Serdica J. Computing **1** (2007), 279–292

Serdica
Journal of Computing

Bulgarian Academy of Sciences
Institute of Mathematics and Informatics

ALGORITHMS FOR FINDING UNITALS AND MAXIMAL ARCS IN PROJECTIVE PLANES OF ORDER 16[*]

Stoicho D. Stoichev

Abstract. Two heuristic algorithms ($M65$ and $M52$) for finding respectively unitals and maximal arcs in projective planes of order 16 are described. The exact algorithms based on exhaustive search are impractical because of the combinatorial explosion (huge number of combinations to be checked). Algorithms $M65$ and $M52$ use unions of orbits of different subgroups of the automorphism group of the 273×273 bipartite graph of the projective plane. Two very efficient algorithms (developed by the author and not described here) are used in $M65$ and $M52$: (i) algorithm *VSEPARN* for computing the generators, orbits and order of the graph automorphism group; (ii) graph isomorphism algorithm derived from *VSEPARN*. Four properties are proved and used to speed up the algorithms $M65$ and $M52$. The results of these algorithms are published. After changing only the parameters of these algorithms they can be used for determining unitals in projective planes of different orders.

ACM Computing Classification System (1998): G.2.1.

Key words: Unital, Maximal arc, Projective plane, Graph isomorphism, Graph automorphism group, Algorithm.

[*] The paper has been presented at the International Conference Pioneers of Bulgarian Mathematics, Dedicated to Nikola Obreshkoff and Lubomir Tschakaloff , Sofia, July, 2006.

1. Introduction. We assume familiarity with the basics of the combinatorial designs (cf., e.g. [1]). A $t-(v,k,\lambda)$ *design* D [1] is a set X of points together with a family B of k–subsets of X called blocks with the property that every t points are contained in exactly λ blocks. The design with $t=2$ is called a *block–design.*

The block–design is *symmetric* if the role of the points and blocks can be changed and the resulting configuration is still a block–design. A *projective plane* of order n is a symmetric 2–*design* with $v=n^2+n+1$, $k=n+1$, $\lambda=1$. The blocks of such a design are called *lines.* A *unital* in a projective plane of order $n=q^2$ is a set U of q^3+1 points that meet every line in *one* or $q+1$ points. A *maximal* $\{n(m-1)+m,m\}$*–arc* of degree m in a projective plane of order n is a subset of $n(m-1)+m$ points such that every line meets the set in 0 or m points for some $2\le m\le n$ [2].

An algorithm ($M65$) for finding unitals with $q=4$ in projective planes of order $n=16$ is described. In this case the projective plane is $2-(273,17,1)$ design, the unital is a subset of $q^3+1=4^3+1=65$ points and every line meets 1 or 5 points from the subset.

The results from algorithm $M65$ for known planes of order 16 are given in [7]. By slight changes algorithm $M65$ has been transformed to algorithm $M52$ for finding maximal arcs of degree $m=4$ in projective planes of order 16. In this case the maximal arc is a subset of $n(m-1)+m=16.3+4=52$ points and every line meets the subset in 0 or 4 points. The results from this algorithm for known planes of order 16 are given in [2].

The numbers of the nonisomorphic unitals found by algorithm $M65$ are shown on Table 1 – the algorithm itself checks for nonisomorphism. Known are some unitals found by R. Mathon and shown on Table 2 (in private communication [5]). The total numbers of unitals found by algorithm $M65$ and R. Mathon are respectively 116 and 47. The comparison of the results from Table 1 and Table 2 gives: (i) full coincidence for planes PG(2,16), HALL and LMRH (ii) no unitals were found in planes JOHN, BBS4, DSFP, DEMP by R. Mathon (iii) the unitals found by R. Mathon are subsets of the unitals found by M65 for planes MATH, JOWK, SEMI2 and SEMI4 (iiii) the only 2 unitals not found by algorithm $M65$ and found by Mathon are the unital with automorphism group of order 4 for plane BBH1 and the unital of order 2 for plane BBH2.

Let $G(V,E)$, (V-set of vertices and E-set of edges) be a graph and subset $S\in V$. The *relative degree* $rd(x,S)$ of a vertex $x\in V$ to the subset S is the number of vertices adjacent to x and belonging to S.

