SIAM J. ALG. DISC. METH.
Vol. 1, No. 1, March 1980

0196-5212/80/0101-0002 $01.00/0

ON THE STRUCTURE OF *t*-DESIGNS*

R. L. GRAHAM†, S.-Y. R. LI‡ AND W.-C. W. LI¶

Abstract. It is possible to view the combinatorial structures known as (integral) t-designs as $\mathbb{Z}$-modules in a natural way. In this note we introduce a polynomial associated to each such $\mathbb{Z}$-module. Using this association, we quickly derive explicit bases for the important class of submodules which correspond to the so-called null-designs.

Introduction. Among the most fundamental (and least understood) types of combinatorial configurations are the t-designs [2], [5], [6]. These can be defined as follows. Let v, k, t and λ be positive integers satisfying $t \leqq k \leqq v$. A *t-design* $S_\lambda(t, k, v)$ is a collection $\mathcal{B}$ of k-subsets B (called *blocks*) of a v-set V with the property that every t-subset of V occurs as a subset of exactly λ blocks $B \in \mathcal{B}$. (It is not required that blocks be distinct.) It follows from this definition that for any $i \leqq t$, the number of blocks of a t-design which contain a fixed i-subset I of V is exactly

$$\lambda\binom{v-i}{t-i}\Big/\binom{k-i}{t-i} \tag{1}$$

independent of I, which implies, in particular, that a *necessary* condition for existence of an $S_\lambda(t, k, v)$ is that the expressions in (1) are integers for $1 \leqq i \leqq t$. In fact, Wilson [6] has shown that for any $t \leqq k \leqq v$, this is also a *sufficient* condition for the existence of an $S_\lambda(t, k, v)$ provided only that $\lambda \geqq \lambda_0(t, k, v)$ is sufficiently large.

Let M be the free $\mathbb{Z}$-module generated by all the subsets of V; the elements of M are all sums $\bar{c} = \sum_{X \subseteq V} c_X X$, where $c_X \in \mathbb{Z}$. In this terminology, a t-design is just an element $\bar{c} = \sum_{|Y|=k} c_Y Y$ with all $c_Y \geqq 0$ such that for all t-subsets X,

$$\sum_{Y \supseteq X} c_Y = \lambda.$$

A submodule of M of particular interest is the module N_k defined by

$$N_k = \left\{\bar{c} \in M: \sum_{X \subseteq V} c_X = 0 \text{ and when } |X| \neq k,\ c_X = 0\right\}.$$

The elements of N_k are usually called *null-designs* since they result when the (module) difference of two t-designs is formed. In principle, if the structure of null-designs can be sufficiently well understood, then light will be shed on t-designs since any $S_\lambda(t, k, v)$ differs from a given $S'_\lambda(t, k, v)$ by a null-design.

In [2], Graver and Jurkat obtain a generating system for the module N_k from a special construction which they call a "(t, k)-pod". In this note we recast the concept of null-designs in terms of polynomials. From this formulation we reproduce the above generators in a much simpler way. In fact we show that there are basically only five kinds of linear dependence among these generators, and thereby produce in Theorem 4 an

* Received by the editors February 12, 1979, and in revised form April 19, 1979.

† Bell Laboratories, Murray Hill, New Jersey 07974.

‡ Department of Mathematics, University of Chicago, Chicago, Illinois 60637. The work of this author was supported in part by the National Science Foundation under Grant MCS77-03533.

¶ Department of Mathematics, University of Chicago, Chicago, Illinois 60837. The work of this author was undertaken during a visit at the Institute for Advanced Study, Princeton, NJ.

explicit basis for N_k described in terms of simple polynomials. In proving this theorem we use the fact that the $\binom{v}{t}$ by $\binom{v}{k}$ "inclusion" matrix $H_{v,k,t}=(h_{X,Y})$, with $|X|=t$, $|Y|=k$ and

$$h_{X,Y}=\begin{cases}1 & \text{if } X\subseteq Y,\\ 0 & \text{otherwise}\end{cases}$$

has full rank. Although this is well known (see [3] for a short proof), we give a new proof of it by exhibiting an explicit (generalized) inverse for the inclusion matrix.

