Linear and Multilinear Algebra, 1987, Vol. 20, pp. 247–251
Photocopying permitted by license only

Printed in the United States of America

Matrices as the Sum of Four Squares

ANDREW J. GRANVILLE
Queens University, Kingston, Ontario, Canada K7L 3N6

(*Received December 9, 1985; in final form May 14, 1986*)

For each $n \geqslant 2$, every integral $n \times n$ matrix is the sum of at most four squares.

INTRODUCTION

Let R be a given ring, and $M(n, R)$ the set of $n \times n$ matrices with entries in R. For each $M \in M(n, R)$ we let $k = k(M)$ be the minimum number of matrices $A_1, A_2, \ldots, A_k \in M(n, R)$ needed so that $M = A_1^2 + A_2^2 + \cdots + A_k^2$. Newman [3] has conjectured that if R is the ring of rational integers then, for each $n \geqslant 2$, and $M \in M(n, R)$ we have $k(M) \leqslant 3$. In this paper we construct matrices A_i to show that $k(M) \leqslant 4$; this improves on the result of Newman [3] who showed that if $M \in M(n, R)$ then $k(M) \leqslant 7$ (for n even), $\leqslant 9$ (for n odd). $k(M) = 3$ has been confirmed for $n = 2$ by Carlitz [1], and for $n = 3$ and 4 by Griffin and Krusemeyer [2].

In fact, by slightly altering the algorithm presented here, it is possible to prove the following result:

Suppose that R is a ring with a 1, such that every element of the quotient ring $R/2R$ can be expressed as the sum of at most N squares. If $n \geqslant \max(N, 3)$ and $M \in M(n, R)$ then M can be expressed as the sum of four squares in $M(n, R)$.

If R is a field then the problem of sums of squares of matrices is more completely resolved. Griffin and Krusemeyer [2] showed that any matrix over a field R can be expressed as the sum of three squares, and that this is the best possible result. Richman [4] showed that the only matrices in $M(n, R)$ that can not be expressed as the sum of two squares

are those of the form cI_n, where c is not expressible as the sum of two squares in R.

LEMMA 1 *For any integer r there exists integers x, y, z such that $r = x^2 - y^2 + z^2$.*

Proof If r is even let $z = 1$; if r is odd let $z = 0$, so that $t = r - z^2$ is odd. Then let $x = (t + 1)/2$ and $y = (t - 1)/2$.

LEMMA 2 *Any 2×2 integer matrix is expressible as the sum of three squares.*

Proof Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be any integer 2×2 matrix. For

$a - d \equiv$	$0 \bmod 2$	$3 \bmod 4$	$1 \bmod 4$

let

$v =$	0	0	1
$w =$	1	1	0
$x =$	$1 + (a - d)/2$	$(a - d + 5)/4$	$(a - d + 3)/4$
$y =$	$(a - d)/2$	$(a - d - 3)/4$	$(a - d - 5)/4$
$z =$	$d - bc - 1 - y^2$	$d - bc - 1 - y^2$	$d - bc - y^2$

Then

$$M = \begin{pmatrix} v & b \\ c & w \end{pmatrix}^2 + \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}^2 + \begin{pmatrix} 0 & 1 \\ z & 0 \end{pmatrix}^2.$$

LEMMA 3 *For all $n \geqslant 2$, $k(-I_n) \geqslant 3$.*

Proof Richman ([4], Theorem 6) has shown that if K is a field, char $K \neq 2$ then cI_n can be expressed as the sum of two squares of matrices, with entries in the field, if and only if c can be expressed as the sum of two squares in the field.

Now if $-I_n$ can be expressed as the sum of two squares, with integer entries, then it can certainly be expressed as the sum of two squares, with entries in the field of rationals. Thus there exist rational numbers a and b such that $-1 = a^2 + b^2$, which is clearly impossible.

Therefore the least number of squares we need to represent $-I_n$ is 3.