A *partition* $P=C_1C_2\dots C_i\dots C_m$ of the set V is a set of disjoint non–

Table 1. Nonisomorphic unitals found by algorithm $M65$ (total number = 116)

Projective plane	$\|Aut(G)\|$	$\|Aut(U)\|$ – automorphism group orders of found unitals (times*order)	Number of found unitals
MATH	12288	$6 * 128$, $3 * 64$, $1 * 32$, $5 * 16$	15
JOHN	2304	$1 * 48$, $2 * 32$, $1 * 24$, $2 * 16$, $4 * 8$	10
BBH1	18432	$1 * 32$, $4 * 16$, $5 * 8$, $1 * 4$	11
PG(2, 16)	34217164800	$1 * 249600$, $1 * 768$	2
BBS4	3456	$4 * 8$, $2 * 4$	6
JOWK	258048	$1 * 48$, $1 * 32$, $1 * 24$, $1 * 16$, $1 * 12$, $1 * 8$, $1 * 4$	7
DSFP	92160	$1 * 24$, $1 * 12$	2
HALL	55296	$1 * 1200$, $1 * 100$, $1 * 80$, $1 * 48$, $1 * 32$, $1 * 16$	6
DEMP	921600	$1 * 48$, $1 * 24$, $1 * 16$	3
SEMI2	147456	$3 * 192$, $3 * 64$, $3 * 48$	9
SEMI4	884736	$1 * 192$, $3 * 128$, $1 * 64$, $1 * 48$, $2 * 12$, $3 * 8$	11
LMRH	258048	$1 * 32$, $1 * 16$	2
BBH2	3840	$2 * 80$, $4 * 32$, $2 * 20$, $8 * 16$, $1 * 10$, $8 * 8$, $7 * 4$	32

Table 2. Unitals found by R. Mathon (total number = 47, no unitals were found in planes JOHN, BBS4, DSFP, DEMP)

Projective plane	$\|Aut(G)\|$	$\|Aut(U)\|$ – automorphism group orders of found unitals	Number of found unitals by Mathon	Number of found unitals by M65
MATH	12288	$6 * 128$, $3 * 64$, $1 * 16$	10	15
BBH1	18432	$2 * 16$, $1 * 8$, $2 * 4$	5	11
PG(2, 16)		$1 * 249600$, $1 * 768$	2	2
JOWK	258048	$1 * 32$	1	7
HALL	921600	$1 * 1200$, $1 * 100$, $1 * 80$, $1 * 48$, $1 * 32$, $1 * 16$	6	6
SEMI2	147456	$3 * 192$	3	9
SEMI4		$1 * 192$, $2 * 128$, $1 * 12$, $1 * 8$	5	11
LMRH	258048	$1 * 32$, $1 * 16$	2	2
BBH2	3840	$1 * 80$, $1 * 20$, $3 * 16$, $2 * 8$, $5 * 4$, $1 * 2$	13	32

empty subsets C_i, $i = 1, 2, \dots, m$ called usually *cells* (*blocks or classes*).

A partition P is an *equitable partition* [3] with respect to the graph $G(V, E)$ if for any $C_1, C_2 \in P$ (not necessarily distinct) we have $rd(x, C_2) = rd(y, C_2)$ for every $x, y \in C_1$. This means that the relative degrees of each vertex in a given cell to any given cell in the partition are equal. The relative degree of a cell C_1 to a cell C_2, $rd(C_1, C_2)$, in an equitable partition P, is the relative degree of any vertex x in the cell C_1 to the cell C_2, $rd(C_1, C_2) = rd(x, C_2)$, $\forall x \in C_1$. The degree $rd(C_1, C_2)$ is called *output relative degree* of the cell C_1 to the cell C_2, and *input relative degree* to the cell C_2 *from* the cell C_1.

An *isomorphism* [3] α between two graphs $G_1(V_1, E_1)$ and $G_2(V_2, E_2)$ is a bijection $y_i = \alpha(x_i)$, $x_i \in V_1$, $y_i \in V_2$, $i = 1, 2, \dots, n$, between the vertices of graphs, such that if two vertices $p, q \in V_1$ are adjacent (nonadjacent) in G_1, then the corresponding vertices $\alpha(p)$, $\alpha(q)$ are adjacent (nonadjacent) in G_2. The isomorphism is a relation that preserves the adjacency of the vertices. Two graphs G_1 and G_2 are isomorphic, $G_1 \cong G_2$, if there is at least one isomorphism between them.

An *automorphism* [3] α is an isomorphism of a graph $G(V, E)$ to itself. The set of all automorphisms of a graph form a group under the operation of function composition. This group is called the *automorphism group* of the graph, denoted $Aut(G)$ or $A(G)$. The *order of the group*, $|Aut(G)|$ is the number of the group authomorphisms.

The *generators for the group $Aut(G)$* are a subset of the group such that every group automorphism can be written as a finite product of the automorphisms of this subset.

Two vertices x and y of the graph $G(V, E)$ are called *similar*, $x \sim y$, if there is an automorphism $\alpha \in Aut(G)$, $y = \alpha(x)$.

The set of all vertices similar to vertex x under some subgroup $H \subseteq Aut(G)$ is called *orbit* $O(x)$ of x with respect to the subgroup H [3].

