TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 164, February 1972

AN OPTIMIZATION PROBLEM FOR UNITARY AND ORTHOGONAL REPRESENTATIONS OF FINITE GROUPS

BY
D. Ž. DJOKOVIĆ AND I. F. BLAKE(1)

Abstract. Let $G \to \mathrm{GL}(V)$ be a faithful orthogonal representation of a finite group G acting in an Euclidean space V. For a unit vector x we choose $g \neq 1$ in G so that $|gx-x|$ is minimal and put $\delta(x)=|gx-x|$. We study the class of vectors x which maximize $\delta(x)$ and have the additional property that $|gx-x|$ depends only on the conjugacy class of $g \in G$. For some special types of representations we are able to characterize completely this class of vectors.

1. **Introduction.** Let G be a finite group and V a finite-dimensional real (resp. complex) vector space. We assume that V is equipped with a symmetric (resp. hermitian) positive definite form (x, y) and so V is an Euclidean (resp. unitary) space. In the hermitian case we stipulate that $(\lambda x, \mu y)=\lambda\bar{\mu}(x, y)$.

Let T be an orthogonal (resp. unitary) representation of G on V. Instead of $T(g)x$ we shall write gx ($g \in G$, $x \in V$). V as a G-module has an orthogonal splitting into irreducible submodules. The number of summands is the *length* of V. If every irreducible submodule of V is isomorphic to a fixed irreducible G-module W then we shall say that V is *homogeneous of type* W. For $x \in V$ choose $g \in G\backslash N$ such that $|gx-x|$ is minimal and put $\delta(x)=|gx-x|$. Here $N=\ker T$.

Definition 1. *A vector $x \in V$ is optimal if $x \neq 0$ and $\delta(x)=\sup \delta(y)$ where the supremum is over all $y \in V$ such that $|y|=|x|$. We say that x is strongly optimal if it is optimal and $|gx-x|$ depends only on the conjugacy class of $g \in G$.*

If x is optimal or strongly optimal so is λx for $\lambda \neq 0$. It is clear that optimal vectors exist. If $N \neq G$ then $\delta(x)>0$ for optimal x.

The problem of finding optimal vectors was raised by D. Slepian in his paper [4] where he studies the group codes. Such codes possess many desirable properties from a communication theory point of view. We shall determine all strongly optimal vectors for some particular G-modules.

We consider only orthogonal (resp. unitary) finite dimensional representations of G. All isomorphisms of G-modules are assumed to preserve the length. By

Received by the editors February 9, 1971.

AMS 1970 *subject classifications*. Primary 20C15.

Key words and phrases. Unitary and orthogonal representations, characters, irreducible modules, homogeneous modules, group algebra, Schur's lemma, Wedderburn's theorem.

(1) The work of the first author was supported by NRC Grant A-5285 and of the second author by NRC Grant A-7382.

R, ***C***, ***H*** we denote real numbers, complex numbers and quaternions, respectively. ***RG*** and ***CG*** are the group algebras of G.

2. **Formula for distances.** Let K be a conjugacy class of G and $|K|$ the number of elements in K.

THEOREM 1. *Let V be a real or complex G-module and $V=V_1\oplus\cdots\oplus V_s$ the decomposition into homogeneous components. Thus $V_i\perp V_j$ for $i\neq j$. If $x=x_1+\cdots+x_s$, $x_i\in V_i$ then*

$$\frac{1}{|K|}\sum_{g\in K}(gx,x)=\sum_{i=1}^{s}\frac{|x_i|^2}{n_i}\chi_i^K, \tag{1}$$

and

$$\frac{1}{|K|}\sum_{g\in K}|gx-x|^2=2|x|^2-2\sum_{i=1}^{s}\frac{|x_i|^2}{n_i}\operatorname{Re}\chi_i^K. \tag{2}$$

Here, χ_i is the character of G afforded by some irreducible submodule of V_i, $n_i=\chi_i(1)$ and $\chi_i^K=\chi_i(g)$ for $g\in K$.

Proof. Note that (1) implies (2). We shall prove (1) only for V complex. The proof for real V is similar. When V is real irreducible this has been proved by Slepian [4].

Let us assume first that V is irreducible. Then by Schur's lemma $\sum_{g\in K}T(g)=\lambda\cdot 1$ where T is the representation afforded by V and λ a scalar. By taking traces we get $\lambda=(1/n)|K|\chi^K$ where χ is the character afforded by V, $n=\chi(1)$ and $\chi^K=\chi(g)$ for $g\in K$. Thus $\sum_{g\in K}(gx,x)=\lambda|x|^2$ and (1) is valid in this case.

