Univ. u Novom Sadu
Zb. Rad. Prirod.–Mat. Fak.
Ser. Mat. 24, 2 (1994), 95-99

Review of Research
Faculty of Science
Mathematics Series

A METHOD FOR CONSTRUCTION OF BLOCKS OF $PG_2(3,2)$ AND $PG_3(4,2)$

Vojislav Mudrinski
Institute of Mathematics, University of Novi Sad
Trg Dositeja Obradovića 4, 21000 Novi Sad, Yugoslavia

Abstract

We describe a simple method for construction of blocks of projective spaces $PG_{n-1}(n,2)$. The method uses an irreducible polynomial p of degree $n+1$ over $GF(2)$, which is "good" in the sense that the degrees x^0, x, x^2, ..., $x^{2^{n+1}-2}$, reduced by p , are all different non-zero binary polynomials of degree at most n. We found "good" polynomials for $n=3$ and $n=4$, which gave the blocks of $PG_2(3,2)$ and $PG_3(4,2)$.

AMS Mathematics Subject Classification (1991): 05B25
Key words and phrases: block design, finite projective geometry

1. Preliminaries

$PG(n,q)$ ($n-$ *dimensional projective space* over $GF(q)$) ([1]) is the set of all subspaces of an $(n+1)-$dimensional vector space over $GF(q)$. $PG_d(n,q)$ denotes an incidence structure, the points and the blocks of which are respectively $1-$dimensional and $(d+1)-$dimensional subspaces of $PG(n,q)$.

In this paper we shall deal merely with the case $q=2$ and $d=n-1$.

A t-(v,k,λ) *design* ([2]) is an incidence structure on v points, which consists of some $k-$sized sets of points (called *blocks*) without repetitions and which satisfies the property that each t points is contained in exactly λ blocks. The projective space $PG_{n-1}(n,2)$ ([1]) is a 2-$(2^{n+1}-1, 2^n-1, 2^{n-1}-1)$ design. It is known that this design is *symmetric* in the sense that the number of its points (v) is equal to the number of blocks.

A *Singer group* G of a symmetric 2-(v,k,λ) design $\mathcal{D}$ is a subgroup of the group $Aut(\mathcal{D})$ of all automorphisms of $\mathcal{D}$, which satisfies the following two conditions:

- G operates transitively both on the points and the blocks of D
- the identity is the only permutation of G, which has fixed points

Theorem 2.10 from [2] says that $PG_{n-1}(n,2)$ has a cyclic Singer group for $n \geq 2$.

A *difference set* of a Singer group G is a set $D(P,y) = \{g \in G \mid g(P) \in y\}$, where P is a point and y is a block of the associated symmetric 2-(v,k,λ) design.

Some symmetric 2-(v,k,λ) designs can be constructed by using the Singer group and a difference set $D(P,y)$. The difference set can be easily bijected to a block, which initializes the design. In particular, if the Singer group is cyclic and the point set is $S_v = \{0,...,v-1\}$, then all the blocks of the design can be obtained from some block y as the sets with the elements $(a+i) \bmod v$, where a stands for an arbitrary element of the block y, while i is an element of the set S_v.

However, on the page 65 of [2] the author writes:
"Notice that although Theorem 2.10. guarantees the existence of a cyclic Singer group H, it does not help us much to find a difference set for H. In fact, the practical problem of finding difference sets is very difficult".

2. Construction

The cyclic Singer group of $PG_{n-1}(n,2)$, the existence of which was proved by Theorem 2.10 from [2], is a group of transformations of the form:

$$w \rightarrow w * f , \qquad (1)$$

where w and f are $(n+1)$-dimensional binary vectors.

Let v denote a non-zero polynomial of the form

$$v = v_0 + v_1 \cdot x + ... + v_n \cdot x^n ,$$

where $v_i \in \{0,1\}$ for $0 \leq i \leq n$.

