The use of blocking sets in Galois geometries and related research areas

Leo Storme

Ghent University
Dept. of Mathematics
Krijgslaan 281 - S22
9000 Ghent
Belgium

Bangalore, August 31, 2010

Outline

1. Galois geometries
   - Finite fields
   - The projective plane PG$(2, q)$
   - The 3-space PG$(3, q)$
2. Blocking sets
3. Maximal partial spreads of PG$(3, q)$
4. Applications in coding theory
   - Linear codes
   - Griesmer bound and minihypers
   - Extendability results and blocking sets
5. Applications in cryptography

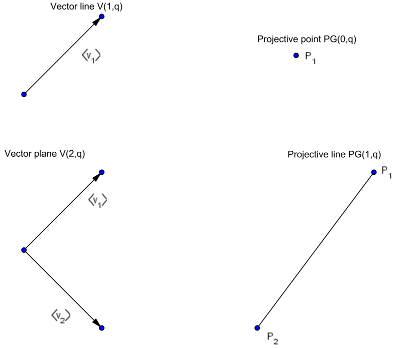
OUTLINE

UNIVERSITEIT GENT

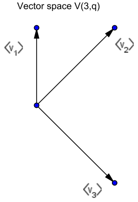
FINITE FIELDS

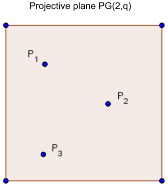
- q = prime number.
  - **Prime fields** $\mathbb{F}_q = \{0, 1, \ldots, q-1\} \pmod{q}$.
  - Binary field $\mathbb{F}_2 = \{0, 1\}$.
  - Ternary field $\mathbb{F}_3 = \{0, 1, 2\} = \{-1, 0, 1\}$.
- **Finite fields** $\mathbb{F}_q$: q prime power.

From $V(3, q)$ to PG$(2, q)$

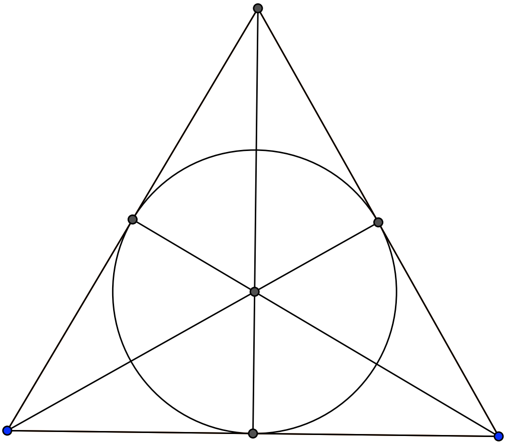


From $V(3, q)$ to PG$(2, q)$

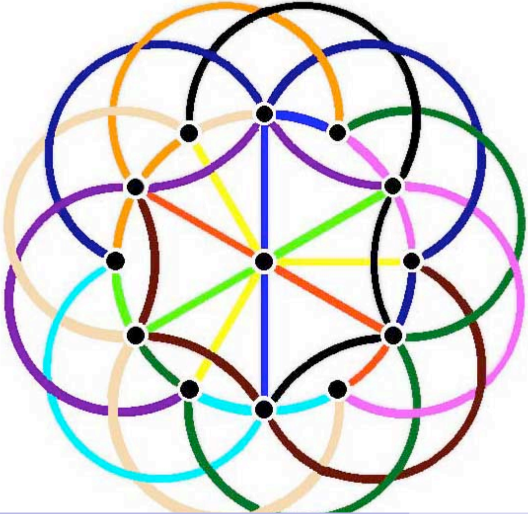




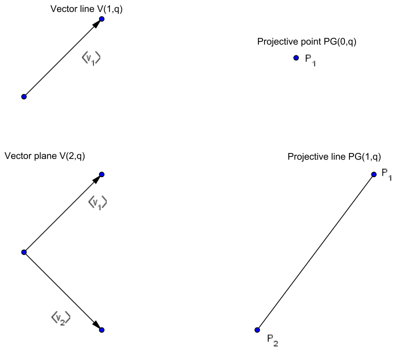
The Fano plane PG(2, 2)



