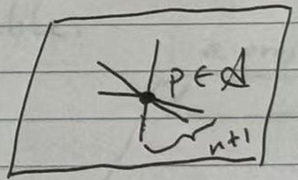
Def. 2.7. An (m,k)-arc in a projective plane of order n is a set of m points, no $(k+1)$ of which are collinear.

Remark 2.8. Note that $(m,2)$-arcs are just arcs discussed yesterday.

Thm. 2.9. Let $\mathcal{A}$ be an (m,k)-arc in a projective plane of order n. Then $|\mathcal{A}| \leq 1+(n+1)(k-1)$.

Equality holds implies that every line meets $\mathcal{A}$ in 0 or k points.

Proof: Let $P \in \mathcal{A}$.



$$|\mathcal{A}| \leq 1+(n+1)(k-1)$$

When equality holds,

if $|l \cap \mathcal{A}| \geq 1$, then $|l \cap \mathcal{A}| = k$.

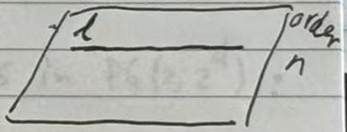
Hence $\forall l \in \mathcal{L}$, $|l \cap \mathcal{A}| = \begin{cases} 0 \\ k \end{cases}$.

Def. 2.10. An (m, k)-arc in a proj plane of order n, with $m = 1 + (n+1)(k-1)$, i.e. maximum sized (m, k)-arc is called a <u>perfect arc</u>.

(sometimes, maximal arc)

Corollary 2.11. Take the points of a perfect (m, k)-arc as the points of an incidence structure, take all the nonempty intersections of the lines with the perfect arc as <u>blocks</u> (区组), we obtain a $2-(m, k, 1)$ design with $m = 1 + (n+1)(k-1)$. Moreover, the design is resolvable.

a proj plane of order n



Examples 2.12

(i) The set of n^2 points not on a fixed line of a projective plane of order n is a perfect (n^2, n)-arc

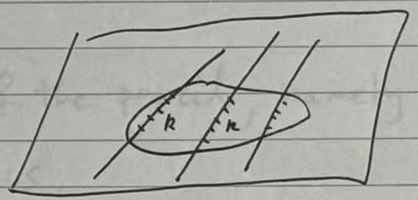
2p no $n+1$ points of the arc are collinear

The corresponding Steiner system is an affine plane of order n

(ii) The hyperoval of a projective plane of order n, n even, is a perfect $(n+2, 2)$-arc. The corresponding design is trivial (block size $= 2$, a $2-(n+2, 2, 1)$ design

Theorem 2.13. If $\exists$ a perfect (m, k)-arc in a proj plane of order n, then $k | n$.

proof :



$$m = 1 + (n+1)(k-1)$$

$$k \mid m = nk + k - n \quad \Rightarrow \quad k \mid n$$

Denniston's Construction of Perfect (m, k)-arcs in $PG(2, 2^d)$:

We will construct perfect (m, k)-arcs in $PG(2, 2^d)$ for all $k \mid 2^d$. Write $k = 2^t$, $m = 1 + (2^d+1)(2^t-1)$

$$= 2^{d+t} - 2^d + 2^t$$

Let $X^2 + bX + 1$ be an <u>irreducible</u> quadratic poly over $\mathbb{F}_q$, $q = 2^d$. That is, $Tr_{2^d/2}\left(\frac{1}{b}\right) = 1$.

Consider the following pencil of conics:

$$\begin{cases} F_\lambda(X, Y, Z) = X^2 + bXY + Y^2 + \lambda Z^2, & \lambda \in \mathbb{F}_q \\ F_\infty = Z^2 \end{cases}$$

Two members of the pencil, namely F_0 and F_∞, are degenerate conics.

