Codes and modules associated with designs and t-uniform hypergraphs

Richard M. Wilson

California Institute of Technology

(1) Smith and diagonal form

(2) Solutions of linear equations in integers

(3) Square incidence matrices

(4) A chain of codes

(5) Self-dual codes; Witt's theorem

(6) Symmetric and quasi-symmetric designs

(7) The matrices of t-subsets versus k-subsets, or t-uniform hypergaphs

(8) Null designs (trades)

(9) A diagonal form for N_t

(10) A zero-sum Ramsey-type problem

(11) Diagonal forms for matrices arising from simple graphs

1. 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 $i = j$; but D is not necessarily square. We call any matrix D that arises in this way a *diagonal form* for A.

As a simple example,

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

The matrix on the right is a diagonal form for the middle matrix on the left.

Let the diagonal entries of D be $d_1, d_2, d_3, \ldots$.

$$\begin{pmatrix} 2 & 0 & 0 & \cdots \\ 0 & 24 & 0 & \cdots \\ 0 & 0 & 120 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

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 we have defined them, the number of invariant factors of a matrix (or the number of diagonal entries of a diagonal form) is equal to the minimum of the number of rows and the number of columns. But here and in the sequel, d_i may be interpreted as 0 if the index i exceeds the number of rows or columns. It is clear that the invariant factors (or diagonal entries) of A and $A^\top$ are the same apart from trailing zeros 0.

Some examples follow.

$$\begin{pmatrix} 3 & 1 & 4 \\ 4 & -2 & 7 \end{pmatrix} \to \begin{pmatrix} 3 & 1 & 4 \\ 1 & -3 & 3 \end{pmatrix} \to \begin{pmatrix} 3 & 1 & 1 \\ 1 & -3 & 2 \end{pmatrix}$$

$$\to \begin{pmatrix} 3 & 0 & 1 \\ 1 & -5 & 2 \end{pmatrix} \to \begin{pmatrix} 0 & 0 & 1 \\ -5 & 5 & 2 \end{pmatrix} \to \begin{pmatrix} 0 & 0 & 1 \\ 0 & 5 & 2 \end{pmatrix}$$

$$\to \begin{pmatrix} 0 & 0 & 1 \\ 0 & 5 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix}$$

$$\begin{pmatrix}
2 & 85 & 36 & 24 & 96 & 60 & 54 & 70 & 95 & 80 \\
50 & 46 & 82 & 88 & 94 & 25 & 2 & 1 & 21 & 40 \\
85 & 86 & 52 & 4 & 24 & 45 & 57 & 94 & 38 & 58 \\
95 & 89 & 31 & 49 & 23 & 1 & 74 & 21 & 69 & 81 \\
18 & 57 & 28 & 27 & 39 & 21 & 70 & 45 & 38 & 89 \\
22 & 97 & 86 & 90 & 78 & 97 & 42 & 74 & 69 & 30 \\
53 & 63 & 63 & 31 & 23 & 88 & 38 & 56 & 61 & 28 \\
98 & 61 & 95 & 16 & 23 & 68 & 32 & 6 & 78 & 17 \\
47 & 81 & 42 & 41 & 59 & 68 & 18 & 16 & 37 & 73 \\
65 & 87 & 1 & 3 & 85 & 35 & 55 & 52 & 76 & 94
\end{pmatrix}$$

The invariant factors of this 10 by 10 matrix are

$$1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 12822667799386148 37.$$

$$\begin{pmatrix}
52 & 7 & 85 & 52 & 79 & 20 & 69 & 34 & 55 & 1 & 19 \\
57 & 40 & 62 & 92 & 41 & 45 & 64 & 6 & 5 & 9 & 33 \\
15 & 90 & 81 & 96 & 77 & 97 & 64 & 30 & 42 & 8 & 92 \\
81 & 95 & 88 & 21 & 6 & 91 & 29 & 8 & 24 & 93 & 35 \\
36 & 32 & 52 & 64 & 74 & 97 & 49 & 41 & 44 & 28 & 0 \\
29 & 75 & 42 & 76 & 98 & 90 & 37 & 1 & 88 & 8 & 63 \\
88 & 44 & 88 & 92 & 44 & 74 & 12 & 26 & 2 & 67 & 78 \\
74 & 30 & 26 & 53 & 15 & 37 & 62 & 7 & 56 & 31 & 88 \\
52 & 61 & 21 & 48 & 90 & 94 & 60 & 78 & 72 & 56 & 81 \\
90 & 55 & 90 & 4 & 67 & 41 & 63 & 33 & 46 & 20 & 87
\end{pmatrix}$$

The invariant factors of this 10 by 11 matrix are

$$1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 2.$$

The phenomena observed above are explained by the fact that if $s_1, s_2, \ldots, s_n$ are the invariant factors of a matrix A, then *the product $\sigma_k = s_1 s_2 \ldots s_k$ is the* gcd *of the determinants of all k by k submatrices of A*. (These numbers σ_k are called the *determinantal divisors* of A.) E.g. for a 10 by 10 "random" matrix, $s_1 s_2 \cdots s_9$ is the gcd of the 100 determinants of the 9 by 9 submatrices, and this is "probably" 1. The product $s_1 s_2 \cdots s_{10}$ is, up to sign, the determinant of A, which is more-or-less large on the average.

