Journal of Combinatorial Theory, Series A **93**, 391–396 (2001)
doi:10.1006/jcta.2000.3116, available online at http://www.idealibrary.com on IDEAL

NOTE

A New Proof of a Classical Theorem in Design Theory[1]

G. B. Khosrovshahi[2] and B. Tayfeh-Rezaie

Department of Mathematics, University of Tehran, and Institute for Studies in Theoretical Physics and Mathematics (IPM), Tehran, Iran

Communicated by the Managing Editors

Received November 1, 1999

We present a new proof of the well known theorem on the existence of signed (integral) t-designs due to Wilson and Graver and Jurkat.

1. INTRODUCTION

Given integers t, k, and v such that $0 \leqslant t \leqslant k \leqslant v$, the *inclusion matrix* $W_{tk}(v)$ is a $(0, 1)$ matrix whose rows are indexed by the t-subsets T and whose columns are indexed by the k-subsets K (called blocks) of a v-set X and $W_{tk}(v)(T, K) = 1$ if and only if $T \subseteq K$. We simply write W_{tk} instead of $W_{tk}(v)$ if there is no danger of confusion.

An integral solution $\mathbf{x}$ of the equation

$$W_{tk}\mathbf{x} = \lambda \mathbf{e}, \tag{1}$$

where $\mathbf{e}$ is a column vector of all ones and λ is a positive integer, is called a *signed* (*integral*) t-(v, k, λ) *design*. We index the blocks to the positions of $\mathbf{x}$ in the similar ordering of indices of columns of W_{tk}. So $\mathbf{x}(B)$ is the number of appearances of block B in design $\mathbf{x}$.

For $\lambda = 0$, the integral solutions of (1) are called (v, k, t) *trades*. Clearly, the set of all (v, k, t) trades, denoted by $N_{tk}(v)$ or simply N_{tk}, is a $\mathbb{Z}$-module.

[1] This research was partially supported by a grant from IPM.

[2] To whom correspondence should be addressed at IPM, P.O. Box 19395-5746, Tehran, Iran. E-mail: rezagbk@ipm.ac.ir.

0097-3165/01 $35.00

THEOREM 1. *A signed t-(v, k, λ) design exists if and only if*

$$\lambda \binom{v-i}{t-i} \equiv 0 \qquad \left(\mathrm{mod} \binom{k-i}{t-i}\right), \tag{2}$$

for $i = 0, ..., t$.

Theorem 1 was first proved by J. E. Graver and W. B. Jurkat [3]. At the same time, R. M. Wilson independently proved a general result, which asserts that the equation $W_{tk}\mathbf{x} = \mathbf{a}$ has an integral solution if and only if $(1/\binom{k-i}{t-i})\, W_{it}\mathbf{a}$ are integral for $i = 0, ..., t$ [8]. When applied to a constant vector $\mathbf{a}$, it results in Theorem 1. Later, Wilson published a nicer proof of his result in [9]. His both proofs are inductive and use the following well known recursive structure of W_{tk}:

$$W_{tk}(v) = \begin{bmatrix} W_{t-1,k-1}(v-1) & 0 \\ W_{t,k-1}(v-1) & W_{t,k}(v-1) \end{bmatrix}.$$

The inductive proof of Graver and Jurkat is of a different nature and is more technical. They consider a signed $(t-1)$-(v, k, λ') design and by adding a $(v, k, t-1)$ trade to it, then produce a signed t-(v, k, λ) design. To find an appropriate trade, one needs a basis of N_{tk}. A few different bases have been introduced in the literature [1, 2, 5, 6]. A simple and fast algorithm for producing a basis in [5] is presented. By utilizing this basis, a flexible algorithm for generating signed designs based on the proof of Graver and Jurkat has been presented in [4].

In this paper, we prove the existence of a so-called *standard basis* for N_{tk} which can also be extracted from the basis of [5] as in [6]. We then show how a signed design is simply obtained by the elements of this basis.

