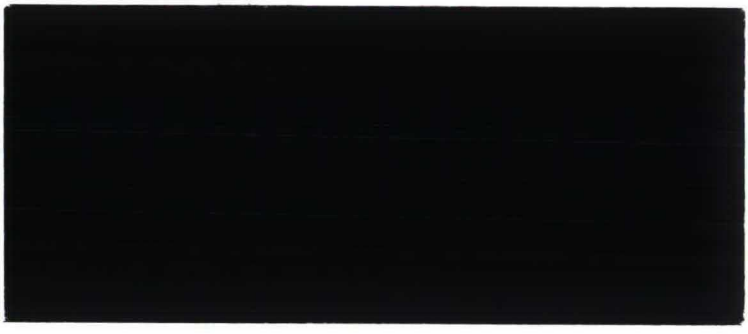

QUADRATIC FORMS IN DESIGN THEORY

M.J. Coster

Research Memorandum FEW 635

Communicated by Dr.ir. W.H. Haemers

Quadratic forms in Design Theory.

M.J. Coster

January 12, 1994

Abstract

This report describes the Grothendieck Group for rational congruence classes of positive definite integral matrices. The main result is an explicite diagonal matrix for each class of this Grothendieck Group. We give some applications in design theory.

Keywords: quadratic forms, designs, positive definite integral matrices, decomposition.

1 Introduction.

Let M be an integral positive definite symmetric matrix. In this paper we consider conditions for which M can be written as $M = AA^{\mathsf{T}}$, where A is an integral square matrix (in this case we say that M is *decomposable*). There is a one-one relation between integral positive definite symmetric matrices and positive definite quadratic forms with integral coefficients. Though the theory can completely be described in terms of quadratic forms, we prefer the use of matrices. The reason to do this is the fact that our applications deal with matrices. The theory on quadratic forms can be found in [1, 3]. In these books the theory is described in its generality. We consider just a special case.

We will denote by $\mathcal{S}$ the set of positive definite integral symmetric matrices. We denote by $\mathcal{G}$ the related Grothendieck group. This group will be defined formally in Section 3. In Section 4 we consider the structure of $\mathcal{G}$. This structure is completely described by Theorem 4.3. As a consequence of this theorem we can write each element g of $\mathcal{G}$ uniquely as a sum of infinitely many generators. We will show as a consequence that $\mathcal{G} \cong C_2 \otimes V_4^{\infty} \otimes C_4^{\infty}$, where V_4 is the 4-group of Klein.

The second part of the paper deals with some decomposition problems which arise in design theory. Usually one solves these problems with the Hasse–Minkowski invariants. We will show that these problems can be solved easily without using the original Hasse Principle. In this paper we will mainly develop tools for design theory. We end with a general application. In Section 6 we will apply our method to the lattice graph. An application to Quasi Symmetric designs is given in [4].

2 Notation.

The following notation will be used frequently in this paper. Most notations will be explained again in the text.

$\left(\frac{\cdot}{\cdot}\right)$ The Legendre symbol.

$n^\star$ The squarefree part of an integer n.

$\mathcal{S}$ is the set of positive definite symmetric integral matrices.

$\mathcal{G}$ is the Grothendieck Group associated to $\mathcal{S}$.

"$\oplus$" is a matrix addition.

"$\ominus$" is a matrix addition.

"$\cong$" is the congruence relation.

$\langle A\rangle$ is the class of the matrix A. (if A is a positive integer then $\langle A\rangle = \langle (A)\rangle$.

$\langle \lambda \cdot p|$ is the class of the matrix $\langle \lambda pq\rangle \oplus \langle \lambda q\rangle \oplus 3\langle \lambda\rangle$, where q is a prime depending on p.

I_n is the $n \times n$-identity matrix.

J_n is the $n \times n$ all one matrix.

$\underline{j}$ is the all 1–vector.

K_n $= I_n + J_n$.

M_n $= (n+1)I_n - J_n$.

3 Basic Theory.

Let $\mathcal{S}$ be the set of positive definite symmetric integral matrices, including the empty set element. We define an addition on $\mathcal{S}$ in the following way. Let A, $B \in \mathcal{S}$ then we define $A \oplus B = \begin{pmatrix} A & \bigcirc \\ \bigcirc & B \end{pmatrix}$. (If A is an $m \times m$-matrix and B is an $n \times n$-matrix then $A \oplus B$ is an $(m+n) \times (m+n)$-matrix, with on the diagonal the original matrices A and B). The set $\mathcal{S}$ with the addition $\oplus$ is a semigroup, (i.e. it satisfies the grouplaws, except of the existence of an inverse), with unity 0, the empty set element. Now we define a relation. Let A and B be two elements of $\mathcal{S}$ of dimensions m and n respectively. We say $A \cong B$ if there exists an integral $k \times k$-matrix Q such that $Q(A \oplus I_{k-m})Q^{\mathsf{T}} = B \oplus I_{k-n}$. The relation $\cong$ is an equivalence relation, called *rational equivalence relation* (see [1, 3]). The result is based on the Witt cancelation. We denote the class of the matrix A by $\langle A\rangle$. It is well-known that each equivalence class contains a diagonal matrix (i.e. a matrix with zeroes outside the diagonal), see [1]. We denote the 1×1-matrix equivalence class $\langle (a)\rangle$ simply by $\langle a\rangle$. Each class $\langle A\rangle$ can be written as $\langle A\rangle = \bigoplus_i \langle a_i\rangle$ for some positive integers a_i. Notice that $\langle I_n\rangle = \langle 1\rangle = \langle \emptyset\rangle = 0$. The following Lemma can also be found in [1].

Lemma 3.1 *Let $a, b \in \mathbb{Z}_{>0}$. Then we have*

(1) $\langle ab^2\rangle = \langle a\rangle$,

(2) $\langle a\rangle \oplus \langle b\rangle = \langle a+b\rangle \oplus \langle ab(a+b)\rangle$.

