NEW RESULTS ON GRIESMER CODES AND ARCS

Assia Rousseva
Sofia University

Ivan Landjev
New Bulgarian University

– ALCOMA 2015, Kloster Banz, 15.-20.03.2015 –

1. Linear Codes over Finite Fields

◇ **Linear** $[n, k]_q$ **code**: $C < \mathbb{F}_q^n$, $\dim C = k$

◇ $[n, k, d]_q$-**code**: $d = \min\{d(\boldsymbol{u}, \boldsymbol{v}) \mid \boldsymbol{u}, \boldsymbol{v} \in C, \boldsymbol{u} \neq \boldsymbol{v}\}$.

- n - the **length** of C;

- k - the **dimension** of C;

- d - the **minimum distance** of C.

◇ A_i – number of codewords of (Hamming) weight i

◇ $(A_i)_{i \geq 0}$ – the **spectrum** of C

The Main Problem in Coding Theory.

Optimize one of the parameters n, k, d, given the other two.

$n_q(k,d)$ - minimal length of a linear code over $\mathbb{F}_q$ of dimension k and minimum distance d;

$K_q(n,d)$ - maximal dimension of a linear code over $\mathbb{F}_q$ of length n and minimum distance d;

$D_q(n,k)$ - maximal minimum distance of a linear code over $\mathbb{F}_q$ of length n and dimension k.

optimality with respect to $n \Longrightarrow$ optimality with respect to k and d

◇ Griesmer bound: Let $\mathcal{C}$ be an $[n,k,d]_q$-code. Then

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

Theorem. Given the integer k and the prime power q, Griesmer $[g_q(k,d),k,d]_q$-codes exist for all sufficiently large d.

The problem of finding the exact value of $n_q(k,d)$ is solved for

- $q=2$: $k \leq 8$ for all d;
- $q=3$: $k \leq 5$ for all d;
- $q=4$: $k \leq 4$ for all d;
- $q=5,7,8,9$: $k \leq 3$ for all d;
- $q=5$: $k=4$ – four values of d for which $n_5(4,d)$ is not known.

http://www.mi.s.osakafu-u.ac.jp/ maruta/griesmer.htm

The Open Cases for $q = 5$, $k = 4$

d	$g_5(4,d)$	$n_5(4,d)$	$\mathcal{K}$	$\mathcal{K}\vert_H$
81	103	103–104	$(103,22)$	$(22,5)$-arc
82	104	104–105	$(104,22)$	in $\mathrm{PG}(2,5)$
161	203	203–204	$(203,42)$	$(42,9)$-arc
162	204	204–205	$(204,42)$	in $\mathrm{PG}(2,5)$

2. Divisible and Quasidivisible Arcs

◇ A multiset in $\mathrm{PG}(k-1,q)$ is a mapping

$$\mathcal{K}:\left\{\begin{array}{ccc}\mathcal{P} & \rightarrow & \mathbb{N}_0,\\ P & \rightarrow & \mathcal{K}(P).\end{array}\right.$$

◇ $\mathcal{K}(P)$ – multiplicity of the point P.

◇ $\mathcal{Q}\subset\mathcal{P}$: $\mathcal{K}(\mathcal{Q})=\sum_{P\in\mathcal{Q}}\mathcal{K}(P)$ – multiplicity of the set $\mathcal{Q}$.

◇ $\mathcal{K}(\mathcal{P})$ – the cardinality of $\mathcal{K}$.

◇ Points, lines, ... ,hyperplanes of multiplicity i are called i-points, i-lines, ... , i-hyperplanes.

◇ a_i – the number of hyperplanes H with $\mathcal{K}(H)=i$

◇ $(a_i)_{i\geq 0}$ – the spectrum of $\mathcal{K}$

Definition. (n, w)-arc in $\mathrm{PG}(k-1, q)$: a multiset $\mathcal{K}$ with

1) $\mathcal{K}(\mathcal{P}) = n$;

2) for every hyperplane H: $\mathcal{K}(H) \leq w$;

3) there exists a hyperplane H_0: $\mathcal{K}(H_0) = w$.

Definition. (n, w)-blocking set in $\mathrm{PG}(k-1, q)$

(or (n, w)-minihyper): a multiset $\mathcal{K}$ with

1) $\mathcal{K}(\mathcal{P}) = n$;

2) for every hyperplane H: $\mathcal{K}(H) \geq w$;

3) there exists a hyperplane H_0: $\mathcal{K}(H_0) = w$.

Definition. An (n,w)-arc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$ is called t-extendable, if there exists an $(n+t,w)$-arc $\mathcal{K}'$ in $\mathrm{PG}(k-1,q)$ with $\mathcal{K}'(P) \geq \mathcal{K}(P)$ for every point $P \in \mathcal{P}$. An 1-extendable arc is called extendable.