LEMMA 4 *For $n \geqslant 3$, any integer $n \times n$ matrix is expressible as the sum of four squares.*

Proof Suppose that M is a given $n \times n$ matrix, with integer entries, labelled $m_{i,j}$. We will define an integer $n+1 \times n+1$ matrix A, and use this to establish the result.

Now, by Lemma 1, we know that there exists integers $a_{1,1}, a_{2,2}, a_{3,3}$ such that

$$\sum_{i=1}^{n} (-1)^{i+1} m_{i,i} + (-1)^n .2 = a_{1,1}^2 - a_{2,2}^2 + a_{3,3}^2.$$

Define $a_{i,i} = 0$ for $4 \leqslant i \leqslant n+1$ and $a_{i,i+1} = 0$ for $1 \leqslant i \leqslant n$.

We now define, by induction on d, the values of $a_{i,i-d-1}$ (for $d+2 \leqslant i \leqslant n+1$, $0 \leqslant d \leqslant n-1$) and of $a_{i,i+d+1}$ (for $1 \leqslant i \leqslant n-d$, $1 \leqslant d \leqslant n-1$); we do this by considering certain values of $m'_{i,i-d}$ ($d \geqslant 0$) and $m'_{i,i+d}$ ($d \geqslant 1$), which depend on $a_{i,j}$ where $|i-j| \leqslant d$ (i.e. these values are already known under the induction hypothesis). Let

$$\begin{aligned}
m'_{i,i} &= m_{i,i} - a_{i,i}^2 && (1 \leqslant i \leqslant n-1)\\
&= m_{n,n} - a_{n,n}^2 - 2 && (i = n)\\
m'_{i,i-1} &= m_{i,i-1} - (a_{i,i} + a_{i-1,i-1}) && (2 \leqslant i \leqslant n)\\
m'_{i,i-2} &= m_{i,i-2} - (a_{i,i-1} \cdot a_{i-1,i-2} + 1) && (3 \leqslant i \leqslant n)\\
m'_{i,i-d} &= m_{i,i-d} - \sum_{k=i-d+1}^{i-1} a_{i,k} \cdot a_{k,i-d} && (3 \leqslant d \leqslant n-1, d+1 \leqslant i \leqslant n)\\
m'_{i,i+1} &= m_{i,i+1} && (1 \leqslant i \leqslant n-1)\\
m'_{i,i+2} &= m_{i,i+2} - 1 - a_{i,i+2} \cdot (a_{i,i} + a_{i+2,i+2}) && (1 \leqslant i \leqslant n-2)\\
m'_{i,i+d} &= m_{i,i+d} - \sum_{k=i+1}^{i+d-1} a_{i,k} \cdot a_{k,i+d}\\
&\quad - a_{i,i+d} \cdot (a_{i,i} + a_{i+d,i+d}) && (3 \leqslant d \leqslant n-1, 1 \leqslant i \leqslant n-d).
\end{aligned}$$

Then let

$$a_{i,i-d-1} = \sum_{j=d+1}^{i-1} (-1)^{i+j+1} m'_{j,j-d} \quad (0 \leqslant d \leqslant n-1, d+2 \leqslant i \leqslant n+1)$$

and

$$a_{i,i+d+1} = \sum_{j=1}^{i} (-1)^{i+j} m'_{j,j+d} \qquad (1 \leqslant d \leqslant n-1, 1 \leqslant i \leqslant n-d).$$

So we have completely defined the matrix A, and each entry is an integer. We will take $a_{i,0} = a_{0,i} = 0$ for each i, and we note that

$$a_{n+1,n} = \sum_{j=1}^{n} (-1)^{n+j}(m_{j,j} - a_{j,j}^2) - 2 = 0.$$

We now define 4 $n \times n$ matrices R, S, T, V as follows:

$(R)_{i,j} = a_{i,j}$ $(i > j)$, 1 $(i = j - 1)$, 0 (otherwise)

$(S)_{i,j} = a_{i,j}$ $(i \leqslant j)$, 1 $(i = j + 1)$, 0 (otherwise)

$(T)_{i,j} = a_{i,n+1}$ $(j = n, i < n)$, 1 $(i = j = n)$, 0 (otherwise)

$(V)_{i,j} = a_{n+1,j}$ $(i = n, j < n)$, 1 $(i = j = n)$, 0 (otherwise).