$$Z(F_0) = \langle (0,0,1) \rangle \quad \text{a point}$$

$$Z(F_\infty) = \text{the line } Z = 0$$

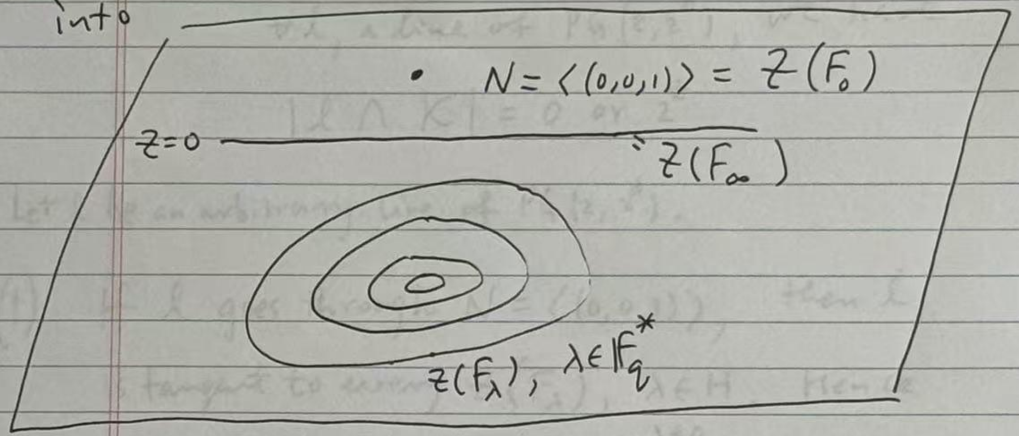
For any $\lambda \in \mathbb{F}_q \setminus \{0\}$,

$Z(F_\lambda)$ is a nondegenerate conic with knot $N = \langle (0,0,1) \rangle$

And $Z(F_\lambda) \cap Z(F_{\lambda'}) = \phi$ if $\lambda \neq \lambda'$

Therefore the whole plane $PG(2, 2^d)$ is partitioned

into



$$1 + (q+1) + \underbrace{(q-1)}_{\lambda \neq 0}(q+1) = q^2 + q + 1.$$

Theorem 2.14. (Denniston 1969)

In $PG(2, 2^d)$, let

$$K = \bigcup_{\lambda \in H} Z(F_\lambda),$$ where H is any subgroup of $(\mathbb{F}_{2^d}, +)$ of size 2^t.

Then K is a perfect $(m = 1 + (2^d+1)(2^t-1), \ k = 2^t)$-arc.

proof: We need to show that

$$\forall \ell, \text{ a line of } PG(2,2^d), \text{ we have}$$

$$|\ell \cap K| = 0 \text{ or } 2^t$$

Let ℓ be an arbitrary line of $PG(2,2^d)$.

(1) If ℓ goes through $N = \langle(0,0,1)\rangle$, then ℓ is tangent to every $Z(F_\lambda)$, $\underset{\lambda \neq 0}{\lambda \in H}$. Hence

$$|\ell \cap K| = 1 + (2^t - 1) = 2^t$$

(2) Now assume that ℓ doesn't go through N. So the $(q+1)$ pts of ℓ consists of one pt on $Z(F_\infty)$, and two each on $\frac{1}{2}q$ conics of the pencil.

Assume that $\ell = \left\langle \begin{pmatrix} a_0 \\ a_1 \\ a_2=1 \end{pmatrix} \right\rangle$ ($\because$ ℓ doesn't go through $N=\langle(0,0,1)\rangle$)

$\therefore$ 이% assume $a_2 = 1$

$\lambda \in \mathbb{F}_q$, $\ell \cap Z(F_\lambda) = \phi$

$$\Leftrightarrow \begin{cases} a_0X + a_1Y + Z = 0 \\ X^2 + bXY + Y^2 + \lambda Z^2 = 0 \end{cases} \text{ has no Solutions } (x,y,z) \neq (0,0,0)$$

$$\iff (1+\lambda a_0^2)X^2 + bXY + (1+\lambda a_1^2)Y^2 = 0$$

$$\iff \mathrm{Tr}_{2^d/2}\left(A + B\lambda + C\lambda^2\right) = 1,$$

where $A = \frac{1}{b^2}$, $B = \frac{a_0^2 + a_1^2}{b^2}$, $C = \frac{a_0^2 a_1^2}{b^2}$

