BULLETIN 13 (3), 1970

ON SETS OF TERNARY VECTORS WHOSE ONLY LINEAR DEPENDENCIES INVOLVE AN ODD NUMBER OF VECTORS

BY
E. R. BERLEKAMP

ABSTRACT. Recent efforts to generalize a classic result of Hajos [3] on the decomposition of finite abelian groups into direct sums of subsets (see Fuchs [1, Chap. XV]) led B. Gordon [2] to the following conjecture. If $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_M$ are r-dimensional row vectors over $GF(3)$ such that: (i) Any weighted ($\pm$) sum of any even number of $\vec{v}$'s is nonzero. (ii) For each r-dimensional $\vec{y}$, there exists an s such that

$$\vec{v}_s \cdot \vec{y}^t = 0.$$

Then there exists a subset of either 1 or 4 $\vec{v}$'s which satisfies the same conditions.
This paper proves Gordon's conjecture.

THEOREM 1. *Every nonzero vector in the row space of a $k \times n$ matrix with linearly independent rows over* GF(3) *has odd weight iff the matrix contains an odd number of each of the possible* $(3^k-1)/2$ *classes of nonzero columns* (*classes equivalent with respect to multiplication by* ± 1).

Proof. The 'if' clause follows immediately from the fact that the weight of every vector is the sum of $(3^k-1)/2-(3^{k-1}-1)/2=3^{k-1}$ odd numbers.

We prove the 'only if' clause by induction on k. Let $\vec{a}$ be an arbitrary k-dimensional vector over GF(3), and let $n_{\vec{a}}$ be the number of columns of $\mathcal{M}$ which are equal to $\vec{a}^t$.

We first consider the case $k=2$. The weights w_1, w_2, w_+, and w_- of the first row, the second row, the sum of the two rows, and the difference of the two rows are then given by

$$\begin{bmatrix} w_1 \\ w_2 \\ w_+ \\ w_- \end{bmatrix} = \begin{bmatrix} 00 & 11 & 11 & 11 \\ 11 & 00 & 11 & 11 \\ 11 & 11 & 00 & 11 \\ 11 & 11 & 11 & 00 \end{bmatrix} \begin{bmatrix} n_{[0,1]} \\ n_{[0,-1]} \\ n_{[1,0]} \\ n_{[-1,0]} \\ n_{[1,-1]} \\ n_{[-1,1]} \\ n_{[1,1]} \\ n_{[-1,-1]} \end{bmatrix}.$$

Received by the editors January 14, 1969.

Since the binary equations

$$\begin{bmatrix}0111\\1011\\1101\\1110\end{bmatrix}\begin{bmatrix}x\\y\\z\\w\end{bmatrix}=\begin{bmatrix}1\\1\\1\\1\end{bmatrix}$$

have the unique solution $x=y=z=w=1$ over GF(2), we conclude that if w_1, w_2, w_+, and w_- are all odd, then $n_{[0,1]}+n_{[0,-1]}$, $n_{[1,0]}+n_{[-1,0]}$, $n_{[1,-1]}+n_{[-1,1]}$, and $n_{[1,1]}+n_{[-1,-1]}$ are also odd. This proves the theorem for $k=2$.

We now assume that the theorem is true for all $k<K$. Let $\vec{u}$ be the bottom row of $\mathscr{M}$, and let $\vec{v}$ be an arbitrary vector in the space spanned by the first $K-1$ rows of $\mathscr{M}$. Applying the theorem to the $2\times n$ matrix whose rows are $\vec{v}$ and $\vec{u}$ reveals that the total weight of $\vec{v}$ in those columns in which $\vec{u}$ has 0 must be odd.

Let $\mathscr{M}'$ be the submatrix of $\mathscr{M}$ consisting of those n' columns which have a 0 in the bottom row, and let $\mathscr{M}''$ be the $K-1\times n'$ matrix consisting of the top $K-1$ rows of $\mathscr{M}'$. Then every nonzero vector in the row space of $\mathscr{M}''$ must have odd weight. Since this matrix has only $K-1$ rows, this implies that $\mathscr{M}''$ contains each possible $(3^{K-1}-1)/2$ nonzero classes of columns an odd number of times. Transforming back to $\mathscr{M}$, this implies that if $\vec{a}=[a_1, a_2, \ldots, a_K]$ and if $a_K=0$ but $\vec{a}\neq\vec{0}$, then $n_{\vec{a}}+n_{-\vec{a}}$ is odd.