We suggest the transformation (1) to be replaced by the mapping

$$v \rightarrow v \cdot x \pmod{p} \qquad (2),$$

where p is an irreducible binary polynomial of degree $n+1$, which is "good" in the sense that the degrees $1 = x^0, x, x^2, ..., x^{2^{n+1}-2}$, reduced by p, are all different non-zero binary polynomials of degree $\leq n$ (denote these polynomials by $p_1, p_2, ..., p_{2^{n+1}-1}$ respectively).

A block [1] of $PG_{n-1}(n,2)$ can be constructed as the set of all those 2^n-1 polynomials p_i, which are of degree $\leq n-1$. This is in accordance with the fact that the blocks are hyperplanes of the geometry. Each hyperplane may be viewed as the algebraic closure of the set, which is obtained by excluding one element from a base of the vector space. We choose the base to be $\{1, x, x^2, ..., x^n\}$ and the excluded element to be x^n. The "goodness" of the polynomial p provides that the cyclic automorhism group generated by the mapping (2) is transitive (which implies that it is a Singer group).

3. The blocks of $PG_2(3,2)$ and $PG_3(4,2)$

In this section we apply the above construction of blocks of $PG_{n-1}(n,2)$ to the cases $n = 3$ and $n = 4$ (the case $n = 2$ corresponds to the well-known Fano geometry). Our hypothesis is that the construction can be generalized to the cases $n > 4$ as well.

[1] also the corresponding difference set

3.1. Case $n = 3$

We have found that the irreducible binary polynomial $p = 1 + x + x^4$ is "good". This polynomial gave us the following initial block for the construction of $PG_2(3,2)$:

$$(p_1, p_2, p_3, p_5, p_6, p_9, p_{11}) = (1, x, x^2, 1+x, x+x^2, 1+x^2, 1+x+x^2).$$

Let the numbers "1","2",...,"15" be the abbreviations for the polynomials p_1, p_2, ... , p_{15} respectively. The complete list of blocks of $PG_2(3,2)$ looks as follows:

(1,2,3,5,6,9,11)	(2,3,4,6,7,10,12)	(3,4,5,7,8,11,13)
(4,5,6,8,9,12,14)	(5,6,7,9,10,13,15)	(1,6,7,8,10,11,14)
(2,7,8,9,11,12,15)	(1,3,8,9,10,12,13)	(2,4,9,10,11,13,14)
(3,5,10,11,12,14,15)	(1,4,6,11,12,13,15)	(1,2,5,7,12,13,14)
(2,3,6,8,13,14,15)	(1,3,4,7,9,14,15)	(1,2,4,5,8,10,15)

This is an explicit representation of $PG_2(3,2)$ as a 2-$(15,7,3)$ design.

We have also found that $p = 1 + x + x^2 + x^3 + x^4$ is an example of an irreducible binary polynomial of degree $n+1$, which is not "good". More precisely, it turns out that the polynomials p_i, p_{i+5} and p_{i+10} coincide for $i = 1, 2, ..., 5$. This implies that the mapping (2) does not give a Singer group (it gives merely a cyclic group of order 5).

3.2. Case $n = 4$

The blocks of $PG_3(4,2)$ can be analogously obtained from the "good" irreducible binary polynomial $p = 1 + x^2 + x^5$.

We have obtained the following initial block:

$$(p_1, p_2, p_3, p_4, p_6, p_7, p_9, p_{12}, p_{13}, p_{19}, p_{20}, p_{21}, p_{24}, p_{28}, p_{30}).$$

Acknowledgement. I am thankful to prof. Dragan Acketa for calling "non-good" polynomials to my attention.

References

[1] Beth, T., Jungnickel, D., Lenz, H., Design theory, Bibliographisches Institut Mannheim/Wien/Zürich, 1985.

[2] Hughes D.R., Piper F.C., Design theory, Cambridge University Press, 1985.

Received by the editors October 10, 1992.