Hence the set $\mathcal{S}$ with the operation $\oplus$ and equivalence under $\cong$ is a semigroup. We denote this semigroup by $\mathcal{G}$ (hence $\mathcal{G} = (\mathcal{S}/\cong, \oplus)$). This is the *Grothendieck group*. The following lemma shows that $\mathcal{G}$ is indeed a group.

Corollary 3.2 *Let $a, b, c, n \in \mathbb{Z}_{>0}$. Then we have*

(1) $2\langle c(a^2+b^2)\rangle = 2\langle c\rangle$,

(2) $4\langle n\rangle = 0$.

Proof.

(1) $2\langle c\rangle = \langle a^2c\rangle \oplus \langle b^2c\rangle = \langle c(a^2+b^2)\rangle \oplus \langle a^2b^2c(a^2+b^2)\rangle$,

(2) $0 = 2\langle a^2+b^2\rangle \oplus 2\langle c^2+d^2\rangle =$
$2\langle a^2+b^2+c^2+d^2\rangle \oplus 2\langle (a^2+b^2)(c^2+d^2)(a^2+b^2+c^2+d^2)\rangle =$
$4\langle a^2+b^2+c^2+d^2\rangle$. Now apply Legendre's Theorem which says that every positive rational integer can be written as sum of four squares.

Corollary 3.2 says that the inverse of $\langle a\rangle$ is $3\langle a\rangle$. Hence each element of $\mathcal{G}$ has an inverse. Therefore $\mathcal{G}$ is a group. Therefore we are able to define $\ominus\langle a\rangle = 3\langle a\rangle$. We extend this definition to $\ominus\langle a\rangle = 3\langle a\rangle = \langle -a\rangle$. This definition becomes usefull because of the following generalization of Lemma 3.1. This lemma is new as far as we know. The advantage of using this lemma is that it deducts a lot of calculations in the remainder of the paper.

Lemma 3.3 *Let $a, b \in \mathbb{Z}\backslash\{0\}$. Then we have*

(1) $\langle ab^2\rangle = \langle a\rangle$,

(2) *If $a+b \neq 0$ then $\langle a\rangle \oplus \langle b\rangle = \langle a+b\rangle \oplus \langle ab(a+b)\rangle$.*

Proof. The extension of Lemma 3.1 **(1)** is easy to prove and the proof is left to the reader. We will proof Lemma 3.1 **(2)**. We have to distinguish 4 cases namely (*i*): $a > 0$ and $b > 0$; (*ii*): $a < 0$ and $b < 0$; (*iii*): $a + b > 0$ and $ab < 0$; (*iv*): $a + b < 0$ and $ab < 0$. Case (*i*) was proved in Lemma 3.1. For case (*ii*) multiply case (*i*) by -1. In case (*iii*) we may assume that $a > 0$ and $b < 0$. Substitute b by $-c$ and notice that $\langle a-c\rangle \oplus \langle c\rangle = \langle a\rangle \oplus \langle ac(a-c)\rangle$. For proving case (*iv*) multiply case (*iii*) by -1. □

4 The Main Theorem.

The main theorem describes the Grothendieck Group in our special case (positive definite). We introduce the p-excess (cf. [3]; It is possible to prove the Main Theorem avoiding the p-excess, but the p-excesses make the proofs shorter.) Let $g \in \mathcal{G}$, $g = \bigoplus_k \langle a_k\rangle$, with a_k integers. For p an odd prime we define the p-excess by

$$p\text{-excess}(\langle a\rangle) = \begin{cases} 0 \bmod 8 & \text{if } p \nmid a^\star, \\ p-1 \bmod 8 & \text{if } \left(\frac{a^\star/p}{p}\right) = 1, \\ p+3 \bmod 8 & \text{if } \left(\frac{a^\star/p}{p}\right) = -1. \end{cases} \tag{1}$$

Now p-excess$(g) = \sum p$-excess$(\langle a_k \rangle)$. The 2-excess is defined by

$$2\text{-excess}(\langle a \rangle) = \begin{cases} 1 - a \bmod 8 & \text{if } a \text{ odd} \\ \frac{1}{2}(1 - \frac{a}{2})^2 \bmod 8 & \text{if } a \text{ even.} \end{cases} \tag{2}$$

Now 2-excess$(g) = \sum 2$-excess$(\langle a_k \rangle)$.

Note. It is easy to verify by straight calculation that p-excess$(\langle a \rangle \oplus \langle b \rangle) \equiv p$-excess$(\langle a + b \rangle \oplus \langle ab(a+b) \rangle)$ mod 8, for each prime p.

In [3], Conway and Sloane prove a theorem about p-excesses. Here we will give the positive definite version.

Theorem 4.1 *Let $g, h \in \mathcal{G}$. Suppose $g = \bigoplus \langle a_i \rangle$ and $h = \bigoplus \langle b_j \rangle$. Then $g = h$ is equivalent to $\prod a_i \cdot \prod b_j$ is a square and p-excess$(g) \equiv p$-excess(h) mod 8 for all primes p.*

Note. In the general case it is important to consider the (-1)-excess. However in our situation we have (-1)-excess $= 0$.

Let p and q be two primes then we like to express $\langle pq \rangle$ in terms of $\langle p \rangle$ and $\langle q \rangle$. For example $\langle 55 \rangle = \langle 5 \rangle \oplus \langle 11 \rangle$ and $\langle 21 \rangle = \langle 7 \rangle \ominus \langle 3 \rangle$. But $\langle 10 \rangle$ cannot be expressed in terms of $\langle 2 \rangle$ and $\langle 5 \rangle$ as described above. On the other hand notice that $\langle 10 \rangle \oplus \langle 2 \rangle = \langle 15 \rangle \oplus \langle 3 \rangle$. Our goal of the Main Theorem is to express each class of the Grothendieck Group $\mathcal{G}$ in terms of $\langle p \rangle$, where p is a prime. In order to split $\langle 10 \rangle$ in terms of $\langle 2 \rangle$ and $\langle 5 \rangle$, we introduce the symbol $\langle p|$.

