ELSEVIER

Available online at www.sciencedirect.com
SCIENCE DIRECT®

Linear Algebra and its Applications 416 (2006) 288–297

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

Minimal blocks of binary even-weight vectors

Joseph P.S. Kung

Department of Mathematics, University of North Texas, P.O. Box 311430, Denton, TX 76203, USA

Received 16 August 2005; accepted 8 November 2005
Available online 19 January 2006
Submitted by R.A. Brualdi

Abstract

Odd circuits are minimal 1-blocks over GF(2) and the odd circuit of size $2t + 1$ can be represented by the vectors of Hamming weight $2t$ in a $(2t + 1)$-dimensional vector space over GF(2). This is the tip of an iceberg. Let $f(2t, k, 2)$ be the maximum number of binary k-dimensional column vectors such that for all s, $1 \leqslant s \leqslant t$, no $2s$ columns sum to the zero vector. If $k = 2$, $k = 3$, $k = 4$, or $k \geqslant 5$ and $2t$ is sufficiently large (for example, $2t \geqslant 2^k - k + 1$ suffices), then the set of vectors of weight $2t$ in a $(f(2t, k, 2) + 2t - 1)$-dimensional vector space over GF(2) is a minimal k-block over GF(2).

AMS classification: 05B35; 05C15; 05C22; 11T71; 15A06

Keywords: Blocks; Minimal blocks; Binary matroids; Critical problem

1. Blocks and the critical problem

Minimal and tangential blocks were first defined in the 1966 paper [8] of Tutte. A *k-block* M over GF(q) can be defined as a set of points in projective space PG$(n - 1, q)$ such that every codimension-k subspace in PG$(n - 1, q)$ contains at least one point in M. If X is a flat in M, a *tangent* of X is a codimension-k subspace U such that

$$M \cap U = X.$$

A k-block M is *minimal* if every point has a tangent. It is *tangential* if every flat of rank not exceeding $n - k$ has a tangent. Blocks can also be defined using the critical problem of Crapo and

E-mail address: kung@unt.edu

0024-3795/$ - see front matter
doi:10.1016/j.laa.2005.11.014

Rota [1]. The critical problem approach shows that the properties of being a k-block, a minimal k-block, or a tangential k-block depend only on the linear matroid defined by the set M.

The graph-theoretic or coloring analogue of a minimal k-block is a *minimal* $(h+1)$-*chromatic graph*, a graph with chromatic number $h+1$ such that deleting any one of its edges results in a graph with chromatic number h. Indeed, a minimal (2^k+1)-chromatic graph is a minimal k-block over GF(2). Thus, there are many graphical minimal blocks known, in principle and in explicit form. However, the only known graphic tangential k-blocks over GF(2) are the cycle matroids of complete graphs on 2^k+1 vertices. Indeed, if Hadwiger's conjecture is true, then all graphical tangential blocks are cycle matroids of complete graphs.

The situation in graph theory is far from typical. There are many non-graphical tangential blocks, to the extent that in matroid theory, tangential blocks have held center stage. However, as Tutte showed in [8], knowledge about minimal blocks can be the key to understanding tangential blocks, particularly those which split as a set into the union of two proper flats. In addition, the complement $\mathrm{PG}(r-1,q)\backslash M$ of a rank-r minimal k-block M over $\mathrm{GF}(q)$ is *extremal* in the restriction-closed class of $\mathrm{GF}(q)$-representable matroids not containing $\mathrm{PG}(r-k-1,q)$ as a submatroid, in the sense that any proper rank-r extension of $\mathrm{PG}(r-1,q)\backslash M$ contains $\mathrm{PG}(r-k-1,q)$ as a restriction. See [3, Section 3].

Besides Tutte's work, the only other result on minimal blocks is Oxley's theorem that a series connection of two minimal k-blocks is again a minimal k-block [6]. Apart from a few small examples, all the previously known minimal blocks are tangential blocks or series connections of minimal blocks. In this paper, we use a linear algebra method to show that certain sets of binary vectors of even weight are minimal blocks. This direct method originated in [5] and is robust in two ways: it works independently of dimension and it works for polymatroids as well as matroids.

Nothing more than elementary linear algebra is needed to read this paper. However, some familiarity with matroid theory (see [1,7]) and the critical problem (see [4]) is necessary to see why the results are interesting. A survey of minimal blocks can be found in Section 8.3 of [4].

