Sequences and functions derived from projective planes and their difference sets

Alexander Pott, Qi Wang, Yue Zhou

Otto-von-Guericke-University Magdeburg

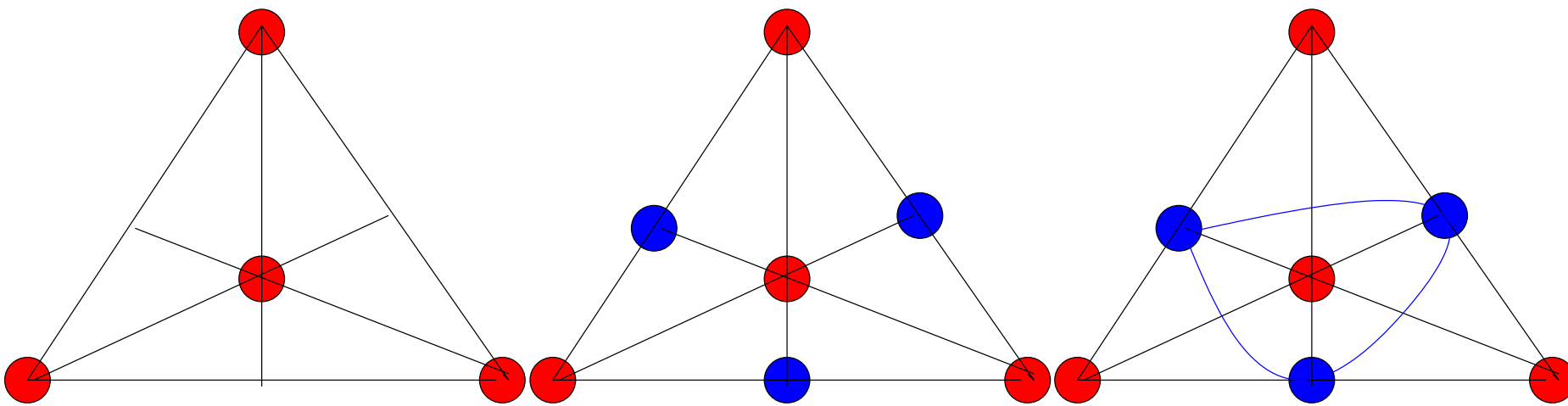
WAIFI, July 2012

Outline

- Projective Planes and Difference Sets.
- Residual Planes and (Relative) Difference Sets.
- Sequences and Functions derived from residual planes using projections.
- Some Theorems/Problems/Conclusions.

Projective Planes

- points
- lines
- 2 points on a unique line
- 2 lines intersect
- quadrangle

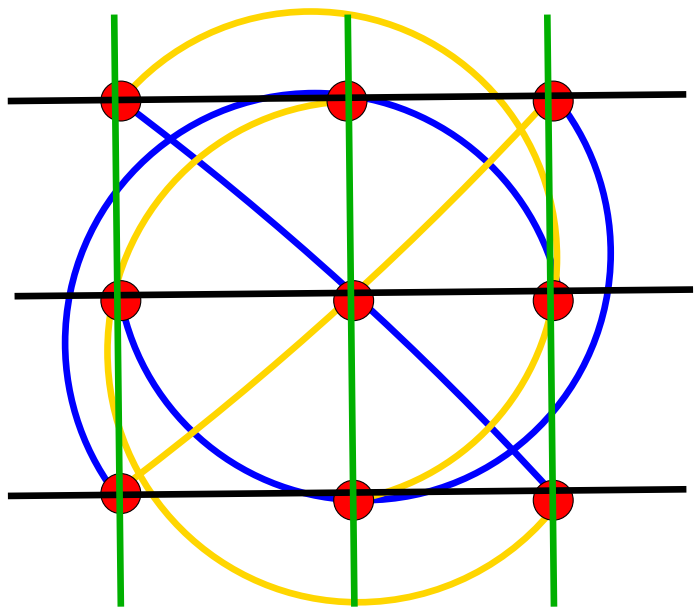


Properties of projective planes

- ♯ points = ♯ lines = $n^2 + n + 1$.
- ♯ lines through a point: $n + 1$.
- ♯ points on a line: $n + 1$.
- n order

Example

$n = 3$



Constructions of Planes

Finite Fields $\mathbb{F}_q$:

- Points: 1- dimensional subspaces of $\mathbb{F}_q^3$.
- Lines: 2- dimensional subspaces of $\mathbb{F}_q^3$.

