# Codes and modules associated with designs and $t$-uniform hypergraphs

—Abstract and summary—

Richard M. Wilson
*California Institute of Technology*

**Abstract.** The first part of these lectures introduces the Smith normal form and the invariant factors of an integer matrix, and the relation of Smith form to systems of linear diophantine equations. We give selected examples of how invariant factors appear and may be applied to the theory of combinatorial designs. Importantly, we may sometimes construct sefl-dual $p$-ary codes from hypothetical designs and sometimes deduce the non-existence of designs from a theorem of Witt. In the second part of the notes, we are concerned with diagonal forms of various incidence matrices arising from $t$-designs and $t$-uniform hypergraphs. Applications are given to a certain zero-sum Ramsey-type problem involving $t$-uniform hypergraphs.

## 1. Introduction

In these lecture notes, we survey some appearances of Smith normal form (or invariant factors, or elementary divisors) of integer matrices that arise in the theory of combinatorial designs. We are also concerned with the $p$-ary codes that are generated by or arise from integer matrices, for primes $p$.

The invariant factors, and hence the rank modulo a prime $p$, of a matrix $A$ do not change on row or column permutations of the rows and columns (or transpose). Thus they do not depend on the ordering of the vertices when $A$ is the adjacency matrix of a graph $G$, or on the ordering of points and blocks or some incidence structure $\mathcal{S}$. etc. Thus the invariant factors of the adjacency matrix of a graph $G$, or the incidence matrix of $\mathcal{S}$, are *invariants* of $G$ or $\mathcal{S}$, respectively, and are also the same for two isomorphic graphs or incidence matrices. So, for example, two graphs can be shown to be nonisomorphic by showing that they have different invariant factors.

The simplest way to get a $p$-ary code from an integer matrix $A$ is to take its row space modulo $p$. The dimension of this code is the $p$-rank of $A$, and it is equal to the number of invariant factors of $A$ that are not divisible by $p$. A chain of $p$-ary codes $C_0 \subseteq C_1 \subseteq C_2 \subseteq \ldots$ may be defined so that the dimension of $C_j$ is the number of invariant factors of $A$ that are not divisible by $p^{j+1}$.

If $A$ is the incidence matrix, or modified incidence matrix, of a hypothetical design, it is sometimes possible to show that one of these codes is self-dual with respect to an appropriate inner product. Witt's theorem (see Section 5) may imply that a code with these properties does not exist, in which case we may conclude that the hypothetical

design does not exist. Nonexistence results of this type are sometimes consequences of the Hasse-Minkowski theory of rational congruence, but at other times may be proved when the theory of rational congruence does not appear to apply. A self-dual binary code of length 112 would arise from a hypothetical projective plane of order 10; in this case, coding theory and extensive calculations by Lam and others shows that no such plane exists; see [12].

Inclusion matrices of $t$-subsets verusus $k$-subsets, and, more generally, incidence matrices of $t$-subsets and the $t$-uniform hypergraphs isomorphic to a given $t$-uniform hypergraph $H$, are introduced in Section 7. Diagonal forms for the inclusion matrices are described. The results of Section 7 are applied to the binary case of a zero-sum Ramsey-type problem introduced by Alon and Caro [1] in Section 9. In Section 10, we describe some recent joint work with Tony Wong on diagonal forms of the latter incidence matrices, in particular when $t = 2$, and $H$ is a simple graph.

Most proofs are omitted in this summary. Many will be supplied in the lectures or in more extensive notes.

## 2. Smith and diagonal form

Given an $r$ by $m$ integer matrix $A$, there exist unimodular matrices $E$ and $F$, of orders $r$ and $m$, so that $EAF = D$ where $D$ is an $r$ by $m$ diagonal matrix. Here 'diagonal' means that the $(i, j)$-entry of $D$ is 0 unless $i = j$; we do not require that $D$ is square. We call any matrix $D$ that arises in this way a *diagonal form* for $A$.

Let the diagonal entries of $D$ be $d_1, d_2, d_3, \ldots$. Here and in the sequel, $d_i$ may be interpreted as 0 if the index $i$ exceeds the number of rows or columns. If all diagonal entries $d_i$ are nonnegative and $d_i$ divides $d_{i+1}$ for $i = 1, 2, \ldots$, then $D$ is called the *integer Smith normal form* of $A$, or simply the Smith form of $A$, and the integers $d_i$ are called the *invariant factors*, or the *elementary divisors* of $A$. The Smith form is unique; the unimodular matrices $E$ and $F$ are not.

As a simple example, let $A = \begin{pmatrix} 3 & 1 & 4 \\ 4 & -2 & 7 \end{pmatrix}$. We have

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 1 & 4 \\ 4 & -2 & 7 \end{pmatrix} \begin{pmatrix} 0 & -1 & 3 \\ 1 & -1 & -1 \\ 0 & 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix}$$

where the first and the third matrices are unimodular. Thus $D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix}$ is a diagonal form of $A$.