If $\mathscr{B}$ is an invertible $K\times K$ matrix over GF(3), and if we let $\mathscr{M}'''=\mathscr{B}\mathscr{M}$, then $n'''_{\mathscr{B}\vec{a}}=n_{\vec{a}}$. Applying the previous arguments to $\mathscr{M}'''$ reveals that if the last component of $\mathscr{B}\vec{a}$ is 0, then $n_{\vec{a}}+n_{-\vec{a}}$ is odd. But since $\mathscr{B}$ is an arbitrible invertible matrix, n_a $+n_{-\vec{a}}$ must be odd for all nonzero $\vec{a}$. Q.E.D.

THEOREM 2. *Let $\mathscr{D}$ be a $k\times(3^k-1)/2$ matrix over* GF(3), *all of whose columns are nonzero and not equal to $\pm$ each other. Then if $k=1$ or 2, all solutions of the equation*

$$\mathscr{D}\vec{x}=\vec{0}$$

have some zero component(s), but if $k\geq 3$, then the equation

$$\mathscr{D}\vec{x}=\vec{0}$$

has a solution $\vec{x}$ which has only nonzero components.

LEMMA. *The only solutions of the equation $2^i+1=3^j$ are $i=1, j=1$, and $i=3, j=2$.*

Proof of Lemma. The multiplicative order of 2 mod 3^j is $2\cdot 3^{j-1}$. If $2^i\equiv -1 \bmod 3^j$, then $2^{2i}\equiv 1 \bmod 3^j$, $2\cdot 3^{j-1}$ must divide $2i$, and $3^{j-1}\leq i$. On the other hand, if $2^i\leq 3^j$, then $i\leq(\log_2 3)j$. Since we then have $3^{j-1}\leq j(\log 3)$, we conclude that $j\leq 2$. Q.E.D.

Proof of Theorem 2. The theorem is easily checked for $k=1$ or 2. For $k\geq 3$, we shall construct a matrix $\mathscr{D}$ such that

$$\mathscr{D}\vec{1}^t=\vec{0}$$

https://doi.org/10.4153/CMB-1970-068-8 Published online by Cambridge University Press

where $\vec{1}=[1, 1, 1, \ldots, 1]$. From this, we can obtain a completely nonzero vector in the null space of any other legitimate $\mathscr{D}$ matrix by changing signs of corresponding columns of $\mathscr{D}$ and components of $\vec{x}$, and then by appropriately permuting the columns of $\mathscr{D}$.

To construct the $\mathscr{D}$ matrix, we shall select $n=(3^k-1)/2$ elements from the Galois field GF(3^k), such that the elements are all distinct, not zero, and not equal to the negatives of each other, and such that their sum is zero. By representing each of these elements as a k-dimensional column vector over GF(3) with respect to any appropriate basis of GF(3^k) over GF(3), we may then obtain the desired $\mathscr{D}$ matrix.

The n elements of GF(3^k) are chosen as follows: Write $2n=3^k-1=2^m j$, where j is odd. According to the Lemma, $j>1$. Let α be a primitive element of GF(3^k), and select the n elements α^{l+i2^m}, $0\le l<2^{m-1}$, $0\le i<j$. Since the first $2n$ powers of α are distinct, no two of these n elements are equal. If $-\alpha^{l'+i'2^m}=\alpha^{l+i2^m}$, then

$$\begin{aligned}(l-l')+(i-i')2^m &\equiv 2^{m-1}j \bmod 2^m j,\\ (l-l') &\equiv 2^{m-1} \bmod 2^m,\\ l &\equiv l' \bmod 2^{m-1},\\ l &= l',\\ 0 &\equiv 2^{m-1} \bmod 2^m.\end{aligned}$$

Since this is a contradiction, we conclude that *no* element in our set is the negative of any other element in our set. Finally, we check that

$$\left(\sum_{l=0}^{2^{m-1}-1}\alpha^l\right)\left(\sum_{i=0}^{j-1}\alpha^{i2^m}\right)=0$$

because the sum of the jth roots of unity vanishes for any $j>1$ and therefore

$$\sum_{i=0}^{j-1}(\alpha^{2^m})^i=0.$$

Q.E.D.