Definition. Let $p \equiv 1 \bmod 4$ be a prime. Then $\langle p| = \langle pq \rangle \oplus \langle q \rangle$, where $q \not\equiv 1 \bmod 4$ is an arbitrary prime for which $\left(\frac{q}{p}\right) = -1$. Notice that such a prime q always exists, cf. [6],Thm. 15 and Thm. 84.

Note. The symbol $\langle p|$ is well defined, independent of the choice of q. To see this, suppose $\langle p| = \langle pq \rangle \oplus \langle q \rangle$. Then q-excess$(\langle p|) = q$-excess$(\langle pq \rangle) + q$-excess$(\langle q \rangle) = 2q - 2 + 4 \equiv 0 \bmod 8$.

We extend the definition of $\langle p|$ to

Definition. Let $p \equiv 1 \bmod 4$ and λ a non-zero integer then we denote by $\langle \lambda \cdot p| = \langle \lambda pq \rangle \oplus \langle \lambda q \rangle \ominus \langle \lambda \rangle$, where q is a prime as was defined in the previous definition.

It is easy to derive the following laws of addition.

Lemma 4.2 *Let p and q be two primes and let λ be a non-zero integer. Then we have*

$$(i) \quad \langle \lambda pq \rangle = \begin{cases} \langle \lambda p \rangle \oplus \langle \lambda q \rangle \ominus \langle \lambda \rangle & \text{if } \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = 1 \\ \langle \lambda p \rangle \ominus \langle \lambda q \rangle \oplus \langle \lambda \rangle & \text{if } \left(\frac{q}{p}\right) = 1, \text{ and } p \equiv q \equiv 3 \bmod 4 \\ \langle \lambda \cdot p| \oplus \langle \lambda \cdot q| \ominus \langle \lambda \rangle & \text{if } \left(\frac{q}{p}\right) = -1 \text{ and } p \equiv q \equiv 1 \bmod 4 \\ \langle \lambda \cdot p| \ominus \langle \lambda q \rangle \oplus \langle \lambda \rangle & \text{if } \left(\frac{q}{p}\right) = -1 \text{ and } p \equiv 1 \bmod 4,\ q \equiv 3 \bmod 4 \end{cases}$$

$$(ii)\quad \langle \lambda q \cdot p| \;=\; \begin{cases} \langle \lambda \cdot p| \oplus \langle \lambda q\rangle \ominus \langle \lambda\rangle & \text{if } \left(\frac{q}{p}\right) = 1 \\ \langle \lambda p\rangle \ominus \langle \lambda q\rangle \oplus \langle \lambda\rangle & \text{if } \left(\frac{q}{p}\right) = -1 \text{ and } q \equiv 3 \bmod 4 \\ \langle \lambda p\rangle \oplus \langle \lambda \cdot q| \ominus \langle \lambda\rangle & \text{if } \left(\frac{q}{p}\right) = -1 \text{ and } q \equiv 1 \bmod 4 \end{cases}$$

Proof. All equations can be verified by p-excesses or by straight calculation. We will show by straight calculation that if $\left(\frac{q}{p}\right) = -1$ and $p \equiv q \equiv 1 \bmod 4$ then $\langle \lambda pq\rangle = \langle \lambda \cdot p| \oplus \langle \lambda \cdot q| \ominus \langle \lambda\rangle$. We need a lemma which will be proven in the following section. First notice that there exists a prime r such that $r \equiv 3 \bmod 4$, $\left(\frac{r}{p}\right) = -1$ and $\left(\frac{r}{q}\right) = -1$ (See [6],Thm. 15 and Thm. 84). Lemma 5.1 tells us that $\langle \lambda pr\rangle = \langle \lambda qr\rangle \oplus \langle \lambda pq\rangle \ominus \langle \lambda\rangle$. Hence $\langle \lambda pq\rangle = \langle \lambda pr\rangle \ominus \langle \lambda qr\rangle \oplus \langle \lambda\rangle = (\langle \lambda pr\rangle \oplus \langle \lambda r\rangle \ominus \langle \lambda\rangle) \oplus (\langle \lambda qr\rangle \oplus \langle \lambda r\rangle \ominus \langle \lambda\rangle) \oplus 2\langle \lambda qr\rangle \oplus 2\langle \lambda r\rangle \oplus 2\langle \lambda\rangle \oplus \langle \lambda\rangle$. Now apply Lemma 3.2, (**2**). Then we have $= \langle \lambda pq\rangle = < \lambda \cdot p| \oplus \langle \lambda \cdot q| \oplus 4\langle \lambda r\rangle \ominus \langle \lambda\rangle$. □

Each element of the Grothendieck Group $\mathcal{G}$ can be represented in diagonal form. The Theorem below shows that there is a unique representation in terms prime elements.

Theorem 4.3 (Main Theorem.) *Let $\mathcal{S}$ be the set of positive definite integral symmetric matrices. Let $\mathcal{G} = (\mathcal{S}/\cong, \oplus)$ be the associated Grothendieck Group. Let $g \in \mathcal{G}$. Then g can be written in a unique way as follows.*

$$g = \delta\,\langle 2\rangle \oplus \bigoplus_i (\delta_i\,\langle p_i\rangle \oplus \epsilon_i\,\langle p_i|) \oplus \bigoplus_j \eta_j\,\langle q_j\rangle, \tag{3}$$

where p_i and q_j are primes with $p_i \equiv 1 \bmod 4$ and $q_j \equiv 3 \bmod 4$, where δ, δ_i and ϵ_i are 0 or 1, while $\eta_j \in \{0, 1, 2, 3\}$.

Proof. Let $g = \bigoplus \langle a_j\rangle$. It is sufficient to prove that $\langle a_j\rangle$ can be written in the form of Formula 4.3. Suppose $a_j = \prod p_i$. Then it is a consequence of Lemma 4.2 that a_j can be written in the form of Formula 4.3.