We shall be working in both the vector space $\mathrm{GF}(q)^N$ and the projective space $\mathrm{PG}(N-1,q)$. In both, we choose a fixed basis $e_1, e_2, \ldots, e_N$ and use the following compact notation: if $I \subseteq \{1, 2, \ldots, N\}$, then

$$e[I] = \sum_{i:i\in I} e_i.$$

The *Hamming weight* of a vector or point (relative to the fixed basis) is the number of non-zero coordinates in it; the *support* is the set of positions with non-zero coordinates. We will use repeatedly the fact that a codimension-k subspace U in $\mathrm{GF}(q)^N$ or $\mathrm{PG}(n-1,q)$ is the null space $\{x : Ax^{\mathrm{T}} = 0\}$ of a rank-k matrix A.

Let A be a matrix. We denote by A_i the column indexed by i in A. A *dyad* in A is a pair of columns A_i and A_j such that $A_i = A_j$.

2. Binary even-weight vectors

In Sections 2 and 3, we shall work over a finite field $\mathrm{GF}(2^r)$ having characteristic 2. The set $W(s,N)$ is the binary matroid represented by the subset

$$\{e[I] : |I| = s\}$$

of weight-s points in $\mathrm{PG}(N-1,2)$. When s is even, the weight-s points are in the hyperplane H defined by the equation $x_1 + x_2 + \cdots + x_N = 0$ and they span H. Thus, for even s, the matroid $W(s,N)$ has rank $N-1$.

Let t be a positive integer. A $k \times m$ matrix A with entries in $\mathrm{GF}(2^r)$ is said to be $2t$-*sharp* if for every positive even number $2s$ not exceeding $2t$, no $2s$ columns sum to the zero vector, or, briefly, "sum to zero". This condition is equivalent to the null space of A and the union

$$\bigcup_{s=1}^{t} W(2s, m)$$

have empty intersection. By definition, a $2t$-sharp matrix has distinct columns. Being $2t$-sharp is preserved under column permutations and non-singular row operations. The parity check matrix of a binary linear code with minimum distance greater than $2t$ is a $2t$-sharp matrix over $\mathrm{GF}(2)$, but binary $2t$-sharp matrices can be bigger.

Let $f(2t, k, 2^r)$ be the maximum number m such that there exists a $k \times m$ $2t$-sharp matrix over $\mathrm{GF}(2^r)$. For example, $f(2, k, 2^r)$ equals 2^{rk}, the number of distinct k-dimensional vectors over $\mathrm{GF}(2^r)$. Because being $2t$-sharp implies being $2s$-sharp if $t \geqslant s$, $f(2t, k, 2^r)$ is a non-increasing function of $2t$. In addition, the $k \times (k+1)$ matrix constructed by adding the zero column to the $k \times k$ identity matrix is $2t$-sharp for any t. We conclude that if $2t \geqslant 2s$,

$$k + 1 \leqslant f(2t, k, 2^r) \leqslant f(2s, k, 2^r) \leqslant f(2, k, 2^r) = 2^{rk}. \tag{1}$$

The lower bound is sharp for suitable values of $2t$ when $r = 1$. Indeed, if k is odd, then $f(k + 1, k, 2) = k + 1$, and if k is even, $f(k + 2, k, 2) = k + 1$. Another easy lower bound, useful for doing small cases, is $f(4, k, 2) \geqslant k + k/2$ if k is even and $f(4, k, 2) \geqslant k + (k - 1)/2$ if k is odd. This bound follows from the fact that the columns of an identity matrix, together with weight-2 columns having mutually disjoint supports, form a 4-sharp matrix. Finally, since $\mathrm{GF}(2^r)$ is a r-dimensional vector space over $\mathrm{GF}(2)$,

$$f(2t, k, 2^r) = f(2t, rk, 2).$$

We begin with the case $k = 2$. This case gives the ideas behind our method free of technicalities. There are four 2-dimensional binary vectors. These four vectors sum to zero, and any three can be chosen as the columns of a 2-sharp matrix. Hence, when $t \geqslant 2$, $f(2t, 2, 2) = 3$.

Theorem 2.1. *When $t \geqslant 2$, the matroid $W(2t, 2t + 2)$ is a minimal 2-block over* $\mathrm{GF}(2)$.

