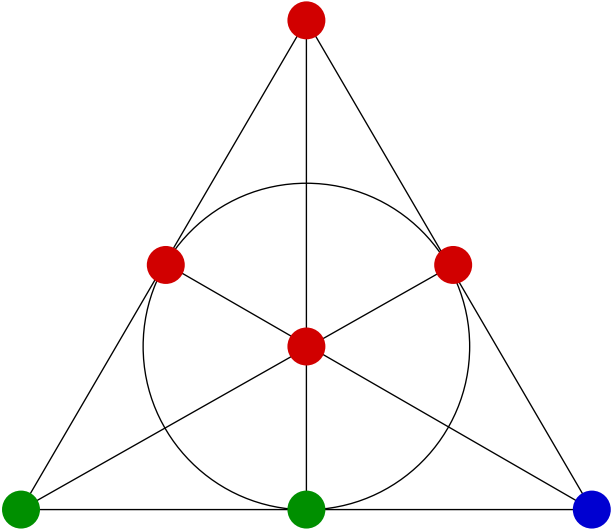
Example: $\bar{\chi}(\mathrm{PG}(2,2)) = 3$



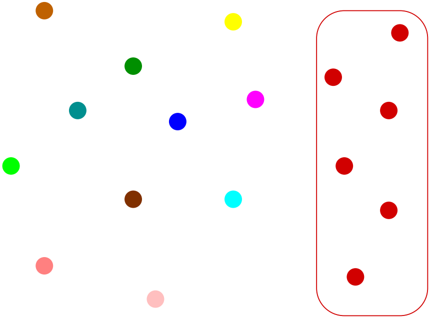
Example: $\bar{\chi}(\mathrm{PG}(2,2)) = 3$



Example: $\bar{\chi}(\mathrm{PG}(2,2)) = 3$



Trivial coloring



$v := q^2 + q + 1$, the number of points in Π_q.

$\tau_2 :=$ the size of the smallest double blocking set in Π_q.

Then $\bar{\chi}(\Pi_q) \geq v - \tau_2 + 1$.

We call this a *trivial coloring*.

Remark: if a coloring contains a monochromatic 2BS, it is not

Theorem (Bacsó, Tuza, 2007)

As $q \to \infty$,

- $\bar{\chi}(\Pi_q) \le v - (2q + \sqrt{q}/2) + o(\sqrt{q})$;
- *for q square,* $\bar{\chi}(\mathrm{PG}(2,q)) \ge v - (2q + 2\sqrt{q} + 1) = v - \tau_2 + 1$;
- $\bar{\chi}(\mathrm{PG}(2,q)) \le v - (2q + \sqrt{q}) + o(\sqrt{q})$;
- *for q non-square,* $\bar{\chi}(\mathrm{PG}(2,q)) \le v - (2q + Cq^{2/3}) + o(\sqrt{q})$.

Theorem

Let $q = p^h$, p prime. Let $\tau_2(\mathrm{PG}(2,q)) = 2(q+1)+c$. Suppose that one of the following two conditions holds:

1. $206 \le c \le c_0 q - 13$, *where* $0 < c_0 < 1/2$, $q \ge q(c_0) = 2(c_0+2)/(2/3 - c_0) - 1$, *and* $p \ge p(c_0) = 50c_0 + 24$.
2. $q > 256$ *is a square.*

Then $\bar{\chi}(\mathrm{PG}(2,q)) = v - \tau_2 + 1$, and equality is reached only by trivial colorings.

Simpler form of the above theorem:

Theorem

Let $q = p^h$, p prime. Suppose that either $q > 256$ is a square, or $h \ge 3$ odd and $p \ge 29$. Then $\bar{\chi}(\mathrm{PG}(2,q)) = v - \tau_2 + 1$, and equality is reached only by trivial colorings.

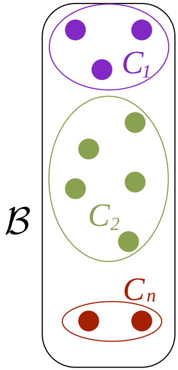
Remark: if $\tau_2(\mathrm{PG}(2,q)) < 8q/3$, $q > q(\tau_2)$, then $\bar{\chi} \lesssim v - \tau_2 + 10$.

$C_1, \ldots, C_n$: color classes of size at least two (only these are useful)

C_i colors the line ℓ iff $|\ell \cap C_i| \geq 2$.

All lines have to be colored, so $\mathcal{B} = \bigcup_{i=1}^{n} C_i$ is a double blocking set.