Desarguesian plane.

- Isomorphisms of planes: Incidence preserving maps from points to points and lines to lines.
- Automorphism group: Incidence preserving permutation on points.

Example

Automorphism group of Desarguesian plane is $\mathrm{P\Gamma L}(3, q)$.

The BIG questions about projective planes

- n a prime power?
- More than one example if $n = p$?
- Classification according to groups?
- How many?

Difference sets

Definition

- G group of order v (here: abelian).
- $D \subseteq G$ subset of size k.
- $g = d - d'$ has exactly λ solutions $d, d' \in D$ for all $g \neq 0$.

Then D is a (v, k, λ)-difference set in G.

Example

- $D = G$ is a (v, v, v) difference set.
- $D = G \setminus \{g\}$: $(v, v-1, v-2)$ difference set.
- $D = \{0, 1, 3\}$ in $\mathbb{Z}_7$: $(7, 3, 1)$ difference set.

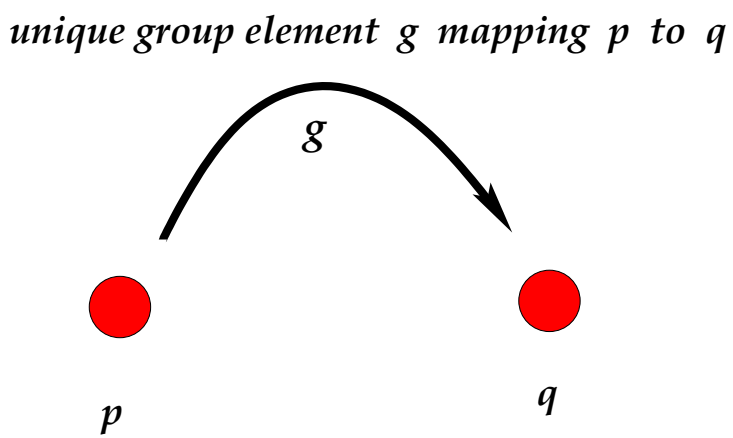
Difference sets and planes

The existence of an $(n^2 + n + 1, n + 1, 1)$-difference set gives rise to a plane of order n:

- Points: elements in G.
- Lines: shifts $D + g := \{d + g \ : \ d \in D\}$.

shift plane corresponding to D in G.

G acts a regular automorphism group on its shift plane.



Difference sets and planes (cont'd)

Theorem

A plane is a shift plane if and only if it has an automorphism group acting regularly on points and lines.

Example

Desarguesian plane is a shift plane: Regular group is

$$\mathbb{F}_{q^3}^*/\mathbb{F}_q^*.$$

Conjecture

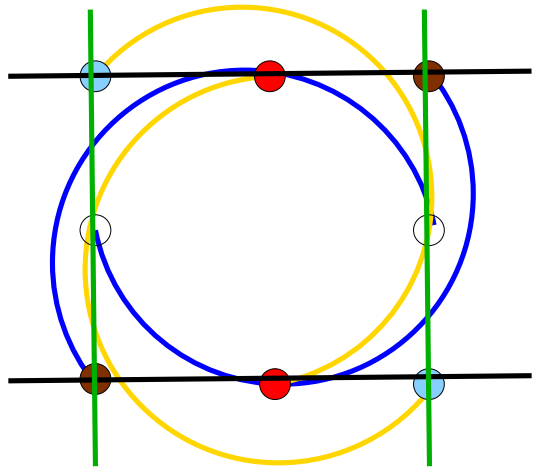
Shift planes are Desarguesian (HUANG, SCHMIDT 2008). *If G is abelian, then G is cyclic.*

Even under the difference set assumption the prime power conjecture is open. (GORDON 1998)

Residual planes

Delete one line l and all lines through P (P not on l).

$n^2 - 1$ points and lines. However: Some points are not joined by a line any more:



Question

Has this residual plane a difference set type representation?

