

SOLUTIONS TO THE 1-DESIGN EQUATIONS

Martin Dowd

1613 Wintergreen Pl.

Costa Mesa, CA 92626, USA

Abstract: The 1-designs with given values for the parameters v and k can be characterized as nonnegative integer solutions to a system of linear equations with integer coefficients. Some facts about these equations are proved.

AMS Subject Classification: 05B05

Key Words: block designs, linear Diophantine equations

1. Introduction

Suppose v and k are integers with $1 \leq k \leq v$. A 1-design with parameters v and k is a v row by b column matrix for some b , with elements either 0 or 1, such that each column contains k 1's, and each row contains r 1's for some r . Such a matrix is exactly the incidence matrix of a "biregular bipartite graph", with v vertices of degree r in one class, and b vertices of degree k in the other class.

There is a well-known system of linear equations associated with 1-designs. These are in fact defined for t -designs, and are used in asymptotic existence theory (see [1]). In [12], some facts concerning magic squares are proved by applying algebraic methods to a system of linear equations associated with the configurations. This suggests that it is of interest to investigate the system of equations associated with the 1-designs.

2. Existence

For a 1-design to exist, clearly $bk = vr$ must hold. Letting $r_0 = k/\gcd(v, k)$, r must be a multiple of r_0 .

Theorem 1. *There is a 1-design for parameters v and k , with $r = r_0$.*

Proof. Let $v' = v/\gcd(v, k)$ and $k' = k/\gcd(v, k)$. There is a bipartite graph with two classes of size v' , regular of degree $k' = r_0$ (let the edges be between i and $i + s \pmod{v'}$ for $0 \leq i < v'$ and $0 \leq s < k'$). Now replicate one of the classes $\gcd(v, k)$ times. \square

3. The Equations

Given v and k , let C_k^v denote the set of k element subsets of $\{1, \dots, v\}$. The elements of C_k^v may be considered as the ordered k -tuples $\langle i_1, \dots, i_k \rangle$ where $1 \leq i_1 < \dots < i_k \leq v$; or as the 0-1 vectors of length n where k elements are 1. C_k^v will be considered to be ordered as the k -tuples ordered lexicographically.

Let M be the $v \times \binom{v}{k}$ 0-1 matrix whose rows are labeled with the elements $R \in C_1^v$ and whose columns are labeled with the elements $C \in C_k^v$, such that $M_{RC} = 1$ iff $R \subseteq C$.

Let x denote the column of height $\binom{v}{k}$ of indeterminates x_C for $C \in C_k^v$. Let $J_{m \times n}$ denote the $m \times n$ all 1's matrix. Clearly, there is a 1-design with parameters v, k, r iff the system of linear equations $Mx = J_{v \times 1}r$ has a nonnegative integral solution. For $v > 1$ let H be the $v - 1 \times v$ matrix where H_{ij} equals -1 if $j = 1$, $+1$ if $j = i + 1$, and 0 otherwise. The nonnegative solutions of the homogeneous system $HMx = 0$ correspond to the 1-designs; the parameter b for the solution x equals $\sum_C x_C$.

4. Right Inverse

A right inverse to the t -design equations matrix can be computed by a method given in [1] (see lemma VIII.7.6). For example, for $t = 1$, $v = 4$, $k = 2$, $MR = I$ where I is the identity matrix and

$$M = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, R = \frac{1}{6} \cdot \begin{bmatrix} 2 & 2 & -1 & -1 \\ 2 & -1 & 2 & -1 \\ 2 & -1 & -1 & 2 \\ -1 & 2 & 2 & -1 \\ -1 & 2 & -1 & 2 \\ -1 & -1 & 2 & 2 \end{bmatrix}.$$

The existence of a right inverse implies that M is full rank, and also that HM is. The matrix R suffers from a deficiency, though. The column vector $a = [2, 0, 0, 0]^T$ is in the column space over the integers \mathcal{Z} of M , but $Ra = (1/3)[2, 2, 2, -1, -1, -1]^T$ is not integral.

Suppose M is an integer $m \times n$ matrix of rank m . A right inverse R to M will be said to be strong if, whenever a is in the column space over \mathcal{Z} of M , Ra is integral.