We use $v - |\mathcal{B}| + n$ colors.



To reach the trivial coloring, we must have $v - |\mathcal{B}| + n \geq v - \tau_2 + 1$, thus we need

$$n \geq |\mathcal{B}| - \tau_2 + 1$$

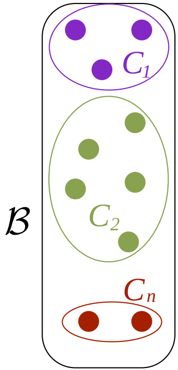
colors in $\mathcal{B}$. Also $n \leq |B|/2$, so $|B| \leq 2\tau_2 \leq 6q$.

$C_1, \ldots, C_n$: color classes of size at least two (only these are useful)

C_i colors the line ℓ iff $|\ell \cap C_i| \geq 2$.

All lines have to be colored, so
$\mathcal{B} = \bigcup_{i=1}^{n} C_i$ is a double blocking set.

We use $v - |\mathcal{B}| + n$ colors.

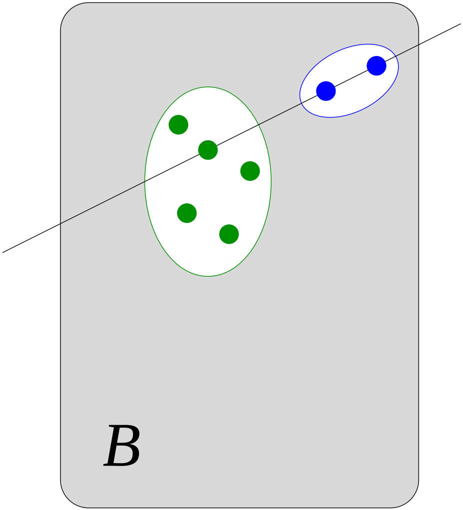


To reach the trivial coloring, we must have $v - |\mathcal{B}| + n \geq v - \tau_2 + 1$, thus we need

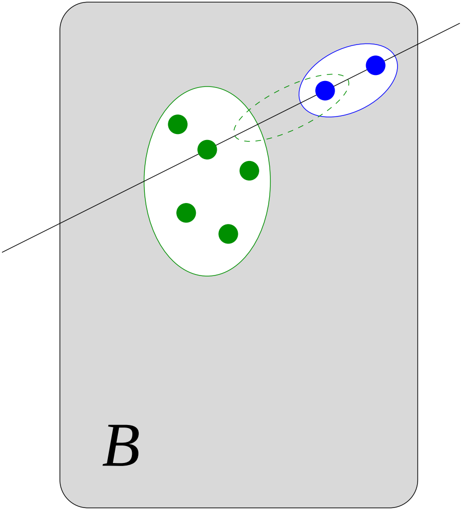
$$n \geq |\mathcal{B}| - \tau_2 + 1$$

colors in $\mathcal{B}$. Also $n \leq |B|/2$, so $|B| \leq 2\tau_2 \leq 6q$.

