PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 42, Number 1, January 1974

A THEOREM OF HURWITZ AND RADON AND ORTHOGONAL PROJECTIVE MODULES[1]

A. V. GERAMITA AND N. J. PULLMAN

ABSTRACT. We find the maximum number of orthogonal skew-symmetric anticommuting integer matrices of order n for each natural number n and relate this to finding free direct summands of certain generic projective modules.

While studying composition of quadratic forms, Hurwitz [4] and Radon [6] considered families of orthogonal matrices $\{A_1, \cdots, A_s\}$ satisfying the conditions

$$A_i = -A_i^t, \qquad i = 1, \cdots, s \tag{1}$$

$$A_iA_j = -A_jA_i, \qquad i \neq j. \tag{2}$$

DEFINITION. (1) A family of orthogonal matrices satisfying (1) and (2) above will be called a *Hurwitz-Radon* (H-R) *family*.

If n is a positive integer and $n=2^ab$, b odd, then we write $a=4c+d$ where $0 \leqq d < 4$. If we denote by $\rho(n)$ the number $8c+2^d$ the main theorem of Radon states:

THEOREM A [6]. (1) *Any H-R family of real matrices of order n has fewer than* $\rho(n)$ *members.*

(2) *There is an H-R family of real matrices of order n having exactly* $\rho(n)-1$ *members.*

In the first section we prove an analogous theorem for integer matrices and in §II we consider some applications to the study of projective modules.

We are indebted to R. Gabel for having furnished us with a copy of his Brandeis thesis. The ideas studied here were inspired by that work and represent a simplification and extension of one part of that thesis. Gabel

---

Presented to the Society, November 25, 1972; received by the editors September 7, 1972 and, in revised form, January 30, 1973.

AMS (MOS) subject classifications (1970). Primary 15A36, 15A63, 10J05, 13C10.

Key words and phrases. Anticommuting skew-symmetric orthogonal matrices, integer matrices, projective modules.

[1] This research was supported in part by National Research Council of Canada Grants A8488 and A4041.

has independently extended this part of his thesis. His presentation of these results will appear in a separate paper in the Journal of Algebra.

I. **Hurwitz-Radon theorem for integer matrices.** In order to extend Theorem A to integer matrices it is sufficient to show that for every integer n there is an H-R family of integer matrices of order n having exactly $\rho(n)-1$ members.

If

$$A=\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad P=\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } \quad Q=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

then

(a) $\{A\}$ is an H-R family of $\rho(2)-1$ integer matrices of order 2;

(b) $\{A\otimes I_2, P\otimes A, Q\otimes A\}$ is an H-R family of $\rho(4)-1$ integer matrices of order 4, and

(c) $\{I_2\otimes A\otimes I_2,\ I_2\otimes P\otimes A,\ Q\otimes Q\otimes A,\ P\otimes Q\otimes A,\ A\otimes P\otimes Q,\ A\otimes P\otimes P,\ A\otimes Q\otimes I_2\}$ is an H-R family of $\rho(8)-1$ integer matrices of order 8.

THEOREM 1. *There is an H-R family of integer matrices of order n having $\rho(n)-1$ members.*

PROOF. Suppose that $\{M_1, \cdots, M_s\}$ is an H-R family of integer matrices of order n, then

(1) $\{A\otimes I_n\}\cup\{Q\otimes M_i \mid i=1, \cdots, s\}$ is an H-R family of $s+1$ integer matrices of order $2n$.

(2) If $\{L_1, \cdots, L_m\}$ is an H-R family of integer matrices of order k,

$$\{P\otimes I_k\otimes M_i \mid 1\leqq i\leqq s\}\cup\{Q\otimes L_j\otimes I_n \mid 1\leqq j\leqq m\}\cup\{A\otimes I_{nk}\}$$

is an H-R family of $s+m+1$ integer matrices of order $2nk$.

That the matrices are orthogonal and skew-symmetric follows from the fact that $(A\otimes B)^t=A^t\otimes B^t$. The members of these families anticommute because the product of any two distinct members is skew-symmetric.

To prove the theorem it is enough to note that a, b, and c take care of the cases $n=2, 4, 8$, then (1) gives $n=16$ and (2) gives the transition from n to $16n$ (with $k=8$, $m=7$). The transition from $n=2^a$ to $n=2^ab$, b odd, is given by $\otimes I_b$.