Theorem 2. *Suppose M is an integer $m \times n$ matrix of rank m . Let A be an $m \times m$ matrix whose columns generate over \mathcal{Z} the column space over \mathcal{Z} of M . For each column A_i of A let X_i be a column vector such that $MX_i = A_i$. Let X be the matrix with columns X_i . Then $R = XA^{-1}$ is a strong right inverse to M .*

Proof. Clearly $MX = A$, whence $MRA = MXA^{-1}A = MX = A$, so $MR = I$. Further, RA_i is integral for each i , whence Ra is integral for any a in the column space. □

In the case where M is the 1-design equations, the column space is well-known to consist of the integer vectors whose sum is divisible by k ([1], lemma VII.7.8). The matrix A may be taken as having $A_{11} = k$, $A_{1i} = -1$ for $2 \leq i \leq v$, $A_{ii} = 1$ for $2 \leq i \leq v$, and $A_{ij} = 0$ otherwise. Indexing the rows and columns of M from 0, the columns of M which have a 1 in row i for $0 \leq i < v - k - 1$ form a sequence of length $\binom{v-1-i}{k-1}$. Let $\{j_i : 0 \leq i < v - k - 1\}$ be the set of indexes of the first column of each of these sequences, so that $j_i = \sum_{l=0}^i \binom{v-1-l}{k-1}$. Let M_C be the matrix whose i th column for $0 \leq i < v - k - 1$ is column j_i of M ; and whose last $k + 1$ columns are the last $k + 1$ columns of M .

The inverse M_C^{-1} of M_C can be computed recursively. When $v = k + 1$, let N the $(k + 1) \times (k + 1)$ matrix which is all 1's, except $-(k - 1)$ on the antidiagonal. Then $MN = kI$, whence $M_C^{-1} = (1/k)N$. Writing M_v, N_v , etc., for the matrices for v vertices,

$$M_C = \begin{bmatrix} 1 & 0's \\ t & M_{C,v-1} \end{bmatrix}; \text{ let } N = \begin{bmatrix} k & 0's \\ u & N_{v-1} \end{bmatrix},$$

where t has 1 in the top $k - 1$ rows and 0 in the remaining rows, and $tk + M_{C,v-1}u = 0$, whence $u = -N_{v-1}t$. Let $M_C^{-1} = (1/k)N$.

Let the j_i th column of R be the i th column of M_C^{-1} for $0 \leq i < v - k - 1$, let the last $k + 1$ columns of R be the last $k + 1$ columns of M_C^{-1} , and let the remaining columns of R be 0.

Theorem 3. *With R as above, R is a strong right inverse to M . Further the elements of N all have absolute value at most k .*

Proof. Inductively, $M_C N = kI$, and $MR = I$ follows. The lower right $(k + 1) \times (k + 1)$ submatrix of N is a copy of N_{k+1} . Each element to the left is the negative of the sum of the $k - 1$ elements to its right. Fixing k , and indexing from 0, let ρ_j be row j of N_{k+1} ; its elements are 1, except element $k - j$ is $-(k - 1)$. If σ is a string over \mathcal{Z} and d is a non-negative integer less than or equal to its length let $\sigma_{\rightarrow d}$ be the rightmost d elements of σ . Let α be the string $0^{k-2}, -k, k$. From preceding remarks it is easy to see that for $0 \leq i \leq v - k - 1$ row i of N equals $\alpha_{\rightarrow d} \alpha^e 0^f$ where $f = v - 1 - i$, and d and e are determined by the division law from $d + ek = v - f$. Let β be the string $1^{k-1}, -(k - 1)$. For $0 \leq j < k + 1$ let $i = (v - k - 1) + j$; row i of N equals $\beta_{\rightarrow d} \beta^e 1^f \rho_j$ where $f = \min(v - k - i, j)$, and $d + ek = v - f - k - 1$. It is readily verified that if x is an element of a row, and y is an element to its right, then $-x + y$ is divisible by k . It follows that every element of NA is divisible by k . □