The uniqueness of Formula 4.3 follows immediately from Theorem 4.1 or can be proven on induction. □

Note. The Grothendieck Group can be seen as $C_2 \otimes V_4^\infty \otimes C_4^\infty$, where $C_n = \mathbb{Z}/n\mathbb{Z}$ and V_4 is the 4–group of Klein. C_2 is related to the prime 2, V_4 is related to primes $p \equiv 1 \bmod 4$ and C_4 is related to primes $q \equiv 3 \bmod 4$.

We conclude with 3 usefull corollaries which follow immediately from the Main Theorem.

Corollary 4.4 *Let $g \in \mathcal{G}$. Suppose $g = \bigoplus_k \langle a_k\rangle$, with $\prod a_k$ is a square. Then g can be written uniquely as*

$$g = \bigoplus_i \delta_i(\langle p_i\rangle \oplus \langle p_i|) \;\oplus\; 2\bigoplus_j \epsilon_j \langle q_j\rangle, \tag{4}$$

where p_i and q_j are primes with $p_i \equiv 1 \bmod 4$ and $q_j \equiv 3 \bmod 4$, and where δ_i and ϵ_j are 0 or 1.

Corollary 4.5 *Let $g \in \mathcal{G}$. Suppose $g = \langle A \rangle \oplus 2\bigoplus_k \langle a_k \rangle$. If $g = 0$ then $\det A$ must be a square.*

Corollary 4.6 *Let $g \in \mathcal{G}$. Suppose $g = 2\bigoplus_k \langle a_k \rangle$. Then*

$$g = 2\bigoplus_j \langle q_j \rangle,$$

where q_j are primes with $q_j \equiv 3 \bmod 4$.

5 The relation with Diophantine Equations.

The following lemmas deal with the relation between equalities in the Grothendieck Group and related Diophantine equations.

Lemma 5.1 *Let a, b and c be positive integers which are squarefree and relatively prime in pairs. Let λ be an arbitrary non-zero integer. Then the following three statements are equivalent:*

(1) *For all primes p dividing a the Legendre symbol $\left(\frac{bc}{p}\right) = 1$, for all primes q dividing b, $\left(\frac{ac}{q}\right) = 1$ and for all primes r dividing c, $\left(\frac{-ab}{r}\right) = 1$.*

(2) $\langle \lambda ac \rangle \oplus \langle \lambda bc \rangle = \langle \lambda ab \rangle \oplus \langle \lambda \rangle$,

(3) *$aX^2 + bY^2 = cZ^2$ has a non trivial integral solution in X, Y and Z,*

Lemma 5.2 *Let a, b and c be positive integers which are squarefree and relatively prime in pairs. Let λ be an arbitrary non-zero integer. Then the following three statements are equivalent:*

(1) *For all primes p dividing a, $\left(\frac{-bc}{p}\right) = 1$, For all primes q dividing b, $\left(\frac{-ac}{q}\right) = 1$, For all primes r dividing c, $\left(\frac{-ab}{r}\right) = 1$.*

(2) $\langle \lambda ab \rangle \oplus \langle \lambda ac \rangle \oplus \langle \lambda bc \rangle \oplus \langle \lambda \rangle = 0$.

(3) *$aX^2 + bY^2 + cZ^2 = abcW^2$ has an integral solution in X, Y, Z and W with $XYZ \neq 0$,*

Proof. (Lemma 5.1 and Lemma 5.2.)

(1)⇔(2) Can be derived from the p-excesses which were defined in the previous section, (See also [3], pp. 372, Theorem 4.) First prove **(1)⇔(2)** in case that $\lambda = 1$. Then apply the definition of $\oplus$ in order to show that $\lambda = 1$ can be replaced by an arbitrary non-zero integer.

(1)⇔(3) This equivalence is based on a theorem of Legendre. See [5], pp. 423–433, [7] and [8], pp. 42–51. □

Lemma 5.3 *Let a, b and c be integers which are squarefree and relatively prime in pairs. And suppose that $\langle ac\rangle \oplus \langle bc\rangle = \langle ab\rangle$. We have*

(1) *If abc is odd then $a \equiv c \bmod 4$ or $b \equiv c \bmod 4$,*

(2) *If c is even then $a+b \equiv 0 \bmod 8$ or $a+b \equiv c \bmod 8$,*

(3) *If ab is even, say a is even then $a+b \equiv c \bmod 8$ or $b \equiv c \bmod 8$.*

Proof. We calculate the 2-excess of $\langle ac\rangle$, $\langle bc\rangle$ and $\langle ab\rangle$ respectivily. We distinguish the same cases as in the lemma.

(1) The 2-excess identity reads $(1-ac)+(1-bc)-(1-ab) \equiv 0 \bmod 8$. Since $c^2 \equiv 1 \bmod 8$, we have $c^2 - ac - bc + ab = (c-a)(c-b) \equiv 0 \bmod 8$. Notice that $a-c$ and $b-c$ are even. Hence $a \equiv c \bmod 4$ or $b \equiv c \bmod 4$.

(2) Let $c = 2C$. Now The 2-excess identity reads $\frac{1}{2}(1-aC)^2 + \frac{1}{2}(1-bC)^2 - (1-ab) \equiv 0 \bmod 8$ or $a^2C^2 + b^2C^2 - 2aC - 2bC + 2ab \equiv 0 \bmod 16$. Notice that $a^2C^2 + b^2C^2 \equiv a^2 + b^2 \bmod 16$. Hence $(a+b-C)^2 \equiv C^2 \bmod 16$.

(3) Let $a = 2A$. Now The 2-excess identity reads $\frac{1}{2}(1-Ac)^2 + (1-bc) - \frac{1}{2}(1-Ab)^2 \equiv 0 \bmod 8$ or $A^2c^2 - A^2b^2 - 2Ac - 2bc + 2Ab + 2 \equiv 0 \bmod 16$. Notice that $A^2c^2 + A^2b^2 \equiv b^2 + c^2 - 2 \bmod 16$. Hence $(A+b-c)^2 \equiv A^2 \bmod 16$. □

Another proof can be given by applying Lemma 5.1, **(2)**⇔**(3)**. Notice that $X^2 \equiv 0, 1$ or $4 \bmod 8$.