Suppose D is a commutative domain in which $2\neq 0$. Since the H-R families constructed above have as entries only 0, 1 and -1, they exist as H-R families over D. Therefore $\rho(n)-1$ gives a lower bound for the maximum number of members in any H-R family of matrices over D of order n.

II. **Applications to the study of projective modules.** In this section all rings considered will be commutative with identity and modules will be unitary and finitely generated.

DEFINITION. (2) An R-module P is called *stably free* if there are integers m, n such that $P \oplus R^m \simeq R^n$. In such an instance, we say that P is stably free of *type* (m, n).

We first note that the "type" of a stably free module is in no way uniquely determined by the module. Also note that a stably free R-module of type (m, n) is nothing more than a projective R-module which can be realized as the kernel of an epimorphism from R^n to R^m.

The following three definitions and the proposition following them may all be found in Gabel [3] where these notions were first formulated.

DEFINITION. (3) A stably free R-module P is called *orthogonal* if $P \simeq \ker \alpha$ where $\alpha: R^n \to R^m$ is an epimorphism and $\alpha\alpha^t = 1_{R^m}$. (We are freely considering homomorphisms of free modules as matrices and then "t" denotes transpose.)

Note that if we let L be R with the quadratic form $x \mapsto x^2$ then α^t embeds R^m into L^n as a nonsingular submodule whose orthogonal complement is isomorphic to P. The quadratic structure on P is the one induced by the quadratic structure on L^n. (For details see Bass [2].) On the other hand if P is a quadratic module such that $P \oplus L^m \simeq L^n$ (where the sum is orthogonal and the isomorphism preserves the quadratic forms) then P is an orthogonal projective module. These remarks then constitute an alternative definition of orthogonal projective modules which we shall have occasion to use.

DEFINITION. (4) Let R be a ring; m, n integers where $m \leqq n$, and $\{X_{ij}\}$, $1 \leqq i \leqq m$, $1 \leqq j \leqq n$, a doubly indexed set of indeterminates. We define the R-algebra

$$R^0_{m,n} = R[X_{11}, \cdots, X_{ij}, \cdots, X_{m,n}]/I^0_{m,n}(R)$$

where $I^0_{m,n}(R)$ is the ideal of $R[X_{11}, \cdots, X_{ij}, \cdots, X_{m,n}]$ generated by the m^2 elements of the $m \times m$ matrix $[X_{ij}][X_{ij}]^t$—(the $m \times m$ identity matrix).

(5) We define $\alpha^0_{m,n}(R): (R^0_{m,n})^n \to (R^0_{m,n})^m$ by the matrix $[\bar{X}_{ij}]$ (the "$\bar{\ }$" denotes the canonical images of the X_{ij} in $R^0_{m,n}$) and set $P^0_{m,n}(R) = \ker \alpha^0_{m,n}(R)$.

The following proposition indicates the significance of these definitions.

PROPOSITION 1. (1) *$\alpha^0_{m,n}(R)$ is an epimorphism and $P^0_{m,n}(R)$ is an orthogonal stably free $R^0_{m,n}$-module of type (m, n).*

(2) *If $R \to S$ is a ring homomorphism then there is a canonical R-algebra map $R^0_{m,n} \to S^0_{m,n}$ such that $P^0_{m,n}(R) \otimes_{R^0_{m,n}} S^0_{m,n} \simeq P^0_{m,n}(S)$ as $S^0_{m,n}$-modules.*

(3) *If S is any R-algebra and P is a stably free orthogonal S-module of type (m, n) then there is a canonical R-algebra map $R^0_{m,n} \to S$ such that $P^0_{m,n}(R) \otimes_{R^0_{m,n}} S \simeq P$ as S-modules.*

EXAMPLE. Let R denote the real number field, then

$$R^0_{1,n} = R[X_1, \cdots, X_n] \Big/ \left(\sum_{i=1}^{n} X_i^2 - 1\right)$$

and

$$P^0_{1,n}(R) = \ker \alpha,$$

where $\alpha = [\bar{X}_1, \cdots, \bar{X}_n] : (R^0_{1,n})^n \to R^0_{1,n}$. Let $\mathscr{C}_R(S^{n-1})$ denote the ring of continuous real-valued functions on S^{n-1}. We may consider $R^0_{1,n} \subset \mathscr{C}_R(S^{n-1})$ and then via the inclusion map we have $P^0_{1,n}(R) \otimes_{R^0_{1,n}} \mathscr{C}(S^{n-1}) = \bar{P}$, which may be identified with the module of cross sections of the tangent bundle to S^{n-1} [8].