THEOREM 3. *Let $\mathscr{D}$ be a $k\times n$ matrix with linearly independent rows over* GF(3), *which contains an odd number of each of the possible* $(3^k-1)/2$ *classes of columns, and no all-zero columns. If all solutions of the equation*

$$\mathscr{D}\vec{x}=\vec{0}$$

have some zero component(s), then the dimensions of $\mathscr{D}$ are either 1×1 *or* 2×4.

Proof. If $k=1$ and $n\ge 3$, then we may choose a pair of signs of $\vec{x}$ so as to cancel the effects of a pair of columns of $\mathscr{D}$, and so on, until we reduce to the case when $n=3$. If $k=1$ and $n=3$, an appropriate choice of signs solves $\mathscr{D}\vec{x}=\vec{0}$ via $1+1+1=0$.

If $k=2$ and $n>6$, then we may choose the signs of a pair of components of $\vec{x}$ so as to cancel the effects of a pair of columns of $\mathscr{D}$ in the same class, and continue this procedure until we reduce to the case $5\le n\le 6$. Since there must be an odd

number of columns remaining in each of the four classes, $n=6$. By appropriate permutation of columns, we may bring the three columns in the same class of the first three positions. By an appropriate invertible linear transformation of rows, another permutation of columns, and appropriate scalar multiplications of columns, we may reduce everything to the case

$$\mathscr{D} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & -1 \end{bmatrix}$$

which has null space including the completely nonzero vector

$$\vec{x} = [1 \quad 1 \quad 1 \quad -1 \quad -1 \quad 1]$$

Finally, if $k \geq 3$, then we may choose the signs of the components of $\vec{x}$ so as to cancel the effects of any pair of columns of $\mathscr{D}$ in the same class. After we have thus cancelled all but one column in each class, we may apply Theorem 2. Q.E.D.

THEOREM 4. *If $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_M$ are r-dimensional row vectors over* GF(3) *such that:*

(i) *Any weighted* ($\pm$) *sum of any even number of $\vec{v}$'s is nonzero.*

(ii) *For each r-dimensional $\vec{y}$, there exists an s such that $\vec{v}_s \vec{y}^t = 0$.*

Then there exists a subset of either 1 *or* 4 *$\vec{v}$'s which satisfies the same conditions.*

Proof. Let $\mathscr{V}$ be the $M \times r$ matrix whose rows are $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_M$, and let $\mathscr{D}$ be a matrix which satisfies

$$\mathscr{D}\mathscr{V} = 0$$

and has as many linearly independent rows as possible. Then if $\vec{x} = \mathscr{V}\vec{y}$, $\mathscr{D}\vec{x} = \mathscr{V}\vec{y} = \vec{0}$, and conversely, if $\mathscr{D}\vec{x} = \vec{0}$, then there exists some $\vec{y}$ such that $x = \mathscr{V}\vec{y}$. Thus condition (ii) becomes

(ii′) If $\mathscr{D}\vec{x} = \vec{0}$, then $\vec{x}$ has at least one zero component.

Condition (i) ensures that the weight of every vector in the row space of $\mathscr{D}$ is odd. Hence, $\mathscr{D}$ satisfies the hypotheses of Theorem 1. If we omit the all-zero columns of $\mathscr{D}$ and the corresponding $\vec{v}$'s, we obtain a new $\mathscr{D}$ matrix which now satisfies the hypotheses of Theorem 3. The dimensions of this $\mathscr{D}$ are either 1×1 or 2×4, so the number of remaining v's is either 1 or 4. Q.E.D.

REFERENCES

1. L. Fuchs, *Abelian groups*, Publ. House of the Hungarian Acad. of Sci. Budapest, 1958.

2. B. Gordon, (unpublished communication), 1968.

3. G. Hajos, *Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter*, Math. Z. **47** (1942), 427–467.

BELL TELEPHONE LABORATORIES, INC.,
MURRAY HILL, NEW JERSEY