Finding Simple t-Designs by Using Basis Reduction

Donald L. Kreher and Stanisław P. Radziszowski

Rochester Institute of Technology
School of Computer Science and Technology

ABSTRACT

In 1976, Kramer and Mesner observed that finding a t-design with a given automorphism group can be reduced to solving a matrix problem of the form

$$AX = M, \quad X[i] = 0 \text{ or } 1, \quad \text{for all } i, \quad 1 \le i \le n,$$

where A is an m by n positive integer matrix built from the required automorphism group and M is a particular m dimensional integer vector. This problem is NP-complete. We present an algorithm that searches for a solution when given an instance of this 0-1 matrix problem. This algorithm always halts in polynomial time but does not always find a solution when one exists. The problem is first converted to one of finding a particular short vector in a lattice and then uses a lattice basis reduction algorithm due to A.K. Lenstra, H.W. Lenstra and L. Lovász [9] to attempt to find it. We apply this method to the search for simple t-designs with $t \ge 6$ and duplicate the results of Leavitt, Kramer and Magliveras [3,10] in substantially shorter time. Furthermore, a new simple 6-design was found using the algorithm described in this paper.

1. Introduction

A *t-design*, or t–(v,k,λ) *design* is a pair $(X,\mathcal{B})$ with a v-set X of *points* and a family $\mathcal{B}$ of k-subsets of X called *blocks* such that any t points are contained in exactly λ blocks. The problem is of course to find them. As an illustration of the principles involved in our algorithm we give a small example.

Example of a 2-(7,3,1) design.

The well known projective plane of order 2 is the 2-(7,3,1) design $(X,\mathcal{B})$ given by:

$$X = \{1,2,3,4,5,6,7\}$$

and

$$\mathcal{B} = \{124,235,346,457,156,267,137\}$$

Both authors were supported in part by the National Science Foundation under grant DCR-8606378

This design can be represented by the picture found in figure 1. The points of the 6 lines and 1 circle in this picture form the blocks of this design.

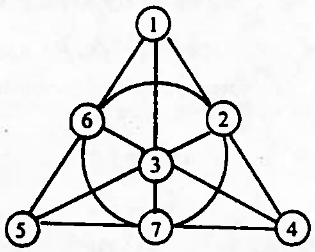


Figure 1: The 2-(7,3,1) design.

An *automorphism* of a t-(v,k,λ) design (X,*B*) is a permutation of X which preserves *B*. It is clear from figure 1 that this 2-(7,3,1) design has

$$G = \langle(1\ 4\ 5)(2\ 7\ 6),(2\ 6)(4\ 5)\rangle \simeq S_3$$

as an automorphism group. We note that the full automorphism group of this design is $PSL_2(7)$ and is generated by (1 4 5)(2 7 6), (2 6)(4 5), and (1 2 3 4 5 6 7).

In 1973, Kramer and Mesner [4] made the following observation:

A t-(v,k,λ) design exists with $G \leq Sym(X)$ as an automorphism group if and only if there is a (0,1)-solution U to the matrix equation

$$A_{tk}U = \lambda J_m, \qquad (1)$$

where:

a. The m rows of A_{tk} are labeled by the G-orbits of t-subsets of X;

b. The n columns of A_{tk} are labeled by the G-orbits of k-subsets of X;

c. $A_{tk}[\Delta,\Gamma] = |\{K \in \Gamma : K \supset T_0\}|$ where $T_0 \in \Delta_i$ is any representative;

d. $J_m = [1,1,1,...,1]^T$.

Following our example, the A_{23} matrix for $G = \langle(1\ 4\ 5)(2\ 7\ 6),(2\ 6)(4\ 5)\rangle \simeq S_3$, is given in figure 2. Observe that $U = [0,1,0,0,0,0,1,0,0,1]^T$ gives a solution to the equation $A_{23}U = \lambda J_m$ with $\lambda = 1$ and thus gives a 2-(7,3,1) design.