In the general case we decompose each V_i into orthogonal sum of irreducible submodules $V_i=V_{i1}\oplus\cdots\oplus V_{ik_i}$ and write $x_i=x_{i1}+\cdots+x_{ik_i}$, $x_{ij}\in V_{ij}$. Then

$$\begin{aligned}\sum_{g\in K}(gx,x)&=\sum_{i,j}\sum_{g\in K}(gx_{ij},x_{ij})\\&=|K|\sum_{i,j}\frac{|x_{ij}|^2}{n_i}\chi_i^K\end{aligned}$$

which proves (1).

DEFINITION 2. *Let V be a real or complex G-module and $x\in V$. We say that x is balanced, resp. strongly balanced, if* Re (gx,x), *resp.* (gx,x), *depends only on the conjugacy class of $g\in G$.*

We note that in the case when V is real, balanced and strongly balanced vectors coincide. If V is complex let V^0 be the real G-module obtained by restriction of scalars. Then x is balanced in V if and only if it is balanced in V^0.

COROLLARY 1. *x is balanced, resp. strongly balanced if and only if*

$$\operatorname{Re}(gx,x)=\sum_{i=1}^{s}\frac{1}{n_i}|x_i|^2\operatorname{Re}\chi_i(g),\qquad\forall g\in G;$$

resp.

$$(gx,x)=\sum_{i=1}^{s}\frac{1}{n_i}|x_i|^2\chi_i(g),\qquad\forall g\in G.$$

COROLLARY 2. *Let V be a real or complex G-module and V^0 the real G-module obtained from V by restriction of scalars. Assume that V^0 is homogeneous. If $x \in V$, $x \neq 0$ then x is balanced if and only if it is strongly optimal. A necessary and sufficient condition for this is that* $\operatorname{Re}(gx, x) = (1/n)|x|^2 \operatorname{Re} \chi(g)$, $\forall g \in G$. *Here, χ is the character afforded by an arbitrary irreducible submodule of V and $n = \chi(1)$.*

3. **Decompositions of homogeneous modules.** Let W be an irreducible real or complex G-module and let D be the endomorphism ring of W as a G-module. By Schur's lemma D is a division ring. If W is complex then $D = \boldsymbol{C}$. If W is real then $D = \boldsymbol{R}$, $\boldsymbol{C}$ or $\boldsymbol{H}$. If $D = \boldsymbol{R}$ we shall say that W is of the first kind, if $D = \boldsymbol{H}$ then W is of the second kind and if $D = \boldsymbol{C}$ then W is of the third kind [3, p. II-47].

THEOREM 2. *If $\sigma \in D$ then $\sigma^* = \bar{\sigma}$ where $\bar{\sigma}$ is the conjugate of σ in D and σ^* is the adjoint of σ with respect to the form (x, y).*

Proof. The form $(\sigma x, \sigma y)$ is G-invariant. Since W is irreducible we have

$$(\sigma x, \sigma y) = f(\sigma) \cdot |\sigma|^2 (x, y), \qquad \forall x, y \in W,$$

where $f(\sigma) > 0$. The function f is continuous for $\sigma \neq 0$, $f(1) = 1$, $f(\lambda\sigma) = f(\sigma)$ for real λ and $f(\sigma\tau) = f(\sigma) f(\tau)$. These properties imply that $f(\sigma) = 1$ for all $\sigma \in D$.

THEOREM 3. *Let V be a homogeneous real or complex G-module of type W and length k. Let $V = V_1 \oplus \cdots \oplus V_k$ be a fixed orthogonal splitting into irreducible submodules and $f_i \colon W \to V_i$ a fixed set of G-isomorphisms.*

(a) *Let $\sigma = (\sigma_{ij})$, $1 \leqq i, j \leqq k$, be a unitary matrix over D, i.e. $\sigma^* \sigma = 1$ where σ^* is the conjugate transpose of σ. Define*

$$f'_j = \sum_{i=1}^{k} f_i \sigma_{ij}, \qquad 1 \leqq j \leqq k.$$

Then each f'_j is a G-monomorphism and $V = f'_1(W) \oplus \cdots \oplus f'_k(W)$ is an orthogonal splitting.

(b) *Every orthogonal splitting of V into irreducible submodules can be obtained by the method described in* (a).