The polynomial ring. Let $\mathbb{Z}[x_1,\cdots,x_v]$ denote the polynomial ring with v variables over $\mathbb{Z}$. For $\sigma\in S_v$, the group of permutations on $\{1,2,\cdots,v\}$, and f in $\mathbb{Z}[x_1,\cdots,x_v]$, define the polynomial $f^\sigma\in\mathbb{Z}[x_1,\cdots,x_v]$ by

$$f^\sigma(x_1,\cdots,x_v)=f(x_{\sigma(1)},\cdots,x_{\sigma(v)}).$$

We shall say that f is x^2-*free* if every monomial appearing in it is squarefree. With each multiset $\mathcal{B}$ of subsets of $V=\{1,2,\cdots,v\}$ we can associate a polynomial $f_{\mathcal{B}}$ by

$$f_{\mathcal{B}}=\sum_{B\in\mathcal{B}}\prod_{i\in B}x_i. \tag{2}$$

If $\mathcal{B}$ forms a t-design $S_\lambda(t,k,v)$, then the polynomial $f_{\mathcal{B}}$ is a positive integral linear combination of squarefree monomials of degree k with the property (by (1)) that for all $\sigma\in S_v$,

$$f^\sigma(x_1,\cdots,x_t,1,\cdots,1)=\lambda\sum_{i=0}^{t}\frac{\binom{v-t}{t-i}}{\binom{k-i}{t-i}}a_i^\sigma(x_1,\cdots,x_t), \tag{3}$$

where $a_i^\sigma(x_1,\cdots,x_t)$ denotes the ith symmetric function of the x_j's. Thus, a null-design, being the difference of two t-designs, is a homogeneous x^2-free polynomial g of degree k satisfying

$$g^\sigma(x_1,\cdots,x_t,x,\cdots,x)\equiv 0 \tag{4}$$

for all $\sigma\in S_v$. These g form a $\mathbb{Z}$-module N (in the obvious way) which is free since it is contained in the free $\mathbb{Z}$-module of rank $\binom{v}{k}$ generated (over $\mathbb{Z}$) by all the monomials $\{\prod_{i\in I}x_i\colon I\subseteq V,|I|=k\}$.

Generators for null-designs.

THEOREM 1. (*Graver–Jurkat*). *The module N of null-designs is generated over $\mathbb{Z}$ by the collection $\{\phi^\sigma\colon\sigma\in S_v\}$, where*

$$\phi(x_1,\cdots,x_v)=(x_1-x_2)(x_3-x_4)\cdots(x_{2t+1}-x_{2t+2})x_{2t+3}\cdots x_{k+t+1}.$$

This collection is void when $v\leqq k+t$ or $k\leqq t$.

Proof. Suppose f is a nonzero null-design. Without loss of generality, we may assume that the monomial $x_1\cdots x_k$ occurs in f with a nonzero coefficient c. Thus

$$f(\overbrace{1,\cdots,1}^{k},0,\cdots,0)=c\neq 0.$$

It follows from (4) that $k < v-t$ and $v-k < v-t$, i.e.,

$$v \geqq k+t+1 \quad \text{and} \quad k \geqq t+1.$$

In particular, this proves the theorem for the case that $v \leqq k+t$ or $k \leqq t$. □

We now show that f is generated by the ϕ^σ, $\sigma \in S_v$. The proof is by induction on t and, for a fixed t, by induction on v. Because f is x^2-free, we can write

$$f(x_1, \cdots, x_v) = g(x_1, \cdots, x_{v-1}) + h(x_1, \cdots, x_{v-1})x_v.$$

For any permutation $\tau \in S_{v-1}$ and any values of $x_1, \cdots, x_{t-1}, x_v$ and x, we have

$$\begin{aligned} 0 &= f^\tau(x_1, \cdots, x_{t-1}, x, \cdots, x, x_v) \\ &= g^\tau(x_1, \cdots, x_{t-1}, x, \cdots, x) + h^\tau(x_1, \cdots, x_{t-1}, x, \cdots, x)x_v, \end{aligned}$$

and therefore

$$h^\tau(x_1, \cdots, x_{t-1}, x, \cdots, x) = 0.$$

This shows that h is a null-design with parameters $(t-1, k-1, v-1)$ when $t \geqq 1$. Let

$$\theta(x_1, \cdots, x_{v-1}) = (x_1 - x_2) \cdots (x_{2t-1} - x_{2t})x_{2t+1} \cdots x_{k+t-1}.$$