Definition. An arc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$ with $\mathcal{K}(\mathcal{P}) = n$ and spectrum (a_i) is said to be divisible with divisor Δ, $\Delta > 1$, if $a_i = 0$ for all $i \not\equiv n \pmod{\Delta}$.

Definition. An arc $\mathcal{K}$ with $\mathcal{K}(\mathcal{P}) = n$ and spectrum (a_i) is said to be t-quasidivisible with divisor Δ, $\Delta > 1$, (or t-quasidivisible modulo Δ) if $a_i = 0$ for all $i \not\equiv n, n+1, \ldots, n+t \pmod{\Delta}$.

3. Linear codes as multisets of points

$[n,k,d]_q$-code C of full length	$\Leftrightarrow$	$(n, w = n-d)$-arc $\mathcal{K}$ in $\mathrm{PG}(k-1,q)$
$\mathbf{0} \neq \boldsymbol{u} \in C$, $\mathrm{wt}(\boldsymbol{u}) = u$	$\Leftrightarrow$	a hyperplane H with $\mathcal{K}(H) = n-u$,
extendable $[n,k,d]_q$-code C	$\Leftrightarrow$	extendable $(n, n-d)$-arc $\mathcal{K}$
divisible $[n,k,d]_q$-code $A_i = 0$ for all $i \not\equiv 0 \pmod{\Delta}$	$\Leftrightarrow$	divisible $(n, n-d)$-arc in $\mathrm{PG}(k-1,q)$ $a_i = 0$ for all $i \not\equiv n \pmod{\Delta}$
t-quasidivisible $[n,k,d]_q$-code $A_i = 0$ for all $i \not\equiv -j \pmod{q}$ $j \in \{0,1,\ldots,t\}$	$\Leftrightarrow$	t-quasidivisible $(n, n-d)$-arc in $\mathrm{PG}(k-1,q)$ $a_i = 0$ for all $i \not\equiv n+j \pmod{q}$

◇ Griesmer arcs: arcs associated with codes meeting the Griesmer bound

Griesmer $[n, k, d]_q$ codes $\Leftrightarrow$ Griesmer (n, w)-arcs in $\mathrm{PG}(k-1, q)$

$n = \sum_{i=0}^{k-1} \lceil d/q^i \rceil$ $\qquad$ $n = \sum_{i=0}^{k-1} \lceil (n-w)/q^i \rceil$

◇ If $d = n - w = sq^{k-1} - \varepsilon_{k-2}q^{k-2} - \ldots - \varepsilon_1 q - \varepsilon_0$, and

w_i := maximal multiplicity of a subspace of codimension i, $i = 0, \ldots, k-1$. Then

$$w_i = sv_{k-i} - \varepsilon_{k-2}v_{k-i-1} - \ldots - \varepsilon_{i+1}v_2 - \varepsilon_i v_1,$$

where $v_k = (q^k - 1)/(q - 1)$.

4. Some Extension Results

Theorem. (R. Hill, P. Lizak, 1995, geometric version) Let $\mathcal{K}$ be a (n, w)-arc in $\mathrm{PG}(k-1, q)$ with $\gcd(n-w, q) = 1$. Let further $\mathcal{K}(H) \equiv n$ or $w \pmod q$ for all hyperplanes H. Then $\mathcal{K}$ is extendable to a divisible $(n+1, w)$-arc in $\mathrm{PG}(k-1, q)$. In particular, every 1-quasidivisible arc with divisor q is extendable.

Theorem. (T. Maruta, 2004, geometric version) Let $\mathcal{K}$ be a 2-quasidivisible (n, w)-arc in $\mathrm{PG}(k-1, q)$, $q \geq 5$, odd, with divisor q. Then $\mathcal{K}$ is extendable to an $(n+1, w)$-arc in $\mathrm{PG}(k-1, q)$.

$\diamond$ $\mathcal{K}$ - t-quasidivisible (n, w)-arc in $\Sigma = \mathrm{PG}(k-1, q)$, i.e. for every hyperplane H, we have $\mathcal{K}(H) \equiv n, n+1, \ldots, n+t \pmod{q}$, where $0 < t < q$ is an integer constant.

$\diamond$ Define an arc $\widetilde{\mathcal{K}}$ in the dual space $\widetilde{\Sigma}$

$$\widetilde{\mathcal{K}} : \begin{cases} \mathcal{H} & \rightarrow & \mathbb{N}_0, \\ H & \rightarrow & \widetilde{\mathcal{K}}(H) := n + t - \mathcal{K}(H) \pmod{q}. \end{cases}$$

where $\mathcal{H}$ is the set of all hyperplanes of Σ.

Theorem. Let $\mathcal{K}$ be an (n, w)-arc in $\Sigma = \mathrm{PG}(k-1, q)$ which is t-quasidivisible modulo q, $t < q$.