Invariant factors of the incidence matrices of some finite projective planes:

$PG_2(8)$	$1^{28}, 2^9, 4^9, 8^{26}, 72^1$
$PG_2(9)$	$1^{37}, 3^{18}, 9^{35}, 90^1$
Hall(9)	$1^{41}, 3^{10}, 9^{39}, 90^1$
dual Hall(9)	$1^{41}, 3^{10}, 9^{39}, 90^1$
Hughes(9)	$1^{41}, 3^{10}, 9^{39}, 90^1$
order 10^*	$1^{56}, 10^{54}, 110^1$

bordered $PG_2(8)$	$1^{28}, 2^9, 4^9, 8^{28}$
bordered $PG_2(9)$	$1^{37}, 3^{18}, 9^{37}$
bordered Hall(9)/dual	$1^{41}, 3^{10}, 9^{41}$
bordered Hughes(9)	$1^{41}, 3^{10}, 9^{41}$
bordered order 10^*	$1^{56}, 10^{56}$

Here is the $\binom{6}{2}$ by $\binom{6}{3}$ inclusion matrix of the 2-subsets versus the 3-subsets of a 6-set. The diagonal entries of one diagonal form are

$$1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 2,\ 2,\ 2,\ 2,\ 2,\ 3$$

$$\begin{pmatrix}
1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}$$

The invariant factors of the traingular graph $T(n)$ (the line graph $L(K_n)$ of the complete graph) are [see Brouwer and Van Eijl]:

$$\begin{array}{ll} (1)^{n-2},\ 2^{(n-2)(n-3)/2},\ (2n-8)^{n-2},\ (n-2)(n-4) & \text{if } n \geq 4 \text{ is even,} \\ (1)^{n-1},\ 2^{(n-1)(n-4)/2},\ (2n-8)^{n-2},\ 2(n-2)(n-4) & \text{if } n \geq 5 \text{ is odd.} \end{array} \tag{1}$$

$T(n)$ is strongly regular and determined up to isomorphism by its parameters *except* when $t = 8$, in which case there are three other SRGs (called the Chang graphs) with the same parameters. The invariant factors of the Chang graphs are $1^8,\ 2^{12},\ 8^7,\ 24^1$.

In these notes, module will always mean $\mathbb{Z}$-module, i.e. a module over the ring $\mathbb{Z}$ of integers. These may also be called lattices.

Let A be an r by m integer matrix. We use $\text{row}_{\mathbb{Z}}(A)$ to denote the module generated by the rows of A, a submodule of $\mathbb{Z}^m$; similarly, $\text{col}_{\mathbb{Z}}(A)$ will denote the module generated by the columns of A, a submodule of $\mathbb{Z}^r$.

Suppose $D = EAF$ is a diagonal form for A, where E and F are unimodular. Then A has the same row-module as DF^{-1}; that is, a $\mathbb{Z}$-spanning set for $\text{row}_{\mathbb{Z}}(A)$ consists of the vectors

$$d_1\mathbf{f}_1,\ d_2\mathbf{f}_2,\ \ldots,\ d_m\mathbf{f}_m \tag{2}$$

where $\mathbf{f}_i$ is the i-th row of F^{-1}. The vectors $\mathbf{f}_1, \ldots, \mathbf{f}_m$ form a $\mathbb{Z}$-basis for $\mathbb{Z}^m$; the $\mathbf{f}_i$'s for which $d_i \neq 0$ form a $\mathbb{Z}$-basis for the integer vectors in the row space of A. A $\mathbb{Z}$-basis for $\text{row}_{\mathbb{Z}}(A)$ consists of those vectors $d_i\mathbf{f}_i$ where $d_i \neq 0$.

Proposition 1 *If* $\mathbf{v}$ *is an integer vector and* g *is the* lcm *of the nonzero* d_i*'s, then* $g\mathbf{v} \in \text{row}_{\mathbb{Z}}(A)$*. If* $\mathbf{v}$ *is an integer vector in the row space of* A*, and* g' *is the* lcm *of the nonzero* d_i*'s, then* $g\mathbf{v} \in \text{row}_{\mathbb{Z}}(A)$*.*

Example:

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

A $\mathbb{Z}$-basis for $\mathrm{row}_{\mathbb{Z}}(A)$ consists of the first two rows of DF^{-1}, and these are $(3, 1, 4)$ and $5(2, 0, 3)$.

The p-rank of A (the rank of A over the field $\mathbb{F}_p$) is 2 except that the 5-rank is only 1.

The map

$$a_1\mathbf{f}_1 + \cdots + a_m\mathbf{f}_m \mapsto (a_1 (\text{mod } d_1), \ldots, a_m (\text{mod } d_m))$$

is a homomorphism with kernel $\text{row}_{\mathbb{Z}}(A)$, so

$$\mathbb{Z}^m / \text{row}_{\mathbb{Z}}(A) \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r}. \tag{3}$$

Here $\mathbb{Z}_0 = \mathbb{Z}$.

Let $s_1, s_2, \ldots, s_n$ be the invariant factors of a square integer matrix A. Note that if A is nonsingular, then s_n is the least value of t so that tA^{-1} is integral. One way to see this is to use the formula

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

where A^{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 $\det(A) = s_1 \cdots s_n$.

Another way to understand is to use the fact that that s_n is the lcm of the invariant factors and Proposition 1. The relation $AB = I$ means that each column of I is a rational linear com-

bination of the columns of A, so that the columns of $s_n I$ are integer linear combinations of the columns of A.

2. 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

$$\mathbf{e}_i\mathbf{b} \equiv 0 \pmod{d_i} \quad \text{for } i = 1, 2, \ldots, r. \tag{4}$$

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

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

has an integer solution if and only if $a \equiv 0 \pmod{1}$ (that is, a is an integer) and $2a + b \equiv 0 \pmod{5}$.