An *orbit partition* (or *automorphism partition*) $P = O_1 O_2 \dots O_i \dots O_m$ is a partition whose cells are equal to the orbits of vertices under some subgroup $H \subseteq Aut(G)$. It is easy to show that the orbit partition is equitable.

Some *properties of an equitable partition P*:

($\mathrm{P_a}$) $rd(C, S) \geq 0, C$ is a cell of P, and S is a union of cells of P;

($\mathrm{P_b}$) $rd(C, S_1 \cup S_2) = rd(C, S_1) + rd(C, S_2)$, S_1 and S_2 are different union of cells of P;

($\mathrm{P_c}$) $rd(C_1, C_2)|C_1| = rd(C_2, C_1)|C_2|$, C_1 and C_2 are cells (not necessarily different) of P.

Properties ($\mathrm{P_a}$) and ($\mathrm{P_b}$) are obvious. Property ($\mathrm{P_c}$) shows the number of edges between the cells C_1 and C_2, defined by two ways (left and right side of the equation).

2. Graph representation of a projective plane of order 16. A projective plane of order $n = 16$ has $n^2 + n + 1 = 273$ points and 273 lines, each line meets $n + 1 = 17$ points and each point is contained in 17 lines. The graph corresponding to such a plane is a regular bipartite 273×273 graph of degree 17: each vertex from *part I* (273 vertices, denoted $I273$) of the graph corresponds to a point of the plane and each vertex from *part II* (273 vertices, denoted $II273$) of the graph corresponds to a line of the plane. For the dual plane the inverse is true.

The graphs for all 13 known planes of order 16 are available on Gordon Royle's web site [9]. These graphs and the graphs of the projective planes of order 25, 27 and 49 are among the most "difficult" known examples for graph isomorphism and automorphism algorithms. The smallest examples of such graphs are given by R. Mathon in [4]. Two very efficient approximation and exact algorithms [8] (developed by the author and not described here) are called many times in $M65$ and $M52$: algorithm *VSEPARN* for computing the generators, orbits and order of the graph automorphism group and a graph isomorphism algorithm derived from *VSEPARN*. McKay's algorithm [6] for these problems is well known but cannot be used here.

3. Unitals and maximal arcs in a graph of a projective plane of order 16. A *unital* in the graph of a projective plane of order $n = 16 = q^2 = 4^2$ is defined as follows: the vertices of part I of the plane graph are divided in two subsets $M65I$ and $M208II$, where $|M65I| = 65$ and $|M208II| = 208$, $(65 + 208 = 273)$.

Each vertex from part II has 1 or 5 adjacent vertices from $M65I$.

The subsets of part II are $M65II$ and $M208II$, $|M65II| = 65$, $|M208II|$ $= 208$. Each vertex from $M65II$ has one adjacent vertex from $M65I$ (the inverse is true). Each vertex from $M208II$ has 5 adjacent vertices from $M65I$. Each vertex from $M208I$ has 12 adjacent vertices from $M208II$. This is proven by the following theorem.

Theorem. *Given: graph* $G546$ *of some projective plane of order* 16 *and unitial* U *of* $G546$*, represented by subsets* $M65I$*,* $M208I \in P_1$*, and subsets* $T_1, T_2 \in P_2$ *such that:* $|M65I| = 65$*;* $|M208I| = 208$*;* $rd(T_1, M65I) = 1$*;* $rd(T_2, M65I) = 5$*;* $|T_1| + |T_2| = 273$*. Then:*

(*a*) $|T_1| = 65$; $|T_2| = 208$;
(*b*) $rd(M65I, T_1) = 1$; $rd(M208I, T_1) = 5$; $rd(T_1, M208I) = 16$;
(*c*) $rd(T_2, M208I) = 12$; $rd(M208I, T_2) = 12$; $rd(M65I, T_2) = 16$.

Proof. Applying property ($\mathrm{P_c}$) for $M65I$ and $T1$ we have $rd(T_1, M65I)|T_1| = rd(M65I, T_1)|M65I|$ and

(1) $$|T_1| = 65rd(M65I, T_1).$$

Property ($\mathrm{P_c}$) gives for T_2 and $M65I$:
$rd(T_2, M65I)|T_2| = rd(M65I, T_2)|M65I|, \quad 5|T_2| = 65rd(M65I, T_2)$ and

(2) $$|T_2| = 13rd(M65I, T_2)$$

We have also

(3) $$rd(M65I, T_1 + T_2) = 17 = rd(M65I, T_1) + rd(M65I, T_2).$$

We add condition (iii):

(4) $$|T_1| + |T_2| = 273.$$

The solutions of equations (1)–(4) are:
$|T_1| = 65; \quad |T_2| = 208; \quad rd(M65I, T_1) = 1; \quad rd(M65I, T_2) = 16.$
For symmetry we denote T_1 by $M65II$ and T_2 by $M208II$.
From
$rd(M208II, M65I + M208I) = 17 = rd(M208II, M65I) + rd(M208II, M208I) = 5 + rd(M208II, M208I)$ we obtain $rd(M208II, M208I) = 12$, from $|M208I| = |M208II|$ and ($\mathrm{P_c}$) we have $rd(M208I, M208II) = 12$ and $rd(M208I, M65II) = 17 - rd(M208I, M208II) = 17 - 12 = 5$.