This single observation led directly to the discovery of many previously unknown designs, and probably has the best chance in leading to the discovery of an infinite family of t-designs with $t \geq 6$ and *small* λ. Recently Teirlink [11] has shown to our amazement, using other techniques, that there exist simple t-designs for all values of t, however, these designs

	123 347 136 356 357 234	124 457 156	125 147 146 456 157 245	126 247 567
(12 47 16 56 57 24)	1	1	1	1
(13 34 35)	2	0	0	0
(14 45 15)	0	1	2	0
(17 46 25)	0	0	2	0
(23 37 36)	2	0	0	0
(26 27 67)	0	0	0	1
		↑		

Figure 2. The A_{23} matrix of G = <

have $\lambda=(t+1)!^{(2t+1)}$. In particular, the following sig were obtained by solving equation (1):

1975: A 5-(17,8,80) the first example of a Kramer [2].

1984: A 5-(33,6,42) and a 5-(33,7,126) the se an odd number of points, Magliveras ar

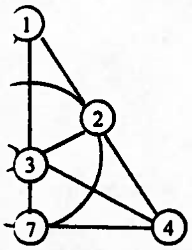
1984: A 6-(33,8,36) the first example of a 6-d

1984: A 6-(20,9,112) the second example Magliveras [3].

Recently, we have discovered a 5-(13,6,4) design techniques described below.

In order to effectively use the Kramer-Mesner need to be solved.

re found in figure 1. The points of the 6 lines
this design.



: 2-(7,3,1) design.

(X,B) is a permutation of X which preserves B.
sign has

- 6),(2 6)(4 5)> $\simeq$ S_3

the full automorphism group of this design is
2 6)(4 5), and (1 2 3 4 5 6 7).

ollowing observation:

m(X) as an automorphism group if and only
trix equation

$= \lambda J_m$ (1)

the G-orbits of t-subsets of X;
d by the G-orbits of k-subsets of X;
ere $T_0 \in \Delta_i$ is any representative;

G = <(1 4 5)(2 7 6),(2 6)(4 5)> $\simeq$ S_3, is given in
0,1]^T gives a solution to the equation $A_{23}U = \lambda J_m$

to the discovery of many previously unknown
in leading to the discovery of an infinite family of
Teirlink [11] has shown to our amazement , using
-designs for all values of t, however, these designs

	123 347 136 356 357 234	1?4 45? 15?	125 147 146 456 157 245	126 247 567	127 467 167 256 257 246	134 345 135	137 346 235	145	236 237 367	267
(12 47 16 56 57 24)	1	[illegible]	1	1	1	0	0	0	0	0
(13 34 35)	2	[illegible]	0	0	0	2	1	0	0	0
(14 45 15)	0	[illegible]	2	0	0	1	0	1	0	0
(17 46 25)	0	[illegible]	2	0	2	0	1	0	0	0
(23 37 36)	2	[illegible]	0	0	0	0	1	0	2	0
(26 27 67)	0	[illegible]	0	1	2	0	0	0	1	1
							↑			↑

Figure 2. The A_{23} matrix of G = <(1 4 5)(2 7 6),(2 6)(4 5)>

have $\lambda=(t+1)!^{(2t+1)}$. In particular, the following significant results in the theory of t-designs were obtained by solving equation (1):

1975: A 5-(17,8,80) the first example of a 5-design on an odd number of points, Kramer [2].

1984: A 5-(33,6,42) and a 5-(33,7,126) the second and third examples of 5-designs on an odd number of points, Magliveras and Leavitt [10].

1984: A 6-(33,8,36) the first example of a 6-design, Magliveras and Leavitt [10].

1984: A 6-(20,9,112) the second example of a 6-design, Kramer, Leavitt and Magliveras [3].

Recently, we have discovered a 5-(13,6,4) design [7] and a 6-(14,7,4) design using the techniques described below.

In order to effectively use the Kramer-Mesner observation the following three problems need to be solved.

1. Create a list of groups that are good candidates for finding t-designs;
2. Find an efficient algorithm for constructing the A_{tk} matrices;
3. Obtain an effective procedure for solving the equation $A_{tk}U = \lambda J_m$ for (0,1)-vector U.

We propose to solve the last of these problems by using basis reduction. We already have found a solution to 2 although its efficiency could still be improved. The projective special linear groups seem to be good candidates for finding t-designs, see [3], however other groups have also proved to be fruitful. Thus a careful study of the algebra of the A_{tk} matrices [5,6] should be completed.