Let $s_1, s_2, \ldots, s_n$ be the invariant factors of a $n$ by $n$ integer matrix $A$. If $A$ is nonsingular, then $s_n A^{-1}$ is integral. One way to see this is to use the formula

$$A^{-1} = \frac{1}{\det(A)} A^{\mathrm{adj}}$$

where $A^{\mathrm{adj}}$ is the classical adjoint of $A$, with $(i, j)$-entry $(-1)^{i+j} \det(A_{ji})$ and where $A_{ji}$ is the result of deleting row $j$ and column $i$ from $A$. The determinant $\det(A_{ji})$ is an integer divisible by $s_1 s_2 \cdots s_{n-1}$ and $\det(A) = s_1 \cdots s_n$.

## 3. Solutions of linear equations in integers

Diagonal forms are related to solutions of systems of linear equations or congruences in integers. This, in fact, was the topic of H. J. S. Smith's original paper on the subject.

Let $A$ be an $r$ by $m$ integer matrix. Suppose $EAF = D$ where $E$ and $F$ are unimodular and $D$ is diagonal with diagonal entries $d_1, d_2, \ldots$. The system $A\mathbf{x} = \mathbf{b}$ is equivalent to $(AF)(F^{-1}\mathbf{x}) = \mathbf{b}$, and this has integer solutions $\mathbf{x}$ if and only if $(AF)\mathbf{z} = \mathbf{b}$ has an integer solution $\mathbf{z}$. This in turn will have integer solution if and only if $EAF\mathbf{z} = E\mathbf{b}$, or $D\mathbf{z} = E\mathbf{b}$, has integer solutions.

In other words, if we let $\mathbf{e}_i$ denote the $i$-th row of $E$, the system $A\mathbf{x} = \mathbf{b}$ has integer solutions if and only if

$$\mathbf{e}_i\mathbf{b} \equiv 0 \pmod{d_i} \quad \text{for } i = 1, 2, \ldots, r. \tag{1}$$

If the conditions (1) hold, then the integer solutions are easy to describe.

As a simple example,

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 1 & 4 \\ 4 & -2 & 7 \end{pmatrix} \begin{pmatrix} 0 & -1 & 3 \\ 1 & -1 & -1 \\ 0 & 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix}$$

and so the system of equations

$$\begin{aligned} 3x + y + 4z &= a \\ 4x - 2y + 7z &= b \end{aligned}$$

has an integer solution if and only if $2a + b \equiv 0 \pmod{5}$.

## 4. Square incidence matrices

The following two theorems are from Newman [16].

**Theorem 4.1** *Suppose $A$ is an $n$ by $n$ integer matrix such that $AA^\top = mI$ for some integer $m$. Let $s_1, s_2, \ldots, s_n$ be the invariant factors of $A$. Then $s_i s_{n+1-i} = m$ for $i = 1, 2, \ldots, n$.*

**Proof.** If $cA^{-1}$ is an integer matrix for some integer $c$, then the invariant factors of $cA^{-1}$ are $c/s_n, c/s_{n-1}, \ldots, c/s_2, c/s_1$. To see this, suppose $EBF = D$ for some unimodular matrices $E$ and $F$, where $D = \text{diag}(s_1, s_2, \ldots, s_n)$ is the Smith form, of $A$, with diagonal entries

$$s_1 \mid s_2 \mid \cdots \mid s_n. \tag{2}$$

Then $F^{-1}(cA^{-1})E^{-1} = cD^{-1}$. That is, $cD^{-1}$ is a diagonal form for $cA^{-1}$. It is not necessarily the Smith form, since the diagonal element $c/s_{i+1}$ divides $c/s_i$ and not the other way around. But the invariant factors of $cA^{-1}$ in the correct order will be

$$\frac{c}{s_n} \mid \frac{c}{s_{n-1}} \mid \cdots \mid \frac{c}{s_2} \mid \frac{c}{s_1}. \tag{3}$$

If $AA^\top = mI$, then $A^\top = mA^{-1}$ is integral and the invariant factors of $A^\top$ are those in (3) with $c$ replaced by $m$. But the invariant factors of the transpose of a matrix are the same as those of the orignal matrix, and so the factors in (2) are, by the uniquess of the Smith form, identical to those in (3), with $c$ replaced by $m$, and the result follows. □

A *Hadamard matrix* of order $n$ is an $n$ by $n$ matrix $H$, with entries $+1$ and $-1$ only, so that $HH^\top = nI$. It is known that the existence of a Hadamard matrix of order $n$ implies $n = 1, 2,$ or $4m$ for some integer $m$.

**Theorem 4.2** *If $H$ is a Hadamard matrix of order $n = 4t$, and $t$ is squarefree, then the invariant factors of $H$ are*

$$(1)^1, \quad (2)^{2t-1}, \quad (2t)^{2t-1}, \quad (4t)^1.$$

**Proof.** By Theorem 4.1, the invariant factors $s_i$ of $H$ satisfy $s_i s_{n+1-i} = n = 4t$. Since the entries of $H$ are $\pm 1$, it is clear that $s_1 = 1$, and since the 2-rank of $H$ is 1, all invariant factors of $H$ are even except for the smallest, $s_1$. For $i \leq n/2$, $s_i$ divides $s_{n+1-i}$, so $s_i^2$ divides $4t$. Since $t$ is squarefree, we conclude that $s_i$ divides 2, and so is equal to 2 for $i = 2, 3, \ldots, n/2$. The theorem follows. □

A *conference matrix* of order $n$ is an $n$ by $n$ matrix $C$, with 0's on the diagonal and non-diagonal entries $+1$ and $-1$ only, so that $CC^\top = (n-1)I$. It is clear that the order of a conference matrix, if greater than 1, is even.