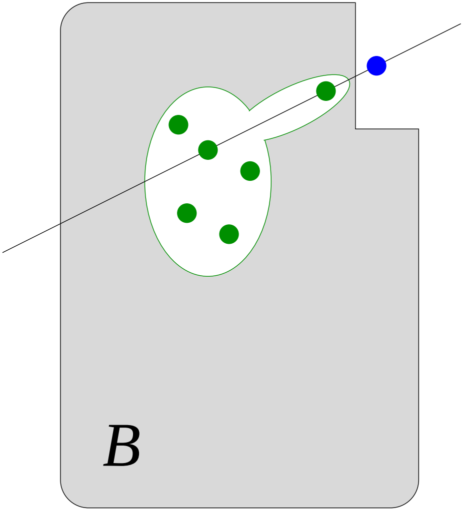
Eliminating color classes of size two



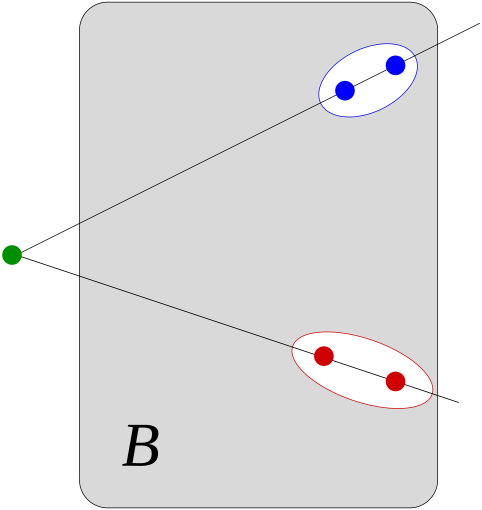
Eliminating color classes of size two



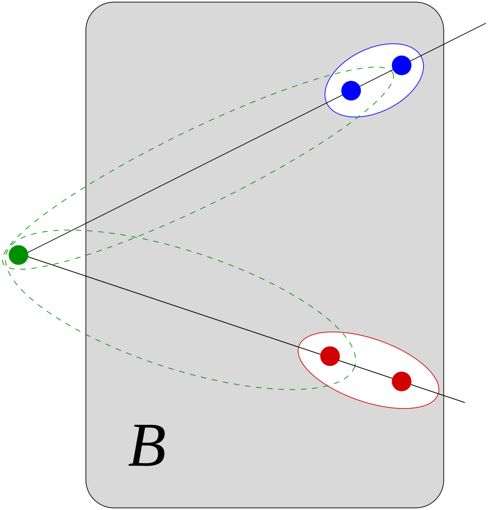
Eliminating color classes of size two



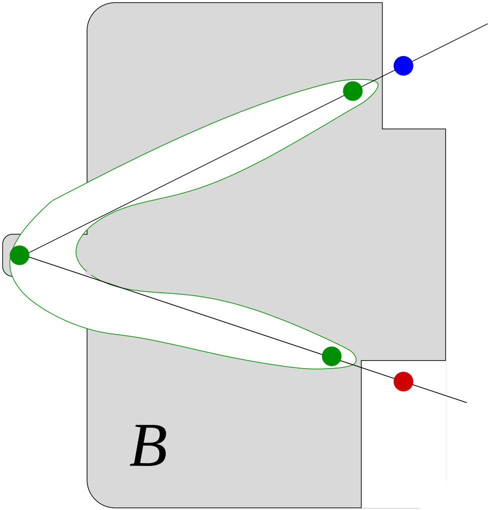
Eliminating color classes of size two



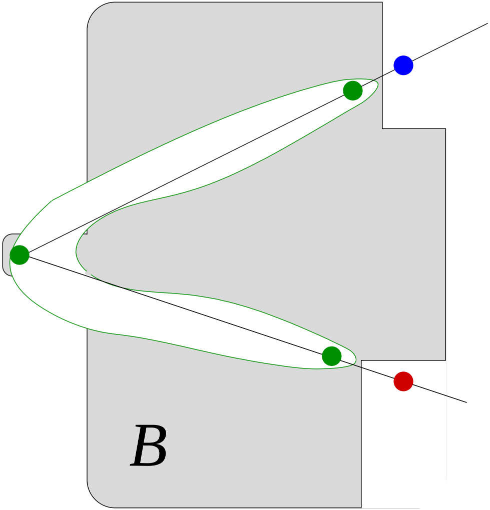
Eliminating color classes of size two



Eliminating color classes of size two



Eliminating color classes of size two



So there is at most one color class of size two.

$|\mathcal{B}| \gtrsim 3q - \varepsilon$

Recall that $\tau_2 \lesssim 2.5q$.

$L(C_i) :=$ the number of lines colored by C_i. Then $L(C_i) \leq \binom{|C_i|}{2}$.

By convexity, to satisfy

$$q^2 + q + 1 \leq \sum L(C_i) \leq \sum \binom{|C_i|}{2},$$

the best is to have one giant, and many dwarf color classes. But as

$$|\mathcal{B}| - \tau_2 + 1 \leq n \leq 1 + \frac{|\mathcal{B}| - \left|C_{\text{giant}}\right|}{3},$$

$|C_g iant| \leq 3\tau_2 - 2|B|$, too small.

$|\mathcal{B}| \gtrsim 3q - \varepsilon$

Recall that $\tau_2 \lesssim 2.5q$. Say, $\tau_2 \approx 2.5q$.

$L(C_i) :=$ the number of lines colored by C_i. Then $L(C_i) \leq \binom{|C_i|}{2}$.

By convexity, to satisfy

$$q^2 + q + 1 \leq \sum L(C_i) \leq \sum \binom{|C_i|}{2},$$

the best is to have one giant, and many dwarf color classes. But as

$$0.5q \lesssim |\mathcal{B}| - \tau_2 + 1 \leq n \leq 1 + \frac{|\mathcal{B}| - \left|C_{\text{giant}}\right|}{3},$$

$|C_g iant| \leq 3\tau_2 - 2|B|$, too small: $|C_{\text{giant}}| \lesssim 1.5q$.