We will have use for the following lemma.

Lemma 2 *Given a rational matrix A and a column vector* $\mathbf{b}$*, the system* $A\mathbf{x} = \mathbf{b}$ *has an integer solution* $\mathbf{x}$ *if and only if for any rational row vector* $\mathbf{y}$*,*

$$\mathbf{y}A \text{ integral} \quad \text{implies} \quad \mathbf{y}\mathbf{b} \text{ is an integer.} \tag{5}$$

Proof. The 'if' direction is easy: If $A\mathbf{x} = \mathbf{b}$ with $\mathbf{x}$ integral and $\mathbf{y}A$ is integral, then

$$\mathbf{y}\mathbf{b} = \mathbf{y}(A\mathbf{x}) = (\mathbf{y}A)\mathbf{x} \quad \text{is an integer.}$$

If $A\mathbf{x} = \mathbf{b}$ has no solutions, then there is a row vector $\mathbf{e}_i$ and integer d_i, as in (4) above, so that $\mathbf{e}_i\mathbf{b} \not\equiv 0 \pmod{d_i}$. For sim-

plicity, assume all d_i are nonzero, and let $\mathbf{y} = \frac{1}{d_i}\mathbf{e}_i$; then $\mathbf{yb}$ is not an integer. We have

$$\mathbf{y}A = (0\ldots,0,\frac{1}{d_i},0,\ldots,0)EA = (0\ldots,0,\frac{1}{d_i},0,\ldots,0)DF^{-1},$$

which is the i-th row of F^{-1} and so is an integer vector. $\square$

Suppose $EA = DU$ for any E with rows $\mathbf{e}_i$, square or not, and where D is diagonal with diagonal entries d_i, and U is integral. Then the conditions $\mathbf{e}_i\mathbf{b} \equiv 0 \pmod{d_i}$ are clearly necessary for the existence of an integer solution $\mathbf{x}$ of $A\mathbf{x} = \mathbf{b}$.

Theorem 3 *Let A be an r by m matrix. Suppose $EA = DU$ where E, D, and U are integer matrices with E unimodular and D diagonal. If the conditions $\mathbf{e}_i\mathbf{b} \equiv 0 \pmod{d_i}$ are sufficient for the existence of an integer solution $\mathbf{x}$ of $A\mathbf{x} = \mathbf{b}$, then D, with extra columns of 0's if necessary to make it r by m, is a diagonal form for A.*

3. Square incidence matrices

The following two theorems are from Newman.

Theorem 4 *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 $EAF = D$ for some unimodular matrices E and F, where $D = \mathrm{diag}(s_1, s_2, \ldots, s_n)$ is the Smith form, of A, with diagonal entries

$$s_1 \mid s_2 \mid \cdots \mid s_n. \tag{6}$$

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

$$\frac{c}{s_n} \mid \frac{c}{s_{n-1}} \mid \cdots \mid \frac{c}{s_2} \mid \frac{c}{s_1}. \tag{7}$$

If $AA^\top = mI$, then $A^\top = mA^{-1}$ is integral and the invariant factors of $A^\top$ are those in (7) 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 (6) are, by the uniquess of the Smith form, identical to those in (7), with c replaced by m, and the result follows. $\square$

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 5 *If H is a Hadamard matrix of order $n = 4t$ with t 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, the invariant factors s_i of H satisfy $s_i s_{n+1-i} = n = 4t$. Since the entries of H are ± 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 6 *If C is a conference matrix of order $n = 2t$ with $n-1$ squarefree, then the invariant factors of C are*

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

An extension of Theorem 4 is given below. We will give the proof at the end of the next section.

Theorem 7 *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 $\det(U) = \pm\det(V)$ 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 2-(v, k, λ)-*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 λ of the blocks. We usualy assume $2 \leq k \leq v - 2$. For background on designs, and proofs of the observations of the next two paragraphs, see Chapter 19.

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

$$NN^{\top} = (r - \lambda)I + \lambda J \tag{8}$$

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; J the matrix of all 1's.

For later reference, we note that

$$((r-\lambda)I + \lambda J)^{-1} = \frac{1}{r-\lambda}(I - \frac{\lambda}{rk}J). \tag{9}$$

Also $JN = kJ$.

When $|X| = |\mathcal{B}|$, i.e. $v = b$, the design is said to be a (v, k, λ)-*symmetric design*. Here the incidence matrix N is square of order v. We have $r = k$ and the relation $\lambda(v-1) = k(k-1)$. Then $NN^\top = nI + \lambda J$ where $n = k - \lambda$. A *projective plane* of order n is a $(n^2+n+1, n+1, 1)$-symmetric design.

Two square symmetric matrices B and C are said to be *rationally congruent* when there exists a nonsingular matrix A so that $ABA^\top = C$. The Hasse-Minkowski Theorem gives necessary and sufficient conditions for two rational B and C to be rationally congruent. If there exists a (v, k, λ)-symmetric design, then the equation $NN^\top = nI + \lambda J$ means that the v by v matrices I and $nI + \lambda J$ are rationally congruent. The following classic theorem may be derived from the Hasse-Minkowski Theorem, though

more elementary proofs are known.

Theorem 8 (Bruck-Ryser-Chowla) *If there exists a (v, k, λ)-symmetric design with v odd, then the equation*

$$x^2 = ny^2 + (-1)^{(v-1)/2}\lambda z^2$$

has a solution in integers x, y, z, not all zero.