2. PRELIMINARIES

There is an easy but important equation

$$W_{it}\, W_{tk} = \binom{k-i}{t-i}\, W_{ik}, \tag{3}$$

which holds for $0 \leqslant i \leqslant t$. Let $\bar{W}_{tk}$ be a $(0, 1)$ matrix in the sense of W_{tk}, but define it as $\bar{W}_{tk}(T, K) = 1$ if and only if $T \cap K = \emptyset$. By the inclusion-exclusion principal we have

$$\bar{W}_{tk} = \sum_{i=0}^{t} (-1)^i\, W_{it}^T\, W_{ik}. \tag{4}$$

The following lemma is a well-known fact and a few different proofs of it appear in the literature. (See, for example, [3, 8, 9].) Here, for the sake of completeness we present a shorter proof.

LEMMA 1. *W_{tk} is a full rank matrix over rationals.*

Proof. First let $k = v - t$. We can order the indices of rows and columns of $\bar{W}_{tk}$ such that we have $\bar{W}_{tk} = I$. If $\mathbf{x} \in N_{tk}$, then by (3), $\mathbf{x} \in N_{ik}$ for $0 \leqslant i \leqslant t$. By (4), it yields that $\mathbf{x} = \mathbf{0}$. Therefore, $N_{tk} = 0$ and W_{tk} is full rank.

Now, let $k < v - t$. By (3), we have

$$W_{tk} W_{k,\, v-t} = \binom{v-2t}{k-t} W_{t,\, v-t}.$$

This shows that W_{tk} is full rank, because $W_{t,\, v-t}$ is invertible. If $k > v - t$, then by (3), we have

$$W_{v-k,\, t} W_{t,\, k} = \binom{2k-v}{k+t-v} W_{v-k,\, k}.$$

Since $W_{v-k,\, t}$ is invertible so W_{tk} is full rank. ∎

Let $k < v - t$ and let $\mathrm{col}_{\mathbb{Z}}(W_{tk})$ denote the $\mathbb{Z}$-module generated by the columns of W_{tk}. A consequence of Lemma 1 is that $\dim(\mathrm{col}_{\mathbb{Z}}(W_{tk})) = \binom{v}{t}$. Are there $\binom{v}{t}$ columns in W_{tk} such that they form a basis for $\mathrm{col}_{\mathbb{Z}}(W_{tk})$? In order to answer this question we present the notion of starting blocks which were initially introduced in [5]. Let $X = \{1, ..., v\}$ and $B = \{b_1, ..., b_k\}$ be a block such that $b_1 < b_2 < \cdots < b_k$. B is called a *starting block* if

$$b_i \leqslant \begin{cases} v-k-t+2i-2, & 1 \leqslant i \leqslant t+1, \\ v-k+i, & t+2 \leqslant i \leqslant k. \end{cases}$$

The other blocks are called *non-starting blocks*.

Observation. Let $Y = \{1, ..., v-k-t\}$. The starting blocks corresponding to the triple (v, k, t) on the set X have the following property: If we choose from the starting blocks the ones containing i $(i \in Y)$ and omit i from them, then the resulting blocks form the starting blocks of the triple $(v-1, k-1, t-1)$ over the set $X \backslash \{i\}$. (It will of course be necessary to shift the elements of the set $X \backslash \{i\}$.) On the other hand, the starting blocks not containing i $(i \in Y)$ can be regarded as the starting blocks for the triple $(v-1, k, t)$ on the set $X \backslash \{i\}$. The same argument is true about the non-starting blocks. It is easily seen by induction that the number of non-starting blocks is equal to $\binom{v}{t}$.

3. MAIN RESULTS

In Section 2, we showed that $\mathrm{col}_{\mathbb{Z}}(W_{tk})$ has dimension $\binom{v}{t}$ which is equal to the number of non-starting blocks or columns of W_{tk}. We prove that these columns form a basis for $\mathrm{col}_{\mathbb{Z}}(W_{tk})$. This fact was first proved in [7] differently.