$|\mathcal{B}| \gtrsim 3q - \varepsilon$

Recall that $\tau_2 \lesssim 2.5q$. Say, $\tau_2 \approx 2.5q$.

$L(C_i) :=$ the number of lines colored by C_i. Then $L(C_i) \le \binom{|C_i|}{2}$.

By convexity, to satisfy

$$q^2 + q + 1 \le \sum L(C_i) \le \sum \binom{|C_i|}{2},$$

the best is to have one giant, and many dwarf color classes. But as

$$0.5q \lesssim |\mathcal{B}| - \tau_2 + 1 \le n \le 1 + \frac{|\mathcal{B}| - \left|C_{\text{giant}}\right|}{3},$$

$|C_g iant| \le 3\tau_2 - 2|B|$, too small: $|C_{\text{giant}}| \lesssim 1.5q$.

However, if $\left|C_{\text{giant}}\right| \ge q + 2$, we use $L(C_i) \le \frac{(q+1)}{2}|C_i|$.

$\tau_2 + \varepsilon' \lesssim |\mathcal{B}| \lesssim 3q - \varepsilon$

Lemma

Let $\mathcal{B}$ be t-fold blocking set in $\mathrm{PG}(2,q)$, $|\mathcal{B}| = t(q+1)+k$, and $P \in \mathcal{B}$ be an essential point of $\mathcal{B}$. Then there are at least $(q+1-k-t)$ t-secants of $\mathcal{B}$ through P.

Corollary

Let $\mathcal{B}$ be a t-fold blocking set with $|\mathcal{B}| \le (t+1)q$ points. Then there is exactly one minimal t-fold blocking set in $\mathcal{B}$, namely the set of essential points.

Remark

Harrach has a recent result on the unique reducibility of weighted t-fold $(n-k)$-blocking sets in the projective space $\mathrm{PG}(n,q)$.

Lemma

Let $\mathcal{B}$ be t-fold blocking set in $\mathrm{PG}(2, q)$, $|\mathcal{B}| = t(q+1) + k$, and $P \in \mathcal{B}$ be an essential point of $\mathcal{B}$. Then there are at least $(q + 1 - k - t)$ t-secants of $\mathcal{B}$ through P.

Corollary

Let $\mathcal{B}$ be a t-fold blocking set with $|\mathcal{B}| \leq (t+1)q$ points. Then there is exactly one minimal t-fold blocking set in $\mathcal{B}$, namely the set of essential points.

Remark

Harrach has a recent result on the unique reducibility of weighted t-fold $(n-k)$-blocking sets in the projective space $\mathrm{PG}(n, q)$.

$\tau_2 + \varepsilon' \lesssim |\mathcal{B}| \lesssim 3q - \varepsilon$

Lemma

Let $\mathcal{B}$ be t-fold blocking set in $\mathrm{PG}(2,q)$, $|\mathcal{B}| = t(q+1)+k$, and $P \in \mathcal{B}$ be an essential point of $\mathcal{B}$. Then there are at least $(q+1-k-t)$ t-secants of $\mathcal{B}$ through P.

Corollary

Let $\mathcal{B}$ be a t-fold blocking set with $|\mathcal{B}| \leq (t+1)q$ points. Then there is exactly one minimal t-fold blocking set in $\mathcal{B}$, namely the set of essential points.

Remark

Harrach has a recent result on the unique reducibility of weighted t-fold $(n-k)$-blocking sets in the projective space $\mathrm{PG}(n,q)$.

Lemma

Let $\mathcal{B}$ be t-fold blocking set in $\mathrm{PG}(2,q)$, $|\mathcal{B}| = t(q+1)+k$, and $P \in \mathcal{B}$ be an essential point of $\mathcal{B}$. Then there are at least $(q+1-k-t)$ t-secants of $\mathcal{B}$ through P.

Corollary

Let $\mathcal{B}$ be a t-fold blocking set with $|\mathcal{B}| \leq (t+1)q$ points. Then there is exactly one minimal t-fold blocking set in $\mathcal{B}$, namely the set of essential points.

Remark

Harrach has a recent result on the unique reducibility of weighted t-fold $(n-k)$-blocking sets in the projective space $\mathrm{PG}(n,q)$.

