How to Overcome the Combinatorial Explosion in the Construction of Block Designs*

(To the 60^{th} Anniversary of Prof. Dr. Zvonimir Janko)

Mario Essert

Faculty of Mechanical Engineering and Naval Architecture, Zagreb, Croatia

The construction of the symmetric block design (v, k, λ) with larger parameters $(k \geq 9)$ is a huge computational problem. This article describes one method which improves the computational task of the construction in regard to the computer memory and time requirements. This method has been described for the construction of the $(71, 21, 6)$ block design on which operates the Frobenius group of order 21.

Keywords: Incidence Structure, Indexing, Prepared Vectors

1. Introduction

The central part of discrete mathematics today is the construction of block designs, as a special case of incidence structures. An *incidence structure* $\mathscr{D} = (\mathscr{P}, \mathscr{B}, I)$ consists of two finite sets: a point set $\mathscr{P}$ and a line set $\mathscr{B}$, on which the incidence relation $I \subseteq \mathscr{P} \times \mathscr{B}$ is given. Let $P \in \mathscr{P}, x \in \mathscr{B}$. We say that P is on x (or that x is going through P) if $(P, x) \in I$.

A symmetric block design with parameters (v, k, λ) is an incidence structure which consists of v subsets (called blocks or lines) of k elements (called points) taken from a set of v elements such that any two blocks contain exactly λ elements (*Beutelspacher*, 1982, *Hughes & Piper*, 1985). For $P \in \mathscr{P}$ and $x \in \mathscr{B}$ we denote all the blocks through the point P as $\langle P \rangle = \{y \in \mathscr{B} | (P, y) \in I\}$, and all the points which are on the line x as $\langle x \rangle = \{Q \in \mathscr{P} | (Q, x) \in I\}$. A *symmetric block design* with parameters (v, k, λ) can be now defined as:

$$|\mathscr{P}| = |\mathscr{B}| = v, \qquad (1)$$

$$|\langle x \rangle| = |\langle P \rangle| = k \quad \text{for all } x \in \mathscr{B}, P \in \mathscr{P}, \qquad (2)$$

$$|\langle x \rangle \cap \langle y \rangle| = |\langle P \rangle \cap \langle Q \rangle| = \lambda \quad \text{for all } x, y \in \mathscr{B},\ x \neq y \text{ and } P, Q \in \mathscr{P}, P \neq Q. \qquad (3)$$

We call the conditions (3) *the consistence conditions.*

Construction of such designs with larger parameters $(k \geq 9)$ can usually be done with a computer, but even so, due to an extremely large number of combinatorial possibilities, certain additional assumptions have to be used to speed up the process of construction. The basic assumption is that a certain automorphism group $\mathscr{G}$ operates on the design. That leads to the method of using *tactical decomposition* for the construction of orbit structures (*Janko*, 1986, *Ćepulić*, 1990).

Let $\mathscr{G} \leq \operatorname{Aut} \mathscr{D}$ be an (incidence preserving) automorphism group of $\mathscr{D}$. Then $\mathscr{P} = \cup \mathscr{P}_i = \cup P_i \mathscr{G}$ and $\mathscr{B} = \cup \mathscr{B}_j = \cup x_j \mathscr{G}$ are the partitions of $\mathscr{P}$ and $\mathscr{B}$ into $\mathscr{G}$-orbits, with representatives $P_i \in \mathscr{P}$ and $x_j \in \mathscr{B}$. (Symbol $\cup$ denote union of disjoint sets).

We denote the length of particular orbits with $|\mathscr{P}_i| = \omega_i$ and $|\mathscr{B}_j| = \Omega_j$. These two partitions

* This work was supported by the Commission of European Communities, EC — Postdoctoral Fellowship, Contract: CI1/0587, and was made at Mathematical Institute, University Heidelberg.

define a tactical decomposition of $\mathscr{D}$.