REMARKS. (1) If we let Z denote the rational integers then if R is any ring it is a Z-algebra and there is a ring homomorphism $Z \to R$. By part (3) of Proposition 1 any orthogonal projective R-module can be obtained from a $P^0_{m,n}(Z)$, for appropriate m, n, by a base change. This justifies our calling $P^0_{m,n}(Z)$ the *generic*, orthogonal, stably free projective of type (m, n).

(2) If we consider only the family of rings which are K-algebras for some commutative ring K, then the modules $P^0_{m,n}(K)$ are "generic" for the orthogonal projectives of type (m, n) over rings in this family. We will thus abusively refer to all the modules $P^0_{m,n}(R)$, for any ring R, as generic.

(3) If R is any commutative ring and $Z \to R$ a ring homomorphism then by part (2) of Proposition 1 we have $P^0_{m,n}(Z) \otimes_{Z^0_{m,n}} R^0_{m,n} \simeq P^0_{m,n}(R)$. So if $P^0_{m,n}(R)$ is *not* free for any ring R then $P^0_{m,n}(Z)$ is not free. On the other hand if $P^0_{m,n}(Z)$ has a free summand of rank r then so does $P^0_{m,n}(R)$ for every commutative ring R.

The next proposition gives us a way of relating various generic projectives.

PROPOSITION 2. *There is a ring homomorphism* $R^0_{m+1,n+1} \to R^0_{m,n}$ *such that*

$$P^0_{m+1,n+1}(R) \underset{R^0_{m+1,n+1}}{\otimes} R^0_{m,n} \xrightarrow{\simeq} P^0_{m,n}(R).$$

PROOF. We send $R \to R$ by the identity map and $X_{ij} \to X_{ij}$ for $1 \leqq i \leqq m$, $1 \leqq j \leqq n$. We send $X_{m+1,n+1} \to 1$ and $X_{m+1,k} \to 0$ for $1 \leqq k \leqq n$ and $X_{l,n+1} \to 0$ for $1 \leqq l \leqq m$. This gives a map $R[X_{rs}] \to R[X_{uv}]$ for $1 \leqq r \leqq m+1$, $1 \leqq s \leqq n+1$, $1 \leqq u \leqq m$, $1 \leqq v \leqq n$ which takes $I^0_{m+1,n+1}(R)$ into $I^0_{m,n}(R)$ and so defines a map $\phi : R^0_{m+1,n+1} \to R^0_{m,n}$. The proof now follows exactly as in Raynaud [7, Proposition 2.4].

COROLLARY. *If $R=\boldsymbol{R}$ or Z then $P^0_{m,n}(R)$ is not free except possibly if $n-m=1, 3, 7$.*

PROOF. By repeated use of Proposition 1 we have

$$P^0_{m,n}(R) \underset{R^0_{m,n}}{\otimes} R^0_{1,n-m+1} \simeq P^0_{1,n-m+1}(R).$$

So $P^0_{m,n}(R)$ can be free only when $P^0_{1,n-m+1}(R)$ is free. It is known [8] that $P^0_{1,n-m+1}(\boldsymbol{R})$ is free precisely when $n-m+1=2$, 4, or 8. Thus, $P^0_{1,n-m+1}(Z)$ can be free only if $n-m+1=2, 4, 8$.

REMARKS. (1) If $n-m=1$ then $P^0_{m,n}(R)$ is free for any ring R since then it is a stably free projective $R^0_{m,n}$-module of rank one.

(2) We shall show that $P^0_{1,4}(Z)$ and $P^0_{1,8}(Z)$ are free, (Corollary 1 to Theorem 3) but if $m>1$ we have no results about the freeness of $P^0_{m,n}(Z)$ for $n-m=3$, 7. Some results of James [5] seem to be relevant here. Also, the referee has kindly pointed out that the paper of Raynaud cited above can also be applied here. In particular he states that $R^0_{m,n}$ represents the scheme SO_n/SO_{n-m}. The relation between sections and summands of $P^0_{m,n}(R)$ then applies and Raynaud's results on the nonexistence of sections for $SO_{2n+1} \to SO_{2n+1}/SO_{2n-1}$ give results on $P^0_{m,n}(R)$, at least if $\frac{1}{2}$ and $\sqrt{-1} \in R$. (The SO_n needed here is the one for the quadratic form $X_1^2+\cdots+X_n^2$, not the split SO_n.)

