Upper bounds on the covering number of Galois-planes with small order

T. Illés and D. Pisinger

Abstract

Our paper deals with a problem of P. Erdős' related to the covering number of blocking sets of finite projective planes. An integer linear programming (*ILP*) formulation of Erdős' problem is introduced for projective planes of given orders. The mathematical programming based approach for this problem is new in the area of finite projective planes. Since the ILP problem is $\mathcal{NP}$-hard and may involve up to 360.000 boolean variables for the considered problems, we propose a heuristic based on simulated annealing. The computational study gives a new insight into the structure of projective planes and their (minimal) blocking sets. This computational study indicates that the current theoretical results may be improved.

Key words: *Galois-plane, blocking sets, 0-1 programming, simulated annealing*

AMS Subject Classification : **90C10, 51E21**

1 Introduction

In the beginning of the 1980's P.Erdős asked whether there exists an absolute constant γ^* such that every projective plane $\Pi(q)$ has a blocking set B where the covering number of B is not larger than γ^*. Although this deep question, which has some relation to graph and number theory, was raised more than 15 years ago — nobody have been able to answer it. The only known results are some upper bounds on the covering numbers of a blocking set, which however by no means lead to some constant value γ^*.

Our approach in this paper is to use metaheuristics to construct blocking sets with small covering numbers, and study the numerical results in order to uncover special structural properties, getting an impression of whether the existence of a supremum γ^* is plausible. Although a numerical study is not a formal proof, our results indicate that the currently best known upper bounds apparently may be tightened, leading to a slight indication of that further work may answer Erdős problem in an affirmative way. However, first we need some definitions:

Let $\Pi(q)$ denote a collection of *point*s and *subset*s of these points. Each of these subsets is referred to as *line*. $\Pi(q)$ is assumed to satisfy four *axiom*s:

(i) Each pair of distinct points lies on a unique line.

(ii) Each pair of distinct lines intersects at a uniquely determined point.

(iii) There are four points of which at most two lie on the same line.

(iv) $\Pi(q)$ has a line with $q+1$ points, where q is a given integer such that $q \geq 2$.

A collection $\Pi(q)$ of points and lines satisfying all of the above axioms is called a *finite projective plane of order* q. It can be deducted (see for example, Kárteszi [13]) from these axioms that

- Each line has $q+1$ points.
- There are $q+1$ lines through each point.
- $\Pi(q)$ has in total q^2+q+1 points and q^2+q+1 lines.

Any finite projective plane of order q can be represented by its *point-line incidence* matrix, $L = (l_{ij})$, $i, j = 1, 2, \ldots, q^2+q+1$, where

$$l_{ij} = \begin{cases} 1, & \text{if the } i^{th} \text{ line contains the } j^{th} \text{ point} \\ 0, & \text{otherwise.} \end{cases}$$

The incidence matrices for a special type of finite projective planes called *Galois–planes* can be generated easily from *difference sets*, $\mathcal{D} = \{d_1, d_2, \ldots, d_{q+1}\}$ where $1 \leq d_1 < d_2 < \ldots < d_{q+1} \leq q^2+q+1$ and all the differences

$$\delta_{ij} = \begin{cases} d_j - d_i, & \text{if } i < j \\ q^2+q+1-d_j+d_i, & \text{if } i > j, \end{cases} \tag{1}$$

have different values.

A line of a Galois-plane of order q can be obtained as the set

$$l_1 = \{P_{d_1}, P_{d_2}, \ldots, P_{d_{q+1}}\} \tag{2}$$

of points, where $\mathcal{D} = \{d_1, d_2, \ldots, d_{q+1}\}$ form a difference set. (For more details see [13,11].)

The incidence matrix L of the Galois–plane can be generated from any difference set. First, using (2) we generate l_1 from the given difference set as

$$l_{1j} = \begin{cases} 1, & \text{if} j \in \mathcal{D}, \\ 0, & \text{otherwise.} \end{cases} \qquad j = 1, \ldots, q^2+q+1 \tag{3}$$

Such a line of the Galois–plane fully characterizes all the other lines, as all succeeding lines are translations of l_1 in the following way,

$$l_{ij} = l_{1,\alpha(i,j)} \qquad i, j = 1, \ldots, q^2+q+1 \tag{4}$$

where $\alpha(i,j) = 1 + ((i+j-2) \bmod q^2+q+1)$.

Let us illustrate how we can obtain the incidence matrix of a Galois-plane of order 4.

Example 1 *Let $q = 4$ be given and find first a difference set $\mathcal{D}$. Using (1) it is easy to verify that $\mathcal{D} = \{1, 3, 8, 9, 12\}$ form a difference set. Therefore*

$$l_1 = (1,0,1,0,0,0,0,1,1,0,0,1,0,0,0,0,0,0,0,0,0)$$

is the incidence vector of the first line (see (3)). Now we are ready to build up the line-point incidence matrix of Galois–plane of order 4 using equation (4).

$$L_4 = \begin{pmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Let $\Pi(q)$ be a projective plane of order q. A subset B of $\Pi(q)$ is called a *blocking set* if B intersects every line but contains no line. A blocking set is called *minimal* if it does not contain a smaller blocking set as a subset. The following upper and lower bounds for the size of minimal blocking sets were proved by Bruen [4], and Bruen and Thas [5]

$$q + \sqrt{q} + 1 \leq |B| \leq q\sqrt{q} + 1. \tag{5}$$

If B is a non-minimal blocking set then the upper bound on $|B|$ is $q^2 - \sqrt{q}$, [4].

Example 2 *It is easy to verify that*

$$\mathcal{B} = \{2, 3, 6, 9, 10, 11, 12, 20, 21\}$$

form a (minimal) blocking set of the Galois–plane of order 4 given by the incidence matrix L_4.