2. The Orbit Structures

The first step in the construction of symmetric block designs is the construction of orbit structures. Only those block designs which have an orbit structure can be fully constructed. *The orbit structure* is the matrix (μ_{ij}) or dually (M_{ij}) where $\mu_{ij} = |\langle x\rangle \cap \mathscr{P}_i|$, $x \in \mathscr{B}_j$ and $M_{ij} = |\langle P\rangle \cap \mathscr{B}_j|$, $P \in \mathscr{P}_i$. It can be proved (see [3]) that the following holds:

$$\sum_i \omega_i = \sum_j \Omega_j = v \tag{4}$$

$$\sum_i \mu_{ij} = \sum_j M_{ij} = k \tag{5}$$

$$[x_j, x_j] := \sum_i \mu_{ij}(M_{ij}-1) = \lambda(\Omega_j-1) \tag{6}$$

$$[x_j, x_k] := \sum_i \mu_{ij} M_{ik} = \lambda\Omega_k \tag{7}$$

$$\omega_i M_{ij} = \Omega_j \mu_{ij} \tag{8}$$

In the method of construction of orbit structures V. Ćepulić introduced canonical forms for lines and designs (see [3]). Using the formula (6) we construct all possible (lexicographically ordered) x_j types which belong to the particular line orbit $\mathscr{B}_j$ (layer) and satisfy $[x_j, x_j]$ which we call the *inner product*. The next step is building the partial orbit structures $\mathscr{D}_P$, layer by layer, satisfying (7). This consistence condition for lines from different layers $[x_j, x_k]$ is called *outer product* (see [10], [11], [12]). Each line must be consistent with all previous lines of the considered beginning orbit structure. If there exists some $\alpha \in N_S(\mathscr{G})$ such that $\mathscr{D}_P\alpha < \mathscr{D}'_P$, we can ommit such $\mathscr{D}'_P$, retaining only those $\mathscr{D}_P$ among the isomorphic ones, which are the first in the sense of the defined precedence (α denotes the element from the group normalizer $N_S(\mathscr{G})$ of $\mathscr{G}$ in the symmetric group S over the set $\mathscr{P} \cup \mathscr{B}$). A good convergence of the construction process is obtained in many cases by eliminating a lot of isomorphic designs (*Essert*, 1992) in such a way.

Each orbit can be denoted by an orbit mark (the big number), so the orbit structure can also be represented by explicitely writing an orbit mark, as many times as there are points μ_{ij} in the particular point orbit $\mathscr{P}_i$. In this way we obtain a line representative with k points.

At this moment we can not distinguish the points which belong to the same orbit. Therefore, each point must be supplied with an *index*. This second process of the construction we call *indexing*.

Example

Suppose that the nonabelian group $\mathscr{G}$ of order 21 (the so called Frobenius group) operates on the design (71,21,6). We denote this group with

$$\mathscr{F}_{21} = \langle \rho, \mu \mid \rho^7 = \mu^3 = 1, \rho^\mu = \rho^2\rangle$$

The subgroups $\langle\rho\rangle$ and $\langle\mu\rangle$ are represented as permutation groups on the indices for each orbit. The group operation on each line representative provides the ρ-images of each index and so the ρ-images for each line.

The action of a subgroup $\langle\rho\rangle$ of order 7 of $\mathscr{G}$ on 71 points is:

$$\rho = \{(\infty)(I_0, I_1, I_2, I_3, I_4, I_5, I_6),$$
$$I = \mathsf{1, 2, 3, 4, 5, 6, 7, 8, 9, 10}\},$$

where I (an orbital mark, the big number) denotes a particular orbit. Note that there are ten orbits of length 7 and one of length 1. One orbit structure, among the 28 constructed, is shown below:

