On the additive embedding of $\mathsf{PG}(2, q)$ into $\mathsf{AG}(3, q)$

CoDesCo Sevilla, 11.7.2024

Projective plane:

any two points are incident with a line

any two line are incident with a point

there exists a quadrilater.

With two operations $F(+,\times)$ we characterize some of them, as

points: (x,y)

lines: $ax+by+c=0$

For instance, Hughes planes, where F is a near-field

(e.g., one of the the seven exceptional ones...)

How to ”characterize” projective planes with one operation $G(+)$?

Points are (not necessarily all the) elements of $G(+)$

Lines are k-subsets such that...

Points $P_j = (x, y)$ of lines in AG$(2, q)$ are such that

$$P_1 + \cdots + P_q = (0, 0)$$

so why not take THIS as a condition?

Theorem (Caggegi, F., Pavone 2017)

With the exeptions of the trivial $2-(v, v-1, v-2)$ design,

any *linked* $t-(v, k, \lambda)$ design $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ can be embedded

in a commutative group $G_{\mathcal{D}}$,

so that

$$\{P_1, \ldots, P_k\} \text{ is a block } \iff P_1 + \cdots + P_k = 0$$

Remark the sufficiency!

M. Pavone *A quasidouble of the affine plane of order* 4 *etc.*, FFA (92), 2023.

A resolvable* $2-(16,4,2)$ design $\mathcal{D}_2$ on the set $\mathrm{GF}(4)\times\mathrm{GF}(4)$,

obtained joining the 20 lines of $\mathcal{D}_1 = \mathrm{AG}(2,4)$

with those one gets applying a GF(2)-linear map (which is not GF(4)-linear).

Note: $G_{\mathcal{D}_1} = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2 \oplus \left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)^5$, whereas $G_{\mathcal{D}_2} = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^2 \oplus \left(\frac{\mathbb{Z}}{4\mathbb{Z}}\right)^3$

*not *affine* resolvable!
resolvable = blocks can be partitioned into parallel classes, i.e. partitions of its ground set.
affine resolvable = resolvable, and such that two non-parallel blocks meet in the same number of points.

An interesting part of this construction is a (cyclic) decomposition of the

$2-(16,4,7)$ point-plane design AG(4, 2) (having 140 blocks, here planes)

into seven disjoint isomorphic copies of the

$2-(16,4,1)$ design AG(2, 4) (having 20 blocks, here lines)

which produces, in addition, a solution to Kirkman's schoolgirl problem.

Which one?

$PG(3,2)$ underlies two non-isomorphic $KTS(15)$, commonly denoted by

1a (second published solution, by Cayley) and

1b (first published solution, by Kirkman).

PG$(3,2)$ underlies two non-isomorphic KTS(15), commonly denoted by

1a (second published solution, by Cayley) and

1b (first published solution, by Kirkman).

The solution given before is 1b.

Back to $\mathcal{P} \hookrightarrow G_{\mathcal{D}}$, the bad news is that $G_{\mathcal{D}}$ is huge:

for $k = p + 1$, we find that $G_{\mathcal{D}} = \mathrm{GF}(p)^{\frac{v-1}{2}}$

But if we are willing of loosing the fact that

blocks are *the only* zero k-subsets,

then we get an incredibly small embedding:

Buratti, M., Nakić, A.

Additivity of symmetric and subspace 2-designs

Des. Codes Cryptogr. (2024).

PG$(2, q)$ can be embedded in AG$(3, q)$ so that

$$\{P_1, \ldots, P_q\} \text{ is a block} \Longrightarrow P_1 + \cdots + P_q = 0$$

Actually, they proved that

a cyclic symmetric $2-(v,k,\lambda)$ is additive under $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^t$

for p dividing $k-\lambda$, but not v,

and t the exponent of $p \mod v$.

Thus they embedded PG(n,q) into the AG$(n+1,q)$

with the property that the coordinate sum of the points

of the images of (projective) hyperplanes is zero.

Clearly $\mathsf{AG}(3,q) = \mathsf{GF}(q)^3 = \mathsf{GF}(q^3)$ and

$\mathsf{GF}(q^3)^* = \mathsf{GF}(q)^* \times U$,

with $\mathsf{GF}(q)^* = \mathsf{Ker}(x \mapsto x^{q-1})$ and $U = \mathsf{Im}(x \mapsto x^{q-1})$,

that is, putting $\mathsf{GF}(q^3)^* = \langle \gamma \rangle$

$\mathsf{GF}(q)^* = \langle \gamma^{q^2+q+1} \rangle$,

$U = \langle \gamma^{q-1} \rangle$

In particular, $|U| = \left| \frac{\mathsf{GF}(q^3)^*}{\mathsf{GF}(q)^*} \right| = \frac{|\,\mathsf{AG}(3,q)|}{|\,\mathsf{GF}(q)^*|} = q^2 + q + 1 = \mathsf{PG}(2,q)$.

Do *all* k-sets in $\mathrm{AG}(n+1, q)$ form a 2-design?

No, only a 1-design (or *tactical configuration*).

Do *all* k-sets in AG$(n+1,q)$ form a 2-design?

No, only a 1-design (or *tactical configuration*).

Possibly a noble one?

No, just a plebean:

$$r = \frac{1}{q^{n+1}}\left(\binom{q^{n+1}-1}{\frac{q^n-1}{q-1}} - (q^{n+1}-1)\binom{q^n-1}{\frac{q^{n-1}-1}{q-1}}\right),$$

Do *all* k-sets in AG$(n+1,q)$ form a 2-design?

No, only a 1-design (or *tactical configuration*).

Possibly a noble one?

No, just a plebean:

$$r = \frac{1}{q^{n+1}} \left(\binom{q^{n+1}-1}{\frac{q^n-1}{q-1}} - (q^{n+1}-1)\binom{q^n-1}{\frac{q^{n-1}-1}{q-1}} \right),$$

However, this makes the point-hyperplanes 2-design of PG(n,q) a sub-design of the 1-$(q^{n+1}-1, \frac{q^n-1}{q-1}, r)$ design, whose automorphisms are just the ones induced by the elements in GL$(n+1,q)$, as proved in

G. Falcone and M. Pavone

Permutations of zero-sumsets in a finite vector space. *Forum Math.*, 2021.

What about automorphisms?

Note that the BN-representation corresponds, in the $\mathbb{R}$-case, to the identification of the real projective line with $\mathsf{SO}(2,\mathbb{R})$ in the decomposition $\mathbb{C}^* = \mathbb{R}^* \times \mathsf{SO}(2,\mathbb{R})$

Skipping the case of the $\mathbb{R}$-plane, we have as well

$\mathbb{H}^* = \mathbb{R}^* \times \mathsf{Spin}(3,\mathbb{R})$

Also, the Frobenius map *could* induce an automorphism, as

$F(x^{q-1}) = F(x)^{q-1}$ and $F(x + y) = F(x) + F(y)$

... but it does not.

(Tried with the example in BN paper).

THANK YOU!