Let us write down the incidence vector $x_{\mathcal{B}}$ *of the blocking set* $\mathcal{B}$

$$x_{\mathcal{B}} = (0, 1, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1)$$

then

$$w^T = (L_4 x_{\mathcal{B}})^T = (3, 3, 3, 1, 1, 1, 3, 1, 1, 3, 3, 1, 3, 3, 1, 1, 1, 1, 3, 3, 3)$$

says that first line contains 3 points from $\mathcal{B}$*, second line contains 3 points from* $\mathcal{B}$*, etc. Because*

$$e \leq w \leq 4e,$$

where e *is the all ones vector of size 21, we know that* $\mathcal{B}$ *is a blocking set, because it covers all the lines (lower bound), but contains no line (upper bound). There is a tangent on each point of the blocking set* $\mathcal{B}$*, therefore it is minimal.*

Except a few upper bounds, not much is known about the covering number of a finite projective plane (Section 2) and nearly nothing about the structure of those (minimal) blocking sets which correspond to the best known bounds. However, the related question of Erdős (Section 2) is more than 15 years old, but the only computational investigation is due to Béres and Illés [2] for small prime orders up to $q = 89$. The investigation was based on a formulation of Erdős problem as an integer linear programming problem.

Béres and Illés [2] showed, that for a quite small value of q ($q = 29$) with CPLEX 2.1 [8] even finding a feasible solution is practically impossible, although they used a fast workstation for the computations. This prompted them to introduce a greedy heuristic. For all prime orders up to $q = 89$ they were able to obtained better bounds on $\gamma(\Pi(q))$ than those known from the theoretical considerations (see Section 2). However it is still an open question whether their greedy algorithm gives the best known bounds on $\gamma(\Pi(q))$ for all prime orders or not.

Béres and Illés observed that the running time of their greedy algorithm increases very fast with the order of the finite projective plane. (The running time of the greedy algorithm for the projective plane of order 11 was just few minutes, while for the case $q = 89$ it took three days on PC-AT 386/25Mhz with 2 Mbyte RAM.) These experiments showed that even with the greedy heuristics only small instances can be handled. That is the reason why we are using more sophisticated heuristics (simulated annealing) to obtain upper bounds on $\gamma(\Pi(q))$ for bigger orders.

The goals of this numerical study are: (1) to compute better upper bounds for the covering number of finite projective plane with given, small orders than those known in the literature; (2) to show that for some questions arising in the area of finite projective plane geometry there is a reasonably good and generally not used tool (integer linear programming formulation of the problem and simulated annealing algorithm) to make computational experiments in order to gain insight into the problem; and finally (3) to obtain some informations about the structure of (minimal) blocking sets with reasonably small covering numbers.

The paper is organized as follows. The covering number of a finite projective plane is introduced and the related results are discussed in Section 2. Furthermore, this section contains a possible integer programming formulation of Erdős question. Section 3 deals with the simulated annealing reformulation of the integer linear programming problem and the generic form of annealing algorithm is presented. Computational results are given in Section 4. Conclusions and remarks close the paper in Section 5.

2 The covering number of a finite projective plane

A projective plane $\Pi(q)$ has property $B(\gamma)$ if there is a blocking set B whose intersection with each line of $\Pi(q)$ contains less than γ points. For a blocking set B, $\gamma(B)$ denotes the maximum number of collinear points of B, and $\gamma(B)$ is called the *covering number of the blocking set* B.[1] The covering number of a given blocking set, B can be given as

$$\gamma(B) = \max_i w_i = \max_i (L_q x_B)_i. \tag{6}$$

Using the result of Béres and Illés [2], stricter lower and upper bounds on the size of the blocking sets can be derived. They depend on the covering number $\gamma(B)$.

[1] The minimal blocking set, $\mathcal{B}$ given in Example 2 has covering number, $\gamma(\mathcal{B}) = 3$.

(Béres-Illés [2])

Result 1 *Let us assume that a minimal blocking set, B of the projective plane of order q is given. If B has covering number $\hat{\gamma} := \gamma(B)$, then the size $|B|$ of B satisfies the following inequality*

$$\frac{1}{2}\left(1+(\hat{\gamma}-1)(q+1)-\sqrt{f(\hat{\gamma},q)}\right) \leq |B| \leq \frac{1}{2}\left(1+(\hat{\gamma}-1)(q+1)+\sqrt{f(\hat{\gamma},q)}\right), \qquad (7)$$

where $q \geq 8$, $\hat{\gamma} > 3$, and $f(\hat{\gamma},q) = ((\hat{\gamma}-1)(q+1)-1)^2 - 4(\hat{\gamma}-1)q^2$.

The smallest γ for which $\Pi(q)$ has property $B(\gamma)$ is called the *covering number of the finite projective plane of order q*, denoted by $\gamma(\Pi(q))$, and it can be expressed as

$$\gamma(\Pi(q)) = 1 + \min_B \gamma(B) = 1 + \min_B \max_i (L_q x_B)_i. \qquad (8)$$

The set of all blocking sets of a finite projective plane $\Pi(q)$ can be described by using their incidence vectors as

$$\mathcal{Q} = \left\{x \in \{0,1\}^{q^2+q+1} | e \leq L_q x \leq qe\right\} \quad \text{and} \quad \hat{\mathcal{Q}} = \operatorname{conv}\mathcal{Q}, \qquad (9)$$

where L_q denotes the point-line incidence matrix of $\Pi(q)$. Then (8) can be written as

$$\gamma(\Pi(q)) = 1 + \min_{x\in\mathcal{Q}} \max_i (L_q x)_i. \qquad (10)$$

Erdős has asked whether there exists an absolute constant γ^* such that every projective plane has property $B(\gamma^*)$.

We may introduce the set

$$\mathcal{Q}_{\gamma^*} = \left\{x \in \{0,1\}^{q^2+q+1} | e \leq L_q x \leq \gamma^* e\right\}, \qquad (11)$$

and restate Erdős question in the following way: does there exist an absolute constant γ^* such that $\mathcal{Q}_{\gamma^*} \neq \emptyset$ for every finite projective plane ?