We summarize the results from the theorem:

(5) $$\begin{array}{lll} rd(x, M65II) = 1, & rd(x, M208II) = 16, & \text{for } x \in M65I; \\ rd(x, M65II) = 5, & rd(x, M208II) = 12, & \text{for } x \in M208I; \\ rd(x, M65I) = 1, & rd(x, M208I) = 16, & \text{for } x \in M65II; \\ rd(x, M65I) = 5, & rd(x, M208I) = 12, & \text{for } x \in M208II. \end{array}$$

Algorithm $M65$ finds subsets $M65I$, $M65II$, $M208I$, $M208II$ that hold the above conditions.

In the case of maximal arcs of degree $m = 4$ the vertices of part I and II of the plane graph are divided in two subsets $M52I$, $M221I$ and $M52II$, $M221II$ $(n(m-1) + m = 16.3 + 4 = 52)$, where $|M52I| = |M52II| = 52$, $|M221I| = |M221II| = 221$.

The relative degrees of these subsets are (easy to prove):

(6) $$\begin{array}{lll} rd(x, M52II) = 0, & rd(x, M221II) = 17, & \text{for } x \in M52I; \\ rd(x, M52II) = 4, & rd(x, M221II) = 13, & \text{for } x \in M221I; \\ rd(x, M52I) = 0, & rd(x, M221I) = 17, & \text{for } x \in M52II; \\ rd(x, M52I) = 4, & rd(x, M221I) = 13, & \text{for } x \in M221II. \end{array}$$

Algorithm $M52$ finds subsets $M52I$, $M52II$, $M221I$, $M221II$ satisfying the above conditions. Algorithm $M52$ is derived from algorithm $M65$ only by changing some parameters of $M65$ (65 to 52, 208 to 221, 5 to 4, 1 to 0, etc.). That's why we describe only algorithm $M65$. Algorithm $M65$ can be used also after changing its parameters to finding unitals and maximal arcs of planes of other orders (the authors are using it now for finding unitals of planes of order 25).

Corollary 1. *There is* $1-1$ *correspondence* $x_i - y_i$, $i = 1, \dots, 65$, $x_i \in M65I$, $y_i \in M65II$ *(between the vertices of the sets* $M65I$ *and* $M65II$*), such that* (x_i, y_i) *is an edge.*

This follows from: $|M65I| = |M65II| = 65$ and

$$rd(M65I, M65II) = rd(M65II, M65I) = 1.$$

Corollary 2. *Let* O_1 *be an orbit under some subgroup* $H \subseteq Aut(G546)$ *and let* $O_1 \in M65I$*. Then there is only one orbit* $O_2 \in M65II$ *such that* $|O_1| = |O_2|$ *and* $rd(O_1, O_2) = rd(O_2, O_1) = 1$*.*

Proof. Let we consider an edge $(x, y) \in E$, where $x_i \in O_1 \subseteq M65I$ and $y \in O_2 \subseteq M65II$. The existence of such an edge is proven in Corollary 1. For each vertex $u \in O_1$ there is an automorphism $\alpha \in H$ such that $u = \alpha(x) \in O_1$. The edge (x, y) has unique image (u, v) under α, where $v = \alpha(y) \in O_2$. This means that for each vertex $u \in O_1$ there is one corresponding vertex $v \in O_2$ and vice versa, i.e. $|O_1| = |O_2|$ and $rd(O_1, O_2) = rd(O_2, O1) = 1$.

4. Exhaustive search algorithm. If for finding unitals we generate all combinations $\binom{273}{65} \approx 6.74 \times 10^{65}$ and check each combination for unital requirements (conditions (1)) the execution time will be $t_1 \approx 5.13 \times 10^{51}$ years, if for one combination we spend $t = 1$ μs and the execution time will be $t_2 \approx 5.13 \times 10^{48}$ years, if for one combination check we spend $t = 1$ ns. This is combinatorial explosion and such an algorithm is useless. The same situation is in the case of maximal arcs algorithm if the exhaustive search is used. Again the number of combinations $\binom{273}{52} \approx \quad 3.293 \times 10^{56}$ to be checked is extraordinary high and the algorithm is impractical.