	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}
I	∞	1	2	3	4	5	6	7	8	9	10
b_0	0	7	7	7	0	0	0	0	0	0	0
b_1	0	4	1	1	3	3	3	3	1	1	1
b_2	0	1	4	1	0	3	3	3	1	1	1
b_3	0	3	3	0	3	1	1	1	3	3	3
b_4	0	3	0	3	0	2	2	2	3	3	3
b_5	1	2	2	2	2	1	2	3	0	2	4
b_6	1	2	2	2	2	2	3	1	2	4	0
b_7	1	2	2	2	2	3	1	2	4	0	2
b_8	0	1	2	3	3	0	4	2	3	1	2
b_9	0	1	2	3	3	4	2	0	1	2	3
b_{10}	0	1	2	3	3	2	0	4	2	3	1

The point orbits we denote with p_i, line orbits with b_i and the length of orbits with ω_i . The orbits of length one are usually denoted with ∞ (fixed points), and the others with big numbers. It is easy to see that the equations (4)–(8) are satisfied. See also that the line representative, for example b_2, can be represented by the big numbers as:

1 2 2 2 2 3 5 5 5 6 6 6 7 7 7 8 9 10

3. Indexing

The process of setting indices on big points and lifting an orbit structure by means of a permutation group, so that the consistence conditions are satisfied, is called *indexing*.

To obtain a design, all line images must be mutually consistent. The consistence condition for this inner product, also called “Hamming length”, is following from (6) as:

$$H(b_i) = (|\rho| - 1)(\lambda - f_i), \qquad (9)$$

where f_i is the number of fixed points of line b_i and $|\rho|$ is the order of automorphism ρ.

Two line representatives which belong to different orbits with indices which satisfy (9), must also be mutually consistent. This outer product follows from (7) and is often called “Game (germ. Spiel) product”:

$$Sp(b_i, b_j) = |\rho|(\lambda - f_{i,j}), \qquad (10)$$

where $f_{i,j}$ is the number of fixed points which are common for b_i and b_j, $i \neq j$.

The first step of the construction is to obtain all indices for the particular line orbit which satisfy (9). The second step is to connect successively the line orbits by means of the condition (10).

4. The Method of Saved Vectors

The problem which arises is that very quickly the number of correct solutions becomes astronomically large. The mathematical answer to this combinatorial explosion is the usage of the automorphisms which normalize our group $\mathscr{G}$, and *reduce indices*. The computational answer is to prepare relevant information in the computer memory, before the process of the construction begins.

From the group multiplication table *GMT* of order *DIM*, we can construct the new incidence table IT, which shows us when two points from the same orbit are incident in the lifting process. The C-program (with the variables i, $i1$ and j) for this action is:

```
for(i=0; i<DIM; i++)
  for(j=0; j<DIM; j++)
    for(i1=0; i1<DIM; i1++)
      if (i == GMT[i1][j]) {
        IT[i][j]=i1;
        break;
      }
```

Using this table IT as the argument in the function HAMM we have constructed for the particular $\langle x_j \rangle \cap \mathscr{P}_i = \mathscr{P}_{ix}$ one vector (INCV) consisting of the numbers of incidences. Obviously, $|\mathscr{P}_{ix}| = \mu_{ij}$. If there are t-point orbits, we also have to construct t vectors for every line representative. But, since the same μ_{ij} usually appears several times in the same line (and also in the other line orbits), our generated vectors can be used for all of them (i.e. for their related $\mathscr{P}_{ix}$). The C-program for this function is:

```
void HAMM(Pi,Wi,IT,INCV)
  int *Pi, Wi;  /* the set 𝒫ix and
                   its length Wi*/
  int (*IT)[DIM];  /* the table of
                   incidence */
  int *INCV;      /* the resulted vector */
{
  int i1, i2, a, b;
  for (i1=0; i1<Wi; i1++) {
    a=Pi[i1];
    for (i2=i1+1; i2<Wi; i2++) {
      b=Pi[i2];
      INCV[IT[b][a]]++;
      INCV[IT[a][b]]++;
    }
}
  }    /* hamm */
```

The investigation of the inner product in this way is reduced to in summing t vectors with the condition that in all vector elements (except null) the sum must be λ.