We can say a few simple things about the invariant factors $s_1, s_2, \ldots, s_v$ of the incidence matrix N of a symmetric design in general. The equation (8) implies $\det(N) = \pm n^{(v-1)/2}k$, so $s_1 s_2 \cdots s_v = n^{(v-1)/2}k$. We have

$$N^{-1} = N^\top((nI + \lambda J)^{-1} = \frac{1}{n}N^\top - \frac{\lambda}{nk}J.$$

The smallest integer t such that tN^{-1} is integral is $s_v = nk/(k, \lambda)$. It is easy to see that there are 2 by 2 submatrices of N equivalent to $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, and this implies $s_1 = s_2 = 1$.

Theorem 9 (Deretzky) *Let N be the incidence matrix of a (v, k, λ)-symmetric design where k and λ are relatively prime, and write $n = k - \lambda$. The invariant factors of N satisfy*

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

Proof. Let N be the incidence matrix of a (v, k, λ)-symmetric design. We have already seen that $s_v = nk$ and $s_1 s_2 \cdots s_v = \det(N) = \pm k n^{(v-1)/2}$. The product of the other invariant factors is a power of n and all divide nk; thus when $(n, k) = 1$, every other invariant factor divides n.

Now consider the matrix

$$A = \left[\begin{array}{ccc|c} & N & & \begin{matrix}1\\ \vdots \\ 1\end{matrix} \\ \hline \lambda & \cdots & \lambda & k \end{array}\right] \tag{10}$$

of order $v+1$. Let $D = \mathrm{diag}(1,1,\ldots,1,-\lambda)$, of order $v+1$. It may be checked that $ADA^\top = nD$. If $(k,\lambda) = 1$, then $(n,\lambda) = 1$, and by Theorem 7, $t_i t_{v+2-i} = n$.

We now relate the invariant factors $s_1, s_2, \ldots, s_v$ of N to those of A. The column module of N contains a constant column, say $c\mathbb{1}$, if any only if c is a multiple of k. This is because the columns of N are linearly independent and sum to the vector of all k's.

So the column module of

$$[N, \mathbb{1}] = \left[\begin{array}{c|c} N & \begin{matrix}1\\ \vdots \\ 1\end{matrix} \end{array}\right]$$

contains the column module of N as an index k submodule. This means the invariant factors of $[N, \mathbb{1}]$ are $s_1, s_2, \ldots, s_{v-1}, n$ (easy details omitted).

If the sum of all rows of $[N, \mathbb{1}]$ is subtracted from the bottom row of A, we obtain a matrix A', with the same invariant factors $t_1, \ldots, t_{v+1}$ as A, and whose last row is $-(n, n, \ldots, n, v-k)$. In general we have $\lambda(v-k) = n(k-1)$, so the assumption that $(k, \lambda) = 1$ implies $v - k \equiv 0 \pmod{n}$ and thus the entire last row

of A' is divisible by n.

Using integer row operations in the first v rows of A' and columns operations, we may reduce A' to

$$A'' = \begin{pmatrix} s_1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & s_2 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & & \ddots & \cdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & s_{v-1} & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & n & 0 \\ \bullet & \bullet & \bullet & \cdots & \bullet & \bullet & \bullet \end{pmatrix}.$$

Since $s_1, \ldots, s_{n-1}, n$ divide n and the last row of A'' is divisible by n, subtracting intgeral multiple of the first v rows from the last

gives

$$A''' = \begin{pmatrix} s_1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & s_2 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & & \ddots & \cdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & s_{v-1} & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & n & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \bullet \end{pmatrix}.$$

Since the product $t_1 t_2 \cdots t_{v+1}$ is $n^{(v+1)/2}$ and the product $s_1 \cdots s_{v-1} n$ is $n^{(v-1)/2}$, the lower left entry must be $\pm n$. $\square$

4. A chain of codes

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 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 or 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.

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

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

We have $\mathcal{M}_0(A) = \mathrm{row}_{\mathbb{Z}}(A)$ 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 10 *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}.*

Proof. With the notation of (2), a $\mathbb{Z}$-basis for $\mathrm{row}_{\mathbb{Z}}(A)$ is provided by the nonzero members of

$$d_1\mathbf{f}_1,\ d_2\mathbf{f}_2,\ \ldots\ , d_m\mathbf{f}_m$$

where $\mathbf{f}_1, \mathbf{f}_2, \ldots, \mathbf{f}_m$ are the rows of a unimodular matrix—and so are linearly independent modulo p. An integer vector $a_1\mathbf{f}_1 + \cdots + a_m\mathbf{f}_m$ is in $\mathcal{M}(A)$ if and only if $a_i \equiv 0 \pmod{d_i}$ for every i, so $p^j(c_1\mathbf{f}_1 + \cdots + c_m\mathbf{f}_m) \in \mathcal{M}(A)$ if and only if $p^j c_i \equiv 0 \pmod{d_i}$. If p^{j+1} divides d_i, then this congruence implies $c_i \equiv 0 \pmod{p}$; but if the p-contribution to d_i is at most p^j, then there values

of $c_i \not\equiv 0 \pmod{p}$ for which $p^j c_i \equiv 0 \pmod{d_i}$, so $\mathbf{f}_i$, when read modulo p is in $C_j(A)$. It is now clear that the set of $\mathbf{f}_i$ so that p^{j+1} does not divide d_i is a basis for $C_j(A)$. $\square$

Lemma 11 *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.*

Proof. We will show $C_i(LM) = C_i(M)$ for all i.