When $t \geqq 1$, we may assume by the induction hypothesis on t that h is an integral linear combination of θ^τ, $\tau \in S_{v-1}$. Of course this is also true when $t = 0$. Thus we can write

$$h(x_1, \cdots, x_{v-1}) = \sum_{\tau \in S_{v-1}} c_\tau \theta^\tau$$

with $c_\tau \in \mathbb{Z}$. Since $v > k+t$, there exists, for each τ, a variable $x(\tau) \neq x_v$ not appearing in θ^τ. Therefore $\theta^\tau(x_v - x(\tau))$ is equal to $\phi^{\sigma(\tau)}$ for some $\sigma(\tau) \in S_v$. Now the polynomial

$$\begin{aligned} f - \sum_{\tau \in S_{v-1}} c_\tau \phi^{\sigma(\tau)} &= g + hx_v - \sum_\tau c_\tau \theta^\tau (x_v - x(\tau)) \\ &= g + \sum_\tau c_\tau \theta^\tau x(\tau) \end{aligned}$$

is a null-design with parameters $(t, k, v-1)$, which by induction on v, is an integral linear combination of the ϕ^σ, $\sigma \in S_{v-1}$. This proves the theorem. □

Note that it follows from Theorem 1 that when $v \leqq k+t$, the only null design is $f \equiv 0$, which in turn implies that the only t-designs are the trivial design (the set of all k-subsets of V) and its multiples. This has previously been pointed out by Wilson [6]. We also remark that a topological proof of the special case of the theorem with $k=3$, $t=2$ has appeared in [4].

A basis for null-designs. Our next task will be to remove the linear dependence from the set of generators $\{\phi^\sigma : \sigma \in S_v\}$. Note that this set actually contains $v!/(t+1)!(k-t-1)!(v-k-t-1)!$ elements, substantially more than the $\binom{v}{k} - \binom{v}{t}$ we eventually shall be left with.

There are 5 kinds of linear dependence which will be removed. They are indicated symbolically as follows: For $a < b < c < d$, replace

(i) $b-a$ by $-(a-b)$;
(ii) $(b-c)a$ by $(a-c)b-(a-b)c$;
(iii) $(b-c)\bar{a}$ by $(a-c)-(a-b)$;
(iv) $(a-d)\bar{b}c$ by $(a-b)c-(a-b)d+(a-c)d-(a-c)b+(a-d)b$;
(v) $(a-d)(b-c)$ by $(a-c)(b-d)-(a-b)(c-d)$.

The meaning of this notation is as follows. If ϕ^σ is of the form $(x_{\sigma(1)}-x_{\sigma(2)})\cdots(x_b-x_a)\cdots x_{\sigma(2t+3)}\cdots$ with $a<b$, for example, then using (i) we replace it by $-\phi^{\sigma'}$ where

$$\sigma'(j)=\begin{cases} a & \text{if } \sigma(j)=b,\\ b & \text{if } \sigma(j)=a,\\ \sigma(j) & \text{otherwise.}\end{cases}$$

In other words, replace ϕ^σ by

$$-(x_{\sigma(1)}-x_{\sigma(2)})\cdots(x_a-x_b)\cdots x_{\sigma(2t+3)}\cdots.$$

In (iii) and (iv) the bar over the variable indicates that the replacement may be made provided that variable does not already occur in ϕ^σ. Thus, with (iii), for example,

$$\phi^\sigma=(x_{\sigma(1)}-x_{\sigma(2)})\cdots(x_b-x_c)\cdots$$

is replaced by the two terms

$$(x_{\sigma(1)}-x_{\sigma(2)})\cdots(x_a-x_c)\cdots$$
$$-(x_{\sigma(1)}-x_{\sigma(2)})\cdots(x_a-x_b)\cdots$$

provided x_a does not occur in ϕ^σ.

Let $S^*_{v,k,t}$ consist of those $\sigma\in S_v$ which satisfy:

(a) $\sigma(1)<\sigma(3)<\cdots<\sigma(2t+1)$;

(b) $\sigma(2)<\sigma(4)<\cdots<\sigma(2t+2)$;

(c) $\sigma(2i-1)<\sigma(2i)$, $1\leqq i\leqq t+1$;

(d) $\sigma(2t+1)<\sigma(2t+3)<\sigma(2t+4)<\cdots<\sigma(k+t+1)$;

(e) $\sigma(2t+1)<\sigma(k+t+2)<\sigma(k+t+3)<\cdots<\sigma(v)$;

(f) If $2t+3\leqq i\leqq k+t+1<j\leqq v$ and $\sigma(i)<\sigma(2t+2)$ then $\sigma(i)<\sigma(j)$.