Lemma 5.4 *Let a, b and c be integers which are squarefree and relatively prime in pairs. And suppose that $\langle ab\rangle \oplus \langle ac\rangle \oplus \langle bc\rangle = 0$. Then*

(1) *If abc is odd then $a \equiv b \equiv c \bmod 4$,*

(2) *If abc is even, say a is even then $b+c \equiv 4 \bmod 8$ or $a+b+c \equiv 4 \bmod 8$.*

Proof. The proof is comparable to the proof of the previous lemma. □

6 Some applications.

In this Section we will give two applications. The first application is the well-known Theorem of Bruck-Chowla-Ryser (see [2]. The second application deals with the Lattice graph. For another application see [4].

Before we give the two applications we will prove a lemma which expresses $\langle \alpha I_n + \beta J_n\rangle$ in terms of diagonal elements.

Lemma 6.1 *Let $K_n = I_n + J_n$ and $M_n = (n+1)I_n - J_n$, then we have*

(1) $\langle \lambda K_n\rangle = (n+1)\langle \lambda\rangle \ominus \langle \lambda(n+1)\rangle$,

(2) $\langle \alpha I_n + \beta J_n\rangle = n\langle \alpha\rangle \ominus \langle \alpha n\rangle \oplus \langle n(\beta n + \alpha\rangle$,

(3) $\langle \lambda M_n\rangle = (n+1)\langle \lambda(n+1)\rangle \ominus \langle \lambda\rangle$.

Proof. Let $Q_n = \begin{pmatrix} -I_{n-1} & \underline{j} \\ \underline{j}^\top & 1 \end{pmatrix}$ be an $n \times n$-matrix. We easily calculate that $Q_n(\alpha I_n + \beta J_n)Q_n = \begin{pmatrix} \alpha K_{n-1} & \underline{0} \\ \underline{0}^\top & n(\beta n + \alpha) \end{pmatrix}$. Especially $M_{n+1}\lambda I_{n+1} M_{n+1} = \begin{pmatrix} \lambda K_n & \underline{0} \\ \underline{0}^\top & \lambda(n+1) \end{pmatrix}$.

Hence $(n+1)\langle\lambda\rangle = \langle\lambda K_n\rangle \oplus \langle\lambda(n+1)\rangle$, which proves (**1**).
The proofs of (**2**) and (**3**) can be found from $\langle\alpha I_n + \beta J_n\rangle = \langle\alpha K_{n-1}\rangle \oplus \langle n(\beta n + \alpha)\rangle$. □

We give another proof of:

Theorem 6.2 (Bruck, Chowla and Ryser) *Let $\mathcal{D}$ be a symmetric 2-(v, k, λ)-design. Then v, k and λ satisfy the following identity:*

If v is even then $k - \lambda$ is a square.

If v is odd then

$$(k-\lambda)X^2 + (-1)^{\frac{v-1}{2}} v Y^2 = Z^2 \tag{5}$$

has a non-trivial integral solution in X, Y and Z.

Proof. Let A the associated incidence matrix. Then $AA^\top = (k-\lambda)I_v + \lambda J_v$. Therefore $\langle (k-\lambda)I_v + \lambda J_v\rangle = 0$. Now apply Lemma 6.4. We conclude that

$$v\langle k-\lambda\rangle \ominus \langle v(k-\lambda)\rangle \oplus \langle v(v\lambda + (k-\lambda))\rangle = 0. \tag{6}$$

Notice that $v\lambda + (k-\lambda) = k^2$. Now Formula 6 can be read as

$$v\langle k-\lambda\rangle \ominus \langle v(k-\lambda)\rangle \oplus \langle v\rangle = 0. \tag{7}$$

If v is even then the number of diagonal elements in which the factor $\langle k-\lambda\rangle$ appears is odd. Hence $k-\lambda$ must be a square. If v is odd then $v \equiv (-1)^{\frac{v-1}{2}} \bmod 4$. Hence Formula 6 can be written in the form

$$\langle v\rangle \oplus (-1)^{\frac{v-1}{2}}\langle k-\lambda\rangle = \langle v(k-\lambda)\rangle. \tag{8}$$

Now apply Lemma 5.1. □

The second application deals with the Lattice graph. We consider the complete bipartite graph on $2n$ vertices, $\mathcal{K}_{nn}$. Let $P_0, \ldots, P_{n-1}$ be vertices at one half of the graph, and let $P_n, \ldots, P_{2n-1}$ be the other vertices. We denote by $\mathcal{L}_n$ the linegraph on n^2 vertices corresponding to the n^2 edges of $\mathcal{K}_{nn}$, (also known as the Lattice graph). We denote the vertices of $\mathcal{L}_n$ by B_i, with $0 \le i \le n^2 - 1$. Let $0 \le a, b \le n-1$. Then the vertex B_{an+b}

of $\mathcal{L}_n$ corresponds to the edge $\overline{P_a P_{n+b}}$ of $\mathcal{K}_{nn}$. We denote by L_n the adjacency matrix corresponding to $\mathcal{L}_n$. The eigenvalues of L_n are

$$[2(n-1)]^1, [n-2]^{2(n-1)} \text{ and } [-2]^{(n-1)^2}.$$

In this section we will give decomposability conditions for a matrix of the form

$$\mathbb{L}_n = \alpha I + \beta L_n + \gamma J.$$

A main role is played by the eigenvalues of $\mathbb{L}_n$. It can be verified easily that the eigenvalues of $\mathbb{L}_n$ are

$$\begin{aligned} r_0 &= \alpha + 2\beta(n-1) + \gamma n^2 \\ r_1 &= \alpha + \beta(n-2) \\ r_2 &= \alpha - 2\beta \end{aligned}$$

We will consider $\mathbb{L}_n$ being a function of r_0, r_1, r_2. Our main theorem decompose $\mathbb{L}_n(r_0, r_1, r_2)$.