(c) *Two unitary matrices σ and τ give rise to the same splitting if and only if $\sigma = \tau\lambda$ where λ is a diagonal unitary matrix.*

Proof. (a) It is clear that $f'_j(gx) = g f'_j(x)$ holds for all $g \in G$, $x \in V$. The remaining assertions follow from

$$\begin{aligned} (f'_i(x), f'_j(y)) &= \sum_{r=1}^{k} (f_r \sigma_{ri} x, f_r \sigma_{rj} y) \\ &= \sum_{r=1}^{k} (\sigma_{ri} x, \sigma_{rj} y) = \left(\left(\sum_{r=1}^{k} \bar{\sigma}_{rj} \sigma_{ri} \right) x, y \right) = \delta_{ij}(x, y), \end{aligned}$$

where we used Theorem 2 and δ_{ij} is the Kronecker symbol.

(b) Let $V = V'_1 \oplus \cdots \oplus V'_k$ be an arbitrary orthogonal splitting of V into irreducible submodules. Let $f'_i \colon W \to V'_i$, $1 \leqq i \leqq k$, be G-isomorphisms and let π_i,

$1 \leqq i \leqq k$, be the orthogonal projector on V_i. By definition of D we have $\pi_j \circ f_i' = f_j \sigma_{ji}$ for some $\sigma_{ji} \in D$. For $x, y \in W$ we have

$$\delta_{ij}(x, y) = (f_i'(x), f_j'(y)) = \left(\sum_{r=1}^{k} f_r \sigma_{ri} x, \sum_{r=1}^{k} f_r \sigma_{rj} y\right)$$
$$= \sum_{r=1}^{k} (\sigma_{ri} x, \sigma_{rj} y) = \left(\sum_{r=1}^{k} \bar{\sigma}_{rj} \sigma_{ri} x, y\right).$$

This implies that the matrix $\sigma = (\sigma_{ij})$ is unitary.

(c) Assume that two unitary matrices $\sigma = (\sigma_{ij})$ and $\tau = (\tau_{ij})$ give rise to the same splitting of V. Then $\sum_{r=1}^{k} f_r \sigma_{ri} = (\sum_{r=1}^{k} f_r \tau_{ri}) \lambda_i$ for some $\lambda_i \in D$. Thus $\sigma_{ri} = \tau_{ri} \lambda_i$, i.e. $\sigma = \tau \lambda$ where λ is a diagonal matrix.

Definition 3. *A vector $x \in V$ is principal if there exists a scalar λ and the vectors $t_i \in W$ $(1 \leqq i \leqq k)$ such that $|t_i| = 1$ $(1 \leqq i \leqq k)$, the subspaces Dt_i $(1 \leqq i \leqq k)$ are orthogonal to each other and $x = \lambda \sum_{i=1}^{k} f_i(t_i)$.*

(*The notation is the same as in Theorem* 3.)

Theorem 4. *The definition of principal vectors is independent of the choice of the splitting $V = V_1 \oplus \cdots \oplus V_k$ and the isomorphisms $f_i \colon W \to V_i$. The same is true for the subspace of W spanned by $t_1, \ldots, t_k$ if $x \neq 0$.*

Proof. Let V_i', f_i', σ be as in the proof of Theorem 3. Write $x = x_1' + \cdots + x_k'$, $x_i' \in V_i'$. We have

$$\sum_{s=1}^{k} x_s' = \sum_{r=1}^{k} x_r = \sum_{r=1}^{k} f_r f_r^{-1} x_r = \sum_{r,s=1}^{k} f_s' \tau_{sr} f_r^{-1} x_r$$

where $\tau = (\tau_{sr})$ is some unitary matrix over D. Thus $f_s'^{-1}(x_s') = \sum_{r=1}^{k} \tau_{sr} f_r^{-1}(x_r)$.

All the assertions follow from this equality. Let for instance $D = \boldsymbol{H}$. Then

$$(f_s'^{-1}(x_s'), f_t'^{-1}(x_t')) = \sum_{i,j=1}^{k} (\tau_{si} f_i^{-1} x_i, \tau_{tj} f_j^{-1} x_j)$$
$$= \sum_{i=1}^{k} (\tau_{si} f_i^{-1} x_i, \tau_{ti} f_i^{-1} x_i) = \sum_{i=1}^{k} \operatorname{Re}(\bar{\tau}_{ti} \tau_{si})(f_i^{-1} x_i, f_i^{-1} x_i)$$
$$= \sum_{i=1}^{k} \operatorname{Re}(\tau_{si} \bar{\tau}_{ti}) |x_i|^2 = \delta_{st} |x_1|^2.$$

4. **Strongly balanced vectors.** In the real (resp. complex) group algebra of G we introduce symmetric (resp. hermitian) positive definite form by

$$\left(\sum_{g \in G} \xi(g) g, \sum_{g \in G} \eta(g) g\right) = \sum_{g \in G} \xi(g) \overline{\eta(g)}.$$

Then the left regular representation of G is orthogonal (resp. unitary).