The following lemma is immediate from an induction argument on t and the identity $\binom{n}{r}=\binom{n-1}{r}+\binom{n-1}{r-1}$. Let $g(v,k,t)=\text{g.c.d.}\{\binom{v-i}{k-i}\mid i=0,\dots,t\}$.

Lemma 2. $\binom{v-t}{k}\equiv 0 \pmod{g(v,k,t)}$.

Let $\mathbf{x}$ and $\mathbf{y}$ be two integral vectors. By notation $\mathbf{x}\equiv\mathbf{y} \pmod n$ we mean that there is an integral vector $\mathbf{c}$ such that $\mathbf{x}-\mathbf{y}=n\mathbf{c}$.

Lemma 3. *Let $\mathbf{x}\in N_{tk}$ and $\mathscr{B}$ be the set of all starting blocks.*

(i) *If $\mathbf{x}(B)=0$ for every $B\in\mathscr{B}$, then $\mathbf{x}=\mathbf{0}$.*

(ii) *If $\mathbf{x}(B)\equiv 0 \pmod n$ for every $B\in\mathscr{B}$, then $\mathbf{x}\equiv\mathbf{0} \pmod n$.*

(iii) *If $\mathbf{x}(B)=1$ for every $B\in\mathscr{B}$, then $\mathbf{x}\equiv\mathbf{e} \pmod{g(v,k,t)}$.*

Proof. The proofs of the different parts are very similar. Thus, we only prove part (iii). The proof is by induction on t. If $t=0$, then there is just one non-starting block B and $\mathbf{x}(B)=-\binom{v}{k}+1$. But then, by Lemma 2, it follows that $\mathbf{x}(B)\equiv 1 \pmod{g(v,k,0)}$. We prove the statement for the triple (v,k,t) under the induction hypothesis. Recall that $X=\{1,\dots,v\}$ and $Y=\{1,\dots,v-k-t\}$. Let C be a non-starting block such that $C\cap Y\neq\varnothing$. Then, by the induction hypothesis and the observation in Section 2,

$$\mathbf{x}(C)\equiv 1 \qquad \pmod{g(v-1,k-1,t-1)},$$

and since $g(v,k,t)\mid g(v-1,k-1,t-1)$, we obtain that

$$\mathbf{x}(C)\equiv 1 \qquad \pmod{g(v,k,t)}. \tag{5}$$

Now assume that B is a non-starting block such that $B\cap Y=\varnothing$. Let $T=X\setminus(B\cup Y)$. Then, $|T|=t$, and by (3) and (4),

$$\sum_{C\cap T=\varnothing}\mathbf{x}(C)=0,$$

so by (5) and Lemma 2, we have

$$\begin{aligned}\mathbf{x}(B) &= -\sum_{C \subset B \cup Y,\, C \neq B} \mathbf{x}(C)\\ &\equiv -\binom{v-t}{k} + 1 \qquad (\operatorname{mod} g(v, k, t))\\ &\equiv 1 \qquad (\operatorname{mod} g(v, k, t)).\end{aligned}$$

This establishes the statement of part (iii). ∎

THEOREM 2. *The non-starting columns of* W_{tk} *form a basis of* $\operatorname{col}_{\mathbb{Z}}(W_{tk})$.

Proof. By Lemma 3(i), those $\binom{v}{t}$ columns are independent over the rationals. So by Lemma 1 every starting column can be written as a rational linear combination of the non-starting columns. But then, Lemma 3(ii) implies that every starting column is an integral linear combination of the non-starting columns. ∎

COROLLARY 1. *Let* $\mathscr{B} = \{B_i : 1 \leqslant i \leqslant \binom{v}{k} - \binom{v}{t}\}$ *be the set of all starting blocks. There is a basis* $\{\mathbf{x}_i : 1 \leqslant i \leqslant \binom{v}{k} - \binom{v}{t}\}$ *for* N_{tk} *such that* $\mathbf{x}_i(B_j) = \delta_{ij}$ *for* $1 \leqslant i, j \leqslant \binom{v}{k} - \binom{v}{t}$.