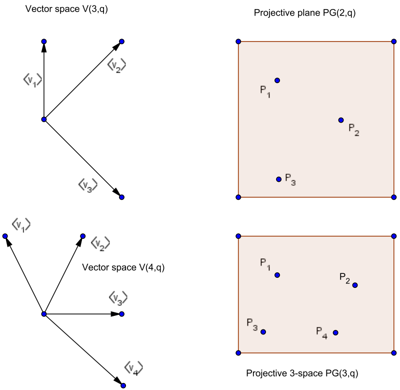
THE PLANE PG(2, 3)



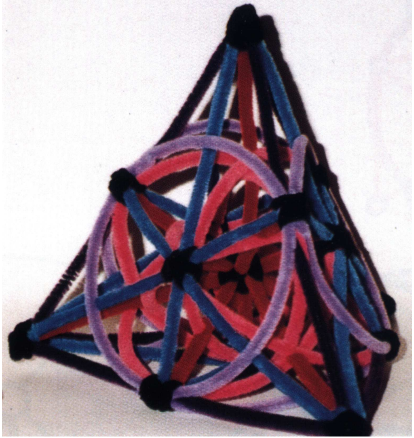
From $V(4, q)$ to PG(3, q)



From $V(4, q)$ to PG$(3, q)$



PG(3, 2)



From $V(n+1, q)$ to PG(n, q)

1. From $V(1, q)$ to PG$(0, q)$ (projective point),
2. From $V(2, q)$ to PG$(1, q)$ (projective line),
3. ...
4. From $V(i+1, q)$ to PG(i, q) (i-dimensional projective subspace),
5. ...
6. From $V(n, q)$ to PG$(n-1, q)$ ($(n-1)$-dimensional subspace = hyperplane),
7. From $V(n+1, q)$ to PG(n, q) (n-dimensional space).

OUTLINE

DEFINITION AND EXAMPLE

DEFINITION

Blocking set B in PG$(2, q)$ is set of points, intersecting every line in at least one point.

EXAMPLE

Line L in PG$(2, q)$.

DEFINITION

DEFINITION

(1) Point r of blocking set B in PG$(2, q)$ is *essential* if $B \setminus \{r\}$ is no longer blocking set.

DEFINITION

Blocking set B is *minimal* if and only if all of its points are essential.

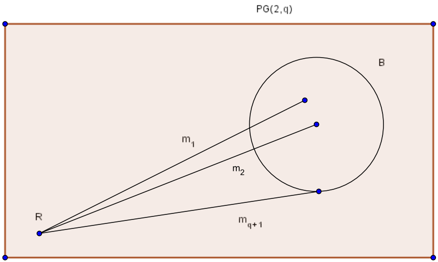
EXAMPLE

Line L of PG$(2, q)$ is minimal blocking set B of size $q + 1$.

Bose-Burton theorem

Theorem

For every blocking set B in $PG(2, q)$, $|B| \geq q + 1$ and $|B| = q + 1$ if and only if B is equal to line L.



NON-TRIVIAL BLOCKING SET IN PG$(2, q)$

DEFINITION

Non-trivial blocking set B in PG$(2, q)$ does not contain a line.

$q + r(q) + 1$ = size of smallest non-trivial blocking set in PG$(2, q)$.

- (Blokhuis) $r(q) = (q + 1)/2$ for $q > 2$ prime,
- (Bruen) $r(q) = \sqrt{q}$ for q square,
- (Blokhuis) $r(q) = q^{2/3}$ for q cube power.

UNIVERSITEIT GENT

Baer subplane in PG$(2, q)$, q square

- *Baer subplane* in PG$(2, q)$, q square, is subplane PG$(2, \sqrt{q})$.
- Baer subplane in PG$(2, q)$, q square, is minimal non-trivial blocking set in PG$(2, q)$, q square, of size $q + \sqrt{q} + 1$.

Theorem

(1) (Bruen) Smallest non-trivial blocking sets in PG$(2, q)$, q square, have size $q + \sqrt{q} + 1$, and are equal to Baer subplanes PG$(2, \sqrt{q})$.
(2) (Szőnyi) Every non-trivial blocking set B in PG$(2, q)$, $q = p^2$, p prime, of size $|B| < 3(q + 1)/2$, contains Baer subplane PG$(2, \sqrt{q})$.

General blocking sets

Definition

Blocking set B in $PG(n, q)$ with respect to k-subspaces is set of points, intersecting every k-subspace in at least one point.

Example

$(n-k)$-dimensional subspace PG$(n-k, q)$ in PG(n, q).