In other words the question is whether the covering number for any finite projective plane of order q is independent of q or not. If it is independent then there must exist an absolute constant which bounds the covering number of any finite projective plane.

The following bounds on $\gamma(B)$ are known, all of them depending on q. Erdős, Silvermann and Stein [10] proved that every projective plane of order q has property $B(c\ log\ q)$ if q is sufficiently large and $c > 2e$. Their proof is based on a probabilistic method. In the same paper they gave a construction to derive blocking set with property $B(q-\sqrt{q})$. Abbott and Liu [1] improved their result for Galois-planes $PG(2,q)$, where q is an odd prime power, obtaining $B(c\ log\ q)$, with $c > \frac{2}{log 2}$. When p is odd prime then Abbott and Liu [1] proved that $PG(2,p)$ has property $B(2h(p)+3)$, where $h(p)$ denotes the longest block of *consecutive non-residues* modulo p. The best known estimate [7] of $h(p)$ is $h(p) = O(p^{\frac{1}{4}+\epsilon})$. Szőnyi [16,17] got a very similar result for $PG(2,q)$, where $q \equiv 1$ or $3 (\mathrm{mod}\ 4)$. He proved that there exists a minimal blocking set B, which is the union of k different parabolas[2] such that $A = \{a_1, a_2, ..., a_k\} \subset GF(q)$ and the parameters

[2]A *parabola* is a set of points $P_a := \{(x,y) \in GF(q)^2 \mid y = x^2 + a, a \in GF(q)\} \subset \Pi(q)$, where $GF(q)$ denotes the Galois field of order q.

of the parabolas satisfy the following property: $a_i - a_j$ is a non-square in the Galois-field $GF(q)$ for every $i \neq j,\ i,j = 1,2,...,k$ and suppose that A is maximal subject to inclusion. Then B has property $B(2k+1)$.

Much better results are known for Galois-planes, where the order is a prime power. Bruen and Fisher [6] proved that $PG(2,3^s), s \geq 2$ has property $B(5)$. This was generalized by Boros [3] proving that $PG(2,p^s), p > 2$ prime and $s \geq 2$ has property $B(p+2)$. The Galois-planes $PG(2,2^s), s \geq 2$ has property $B(6)$ if s is even and $B(7)$ if s is odd [12].

Now we are ready to give a possible Integer Linear Programming (ILP) formulation of Erdős problem, as the following relaxation of (10)

$$(ILP) \quad \begin{cases} \min \gamma \\ e \leq Lx \leq (\gamma - 1)e \\ 5 \leq \gamma \leq q+1 \\ x \in \{0,1\}^n \end{cases}$$

where $n = q^2 + q + 1$ and q denotes the order of a projective plane, γ is an integer, and $e = (1,1,...,1) \in \mathcal{R}^n$. Here L denotes the point-line incidence matrix of $\Pi(q)$. The lower bound on γ comes from the results of Béres and Illés (Proposition 2.1. – 2.2., [2]), while the upper bound is a trivial consequence of the definition of blocking sets. Using the results of Béres and Illés it is a natural assumption that $q \geq 8$.

If $\gamma - 1 = q$ then all feasible solutions of (ILP) are incidence vectors of a blocking set. For a given value of $\gamma - 1$, the feasible solutions indicate such blocking sets which has property $B(\gamma)$. The objective value of an optimal solution of the (ILP) gives the minimal covering number of the projective plane of $\Pi(q)$. The (ILP) model is an $\mathcal{NP}$-complete formulation of Erdős question. The LP-relaxation has a trivial optimal solution with $\gamma - 1 = 4$ and $x = (\frac{4}{q+1}, \frac{4}{q+1}, ..., \frac{4}{q+1})$. But this solution gives no information about the integer optimum, since if q is large, then all entries in x are very small (nearly zero), although we know that x must contain several ones, as well.

3 Simulated annealing

Since the (ILP) problem is $\mathcal{NP}$-hard, and it may involve thousands of boolean variables for large values of q, we decided to use Simulated annealing to solve the problem heuristically.

Simulated annealing has its roots in the Metropolitan algorithm [14] which was used to simulate the cooling of material in a heat bath. The slower a melted material was cooled, the larger crystals could be grown. It is interesting to note that Erdős problem has a typical "crystalline" structure due to the symmetry of the matrix L in our representation.[3] The literature on Simulated annealing is broad, and the technique has been used for numerous problems. See e.g. Dowsland [9] for a survey. Most papers however agree on the fact that annealing performs better on uniform data than on data which are clustered, due to the smoother topography generated by the uniform problems. Erdős problem has an extremely uniform formulation.

The simulated annealing process we used has the normal structure occurring in the literature, thus the reader is referred to [9] for a general introduction. We will here only outline the specific choices made for adapting the heuristic to our problem. The main structure of the algorithm may be sketched as:

[3] We used the cyclic representation of the line-to-point incidence matrix of the given Galois-plane, [13].

```
starting solution s_0 is x_i = 0 for i = 1, ..., n
initial temperature is t ← T
repeat
  for i = 1 to M do
    randomly select s ∈ N(s_0)
    δ ← f(s) − f(s_0)
    if δ < 0 then s_0 ← s
    else
      x ← random[0, 1]
      if (x < e^{−δ/t}) then s_0 ← s
  end
  t ← αt
until stop criteria
```

The starting temperature was chosen as $T = 2.0$ as this gave an appropriate initial accept ratio. The cooling factor was chosen as $\alpha = 0.9995$ and we decreased the temperature after $M = 10\,000$ iterations of the inner loop. If no solution was accepted within a period of qM iterations, the process was terminated. An upper limit on the number of iterations was set to $K = 100\,000\,000$, but in all cases the search stopped before this limit was reached.