Theorem 6.3 *Let $\mathbb{L}_n = \mathbb{L}_n(r_0, r_1, r_2)$ be defined as above. Then we have*

$$\langle \mathbb{L}_n \rangle = \langle r_0 \rangle \oplus 2n\langle r_1 n \rangle \oplus 2\langle r_1 \rangle \oplus 2n\langle r_2 \rangle \oplus 2 \bigoplus_{i=5}^{n-1} i\langle r_2 i \rangle. \tag{9}$$

As a consequence of this theorem we have the following corollary:

Corollary 6.4 *Let $\mathbb{L}_n = \mathbb{L}_n(r_0, r_1, r_2)$ be defined as above. And suppose that $\mathbb{L}_n$ is decomposable. Then r_0 must be a square and we have*

(*i*) *If* $n \equiv 0 \bmod 4$ *then* $2\langle r_1 \rangle \oplus \mathcal{P}(n) = 0$,

(*ii*) *If* $n \equiv 1 \bmod 4$ *then* $2\langle n \rangle \oplus 2\langle r_2 \rangle \oplus \mathcal{P}(n) = 0$,

(*iii*) *If* $n \equiv 2 \bmod 4$ *then* $2\langle r_1 \rangle \oplus 2\langle r_2 \rangle \oplus \mathcal{P}(n) = 0$,

(*iv*) *If* $n \equiv 3 \bmod 4$ *then* $2\langle n \rangle \oplus \mathcal{P}(n) = 0$,

where $\mathcal{P}(n) = 2 \bigoplus_{i=4}^{\frac{n}{2}} \langle 2i-1 \rangle$.

Proof. Since $\mathbb{L}_n$ is decomposable, Formula 9 must be equal to zero. Except of the first term of the right-hand part $\langle r_0 \rangle$ all terms appear in pairs. Therefore r_0 must be a square, (see Corollary 4.5). We consider four cases depending on n mod 4. We share the terms $2n\langle r_1 n \rangle$ and $2\langle r_1 \rangle$ which results, applying Corollary 4.6, in $2\langle r_1 \rangle$ for even n and $2\langle n \rangle$ for odd n. The other terms can be simplified to $\mathcal{P}(n)$ or $2\langle r_2 \rangle \oplus \mathcal{P}(n)$ (depending on n). □

Note. For $n \geq 8$ the sum $\mathcal{P}(n)$ will never be equal to 0. $\mathcal{P}(n)$ grows rather fast. For example $\mathcal{P}(8) = 2\langle 7 \rangle$, $\mathcal{P}(12) = 2\langle 7 \rangle \oplus 2\langle 11 \rangle$ and $\mathcal{P}(20) = 2\langle 3 \rangle \oplus 2\langle 7 \rangle \oplus 2\langle 11 \rangle \oplus 2\langle 19 \rangle$.

In order to prove the theorem we will use a lemma. This lemma expresses $\mathbb{L}_n$ in terms of $\mathbb{L}_{n-1}$.

Lemma 6.5

$$\langle \mathbb{I}_n(r_0, r_1, r_2)\rangle = \langle r_0\rangle \oplus 2\langle r_1(nI_{n-1} - J)\rangle \oplus \langle r_2(3I_{(n-1)^2} + L_{n-1} + J)\rangle.$$

Proof. We are searching a matrix Q such that $Q^\top \mathbb{I}_n Q$ is of the form as desired in the lemma. We build up Q from three submatrices F_0, F_1 and F_2, such that $Q = (F_0|F_1|F_2)$. We construct F_i from E_i which are defined by

$$\begin{array}{lcll} E_0 & = & \frac{1}{n^2}J & = \mathbb{I}_n(1,0,0), \\ E_1 & = & \frac{1}{n^2}(2nI + nL_n - 2J) & = \mathbb{I}_n(0,1,0), \\ E_2 & = & \frac{1}{n^2}((n^2-2n)I - nL_n + J) & = \mathbb{I}_n(0,0,1). \end{array}$$

These matrices E_i satisfy $E_iE_j = \delta_{ij}E_i$. Let $\underline{1}$ be the all one vector, let U be an $n^2 \times 2(n-1)$ matrix defined by $U = (u_{ij})$, where

$$u_{ij} = \begin{cases} 1 & \text{if } P_j \in B_i \text{ for } \quad 1 \le j \le 2(n-1) \text{ and} \\ & \qquad\qquad\quad 0 \le i \le n^2 - 1, \\ 0 & \text{else,} \end{cases}$$

and let V be an $n^2 \times (n-1)^2$ matrix defined by $V = (v_{ij})$, where

$$v_{ij} = \begin{cases} 1 & \text{if either } \ i = 1 \\ & \text{or} \qquad\ i = an + (b+1) \text{ and } j = (a-1)(n-1) + b, \\ -1 & \text{if either } \ i = b+1 \text{ and } j = (a-1)(n-1) + b, \\ & \text{or} \qquad\ i = an + 1 \text{ and } j = (a-1)(n-1) + b, \\ & \quad (\text{where } 1 \le a, b \le n-1) \\ 0 & \text{else.} \end{cases}$$

Now we construct the matrices F_i by

$$\begin{array}{lcl} F_0 & = & \frac{1}{n}E_0\underline{1}, \\ F_1 & = & E_1U, \\ F_2 & = & E_2V. \end{array}$$

Since $\mathbb{I}_n E_i = r_i E_i$ for $0 \le i \le 2$ we get

$$Q^\top \mathbb{I}_n(r_0, r_1, r_2)Q = r_0F_0^\top F_0 \oplus r_1F_1^\top F_1 \oplus r_2F_2^\top F_2.$$