Example

For the cyclic automorphism ρ of order 7 the incidence table IT will be:

IT	0	1	2	3	4	5	6
0	0	6	5	4	3	2	1
1	1	0	6	5	4	3	2
2	2	1	0	6	5	4	3
3	3	2	1	0	6	5	4
4	4	3	2	1	0	6	5
5	5	4	3	2	1	0	6
6	6	5	4	3	2	1	0

For the two indices from the same orbit, for example, 2 and 6, the incidence will be at 3^{rd} and 4^{th} step (see IT(2,6) and IT(6,2)). For the

1_0	1_1	1_2	1_4	2_0	3_0	4_1	4_2	4_4	5_0	5_1	5_5	6_0	6_4	6_6	7_0	7_2	7_3	8_0	9_0	10_0
1_0	2_0	2_3	2_5	2_6	3_0	5_2	5_5	5_6	6_1	6_6	6_3	7_4	7_3	7_5	8_4	8_6	9_2	9_3	10_1	10_5
1_1	1_2	1_4	2_3	2_5	2_6	4_3	4_5	4_6	5_0	6_0	7_0	8_3	8_4	8_5	9_5	9_2	9_6	10_6	10_1	10_3
1_1	1_2	1_4	3_1	3_2	3_4	5_3	5_5	6_5	6_6	7_6	7_3	8_2	8_5	8_6	9_1	9_6	9_3	10_4	10_3	10_5
∞	1_4	1_5	2_0	2_5	3_3	3_6	4_3	4_4	5_0	6_4	6_5	7_1	7_3	7_6	9_2	9_4	10_1	10_2	10_4	10_5
∞	1_1	1_3	2_0	2_3	3_6	3_5	4_6	4_1	5_1	5_3	6_2	6_6	6_5	7_0	8_4	8_1	9_2	9_4	9_1	9_3
∞	1_2	1_6	2_0	2_6	3_5	3_3	4_5	4_2	5_4	5_5	5_3	6_0	7_2	7_6	8_4	8_1	8_2	8_6	10_1	10_2
1_5	2_2	2_4	3_0	3_4	3_6	4_2	4_3	4_6	6_0	6_2	6_5	6_6	7_5	7_6	8_0	8_4	8_6	9_0	10_1	10_3
1_3	2_4	2_1	3_0	3_1	3_5	4_4	4_6	4_5	5_0	5_4	5_3	5_5	6_3	6_5	8_0	9_2	9_6	10_0	10_1	10_5
1_6	2_1	2_2	3_0	3_2	3_3	4_1	4_5	4_3	5_6	5_3	7_0	7_1	7_6	7_3	8_4	8_5	9_0	9_2	9_3	10_0

Fig. 1

tree indices, for example 2, 3, and 6, the lifting process will be: $236 \to \underline{3}40 \to 451 \to 5\underline{62} \to \underline{6}0\underline{3} \to 014 \to 1\underline{2}5$ which gives the incidence vector: 0 1 0 2 2 0 1, i.e. there are one incidence in the first and sixth step, and two incidences in the third and fourth step. It is easy to see that the *HAMM* function will give the same answer. For IT(2,3)=6 — increment the sixth element of the originally cleaned vector INCV, IT(3,2)=1 — increment the first element (vectors in the C language have the null element), IT(2,6)=3 — for the third element, and so on: (6,2)=4, (3,6)=4, (6,3)=3.

Since these operations are equal for all equal indices, no matter in which orbit they appear, the idea is to make and store these vectors for all $\mathscr{P}_{ix}$ (with different lengths) before the process of the construction begins.

The analogous operation of the vector generation (*SIV*) can be applied for the outer products, equation (10), using the C-function:

```
void SPIEL(Pi,Wi,Pj,Wj,IT,SIV)
  int *Pi, Wi;
  int *Pj, Wj;
  int (*IT)[DIM];
  int *SIV;
/* outer product for the sets $\mathscr{P}_{ix}$ from the
$i$-point orbit of line $x$ and the sets $\mathscr{P}_{iy}$
from the same $i$-point orbit of line $y$ */
{
  int i1, i2, a, b;
  for (i2=0; i2<Wj; i2++) {
    b=Pj[i2];
    for (i1=0; i1<Wi; i1++) {
      a=Pi[i1];
      SIV[IT[b][a]]++;
    }
  }
} /* Spiel */
```

Note that for the outer product the null element of the summed vector must also be λ.