For example, in the case $v = 4, k = 2$ considered above, R equals

$$\frac{1}{3} \cdot \begin{bmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \end{bmatrix}.$$

5. Kernel

A matrix K whose columns generate the kernel of M may be specified by recursion. For the basis $v = k + 1$ K is the empty matrix. For $v > k + 1$ write

$$M = \begin{bmatrix} 1's & 0 \\ M_b & M_{v-1} \end{bmatrix} \text{ and } K = \begin{bmatrix} K_t & 0 \\ K_b & K_{v-1} \end{bmatrix}.$$

M has height 1 in the top row, height $v - 1$ in the bottom row, width $\binom{v-1}{k-1}$ in the left column, and width $\binom{v-1}{k}$ in the right column. K has height $\binom{v-1}{k-1}$ in the top row, height $\binom{v-1}{k}$ in the bottom row, width $\binom{v-1}{k-1} - 1$ in the left column, and width $\binom{v-1}{k} - v + 1$ in the right column. K_t has -1 's in the top row, and an identity matrix below this. K_b must satisfy $M_b K_t + M_{v-1} K_b = 0$. Let $K_b = -R_{v-1} M_b K_t$.

Theorem 4. *The matrix K defined above is integral, and its column space equals the kernel over \mathcal{Z} of M . Further the elements of K all have absolute value at most k , and this bound is tight for sufficiently large v .*

Proof. For each column of $M_b K_t$, the sum of its elements is 0, whence K_b is integral, whence inductively K is. By construction each column of K is in the kernel. Conversely, suppose x is in the kernel. Let x_t denote the top $\binom{v-1}{k-1} - 1$ rows of x . Then $x_t = \sum_i c_i K_{ti}$ where the K_{ti} are the columns of K_t , for some integers c_i . Let $y = \sum_i c_i K_i$ where the K_i are the columns of K . Let $z = x - y$. Let z_b be the bottom $\binom{v-1}{k} - v + 1$ rows of z . Then z_b is in the kernel of M_{v-1} , whence inductively it is in the column space of K_{v-1} , whence x is in the column space of K . To prove the bound, by induction it suffices to prove it for K_b , for which it clearly suffices to prove that for $N_{v-1} M_{v-1, k-1} K_t$ the bound is k^2 . An element of a row of this matrix is the sum of l elements of the first $k - 1$ elements of the corresponding row of N_{v-1} , where $l < k - 1$, minus the sum of l elements to the right of the first $k - 1$. The claims for the bound follow. \square

Write M_H for the matrix HM defined in Section 3. Recall the value r_0 from Section 2, and write Q for the column matrix $RJ_{v \times 1} r_0$. Write K_H for the matrix K , with Q added as an additional column.

Theorem 5. *The matrix K_H defined above is integral, and its column space equals the kernel over \mathcal{Z} of M_H . Further the elements of K_H all have absolute value at most k .*

Proof. $M_H x = 0$ iff $Mx = MRJ_{v \times 1} r$ for some integer r such that $r_0 | r$. That K_H is a generator matrix for the kernel of M_H follows. To prove the bound for K_H it suffices to prove the bound of k for $NJ_{v \times 1}$, and this follows from the characterization of the rows of N . \square

6. Minimal Solutions

On \mathcal{Z}^n let \leq denote the product order, where $x \leq y$ iff $x_i \leq y_i$ for all i . This is readily verified to be a partial order. Dickson’s lemma ([3]) states that, restricting \leq to \mathcal{N}^n , any subset has finitely many minimal elements. Let M be any integer matrix. An integer solution to the system $Mx = 0, x \geq 0$, is said to be minimal if it is minimal in the product order among the nonzero solutions. The set of minimal elements is known as the Hilbert basis of the nonzero solutions.

Various authors have given bounds on the size of a minimal element (see [7] for a discussion). For convenience a brief treatment will be given here. For a real matrix A let $|A|_\infty$ denote the max norm $\max_{ij} |A_{ij}|$, and similarly for a vector. For a vector x let $\text{supp}(x)$ denote the support $\{i : x_i \neq 0\}$. The reader is assumed to be familiar with the notion of a basic solution to the real system $Mx = 0$; see [10] for example.