**Theorem 4.3** *If $C$ is a conference matrix of order $n = 2t$, and $n - 1$ is squarefree, then the invariant factors of $C$ are*

$$(1)^t, \quad (n-1)^t.$$

**Theorem 4.4** *Suppose $A$ is an $n$ by $n$ integer matrix such that $AUA^\top = mV$ for some integer $m$, where $U$ and $V$ are square matrices of order $n$ with determinants relatively prime to $m$. Let $s_1, s_2, \ldots, s_n$ be the invariant factors of $A$. Then $s_i s_{n+1-i} = m$ for $i = 1, 2, \ldots, n$.*

A $(v, k, \lambda)$-*design* consists of a $v$-set $X$ (of *points*) and a family $\mathcal{B}$ of $k$-subsets (called *blocks*) of $X$ so that any two distinct points are contained in exactly $\lambda$ of the blocks. For background on designs, and proofs of the observations of the next two paragraphs, see Chapter 19 of [15].

The incidence matrix $N$ of such a design is the $v$ by $b$ matrix (here $b = |\mathcal{B}| = \lambda v(v-1)/(k(k-1))$ is the number of blocks) with rows indexed by the elements of $X$, columns indexed by the elements of $\mathcal{B}$, and where

$$N(x, B) = \begin{cases} 1 & \text{if } x \in B, \\ 0 & \text{otherwise.} \end{cases}$$

It is well known that

$$NN^\top = (r-\lambda)I + \lambda J \tag{4}$$

where $r = \lambda(v-1)/(k-1)$ is the number of blocks that contain any given point. Here $I$ and $J$ are $v$ by $v$ matrices, where $I$ is the identity and $J$ the matrix of all 1's.

When $|X| = |\mathcal{B}|$, i.e. $v = b$, the design is said to be a $(v,k,\lambda)$-*symmetric design*. Here the incidence matrix is square of order $v$. We have $r = k$ and a fundamental relation $\lambda(v-1) = k(k-1)$. It is clear that the sum of all rows of $N$ is the row vector $(k,k,\ldots,k)$, and the sum of all columns of $N$ is the transpose of this vector. The equation (4) implies $\det(N) = \pm n^{(v-1)/2}k$.

**Theorem 4.5** (Deretzky [6]) *Let $N$ is the incidence matrix of a $(v,k,\lambda)$-symmetric design where $k$ and $\lambda$ are relatively prime, and write $n = k-\lambda$. The invariant factors of $N$ satisfy*

$$s_1 = s_2 = 1, \quad s_i s_{v+2-i} = n \quad \textit{for } i = 3,4,\ldots,v-1, \quad \textit{and } s_v = nk.$$

## 5. Self-dual codes; Witt's theorem

A *$p$-ary linear code* of length $n$ is a subspace $C$ of the vector space $\mathbb{F}_p^n$ of ordered $n$-tuples of elements of the field $\mathbb{F}_p$ of $p$ elements. Here $p$ is a prime, and we normally think of members of $C$ and $\mathbb{F}_p^n$ as row vectors. All codes in these notes will be linear codes over a prime field.

Given a $p$-ary code $C$, the *dual code* $C^\perp$ is defined as the set of $\mathbf{a} \in \mathbb{F}_p^n$ such that $\langle \mathbf{a}, \mathbf{c}\rangle = 0$ for all $\mathbf{c} \in C$. Here $\langle \mathbf{a}, \mathbf{c}\rangle$ is the standard inner product of the two vectors, i.e. $\langle \mathbf{a}, \mathbf{c}\rangle = a\mathbf{c}^\top$. The dimensions $\dim(C)$ and $\dim(C^\top)$ sum to $n$. The code $C$ is *self-orthogonal* when $C \subseteq C^\perp$, and *self-dual* when $C = C^\perp$. A self-dual code of lenth $n$ has dimension $n/2$.

Given an $r$ by $m$ integer matrix $A$, we may consider the rows as vectors in $\mathbb{F}_p^m$. The row space $\mathrm{row}_p(A)$ of $A$ over $\mathbb{F}_p$ is, of course, a $p$-ary linear code; $C^\perp$ is the null space of $A$ over $\mathbb{F}_p$. Multiplying a matrix on the right of left by a unimodular matrix does not change its rank modulo $p$, so the dimension of $C = \mathrm{row}_p(A)$ is the rank modulo $p$ of a diagonal form $D$ of $A$, and this is the number of diagonal entries of $D$ that are *not* divisible by $p$.