The neighbourhood function $N(s)$ was constructed as follows: Basically we wish to choose a random variable x_j and change its value to $1 - x_j$. Since the number of variables with value 1 however is far smaller than the number of variables with value 0 we would mainly investigate transitions $0 \to 1$ and very seldom $1 \to 0$. Thus two sets V_0 and V_1 are maintained, such that $x_j = 0, j \in V_0$ and $x_j = 1, j \in V_1$. The neighbourhood function now chooses one of the sets V_0 and V_1 with equal probability, and then randomly selects a variable x_j, $j \in V_i$, whose value is changed to $1 - x_j$. Both feasible and infeasible solution vectors x were accepted since this gave most freedom to the algorithm to investigate the solution space.

The objective function of (*ILP*) was not suitable as objective function for the simulated annealing algorithm. Instead a value of γ was chosen, and the problem was solved as a feasibility problem, measuring how much the constraints were violated. A good choice of γ was $\gamma = 1.8 \ln(q)$. Then the objective function f could be expressed as

$$f(x) = \sum_{i=1}^{n} p(\textstyle\sum_{j=1}^{n} L_{ij} x_j,\ \gamma)$$

where $p(a, b)$ is a punishment function chosen as

$$\begin{aligned} p(a,b) &= 4 && \text{if } a < 1, \\ p(a,b) &= (b-a)^2 && \text{if } a > b. \end{aligned}$$

Thus the principle is that each violation of the constraint $Lx \geq e$ is punished by 4 while a violation of $Lx \leq \gamma e$, is punished with the quadratic distance from γ, for each lefthand side exceeding γ. The quadratic expression proved to perform well, since we prefer to have several constraints violated slightly than to have one constraint violated a lot (and thus pushing the dimension γ upward).

The objective function f can be evaluated in $O(q)$ time for each iteration, since only one variable x_j is changed and there are q entries in L with $L_{ij} = 1$. Knowing the previous value of Lx, it is easy to derive the next value Lx' when moving from a solution x to x'. Also the

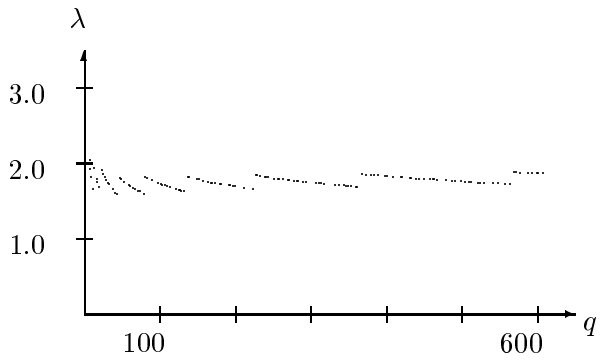

Figure 1: $\lambda = \gamma(B)/\ln(q)$ as function of q

quadratic expressions in $p(a,b)$ can be changed to an additive version by making a table over differences between the square numbers, thus saving the multiplications.

Each time a solution was obtained with an improved objective value, it was checked whether it satisfies $Lx \geq e$. If this was the case, the improved solution was saved. If a solution was found which satisfies all constraints for the given value of γ, we terminated the solution process. An experiment was run, where γ was decreased each time a solution satisfying $e \leq Lx \leq \gamma e$ was found, but it was not possible to prove feasibility of the tighter problem. Thus this idea was abandoned.

The total running time of the simulated annealing algorithm was thus $O(Kq)$ where K is the upper limit on the number of iterations. The process could often be terminated much earlier since a solution with objective value γ was found.

The incidence matrix L of the projective plane was generated from a difference set using the relation described in (4). The difference set was constructed using a procedure suggested by Moorhouse [15]. Fortunately it was not necessary to store the whole matrix L since all entries can be derived from l_1 in constant time. This brought the space consumption down to $O(n)$ thus making it possible to solve even very large problems with up to $n = 369057$ variables.

4 Computational results

The simulated annealing algorithm was programmed in C and run on a HP9000/735 with 99Mhz processor. We were in the privileged situation that "enough" computational time was available. So as can be seen from our parameters, a very slow cooling rate could be applied. Furthermore each problem was restarted 10 times, to smooth out statistical variations in the solution quality. The total CPU time used for this series of tests was more than 38 days. On the other hand this means that significantly better solutions cannot be expected by the described method just by increasing the computational time.

Prime and prime power values of q between 7 and 607 were considered as presented in Table 1-5. The first two tables give the general solution values while the last three give a more precise description of the blocking set found with the smallest covering number. The entries are as follows:

- q is the order of the projective plane.
- $n = q^2 + q + 1$ is the number of binary variables. Each binary variable corresponds to one of the points of the projective plane.

Table 1: General information about the found solutions

q	n	$\|B\|$	$\gamma(B)$	λ	t
7	57	12	4	2.06	1872
8	73	19	4	1.92	1
9	91	13	4	1.82	1555
11	133	21	4	1.67	54
13	183	24	5	1.95	2262
16	273	33	5	1.80	2411
17	307	44	5	1.76	79
19	381	47	5	1.70	147
23	553	58	6	1.91	2908
25	651	63	6	1.86	2891
27	757	66	6	1.82	2971
29	871	85	6	1.78	137
31	993	86	6	1.75	164
32	1057	90	6	1.73	155
37	1407	106	6	1.66	235
41	1723	116	6	1.62	302
43	1893	126	6	1.60	1135
47	2257	135	7	1.82	3919
49	2451	158	7	1.80	238
53	2863	169	7	1.76	288
59	3541	194	7	1.72	252
61	3783	199	7	1.70	315
64	4161	206	7	1.68	315
67	4557	219	7	1.66	352
71	5113	230	7	1.64	364
73	5403	238	7	1.63	516
79	6321	258	7	1.60	680
81	6643	263	8	1.82	6013
83	6973	269	8	1.81	6701
89	8011	325	8	1.78	436
97	9507	349	8	1.75	519
101	10303	366	8	1.73	543
103	10713	375	8	1.73	549
107	11557	389	8	1.71	561
109	11991	391	8	1.71	612
113	12883	409	8	1.69	630
121	14763	440	8	1.67	713
125	15751	460	8	1.66	797
127	16257	455	8	1.65	824
128	16513	470	8	1.65	875
131	17293	477	8	1.64	1877
137	18907	505	9	1.83	10065
139	19461	512	9	1.82	11036
149	22351	599	9	1.80	827
151	22953	618	9	1.79	787
157	24807	632	9	1.78	840
163	26733	658	9	1.77	899
167	28057	672	9	1.76	902
169	28731	684	9	1.75	928
173	30103	695	9	1.75	1029
179	32221	725	9	1.73	1047
181	32943	726	9	1.73	1104