2. The Algorithm

Let X be a v-set, $G \leq Sym(X)$ and consider the matrix **B** below:

$$B = \begin{bmatrix} I_n & 0 \\ A_{tk} & -\lambda J_m \end{bmatrix} \qquad (2)$$

where A_{tk} is the m by n Kramer-Mesner matrix described in (1) and I_n is the n by n identity matrix. Let $\mathbb{L}$ be the n+1 dimensional lattice spanned by the columns of **B**. That is:

$$\mathbb{L} = \{R \in \mathbb{Z}^{m+n} : R = B \cdot S, \text{ for some } S \in \mathbb{Z}^{n+1}\}.$$

Let E_m be the m-dimensional zero vector. Then the following proposition is clear:

PROPOSITION 1: $A_{tk}U = d \cdot \lambda J_m$ *for some integer* d *if and only if* $[U,E_m]^T \in \mathbb{L}$.

Thus to find a (0,1)-solution U to $A_{tk}U = \lambda J_m$ we need only look for a linear combination $U = [U,E_m]^T$ of the columns of B such that U is a (0,1)-vector. If $U \neq J_m$ then we will have found a t-(v,k,d·λ) design for some positive integer d. Note that since the complement of a design is a design then $\|U\|^2 \leq n/2$. That is, U is a particular short vector in $\mathbb{L}$. Our algorithm will try to find for $\mathbb{L}$ a new basis all of whose vectors are as short as we can make them.

2.1. Tools

Before describing our algorithm, we introduce the basic concepts about integer lattices and the L^3 algorithm we use.

Let n be a positive integer. A subset $\mathbb{L}$ of the n-dimensional real vector space R^r, $r \geq n$ is called a *lattice* iff there is a basis $B = \{b_1, b_2, \dots, b_n\}$ of an n-dimensional subspace of R^r such that every member of $\mathbb{L}$ is an <u>integer</u> linear combination of the vectors in B. Recall that given a basis $B = \{b_1, b_2, \dots, b_n\}$ of an n-dimensional subspace of R^r, an orthogonal basis $B^* = \{b_1^*, b_2^*, \dots, b_n^*\}$ of it may be obtained inductively via the Gram-Schmidt process of

orthogonalization as follows:

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*, \text{ for } 1 \leq i \leq n,$$

$$\mu_{ij} = (b_i, b_j^*)/(b_j^*, b_j^*), \text{ for } 1 \leq j < i \leq n,$$

where (·,·) denotes the ordinary inner product on lattice $\mathbb{L}$ will be said to be *y-reduced (or reduced*

i) $|\mu_{ij}| \leq ½$ for $1 \leq j < i \leq n$,

ii) $\|b_i^* + \mu_{ii-1} b_{i-1}^*\|^2 \geq y \cdot \|b_{i-1}^*\|^2$ for $1 < i \leq n$,

where y, ¼ < y < 1 is a constant and ‖·‖ denotes (1982) describe an algorithm, which when present $B = [b_1, b_2, \dots, b_n]$ for a lattice $\mathbb{L}$ as input, produ output. The L^3 algorithm consists of applying transformations:

T1: Interchange vectors b_i and b_{i-1} if $\|b_i^* + \mu_{ii-}$ $1 < i \leq n$, and the global constant $y \in (¼,1)$.

T2: Replace b_i by $b_i - rb_j$, where r = round($|\mu_{ij}| > ½$, for some $1 \leq j < i \leq n$.

The efficient implementation of the sequen mainly on the fact, that old values of μ_{ij} and transformation without using the full process of orth the transformations T1 and T2 using a strateg however as H.W.Lenstra [9] remarks, <u>any</u> sequence the reduced basis.

The L^3 algorithm terminates when neither situation implies that conditions i) and ii) are satisf integer approximation to the basis B^* defined by the and as a consequence contains short vectors, as ca Lenstra et al. [9, prop. 1.11]:

PROPOSITION 2: *Let* $B' = [b_1', b_2', \dots, b_n']$ *be a reduc*

$$\|b_1'\|^2 \leq 2^{n-1} \min(\|b\|^2 : b \in$$

.dates for finding t-designs;

ıg the A_{tk} matrices;

the equation $A_{tk}U = \lambda J_m$ for (0,1)-vector U.

ns by using basis reduction. We already have could still be improved. The projective special finding t-designs, see [3], however other groups ul study of the algebra of the A_{tk} matrices [5,6]

ider the matrix B below:

$$\begin{bmatrix} I_n & 0 \\ A_{tk} & -\lambda J_m \end{bmatrix} \qquad (2)$$

atrix described in (1) and I_n is the n by n identity e spanned by the columns of B. That is:

$= B{\cdot}S$, for some $S \in \mathbb{Z}^{n+1}$).