Self-dual codes may be obtained from certain Hadamard and conference matrices. More generally, suppose $AA^\top = mI$ for some $n$ by $n$ matrix $A$. Suppose $p$ is a prime that divides $m$. Then $AA^\top = O$ over $\mathbb{F}_p$, so $\mathrm{row}_p(A)$ is a self-orthogonal code. Now suppose that $p$ exactly divides $m$, i.e. $p \mid m$ but $p^2 \not| m$. Let $s_1, s_2, \ldots, s_n$ be the invariant factors of $A$. By Theorem 4.1, $s_i s_{n+1-i} = m$, so exactly one of $s_i$ and $s_{n+1-i}$ is divisible by $p$. It follows that the $p$-rank of $A$ is $n/2$ and that $\mathrm{row}_p(A)$ is a self-dual $p$-ary code.

The simplest case of Witt's Theorem, Theorem 5.2 below, is that there exists a self-dual $p$-ary code of length $n$, where $p$ is an odd prime, if and only if $(-1)^{n/2}$ is a square in $\mathbb{F}_p$. This says nothing if $n \equiv 0 \pmod 4$ or if $p \equiv 1 \pmod 4$, because this condition is always true. But when $n \equiv 2 \pmod 4$ and $p \equiv 3 \pmod 4$, there is no self-dual $p$-ary code of length $n$.

Given an $r$ by $m$ integer matrix $A$, we define, for any prime $p$ and nonnegative integer $i$,

$$\mathcal{M}_i(A) = \{\mathbf{x} \in \mathbb{Z}^m : p^i \mathbf{x} \in \text{row}_{\mathbb{Z}}(A)\}.$$

We have $\mathcal{M}_0(A) = \text{row}_{\mathbb{Z}}(A)$ and

$$\mathcal{M}_0(A) \subseteq \mathcal{M}_1(A) \subseteq \mathcal{M}_2(A) \subseteq \ldots.$$

Let

$$C_i(A) = \mathcal{M}_i \pmod p.$$

That is, read all the integer vectors in $\mathcal{M}_i(A)$ to obtain $C_i(A)$. Then each $C_i(A)$ is a $p$-ary linear code. Clearly,

$$C_0(A) \subseteq C_1(A) \subseteq C_2(A) \subseteq \ldots.$$

**Theorem 5.1** *Let $D$ be a diagonal form for $A$, with diagonal entries $d_1, d_2, \ldots$. Then the dimensions of the $p$-ary code $C_j(A)$ is the number of diagonal entries $d_i$ that are not divisible by $p^{j+1}$.*

We may use a symmetric nonsingular matrix $U$ over a field $\mathbb{F}_p$ with $p$ odd to introduce a new inner product $\langle \cdot, \cdot \rangle_U$ for row vectors in ${\mathbb{F}_p}^n$, namely

$$\langle \mathbf{a}, \mathbf{c} \rangle_U = \mathbf{a} U \mathbf{c}^\top.$$

For a linear $p$-ary code $C \subset \mathbb{F}_p^n$, the $U$-dual code of $C$ is

$$C^U = \{\mathbf{a} : \langle \mathbf{a}, \mathbf{c} \rangle_U = 0 \quad \text{for all } \mathbf{c} \in C\}.$$

It is still true that the dimensions of $C$ and ${C}^U$ sum to $n$. In the theory of vector spaces equipped with quadratic forms, a $p$-ary code is said to be *totally isotropic* with respect to $U$ when $C \subseteq C^U$. When $U = I$, totally isotropic is the same as self-dual. We may call $C$ *self-$U$-dual* when $C = C^U$.

**Theorem 5.2** (Witt) *Given a symmetric nonsingular matrix $B$ over a field $\mathbb{F}$ of odd characteristic, there exists a totally isotropic subspace of dimension $m/2$ in ${\mathbb{F}}^m$ if and only if $(-1)^{m/2} \det(B)$ is a square in $\mathbb{F}$.*

**Lemma 5.3** *Let $L$ and $M$ be integer matrices with $L$ square so that $LM$ is defined. Suppose $\det(L)$ is relatively prime to $p$. Then the invariant $p$-factors of $LM$ are the same as those of $M$.*

In the proof, we show $C_i(LM) = C_i(M)$ for all $i$.

**Theorem 5.4** *Suppose $A$ is an $n$ by $n$ integer matrix such that $AUA^\top = p^e V$ for some integer $m$, where $U$ and $V$ are square matrices with determinants relatively prime to $p$. Then $C_e(A) = \mathbb{F}_p^n$ and*

$$C_i^U = C_{e-i-1} \quad \textit{for } i = 0, 1, \ldots, e-1.$$

**Corollary 5.5** (i) *Suppose $H$ is a Hadamard matrix of order $n$ and $p$ a prime so that $p^{2f+1}$ exactly divides $n$. Then $C_f$ is a self-dual $p$-ary code.* (ii) *Suppose $C$ is a conference matrix of order $n$ and $p$ a prime so that $p^{2f+1}$ exactly divides $n-1$. Then $C_f$ is a self-dual $p$-ary code.*

**Proof.** (i) Take $e = 2f+1$, $U = I$, $V = (n/p^f)I$ in Theorem 5.4. For (ii), take $V = ((n-1)/p^f)$. □

**Theorem 5.6** *If there exists a conference matrix of order $n \equiv 2 \pmod 4$, then $n-1$ is the sum of two squares. More generally, if there is a square integer matrix $A$ of order $n \equiv 2 \pmod 4$ so that $AA^\top = mI$, then $m$ is the sum of two squares.*