5. Algorithms *M65* and *M52*. One way to avoid the combinatorial explosion is the use of approximation algorithm. Algorithm $M65$ (Fig. 1) do not generate all possible combinations of class 65 from all 273 vertices of $I273$.

```
1.   Find the orbits of the graph automorphism group; $SU := \emptyset$;
2.   for each vertex of the graph do
       begin
3.       Find the generators of the graph automorphism group;
4.       for each combination of generators (subgroup) do
           begin
5.           Find the orbits of the subgroup (orbits of partitions $P1$, $P2$);
6.           Sort the orbits of partition $P1$, $P2$ in decreasing order of
             their lengths;
7.           Find the relative degrees between orbits of $P1$, $P2$;
8.           Find each combination of orbits of $P1$ with length $= 65$ that
             satisfy the unital requirements (conditions (1));
9.           Find the unital automorphism group order;
10.          Print and put into the stack $SU$ the found unital if it is
             not isomorphic to the previously found unitals in $SU$
           end
         end;
```

Fig. 1. **Algorithm *M65*** (the cases of the largest orbit length ≤ 3 and different orbit lengths of the sequences $P1$ and $P2$ are excluded in step 8, SU is a stack for storing found nonisomorphic unitals)

In the case of the exhaustive search each vertex is considered alone. Instead, M65 generates combinations of orbits of some subgroup of graph automorphism group in order to obtain a combination of orbits with sum of orbit lengths equal to 65. This approach is based on the assumption that the vertices from given orbit have equal behavior and they should be handled together. The number of combinations of orbits is less than the number of combinations of vertices, because the number of orbits is less than the number of vertices. Algorithm $M65$ uses very efficient algorithm *VSEPARN* [9] for finding the generators, orbits and order of the graph automorphism group. The generators in *VSEPARN* depend on the starting vertex. Thus we can generate by *VSEPARN* different sets of generators – the number of sets is equal to number of vertices of the graph (546). For each set of generators we find in $M65$ all subgroups (subset of generators) and their orbits. The orbits of a given subgroup form two equitable partitions: $P1$ (set of orbits of vertices from $I273$) and $P2$ (set of orbits of vertices from $II273$). $P1$ and $P2$ are sorted in decreasing order of their orbit lengths. Example of partitions $P1$ and $P2$ (for some automorphism subgroup of the graph of the plane PG(2, 16)) with their relative degrees are shown on Table 3 (in the last row and column are shown by ***y*** (yes) the orbits holding one of the necessary conditions for inclusion

			$P_2(II273)$												$rd(O_j, O_i) \leq 5$
		j	1	2	3	4	5	6	7	8	9	10	11	12	($\boldsymbol{y}$ – yes
	i	$O_i \setminus O_j$	60	60	60	30	15	15	15	12	3	1	1	1	$\boldsymbol{n}$ – no)
$P_1(I273)$	1	60	5	1	5	$\frac{2}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{5}$	–	–	–	–	$\boldsymbol{y}$
	2	60	2	5	4	$\frac{3}{6}$	$\frac{1}{4}$	–	$\frac{1}{4}$	$\frac{1}{5}$	–	–	–	–	$\boldsymbol{n}$
	3	60	4	5	2	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{2}{8}$	$\frac{1}{5}$	–	–	–	–	$\boldsymbol{n}$
	4	30	$\frac{6}{4}$	$\frac{4}{2}$	$\frac{2}{1}$	2	$\frac{1}{2}$	–	$\frac{1}{2}$	–	$\frac{1}{10}$	–	–	–	$\boldsymbol{n}$
	5	15	–	$\frac{4}{1}$	$\frac{8}{2}$	–	1	2	1	–	$\frac{1}{5}$	–	–	–	$\boldsymbol{y}$
	6	15	$\frac{4}{1}$	$\frac{4}{1}$	$\frac{4}{1}$	$\frac{2}{1}$	1	1	–	–	–	$\frac{1}{15}$	–	–	$\boldsymbol{n}$
	7	15	$\frac{4}{1}$	$\frac{4}{1}$	$\frac{4}{1}$	$\frac{2}{1}$	–	1	1	–	–	–	–	$\frac{1}{15}$	$\boldsymbol{n}$
	8	12	$\frac{5}{1}$	$\frac{5}{1}$	$\frac{5}{1}$	–	–	–	–	1	–	–	$\frac{1}{12}$	–	$\boldsymbol{n}$
	9	3	–	–	–	$\frac{10}{1}$	–	$\frac{5}{1}$	–	–	1	–	$\frac{1}{3}$	–	$\boldsymbol{y}$
	10	1	–	–	–	–	–	–	–	$\frac{12}{1}$	$\frac{3}{1}$	1	–	1	$\boldsymbol{y}$
	11	1	–	–	–	–	–	–	$\frac{15}{1}$	–	–	1	1	–	$\boldsymbol{y}$
	12	1	–	–	–	–	$\frac{15}{1}$	–	–	–	–	–	1	1	$\boldsymbol{y}$
$rd(O_i, O_j) \leq 5$ ($\boldsymbol{y}$ – yes, $\boldsymbol{n}$ – no)			$\boldsymbol{n}$	$\boldsymbol{y}$	$\boldsymbol{n}$	$\boldsymbol{n}$	$\boldsymbol{n}$	$\boldsymbol{y}$	$\boldsymbol{n}$	$\boldsymbol{n}$	$\boldsymbol{y}$	$\boldsymbol{y}$	$\boldsymbol{y}$	$\boldsymbol{y}$	