Let $d = \det(L)$ and let $\mathbf{d}'$ be a multiple of d so that $d' \equiv 1 \pmod{p}$. First, since the rows of LM are integer linear combinations of the rows of M, it is clear that $\mathbf{a} \in \mathcal{M}_i(LM)$ implies

$\mathbf{a} \in \mathcal{M}_i(M)$ and so $C_i(LM) \subseteq C_i(M)$. Suppose $\mathbf{a} \in \mathcal{M}_i(M)$; say $p^i(\mathbf{a}) = \mathbf{c}M$ where $\mathbf{c}$ is an integer vector. Then $p^i(d'\mathbf{a}) = \mathbf{c}(d'L^{-1}))(LM)$, and $\mathbf{c}(d'L^{-1})$ is an integer vector, so $p^i d'\mathbf{a} \in \mathcal{M}_i(LM)$. But $d'\mathbf{a} \equiv \mathbf{a} \pmod{p}$. □

Theorem 12 *Let p be a prime and A an n by n integer matrix. If U and V are square integer matrices with determinants not divisible p, and $AUA^\top = p^e V$, then the invariant factors $s_1, s_2, \ldots, s_n$ of A are such that the p-contribution to $s_i s_{n+1-i}$ is p^e, for all $i = 1, 2, \ldots, n$.*

Proof. As in the proof of Theorem 4, the invariant factors of

$p^e \det(V) A^{-1} = UA^\top(\det(V)V^{-1})$ are

$$p^e \det(V)/s_n, p^e \det(V)/s_{n-1}, \ldots, p^e \det(V)/s_1$$

in that order. By Lemma 11, the invariant p-factors of $UA^\top(\det(V)V^{-1})$ are the same as those of $A^\top$, which are the p-contributions to $s_1, s_2, \ldots, s_n$ in that order. The result follows. □

Theorem 7 is a corollary. If $AUA^\top = mV$ and the determinants of U and V are equal apart for sign, and relatively prime to m, the p-contribution to $s_i s_{n+1-i}$ is p^e whenever $p^e || m$, and it follows that m divides $s_i s_{n+1-i}$. But the product $s_1 \cdots s_n$ is equal to the determinant of A, which is $m^{n/2}$.

5. Self-dual codes; Witt's theorem

A p-ary linear 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 $n/2$.

Theorem 13 *If there exists a self-dual p-ary code of length n, where p is an odd prime, then $(-1)^{n/2}$ is a square in $\mathbb{F}_p$.*

Proof. Let C be a self-dual p-ary code of length n (and dimension $n/2$). Then $C = \mathrm{row}_p(G)$ for some $n/2$ by n matrix G over $\mathbb{F}_p$ that satisfies $GG^\top = O$. By row operations and permutation of columns if necessary, we may assume

$$G = \boxed{I \mid A}$$

where both I and A are square. The equation $GG^\top = O$ means that $AA^\top = -I$; hence $\det(A)^2 = (-1)^{n/2}$. $\square$

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.

Corollary 14 *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. 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 4 gives us a self-dual code of length $n \equiv 2 \pmod 4$ and Theorem 13 implies that -1 is a square in $\mathbb{F}_p$, which implies $p \equiv 1 \pmod 4$. $\square$

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

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

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-orthogonal. We may call C *self-U-dual* when $C = C^U$.

Theorem 15 (Witt) *Given a symmetric nonsingular matrix U 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 $\mathbb{F}$.*

A proof for a diagonal matrix U may be obtained by a minor modification of that of Theorem 13, and the general case is only a little more work using the fact that U is congruent to a diagonal matrix over $\mathbb{F}$.

Theorem 16 *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*

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

In particular, if $e = 2f + 1$, then C_f is a self-U-dual p-ary code of length n.

Proof. Let $\mathbf{x}$ and $\mathbf{y}$ be integer vectors such that $\mathbf{x} \pmod p \in C_i$ and $\mathbf{y} \pmod p \in C_{e-i-1}$. This means

$$p^i(\mathbf{x} + p\mathbf{a}_1) = \mathbf{z}_1 A \quad \text{and} \quad p^{e-i-1}(\mathbf{y} + p\mathbf{a}_2) = \mathbf{z}_2 A$$

for some integer vectors $\mathbf{z}_1$, $\mathbf{z}_2$, $\mathbf{a}_1$, and $\mathbf{a}_2$. Then

$$p^{e-1}\langle \mathbf{x}, \mathbf{y} \rangle = p^{e-1}\mathbf{x}B\mathbf{y}^\top \equiv \mathbf{z}_1 AUA^\top \mathbf{z}_2^\top \equiv 0 \pmod{p^e}.$$

Thus $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ in $\mathbb{F}_p$ and we see $C_{e-i-1} \subseteq C_i^U$.

Let $s_1, s_2, \ldots, s_n$ be the invariant factors of A. By Theorem 12, the p-contribution to $s_i s_{n+1-i}$ is p^e. If p^{j+1} divides s_i, then p^{e-j} cannot divide s_{n+1-i}; that is, we have a one-to-one correspondence between indices i so that p^{j+1} does not divide s_i and those indices $i' = n+1-i$ so that p^{e-j} does not divide $s_{i'}$. By Theorem 10, the dimensions of $C_i(A)$ and $C_{e+1-i}(A)$ sum to n, and this completes the proof. $\square$

Corollary 17 *If there exists a (v, k, λ)-symmetric design with $(k, \lambda) = 1$, then for every prime divisor p of the squarefree part of n, $(-1)^{(v-1)/2}\lambda$ is a square modulo p.*

Proof. Let A be the $v+1$ by $v+1$ matrix in (). If p^{2f+1} exactly divides n, then $C_e(A)$ is a self-D-dual code of length $v+1$, where $D = \text{diag}(1, 1, \ldots, 1, -\lambda)$. □

The proof of the nonexistence of a projective plane of order 10, a $(111, 11, 1)$-symmetric design, was completed in 1989. Extensive computer calculations were required, but computers could not have handled the problem were it not for coding theory. Analysis of and computations concerning the self-dual code of

length 112 that would arise from the Theorem eventually led to a contradiction. Clement Lam played a pivotal part in this work.