**Proof.** It is well known that an integer $m$ is the sum of two squares if and only if no prime $p \equiv 3 \pmod 4$ divides the square-free part of $m$. If $p$ divides the squarefree part of $m$, Theorem **??**ives us a self-dual code of length $n \equiv 2 \pmod 4$ and Witt's Theorem implies that $-1$ is a square in $\mathbb{F}_p$, which implies $p \equiv 1 \pmod 4$. □

## 6. Symmetric and quasi-symmetric designs

**Theorem 6.1** (Lander [14]) *Suppose there exists a symmetric $(v, k, \lambda)$-design where $n$ is exactly divisible by an odd power of a prime $p$. Write $n = p^f n_0$ ($f$ odd) and $\lambda = p^b \lambda_0$ with $(n_0, p) = (\lambda_0, p) = 1$. Then there exists a self-dual $p$-ary code of length $v+1$ with respect to the scalar product corresponding to*

$$U = \begin{cases} \mathrm{diag}(1, 1, \ldots, 1, -\lambda_0) & \textit{if } b \textit{ is even}, \\ \mathrm{diag}(1, 1, \ldots, 1, n_0\lambda_0) & \textit{if } b \textit{ is odd}. \end{cases}$$

*Hence from Witt's Theorem,*

$$\begin{cases} -(-1)^{(v+1)/2}\lambda_0 \textit{ is a square} \pmod p & \textit{if } b \textit{ is even}, \\ (-1)^{(v+1)/2} n_0\lambda_0 \textit{ is a square} \pmod p & \textit{if } b \textit{ is odd}. \end{cases}$$

The following theorem is only one part of results of Calderbank.

**Theorem 6.2** (Calderbank) *Let $\mathcal{B}$ be a 2-$(v, k, \lambda)$, and $p$ be an odd prime that exactly divides $r - \lambda$; further suppose that $|A \cap B| \equiv s \pmod p$ for any two blocks $A$ and $B$ of the design. If $v$ is odd, then $-v(-1)^{(v+1)/2}$ is a square modulo $p$.*

The proof constructs a self-$U$-dual code of length $(v+1)/2$ where $U = \mathrm{diag}(1, 1, \ldots, 1, -v)$.

Blokhuis and Calderbank [2] have results on 2-$(v, k, \lambda)$ designs so that $p^e$ exactly divides $r - \lambda$ and $|A \cap B| \equiv s \pmod{p^e}$ for any two blocks $A$ and $B$ of the design.

## 7. The matrices of $t$-subsets versus $k$-subsets or $t$-uniform hypergaphs

By a $(t, v)$-*vector* based on $X$, or just a $t$-vector if the set $X$ is understood, we mean a (row or column) vector whose coordinates are indexed by the $t$-subsets of an $v$-set $X$. We often use functional notation: if $\mathbf{f}$ is a $t$-vector and $T$ a $t$-subset of $X$, then $\mathbf{f}(T)$ will denote the entry of $\mathbf{f}$ in coordinate position $T$.

For integers $t, k, v$ with $0 \le t \le k \le v$, let $W_{tk}$ or $W_{tk}^v$ denote the $\binom{v}{t}$ by $\binom{v}{k}$ matrix whose rows are indexed by the $t$-subsets of an $v$-set $X$, whose columns are indexed by the $k$-subsets of $X$, and where the entry in row $T$ and column $K$ is

$$W_{tk}(T, K) := \begin{cases} 1 & \text{if } T \subseteq K, \\ 0 & \text{otherwise.} \end{cases}$$

The question of whether there exist integer solutions $\mathbf{x}$ of $W_{tk}\mathbf{x} = \mathbf{1}$ is related to the existence problem for $t$-designs. A simple $t$-$(v, k, \lambda)$ *design* consists of a set $X$ and a set $\mathcal{A}$ of $k$-subsets if $X$ so that every $t$-subset of $X$ is contained in exactly $\lambda$ members of $\mathcal{A}$.

Let $\mathbf{u}$ be the characteristic $k$-vector of a set $\mathcal{A}$ of $k$-subsets of $X$. This means that $\mathbf{u}(A) = 1$ if $A \in \mathcal{A}$ and otherwise $\mathbf{u}(A) = 0$. Then for a $t$-subset $T$ of $X$,

$$(W_{tk}\mathbf{u})(T) = \sum_A \mathbf{u}(A) W_{tk}(A) = \sum_{A \in \mathcal{A}, T \subseteq A} 1 = \lambda.$$

That is, $(X, \mathcal{A})$ is a $t$-design if any only if $W_{tk}\mathbf{u} = \lambda\mathbf{1}$ when here $\mathbf{1}$ is the $t$-vector of all 1's. We allow not-necessarily-simple $t$-$(v, k, \lambda)$ designs where the members of $\mathcal{A}$ may have multiplicities (or, $\mathcal{A}$ may be thought of as a multiset of $k$-subsets). These correspond to $k$-vectors $\mathbf{u}$ of nonnegative integers satisfying $W_{tk}\mathbf{u} = \lambda\mathbf{1}$. Finally, we may consider *signed $t$-designs*, where $k$-subsets are counted with positive or negative multiplicities, and these correspond to integer $k$-vectors $\mathbf{u}$ satisfying $W_{tk} = \mathbf{1}$.