Relative Difference Sets

Definition

- Group G of order mn with subgroup N of order n.
- $D \subseteq G$ of order k.
- $g = d - d'$ has λ solutions for $g \in G \setminus N$ and no solution for $g \in N$.

Then D is a relative (m, n, k, λ) difference set with forbidden subgroup N.

Example ($(4, 2, 3, 1)$-difference set)

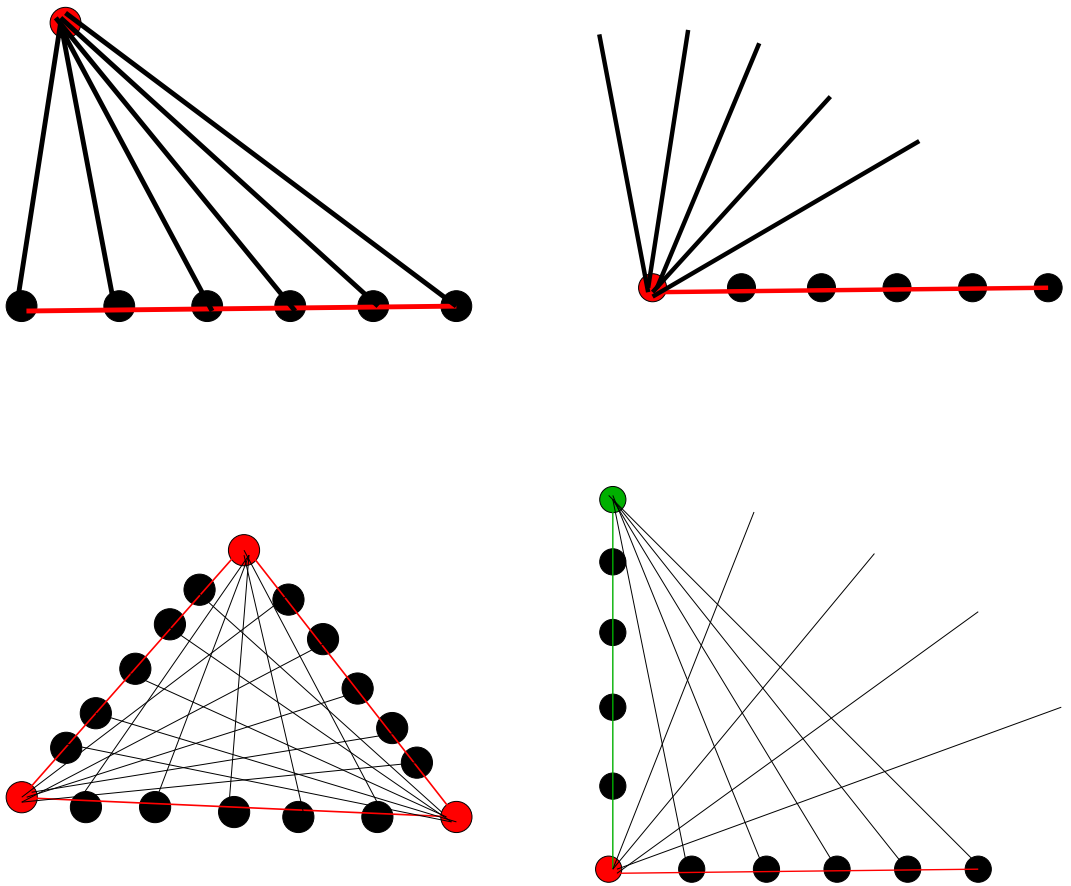
$\{0, 1, 3\} \subset \mathbb{Z}_8$ with forbidden subgroup $\{0, 4\}$.