But we know that $\mathrm{Tr}(A) = 1$

$$\iff \mathrm{Tr}_{2^d/2}\left(B\lambda + C\lambda^2\right) = 0$$

$$\iff \mathrm{Tr}_{2^d/2}\left((B+\sqrt{C})\lambda\right) = 0$$

Here note that $B + \sqrt{C} \neq 0$

$\left[\because B + \sqrt{C} = 0 \Rightarrow \frac{a_0^2 + a_1^2}{b^2} = \frac{a_0 a_1}{b} \Rightarrow b = \frac{a_0^2 + a_1^2}{a_0 a_1} \Rightarrow \mathrm{Tr}\left(\frac{1}{b}\right) = 0, \text{ } \frac{3}{T}/\!/\!_b\right]$

$\therefore \ell \cap Z(F_\lambda) = \phi$

$\iff \lambda \in$ Hyperplane of $(\mathbb{F}_{2^d}, +)$ determined by $B + \sqrt{C}$

Since H is a subgp of $(\mathbb{F}_{2^d}, +)$, either $H \subseteq$ the hyperplane $H_{B+\sqrt{C}}$

or $H \nsubseteq$ the hyperplane $H_{B+\sqrt{C}}$

If $H \subseteq \mathcal{H}_{B+\sqrt{C}}$, then $|\ell \cap K| = 0$

If $H \nsubseteq \mathcal{H}_{B+\sqrt{C}}$, then $\left|H \cap \mathcal{H}_{B+\sqrt{C}}\right| = \frac{1}{2}|H|$

and $|\ell \cap K| = 2 \cdot \frac{1}{2}|H| = |H| = 2^t$

$\square$

From the Denniston $(1+(2^d+1)(2^t-1), 2^t)$-arc in $PG(2,2^d)$, we obtain a Steiner 2-design with parameters

$$v = 2^{d+t} - 2^d + 2^t, \quad k = 2^t \text{ (block size)}, \quad \lambda = 1$$

Consider the block-point incident matrix of this design

$$\begin{array}{c|c|c|}
 & \text{points on } K & \text{pts not on } K \\
\hline
\text{secant lines} & A & \\
\hline
\text{exterior lines} & 0 & \begin{matrix} * * \cdots * \\ * * \cdots * \end{matrix} \\
\hline
\end{array}$$

A: $(0,1)$-incidence matrix of the steiner design

Conjecture (Chandler, Vandendriessche, XIANG, 2015)

$$\operatorname{rank}_{\mathbb{F}_2}(A) = v - \sum_{i=0}^{t} (2^t - 2^i)\binom{d}{i}.$$

(1997) Ball, Blokhuis & Mazzocca : Maximal arcs in Desarguesian planes of odd order do NOT exist.

P.2

Def. 2.15 Let $(\mathcal{P}, \mathcal{L})$ be a proj plane of order n.

A set $\mathcal{U}$ of $n\sqrt{n}+1$ points of $(\mathcal{P}, \mathcal{L})$ is called a unital if $\forall \ell$ (line), $|\ell \cap \mathcal{U}| = 1$ or $\sqrt{n}+1$

Moreover, if $|\ell \cap \mathcal{U}| = 1$, then ℓ is called a tangent line of $\mathcal{U}$.

Def 2.16. The Hermitian Curve in $PG(2,q)$, $q = \square$:

Let $h : V \times V \to \mathbb{F}_q$, $V = \mathbb{F}_q^3$

$$h(x,y) = x_1 y_1^{\sqrt{q}} + x_2 y_2^{\sqrt{q}} + x_3 y_3^{\sqrt{q}}$$

Then h is a nondeg Hermitian form (meaning:

$$h(x+z, y) = h(x,y) + h(z,y)$$
$$h(x, z+y) = h(x,z) + h(x,y)$$
$$h(ax, by) = a b^{\sqrt{q}} h(x,y)$$
$$h(x,y) = h(y,x)^{\sqrt{q}}$$
)

$$\mathcal{H} = \left\{ \langle x \rangle \underset{PG(2,q)}{\in} \;\middle|\; h(x,x)=0 \right\} = \left\{ \langle (x_1,x_2,x_3) \rangle \;\middle|\; x_1^{\sqrt{q}+1} + x_2^{\sqrt{q}+1} + x_3^{\sqrt{q}+1} = 0 \right\}$$

Then $\mathcal{H}$ is called an Hermitian Curve.