Then the following proposition is clear:

nteger d *if and only if* $[U,E_m]^T \in \mathbb{L}$.

λJ_m we need only look for a linear combination t U is a (0,1)-vector. If $U \neq J_m$ then we will have ve integer d. Note that since the complement of a it is, U is a particular short vector in $\mathbb{L}$. Our is all of whose vectors are as short as we can make

introduce the basic concepts about integer lattices

t $\mathbb{L}$ of the n-dimensional real vector space R^r, $r \geq n$ $b_1, b_2, \ldots, b_n$) of an n-dimensional subspace of R^r such linear combination of the vectors in B. Recall that n-dimensional subspace of R^r, an orthogonal basis ned inductively via the Gram-Schmidt process of

orthogonalization as follows:

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*, \text{ for } 1 \leq i \leq n, \qquad (3)$$

$$\mu_{ij} = (b_i, b_j^*)/(b_j^*, b_j^*), \text{ for } 1 \leq j < i \leq n, \qquad (4)$$

where $(\cdot,\cdot)$ denotes the ordinary inner product on R^r. An ordered basis $B = [b_1, b_2, \ldots, b_n]$ for a lattice $\mathbb{L}$ will be said to be *y-reduced (or reduced)* if the following two conditions hold:

i) $|\mu_{ij}| \leq ½$ for $1 \leq j < i \leq n$,

ii) $\|b_i^* + \mu_{ii-1} b_{i-1}^*\|^2 \geq y \cdot \|b_{i-1}^*\|^2$ for $1 < i \leq n$,

where y, $¼ < y < 1$ is a constant and $\|\cdot\|$ denotes ordinary Euclidean length. Lenstra et al. (1982) describe an algorithm, which when presented with y, $¼ < y < 1$ and an ordered basis $B = [b_1, b_2, \ldots, b_n]$ for a lattice $\mathbb{L}$ as input, produces a reduced basis $B' = [b_1', b_2', \ldots, b_n']$ as output. The L^3 algorithm consists of applying a finite number of two kinds of linear transformations:

T1: Interchange vectors b_i and b_{i-1} if $\|b_i^* + \mu_{ii-1} b_{i-1}^*\|^2 \geq y\|b_{i-1}^*\|^2$ does not hold, for some $1 < i \leq n$, and the global constant $y \in (¼, 1)$.

T2: Replace b_i by $b_i - rb_j$, where $r = \text{round}(\mu_{ij})$ is the nearest integer to μ_{ij}, and $|\mu_{ij}| > ½$, for some $1 \leq j < i \leq n$.

The efficient implementation of the sequence of transformations T1 and T2 relies mainly on the fact, that old values of μ_{ij} and $\|b_i^*\|^2$ can be easily updated after each transformation without using the full process of orthogonalization. The L^3 algorithm performs the transformations T1 and T2 using a strategy resembling somewhat the bubble-sort, however as H.W.Lenstra [9] remarks, <u>any</u> sequence of the these transformations will lead to the reduced basis.

The L^3 algorithm terminates when neither T1 nor T2 can be applied and such a situation implies that conditions i) and ii) are satisfied. The resulting reduced basis B' is an integer approximation to the basis B^* defined by the Gram-Schmidt orthogonalization process and as a consequence contains short vectors, as can be seen in the following proposition of Lenstra et al. [9, prop. 1.11]:

PROPOSITION 2: *Let* $B' = [b_1', b_2', \ldots, b_n']$ *be a reduced basis of a lattice L. Then:*

$$\|b_1'\|^2 \leq 2^{n-1} \cdot \min(\|b\|^2 : b \in \mathbb{L} \text{ and } b \neq 0).$$

They also give the following polynomial worst-case running time for its performance [Lenstra et al. (1982), prop 12.6].