Relative difference sets (cont'd)

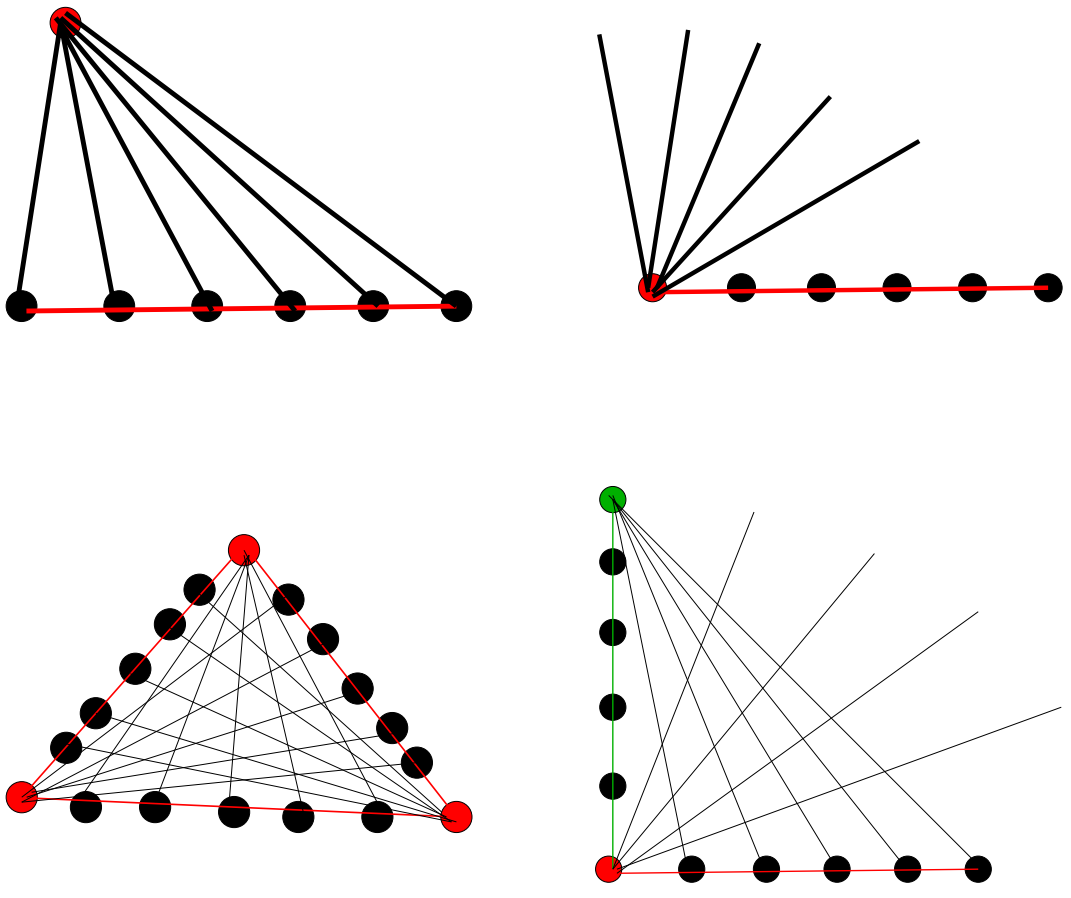
"Relative difference sets with $\lambda = 1$ describe residuals of projective planes!"

One may extend the concept to more than just one forbidden subgroup!

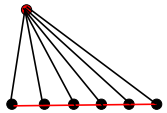
Four types of residuals



These are all! DEMBOWSKI, PIPER 1968



affine difference sets



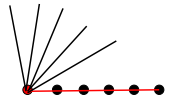
$n^2 - 1$ points, one forbidden subgroup of order $n - 1$.

Example

$$\{x \in \mathbb{F}_{q^2}^* \ : \ x + x^q = 1\}$$

$n = 2$: $\{1, 2, 4\}$ in $\mathbb{Z}_8$.

semifield planes



n^2 points, one forbidden subgroup of order n

Example

$$\{(x, x^2) \in \mathbb{F}_q \times \mathbb{F}_q \ : \ x \in \mathbb{F}_q\}$$

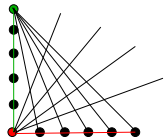
$n = 3$: $\{(0,0),(1,1),(2,1)\}$ in $\mathbb{Z}_3 \times \mathbb{Z}_3$, forbidden subgroup $\{0\} \times \mathbb{Z}_3$. additive/additive

Function F between additive groups of a field such that

$$F(x + a) - F(x)$$

is a permutation (planar functions), for instance $F(x) = x^2$.

nearfield planes



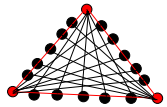
$n^2 - n$ points, one forbidden subgroup of order n, one of order $n - 1$.