By repeatedly applying transformations (i)–(v), we can reduce the set of generators stated in Theorem 1 to a much smaller collection.

LEMMA 2. *The module N is generated by* $\{\phi^\tau: \tau\in S^*_{v,k,t}\}$.

Proof. Because of Theorem 1 and the transformation (i), we need only to consider the polynomials ϕ^σ with $\sigma\in S'_v$, where

$$S'_v=\{\sigma\in S_v: \sigma \text{ satisfies the condition (c)}\}.$$

To each $\sigma\in S'_v$, we attach three values:

$$A_\sigma=\sum_{i=1}^{2t+2}\sigma(i),\qquad B_\sigma=\sum_{i=1}^{k+t+1}\sigma(i)$$

and

$$C_\sigma=\max\{\sigma(2i)-\sigma(2i-1): 1\leqq i\leqq t+1\}.$$

Given two elements σ,σ' of S'_v, we say that $\sigma'<\sigma$ if $(A_{\sigma'},B_{\sigma'},C_{\sigma'})$ is smaller than $(A_\sigma,B_\sigma,C_\sigma)$ according to lexicographic order.

Let $\sigma\in S'_v$. If none of the four transformations (ii)–(v) can be performed on ϕ^σ, then reordering the factors $(x_{\sigma(1)}-x_{\sigma(2)}),\cdots,(x_{\sigma(2t+1)}-x_{\sigma(2t+2)})$ of ϕ^σ, the factors $x_{\sigma(2t+3)},\cdots,x_{\sigma(k+t+1)}$ of ϕ^σ, and the unused variables $x_{\sigma(k+t+2)},\cdots,x_{\sigma(v)}$, respectively, by increasing subscript, we see that $\phi^\sigma=\phi^\tau$ for some $\tau\in S^*_{v,k,t}$. If any of the transformations (ii)–(v) can be performed on ϕ^σ, then it is easy to check that ϕ^σ is a linear combination of $\phi^{\sigma'}$ with $\sigma'\in S'_v$ and $\sigma'<\sigma$. Consequently, ϕ^σ is generated by ϕ^τ with $\tau\in S^*_{v,k,t}$. □

A more combinatorial way to view $S'_{v,k,t}$ is to consider it as the set of linear extensions σ of the partial order $<$ on the set $\{1, \cdots, v\}$ shown in Figure 1 which satisfy (f) (where a linear extension of $<$ means a permutation $\sigma \in S_v$ such that $p < p'$ implies $\sigma(p) < \sigma(p')$).

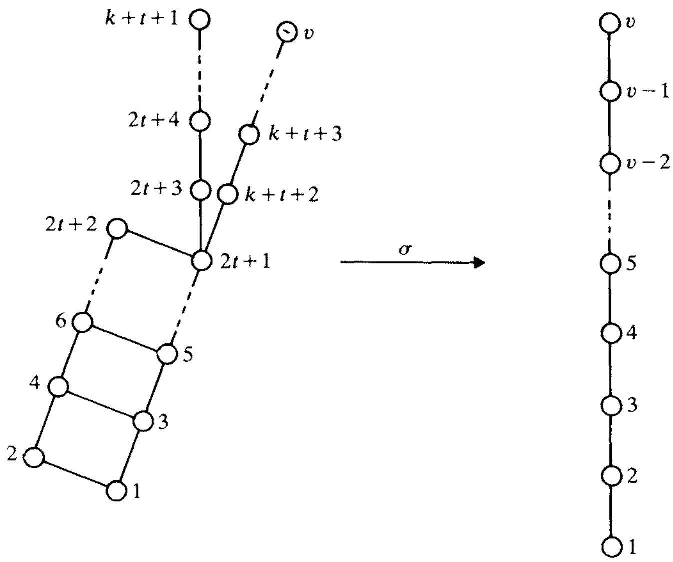

FIG. 1

Let $s_{v,k,t}$ denote $|S^*_{v,k,t}|$. The value of $s_{v,k,t}$ is unexpectedly simple.