Then, for $d \geqslant 0$, we have

$$\begin{aligned}(R^2 + S^2 + T^2 + V^2)_{i,i-d} &= m_{i,i-d} - m'_{i,i-d} \\ &\quad + a_{i,i-d-1} + a_{i+1,i-d} \\ &= m_{i,i-d} - m'_{i,i-d} \\ &\quad + \sum_{j=d+1}^{i-1} (-1)^{i+j+1} m'_{j,j-d} \\ &\quad + \sum_{j=d+1}^{i} (-1)^{i+j} m'_{j,j-d} \\ &= m_{i,i-d}.\end{aligned}$$

Also, for $d > 1$, we have,

$$\begin{aligned}(R^2 + S^2 + T^2 + V^2)_{i,i+d} &= m_{i,i+d} - m'_{i,i+d} \\ &\quad + a_{i-1,i+d} + a_{i,i+d+1} \\ &= m_{i,i+d} - m'_{i,i+d} \\ &\quad + \sum_{j=1}^{i-1} (-1)^{i-1+j} m'_{j,j+d} \\ &\quad + \sum_{j=1}^{i} (-1)^{i+j} m'_{j,j+d} \\ &= m_{i,i+d}.\end{aligned}$$

Thus

$$M = R^2 + S^2 + T^2 + V^2.$$

From Lemmas 2 and 4 we get the following Theorem:

THEOREM *For any $n \geqslant 2$, any integral $n \times n$ matrix can be expressed as the sum of four squares.*

It is possible to prove Lemma 4, for n even, very easily using the following Theorem of Newman [3, Corollary 2].

Let A be any integral $n \times n$ matrix. Then there exist integral $n \times n$ matrices B and C such that $A \equiv B^2 + C^2 \bmod 2$.

LEMMA 5 *For any even integer n, every integral $n \times n$ matrix is expressible as the sum of four squares.*

Proof Let $n = 2k$ and $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ be a given $n \times n$ matrix, where A, B, C, D are the $k \times k$ blocks.

By Newman's Theorem there exist $k \times k$ integral matrices R, S, T such that

$$A + CB - BC - D = R^2 - S^2 + 2T.$$

Let $U = D - I - CB - S^2 - T^2$. Then

$$M = \begin{pmatrix} 0 & B \\ C & I \end{pmatrix}^2 + \begin{pmatrix} R & 0 \\ 0 & S \end{pmatrix}^2 + \begin{pmatrix} 0 & U \\ I & 0 \end{pmatrix}^2 + \begin{pmatrix} T+I & 0 \\ 0 & T \end{pmatrix}^2.$$

In a forthcoming paper David Richman considers matrices in commutative rings with a 1, as sums of nth powers, and proves some remarkable results as to the number of nth powers needed. Indeed he also proves the main theorem of this paper, though using a slightly different construction.

After the work was completed, the author learnt that L. Vaserstein has proved that three squares are sufficient for integer matrices. However, as stated in the introduction, it is possible to adapt the proof given here to many other rings (especially non-commutative rings).

References

[1] L. Carlitz, Solution to problem 140, *Can. Math. Bull.* **11** (1968), 615–619.
[2] M. Griffin and M. Krusemeyer, Matrices as sums of squares, *Linear and Multilinear Algebra* **5** (1977), 33–44.
[3] M. Newman, Sums of squares of matrices, *Pacific J. Math.* **118** (1985), 497–506.
[4] D. Richman, Matrices as sums of squares; a conjecture of Griffin and Krusemeyer, *Linear and Multilinear Algebra* **17** (1985), 289–294.