Suppose M is a full rank integer $m \times n$ matrix where $m \leq n$. Let C denote the set of real solutions to the system $Mx = 0, x \geq 0$. Let β denote $\max\{|x|_\infty\}$ where x ranges over the minimal elements of $C \cap \mathcal{Z}^n$. Let β_B denote the value when x is restricted to be a basic solution, equivalently to lie on an extreme ray of C .

Theorem 6. *With notation as above, $\beta < (n - m)\beta_B$.*

Proof. C is a cone lying in an $(n - m)$ -dimensional subspace, so by Carathéodory’s theorem for cones ([11], corollary 7.1i), if x is a point in C then $x = \sum_i t_i x_i$ where each x_i is a point on an extreme ray, $r_i \geq 0$, and the x_i are affinely independent, so there are at most $n - m$ summands. If x and the x_i are minimal integral vectors, then by a “zonotope” argument (see theorem 4.1 of [5]), $0 \leq r_i < 1$. The theorem follows. □

The bound of the theorem is quite tight. In \mathcal{R}^d consider the d minimal vectors $\langle n, 1, 0, \dots, 0 \rangle, \langle n, n - 1, 0, \dots, 0 \rangle, \langle n, 0, n - 1, 0, \dots, 0 \rangle, \dots, \langle n, 0, \dots, 0, n - 1 \rangle$ for sufficiently large n ; let C be the cone they generate. Let $x = \langle dn - d - 1, n - 1, \dots, n - 1 \rangle$. Then $x \in C$ and for $n - 1$ prime x is minimal.

Theorem 7. *For the system $M_H = 0$ and $x \geq 0, \beta_B \leq v!$.*

Proof. Suppose x is a basic minimal solution of the system $Mx = J_{v \times 1}$ and $x \geq 0$. The maximum of the absolute values of the determinants of the $(v - 1) \times (v - 1)$ minors of M is at most $(v - 1)!$. By well-known arguments (see lemma 2.1 of [10]) $x\Delta = NJ_{v \times 1}$ where Δ is a positive integer and N is an integer matrix of max norm at most $(v - 1)!$. The theorem follows. □

As will be seen in Section 8, this bound can be significantly improved, in some cases at least.

7. Components

A component of a 1-design is defined to be a minor of the incidence matrix, with row set S_R and column set S_C , such that each column incident to a row of S_R is in S_C , and each row incident to a column of S_C is in S_R . If this is so then the minor with row set S_R^{compl} and column set S_C^{compl} is also a component. The 1-design matrix D with parameters v, k, r can be brought by row and column permutation to the form

$$\begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix},$$

where D_i is a 1-design with parameters v_i, k, r and $v = v_1 + v_2$.

Say that a 1-design is connected if it does not have a proper component. Clearly any 1-design D can be decomposed into connected components D_1, \dots, D_t , and the D_i are unique up to order and row and column permutation.

Theorem 8. *A 1-design D is basic iff each of its components is.*

Proof. A 1-design D is basic iff $\{C : x_C \neq 0\}$ is linearly independent. This set S is the disjoint union of subsets S_1, \dots, S_t , where S_i corresponds to the connected component D_i in an obvious way. The set S is clearly linearly independent iff each S_i is. \square

Theorem 9. *A 1-design D is minimal iff one of its components is.*

Proof. A 1-design D is minimal iff no proper subset of its columns is a 1-design. The theorem follows. \square

Non-connected 1-designs provide various useful examples. Let D be the 1-design with $k = 2$ consisting of $v/3$ components, each with 3 vertices. Then for the solution x corresponding to D , $|x|_\infty = 1$. However the maximum absolute value of the determinant of a $(v - 1) \times (v - 1)$ minor of the relevant columns of the system matrix is $2^{v/3}$. This suggests that the maximum max norm of a connected, or connected basic, 1-design is a quantity of interest.

For another example, suppose D is a minimal design with row count r . Add to D a block which is a copy of $J_{k \times r}$. The max norm of the solution corresponding to the resulting 1-design D' is r , and D' is minimal. If D is basic then D' is basic.