PROPOSITION 3: *Let* $\mathbf{B} = [b_1, b_2, ..., b_n]$ *be an ordered basis for an integer lattice* $\mathbb{L}$ *such that* $\|b_i\|^2 \leq \text{Max}$ *for* $1 \leq i \leq n$. *Then the* L^3 *algorithm produces a reduced basis* $\mathbf{B}' = [b_1', b_2', ..., b_n']$ *for* $\mathbb{L}$ *using at most* $O(n^4 \log_2 \text{Max})$ *arithmetic operations, and the integers on which these operations are performed have length at most* $O(n \log_2 \text{Max})$.

In summary, the effect of the L^3 algorithm is such that when given a basis **B** of the n-dimensional lattice $\mathbb{L} \subseteq \mathbb{Z}^r$ it produces a *reduced* basis $\mathbf{B}'$ of $\mathbb{L}$, and:

i. L^3 uses at most $O(n^4)$ arithmetic operations.

ii. $\mathbf{B}'$ is *almost* orthogonal (integer approximation to Gram-Schmidt orthogonal basis).

iii. $\mathbf{B}'$ contains short vectors.

Furthermore, we point out that although it is proven only that $\mathbf{B}'$ does contain a vector shorter than $2^{(n-1)/2}\cdot$(length of shortest nonzero vector in $\mathbb{L}$) [9], in practice the L^3 algorithm find much much shorter vectors [8].

When the number of rows in the A_{tk} matrix is $m = 1$ then (1) reduces to the knapsack or subset-sum problem. The application of using the L^3 algorithm to solve the subset sum problem was first studied in 1985 by J.C. Lagarias and A.M. Odlyzko [8]. Our improvements in this direction are to be presented at the Third SIAM Conference on Discrete Mathematics at Clemson University, May 1986.

When the number of rows in the A_{tk} matrix is greater than 1 then unfortunately L^3 by itself doesn't find t-designs. Thus further reduction methods are necessary.

2.2. Weight Reduction

If **B** is the (n+1)-dimensional reduced basis produced by the L^3 algorithm applied to (2), then there will often exist pairs of indices i and j, $1 \leq i,j \leq n+1$, $i \neq j$, and a choice of ϵ such that

$$v = b_i + \epsilon b_j, \quad \epsilon = \pm 1, \text{ and} \tag{5}$$

$$\|v\| < max\{\|b_i\|, \|b_j\|\}.$$

A pair (i,j), i≠j, satisfies the last condition iff $max\{\|b_i\|^2, \|b_j\|^2\} < 2\cdot|(b_i,b_j)|$. In such a case we can choose ϵ to have a different sign from (b_i,b_j) and substitute the longer of b_i and b_j by v, obtaining a new basis with decreased *total weight*

$$w(\mathbf{B}) = \sum_{p=1}^{n+1} \|b_p\|^2.$$

In the process of finding successive pairs
to recalculate $\|v\|^2$ and (v,b_k) from the definiti
$\|b_i\|^2$ and $inn_{ij} = (b_i,b_j)$, for $1 \leq j < i < n+1$, using fo

$$\|v\|^2 = \|b_i\|^2 + $$

$$(v,b_k) = inn_{ik} + \epsilon \cdot inn_{jk}, \text{ fo}$$

A simple algorithm for finding all such pairs c
for each reduction, producing as output a bas
call it *Weight-Reduction*, is a useful complement
algorithms L^3 and *Weight-Reduction* jointly ten
L^3 or *Weight-Reduction* alone:

B ← L^3(**B**);
repeat
Weight-Reduct
sort basis with
B ← L^3(**B**);
until (w(**B**) does r
Weight-Reduction.

The L^3 algorithm can remove the vector l
shorter vector, since for i = 2 if the transform
(note that this is not true when i > 2). Hence so
that the shortest vector in the basis **B** will not
shorter vector is found.