Let

$$\widetilde{\mathcal{K}} = \sum_{i=1}^{c} \chi_{\widetilde{H}_i} + \widetilde{\mathcal{K}}'$$

for some arc $\widetilde{\mathcal{K}'}$ and c not necessarily different hyperplanes $\widetilde{H_1}, \ldots, \widetilde{H}_c$ then $\mathcal{K}$ is c-extendable. In particular, if $\widetilde{\mathcal{K}}$ contains a hyperplane in its support then $\mathcal{K}$ is extendable.

Theorem. Let $\widetilde{S}$ be a subspace of $\widetilde{\Sigma}$ of positive dimension. Then $\widetilde{\mathcal{K}}(\widetilde{S}) \equiv t \pmod{q}$.

Theorem. (Landjev, Rousseva, Storme, 2014)

Let $\mathcal{K}$ be a t-quasidivisible Griesmer arc in $\mathrm{PG}(k-1,q)$ with parameters (n,w), where

$$d = n - w = sq^{k-1} - \varepsilon_{k-2}q^{k-2} - \ldots - \varepsilon_1 q - \varepsilon_0.$$

Let further $\varepsilon_0 = t, \ldots \varepsilon_{k-2} < \sqrt{q}$. Then $\mathcal{K}$ is t-extendable.

- $\diamond$ $\widetilde{\mathcal{K}}$ is a (tv_{k-1}, tv_{k-2})-arc, where $v_k = \dfrac{q^k-1}{q-1}$
- $\diamond$ $\widetilde{\mathcal{K}}$ is a sum of t hyperplanes

5. $(t \mod q)$-Arcs

Definition. An arc $\mathcal{F}$ is called a $(t \mod q)$-arc if

– all points have multiplicity $\leq t$;

– all subspaces S of positive dimension have multiplicity $\mathcal{F}(S) \equiv t \pmod{q}$.

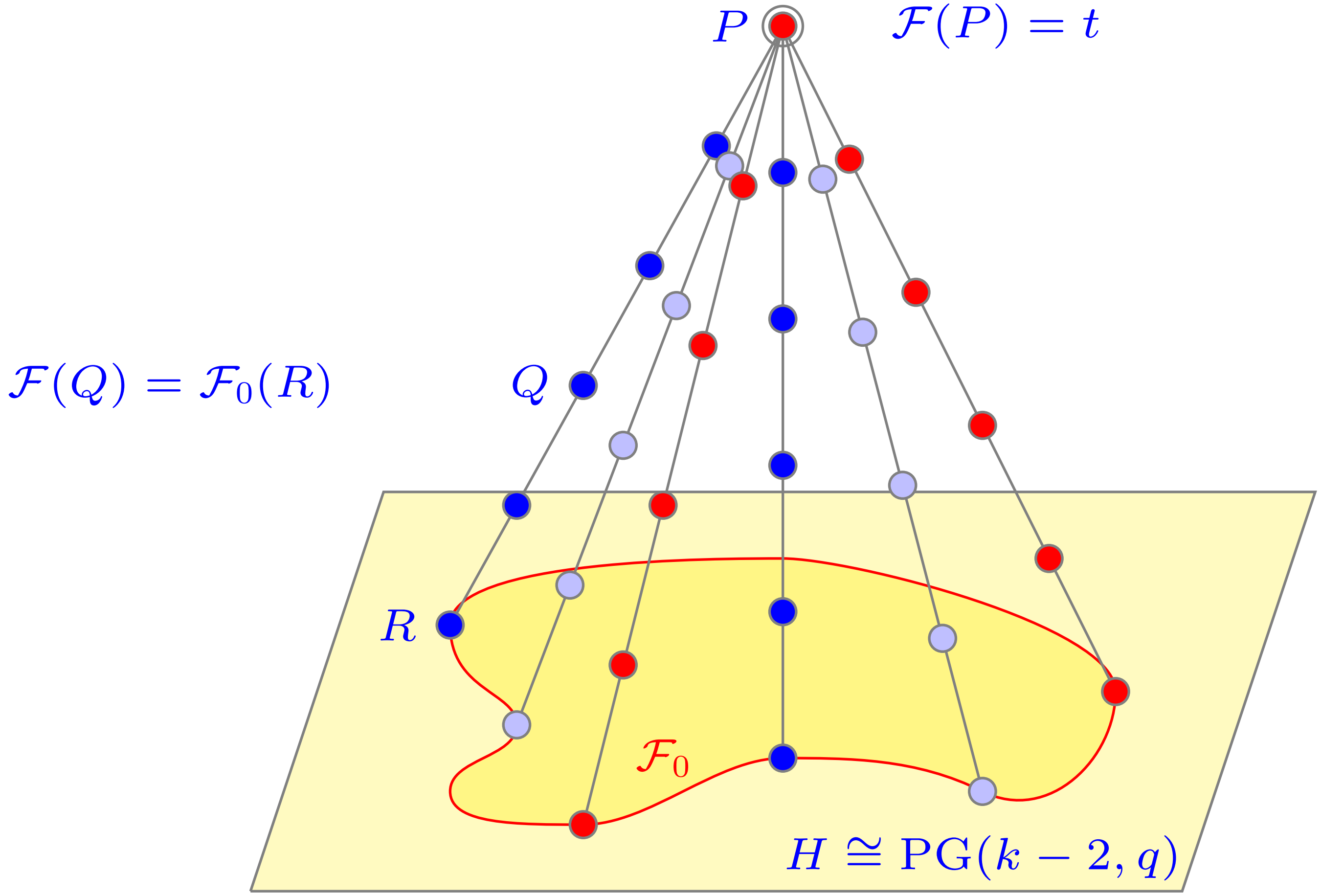
Theorem A. The sum of a $(t_1 \mod q)$-arcs and a $(t_2 \mod q)$-arc is a $(t \mod q)$-arc with $t = t_1 + t_2$. In particular, the sum of t hyperplanes in $\mathrm{PG}(k-1, q)$ is a $(t \mod q)$-arc.