Notice that

$$\begin{array}{lcl} F_0 & = & \frac{1}{n}\underline{1}, \\ F_1 & = & (f_{ij}) \text{ where } f_{ij} = \begin{cases} \frac{n-1}{n} & \text{if } P_j \in B_i \text{ for } \ 1 \le j\ 2(n-1) \text{ and} \\ & \qquad\qquad\quad 0 \le i \le n-1, \\ \frac{-1}{n} & \text{else,} \end{cases} \\ F_2 & = & V \end{array}$$

and

$$\begin{array}{rcl} F_0^\top F_0 & = & 1, \\ \langle F_1^\top F_1\rangle & = & 2\langle nI_{n-1} - J\rangle, \\ F_2^\top F_2 & = & \mathbb{I}_{n-1}(n^2, n, 1). \end{array}$$

This proves the lemma. □

Proof of Theorem 6.2. We will first prove a special case, namely $\langle \lambda \mathbb{I}_n((n+1)^2, n+1, 1)\rangle$. We use induction. For $n = 2$ we get $\langle \lambda \mathbb{I}_2(9,3,1)\rangle = 2\langle\lambda\rangle \oplus 2\langle 3\lambda\rangle$. Now we apply the previous lemma. We have

$$\langle \mathbb{I}_n(\lambda(n+1)^2, \lambda(n+1), \lambda)\rangle = \langle\lambda\rangle \oplus 2\langle\lambda(nI_{n-1} - J)\rangle \oplus \langle\lambda(3I_{(n-1)^2} + L_{n-1} + J)\rangle.$$

We apply Lemma 6.4 which says that $\langle\lambda(nI_{n-1} - J)\rangle = n\langle\lambda n\rangle \ominus \langle\lambda\rangle$. By induction on n we get

$$\begin{aligned} \langle \mathbb{I}_n(\lambda(n+1)^2, \lambda(n+1), \lambda)\rangle &= 2\langle\lambda\rangle \oplus 2\langle 3\lambda\rangle \oplus 2\textstyle\bigoplus_{i=3}^{n}(i\langle\lambda i\rangle \oplus \langle\lambda\rangle) \\ &= 2(n-1)\langle\lambda\rangle \oplus 2\textstyle\bigoplus_{i=5}^{n} i\langle\lambda i\rangle. \end{aligned}$$

Now we can prove the theorem in its generality. We get

$$\begin{aligned} \langle \mathbb{I}_n(r_0, r_1, r_2)\rangle &= \langle r_0\rangle \oplus 2\langle r_1(nI_{n-1} - J)\rangle \oplus \langle r_2(3I_{(n-1)^2} + L_{n-1} + J)\rangle \\ &= \langle r_0\rangle \oplus 2n\langle r_1 n\rangle \oplus 2\langle r_1\rangle \oplus 2n\langle r_2\rangle \oplus 2\textstyle\bigoplus_{i=5}^{n-1} i\langle r_2 i\rangle. \quad \square \end{aligned}$$

This leads to necessary conditions for square partial balanced designs similar to the ones of S.S. Shrikhande and N.C. Jain (cf. [9]).

References

[1] J.W.S. Cassels *Rational Quadratic Forms*, Academic Press, London, (**1978**).

[2] S. Chowla en H.J. Ryser *Combinatorial Problems*, Can. J. Math. 2 (**1950**), 93-99.

[3] J.H. Conway and N.J.A. Sloane *Sphere Packings, Lattices and Groups*, Springer-Verlag New York, (**1988**).

[4] M.J. Coster and W.H. Haemers *Quasi-symmetric Designs related to the Triangular graph*, Research memorandum FEW 596, Tilburg Univ. 1993.

[5] L.E. Dickson *History of the theory of Numbers, Volume II*, Chelsea Publishing Company, New York, 1966.

[6] G.H. Hardy and E.M. Wright *An Introduction to the Theory of Numbers.* Oxford University Press, Oxford, (**1983**), fifth edition.

[7] L.J.Mordell, *On the equation* $ax^2 + by^2 - cz^2 = 0$., Monatshefte für Math. **55** (1951), 323-327.

[8] L.J.Mordell, *Diophantine Equations* Academic Press, inc., London, New York, 1969.

[9] S.S. Shrikhande and N.C. Jain *The Non-existence of some partially balanced incomplete block designs with Latin square type association scheme* Sankhga A 24 (1962), 259-268.

IN 1993 REEDS VERSCHENEN

588 Rob de Groof and Martin van Tuijl
The Twin-Debt Problem in an Interdependent World
Communicated by Prof.dr. Th. van de Klundert

589 Harry H. Tigelaar
A useful fourth moment matrix of a random vector
Communicated by Prof.dr. B.B. van der Genugten

590 Niels G. Noorderhaven
Trust and transactions; transaction cost analysis with a differential behavioral assumption
Communicated by Prof.dr. S.W. Douma

591 Henk Roest and Kitty Koelemeijer
Framing perceived service quality and related constructs A multilevel approach
Communicated by Prof.dr. Th.M.M. Verhallen

592 Jacob C. Engwerda
The Square Indefinite LQ-Problem: Existence of a Unique Solution
Communicated by Prof.dr. J. Schumacher

593 Jacob C. Engwerda
Output Deadbeat Control of Discrete-Time Multivariable Systems
Communicated by Prof.dr. J. Schumacher

594 Chris Veld and Adri Verboven
An Empirical Analysis of Warrant Prices versus Long Term Call Option Prices
Communicated by Prof.dr. P.W. Moerland

595 A.A. Jeunink en M.R. Kabir
De relatie tussen aandeelhoudersstructuur en beschermingsconstructies
Communicated by Prof.dr. P.W. Moerland

596 M.J. Coster and W.H. Haemers
Quasi-symmetric designs related to the triangular graph
Communicated by Prof.dr. M.H.C. Paardekooper

597 Noud Gruijters
De liberalisering van het internationale kapitaalverkeer in historisch-institutioneel perspectief
Communicated by Dr. H.G. van Gemert

598 John Görtzen en Remco Zwetheul
Weekend-effect en dag-van-de-week-effect op de Amsterdamse effectenbeurs?
Communicated by Prof.dr. P.W. Moerland