Let W be an irreducible real (resp. complex) G-module and V the homogeneous component of type W of the group algebra. Let $n = \dim W$ and let k be the length of V. If W is complex then $n = k$. If W is real then $n = k$, $4k$ or $2k$ depending on whether W is of the first, second or third kind. In all cases k is the dimension of W as D-vector space.

Let $V = V_1 \oplus \cdots \oplus V_k$ be an orthogonal splitting into irreducible submodules and $f_i : W \to V_i$ G-isomorphisms.

We can write $1 = e + e'$ where $e \in V$ and $e' \perp V$. Since V is a minimal two-sided ideal of the group algebra of G we have [1, p. 236]

$$e = \frac{n}{|G|} \sum_{g \in G} \overline{\chi(g)} g,$$

e is in the center of the group algebra and it is an idempotent, i.e. $e^2 = e \neq 0$. Since $|e|^2 = (e, e) = (e, 1) = n^2/|G|$, $(ge, e) = (g, e) = (n/|G|)\chi(g) = (1/n)|e|^2\chi(g)$, we see that e is strongly balanced.

Definition 4. *A basis $t_1, \ldots, t_k$ of the D-vector space W is called D-orthonormal basis if $|t_i| = 1$, $1 \leqq i \leqq k$, and the subspaces Dt_i, $1 \leqq i \leqq k$, are orthogonal to each other.*

Theorem 5. *Let V be a homogeneous component of type W of **R**G or **C**G. Then $x \in V$ is strongly balanced if and only if it is principal.*

Proof. *Sufficiency.* Let $t_1, \ldots, t_k$ be a D-orthonormal basis of W and $x = \lambda \sum_{i=1}^k f_i(t_i)$. Then

$$(gx, x) = |\lambda|^2 \sum_{i=1}^k (gf_i(t_i), f_i(t_i)) = \frac{|x|^2}{k} \sum_{i=1}^k (gt_i, t_i).$$

If W is complex or real and of the first kind then $\sum_{i=1}^k (gt_i, t_i) = \chi(g)$.

In the remaining two cases the arguments are similar. We consider only the case when W is real and of the second kind.

Let $e_i \in D$ $(0 \leqq i \leqq 3)$ satisfy $e_0 = 1$, $e_1e_2 = e_3$, $e_2e_3 = e_1$, $e_3e_1 = e_2$, $e_1^2 = e_2^2 = e_3^2 = -e_0$. Then

$$\begin{aligned}\sum_{i=1}^k (gt_i, t_i) &= \sum_{i=1}^k (ge_1t_i, e_1t_i) \\ &= \sum_{i=1}^k (ge_2t_i, e_2t_i) = \sum_{i=1}^k (ge_3t_i, e_3t_i).\end{aligned}$$

Since $4k = n$ and $4k$ vectors t_i, e_1t_i, e_2t_i, e_3t_i $(1 \leqq i \leqq k)$ form an orthonormal basis of W it follows that $\sum_{i=1}^k (gt_i, t_i) = \frac{1}{4}\chi(g)$.

Necessity. Let $x = x_1 + \cdots + x_k$, $x_i \in V_i$, and $t_i = f_i^{-1}(x_i)$. Let T be the representation of G afforded by W and End (W) the algebra of all linear transformations of W. The subalgebra of End (W) generated by $T(g)$, $g \in G$, coincides with the commuting algebra of D in End (W) (see Wedderburn's theorem, [2, p. 445]). Let $W = X \oplus Y$ be a direct decomposition of W as D-vector space where X is spanned by $t_1, \ldots, t_k$. Let P be the projector on Y with kernel X. Then P belongs to the subalgebra generated by $T(g)$, $g \in G$. Since

$$\sum_{i=1}^k (gt_i, t_i) = \frac{|x|^2}{n} \chi(g)$$

holds for all $g \in G$ we must have also

$$\sum_{i=1}^{k} (Pt_i, t_i) = \frac{|x|^2}{n} \operatorname{tr}(P).$$

Thus $\operatorname{tr}(P)=0$ and so $t_1, \ldots, t_k$ is a basis of W as D-vector space.