Theorem B. Let $\mathcal{F}_0$ be a $(t \mod q)$-arc in a hyperplane $H \cong \mathrm{PG}(k-2, q)$. of $\Sigma = PG(k-1, q)$. For a fixed point $P \in \Sigma \setminus H$, define an arc $\mathcal{F}$ in Σ as follows:

- $\mathcal{F}(P) = t$;
- for each point $Q \neq P$: $\mathcal{F}(Q) = \mathcal{F}_0(R)$ where $R = \langle P, Q \rangle \cap H$.

Then the arc $\mathcal{F}$ is a $(t \mod q)$-arc in $\mathrm{PG}(k-1, q)$ of size $q|\mathcal{F}_0| + t$.

Definition. $(t \mod q)$-arcs obtained by Theorem B are called lifted arcs.


P
$\mathcal{F}(P) = t$
$\mathcal{F}(Q) = \mathcal{F}_0(R)$
Q
R
$\mathcal{F}_0$
$H \cong \mathrm{PG}(k-2, q)$

$\mathcal{F}$: an arc in $\Sigma = \mathrm{PG}(k-1, q)$

$\mathcal{H}$ – the set of all hyperplanes in Σ

σ - a function such that $\sigma(\mathcal{F}(H))$ is a non-negative integer for all $H \in \mathcal{H}$.

The arc $\mathcal{F}^\sigma$ in $\widetilde{\Sigma}$

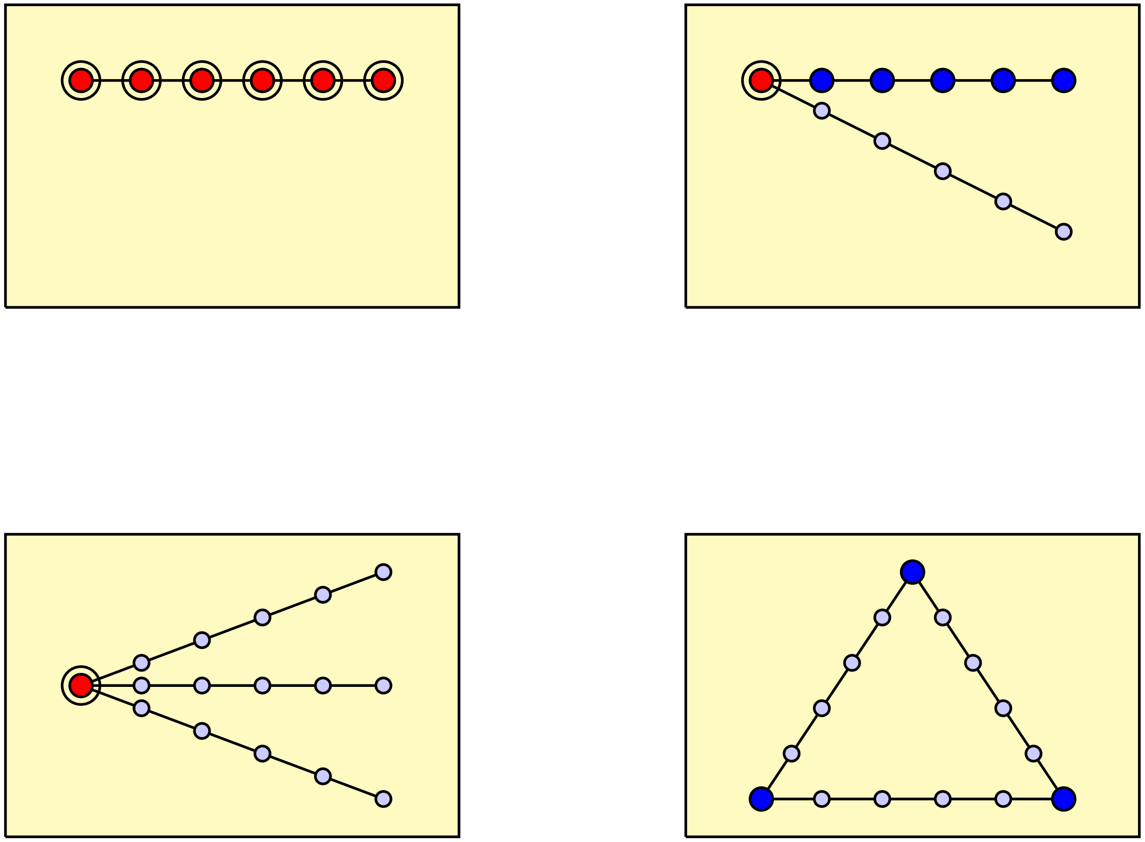
$$\mathcal{F}^\sigma : \begin{cases} \mathcal{H} & \rightarrow & \mathbb{N}_0 \\ H & \rightarrow & \sigma(\mathcal{F}(H)) \end{cases}$$