Example

$$\{(x, x) \in \mathbb{F}_q^* \times \mathbb{F}_q \ : \ x \in \mathbb{F}_q^*\}$$

$n = 4$: $\{(1,2),(2,4),(3,3),(0,1)\}$ in $\mathbb{Z}_4 \times \mathbb{Z}_5$
multiplicative/additive or additive/multiplicative

neofield planes



$(n-1)^2$ points, three forbidden subgroups of order $n-1$.

Example

$$\{(x, 1-x) \in \mathbb{F}_q^* \times \mathbb{F}_q^* \ : \ x \in \mathbb{F}_q, x \neq 0, 1\}$$

$n = 5$: $\{(1,2),(2,0),(0,3)\}$ in $\mathbb{Z}_4 \times \mathbb{Z}_4$

multiplicative/multiplicative

Difference set is graph of a function $F : \mathbb{F}_q^* \to F_q^*$

Projections

D relative difference set in G with forbidden subgroup N.

$$\varphi : G \to G/U, \quad U \leq N$$

maps D to a subset of G/U.

Difference properties of D carry over to difference properties of $\varphi(D)$ in G/U.

Bent functions from planar function $F(x) = x^2$ on F_q, $q = p^m$

The planar function

$$\{(x, F(x)) \in \mathbb{F}_q \times \mathbb{F}_q \ : \ x \in \mathbb{F}_q\}$$

gives bent functions $f(x)$:

$$\{(x, \mathrm{tr}(F(x)) \in \mathbb{F}_q \times \mathbb{F}_p \ : \ x \in \mathbb{F}_q\}$$

The bent function is $f(x) = \mathrm{tr}(F(x)) = \mathrm{tr}(x^2)$.

Bent: $f(x + a) - f(x)$ is balanced!
Follows from: $F(x + a) - F(x)$ permutation.

Sidelnikov sequences

Graph of $F(x) = 1 - x$

$$\{(x, 1-x) \in \mathbb{F}_q^* \times \mathbb{F}_q^* \ : \ x \in \mathbb{F}_q^* \setminus \{0, 1\}\}$$

gives rise to

$$\begin{array}{rccc} f: & \mathbb{Z}_{q-1} & \to & \mathbb{Z}_2 \\ & x & \mapsto & \chi(1-x) \end{array}$$

where χ is a quadratic character: Obtain sequence with perfect (very small!) autocorrelation.

One proof $\{(x, 1-x) : x \neq 0, 1\}$

$$\frac{x}{y} = a \quad \text{and} \quad \frac{1-x}{1-y} = b.$$

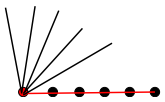
$$\frac{1-ay}{1-y} = b, \qquad 1-ay = b-by, \qquad \frac{1-b}{a-b} = y$$

except $b = 1$ or $a = 1$ or $a = b$.

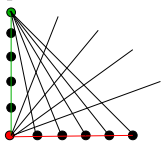
$$DD^{-1} = n + G - N_1 - N_2 - N_3$$

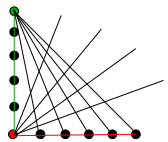
with $N_1 := \{(x, 1)\}$, $N_2 := \{(1, x)\}$, $N_3 = \{(x, x)\}$. Then apply partial characters.

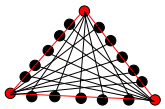
Main observation

bent functions (additive/additive, q odd) 

Legendre sequences (additive/multiplicative, q odd) using

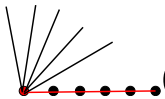
quadratic character 

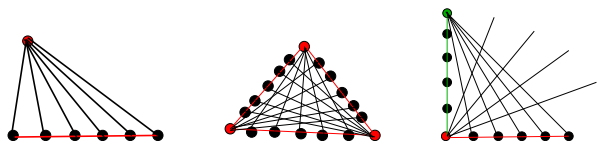
m-sequences (multiplicative/additive) using tr 

Sidelnikov sequences (multiplicative/multiplicative) 

All these objects can be derived from the Desarguesian plane!