5. The Construction

The first step of the construction is to obtain all indices which satisfy equation (9) — joining and summing the saved vectors for all point orbits of the particular line orbit. The second step is to apply the group normalizer and centralizer to the resulted vectors. The third step is to connect successively vectors of line orbits by means of condition (10). The result for our example is (71,21,6) design (*Ademaj, Essert*, 1992), given by its line representatives (Fig. 1)

Each orbit could be fully obtained by simple incrementing modulo 7 for each index in the block representative.

Acknowledgement

I would like to thank my supervisor, professor dr. Zvonimir Janko, for his kindly guidance and assistance.

References

[1] ADEMAJ, E. and ESSERT, M. (1992), *Classification of Symmetric Block Designs for (71,21,6) with Frobenius group of order 21* , preprint

[2] BEUTELSPACHER, A. (1982), *Einführung in die endliche Geometrie I*, Verlag Mannheim, Wien, Zurich

[3] ĆEPULIĆ, V. (1990), *Construction of designs* , preprint, Zagreb

[4] ĆEPULIĆ, V. and ESSERT, M. (1988), *Biplanes (56,11,2) with automorphism group $Z_2 \times Z_2$ fixing some point* , Journal of Comb. Theory, Series A 48(2), pp. 239–246.

[5] ĆEPULIĆ, V. and ESSERT, M. (1988), *Biplanes (56,11,2) with automorphisms of order 4 fixing some point* , Discrete Mathematics 71, Vol 71, pp. 9–17

[6] ESSERT, M. (1992), *The algorithm for elimination of isomorphic orbital structures* , Int. Journal of Computer Math., Vol. 42, pp. 1–5

[7] ESSERT, M. (1990), *An efficient algorithm for saving ordered sets in a compacted form* , Int. J. of Computer Math., Vol. 34, pp. 65–70

[8] HUGHES, D. R. and PIPER, F. C. (1985), *Design theory*, Cambridge University Press, Cambridge.

[9] JANKO, Z. and TRAN, VAN T. (1986), *A new biplane of order 9 with a small automorphism group* , J. of Combin. Theory, Series (A), Vol.42

[10] JANKO, Z. and TRAN, VAN T. (1985), *Construction of the symmetric block design for (71,21,6)* , Discrete Mathematics, Vol. 55, pp. 327–328.

[11] MARANGUNIĆ, LJ. (1992), *Biplanes (79,13,2) with Involutory Automorphism* , J. of Comb. Theory, Series A, Vol. 61, pp. 36–49.

[12] ŠIFTAR, J. (1989), *Nonexistence of a 2–(22,8,4) design with an automorphism of order 3* , Glasnik Matematički, Vol. 24 (44), pp. 3–10.

Received: June, 1993
Accepted: , November 1993

Contact address:
Mario Essert
Faculty of Mechanical Engineering
and Naval Architecture,
Đ. Salaja 1,
41000 Zagreb, Croatia
Telephone +385 41 611–944 / 434
Fax +385 41 514–535
Telex 22648 fsb CROATIA
E-mail mario.essert@x400.srce.hr

MARIO ESSERT (1954) is an Assistant Professor in the Department of Control Eng. at the Faculty of Mechanical Eng. & Naval Arch., University of Zagreb. He received Ph.D. degrees (1987) in the computer science from the Faculty of Electrical Eng. (ETF) at the University of Zagreb. As a member of the Group of Discrete mathematics at ETF (led by prof. dr. V. Ćepulić) he participated in four international coprojects: Mainz (Germany), Kiev (Ukraina), Hangzou (China) and Heidelberg (Germany). His research interest include combinatorial algorithms, control engineering and computer mathematics.