in an unital: input relative degree of the orbit ≤ 5; only the orbits with summary length $= 65 = 60 + 3 + 1 + 1$ are really included). $M65$ does not generate all combinations of orbits with sum of orbits lengths equal to 65 (step 8 of $M65$, Fig. 1), because there are cases when the lengths of orbits are small (with maximal orbit length < 3) and again the number of combinations is very high. They are excluded from consideration in $M65$. That's why the algorithm M65 is inexact. If we allow maximal orbit length $= 1$ and different orbit length sequences of part I and II, $M65$ will become exact algorithm. For example, if the length of orbits are $126 * 2 + 21 * 1 = 273$ (126 orbits of length $= 2$ and 21 orbits of length $= 1$ – this case is common for all 13 planes of order 16) the number of all combinations of orbits with length sum $= 65$ is given in Table 4.

To **reduce the number of the generated subcombinations** (subcombination is a combination that is initial substring of another combination – for example 1 5 7 is subcombination of 1 5 7 9 11) and combinations, each subcombination is checked (procedure **check** in the algorithm of step 8) for holding of some **necessary conditions**. For example, let $O_1O_5O_{11}O_{25}$ be a solution (unital) $|O_1| + |O_5| + |O_{11}| + |O_{25}| = 65$, where O_1, O_5, O_{11} and O_{25} are

Table 4

x	y	$C_{126}^x.C_{21}^y$
32	1	$1.741.10^{31}$
31	3	3.714×10^{32}
30	5	1.835×10^{33}
29	7	3.743×10^{33}
28	9	2.426×10^{33}
27	11	8.234×10^{32}
26	13	1.283×10^{32}
25	15	8.804×10^{30}
24	17	2.380×10^{29}
23	19	1.946×10^{27}
22	21	2.049×10^{24}

$2x + y = 65$; x, y – number of orbits with length 2 and 1 in the combination of orbits with total length 65;
$\sum_{x=32}^{22} C_{126}^x C_{21}^y = 8.85 \times 10^{33}$

orbits. In this case subcombinations O_1, $O_1{+}O_5$, $O_1{+}O_5{+}O_{11}$, $O_1{+}O_5{+}O_{11}{+}O_{25}$ hold the conditions. If given subcombination does not hold all conditions this subcombination can not participate in any subcombination or combination that contains it and they are not generated. In the above example if subcombination $O_1{+}O_2$ does not hold one of the conditions then all subcombinations that contain $O_1 + O_2$ are not generated ($O_1 + O_2 + O_3$, $O_1 + O_2 + O_4$, etc.).

If the orbits are known then step 1 in $M65$ should be omitted. In this case step 2 is executed for short time – otherwise it may take very long time.

The ***current combination S_1*** of orbits from partition P1 (in order S_1 to be in $M65I$) should satisfy the following ***necessary conditions*** (used in step 8 of $M65$):

(C$_1$) $rd(O_j, S_1) \leq 5$ for any orbit $O_j \in P2$;

(C$_2$) For each orbit $Oi \in S1$ there is at least one orbit $Oj \in P2$ such that $rd(O_j, O_i) = 1$ and $|O_j| = |O_i|$, and $rd(O_j, S_1) = 1$;

(C$_3$) Let S_2 be a set of all orbits from $P1$, whose numbers are greater than the number of last orbit in S_1 and let O_j be any orbit from $P2$.

If $rd(O_j, S_1) > 1$, then $rd(O_j, S_1) + rd(O_j, S_2) \geq 5$;

(C$_4$) $|S_1| + |S_{02}| \geq 65$, where S_{02} is the set of orbits $O_j \in P_2$ that have relative degree $rd(O_j, S_1) = 0$. (C$_4$) is true only if $P_1 = P_2$ (this is the second reason for naming this algorithm approximation).

Proof of (C$_1$). Let S_3 be a set of orbits from P_1 that is complement of S_1 to the final combination-unital: $S_1 + S_3 = M65$, $|S_1| + |S_3| = 65$. In order S_1

to be subset of $M65I$ each orbit $O_j \in P_2$ should have relative degree
$rd(O_j, S_1 \cup S_3) \leq 5$ $\{1$ or $5\}$. Thus
$rd(O_j, S_1 \cup S_3) = rd(O_j, S_1) + rd(O_j, S_3 \leq 5$,
$rd(O_j, S_1) \leq 5 - rd(O_j, S_3) \leq 5$ since $rd(O_j, S_3) \geq 0$.