8. $k = 2$

When $k = 2$ a 1-design can be viewed as a regular loop-free multigraph on v vertices; the multiplicity of the edge between vertex i and vertex j is x_{ij} . The degree of the graph is r , the number of 1's in a row of the design.

Theorem 10. *When $k = 2$, $\beta_B \leq 2$.*

Proof. Suppose D is a connected basic 1-design. Then its underlying simple graph G is either a tree or a tree with a single chord. If G has a leaf, then for D to be regular G must be a single edge. Otherwise G must be a cycle. It is now easy to see that if D is a minimal basic 1-design then it is either a degree 1 graph, or a disjoint union of cycles, at least one of which has an odd number of vertices, with multiplicity 2 edges allowed. \square

Theorem 11. *When $k = 2$ and v is odd, $\beta = 2$.*

Proof. If D is a 1-design, r must be even. It then follows that D has a 2-factorization (see corollary 2.1.5 of [4]; this holds for multigraphs, as essentially the same proof shows). \square

Theorem 12. *Suppose $r \geq 3$ is odd. There is a regular graph with degree r and $r^2 + 2r + 1$ vertices, which is minimal and simple. There is a regular multigraph with degree r and $r^2 + 2r + 3$ vertices, which is minimal and has maximum multiplicity r .*

Proof. The graph of the first claim is a generalization of figure 9.5 of [6]. Remove $(r - 1)/3$ parallel edges from the complete graph with $r + 1$ vertices, and connect the degree $r - 1$ vertices to a new vertex. Then take r copies of this, and connect a new vertex to the degree $r - 1$ vertex of each copy. The second claim follows from the first, by adding a multiplicity r edge. \square

It is a question of interest, what is the smallest v such that there is a minimal solution which is not basic. When $v = 6$, by results given above, the max norm of such a solution would be at most 18, whence its length at most 270 and its degree at most 90. An attempt was made to determine the Hilbert basis using the Cocoa [2] “HilbertBasis” function; this ran for 10 hours with no result and was aborted. However, the following can be shown.

Theorem 13. *For $v = 6$ and $k = 2$ every minimal solution is basic.*

Proof. For a minimal non-basic multigraph G the underlying simple graph G' must satisfy the following: G' has at least 7 edges, G' has no degree 0 vertex, G' contains no 1-factor, and G' has no “twig” (edge with one vertex degree 1 and the other degree > 1). A computer readable list of the 6-vertex graphs can be obtained from [9]. A computer program was used to determine that of the 156 such, those satisfying the above restrictions are the two graphs of figure 1. For the left of these, the multiplicities would have to satisfy $a_i + b_i = r$ for $1 \leq i \leq 4$, $\sum_{i=1}^4 a_i = r$, $\sum_{i=1}^4 b_i = r$, where r is the degree. Adding the first 4 equations one obtains $2d = 4d$, so d cannot be positive. For the graph on the right, add c to the left side of the last 2 equations, and obtain $c + d = 0$, which again is impossible. \square

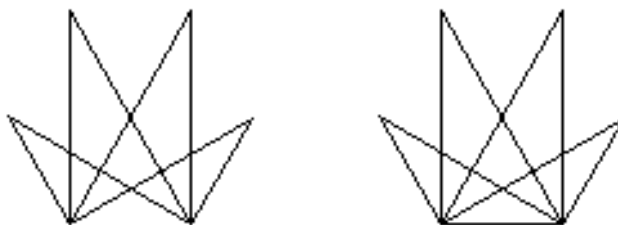


Figure 1: Graphs in proof of theorem 13

Theorem 14. For $v = 8$ and $k = 2$ every minimal solution is basic.