Proof of the lemma

Let $P \in B$ essential, and suppose to the contrary that there are more than $k+t$ long secants through P. Let ℓ be t-secant, $P \notin \ell$.

$$R(M,B) = \prod_{i=1}^{t-1}(M-m_i)\prod_{i=1}^{tq+k}(Mx_i+B-y_i) = g(M)\prod_{i=1}^{tq+k}(Mx_i+B-y_i).$$

As B is a t-fold blocking set,

$$R(M,B) \quad = \quad \sum_{j=0}^{t}(M^q-M)^j(B^q -$$

$(B^q-B)^t g(M)F_0^*(M,B)+(M^q-M)h(M,b),$

where $\deg(F_0^*) \leq k$.
Then for any $m \notin \{m_1,\dots,m_{t-1}\}$,

$$|\{Y=mX+B\} \cap B| > t \iff (B^q-B)^{t+1} \mid R(m,B) \iff (B-b) \mid F_0^*(r$$

Proof of the lemma

Let $P = (x_1, y_1)$. More than $k + t$ long sec's on $P \Rightarrow$ more than k long sec's with $m \notin \{m_1, \ldots, m_{t-1}\}$.

So $Mx_1 + B - y_1 = 0$ and $F_0^*(M, B) = 0$ have more than k common points. Thus $(Mx_1 + B - y_1)$ is a factor of $F_0^*(M, B)$, thus the lines through P and a point of $\ell \setminus B$ are long secants. This gives a contradiction if P is essential.

Clear: if ℓ is a 2-secant to $\mathcal{B}$, then $\ell \cap \mathcal{B}$ is monochromatic.

Let $|\mathcal{B}| = 2(q+1) + k$. Then

Proposition

Every color class containing an essential point of $\mathcal{B}$ has at least $(q-k) \approx 3q - |\mathcal{B}|$ points.

$\mathcal{B} = \mathcal{B}^* \cup \mathcal{B}'$, where $\mathcal{B}^*$ is the set of essential points, $|\mathcal{B}^*| \geq \tau_2$.

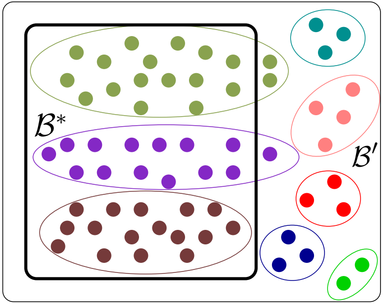
We have

$$|\mathcal{B}| - \tau_2 + 1 \leq n \leq \frac{|\mathcal{B}| - |\mathcal{B}^*|}{3} + \frac{|\mathcal{B}^*|}{q-k},$$

so

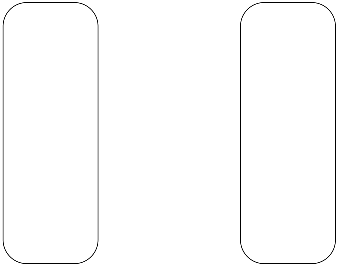
$$\frac{2}{3}(|\mathcal{B}| - \tau_2)(q-k) \leq \tau_2.$$

$\mathcal{B}$

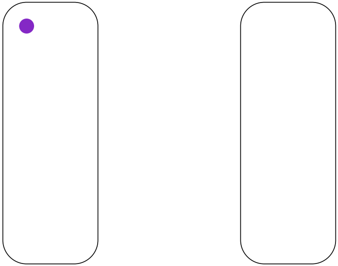


$|\mathcal{B}| \leq \tau_2 + \varepsilon$, $q > 256$ square (so $\tau_2 = 2(q + \sqrt{q} + 1)$)

Blokhuis, Storme, Szőnyi: $\mathcal{B}$ contains two disjoint Baer subplanes, $\mathcal{B}_1$ and $\mathcal{B}_2$. $\mathcal{B}^* = \mathcal{B}_1 \cup \mathcal{B}_2$ can not be monochromatic.

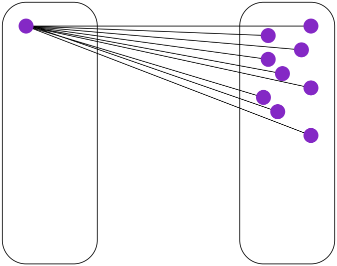


Blokhuis, Storme, Szőnyi: $\mathcal{B}$ contains two disjoint Baer subplanes, $\mathcal{B}_1$ and $\mathcal{B}_2$. $\mathcal{B}^* = \mathcal{B}_1 \cup \mathcal{B}_2$ can not be monochromatic.



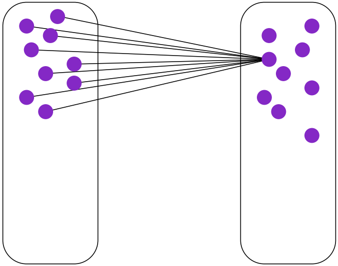
Let $P \in \mathcal{B}_1$ be purple.