Following the above approach one can try
$b_{i_1}, \cdots, b_{i_k}$, for some $k \geq 2$, in the basis **B**, such

$$v = \sum_{p=1}^{k} \epsilon_p b_{i_p}, \text{ for some ch}$$

is shorter than b_{i_k}, where b_{i_k} is the longest vect
of basis **B** can be decreased by substituting b_{i_k} b

$$\|v\| < \|b_{i_k}\| \Leftrightarrow \|v\|^2 = \sum_{j=1}^{k} \|b_{i_j}$$

and a necessary condition for (6) is

worst-case running time for its performance [Lenstra

be an ordered basis for an integer lattice L such that algorithm produces a reduced basis $B' = [b_1', b_2', ..., b_n']$ rithmetic operations, and the integers on which these most $O(n \log_2 Max)$.

algorithm is such that when given a basis B of the n- a *reduced* basis B′ of L, and:

etic operations.

integer approximation to Gram-Schmidt orthogonal

ugh it is proven only that B′ does contain a vector nonzero vector in L) [9], in practice the L^3 algorithm

matrix is m = 1 then (1) reduces to the knapsack or n of using the L^3 algorithm to solve the subset sum J.C. Lagarias and A.M. Odlyzko [8]. Our improvements t the Third SIAM Conference on Discrete Mathematics

e A_{ik} matrix is greater than 1 then unfortunately L^3 by her reduction methods are necessary.

duced basis produced by the L^3 algorithm applied to (2), ndices i and j, $1 \le i,j \le n+1$, $i \ne j$, and a choice of ϵ such

(5)

ndition iff $max(\|b_i\|^2, \|b_j\|^2) < 2 \cdot |(b_i,b_j)|$. In such a case sign from (b_i,b_j) and substitute the longer of b_i and b_j by sed *total weight*

$$w(B) = \sum_{p=1}^{n+1} \|b_p\|^2.$$

In the process of finding successive pairs of indices (i,j) satisfying (5) it is not necessary to recalculate $\|v\|^2$ and (v,b_k) from the definitions, instead we can keep track of the integers $\|b_i\|^2$ and $inn_{ij} = (b_i,b_j)$, for $1 \le j < i < n+1$, using formulas:

$$\|v\|^2 = \|b_i\|^2 + \|b_j\|^2 - 2|inn_{ij}|,$$

$$(v,b_k) = inn_{ik} + \epsilon \cdot inn_{jk}, \text{ for } 1 \le k \le n+1, k \ne i \text{ and } k \ne j.$$

A simple algorithm for finding all such pairs can be designed and implemented in time $O(n^2)$ for each reduction, producing as output a basis with smaller weight. This algorithm, let us call it *Weight-Reduction*, is a useful complement to the L^3 algorithm. When used as follows, the algorithms L^3 and *Weight-Reduction* jointly tend to produce much shorter vectors than using L^3 or *Weight-Reduction* alone:

```
B ← L³(B);
repeat
    Weight-Reduction;
    sort basis with respect to ||b_i||²;
    B ← L³(B);
until (w(B) does not decrease);
Weight-Reduction.
```

The L^3 algorithm can remove the vector b_1 from the basis B only by replacing it with a shorter vector, since for $i = 2$ if the transformation T1 can be applied then $\|b_i\|^2 < \|b_{i-1}\|^2$ (note that this is not true when $i > 2$). Hence sorting the basis with respect to $\|b_i\|^2$ guarantees that the shortest vector in the basis B will not disappear in the next iteration, unless a new shorter vector is found.

Following the above approach one can try in general to find a k-tuple of distinct vectors $b_{i_1}, \cdots, b_{i_k}$, for some $k \ge 2$, in the basis B, such that the vector

$$v = \sum_{p=1}^{k} \epsilon_p b_{i_p}, \text{ for some choice of } \epsilon_p = \pm 1, 1 \le p \le k,$$

is shorter than b_{i_k}, where b_{i_k} is the longest vector in the k-tuple. In the latter case the weight of basis B can be decreased by substituting b_{i_k} by v. Note that

$$\|v\| < \|b_{i_k}\| \Leftrightarrow \|v\|^2 = \sum_{j=1}^{k} \|b_{i_j}\|^2 + \sum_{h \ne j} \epsilon_{i_h}\epsilon_{i_j}(b_{i_h}, b_{i_j}) < \|b_{i_k}\|^2 \quad (6)$$

and a necessary condition for (6) is

$$\sum_{j=1}^{k-1} \|b_{i_j}\|^2 < \sum_{h \neq j} |(b_{i_h}, b_{i_j})|.$$

Consequently, our approach is to search for such k-tuples of vectors by considering the complete graph G, whose vertices are the basis vectors b_i and whose edges are labeled by edge weight $|(b_i,b_j)|$. The endpoints of edges with large weight are "less" orthogonal, hence they are good candidates for the desired k-tuple. We can try to construct it by finding subgraphs of G with large edge weight.