q	n	$\|B\|$	$\gamma(B)$	λ	t
191	36673	764	9	1.71	1276
193	37443	772	9	1.71	1205
197	39007	791	9	1.70	1278
199	39801	803	9	1.70	1150
211	44733	849	9	1.68	1569
223	49953	902	9	1.66	14427
227	51757	914	10	1.84	18045
229	52671	927	10	1.84	17968
233	54523	941	10	1.83	18711
239	57361	974	10	1.83	18642
241	58323	989	10	1.82	18894
243	59293	993	10	1.82	19273
251	63253	1033	10	1.81	19771
256	65793	1052	10	1.80	19803
257	66307	1055	10	1.80	20020
263	69433	1166	10	1.79	1570
269	72631	1187	10	1.79	1666
271	73713	1208	10	1.79	1545
277	77007	1237	10	1.78	1603
281	79243	1234	10	1.77	1768
283	80373	1250	10	1.77	1546
289	83811	1279	10	1.76	2082
293	86143	1290	10	1.76	1868
307	94557	1356	10	1.75	1932
311	97033	1373	10	1.74	1860
313	98283	1378	10	1.74	2259
317	100807	1401	10	1.74	2170
331	109893	1465	10	1.72	2586
337	113907	1493	10	1.72	2922
343	117993	1516	10	1.71	3940
347	120757	1539	10	1.71	3754
349	122151	1545	10	1.71	3537
353	124963	1565	10	1.70	3721
359	129241	1593	10	1.70	26042
361	130683	1605	10	1.70	12792
367	135057	1638	11	1.86	46182
373	139503	1665	11	1.86	46547
379	144021	1705	11	1.85	51259
383	147073	1722	11	1.85	55627
389	151711	1745	11	1.84	56922
397	158007	1777	11	1.84	60157
401	161203	1802	11	1.84	60014
409	167691	1840	11	1.83	64788
419	175981	1887	11	1.82	66379
421	177663	1903	11	1.82	66773
431	186193	1956	11	1.81	69831
433	187923	1958	11	1.81	67941
439	193161	1994	11	1.81	72228
443	196693	2012	11	1.81	74514
449	202051	2043	11	1.80	75462
457	209307	2206	11	1.80	6183
461	212983	2234	11	1.79	5727

Table 2: General information about the found solutions

q	n	$\lvert B\rvert$	$\gamma(B)$	λ	t
463	214833	2233	11	1.79	6331
467	218557	2255	11	1.79	6486
479	229921	2304	11	1.78	6846
487	237657	2350	11	1.78	7768
491	241573	2382	11	1.78	7324
499	249501	2398	11	1.77	7651
503	253513	2421	11	1.77	8062
509	259591	2446	11	1.76	8135
512	262657	2461	11	1.76	8293
521	271963	2515	11	1.76	10085
523	274053	2512	11	1.76	8656
529	280371	2546	11	1.75	8926
541	293223	2609	11	1.75	22197
547	299757	2641	11	1.74	11348
557	310807	2702	11	1.74	64630
563	317533	2716	11	1.74	13039
569	324331	2763	12	1.89	116238
571	326613	2761	12	1.89	123373
577	333507	2797	12	1.89	124763
587	345157	2844	12	1.88	124678
593	352243	2883	12	1.88	131083
599	359401	2918	12	1.88	130924
601	361803	2925	12	1.88	134580
607	369057	2938	12	1.87	135926

- $|B|$ is the size of the blocking set.
- $\gamma(B)$ is the smallest covering number found.
- λ is the quotient $\gamma(B)/\ln(q)$.
- t is the time used for the solution, measured in seconds.
- $1, \ldots, 12$ are the number of i-secants of the blocking set with the smallest covering number, where $i = 1, \ldots, 12$. The numbers of i-secants give some information about the structure of the blocking set.

As seen from the tables, the found solutions have a very uniform structure.

¿From Figure 1 it can be seen that the quotient $\lambda = \gamma(B)/\ln(q)$ is less than 2 for all problems $q \geq 8$ and it becomes as low as 1.63 for some instances. Thus we have shown that projective planes of order q, $7 \leq q \leq 607$, q prime or prime power, has covering number $\gamma(\Pi(q)) < 2\ln(q)$. This does not answer Erdős problem, but may help future investigation.[4]

Figure 2 shows that our numerical experiences does not give indication of existence (or non-existence) of absolute constant γ^*. But the structure of the blocking sets found – described in Table 4-6 – gives some hints about the number of i-secants, which can be useful for further theoretical investigations.

On Figure 3 the size of the blocking sets is plotted together with the known lower and upper bounds. We may hope that larger blocking sets can have much more special structure in the

[4]The blocking sets found are available from the authors upon request.