Comments

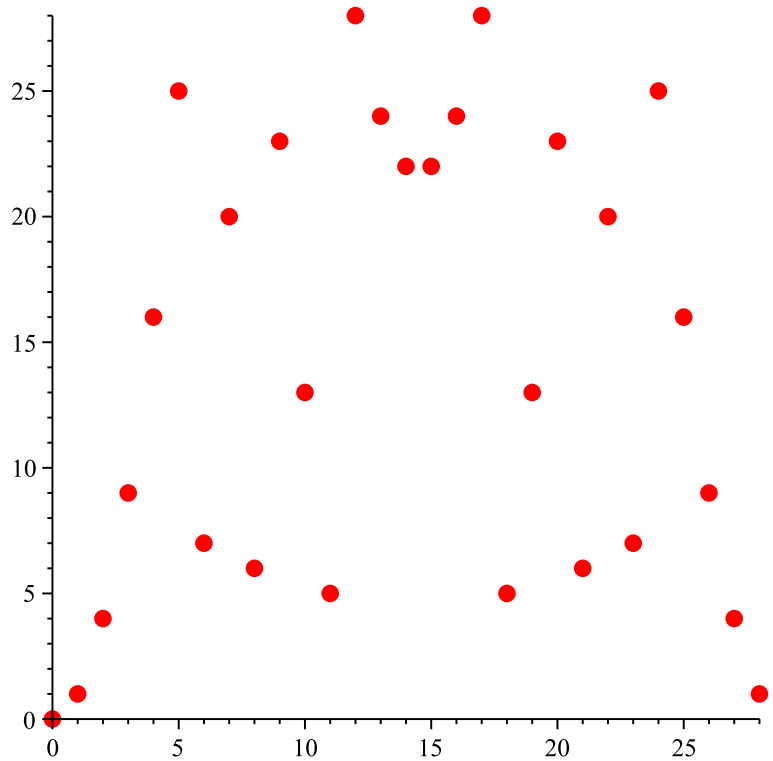
- New constructions from planes: Only in this  case ZHOU, P. since 2010.
- But: Are the known constructions part of a bigger vectorial picture? P., Zhou 2010
- Classification and Nonexistence.
- Ternary (or almost) sequences:



several authors, including TAN, ZHOU, ÖZBUDAKH

additive/additive, planar function x^2

$q = 29$



- Projection onto $\{0\} \times \mathbb{Z}_q$ can be used to prove prime power conjecture! BLOKHUIS, JUNGNICKEL, SCHMIDT 2002
- Projection onto $\{0\} \times \mathbb{Z}_q$ gives interesting Hadamard difference sets DING, WANG 2007

Vectorial Constructions

- $G = 2^s(2^n - 1)$, subgroups N_1 and N_2
- $N_1 = 2^s$, $N_2 = 2^n - 1$.
- $D \subseteq G$, list of nonzero differences covers $G \setminus (N_1 \cup N_2)$ uniformly, no element in N_1, N_2.
- D can be described as the graph of a function $F : N_2 \to N_1$.

Then $\mathrm{tr}(a \cdot F(x))$ is a 2-level autocorrelation function for all a (like an m-sequence).

Theorem

Gordon-Mills-Welch sequences are "vecorial" with $s|n$.

What about the other examples of 2-level autocorrelation functions?

- $(p^m, p^m, p^m, 1)$-difference sets (only p odd)
  - semifield planes
  - many examples if m even
  - not so many if m is odd
- $(p^m, p^{m/2}, p^m, p^{m/2})$-difference sets
  - vectorial bent functions
  - millions of examples.
- $(p^m, p^{(m-1)/2}, p^m, p^{(m-1)/2})$-difference sets
  - vectorial bent functions
  - Existence: ??
- (p^m, p, p^m, p^{m-1})-difference sets
  - bent functions
  - zillions of examples
- $(p^m, p^{(m+1)/2}, p^m, p^{(m+1)/2})$-difference sets
  - Existence: ??
- $(p^m, p^{m/2+1}, p^m, p^{m/2+1})$-difference sets
  - Existence: ??

Conclusion

- Sidelnikov, Legendre, m-sequences and p-ary bent functions are all related to Desarguesian plane.
- Vectorial versions of sequences and functions.
- New types of sequences.
- Classification of planes.
- New interesting problems about vectorial versions.