Proof of (C_2). We shall proof that it is possible in the combination S_1, $|S_1| < 65$, two orbits (O_j, O_k) from P_2 to have relative degree=1 to the orbit O_i from S_1.

Let $O_i \in S_1$, $O_j, O_k \in P_2$ and $rd(O_j, O_i) = rd(O_i, O_k) = rd(O_i, O_j) = rd(O_k, O_i) = 1$ (Fig. 2). It follows from Corollary 2 that in the final combination-unital there is only one orbit say $O_j \in P_2$ corresponding to O_i such that $|O_j| = |O_i|$ and $rd(O_j, O_i) = 1$, $O_j \in M65II$. Obviously $O_k \in M208II$. This means that there is an orbit $O_q \in M65I$ but $O_q \notin S_1$ such that $rd(O_k, O_q) \geq 1$ and consequently $rd(O_k, S_1 + O_q) \geq rd(O_k, O_i + O_q) \geq 2$, i.e. when O_q will be included into S_1, then orbit O_k will be excluded from $M65II$.

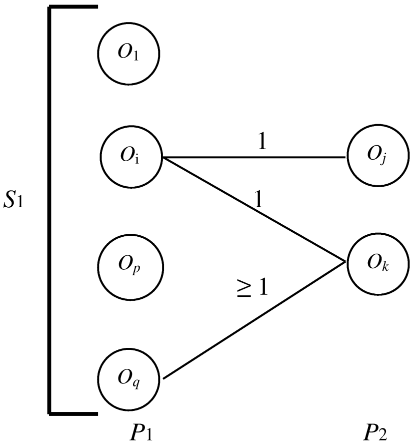

Fig. 2

Proof of (C_3). Let we have two subsets $S_{1c} \in S_2$ and $S_{2c} \in S_2$, such that $S_1 \cup S_{1c} = M65I$ and $S_2 = S_{1c} \cup S_{2c}$ (Fig. 3). The condition $rd(O_j, S_1) > 1$ means that $O_j \in M208II$. Consequently $rd(O_j, S_1 \cup S_{1c}) = 5$, $|S_1| + |S_{1c}| = 65$. We have:
$rd(O_j, S_1) + rd(O_j, S_2) = rd(O_j, S_1) + rd(O_j, S_{1c} \cup S_{2c}) =$
$rd(O_j, S_1) + rd(O_j, S_{1c}) + rd(O_j, S_{2c}) = 5 + rd(O_j, S_{2c}) \geq 5$,
since $rd(O_j, S_{2c}) \geq 0$;

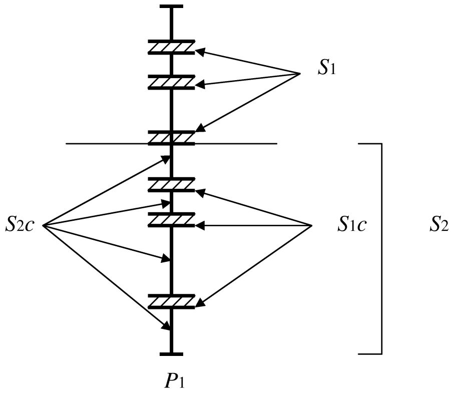

Fig. 3

Proof of (C$_4$). $rd(O_j, M65I) = 1 or 5$ for the final combination-unital $M65I$. If $rd(O_j, M65I) = 1$ then $O_j \in M65II$ and it follows from Corollary 2 that there is corresponding orbit $O_i \in M65I$ such that $|O_i| = |O_j|$, $rd(O_i, O_j) = rd(O_j, O_i) = 1$. If $rd(O_j, M65I) = 5$ then $O_j \in M208II$. It follows from the assumption $P_1 = P_2$ that there is corresponding orbit $O_i \in P_1$, $O_i \in M208I$, $|O_i| = |O_j|$. Consequently part S_{02a} of the orbit, $S_{02a} \in S_{02}$ is in $M65II$ and another part S_{02b}, $S_{02b} \in S_{02}$ is in $M208II$, $S_{02b} \in M208II$. The same is true for the corresponding orbits S_{01a}, S_{01b} from P_1, e.g. $S_{01a} \in M65I$, $S_{01b} \in M208I$. It follows from $P_1 = P_2$ that $|S_{01a}| = |S_{02a}|$ and $|S_{01b}| = |S_{02b}|$.

Consequently $|S_1 + S_{02}| = |S_1| + |S_{01}| = |S_1| + |S_{01a}| + |S_{01b}| = 65 + S_{01b} \geq 65$, since $|S_{01b}| > 0$.