The rest of the proof depends on D. We shall only consider the case $D=\boldsymbol{H}$; the arguments are similar in other cases.

The vectors t_i, e_1t_i, e_2t_i, e_3t_i $(1 \leqq i \leqq k)$ form a basis of W as real vector space. Let A be a linear transformation of W as D-vector space. If $At_j=\sum_{i=1}^k \sigma_{ij}t_i$, $\sigma_{ij} \in \boldsymbol{H}$, $\sigma_{ij}=\alpha_{ij}^0e_0+\alpha_{ij}^1e_1+\alpha_{ij}^2e_2+\alpha_{ij}^3e_3$, $\alpha_{ij}^s \in \boldsymbol{R}$, then

$$Ae_it_j = e_iAt_j = e_i \sum_{r=1}^{k} \sum_{s=0}^{3} \alpha_{rj}^s e_s t_r.$$

By assumption we have $\sum_{j=1}^k (At_j, t_j)=(|x|^2/n) \operatorname{tr}(A)$, i.e.

$$\sum_{r,j=1}^{k} \sum_{s=0}^{3} \alpha_{rj}^s (e_s t_r, t_j) = \frac{|x|^2}{n} \sum_{j=1}^{k} \alpha_{jj}^0.$$

Since α_{ij}^s can be chosen arbitrarily this implies that $(e_st_r, t_j)=0$ if $r \neq j$ or $s \neq 0$, and $|t_1|=|t_2|=\cdots=|t_k|$. Thus x is principal.

Corollary 1. *Let V be as in the theorem. If $x \neq 0$ is strongly balanced then V is generated by x as G-module.*

Proof. Let X be the submodule of V generated by x. Then we can choose an orthogonal splitting $V=V_1 \oplus \cdots \oplus V_k$ into irreducible submodules so that $X=V_1 \oplus \cdots \oplus V_r$ for some r, $1 \leqq r \leqq k$. The theorem implies that $r=k$, i.e. $X=V$.

5. **Balanced vectors.** We need only to consider the complex case. Let W be an irreducible complex G-module. W is of the *first kind* if it is isomorphic to the complexification of a real irreducible G-module. It is of the *second kind* if it affords a real character but is not of the first kind. It is of the *third kind* if the character afforded by W is not real.

Theorem 6. *Let V be a complex G-module such that the real G-module V^0, obtained from V by restriction of scalars, is isomorphic to a homogeneous component of $\boldsymbol{R}G$. Then $x \in V$ is balanced in V if and only if it is principal in V^0.*

Proof. Note that the scalar product in V^0 is introduced by $(x, y)_0=\operatorname{Re}(x, y)$. Thus x is balanced in V if and only if it is balanced in V^0. The assertion now follows from Theorem 5.

If W is an irreducible complex G-module then there exists another irreducible complex G-module $\overline{W}$ such that the characters afforded by W and $\overline{W}$ are conjugate to each other. The module $\overline{W}$ is determined uniquely up to isomorphism. We shall say that $\overline{W}$ is the conjugate module of W. If W is of the first or second kind then $\overline{W} \cong W$. When W is of the third kind then $\overline{W}$ is not isomorphic to W.

If X and Y are complex vector space then an additive mapping $\sigma\colon X\to Y$ is called semilinear if $\sigma(\lambda x)=\bar{\lambda}\sigma(x)$ for all $x\in V$ and $\lambda\in \boldsymbol{C}$. Now let X and Y be complex G-modules. A semilinear mapping $\sigma\colon X\to Y$ is a semilinear G-isomorphism if it is bijective and satisfies the following two conditions:

$$(\sigma x, \sigma y) = (y, x), \qquad \forall x, y\in X,$$
$$\sigma(gx) = g(\sigma x), \qquad \forall x\in X, \forall g\in G.$$

We shall omit the proof of the following

THEOREM 7. *Let W be an irreducible complex G-module. Then there exists a semilinear G-isomorphism $\sigma\colon W\to \overline{W}$. It is unique up to a scalar factor of unit modulus.*

It is easy to see which complex G-modules V satisfy the condition of Theorem 6. Let W be an irreducible complex G-module and write $n=\dim W$.

If W is of the first kind and n is even, say $n=2k$, then we can take $V\cong kW$.

If W is of the second kind then n is even, say $n=2k$, and we can take $V\cong kW$.