is called the σ-dual of $\mathcal{F}$.

Theorem C. Let $\mathcal{F}$ be a $(t \mod q)$-arc in $\mathrm{PG}(2, q)$ of size $mq + t$. Then the arc $\mathcal{F}^\sigma$ with $\sigma(x) = (x - t)/q$ is an $((m - t)q + m, m - t)$-blocking set in the dual plane with line multiplicities $m - t, m - t + 1, \ldots, m$.

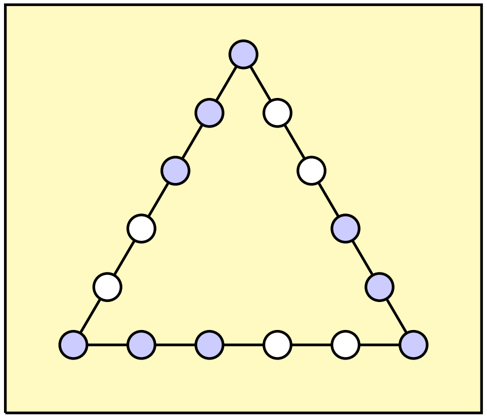
$(3 \mod 5)$-arcs in $\mathrm{PG}(2,5)$

$(18,\{3,8,13,18\})$-arcs



$\mathcal{F}$: $(23, \{3, 8\})$-**arc**

$\mathcal{F}^\sigma$:



$\mathcal{F}^\sigma$: (9,1)-blocking set

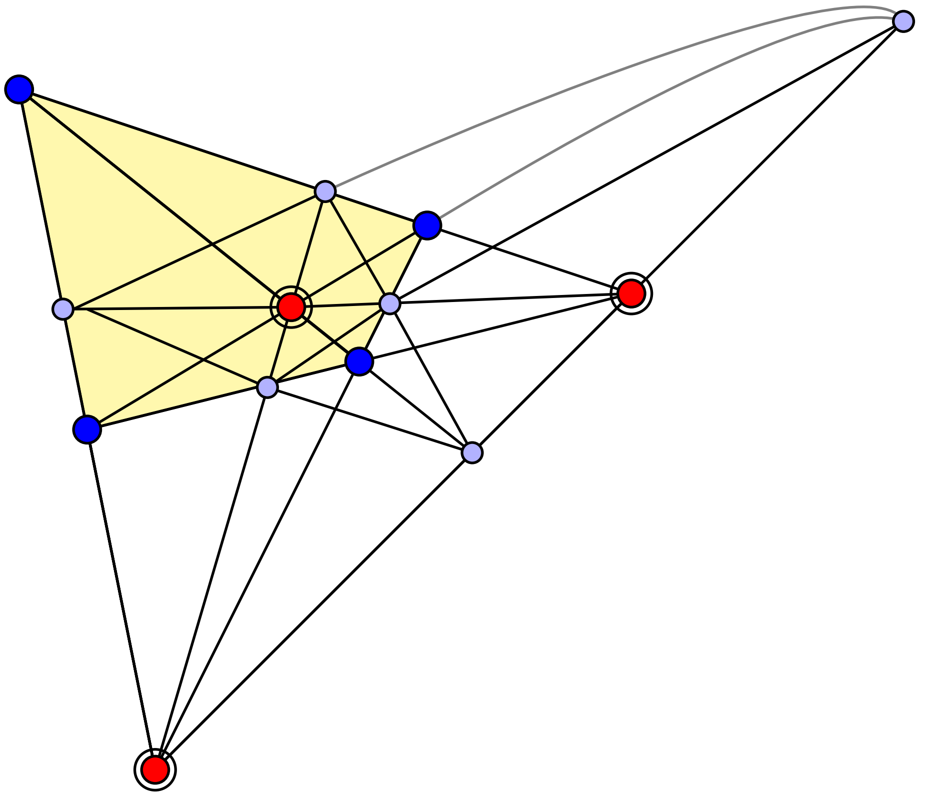
with line multiplicities $1, 2, 3, 4$

$\mathcal{F}$: $(28, \{3, 8\})$-**arc**

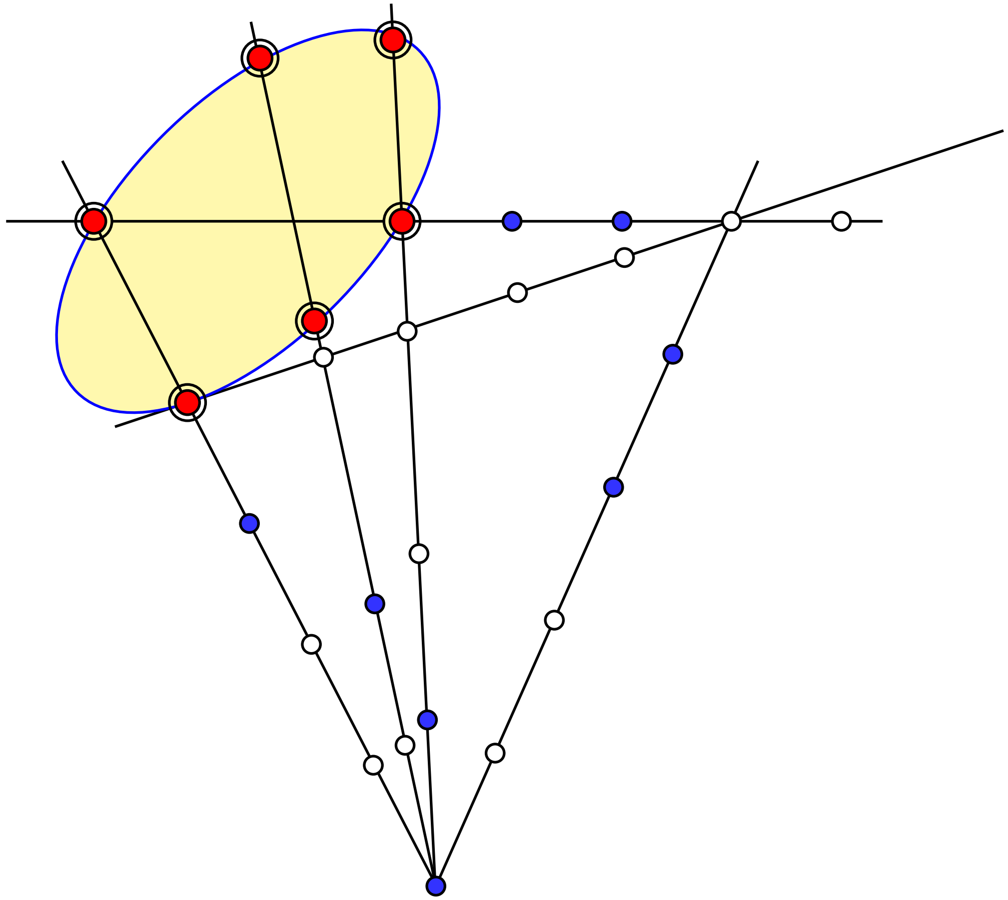
$\mathcal{F}^\sigma$: $(15, 2)$-blocking set with line multiplicities $2, 3, 4, 5$

$\mathcal{F}^\sigma$: the complement of the unique $(16, 4)$-arc without external lines

The $(23, \{3, 8\})$-arc



The $(28, \{3, 8\})$-arc



$\mathcal{F}$: $(33, \{3, 8, 13\})$-**arc**

$\mathcal{F}^\sigma$: $(21, 3)$-blocking set with line multiplicities $3, 4, 5, 6$

$\mathcal{F}^\sigma$ is one of the following:

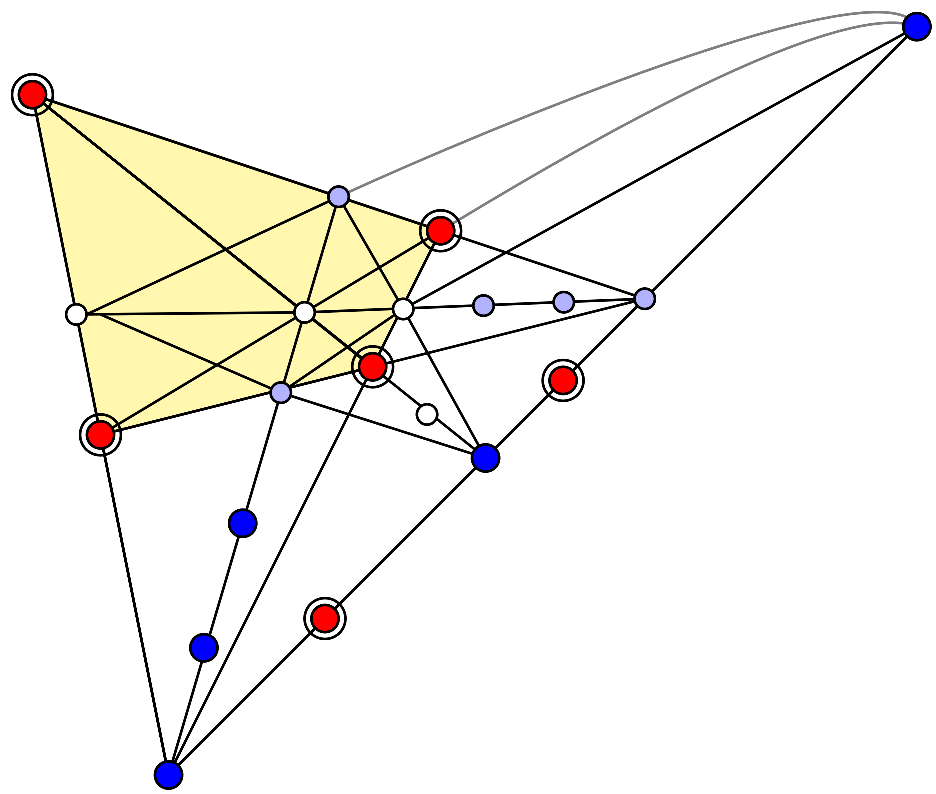
(1) the complement of the seven non-isomorphic $(10, 3)$-arcs; $\Lambda_2 = 0$

(2) the complement of the $(11, 3)$-arc with four external lines; a point not on an external line is doubled; $\Lambda_2 = 1$

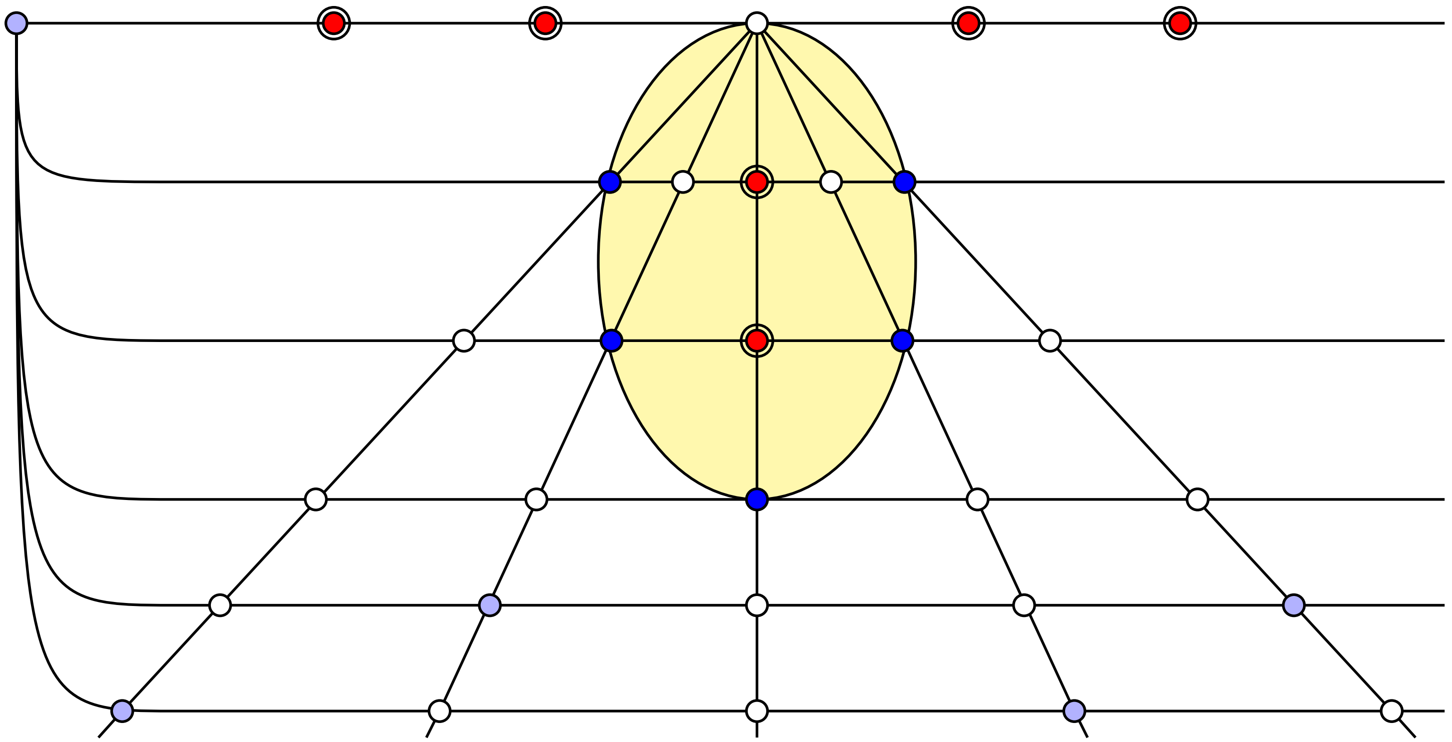
(3) one double point which forms an oval with five of the 0-points; the tangent in the 2-point is a 3-line; $\Lambda_2 = 1$