6. Symmetric and quasi-symmetric designs

Theorem 18 (Lander) *Suppose there exists a symmetric* (v, k, λ)*-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*

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

Hence from Witt's Theorem,

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

Proof. Let N be the incidence matrix of a symmetric (v, k, λ)-design and let p be a prime. Assume $\lambda = p^{2a}\lambda_0$ where $(\lambda_0, p) = 1$ and $a \geq 0$; we will explain later what to do when λ is exactly divisible by an odd power of p. Let

$$A := \begin{pmatrix} & & & p^a \\ & N & & \vdots \\ & & & p^a \\ p^a\lambda_0 & \cdots & p^a\lambda_0 & k \end{pmatrix}, \quad U := \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & -\lambda_0 \end{pmatrix}.$$

The reader should verify, using the properties of N and the relation $\lambda(v-1) = k(k-1)$, that $AUA^\top = nU$.

In the case λ is exactly divisible by an even power of p, we apply Theorem 16 with the matrices A and U as above.

If λ is exactly divisible by an odd power of p, we apply the above case to the *complement* of the given symmetric design, which is a symmetric $(v, v-k, \lambda')$-design where $\lambda' = v - 2k + \lambda$. Say $\lambda' = p^c \lambda'_0$ where $(\lambda'_0, p) = 1$. From $\lambda\lambda' = n(n-1)$, it follows that c is odd and that

$$\lambda_0 \lambda'_0 = n_0(n-1) \equiv -n_0 \pmod{p}.$$

We have replaced what would be $-\lambda'_0$ in the conclusion by $\lambda_0 n_0$, which is allowed since they differ by a square factor modulo p, in order to express the result in terms of the original parameters. □

Theorem 19 (Calderbank) *Let $\mathcal{B}$ be a 2-(v,k,λ), 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 lenth $(v+1)/2$ where $U = \mathrm{diag}(1,1,\ldots,1,-v)$.

Theorem 20 (Blokhuis, Calderbank) *Let $\mathcal{B}$ be a 2-(v,k,λ), and p be an odd prime so that p^e exactly divides $r-\lambda$; further suppose that $|A \cap B| \equiv s \pmod{p^e}$ for any two blocks A and B of the design. ...*

The two theorems above produce self-U-dual codes from non-

square matrices. There would appear to be no way to derive them from the Hasse-Minkowski theory.

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

Incidence or inclusion matrices of s-subsets versus blocks arise in the theory of t-designs and in extremal set theory.

Given any family $\mathcal{F}$ of subsets of a set X, define a matrix M_s with rows indexed by the s-subsets of X and columns by $\mathcal{F}$ by

$$M_s(S, A) = \begin{cases} 1 & \text{if } S \subseteq A, \\ 0 & \text{otherwise.} \end{cases}$$

If $(X, \mathcal{F})$ is a t-(v, k, λ) design with $t \geq 2s$, then an equation of the form

$$M_s M_s^\top = \sum_{i=0}^{s} b_{2s-i}^i W_{is}^\top W_{is}$$

holds. I know of no use of self-dual codes to prove non-existence results for t-designs with $t > 2$.

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 $0 \leq t \leq k \leq v$, 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 $W_{tk}\mathbf{x} = \mathbb{1}$ is related to the existence problem for t-designs. A simple t-(v,k,λ) *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 λ 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 $W_{tk}\mathbf{u} = \lambda\mathbb{1}$ where here $\mathbb{1}$ is the t-vector of all 1's. We allow not-necessarily-simple t-(v,k,λ) 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 $W_{tk}\mathbf{u} = \lambda\mathbb{1}$. 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 $W_{tk} = \mathbb{1}$.

We have $W_{it}W_{tk} \equiv O \pmod{\binom{k-i}{t-i}}$ since, in fact,

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

(this is easy) and thus the congruences (11) are necessary conditions for the existence of integer solutions to $W_{tk}\mathbf{u} = \mathbb{1}$. The case $i = t$, where $W_{tt} = I$, simply requires that each entry of $\mathbf{b}$ is an integer.

The following theorem is due to Graver and Jurkat, and rmw. It is also a consequence of Theorem 23.

Theorem 21 *Let $t + k \leq v$. 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*

$$\lambda\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}} \quad \textit{for} \quad i = 0, 1, \ldots, t. \tag{11}$$

Systems of diophantine linear equations have come up repeatedly in work on the asymptotic existence of design-like structures. Theorem 22 is from 1975.

Theorem 22 *Let G be a simple graph on k vertices and assume $n \geq k+2$. 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,*

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

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 22 played an essential role in the proof given in 1975 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 were need for work on decompositions of 'edge-colored complete graphs' (with Lamken, Draganova, Mutoh).

Though it is immaterial for the intended application, I have been curious about the hypothesis $n \geq k + 2$. It turns out that it may be dropped as long as G is not edgeless, complete, complete bipartite, or the union of two disjoint complete graphs. For example, it is possible to assign signed integer multiplicities x_G to all Petersen-subgraphs of K_{10} so that the sum of these multiplicities over those subgraphs on an edge is always 1.

A common generalization and extension of Theorems 21 and 22 is Theorem 23 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 **??**.