THEOREM 3. *For* $v \geqq k+t+1$, $k \geqq t+1$,

$$s_{v,k,t} = \binom{v}{k} - \binom{v}{t}. \tag{5}$$

Proof. The proof will be by induction on v. First, assume $v = k+t+1$, i.e., $k = v-t-1$. In this case, the "tail" of P beginning with $k+t+2$ is empty and conditions (e) and (f) are satisfied vacuously. We consider two cases. Since σ is a linear extension of P, either $\sigma(v) = v$ or $\sigma(2t+2) = v$. If $\sigma(v) = v$, then by induction the number of σ is $s_{v-1,v-t-2,t} = \binom{v-1}{t+1} - \binom{v-1}{t}$. If $\sigma(2t+2) = v$ then again by induction the number of σ is $s_{v-1,v-t-1,t-1} = \binom{v-1}{t} - \binom{v-1}{t-1}$. Since the sum of these two expressions is $\binom{v}{t+1} - \binom{v}{t} = s_{v,v-t-1,t}$, the induction step is complete in this case.

Now, assume $v > k+t+1$. For a fixed v, we shall argue by induction on k. As before we distinguish cases according to the possible values of $\sigma^{-1}(v)$. In this case there are three possibilities: v, $k+t+1$ or $2t+2$. If $\sigma(v) = v$, then by induction on v the number of these σ is $s_{v-1,k,t} = \binom{v-1}{k} - \binom{v-1}{t}$. If $\sigma(v) = k+t+1$, then by induction on k the number of these σ is $s_{v-1,k-1,t} = \binom{v-1}{k-1} - \binom{v-1}{t}$. If $\sigma(v) = 2t+2$, then condition (f) and the induction hypothesis imply that the number of these σ is $s_{v-1,v-t-1,t-1} = \binom{v-1}{t} - \binom{v-1}{t-1}$. Thus, the sum of these is $s_{v,k,t} = \binom{v}{k} - \binom{v}{t}$ which completes the induction step. Since (5) obviously holds for $v = 2$, the theorem is proved. □

Note that for $v=k+t+1$ or $k=t+1$, the mapping $\sigma: P\to V$ can be interpreted as a "voting sequence" for two candidates A and B [1] with the integers $\{2, 4, \cdots, 2t+2\}$ denoting votes for A, $\sigma(2i)=j$ indicating that the jth vote cast was the ith vote cast for A. The requirement that σ is a linear extension implies that A never leads B during the voting. The number of such σ is well known to be $\binom{v}{t+1}-\binom{v}{t}$ (see [1]).

Finally, we show that the elements of $S^*_{v,k,t}$ are linearly independent over $\mathbb{Z}$. Let $\mathbb{Z}_i[x_1, \cdots, x_v]$ denote the $\mathbb{Z}$-submodule of $\mathbb{Z}[x_1, \cdots, x_v]$ consisting of the homogeneous x^2-free polynomials of degree i. Consider the linear mapping $\mathcal{H}: \mathbb{Z}_k[x_1, \cdots, x_v]\to\mathbb{Z}_t[x_1, \cdots, x_v]$ given by defining

$$\mathcal{H}\Big(\prod_{\substack{j\in J\\|J|=k}} x_j\Big)=\sum_{\substack{I\subseteq J\\|I|=t}}\prod_{i\in I} x_i$$

on a basis of $\mathbb{Z}_k[x_1, \cdots, x_v]$ and extending $\mathcal{H}$ to $\mathbb{Z}_k[x_1, \cdots, x_v]$ by linearity. It is easy to see that $N=\operatorname{Ker}(\mathcal{H})$. Consider the matrix $H_{v,k,t}$ of $\mathcal{H}$ with respect to the basis of monomials of $\mathbb{Z}_k(x_1, \cdots, x_v)$ and $\mathbb{Z}_t(x_1, \cdots, x_j)$, respectively. $H_{v,k,t}$ is a $\binom{v}{t}$ by $\binom{v}{k}$ matrix with rows indexed by t-subsets X of V, columns indexed by k-subsets Y of V and having as its (X, Y) entry 1 if $X\subseteq Y$ and 0 otherwise. For our choice of parameters, $v\geqq k+t+1$ and $k\geqq t+1$. Thus, $H_{v,k,t}$ has at least as many columns as rows. Then as noted earlier, rank $(H_{v,k,t})=\binom{v}{t}$. A direct way to verify this is as follows. Define the $\binom{v}{k}$ by $\binom{v}{t}$ matrix $H^*=(h^*_{Y,X})$ indexed by k-subsets Y and t-subsets X of V by taking

$$h^*_{Y,X}=\frac{(-1)^{k-t}(k-t)}{(-1)^{|Y-X|}|Y-X|}\cdot\frac{1}{\binom{v-t}{|Y-X|}}.$$