The following theorem is from [10] and [21]. It is also a consequence of Theorem 7.3.

**Theorem 7.1** *Let $\mathbf{b}$ be a $t$-vector of height $\binom{v}{t}$ based on a $v$-set $X$. Necessary and sufficient conditions for the existence of an integer $k$-vector $\mathbf{u}$ of height $\binom{v}{t}$ based on $X$ so that $W_{tk}\mathbf{x} = \lambda\mathbf{1}$ are*

$$\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}} \quad \textit{for } i = 0, 1, \ldots, t. \tag{5}$$

Systems of diophantine linear equations have come up repeatedly in work on the asymptotic existence of decompositions of complete graphs ($G$-designs). Theorem 7.2 is from [22].

**Theorem 7.2** *Let $G$ be a simple graph on $k$ vertices and assume $n \ge k + 2$. Let $\mathcal{G}$ be the set of all subgraphs of the complete graph $K_n$ that are isomorphic to $G$. There exists a family $\{x_H : H \in \mathcal{G}\}$ of integers $x_G$ so that for every edge $e$ of $K_n$,*

$$\sum_{H : e \in E(H)} x_H = 1, \tag{6}$$

*where the sum is extended is over those subgraphs $G \in \mathcal{G}$ which contain the edge $e$, if and only if $\binom{n}{2}$ is divisible by the number of edges of $G$, and $n-1$ is divisible by the greatest common divisor of the degrees of the vertices of $G$.*

The conditions that $\binom{n}{2}$ is divisible by the number of edges of $G$, and $n-1$ is divisible by the greatest common divisor of the degrees of the vertices of $G$ are necessary for the existence of a decomposition (a partition of the edges) of $K_n$ into subgraphs isomorphic to $G$. Theorem 7.2 played an essential role in the proof given in [22] that, given $G$, such decompositions exist for all sufficiently large integers $n$ satisfying these conditions. (Such decompositions may also be called *$G$-designs*.) Similar theorems, but about more complicated systems of equations related to decompositions of 'edge-colored complete graphs', may be found in in [13] and [7].

A commonn generalization and extension of Theorems 7.1 and 7.2 is Theorem 7.3 below.

Given a $t$-vector $\mathbf{h}$ based on a $v$-set $X$, we consider the matrix $N_t(\mathbf{h})$ or $N_t$ whose columns are all distinct images of $\mathbf{h}$ under the symmetric group $S_n$ acting on the $t$-subsets of $X$. So $N_t$ has $\binom{v}{t}$ rows and at most $n!$ columns. (For most purposes, it does not matter if $N_t$ has repeated columns.) When $\mathbf{h}$ is the characteristic vector of the complete $t$-uniform hypergraph $K_v^t$, whose hyperedges are all $t$-subsets of $X$, we have $N_t = W_{tk}$. If $t = 2$ and $\mathbf{h}$ is he characteristic 2-vector of a simple graph $G$, then $N_2$ is the matrix of the system of equations in Theorem (6).

**Theorem 7.3** *Let $\mathbf{b}$ be a $t$-vector of height $\binom{v}{t}$ so that the associated signed multihypergraph has at least $t$ isolated vertices. Necessary and sufficient conditions for the existence of an integer solution $\mathbf{x}$ to $N_t\mathbf{x} = \mathbf{b}$ are*

$$W_{it}\mathbf{b} \equiv 0 \pmod{g_i} \quad \textit{for } i = 0, 1, \ldots, t$$

*where $g_i$ is the gcd of all entries of $W_{it}N_t$.*

**Theorem 7.4** *Let $\mathbf{b}$ be a $t$-vector of height $\binom{v}{t}$ so that the associated signed multihypergraph has at least $t$ isolated vertices, and let $g_i$ be the gcd of all entries of $W_{it}N_t$. Then one diagonal form for $N_t$ has diagonal entries*

$$(g_0)^{\binom{n}{t}-\binom{n}{t-1}}, \quad (g_1)^{\binom{n}{t-1}-\binom{n}{t-2}}, \quad \ldots, \quad (g_t)^1.$$

The proofs of Theorems 7.3 and 7.4 require concepts and results from the next section.

## 8. Null designs (trades)

Integer $k$-vectors in the null space of $W_{tk}$ are called *null designs* or *trades*. Integer bases for the modules of null designs have been described by Graver and Jurkat [10], Graham, Li, and Li [9], Frankl, Khosrovshahi and Adjoodani, and others.

Let $\mathcal{M}_t$ be the module of integer row vectors that are orthogonal to the rows of $W_{t-1,t}$. (These are *null $(t-1)$-designs* with block size $t$.) Let $M_t$ be a matrix whose rows

are a $\mathbb{Z}$-basis for $\mathcal{M}_t$. An integer $t$-vector $\mathbf{h}$ is *primitive* when the GCD of the entries of $M_t\mathbf{h}$ is 1. Here $\mathbf{h}$ is being thought of as a column vector.