Proof. There are 12346 graphs on 8 vertices. A graph can be rejected as the underlying simple graph G' if it has at most 8 edges, a vertex of degree 0 or 1 (an edge with two degree 1 vertices can be rejected by a component argument using theorem 13), a 1-factor, or a 2-factor consisting of a 5-cycle and a 3-cycle. After these rejections, there remain 117 graphs. For each of these there is a linear program with 7 equality constraints specifying that the 8 vertices have equal degree in the multigraph, and e inequality constraints $m_i \geq 1$ where there are e edges and m_i is the multiplicity of edge i . Introducing surplus variables and using an implementation of the primal simplex artificial variable method ([10], Section 2.8) one determines that all but one (shown in Figure 2) of these is infeasible. To be consistent with the simple graph on the vertices 0-4, a minimal regular multigraph on these vertices must be the triangle 012 and a multiplicity 2 edge 34, or the triangle 234 and a multiplicity 2 edge 12. It follows that any regular multigraph with the underlying graph given below is 2-factorable. \square

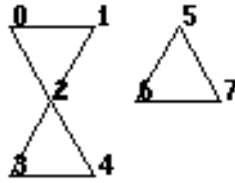


Figure 2: Graph in proof of theorem 14

9. $v \leq 8$

The basic minimal 1-designs for given v and k , up to isomorphism, can be enumerated by computer, as follows.

1. Create an “lrs” input file, for the linear program $Mx = J_{v \times 1}$, $x \geq 0$ (a “C” program for this is convenient).
2. Run “lrs” on the input (“.ine”) file, producing an output (“.ext”) file, containing a list of the vertices of the solution polytope.
3. Clear denominators of the solutions. Define the “signature” of a solution to be the sorted list of its values. Using a “C” program, divide the “.ext” file into a set of “.s6” files, with one file for each signature. In each “.s6” file, a solution is translated to a biregular bipartite graph.
4. Run “shortg” on each “.s6” file, producing a file of graphs, one per each isomorphism class of the input file. The “-f” option can be used; this is facilitated by ensuring that the graph vertices of the “row” class come first in the vertex numbering.

The program “lrs” is an open source vertex enumerator; see [8]. The program “lrs1”, which uses 32 bit numerators and denominators, was used, so further checking might be done. The behavior on all runs performed seemed normal, though; the integers in the output were small. The “.s6” format is used by the “nauty” package (see [9]); the “shortg” program is included in this package.

These steps were performed for the values of v and k listed in table 1. The number of vertices, the number of nonisomorphic graphs, and the list of 1-design lengths are given. Further data may be found on the author’s website “www.hyperonsoft.com”.

v	k	# vertices	# non-iso	lengths
6	3	70	4	2,4,6
7	3	33395	22	7,14,21
8	3	363489	154	8,16,24,32,40,48
8	4	2029615	85	2,4,6,8,10,12,14,16,18

Table 1. Basic minimal 1-designs.

We note that the above method could be improved by adding calls to the “nauty” run-time library to “lrs”.

Theorem 15. *For $v = 6$ and $k = 3$ every minimal solution is basic.*

Proof. The basic minimal solutions all have $|x|_\infty = 1$. A set of columns can be ruled out as the support of a non-basic minimal solution if it has size at most 6, or has the support of a basic minimal solution as a subset. This leaves 20872 possibilities. Writing these out to an “.s6” file, and using “shortg -k”, reduces the number to 69. Checking the LP’s as in the proof of theorem 14, all are infeasible. \square

References

- [1] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge University Press, 1993.
- [2] “<http://cocoa.dima.unige.it/flyer4.html>”
- [3] “http://en.wikipedia.org/wiki/Dickson's_lemma”
- [4] R. Diestel, *Graph Theory*, Springer, 2010.
- [5] J. Foniak and K. Fukuda, *Lectures: Integer Programming*, preprint, 2010.
- [6] F. Harary, *Graph Theory*, Addison-Wesley, 1971.
- [7] S. Hosten, *Degrees of Grobner Bases of Integer Programs*, Ph. D. thesis, Cornell University, 1997.
- [8] “<http://www-cgri.cs.mcgill.ca/avis/C/lrs.html>”
- [9] “<http://cs.anu.edu.au/bdm>”
- [10] C. Papadimitriou and K. Steiglitz, *Combinatorial Optimization: Algorithms and Complexity*, Prentice-Hall, 1982.

- [11] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley-Interscience, [1986]
- [12] R. Stanley, *Combinatorics and Commutative Algebra*, Birkhauser, 1983.