Theorem 23 *Let* $\mathbf{h}$ *be a* t*-vector based on a* v*-set* X *and assume that there are at least* t *isolated vertices. Let* g_i *denote the gcd of all entries of* $W_{it}N_t$*. Necessary and sufficient conditions for the existence of an integer solution* $\mathbf{x}$ *to* $N_t\mathbf{x} = \mathbf{b}$ *for a* t*-vector* $\mathbf{b}$ *of height* $\binom{v}{t}$ *are*

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

If $\mathbf{h}$ is the characteristic 2-vector of the edge set of a graph G, then g_0 is the number of edges of G and g_1 is the gcd of the degrees of G. It $\mathbf{b}$ is the vector of all 1's, then $W_{02}\mathbf{b} = \binom{n}{2}$ and $W_{12}\mathbf{b}$ is a vector of $n-1$'s.

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 Graham, Li, and Li, Frankl, Khosrovshahi and Adjoodani, and others.

Let $\mathcal{N}_t$ 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 Z-basis for $\mathcal{N}_t$. An integer t-vector $\mathbf{h}$ based on a v-set X with $v \geq 2t$ 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.

Don't quote me on this, but probably most t-vectors **h** are primitive.

The elements of all bases are of a certain type that were called (t, k)-pods by Graver and Jurkat and cross-polytopes by GLL. For our purposes, we need only to know a generating set for the integer null space of $W_{t-1,t}$, and we restrict our attention to this case. We use the term t-*pod* for what G and J called a $(t-1, t)$-pod.

Let P denote the choice of t disjoint pairs

$$\{a_1, b_1\}, \{a_2, b_2\}, \ldots, \{a_t, b_t\}, \tag{12}$$

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 (13) below. Let $\mathbf{f}_P$ denote 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

$$\mathbf{f}_P(T) = (-1)^{|T \cap \{b_1, b_2, \ldots, b_n\}|}. \tag{13}$$

It is easy to see that $\mathbf{f}_P$ is orthogonal (with repect to the standard inner product) to all rows of $W_{t-1,t}$. If $\mathbf{v}$ is the $(t-1)$-vector cooresponding to row of $W_{t-1,t}$ indexed by a $(t-1)$-subset S, then

$$\langle \mathbf{v}, \mathbf{f}_P \rangle = \sum_T \mathbf{v}(T)\mathbf{f}_P(T) = \sum_{T : S \subseteq T} f_P(T).$$

If S is not transverse to P, then no t-subsets T that contain it are transverse to P and the sum in () is 0. If S is transverse to P, it meets $t-1$ of the pairs, say all but $\{a_{i_0}, b_{i_0}\}$, and then there are two transverse t-subsets that contain S, namely $T_1 = S \cup \{a_{i_0}\}$ and $T_2 = S \cup \{b_{i_0}\}$. One of $\mathbf{f}_P(T_1)$ and $\mathbf{f}_P(T_2)$ is $+1$ and the other is -1, so the sum in () is again 0.

(Note to self: explain what all this means for graphs. Remark that "most" hypergraphs are primitive.))

Theorem 24 *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.*

Proof. We proceed by induction on $v+t$. First we note that the

case $t = 1$ is easy since W_{01} is a row vector of length $\binom{v}{t}$ and the 1-pods are the vectors with one entry $+1$, a second entry -1, and all other entries 0.

When $v < 2t$, there are no null designs other than the 0-vector, and there are no nonzero t-pods. (Details omitted.)

Now fix $t \geq 2$ and $v \geq 2t$ and assume the statement holds when v is replaced by v' and t by t' where $v' + t' < v + t$. (Induction step omitted.)

The following Lemma is essential to our proof of Theorem 23.

Theorem 25 *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 diagonal form for N_t

The necessary and sufficient conditions for the existence of an integer solution of $N_t\mathbf{x} = \mathbf{b}$ (when $\mathbf{h}$ has at least t isolated vertices) are

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

where g_i is the gcd of all entries of $W_{it}N_t$. These conditions are redundant.

Theorem 26 (W., 1999, 2008) (i) *Given* t, k, v, $t \le k \le v - t$, *the matrix*

$$\bigsqcup_{j=0}^{t} E_{jk} =$$

E_{0k}	1 row
E_{1k}	$v - 1$ rows
E_{2k}	$\binom{v}{2} - v$ rows
$\vdots$	
E_{tk}	$\binom{v}{t} - \binom{v}{t-1}$ rows

with $\binom{v}{t}$ *rows has* p*-rank* $\binom{v}{t}$ *for every prime* p. (ii) *The module*

generated by the rows of W_{tk} is equal to that generated by the rows of the following matrix

$$\bigsqcup_{j=0}^{t} \binom{k-j}{t-j} E_{jk} =$$

$\binom{k}{t} E_{0k}$	1 row
$\binom{k-1}{t-1} E_{1k}$	$v-1$ rows
$\binom{k-2}{t-2} E_{2k}$	$\binom{v}{2} - v$ rows
$\vdots$	
$\binom{k-t}{0} E_{tk}$	$\binom{v}{t} - \binom{v}{t-1}$ rows

.

The rows of E below are independent over F_p for all p.

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	0	1	1	0	1	0	1	0	1	0	1	0	1	0	0	1	0	0
1	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1	0	0	1	0
0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	0	0	1
0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1
0	1	0	1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0
0	0	1	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	0
0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	1	0	0
0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1

The rows of DE generate the same module as those of W_{23}^6.