Blokhuis, Storme, Szőnyi: $\mathcal{B}$ contains two disjoint Baer subplanes, $\mathcal{B}_1$ and $\mathcal{B}_2$. $\mathcal{B}^* = \mathcal{B}_1 \cup \mathcal{B}_2$ can not be monochromatic.



Let $P \in \mathcal{B}_1$ be purple. There are at least $(q - \sqrt{q} - \varepsilon - 1)$ 2-secants on P, so there are a lot of purple points in $\mathcal{B}_2$.

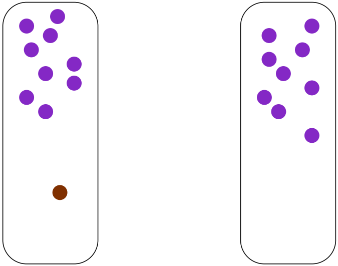
Blokhuis, Storme, Szőnyi: $\mathcal{B}$ contains two disjoint Baer subplanes, $\mathcal{B}_1$ and $\mathcal{B}_2$. $\mathcal{B}^* = \mathcal{B}_1 \cup \mathcal{B}_2$ can not be monochromatic.



Let $P \in \mathcal{B}_1$ be purple. There are at least $(q - \sqrt{q} - \varepsilon - 1)$ 2-secants on P, so there are a lot of purple points in $\mathcal{B}_2$.

The same from $\mathcal{B}_2$: we have at least $2(q - \sqrt{q} - \varepsilon - 1)$ purple points.

Blokhuis, Storme, Szőnyi: $\mathcal{B}$ contains two disjoint Baer subplanes, $\mathcal{B}_1$ and $\mathcal{B}_2$. $\mathcal{B}^* = \mathcal{B}_1 \cup \mathcal{B}_2$ can not be monochromatic.



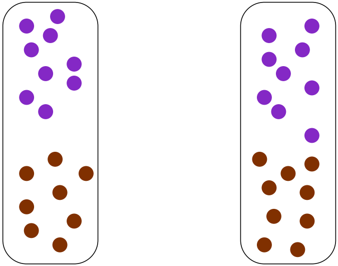
Let $P \in \mathcal{B}_1$ be purple. There are at least $(q - \sqrt{q} - \varepsilon - 1)$ 2-secants on P, so there are a lot of purple points in $\mathcal{B}_2$.

The same from $\mathcal{B}_2$: we have at least $2(q - \sqrt{q} - \varepsilon - 1)$ purple points.

If we have brown points as well:

$|\mathcal{B}| \leq \tau_2 + \varepsilon$, $q > 256$ square (so $\tau_2 = 2(q + \sqrt{q} + 1)$)

Blokhuis, Storme, Szőnyi: $\mathcal{B}$ contains two disjoint Baer subplanes, $\mathcal{B}_1$ and $\mathcal{B}_2$. $\mathcal{B}^* = \mathcal{B}_1 \cup \mathcal{B}_2$ can not be monochromatic.



Let $P \in \mathcal{B}_1$ be purple. There are at least $(q - \sqrt{q} - \varepsilon - 1)$ 2-secants on P, so there are a lot of purple points in $\mathcal{B}_2$.

The same from $\mathcal{B}_2$: we have at least $2(q - \sqrt{q} - \varepsilon - 1)$ purple points.

If we have brown points as well: $|\mathcal{B}| \geq 4(q - \sqrt{q} - \varepsilon - 1)$ $\lightning$

By melting color classes, we may assume $n = 2$, $\mathcal{B}^* = \mathcal{B}^r \cup \mathcal{B}^g$, and let $|\mathcal{B}| = |\mathcal{B}^*| = 2(q+1) + k < 2.5q$.

Theorem (Blokhuis, Lovász, Storme, Szőnyi)

Let B be a minimal t-fold blocking set in $\mathrm{PG}(2, q)$, $q = p^h$, $h \geq 1$, $|B| < tq + (q+3)/2$. Then every line intersects B in $t \pmod{p}$ points.