If W is of the third kind we can choose an integer k $(0\leqq k\leqq n)$ arbitrarily and take $V\cong kW\oplus(n-k)\overline{W}$.

These examples exhaust all the possibilities for V (up to isomorphism).

In what follows we assume that V is the homogeneous component of type W of $\boldsymbol{C}G$ and that W is of the first kind. We shall determine all balanced vectors in V. In this case V (resp. W) is isomorphic to the complexification of a real G-module V^0 (resp. W^0). V^0 is isomorphic to the homogeneous component of type W^0 of $\boldsymbol{R}G$. If (x, y) is the scalar product in a real G-module then we equip its complexification with a scalar product defined by

$$(x_1+ix_2, y_1+iy_2) = (x_1, y_1)+(x_2, y_2)+i(x_2, y_1)-i(x_1, y_2)$$

where x_1, x_2, y_1, y_2 are vectors from the real G-module and i is the imaginary unit.

If $x\in V$ then we can write $x=y+iz$ where $y, z\in V^0$. Let $V^0=V_1\oplus\cdots\oplus V_n$ be an orthogonal splitting of V^0 into irreducible submodules. We fix a system $f_r\colon W^0\to V_r$ $(1\leqq r\leqq n)$ of G-isomorphisms. Then we can write $y=\sum_{r=1}^n f_r(y_r)$, $z=\sum_{r=1}^n f_r(z_r)$ where $y_r, z_r\in W^0$.

Using this notation we have

THEOREM 8. *Let V be the homogeneous component of type W of* $\boldsymbol{C}G$ *and assume that W is of the first kind. Let $e_1, \ldots, e_n$ be a fixed orthonormal basis of W^0 and $y_r=\sum_{s=1}^n \alpha_{sr}e_s$, $z_r=\sum_{s=1}^n \beta_{sr}e_s$. Then x is balanced if and only if* $\operatorname{Re}[(\gamma_{sr})(\gamma_{sr})^*]=\mu I$ *where $\gamma_{sr}=\alpha_{sr}+i\beta_{sr}$.*

Proof. The character χ afforded by W is real. If x is balanced in V then $\operatorname{Re}(gx, x)=(|x|^2/n)\chi(g)$. This can be written as $\sum_{r=1}^n [(gy_r, y_r)+(gz_r, z_r)]=\mu\chi(g)$ where $\mu=|x|^2/n$. Since W^0 is absolutely irreducible we have

$$\sum_{r=1}^{n} [(Ay_r, y_r)+(Az_r, z_r)] = \mu \operatorname{tr}(A)$$

for all linear transformations A.

We identify W^0 with its dual by using the scalar product. Thus we can identify $W^0 \otimes W^0$ with the space of linear mappings $W^0 \to W^0$. We have $(a \otimes b)(u) = (u, a)b$. Taking $A = a \otimes b$ we get

$$\sum_{r=1}^{n} [(y_r, a)(b, y_r) + (z_r, a)(b, z_r)] = \mu(b, a).$$

Since this holds for arbitrary b we must have

$$\sum_{r=1}^{n} [(y_r, a) y_r + (z_r, a) z_r] = \mu a.$$

Since this holds for all a we have

$$\sum_{r=1}^{n} (y_r \otimes y_r + z_r \otimes z_r) = \mu I.$$

Put $A = \sum_{r=1}^{n} y_r \otimes y_r$, $B = \sum_{r=1}^{n} z_r \otimes z_r$.

Then A and B are commuting positive semidefinite operators. Writing y_r and z_r as in the theorem we get

$$A = \sum_{s,t=1}^{n} \left(\sum_{r=1}^{n} \alpha_{sr}\alpha_{tr} \right) e_s \otimes e_t, \qquad B = \sum_{s,t=1}^{n} \left(\sum_{r=1}^{n} \beta_{sr}\beta_{tr} \right) e_s \otimes e_t.$$

Since $A + B = \mu I$ the theorem is proved.

References

1. C. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience, New York, 1966.

2. S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965. MR **33** #5416.

3. J.-P. Serre, *Représentation linéaires des groupes finis*, Hermann, Paris, 1967. MR **38** #1190.

4. D. Slepian, *Group codes for the Gaussian channel*, Bell System Tech. J. **47** (1968), 575–602. MR **38** #6879.

Faculty of Mathematics, University of Waterloo, Waterloo, Ontario, Canada

Department of Electrical Engineering, University of Waterloo, Waterloo, Ontario, Canada