Bose-Burton theorem

Theorem (Bose and Burton)

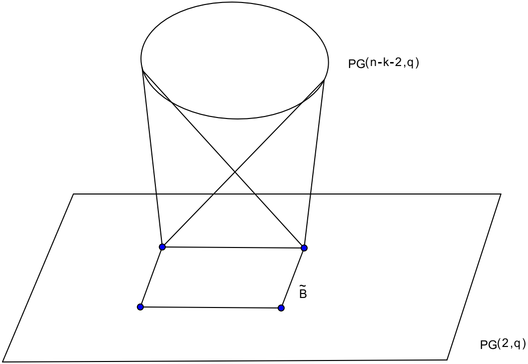
For every blocking set B in $PG(n, q)$ *with respect to* k*-subspaces,* $|B| \geq |PG(n-k, q)|$ *and* $|B| = |PG(n-k, q)|$ *if and only if B is equal to* $(n-k)$*-dimensional subspace* $PG(n-k, q)$.

BEUTELSPACHER-HEIM THEOREM

THEOREM (BEUTELSPACHER AND HEIM)

For non-trivial blocking set B in PG(n, q) with respect to k-subspaces,
$|B| \geq q^{n-k} + r(q)q^{n-k-1} + q^{n-k-1} + q^{n-k-2} + \cdots + q + 1$ *and*
$|B| = q^{n-k} + r(q)q^{n-k-1} + q^{n-k-1} + q^{n-k-2} + \cdots + q + 1$ *if and only if B is equal to cone with $(n-k-2)$-dimensional vertex and base minimal non-trivial blocking set of size $q + r(q) + 1$ in plane skew to vertex.*

BEUTELSPACHER-HEIM THEOREM



OUTLINE

UNIVERSITEIT GENT

DEFINITIONS

- *Spread* $\mathcal{S}$ of PG$(3, q)$ = set of $q^2 + 1$ lines of PG$(3, q)$ partitioning point set of PG$(3, q)$.
- *Partial spread* $\mathcal{S}$ of PG$(3, q)$ = set of pairwise disjoint lines of PG$(3, q)$.
- Partial spread $\mathcal{S}$ of PG$(3, q)$ is called *maximal* when not contained in larger partial spread of PG$(3, q)$.
- Partial spread $\mathcal{S}$ of size $q^2 + 1 - \delta$ has *deficiency* δ.

DEFINITIONS

- *Poor plane*: does not contain line of partial spread $\mathcal{S}$.
- *Hole*: point of PG$(3, q)$ not on line of partial spread $\mathcal{S}$.
- Poor plane has $q + \delta$ holes if $\mathcal{S}$ has deficiency δ.

Link between maximal partial spreads and blocking sets

Theorem

Let $\mathcal{S}$ be maximal partial spread of deficiency $\delta > 0$, then set of holes in poor plane is non-trivial blocking set of size $q + \delta$.

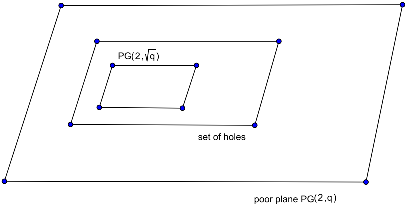
Application for q square

Theorem (Szőnyi)

Every non-trivial blocking set B in $PG(2, q)$, $q = p^2$, p prime, of size $|B| < 3(q+1)/2$, contains Baer subplane $PG(2, \sqrt{q})$.

Consequence: For maximal partial spread $\mathcal{S}$ of deficiency δ, $\delta \leq (q+1)/2$, set of holes in poor plane contains Baer subplane of holes.

APPLICATION FOR q SQUARE



APPLICATION FOR q SQUARE

Question: Where do all these Baer subplanes of holes arise from?
Logical guess: They arise from Baer subgeometries PG$(3, \sqrt{q})$ completely consisting of holes.

Result on maximal partial spreads

Theorem (Metsch and Storme)

Let $q = p^2$, $p > 2$ prime, let $\delta \leq (q+1)/2$. If $\mathcal{S}$ is maximal partial spread of size $q^2 + 1 - \delta$, then

A) $\delta = s(\sqrt{q} + 1)$ *for some integer* $s \geq 2$,

B) *set of holes of* $PG(3, q)$ *is union of* s *pairwise disjoint Baer subgeometries* $PG(3, \sqrt{q})$.