3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
2	2	0	2	2	0	2	0	2	0	2	0	2	0	2	0	0	2	0	0
2	0	2	2	0	2	2	0	0	2	0	2	2	0	0	2	0	0	2	0
0	2	2	2	0	0	0	2	2	2	0	0	0	2	2	2	0	0	0	2
0	0	0	0	2	2	2	2	2	2	0	0	0	0	0	0	2	2	2	2
0	0	0	0	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2
0	1	0	1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0
0	0	1	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	0
0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	1	0	0
0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	1	0
0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1

Theorem 27 *Let h_t be a t-vector with at least t isolated vertices. Let D be the diagonal matrix whose diagonal entries are*

$$(g_0)^1,\ (g_1)^{v-1},\ (g_2)^{\binom{v}{2}-v}\ldots,\ (g_t)^{\binom{v}{t}-\binom{v}{t-1}}.$$

Then $E_t\mathbf{b} \equiv \mathbf{0} \pmod{D}$ are necessary and sufficient conditions for the existence of an integer solution of $N_t\mathbf{x} = \mathbf{b}$. Hence D is a diagonal form for N_t.

10. 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. **Example.** $R(2,5;2) = 7$.

Theorem 28 (Caro, 1996) *When* $\binom{k}{t}$ *is even,* $R(t,k,2) \leq k+t$.

Theorem 29 (W, 2002) *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.

From Theorem 23, for $v \geq k+t$, $\mathbb{1} \in \mathrm{col}_{\mathbb{Z}}(\mathbf{W_{tk}})$ if and only if

$$\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}},$$

for $i = 0, 1, \ldots, t$. It follows that $\mathbb{1} \in \mathrm{col}_{\mathbf{p}}(\mathbf{W_{tk}})$ if and only if

$$\binom{k-i}{t-i} \equiv 0 \pmod{p} \quad \text{implies} \quad \binom{v-i}{t-i} \equiv 0 \pmod{p},$$

for $i = 0, 1, \ldots, t$.

Note that W^v_{tk} can be identified with the transpose of $W^v_{v-k,v-t}$.

Lemma 30 *Let p be a prime, and $t \leq k \leq v$. If $v \leq k+t$, then $\mathbb{1} \in \mathit{row}_{\mathbf{p}}(\mathbf{W^v_{tk}})$ if and only if*

$$\binom{v-t-i}{v-k-i} \equiv 0 \pmod{p} \quad \textit{implies} \quad \binom{v-i}{v-k-i} \equiv 0 \pmod{p},$$

for $i = 0, 1, \ldots, t$.

Lemma 31 *Given integers* k *and* t *and a prime* p*, write*

$$k = a_0 + a_1 p + a_2 p^2 + \cdots + a_\ell p^\ell \quad \textit{and}$$
$$t = b_0 + b_1 p + b_2 p^2 + \cdots + b_\ell p^\ell \tag{14}$$

in their base p *representations, where* $0 \le a_i, b_i < p$ *for* $i = 0, 1, \ldots, \ell$. *Then*

$$\binom{k}{t} \not\equiv 0 \pmod{p} \quad \textit{if and only if} \quad b_i \le a_i \quad \textit{for } i = 0, 1, \ldots, \ell.$$

Theorem 32 (Alon, Caro) *For any graph G with k vertices and an even number of edges,*

$$R(G;2) \leq k+2.$$

Theorem 33 (W) *For any t-uniform hypergraph H on k vertices with an even number of edges,*

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

Proof. We know that

$$E_t N_t = DU$$

where E_t and D are the matrices described in Theorem 27 and the rows of U are linearly independent over all fields. The first

entry of D is g_0, the number of edges of H, and the top row of U is the vector of all ones.

A basis for $\text{row}_p(N_t)$ consists of the rows of U that correspond to diagonal enties of D that are not divisible by p. If p divides g_0, the vector of all ones is not included, and it, of course, is not a linear combination of the other rows of U. That is, $(1, 1, \ldots, 1) \notin \text{row}_p(N_t)$. $\square$

This can be improved to $R(H; 2) \leq k+t-1$ unless H is a complete t-uniform hypergraph. Don't quote me on this, but probably $R(H : 2) = k$ for most t-uniform hypergraphs.

Y. Caro has determined $R(G; 2)$ for all simple graphs G.

Theorem 34 *Let G be a simple graph with k vertices and an even number of edges. Then*

$$R(G;2) = \begin{cases} k & \text{if } G \text{ is complete,} \\ k+1 & \text{if } G \text{ is the union of two complete graphs or a nonc} \\ k+2 & \text{otherwise.} \end{cases}$$

This will be generalized in the next setion.

11. Diagonal forms for N_2 when G is a simple graphs

In this section, we briefly state some recent joint results with Tony W. H. Wong.

Theorem 35 *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 36 *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 δ_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*

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

- N_2 for the Petersen graph (n=10) has diagonal form 1^{35}, 3^1, 0^8, 15^1.

- N_2 for the Petersen graph plus an isolated vertex (n=11) has invariant factors 1^{44}, 3^{10}, 15^1.

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

Theorem 37 *Let* G *be the complete bipartite graph* $K_{r,n-r}$, *where* $2 \leq r \leq n-2$. *Define* m, g, *and* h *as in the statement of*

Theorem 36, so in this case

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

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 as mentioned earlier, and we have reproved the result of Brouwer and Van Eijl.

Theorem 38 *Let G be a simple graph with k vertices and an*

even number of edges. Then

$$R^*(G;p) = \begin{cases} k & \text{if } G \text{ is complete,} \\ k+1 & \text{if } G \text{ is the union of two complete graphs, or is a n} \\ k+2 & \text{otherwise.} \end{cases}$$