Step 8 (Fig. 4) of Algorithm $M65$ (Fig. 1) generates each combination (stored in stack *st*) of labels of orbits of $P1$ in lexicographic order of their subscripts in P_1 that hold the following requirements: (i) it is with length ≤ 65; (ii) it holds all necessary conditions C$_1$ – C$_4$ (procedure **check**). If the current combination $S1$ is with length < 65 and holds all necessary conditions then the next orbit from $P1$ is added to S_1 – this is a *forward move*. If the current combination S_1 does not hold one or more of the requirements then the last added orbit is removed from S_1 (*backward move*) and the generation continues with S_1 and the orbits located in P1 after the removed orbit. When the combination become with length = 65 and it holds all necessary conditions then it is printed and put into stack SU if it is not isomorphic to previously found unitals stored in SU. The next move is backward. The algorithm stops after the generation of all combinations that hold the requirements (steps 13 or 16 – stack *st* is empty).

```
$top := 1$; $S := 0$; $i := 1$; $st(top) := 1$;
repeat
  if $i \le m$ then
    $S := S + d(i)$;
    if $S \le 65$ then
      if $(S + SR(i)) \ge 65$ then
        check (prop);
        if prop then
          if $S = 65$ then
            a unital is found;
            $S := S - d(i)$
          else
            $top := top + 1$
          end {of if $= 65$}
        else
          $S := S - d(i)$
        end {of if prop}
      else
        $S := S - d(i)$; if $top = 1$ then exit;
        $top := top - 1$; $i := st(top)$; $S := S - d(i)$
      end {of if $(S + SR(i))$}
    else
      $S := S - d(i)$
    end {of if $i \le 65$}
  else
    if $top = 1$ then exit;
    $top := top - 1$; $i := st(top)$; $S := S - d(i)$
  end {of if $i \le m$};
  $i := i + 1$; $st(top) := i$
until false
```

Fig. 4. Algorithm of step 8 of Algorithm ***M65***. (m – number of orbits in P_1, st – stack contains the current combination S_1 of orbit labels, $d(i)$ is the length of orbit O_i, S – sum of the lengths of the orbits in st, $SR(i)$ – sum of the orbit lengths of P_1 with labels $> i$)

6. Concluding remarks.

By the algorithms $M65$ and $M52$ we have found new unitals and maximal arcs in projective plane of order 16, but not all of them.

The following approaches can be used to find more or all unitals and maximal arcs: (a) development of improved algorithms $M65$ and $M52$ by finding new conditions for pruning the search tree; (b) using subgraph isomorphism algorithm for $H \subseteq G$, where G is one of 13 graphs of known plane of order 16 and H is a regular disconnected bipartite graph with 130 vertices $(65 + 65)$: each vertex from part one has only one adjacent vertex from part two and vice versa. (c) Transformation of the solution for one plane to solution for another plane (R. Mathon's approach); (d) development of parallel algorithms.

Acknowledgements. The author wish to thank Vladimir Tonchev for suggesting the problem of developing an algorithm for searching unitals in projective planes and for giving the general idea of such an algorithm – use of unions of orbits.

REFERENCES

[1] Colbourn C. J., J. H. Dinitz (Eds.) The CRC handbook of Combinatorial Designs, CRC Press, New York, 1996.

[2] Hamilton N., S. D. Stoichev , V. D. Tonchev. Maximal Arcs and Disjoint Maximal Arcs in Projective Planes of Order 16. *J. Geom.* **67** (2000), 117–126.

[3] Kreher D. L., D. R. Stinson. Combinatorial Algorithms, CRC Press, 1998.

[4] Mathon R. Sample Graphs for Graph Isomorphism Testing. In: Proc. 9th S.-E. Conf. Combinatorics, Graph Theory and Computing, Boca-Raton, 1978, 499–517.

[5] Mathon R. Private communication.

[6] McKay B. D. Practical Graph Isomorphism. *Congresses Numeration*, **30**, 1981, 45–87.

[7] Stoichev S. D., V. D. Tonchev. Unital Designs in Planes of Order 16. *Discrete Applied Mathematics* **102** (2000), 151–158.

[8] Stoichev S. D. Algorithms for a class of graph theory problems – isomorphisms, Hamiltonian circuits etc. Dr.Sc. dissertation, Technical University of Sofia, 1988 (in Bulgarian).

[9] Royle G. F. Known planes of Order 16.
`http://www.cs.uwa.edu/au/~gordon/planes16/index#planes`

Department of Computer Systems
Technical University – Sofia
1000 Sofia, Bulgaria
e-mail:`stoi@tu-sofia.bg`

Received January 30, 2007
Final Accepted September 13, 2007