Theorem 2.17. Let $\mathcal{H}$ be defined above. Let l be any line of $PG(2,q)$. If $|l \cap \mathcal{H}| \geq 2$, then $|l \cap \mathcal{H}| = \sqrt{q}+1$.

proof: Let $\langle x \rangle, \langle y \rangle \in l \cap \mathcal{H}$.

All the points of the line l are $\{\langle y \rangle\} \cup \{\langle x+\lambda y \rangle \mid \lambda \in \mathbb{F}_q\}$

Define a map $\phi : \mathbb{F}_q \to \mathbb{F}_{\sqrt{q}}$

$$\phi(\lambda) = h(x+\lambda y,\, x+\lambda y)$$

$$= \underset{0}{\underset{\parallel}{h(x,x)}} + h(x,y)\lambda^{\sqrt{q}} + \lambda h(y,x) + \underset{0}{\underset{\parallel}{h(\lambda y,\lambda y)}}$$

$$= h(y,x)\lambda + h(x,y)\lambda^{\sqrt{q}}$$

Want $|\phi^{-1}(0)| = ?$

(P.26

Suppose $h(x,y) \neq 0$. For each $a \in \mathbb{F}_{\sqrt{q}}$, $\phi^{-1}(a)$ has at most $\sqrt{q}$ elements because it is defined by a poly of degree $\sqrt{q}$. Now we will see that $|\phi^{-1}(a)| = \sqrt{q}$ for each $a \in \mathbb{F}_q$

$$q = |\mathbb{F}_q| = \left| \bigcup_{a \in \mathbb{F}_{\sqrt{q}}} \phi^{-1}(a) \right|$$

$$= \sum_{a \in \mathbb{F}_{\sqrt{q}}} |\phi^{-1}(a)| \leq \sum_{a \in \mathbb{F}_{\sqrt{q}}} \sqrt{q} = \sqrt{q}\sqrt{q} = q$$

$\Rightarrow |\phi^{-1}(a)| = \sqrt{q}$, $\forall a$. In particular, $|\phi^{-1}(0)| = \sqrt{q}$.

We have seen that the intersection $\ell \cap \mathcal{U}$ has $\sqrt{q}+1$ pts.

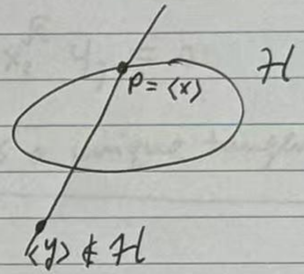
How about the case $h(x,y) = 0$?

We claim that $h(x,y) \neq 0$. If $h(x,y) = 0$, then $\mathcal{H}$ contains an entire line, which makes h degenerate. impossible.

Theorem 2.18 Let $\mathcal{H}$ be defined above. For each $P \in \mathcal{H}$, there exists a unique tangent of $\mathcal{H}$ through P.

proof: Let $P = \langle x \rangle \in \mathcal{H}$

$\langle y \rangle \notin \mathcal{H}$.



$l = \langle x, y \rangle$ = the line through $\langle x \rangle$ & $\langle y \rangle$

$= \{\langle y \rangle\} \cup \{\langle x + \lambda y \rangle \mid \lambda \in \mathbb{F}_q\}$

Suppose $h(x,y) \neq 0$. Then as in the proof of Thm 2.17 we see that $|l \cap \mathcal{H}| = \sqrt{q} + 1$ (so l is a secant line of $\mathcal{H}$)

Suppose $h(x,y) = 0$. We have

$$0 = h(x+\lambda y, x+\lambda y) = \underset{\overset{\shortparallel}{0}}{h(x,x)} + \underbrace{\lambda^{\sqrt{q}} h(x,y)}_{\overset{\shortparallel}{0}} + \overbrace{\lambda h(y,x)}^{\overset{0}{\shortparallel}} + \lambda^{\sqrt{q}+1} h(y,y)$$

Since $h(y,y) \neq 0$, we must have $\lambda = 0$. This shows if $h(x,y) = 0$ & $\langle y \rangle \notin \mathcal{H}$, the line defined by $\langle x \rangle, \langle y \rangle$ is a tangent line through P.