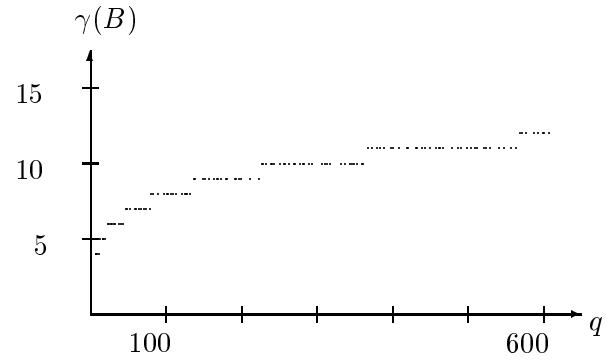

Figure 2: $\gamma(B)$ as function of q

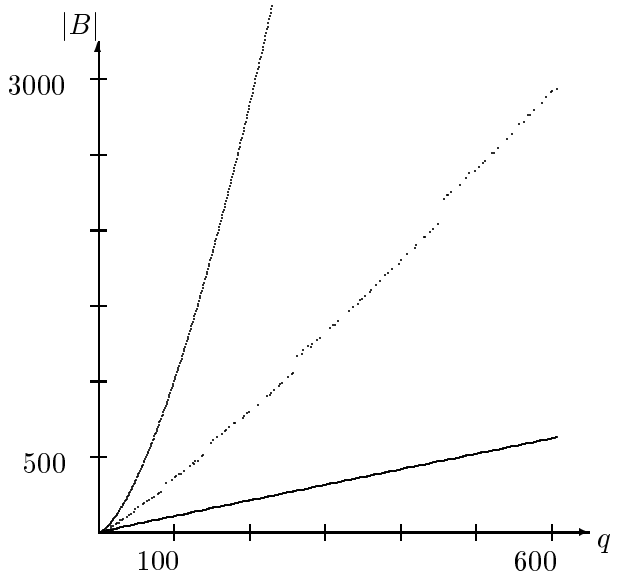

Figure 3: $|B|$ as function of q, lower bound $q+\sqrt{q}+1$, upper bound $q\sqrt{q}+1$

sense that all secants contain fewer points. The size of the obtained blocking sets are far from the upper bounds, thus there is a hope for the existence of blocking sets with smaller covering number for most of the studied cases.

Using the bounds of Béres and Illés [2], described in Result 1 we can modify Figure 3, getting more strict bounds on the size of the blocking sets. Result 1 says that the size of the blocking set depends on the covering number of it, as well. These bounds can be used as cuts in the (*ILP*) formulation of the problem.

5 Concluding remarks

Several attempts were done before reaching the current results. The integer programming approach was not successful because continuous bounds are too weak. Also Lagrangian relaxation of the problem leads to a useless formulation, since the Lagrangian relaxation is weaker than the continuous relaxation. A constructive heuristic was investigated by Béres and Illés [2], but it could not solve large sized problems in reasonable time. We have experimented with tabu search in our research, but the method performed poorly since the uniform problem structure means

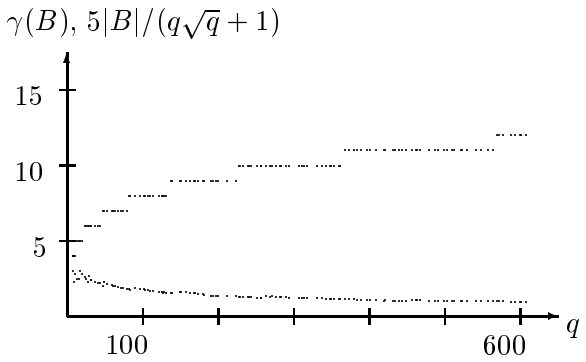

Figure 4: $\gamma(B)$ compared to $|B|/(q\sqrt{q}+1)$ as function of q (the latter is scaled by a factor 5)

that the process stucks easily in a local minima, or somehow repeatedly investigates symmetrical solutions.

Based on the numerical experiences presented in this paper we hope that the existence of blocking sets B with covering number $\gamma(B) < 2\log\ q$ theoretically can be proved for all order, which will improve the result by Abbott and Liu [1].

Numerical results illustrated by Figure 3 suggest that blocking sets with large size can be related to the problem of Erdős in the sense that (relatively) bigger blocking sets contain less points on each secants than the smaller ones. This inspiration is illustrated on Figure 4. The figure shows that when the ratio $|B|/(q\sqrt{q}+1)$ is decreasing, i.e. when the size of the blocking set B is (relatively) small comparing to the possible size of it, then the covering number $\gamma(B)$ is increasing with the same trend.

The present work has demonstrated that metaheuristics can be an efficient tool for solving difficult mathematical problems. Our results demonstrate that the currently best known upper bounds are not tight for $q \leq 607$ and thus it is our hope that the solutions found can serve as inspiration for further theoretical work.

Since the problem has a very compact formulation despite being extremely difficult to solve, we believe that it is well suited as benchmark test for different metaheuristics. A generator of the instances as well as our results can be found at the internet, and we hope that other researchers will take up the challenge. The address is `http://www.diku.dk/~pisinger/erdos.html`.

Acknowledgement

The first author thanks the "Állami Eötvös Ösztöndíj" given by the Hungarian State Fellowship Board for the period of May - July, 1995 spent in Copenhagen when this research project was started. This research was partially supported by Hungarian National Research Council (grants OTKA T 014302 and OTKA T 019492).

This paper was completed while the first author held a research fellowship of Delft University of Technology. The authors appreciate valuable comments given by Professor T. Terlaky and Dr. D. Pasechnik on the earlier version of the paper. They made possible a considerable improvement of the presentation.