For a line ℓ, let

$$\begin{aligned} n_\ell^r &= |\mathcal{B}^r \cap \ell|, \\ n_\ell^g &= |\mathcal{B}^g \cap \ell|, \\ n_\ell &= n_\ell^r + n_\ell^g = |\mathcal{B} \cap \ell|. \end{aligned}$$

Define the set of red, green and balanced lines as

$$\begin{aligned} \mathcal{L}^r &= \{\ell \in \mathcal{L} \colon n_\ell^r > n_\ell^g\}, \\ \mathcal{L}^g &= \{\ell \in \mathcal{L} \colon n_\ell^g > n_\ell^r\}, \\ \mathcal{L}^= &= \{\ell \in \mathcal{L} \colon n_\ell^r = n_\ell^g\}. \end{aligned}$$

Using double counting, we get

$$\sum_{\ell \in \mathcal{L}} n_\ell = |\mathcal{B}^*|(q+1), \text{ hence}$$

$$\sum_{\ell \in \mathcal{L} \colon n_\ell > 2} n_\ell \geq \sum_{\ell \in \mathcal{L}} (n_\ell - 2) = |\mathcal{B}^*|(q+1) - 2(q^2+q+1) \gtrsim kq.$$

On the other hand, $\displaystyle\sum_{\ell\in\mathcal{L}:\ n_\ell>2} n_\ell =$

$$\sum_{\ell\in\mathcal{L}^r:\ n_\ell>2} (n_\ell^r + n_\ell^g) + \sum_{\ell\in\mathcal{L}^g:\ n_\ell>2} (n_\ell^r + n_\ell^g) + \sum_{\ell\in\mathcal{L}^=:\ n_\ell>2} (n_\ell^r + n_\ell^g) \leq$$

$$\sum_{\ell\in\mathcal{L}^r:\ n_\ell>2} 2n_\ell^r + \sum_{\ell\in\mathcal{L}^g:\ n_\ell>2} 2n_\ell^g + \sum_{\ell\in\mathcal{L}^=:\ n_\ell>2} 2n_\ell^r \leq 4\cdot \sum_{\ell\in\mathcal{L}^r\cup\mathcal{L}^=:\ n_\ell>2} n_\ell^r.$$

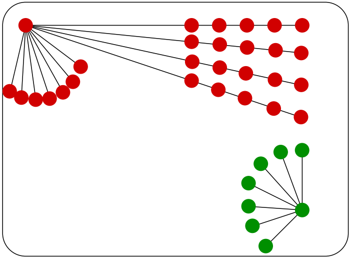
Recall $|\mathcal{B}_r| \leq |\mathcal{B}| - |\mathcal{B}^g| \leq 2q + k - (q-k) = q + 2k < 2q.$

Thus for the average number of long red secants through a red point,

$$\frac{\sum_{\ell\in\mathcal{L}^r\cup\mathcal{L}^=:\ n_\ell>2} n_\ell^r}{\mathcal{B}^r} \geq \frac{kq}{4|\mathcal{B}^r|} \geq \frac{k}{8}.$$

So we see:

$\frac{kp}{16}$ red points on the red long secants through P,
$q-k$ red points on the red two-secants through P,
and $q-k$ green points.



Thus $2q + k \gtrsim |\mathcal{B}| \geq 2q - 2k + \frac{kp}{16}$ ↯

Two disjoint blocking sets

Let $q = p^h$, $h \geq 3$ odd, p not necessarily prime, p odd. Let $m = (q-1)/(p-1) = p^{h-1} + p^{h-2} + \ldots + 1$. Note that m is odd.

Let $f(x) = a(x^p + x)$, $a \in \mathrm{GF}(q)^*$. Then f is $\mathrm{GF}(p)$-linear, and determines the directions $\left\{ \frac{f(x)-f(y)}{(x-y)} : x \neq y \right\}$ $=\{f(x)/x : x \neq 0\}=$ $\{(1 : f(x)/x : 0) : x \neq 0\}=$ $\{(x : f(x) : 0) : x \neq 0\}$. Thus

$$B_1 = \underbrace{\{(x : f(x) : 1)\}}_{A_1} \cup \underbrace{\{(x : f(x) : 0)\}_{x \neq 0}}_{l_1}$$

is a blocking set of Rédei type. Similarly, for $g(x) = x^p$,

$$B_2 = \underbrace{\{(y : 1 : g(y))\}}_{A_2} \cup \underbrace{\{(y : 0 : g(y))\}_{y \neq 0}}_{l_2}$$

is also a blocking set.

Two disjoint blocking sets

$$B_1 = \underbrace{\{(x : f(x) : 1)\}}_{A_1} \cup \underbrace{\{(x : f(x) : 0)\}_{x \neq 0}}_{l_1}$$

$$B_2 = \underbrace{\{(y : 1 : g(y))\}}_{A_2} \cup \underbrace{\{(y : 0 : g(y))\}_{y \neq 0}}_{l_2}$$

$f(x) = 0$ iff $x^p + x = x(x^{p-1} + 1) = 0$. As

$$-1 = (-1)^m \neq x^{(p-1)m} = x^{q-1} = 1,$$

$f(x) = 0$ iff $x = 0$. Also $g(x) = 0$ iff $x = 0$.