Then the (X, X') entry of $H_{v,k,t}H^*$ is

$$(6)\qquad (-1)^{k-t}(k-t)\sum_{\substack{Y\supseteq X\\|Y|=k}}\frac{(-1)^{|Y-X'|}}{|Y-X'|\binom{v-t}{|Y-X'|}}.$$

By partitioning the sum according to the values of $|Y-X'|$, standard binomial coefficient identities show that (6) is equal to 1 if $X=X'$ and 0 otherwise. Thus,

$$H_{v,k,t}H^*=I_{\binom{v}{t}}$$

where I_x denotes the x by x identity matrix. Therefore, the rank of $\mathcal{H}$ is $\binom{v}{t}$ and N, being Ker $(\mathcal{H})$, has dimension $\binom{v}{k}-\binom{v}{t}$. As an immediate consequence we have:

THEOREM 4. *$\{\phi^\sigma: \sigma\in S^*_{v,k,t}\}$ forms a basis for N.*

Concluding remarks.

1. The form of the value of $s_{v,k,t}$, namely, $\binom{v}{k}-\binom{v}{t}$ suggests that there may be a more direct interpretation which would allow one to write this value down at once. If so, what is it?

2. In a similar spirit, one suspects that the inverse of $H_{v,k,t}$ given in (6) may be part of a much more general phenomenon, perhaps involving Möbius inversion. However, we have not pursued this here.

3. Is it feasible to search for new t-designs by starting from known (perhaps trivial) designs and augmenting them by null-designs? We have no computational evidence at present.

4. Consider the set of all polynomials $g \in \mathbb{Z}[x_1, \cdots, x_v]$ satisfying (4). These form an ideal which we denote by $I(v, t)$. Our null-designs are just the x^2-free homogeneous polynomials of degree k in $I(v, t)$. If we were to allow repetitions of elements in the blocks of $\mathfrak{B}$, the corresponding null-designs would consist of *all* homogeneous polynomials of degree k in $I(v, t)$. It is natural to ask for a set of ideal generators for $I(v, t)$ in general.

In view of Theorem 1, one would expect that $\{\psi^\sigma : \sigma \in S_v\}$ generates $I(v, t)$ when $v \geqq 2t+2$, where

$$\psi(x_1, \cdots, x_v) = (x_1 - x_2) \cdots (x_{2t+1} - x_{2t+2}).$$

For general v and t we do the following. Let π be a partition of the set $\{1, \cdots, v\}$ into disjoint subsets $V_1, \cdots, V_{v-t-1}$ having as nearly equal cardinalities as possible. Define

$$\psi_\pi = \prod_{r=1}^{v-t-1} \prod_{\substack{i,j \in V_r \\ i<j}} (x_i - x_j).$$

One of us (W. Li) has conjectured that these ψ_π generate the ideal $I(v, t)$. This is known to be true for $t = 2$.

Note added in proof. This conjecture has now been proved by W. Li and R. Li and will appear in a forthcoming paper.

REFERENCES

[1] W. FELLER, *An Introduction to Probability Theory and its Applications*, vol. 1, John Wiley, New York, 1967.

[2] J. E. GRAVER AND W. B. JURKAT, *The module structure of integral designs*, J. Combinatorial Theory (A), 15 (1973), pp. 75–90.

[3] W. FOODY AND A. HEDAYAT, *On theory and applications of BIB designs with repeated blocks*, Annals Statist., 5 (1977), pp. 932–945.

[4] A. HEDAYAT AND S.-Y. R. LI, *Combinatorial topology and the trade off method in BIB designs*, Proc. Sym. on Combinatorial Mathematics and Optimal Design (Colorado State Univ.), 1978, to appear.

[5] D. R. RAY-CHAUDHURI AND R. M. WILSON, *On t-designs*, Osaka J. Math., 12 (1975), pp. 737–744.

[6] R. W. WILSON, *The necessary conditions for t-designs are sufficient for something*, Utilitas Math., 4 (1973), pp. 207–215.