The elements of all bases are of a certain type that were called $(t,k)$-pods in [10] and cross-polytopes in [9]. For our purposes, we need only to know the generating set for the integer null space of $W_{t,t-1}$, and we restrict our attention to this case, and we use the term $t$-pod.

Let $P$ denote the choice of $t$ disjoint pairs

$$\{a_1,b_1\},\{a_2,b_2\},\ldots,\{a_t,b_t\}, \tag{7}$$

of points. Here the order of the $t$ pairs is not important, but the order of the two points in each pair affects the sign in 8 below. Let $\mathbf{f}_P$ denlote the $t$-vector where $\mathbf{f}_P(T)=0$ unless $T$ contains exactly one point of each pair $\{a_i,b_i\}$, i.e. $T$ is a "transversal" for the pairs, and otherwise

$$\mathbf{f}_P(T)=(-1)^{|T\cap\{b_1,b_2,\ldots,b_n\}|}.$$

It is easy to see that $\mathbf{f}_P$ is orthogonal (with repect to the standard inner product) to all rows of $W_{t-1,t}$.

**Theorem 8.1** *Every integer $t$-vector in the null space of $W_{t-1,t}$ based on a $v$-set, $v\geq t$, is an integer linear combination of $t$-pods.*

**Theorem 8.2** *Let $\mathbf{h}$ be a primitive $t$-vector. Then $N_t\mathbf{x}=\mathbf{b}$ has an integral solution $\mathbf{x}$ if and only if $N'\mathbf{x}'=\mathbf{b}'$ has an integral solution $\mathbf{x}'$, where $N'=W_{t-1,t}N_t$ and $\mathbf{b}'=W_{t-1,t}\mathbf{b}$.*

## 9. A zero-sum Ramsey-type problem

Given $t$ and $k$ with $0\leq t\leq k$ and a prime $p$ so that $\binom{k}{t}\equiv 0 \pmod p$, let $R(t,k;p)$ denote the least integer $n\geq k$ so that if the $t$-subsets of any $n$-set $X$ are colored with the elements of $F_p$, there is always some $k$-subset $A$ of $X$ such that the *sum* of the colors of all $\binom{k}{t}$ of the $t$-subsets of $A$ is 0 in $F_p$.

Equivalently, $R(t,k;p)$ is the least integer $v\geq k$ so that no vector in the $p$-ary code generated by the rows of $W_{tk}$ is all-nonzero, i.e. there are no codewords of weight $\binom{v}{k}$. In particular, $R(t,k;2)$ is the least integer $v\geq k$ so that $(1,1,\ldots,1)$ is not in the binary code generated by the rows of $W_{tk}^v$.

If $H$ is any $t$-uniform hypergraph and $p$ a prime that divides the number of edges of $H$, we let $R(H;p)$ denote the least integer $n$ so that for any coloring of the edges of the $t$-uniform complete hypergraph $K_t^n$ with $F_p$, there exists a subhypergraph $H'$ of $K_t^n$ that is isomorphic to $H$ and such that the sum of the colors on the edges of $H'$ is 0 in $F_p$. So $R(t,k,p)=R(K_t^k;p)$.

It is known that $R(G;2)\leq k+2$ for any graph $G$ with an even number of edges on $k$ vertices [1], and that $R(t,k,2)\leq k+t$ whenever $\binom{k}{t}$ is even [4]. We following two theorems are proved in [27].

**Theorem 9.1** *For any $t$-uniform hypergraph $H$ on $k$ vertices with an even number of edges,*

$$R(H;2) \le k + t.$$

**Theorem 9.2** *When $\binom{k}{t}$ is even, $R(t,k;2)$ is equal to $k + 2^e$ where $2^e$ is the least power of $2$ that appears in the base $2$ representation of $t$ but not in the base $2$ representation of $k$.*

(That $\binom{k}{t}$ is even implies that there are such powers of 2.) In particular, we have $R(t,k;2) = k + t$ when $t$ is a power of 2, and $R(t,k;2) < k + t$ otherwise.

## 10. Diagonal forms for the matrices of 2-subsets versus subgraphs isomorphic to a graph $G$

The results described in this section are joint work with Tony W. H. Wong.

**Theorem 10.1** *A simple graph $G$ is primitive unless $G$ is isomorphic to a complete graph, an edgeless graph, a complete bipartite graph, or the disjoint union of two complete graphs.*

**Theorem 10.2** *Let $G$ be a primitive simple graph with $m$ edges and degrees $\delta_1, \delta_2, \ldots, \delta_n$. Let $h$ denote the gcd of the degrees $\delta_i$ and $m$; let $g$ denote the gcd of all differences $\delta_i - \delta_j$, $i, j = 1, 2, \ldots, n$. Then the invariant factors of $N_2(G, n)$ are*

$$(1)^{\binom{n}{2}-n}, \quad (h)^1, \quad (g)^{n-2}, \quad (mg/h)^1.$$

The nonprimitive graphs may be considered separately. Here is one case.