This basis is called *standard basis*. Now let $\mathbf{z} := \sum \mathbf{x}_i$. By Lemma 3(iii), we have

$$\mathbf{z} \equiv \mathbf{e} \qquad (\operatorname{mod} g(v, k, t)). \tag{6}$$

We can now prove Theorem 1.

Proof of Theorem 1. Let $\mathbf{x}$ be an integral solution of $W_{tk}\mathbf{x} = \lambda\mathbf{e}$. Then, by (3)

$$\begin{aligned}\binom{k-i}{t-i} W_{ik}\mathbf{x} &= W_{it} W_{tk}\mathbf{x}\\ &= \lambda \binom{v-i}{t-i} \mathbf{e},\end{aligned}$$

which implies that

$$\lambda \binom{v-i}{t-i} \equiv 0 \qquad \left(\operatorname{mod} \binom{k-i}{t-i}\right),$$

for $i = 0, ..., t$. Thus, the conditions (2) are necessary.

Now assume that the conditions (2) are satisfied. By the identity

$$\binom{v-i}{t-i}\binom{v-t}{k-t}=\binom{v-i}{k-i}\binom{k-i}{t-i},$$

we obtain that

$$\lambda \equiv 0 \qquad \left(\bmod \frac{\binom{v-t}{k-t}}{g(v,k,t)}\right),$$

or equivalently,

$$\lambda g(v,k,t) \equiv 0 \qquad \left(\bmod \binom{v-t}{k-t}\right). \tag{7}$$

First let $k \geqslant v-t$. By Lucas' Lemma one can easily see that $g(v,k,t)=1$ and trivially $\mathbf{x}=(\lambda/\binom{v-t}{k-t})\,\mathbf{e}$ is integral and is a solution of (1). Now suppose that $k<v-t$. Let $\mathbf{x}=(\lambda/\binom{v-t}{k-t})(\mathbf{e}-\mathbf{z})$. By (6) and (7), $\mathbf{x}$ is integral and

$$W_{tk}\mathbf{x}=\frac{\lambda}{\binom{v-t}{k-t}}W_{tk}\mathbf{e}=\lambda\mathbf{e}. \qquad \blacksquare$$

REFERENCES

1. P. Frankl, Intersection theorems and mod p rank of inclusion matrices, *J. Combin. Theory Ser. A* **54** (1990), 85–94.
2. R. L. Graham, S.-Y. R. Li, and W.-C. W. Li, On the structure of *t*-designs, *SIAM J. Algebraic Discrete Methods* **1** (1980), 8–14.
3. J. E. Graver and W. B. Jurkat, The module structure of integral designs, *J. Combin. Theory Ser. A* **15** (1973), 75–90.
4. A. S. Hedayat, G. B. Khosrovshahi, and D. Majumdar, A prospect for a general method of constructing *t*-designs, *Discrete Appl. Math.* **42** (1993), 31–50.
5. G. B. Khosrovshahi and S. Ajoodani-Namini, A new basis for trades, *SIAM J. Discrete Math.* **3** (1990), 364–372.
6. G. B. Khosrovshahi and Ch. Maysoori, On the bases for trades, *Linear Algebra Appl.* **226–228** (1995), 731–748.
7. G. B. Khosrovshahi and Ch. Maysoori, On the structure of higher incidence matrices, *Bull. Inst. Combin. Appl.* **25** (1999), 13–22.
8. R. M. Wilson, The necessary conditions for *t*-designs are sufficient for something, *Utilitas Math.* **4** (1973), 207–217.
9. R. M. Wilson, A diagonal form for the incidence matrices of *t*-subsets vs. *k*-subsets, *European J. Combin.* **11** (1990), 609–615.