Table 3: Geometrical properties

q	1	2	3	4	5	6	7	8	9	10	11	12
7	36	12	0	9								
8	29	9	16	19								
9	78	0	0	13								
11	84	0	28	21								
13	117	9	33	18	6							
16	137	55	27	37	17							
17	104	56	56	47	44							
19	144	68	63	59	47							
23	192	130	71	75	83	2						
25	230	144	94	82	96	5						
27	284	172	95	103	95	8						
29	206	197	173	124	91	80						
31	271	231	186	136	97	72						
32	282	234	213	147	93	88						
37	370	319	231	223	149	115						
41	456	417	288	229	196	137						
43	474	422	341	255	223	178						
47	571	545	410	281	244	197	9					
49	448	544	467	403	303	166	120					
53	566	607	546	458	353	220	113					
59	604	795	697	540	430	280	195					
61	653	870	736	589	438	288	209					
64	772	932	806	647	479	322	203					
67	818	992	879	741	529	342	256					
71	949	1110	1004	796	601	381	272					
73	994	1159	1050	860	614	442	284					
79	1155	1357	1242	1004	695	522	346					
81	1199	1524	1243	1036	766	512	360	3				
83	1281	1517	1429	1065	742	556	376	7				
89	1030	1450	1660	1395	1046	720	470	240				
97	1264	1820	1923	1655	1227	823	524	271				
101	1365	1896	2084	1848	1350	872	555	333				
103	1360	2030	2168	1881	1398	919	608	349				
107	1484	2197	2328	2025	1459	1052	653	359				
109	1592	2343	2438	2059	1530	1022	656	351				
113	1733	2382	2597	2226	1736	1121	676	412				
121	1891	2905	2838	2564	1933	1335	842	455				
125	2018	2848	3164	2727	2118	1424	904	548				
127	2227	3137	3278	2736	2127	1402	886	464				
128	2134	2999	3295	2917	2140	1498	983	547				
131	2246	3292	3450	2900	2332	1540	980	553				
137	2386	3473	3728	3373	2481	1663	1126	676	1			
139	2447	3634	3844	3362	2567	1753	1201	652	1			
149	2058	3503	4283	4110	3306	2372	1453	830	436			
151	1991	3465	4348	4197	3430	2536	1582	893	511			
157	2264	3889	4767	4536	3725	2574	1602	964	486			
163	2418	4208	5111	4843	3950	2862	1792	1034	515			
167	2528	4465	5454	4982	4259	2929	1820	1041	579			
169	2512	4591	5463	5293	4165	3027	1969	1144	567			
173	2798	4726	5793	5463	4500	3108	1994	1146	575			
179	2921	4981	6107	5899	4865	3354	2170	1255	669			
181	3085	5201	6260	6114	4813	3477	2117	1221	655			

Table 4: Geometrical properties

q	1	2	3	4	5	6	7	8	9	10	11	12
191	3401	5875	7039	6845	5325	3761	2319	1356	752			
193	3527	5974	7192	6850	5470	3831	2507	1396	696			
197	3708	6033	7481	7139	5829	4048	2513	1483	773			
199	3683	6194	7471	7391	6000	4075	2641	1499	847			
211	4093	7075	8553	8260	6609	4619	2875	1679	970			
223	4536	7818	9456	9249	7237	5353	3278	1971	1055			
227	4706	8269	9920	9378	7660	5329	3411	2033	1049	2		
229	4756	8208	10038	9704	7774	5439	3567	2033	1149	3		
233	4989	8550	10343	10019	8062	5647	3651	2112	1145	5		
239	5111	8776	10860	10481	8629	5960	3971	2294	1251	28		
241	5096	8775	10982	10632	8751	6301	4046	2347	1371	22		
243	5238	9124	11063	10796	8891	6398	4010	2454	1302	17		
251	5459	9447	11916	11576	9492	6833	4361	2652	1460	57		
256	5756	9816	12225	12298	9848	7032	4538	2690	1509	81		
257	5701	10070	12555	12041	9910	7194	4565	2665	1529	77		
263	4438	8692	12131	12899	11113	8400	5668	3350	1848	894		
269	4700	9282	12733	13377	11780	8662	5796	3572	1791	938		
271	4626	9180	12692	13558	11955	9014	6046	3679	1961	1002		
277	4688	9672	13258	14179	12555	9279	6366	3798	2151	1061		
281	5254	10284	13797	14731	12748	9514	6251	3689	1992	983		
283	5193	10318	13960	14818	12914	9793	6494	3748	2101	1034		
289	5288	10758	14729	15339	13471	10082	6788	4034	2292	1030		
293	5683	10922	15270	15909	13748	10520	6710	4061	2231	1089		
307	6071	12194	16403	17505	15297	11274	7572	4567	2449	1225		
311	6295	12319	17010	18028	15696	11493	7750	4629	2549	1264		
313	6420	12726	17123	18124	15968	11872	7627	4576	2584	1263		
317	6479	12951	17573	18519	16255	12125	8187	4802	2568	1348		
331	7090	13910	19265	20184	17598	13395	8798	5356	2825	1472		
337	7269	14517	19798	20973	18403	13736	9118	5574	2994	1525		
343	7648	15103	20513	21719	19008	14241	9550	5573	3065	1573		
347	7782	15214	20941	22285	19416	14576	9946	5774	3181	1642		
349	7899	15524	21194	22553	19590	14863	9789	5935	3162	1642		
353	8024	15785	21845	22925	19995	15226	10075	6080	3395	1613		
359	8266	16393	22367	23749	20786	15806	10319	6378	3462	1715		
361	8374	16362	22697	23918	20894	16089	10629	6487	3484	1749		
367	8358	17140	23042	24699	21839	16705	10893	6734	3798	1845	4	
373	8725	17365	24061	25549	22580	17207	11188	7070	3735	2010	13	
379	8744	17671	24455	26187	23700	17727	11976	7264	4094	2184	19	
383	8930	18119	24862	27011	24020	18063	12280	7312	4269	2182	25	
389	9359	18564	25934	27940	24594	18729	12426	7615	4293	2209	48	
397	9770	19616	26935	29052	25726	19436	13017	7689	4384	2304	78	
401	9767	19812	27499	29565	26283	19790	13409	8015	4598	2379	86	
409	10016	20606	28747	30682	27290	20647	13855	8445	4826	2455	122	
419	10698	21412	29831	32240	28776	21692	14647	9005	4989	2538	153	
421	10608	21582	29984	32245	28992	22206	15018	9127	5120	2647	134	
431	10857	22397	31412	33819	30288	23427	15860	9637	5432	2881	183	
433	11120	22775	31726	34493	30487	23461	15789	9630	5428	2818	196	
439	11213	23226	32457	35181	31459	24230	16488	10075	5620	3003	209	
443	11506	23508	32878	36194	31973	24659	16820	10143	5651	3137	224	
449	11746	24071	33820	36864	32886	25347	17364	10738	5820	3143	252	
457	9447	20965	31955	37275	35397	28522	20274	12737	7120	3770	1845	
461	9448	21160	32245	37973	35847	29081	20724	13205	7559	3898	1843	