But all points $\langle y \rangle$ such that $0 = h(x, y)$

$$= h(y, x)$$
$$= y_1 x_1^{\sqrt{q}} + y_2 x_2^{\sqrt{q}} + y_3 x_3^{\sqrt{q}}$$

are incident with the same line, i.e. the line

$$x_1^{\sqrt{q}} y_1 + x_2^{\sqrt{q}} y_2 + x_3^{\sqrt{q}} y_3 = 0.$$

Hence through $p \in \mathcal{H}$, there is a unique tangent line of $\mathcal{H}$

Theorem 2.19. $|\mathcal{H}| = q\sqrt{q} + 1$.

We prove this by counting (p, ℓ), $p \in \mathcal{H}$, $p \in \ell$ in two ways.

Starting with p, we have $|\mathcal{H}| \cdot (q+1)$

Now start with ℓ. The total number of lines is q^2+q+1;

Among these lines, $|\mathcal{H}|$ of them are tangents

So the count is : $|\mathcal{H}| + (q^2+q+1 - |\mathcal{H}|)(\sqrt{q}+1)$

Hence $|\mathcal{H}|(q+1) = |\mathcal{H}| + (q^2+q+1 - |\mathcal{H}|)(\sqrt{q}+1) \Rightarrow |\mathcal{H}| = q\sqrt{q}+1$

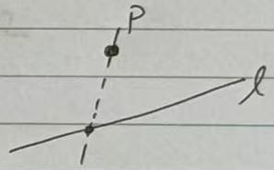
Generalized quadrangles

Def. 3.1 A generalized quadrangle is a point-line incidence structure satisfying the following:

(GQ1): Every line has $s+1$ pt for some $s \geq 1$

(GQ2): Every point lies on $t+1$ lines for some $t \geq 1$

(GQ3): If p is a point not on a line ℓ, then $\exists!$ line through p meeting ℓ



We call (s,t) the order of the GQ, or if $s=t$ we say simply a GQ of order s.

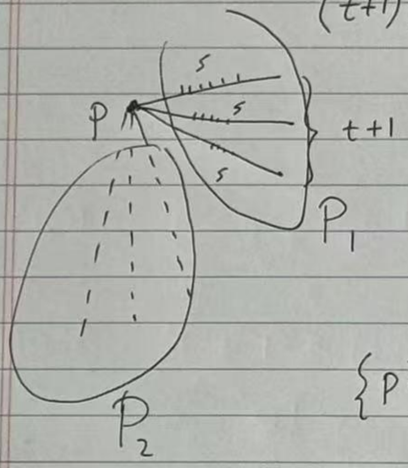
Usually one requires $s, t \geq 2$, giving the so-called thick generalized quadrangle; those with $s=1$ or $t=1$ are thin.

Indeed a generalized quad of order $(s,1)$ is just a 2-net of order $s+1$, i.e., a grid with $(s+1)^2$ points and $2(s+1)$ lines

Theorem 3.2. A GQ of order (s,t) has exactly $(s+1)(st+1)$ points

$(t+1)(st+1)$ lines

proof:



$$\{P\} \cup \mathcal{P}_1 \cup \mathcal{P}_2$$

$$|\mathcal{P}_1| = s(t+1).$$

Count (P', Q), $P' \in \mathcal{P}_1$, $Q \in \mathcal{P}_2$ P' & Q are collinear in two ways.

Start with Q: $|\mathcal{P}_2|(t+1)$

Start with P': $|\mathcal{P}_1| \cdot st$

$$\Rightarrow |\mathcal{P}_2| = \frac{|\mathcal{P}_1| st}{t+1} = s^2 t$$

Hence the # of pts is $1 + s(t+1) + s^2 t = (s+1)(st+1)$