**Theorem 10.3** *Let $G$ be the complete bipartite graph $K_{r,n-r}$, where $2 \le r \le n-2$. Define $m$, $g$, and $h$ as in the statement of Theorem 10.2, so in this case*

$$m = r(n-r), \quad g = n - 2r, \quad h = \mathit{gcd}\{r, n-r\}.$$

*Then the diagonal entries of one diagonal form for $N_2(G, n)$ are*

$$(1)^{n-2}, \quad (2)^{\binom{n}{2}-2n+2}, \quad (h)^1, \quad (2g)^{n-2}, \quad (mg/h)^1.$$

In the case $r = 2$, the matrix $N_2$ is square; it is the adjacency matrix of the line graph of the complete graph $K_n$. Theorem 10.3 is a generalization of result in [3].

## References


[1] [AlonCaro, 1993] N. Alon and Y. Caro, On three zero-sum Ramsey-type problems, *J. Graph Th.* **17** (1993), 177–192.

[2] A. Blokhuis, A.; A. R. Calderbank, Quasi-symmetric designs and the Smith normal form. Des. Codes Cryptogr. **2** (1992), 189–206.

[3] A. E. Brouwer and C. A. van Eijl, On the $p$-rank of the adjacency matrices of strongly regular graphs, *J. Alg. Combinatorics* **1** (1992), 329–346.

[4] [Caro, 1994] Y. Caro, A complete characterization of the zero-sum (mod 2) Ramsey Numbers, *J. Combinat. Thy. Ser. A* **68** (1994), 205–211.

[5] Y. Caro, Binomial coefficients and zero-sum Ramsey numbers, *J. Combinatorial Th., Series A* **80** (1997), 367–373.

[6] Z. Deretsky, On the symmetry of the Smith normal form for $(v,\ k,\ \lambda)$ designs. Linear and Multilinear Algebra **14** (1983), no. 2, 187–193.

[7] Anna Draganova, Yukiyasu Mutoh, Richard M. Wilson, More on decompositions of edge-colored complete graphs, Discrete Mathematics **308** (2008), 2926–2943

[8] P. Frankl, Intersection theorems and mod $p$ rank of inclusion matrices, *J. Combinatorial Theory, Ser. A* **54** (1990), 85–94.

[9] R. L. Graham, S.-Y. R. Li, and W.-C. W. Li, On the structure of $t$-designs, *SIAM J. Alg. Disc. Meth.* **1** (1980), 8–14.

[10] J. E. Graver and W. B. Jurkat, The module structure of integral designs. *J. Combinatorial Theory* **15** (1973), 75–90.

[11] GḂ. Khosrovshahi; B. Tayfeh-Rezaie, Trades and $t$-designs. Surveys in combinatorics 2009, 91–111, London Math. Soc. Lecture Note Ser. **365**, Cambridge Univ. Press, Cambridge, 2009.

[12] C. W. H. Lam, The search for a finite projective plane of order 10. Amer. Math. Monthly **98** (1991), 305–318.

[13] Esther Lamken and Richard M. Wilson, Decompositions of edge-colored complete graphs. ıJ. Combin. Theory Ser. A **89** (2000), no. 2, 149–200.

[14] Eric S. Lander, Symmetric designs: an algebraic approach. London Mathematical Society Lecture Note Series **74**. Cambridge University Press, Cambridge, 1983. xii+306 pp.

[15] J. H. van Lint and R. M. Wilson, A course in combinatorics. Second edition. Cambridge University Press, Cambridge, 2001. xiv+602 pp. ISBN: 0-521-00601-5.

[16] Morris Newman, Invariant factors of combinatorial designs

[17] Morris Newman, Integer Matrices, Academic Press, New york, 1972.

[18] Morris Newman, The Smith normal form. Proceedings of the Fifth Conference of the International Linear Algebra Society (Atlanta, GA, 1995). Linear Algebra Appl. **254** (1997), 367–381.

[19] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley, 1986.

[20] Tonchev, Vladimir D., Quasisymmetric designs and self-dual codes. European J. Combin. **7** (1986), 67–73.

[21] R. M. Wilson, The necessary conditions for $t$-designs are sufficient for something, *Utilitas Mathematics* **4** (1973), 207–217.

[22] R. M. Wilson, Decompositions of complete graphs into subgraphs isomorphic to a given graph, in: *Proc. Fifth British Combinatorial Conference* (C. St. J. A. Nash-Williams and J. Sheehan, eds.), *Congressus Numerantium* **XV**, Utilitas Mathematica Publ. (1975), 647–659.

[23] R. M. Wilson, A diagonal form for the incidence matrices of t-subsets vs. k-subsets, *Europ. J. Combinatorics* **11** (1990), 609–615.

[24] Richard M. Wilson, On set systems with restricted intersections modulo $p$ and $p$-ary $t$-designs. Discrete Math. **309** (2009), 606–612.

[25] Richard M. Wilson, Signed hypergraph designs and diagonal forms for some incidence matrices. Des. Codes Cryptogr. **17** (1999) 289–297.

[26] Richard M. Wilson, Incidence matrices of $t$-designs. Linear Algebra Appl. **46** (1982), 73–82.

[27] Richard M. Wilson, Some applications of incidence matrices of $t$-subsets and hypergraphs, Proceedings of the Third Shanghai Conference on Combinatorics, *Discrete Math.*, to appear.

[28] Richard M. Wilson and Tony W. H. Wong, , to appear.