(4) $\mathrm{PG}(2, 5)$ minus a triangle with vertices of multiplicity $2, 2, 1$; $\Lambda_2 = 2$

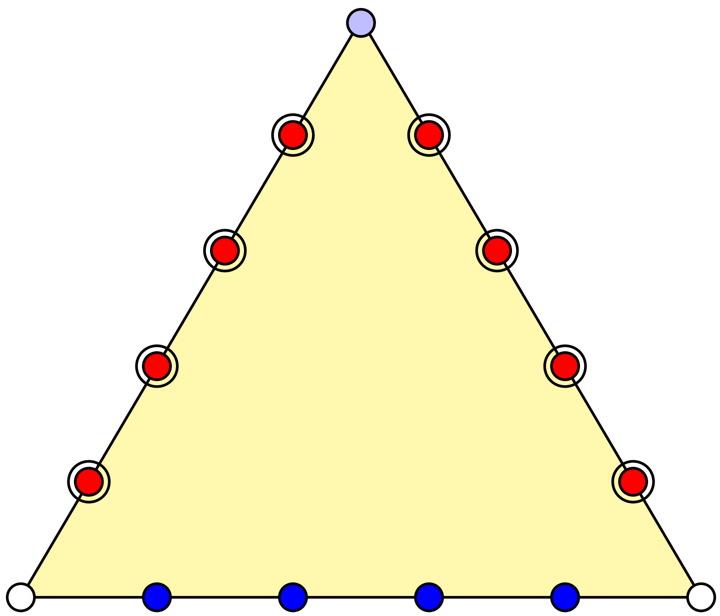
(2) The first $(33, \{3, 8, 13\})$-arc with one 13-line



(3) the second $(33, \{3, 8, 13\})$-arc with one 13-line



(4) $(33, \{3, 8, 13\})$-arc with two 13-lines



Theorem D. Every $(3 \mod 5)$-arc $\mathcal{F}$ in $\mathrm{PG}(3,5)$ with $|\mathcal{F}| \le 153$ is a lifted arc (obtained by Theorem B). In particular, $|\mathcal{F}| = 93, 118$, or 143.

6. The Nonexistence of Some Griesmer Codes

A. The Nonexistence of $[104, 4, 82]_5$-Codes

$$d = 82 = 5^3 - 5^2 - 3 \cdot 5 - 3$$

$$s = 1, \varepsilon_2 = 1, \varepsilon_1 = 3, \varepsilon_0 = t = 3;$$

$$\varepsilon_0, \varepsilon_1 \geq \sqrt{q}$$

$$w_3 = 1, w_2 = 5, w_1 = 22, w_0 = n = 104$$

Theorem E. Let $\mathcal{K}$ be a $(104, 22)$-arc in $\mathrm{PG}(3, 5)$. Then

(i) $\mathcal{K}$ is a Griesmer 3-quasidivisible projective arc;

(ii) $\widetilde{\mathcal{K}}$ is a $(3 \mod 5)$-arc in $\mathrm{PG}(3, 5)$;

(iii) there is no 18-plane π such that $\widetilde{\mathcal{K}}|_\pi$ is the sum of three copies of the same line;

(iv) $|\widetilde{\mathcal{K}}| \leq 143$.

- Hence $|\widetilde{\mathcal{K}}| = 93$ and $\widetilde{\mathcal{K}}$ is a sum of three planes.

- Hence $\mathcal{K}$ is 3-extendable to a (non-existent) $(107, 22)$-arc.

- There is no $[104, 4, 82]_5$-code and

$$n_5(4, 82) = 105.$$

B. The Nonexistence of $[q^3 - 3q - 6, 4, q^3 - q^2 - 3q - 3]_q$-Codes

$\diamond$ $q = 5$: $(104, 22)$-arcs in $\mathrm{PG}(3, 5)$

$\diamond$ $q = 7$: $(316, 46)$-arcs in $\mathrm{PG}(3, 7)$

Plane multiplicities: $1, 8, 15, 22, 29, 36, 43$–49

$\diamond$ $q = 8$: $(482, 61)$-arcs in $\mathrm{PG}(3, 8)$

Plane multiplicities: $10, 42, 58$–61

$\diamond$ $q = 9$: $(696, 78)$-arcs in $\mathrm{PG}(3, 9)$

Plane multiplicities: 75–78

$\diamond$ $q \geq 11$: are 3-extendable since $\varepsilon_i < \sqrt{q}$.

C. The Nonexistence of $[204, 4, 162]_5$-Codes