(3) If C denotes the field of complex numbers, then $P^0_{1,n}(C)$ is free $\forall n$ [8].

(4) It is an easy exercise to show that if R has characteristic $=2$ then $P^0_{1,n}(R)$ is free $\forall n$.

If we cannot have freeness for a generic orthogonal projective we may then ask about free summands in general.

DEFINITION. If M is an R-module let $\rho(M) \in Z$ be the supremum of the ranks of the free summands of M.

By Proposition 1 we have $\rho(P^0_{m,n}(Z)) \leqq \rho(P^0_{m,n}(R))$ and by Proposition 2 $\rho(P^0_{m,n}(R)) \leqq \rho(P^0_{1,n-m+1}(R))$ for any commutative ring. We shall find $\rho(P^0_{1,k}(Z))$ for every integer k. This will generalize the results of [3] in this direction.

If we let $\Gamma(\tau^n)$ denote the $\mathscr{C}_R(S^n)$-module of cross sections of the tangent bundle τ^n of S^n, then we have noted that this module is an orthogonal projective of type $(1, n+1)$. Thus by Proposition 1, part (3), $\rho(P^0_{1,n+1}(Z)) \leqq \rho(\Gamma(\tau^n))$.

THEOREM 2 [1]. $\rho(\Gamma(\tau^n))=\rho(n+1)-1$.

PROOF. This is nothing more than a restatement of Adams' celebrated theorem solving the vector field problem for spheres.

We thus have $\rho(P^0_{1,n}(Z)) \leqq \rho(n)-1$. The next theorem will allow us to change this inequality into equality.

THEOREM 3. *Let R be a commutative ring in which 2 is not a zero divisor. Let $P \oplus L \simeq L^n$ (where L is as in the remarks following Definition 3). If $A_1, \cdots, A_s$ are an H-R family of $n \times n$ matrices then $\rho(P) \geqq s$.*

PROOF. We shall consider the isomorphism above as an identification, then the summand L on the left has the form aR where $a \in L^n$ and $P = (aR)^\perp$ in L^n. Since $A_1, \cdots, A_s$ are an H-R family of $n \times n$ matrices they are, in particular, invertible. Thus since $a \in L^n$ is unimodular, so are $aA_1, aA_2, \cdots, aA_s$. Furthermore $a, aA_1, \cdots, aA_s$ are mutually orthogonal since 2 is not a zero divisor in R and the matrices $A_1, \cdots, A_s$ are an H-R family. Thus $aA_1, \cdots, aA_s \in (aR)^\perp = P$ and hence $P = (aA_1) \oplus \cdots \oplus (aA_s) \oplus Q$. Thus $\rho(P) \geqq s$ as was to be shown.

(*Note.* We would like to thank the referee for his proof of Theorem 3 which is much more efficient than our original proof.)

COROLLARY. $\rho(P^0_{1,n}(Z)) = \rho(n)-1$.

PROOF. We have already remarked that we only needed to show $\rho(P^0_{1,n}(Z)) \geqq \rho(n)-1$ and the corollary now follows immediately from Theorems 1 and 3.

BIBLIOGRAPHY

1. J. F. Adams, *Vector fields on spheres*, Ann. of Math. (2) **75** (1962), 603–632. MR **25** #2614.

2. H. Bass, *Modules which support nonsingular forms*, J. Algebra **13** (1969), 246–252. MR **39** #6875.

3. M. R. Gabel, *Stably free projectives over commutative rings*, Brandeis University, Waltham, Mass., Thesis, February 1972.

4. A. Hurwitz, *Über die Komposition der Quadratischen Formen*, Math. Ann. **88** (1923) 1–25.

5. I. M. James, *Cross-sections of Stiefel manifolds*, Proc. London Math. Soc. (3) **8** (1958), 536–547. MR **20** #7268.

6. J. Radon, *Lineare Scharen Orthogonaler Matrizen*, Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, Vol. 1, 1922, 1–14.

7. M. Raynaud, *Modules projectifs universels*, Invent. Math. **6** (1968), 1–26. MR **38** #4462.

8. R. G. Swan, *Vector bundles and projective modules*, Trans. Amer. Math. Soc. **105** (1962), 264–277. MR **26** #785.

DEPARTMENT OF MATHEMATICS, QUEEN'S UNIVERSITY AT KINGSTON, ONTARIO, CANADA