Outline

UNIVERSITEIT GENT

Linear codes

- **Linear** $[n, k, d]$**-code** C **over** $\mathbb{F}_q$ is:
  - k-dimensional subspace of $V(n, q)$,
  - *minimum distance* d = minimal number of positions in which two distinct codewords differ.

Linear codes

- **Generator matrix of $[n, k, d]$-code C**

$$G = (g_1 \cdots g_n)$$

  - $G = (k \times n)$ matrix of rank k,
  - rows of G form basis of C,
  - codeword of C = linear combination of rows of G.

REMARK

Remark: For linear $[n, k, d]$-code C, n, k, d do not change when column g_i in generator matrix

$$G = (g_1 \cdots g_n)$$

is replaced by non-zero scalar multiple.
Consequence: Interpret columns g_i as projective points.

Griesmer bound and minihypers

Question: Given

- dimension k,
- minimum distance d,

find minimal length n of $[n, k, d]$-code over $\mathbb{F}_q$.
Result: Griesmer (lower) bound

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil = g_q(k, d).$$

MINIHYPERS AND GRIESMER BOUND

Equivalence: (Hamada and Helleseth)

Griesmer (lower) bound
equivalent with
minihypers in finite projective spaces

Definition

Definition

$\{f, m; k-1, q\}$-minihyper F is:

- set of f points in PG$(k-1, q)$,
- F intersects every $(k-2)$-dimensional space in at least m points.

(m-fold blocking set of size f with respect to hyperplanes of PG$(k-1, q)$)

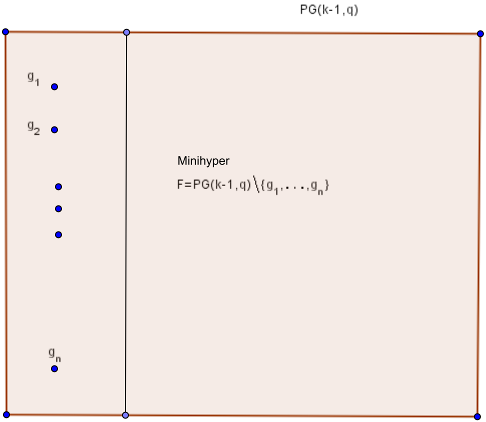
MINIHYPERS AND GRIESMER BOUND

- Let C = $[g_q(k, d), k, d]$-code over $\mathbb{F}_q$.
- If generator matrix

$$G = (g_1 \cdots g_n),$$

minihyper = PG$(k-1, q) \setminus \{g_1, \ldots, g_n\}$.

Minihypers and Griesmer bound



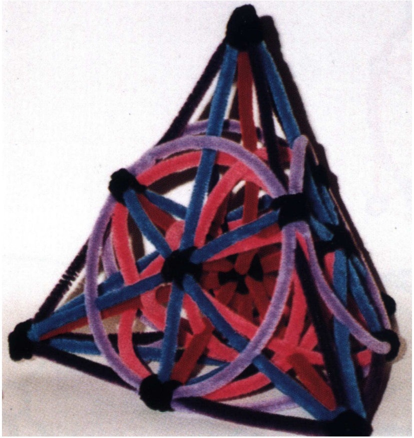
Example

Example: Griesmer [8,4,4]-code over $\mathbb{F}_2$

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

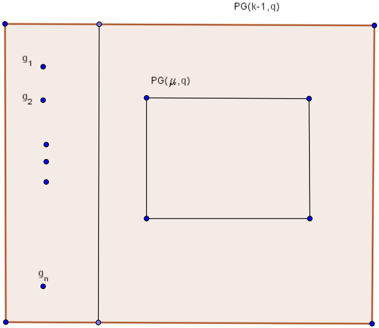
minihyper = PG$(3,2)\setminus$ {columns of G} = plane ($X_0 = 0$).

Corresponding minihyper



Other examples

Example 1. Subspace PG(μ, q) in PG($k-1, q$) = minihyper of $[n = (q^k - q^{\mu+1})/(q-1), k, q^{k-1} - q^{\mu}]$-code (McDonald code).