599 Philip Hans Franses and H. Peter Boswijk
Temporal aggregration in a periodically integrated autoregressive process
Communicated by Prof.dr. Th.E. Nijman

600 René Peeters
On the p-ranks of Latin Square Graphs
Communicated by Prof.dr. M.H.C. Paardekooper

601 Peter E.M. Borm, Ricardo Cao, Ignacio García-Jurado
Maximum Likelihood Equilibria of Random Games
Communicated by Prof.dr. B.B. van der Genugten

602 Prof.dr. Robert Bannink
Size and timing of profits for insurance companies. Cost assignment for products with multiple deliveries.
Communicated by Prof.dr. W. van Hulst

603 M.J. Coster
An Algorithm on Addition Chains with Restricted Memory
Communicated by Prof.dr. M.H.C. Paardekooper

604 Ton Geerts
Coordinate-free interpretations of the optimal costs for LQ-problems subject to implicit systems
Communicated by Prof.dr. J.M. Schumacher

605 B.B. van der Genugten
Beat the Dealer in Holland Casino's Black Jack
Communicated by Dr. P.E.M. Borm

606 Gert Nieuwenhuis
Uniform Limit Theorems for Marked Point Processes
Communicated by Dr. M.R. Jaïbi

607 Dr. G.P.L. van Roij
Effectisering op internationale financiële markten en enkele gevolgen voor banken
Communicated by Prof.dr. J. Sijben

608 R.A.M.G. Joosten, A.J.J. Talman
A simplicial variable dimension restart algorithm to find economic equilibria on the unit simplex using $n(n+1)$ rays
Communicated by Prof.Dr. P.H.M. Ruys

609 Dr. A.J.W. van de Gevel
The Elimination of Technical Barriers to Trade in the European Community
Communicated by Prof.dr. H. Huizinga

610 Dr. A.J.W. van de Gevel
Effective Protection: a Survey
Communicated by Prof.dr. H. Huizinga

611 Jan van der Leeuw
First order conditions for the maximum likelihood estimation of an exact ARMA model
Communicated by Prof.dr. B.B. van der Genugten

612 Tom P. Faith
Bertrand-Edgeworth Competition with Sequential Capacity Choice
Communicated by Prof.Dr. S.W. Douma

613 Ton Geerts
The algebraic Riccati equation and singular optimal control: The discrete-time case
Communicated by Prof.dr. J.M. Schumacher

614 Ton Geerts
Output consistency and weak output consistency for continuous-time implicit systems
Communicated by Prof.dr. J.M. Schumacher

615 Stef Tijs, Gert-Jan Otten
Compromise Values in Cooperative Game Theory
Communicated by Dr. P.E.M. Borm

616 Dr. Pieter J.F.G. Meulendijks and Prof.Dr. Dick B.J. Schouten
Exchange Rates and the European Business Cycle: an application of a 'quasi-empirical' two-country model
Communicated by Prof.Dr. A.H.J.J. Kolnaar

617 Niels G. Noorderhaven
The argumentational texture of transaction cost economics
Communicated by Prof.Dr. S.W. Douma

618 Dr. M.R. Jaïbi
Frequent Sampling in Discrete Choice
Communicated by Dr. M.H. ten Raa

619 Dr. M.R. Jaïbi
A Qualification of the Dependence in the Generalized Extreme Value Choice Model
Communicated by Dr. M.H. ten Raa

620 J.J.A. Moors, V.M.J. Coenen, R.M.J. Heuts
Limiting distributions of moment- and quantile-based measures for skewness and kurtosis
Communicated by Prof.Dr. B.B. van der Genugten

621 Job de Haan, Jos Benders, David Bennett
Symbiotic approaches to work and technology
Communicated by Prof.dr. S.W. Douma

622 René Peeters
Orthogonal representations over finite fields and the chromatic number of graphs
Communicated by Dr.ir. W.H. Haemers

623 W.H. Haemers, E. Spence
Graphs Cospectral with Distance-Regular Graphs
Communicated by Prof.dr. M.H.C. Paardekooper

624 Bas van Aarle
The target zone model and its applicability to the recent EMS crisis
Communicated by Prof.dr. H. Huizinga

625 René Peeters
Strongly regular graphs that are locally a disjoint union of hexagons
Communicated by Dr.ir. W.H. Haemers

626 René Peeters
Uniqueness of strongly regular graphs having minimal p-rank
Communicated by Dr.ir. W.H. Haemers

627 Freek Aertsen, Jos Benders
Tricks and Trucks: Ten years of organizational renewal at DAF?
Communicated by Prof.dr. S.W. Douma

628 Jan de Klein, Jacques Roemen
Optimal Delivery Strategies for Heterogeneous Groups of Porkers
Communicated by Prof.dr. F.A. van der Duyn Schouten

629 Imma Curiel, Herbert Hamers, Jos Potters, Stef Tijs
The equal gain splitting rule for sequencing situations and the general nucleolus
Communicated by Dr. P.E.M. Borm

630 A.L. Hempenius
Een statische theorie van de keuze van bankrekening
Communicated by Prof.Dr.Ir. A. Kapteyn

631 Cok Vrooman, Piet van Wijngaarden, Frans van den Heuvel
Prevention in Social Security: Theory and Policy Consequences
Communicated by Prof.Dr. A. Kolnaar

IN 1994 REEDS VERSCHENEN

632 B.B. van der Genugten
Identification, estimating and testing in the restricted linear model
Communicated by Dr. A.H.O. van Soest

633 George W.J. Hendrikse
Screening, Competition and (De)Centralization
Communicated by Prof.dr. S.W. Douma

634 A.J.T.M. Weeren, J.M. Schumacher, and J.C. Engwerda
Asymptotic Analysis of Nash Equilibria in Nonzero-sum Linear-Quadratic Differential Games. The Two-Player case.
Communicated by Prof.dr. S.H. Tijs