Obviously, the complete analysis of all subgraphs in the graph G would be too expensive, however we are satisfied with heuristic search for just a few of them of relatively small size. They are used to decrease the weight of basis **B** similarly as before. This technique leads to the generalization of the *Weight-Reduction* algorithm and improves further the behavior of the L^3 algorithm.

2.3. Size Reduction

Recall that $[U,E_m]^T \in \mathcal{L}$ if and only if there exist integers $a_1, a_2, \ldots, a_{n+1}$ such that:

$$\begin{bmatrix} U \\ E_m \end{bmatrix} = \mathbf{B} \begin{bmatrix} a_1 \\ \vdots \\ a_{n+1} \end{bmatrix}$$

Whence, it follows that:

If there is one and *only one* j *such that* $b_{hj} \neq 0$ for *some* h, $n < h \leq n+m$, *then* $a_j = 0$. (*)

In this case: we let **B′** be **B** with row h and column j removed and $\mathcal{L}'$ be the lattice spanned by **B′**. Then the (n+m-1)-dimensional vector $[U,E_{m-1}]^T \in \mathcal{L}'$ if and only if the (n+m)-dimensional vector $[U,E_m]^T \in \mathcal{L}$.

To achieve situation (*) for row h, $n < h \leq n+m$, we preform the following two operations:

1. Multiply row h by $c = \max_i \|b_i\|^2$
2. apply *Weight-Reduction* and/or L^3

This almost always produces such a situation.

If this procedure is successfully iterated for each h, $h = n+m, n+m-1, \ldots, n+1$, then the resulting basis **B′** will consist of n-m+1, n-dimensional vectors. Furthermore:

$$U \in \mathcal{L}' \Leftrightarrow A_{tk} U = d \cdot \lambda J_m$$

for some integer d, see proposition 1. Thus the result of these iterations, let us call them

collectively *Size-Reduction*, is a basis of shor
matrix equation $A_{tk} U = d \cdot \lambda J_m$. Consequently,
search the lattice spanned by **B′**. Finally our

ALGORITHM MSV
input basis **B** of the
$\mathbf{B} \leftarrow L^3(\mathbf{B})$
$\mathbf{B} \leftarrow$ *Size-Reduction*(**B**
repeat
Weight-Reduction
sort basis with res
$\mathbf{B} \leftarrow L^3(\mathbf{B})$
until (weight(**B**) = $\sum$
Weight-Reduction.
Check for solution after
Weight-Reduction and L^3.

Figure 3. The M

3. Closing Remarks

We have duplicated the results of Kramer,
took only a few minutes whereas Leavitt's Algor

We would like to thank Jeff Dinitz, Dan A
Michael Wertheimer and especially Andrew Od
encouragement during and after the 17-th South
Theory and Computing at which these results we

Finally, during the week following the co
design by solving, with the MSV algorithm, the
We note that this represents 99 linear Diophantin
the well known extension theorem of Alltop [1]
6-(14,7,4) design [7]. This remarkable design is
Furthermore, we were able to show that there a
that have a cyclic 5-(13,6,4) derived design an
subsets.

$< \sum_{h \neq j} |(b_{i_h}, b_{i_j})|$.

:h for such k-tuples of vectors by considering the
basis vectors b_i and whose edges are labeled by
:ges with large weight are "less" orthogonal, hence
: k-tuple. We can try to construct it by finding

:f all subgraphs in the graph G would be too
neuristic search for just a few of them of relatively
the weight of basis B similarly as before. This
:e *Weight-Reduction* algorithm and improves further

if there exist integers $a_1, a_2, \ldots, a_{n+1}$ such that

$$\begin{bmatrix} J \\ \_m \end{bmatrix} = B \begin{bmatrix} a_1 \\ : \\ a_{n+1} \end{bmatrix}$$

- *that* $b_{hj} \neq 0$ for *some* h, $n < h \leq n+m$, *then* $a_j = 0$. (*)

and column j removed and L' be the lattice spanned
.l vector $[U, E_{m-1}]^T \in L'$ if and only if the (n+m)-

$\leq n+m$, we preform the following two operations:

$b_i\|^2$

or L^3

uation.