BOSE-BURTON THEOREM

THEOREM (BOSE-BURTON)

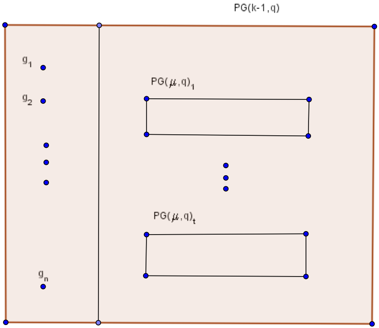
A minihyper consisting of $|PG(\mu, q)|$ points intersecting every hyperplane in at least $|PG(\mu - 1, q)|$ points is equal to a μ-dimensional space $PG(\mu, q)$.

RAJ CHANDRA BOSE

R.C. Bose and R.C. Burton, A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the McDonald codes. *J. Combin. Theory*, 1:96-104, 1966.

Other examples

Example 2. $t < q$ pairwise disjoint subspaces PG$(\mu, q)_i$, $i = 1, \ldots, t$, in PG$(k-1, q)$ = minihyper of $[n = (q^k - 1)/(q-1) - t(q^{\mu+1} - 1)/(q-1), k, q^{k-1} - tq^{\mu}]$-code.



CHARACTERIZATION RESULT

THEOREM (GOVAERTS AND STORME)

For q odd prime and $1 \leq t \leq (q+1)/2$*,*
$[n = (q^k - 1)/(q-1) - t(q^{\mu+1} - 1)/(q-1), k, q^{k-1} - tq^{\mu}]$*-code*
C: minihyper is union of t pairwise disjoint PG(μ, q)*.*

OTHER CHARACTERIZATION RESULTS

- Minihypers involving subspaces of different dimension:
  - Hamada, Helleseth, and Maekawa: ϵ_0 points, ϵ_1 lines, $\ldots$, ϵ_{k-2} PG$(k-2, q)$, where $\sum_{i=0}^{k-2} \epsilon_i < \sqrt{q} + 1$,
  - De Beule, Metsch, and Storme: improvements to Hamada, Helleseth, and Maekawa.
    For q prime, $\sum_{i=0}^{k-2} \epsilon_i < (q+1)/2$.
- Minihypers involving subgeometries over $\mathbb{F}_{\sqrt{q}}$ in PG$(k-1, q)$, q square:
  - Govaerts and Storme,
  - De Beule, Hallez, Metsch, and Storme.

Well-known extendability result

Theorem

Every linear binary $[n, k, d]$-code C, d odd, is extendable to linear binary $[n+1, k, d+1]$-code.

Hill-Lizak result

Theorem (Hill and Lizak)

Let C be linear $[n, k, d]$-code over $\mathbb{F}_q$, with $\gcd(d, q) = 1$ and with all weights congruent to 0 or $d \pmod q$. Then C can be extended to $[n+1, k, d+1]$-code all of whose weights are congruent to 0 or $d+1 \pmod q$.

Proof: Subcode of all codewords of weight congruent to 0 $\pmod q$ is linear subcode C_0 of dimension $k-1$. If G_0 defines C_0 and

$$G = \left(\frac{x}{G_0} \right),$$

then

HILL-LIZAK RESULT

$$\hat{G} = \left(\begin{array}{c|c} x & 1 \\ \hline & 0 \\ G_0 & \vdots \\ & 0 \end{array} \right)$$

defines C. $\square$

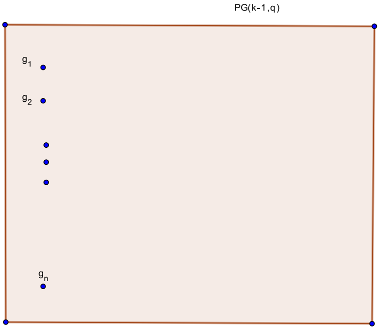
Geometrical counterpart of Landjev

- Let $C = [n, k, d]$-code over $\mathbb{F}_q$.
- If generator matrix

$$G = (g_1 \cdots g_n),$$

then $\{g_1, \ldots, g_n\} = (n, w = n - d; k - 1, q)$-multiarc.

Linear codes and multiarcs



Geometrical counterpart of Landjev

- C linear $[n, k, d]$-code over $\mathbb{F}_q$, $\gcd(d, q) = 1$ and with all weights congruent to 0 or $d \pmod q$. Then C can be extended to $[n+1, k, d+1]$-code all of whose weights are congruent to 0 or $d+1 \pmod q$.
- K =$(n, w; k-1, q)$-multiarc with $\gcd(n-w, q) = 1$ and intersection size of K with all hyperplanes congruent to n or $w \pmod q$. Then K can be extended to $(n+1, w; k-1, q)$-multiarc.