Table 5: Geometrical properties

q	1	2	3	4	5	6	7	8	9	10	11	12
463	9695	21707	32720	38233	36468	29251	20685	12980	7363	3878	1853	
467	9913	21892	33157	38968	36994	29896	21131	13149	7596	3990	1871	
479	10385	23454	35543	40838	38667	31375	22054	13681	7918	4093	1913	
487	10816	23761	36190	42518	40169	32311	23007	14376	8081	4385	2043	
491	10678	23937	36492	42758	41041	33164	23401	14917	8498	4487	2200	
499	11368	25551	38284	44763	41733	34006	24000	14922	8366	4333	2175	
503	11408	25663	39402	44909	42922	34500	23990	15164	8950	4449	2156	
509	12044	26296	39818	46498	43673	35411	24808	15406	8871	4622	2144	
512	12003	26659	40632	46870	44110	35910	24877	15861	8815	4696	2224	
521	12228	27392	41716	48311	45501	37332	26151	16590	9558	4894	2290	
523	12469	28217	42039	49018	46206	37251	26113	16352	9130	4955	2303	
529	12834	28687	42656	49781	47523	38179	26948	16840	9516	5086	2321	
541	13310	29315	45137	52320	49377	39906	28143	17677	10171	5367	2500	
547	13455	30140	45899	53191	50708	40941	28734	18181	10400	5488	2620	
557	13807	30653	47396	54812	52332	42926	30124	19107	11008	5907	2735	
563	14364	31991	48604	56325	53689	43490	30518	18945	11074	5734	2799	
569	14334	32098	49054	57204	54723	44743	31590	20041	11510	6099	2929	6
571	14495	32663	50177	58031	54944	44437	31498	20075	11480	5877	2934	2
577	15012	32922	50340	59112	56795	45585	32380	20342	11734	6292	2981	12
587	15179	34852	52204	60938	58282	47258	33675	21192	12068	6425	3064	20
593	15379	34955	52762	62515	59686	48312	34269	21842	12578	6685	3226	34
599	15811	34909	54168	63400	60832	49408	35316	22378	12998	6797	3337	47
601	15746	35660	54514	63783	61038	50077	35331	22558	12805	6814	3432	45
607	16664	36695	55933	65476	62646	50110	35986	22684	12720	6820	3273	50

References

[1] Abbott, H.L., Liu, A., Property $B(s)$ and projective planes, *Ars Combinatoria*, **20** (1985) 217-220.

[2] Béres L., Illés T., Kis rendű projektív síkok metszésszámának számítógépes vizsgálata, (In Hungarian. English title: Computational investigation of the covering number of finite projective planes with small order), *Alkalmazott Matematikai Lapok*, **3-4.** (1993), to appear.

[3] Boros E., $PG(2,q), p > 2$ has property $B(p+2)$, *Ars Combinatoria*, **25** (1988) 111-114.

[4] Bruen, A.A., Baer subplanes and blocking sets, *Bull. Amer. Math. Soc.* **76** (1970) 342-344.

[5] Bruen, A.A., Thas, J.A., Blocking sets, *Geom. Dedicata* **6** (1977) 193-203.

[6] Bruen, A.A., Fischer, J.C., Blocking sets and complete k-arcs, *Pacific Journal of Math.* **53** (1974) 73-84.

[7] Burgess, D., The distribution of quadratic residues and non-residues, *Mathematica* **4** (1957) 106-112.

[8] CPLEX manual version 2.1., CPLEX Optimization, Inc., 1993.

[9] K.A. Dowsland, Simulated Annealing, In: C.R.Reeves (ed.) *Modern Heuristic Techniques for Combinatorial Problems*, Mc-Graw Hill, London, UK (1995) 20–69.

[10] Erdős P., Silvermann, R., Stein, A., Intersection properties of families containing sets of nearly the same size, *Ars Combinatoria*, **15** (1983) 247-259.

[11] Hirschfeld, J. W. P. *Projective geometries over finite fields*, (Oxford University Press, Oxford 1979).

[12] Illés T., Szőnyi T., Wettl F., Blocking sets and maximal strong representative systems in finite projective planes, *Mitt. Math. Sem. Giessen* **201** (1991) 97-107.

[13] Kárteszi F., *Introduction to finite geometries*, (Akadémiai Kiadó, Budapest 1974).

[14] N. Metropolis, A.W. Rosenbluth, M.N. Rosenbluth, A.H. Teller and E. Teller, Equation of state calculation by fast computing machines, *J.of Chem. Phys.*, **21** (1953) 1087–1091.

[15] E. Moorhouse, Private communication, 1996.

[16] Szőnyi T., Note on the existence of large minimal blocking sets in Galois planes, *Combinatorica* **12** (1992) 227-235.

[17] Szőnyi T., Blocking sets in finite planes and spaces, *Ratio Mathematica* **5** (1992) 93-106.

Tibor Illés
Eötvös Loránd University
Department of Operations Research
Múzeum krt. 6-8.
H-1088 Budapest, Hungary
E-mail: illes@math.elte.hu

David Pisinger
University of Copenhagen
Department of Computer Science
Universitesparken 1
DK-2100 Copenhagen, Denmark
E-mail: pisinger@diku.dk