:rated for each h, $h = n+m, n+m-1, \ldots, n+1$, then the
. n-dimensional vectors. Furthermore:

$L' \Leftrightarrow A_{tk} U = d \cdot \lambda J_m$

. Thus the result of these iterations, let us call them

collectively *Size-Reduction*, is a basis of short vectors for the integer solution space to the matrix equation $A_{tk} U = d \cdot \lambda J_m$. Consequently, to discover a t-$(v,k,d \cdot \lambda)$ design we need only search the lattice spanned by B'. Finally our complete algorithm is given in figure 3.

ALGORITHM MSV (Matrix Short Vector)

```
input basis B of the form in (2)
B←L³(B)
B←Size–Reduction(B)
repeat
    Weight-Reduction
    sort basis with respect to ‖b_i‖²
    B←L³(B)
until (weight(B) = Σ‖b_i‖² does not decrease)
Weight-Reduction.
Check for solution after each
Weight-Reduction and L³.
```

Figure 3. The MSV algorithm

3. Closing Remarks

We have duplicated the results of Kramer, Leavitt and Magliveras [3,10]. Our algorithm took only a few minutes whereas Leavitt's Algorithm took several hours.

We would like to thank Jeff Dinitz, Dan Archdeacon, Earl Kramer, Spyros Magliveras, Michael Wertheimer and especially Andrew Odlyzko for their stimulating conversations and encouragement during and after the 17-th Southeastern Conference on Combinatorics, Graph Theory and Computing at which these results were first presented.

Finally, during the week following the conference we discovered a cyclic 5-(13,6,4) design by solving, with the MSV algorithm, the $A_{5,6}$ matrix with cyclic group G of order 13. We note that this represents 99 linear Diophantine equations in 132 unknowns. Thus applying the well known extension theorem of Alltop [1] we announce the existence of a new simple 6-(14,7,4) design [7]. This remarkable design is the smallest simple 6-design that can exist. Furthermore, we were able to show that there are, up to isomorphism, exactly two 6-designs that have a cyclic 5-(13,6,4) derived design and that they partition the set of all $\binom{14}{7}$ 7-subsets.

References

1. W. O. Alltop, Extending t–designs *J. Combinatorial Theory Series A*, Vol. 18 (1975) 177–186.

2. E.S. Kramer, Some t-Designs for t ≥ 4 and t=17, 18, *Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory and Computing*, Congressus Numerantium XIV (1975) 443-460

3. E.S. Kramer, D.W. Leavitt and S.S. Magliveras, Construction Procedures for t-Designs and the Existence of New Simple 6-Designs, *Annals of Discrete Mathematics* 26 (1985) 247-274.

4. E.S. Kramer and D.M. Mesner, t-Designs on Hypergraphs, *Discrete Mathematics*, Vol.15 (1976) 263-296.

5 D.L. Kreher *Algebraic Methods in the Theory of Combinatorial Designs*, Ph.D. Thesis, University of Nebraska, 1984.

6 D.L. Kreher, An Incidence Algebra For t-Designs with Automorphisms, *to appear, Journal of Combinatorial Theory Series (A)* (1985).

7. D.L. Kreher and S.P. Radziszowski, The Existence of Simple 6-(14,7,4) Designs, *Journal of Combinatorial Theory, Series A* (submitted March 1986).

8. J.C. Lagarias and A.M. Odlyzko, Solving Low-Density Subset Sum Problem, *Journal of the ACM*, Vol.32, No.1 (1985) 229-246.

9. A.K. Lenstra, H.W. Lenstra and L. Lovász, Factoring Polynomials with Rational Coefficients, *Mathematische Annalen*, 261 (1982) 515-534.

10. S.S. Magliveras and D.W. Leavitt, Simple 6-(33,8,36) Designs from $P\Gamma L_2(32)$, *Computational Group Theory, Proceedings of the London Mathematical Society Symposium on Computational Group Theory*, Academic Press, pp. 337-352, 1984.

11. L. Teirlinck, Non-trivial t-Designs without Repeated Blocks Exist for All t, *to appear* (1985).