Geometrical counterpart of Landjev

Proof: Hyperplanes H containing $n \pmod q$ points of K form dual blocking set $\tilde{B}$ with respect to codimension 2 subspaces of PG$(k-1, q)$. Also

$$\tilde{B} = \frac{q^{k-1}-1}{q-1}.$$

By dual of Bose-Burton, $\tilde{B}$ consists of all hyperplanes through particular point P.
This point P extends K to $(n+1, w; k-1, q)$-multiarc. $\square$

Improved results

Theorem (Landjev and Rousseva)

Let $\mathcal{K}$ be $(n, w; k-1, q)$-arc, $q = p^s$, with spectrum $(a_i)_{i \geq 0}$. Let $w \not\equiv n \pmod q$ and

$$\sum_{i \not\equiv w \pmod q} a_i < q^{k-2} + q^{k-3} + \cdots + 1 + q^{k-3} \cdot r(q), \qquad (1)$$

where $q + r(q) + 1$ is minimal size of non-trivial blocking set of $PG(2, q)$. Then $\mathcal{K}$ is extendable to $(n+1, w; k-1, q)$-arc.

Beutelspacher-Heim theorem

Theorem (Beutelspacher and Heim)

For non-trivial blocking set B in $PG(n, q)$ with respect to k-subspaces,
$|B| \geq q^{n-k} + r(q)q^{n-k-1} + q^{n-k-1} + q^{n-k-2} + \cdots + q + 1$ *and*
$|B| = q^{n-k} + r(q)q^{n-k-1} + q^{n-k-1} + q^{n-k-2} + \cdots + q + 1$ *if and only if B is equal to cone with $(n - k - 2)$-dimensional vertex and base minimal non-trivial blocking set of size $q + r(q) + 1$ in plane skew to vertex.*

IMPROVED RESULTS

THEOREM

Let C be non-extendable $[n, k, d]$-code over $\mathbb{F}_q$, $q = p^s$, with $\gcd(d, q) = 1$. If $(A_i)_{i \geq 0}$ is the spectrum of C, then $\sum_{i \not\equiv 0,d \pmod{q}} A_i \geq q^{k-3} \cdot r(q)$, where $q + r(q) + 1$ is minimal size of non-trivial blocking set of $PG(2, q)$.

OUTLINE

1. GALOIS GEOMETRIES
   - Finite fields
   - The projective plane PG$(2, q)$
   - The 3-space PG$(3, q)$
2. BLOCKING SETS
3. MAXIMAL PARTIAL SPREADS OF PG$(3, q)$
4. APPLICATIONS IN CODING THEORY
   - Linear codes
   - Griesmer bound and minihypers
   - Extendability results and blocking sets
5. APPLICATIONS IN CRYPTOGRAPHY

CRYPTOGRAPHY

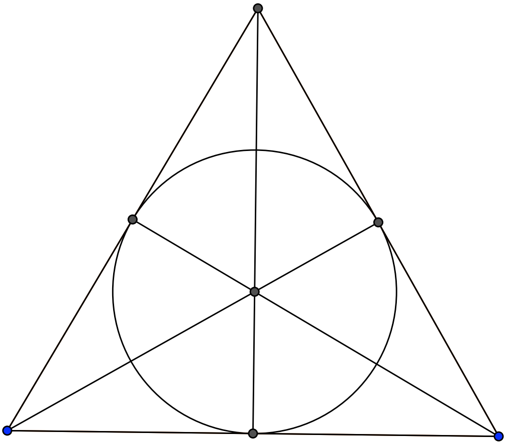
- Transmitter *encrypts* message in secret message.
- Receiver *decrypts* secret message in original message.

APPLICATION IN PAY TELEVISION

(Korjik, Ivkov, Merinovich, Barg, and van Tilborg)

- *subscribers* = points of PG$(2, q)$,
- *codes* = lines of PG$(2, q)$,
- subscriber quits: codes of lines become invalid,
- new issue of codes: only necessary when codes of all lines through subscriber become invalid.

THE FANO PLANE PG$(2, 2)$



Thank you very much for your attention!