$l_2 \cap B_1$ is empty, as $(0 : 0 : 1) \notin l_2$.

If $(x : f(x) : 0) \equiv (y : 1 : g(y)) \in l_1 \cap A_2$, then $g(y) = 0$, hence $y = 0$ and $x = 0$, a contradiction. So $l_1 \cap A_2 = \emptyset$.

Two disjoint blocking sets

$$B_1 = \underbrace{\{(x : f(x) : 1)\}}_{A_1} \cup \underbrace{\{(x : f(x) : 0)\}_{x \neq 0}}_{I_1}$$

$$B_2 = \underbrace{\{(y : 1 : g(y))\}}_{A_2} \cup \underbrace{\{(y : 0 : g(y))\}_{y \neq 0}}_{I_2}$$

Now we need $A_1 \cap A_2 = \emptyset$.

$(y : 1 : g(y)) \equiv (x : f(x) : 1)$ $(x \neq 0)$ iff

$(y; 1; g(y)) = (x/f(x); 1; 1/f(x))$, in which case

$1/f(x) = g(x/f(x)) = g(x)/g(f(x))$.

Thus we need that $g(x) = g(f(x))/f(x) = f(x)^{p-1}$ that is, $x^p = (a(x^p + x))^{p-1} = a^{p-1}x^{p-1}(x^{p-1} + 1)^{p-1}$ has no solution in $\mathrm{GF}(q)^*$.

Two disjoint blocking sets

Equivalent form:

$$\frac{1}{a^{p-1}} = \frac{(x^{p-1}+1)^{p-1}}{x} = (x^{p-1}+1)^{p-1}x^{q-2} =: h(x)$$

should have no solutions $x \in \mathrm{GF}(q)^*$.

Let $D = \{x^m : x \in \mathrm{GF}(q)^*\} = \{x^{(p-1)} : x \in \mathrm{GF}(q)^*\}$. Then $1/a^{p-1} \in D$.

Note that $h(x) \in D \iff x \in D$.

So to find an element a such that $1/a^{(p-1)}$ is not in the range of h, we need that $h|_D : D \to D$ does not permute D.

Permutation polynomials

Theorem (Hermite-Dickson)

Let $f \in \mathrm{GF}(q)[X]$, $q = p^h$, p prime. Then f permutes $\mathrm{GF}(q)$ iff the following conditions hold:

- *f has exactly one root in $\mathrm{GF}(q)$;*
- *for each integer t, $1 \leq t \leq q-2$ and $p \not| t$, $f(X)^t \pmod{X^q - X}$ has degree at most $q-2$.*

A variation for multiplicative subgroups of $\mathrm{GF}(q)^*$:

Theorem

Suppose $d \mid q-1$, and let $D = \{x^d : x \in \mathrm{GF}(q)^*\}$ be the set of nonzero d^{th} powers, $m = |D| = (q-1)/d$. Assume that $g \in \mathrm{GF}(q)[X]$ maps D into D. Then $g|_D$ is a permutation of D if and only if the constant term of $g(x)^t \pmod{x^m - 1}$ is zero for all $1 \leq t \leq m-1$, $p \not| t$.

Two disjoint blocking sets

Recall that $h(X) = (X^{p-1}+1)^{p-1}X^{q-2}$. Let $t = p-1$, that is, consider

$$h^{p-1}(X) = \sum_{k=0}^{(p-1)^2} \binom{(p-1)^2}{k} X^{k(p-1)+(p-1)(q-2)} \pmod{X^m - 1}.$$

Since $k(p-1)+(p-1)(q-2) \equiv (k-1)(p-1) \pmod{m}$, the exponents reduced to zero have $k = 1 + \ell\frac{m}{(m,p-1)}$. Let r be the characteristic of the field $\mathrm{GF}(q)$. As $\binom{(p-1)^2}{1} \equiv 1 \pmod{r}$, it is enough to show that $\binom{(p-1)^2}{k} \equiv 0 \pmod{r}$ for the other possible values of k.

Suppose $h \geq 5$. Then $m/(m,p-1) > m/p > p^{h-2} > p^2$, thus by $k \leq (p-1)^2$, $\ell \geq 1$ does not occur at all. The case $h = 3$ can also be done.

Thank you for your attention!