Proof. Let A be a $2 \times (2t + 2)$ matrix over $\mathrm{GF}(2)$. Let i_α be the number of columns in A equal to the vector α, expressed in base 2. Then $i_0 + i_1 + i_2 + i_3 = 2t + 2$. There are three cases.

(a) The integers i_α are all even. Then there are $t + 1$ disjoint dyads. Picking t of them give $2t$ columns summing to zero.
(b) Two of the integers are even and the other two are odd. Then there are t disjoint dyads and they give $2t$ columns summing to zero.
(c) All the integers i_α are odd. Let i be the minimum of i_0, i_1, i_2, i_3. Then there are i disjoint quadruples consisting of four distinct vectors. Since four distinct columns sum to zero, we obtain $4i$ columns summing to zero. We are left with $i_\alpha - i$ columns equal to α (with one or more of the integers $i_\alpha - i$ equal to zero). Since i is odd, $i_\alpha - i$ are all even. As in case (a), we obtain $2t + 2 - 4i$ disjoint dyads. Picking $2t - 4i$ dyads and adding the $4i$ columns obtained earlier, we get $2t$ columns summing to zero.

This shows that $W(2t, 2t + 2)$ is a 2-block.

To show minimality, observe that the null space of the $2 \times (2t+2)$ matrix

$$\begin{pmatrix} 0 & 0\cdots 0 & 1 & 0 \\ 0 & 0\cdots 0 & 0 & 1 \end{pmatrix}$$

is a tangent for $e[1, 2, \ldots, 2t]$. Tangents for other weight-$2t$ points can be obtained by permuting the columns. $\square$

By Theorem 2.1, $W(4, 6)$ is a minimal 2-block over GF(2) having 15 points and rank 5. As one might expect from the tangential 2-block conjecture [8], $W(4, 6)$ is not a tangential k-block. For example, the rank-2 flat $\{e[1, 2, 3, 4], e[2, 3, 4, 5]\}$ does not have a tangent.

There are two other simple cases besides Theorem 2.1. The first is the case $k = 1$. There are two 1-dimensional column vectors over GF(2) and the matrix (0 1) is 2-sharp. Hence $f(2t, 1, 2) = 2$. A simpler version of the proof of Theorem 2.1 shows that the matroids $W(2t, 2t+1)$ are binary minimal 1-blocks. Since $W(2t, 2t+1)$ is isomorphic to a circuit with $2t+1$ points, this result is the easier implication of Tutte's odd circuit lemma [8], that a matroid is a minimal 1-block over GF(2) if and only if it is an odd circuit.

The other simple case is when $2t = 2$. Since being 2-sharp is just having distinct columns, $f(2, k, 2^r) = 2^{rk}$. Because a matrix with $2^{rk}+1$ columns must contain a dyad, it is easy to show that $W(2, 2^{rk}+1)$ is a minimal k-block over GF(2^r). Alternatively, one can observe that $W(2, 2^{rk}+1)$ is the cycle matroid of the complete graph on $2^{rk}+1$ vertices. As is well known, this is a tangential (hence, minimal) k-block over GF(2^r).

Our main results are motivated by the preceding three examples. We begin with a theorem which holds generally.

Theorem 2.2. *If the matroid $W(2t, f(2t, k, 2^r) + 2t - 1)$ is a k-block* (*over* GF(2^r)), *then it is a minimal k-block.*

Proof. We shall find a tangent for each point in $W(2t, f(2t, k, 2^r) + 2t - 1)$. Since the symmetric group acts transitively on $2t$-subsets, we need only consider the vector $e[1, 2, \ldots, 2t]$. Consider the $k \times (f(2t, k, 2^r) + 2t - 1)$ matrix A constructed by choosing columns $2t$ to $f(2t, k, 2^r) + 2t - 1$ so that submatrix A' consisting of those columns is $2t$-sharp, and then setting the initial columns $1, 2, \ldots, 2t-1$ equal to column $2t$. Since the first $2t$ columns are equal, $e[1, 2, \ldots, 2t]$ is in the null space of A.

To finish the proof, we will show that if $e[I]$, where $|I| = 2t$, is in the null space of A, then $I = \{1, 2, \ldots, 2t\}$, Since the submatrix A' is $2t$-sharp, I is not contained in $\{2t, 2t+1, \ldots, f(2t, k, 2^r) + 2t - 1\}$, or, equivalently, at least one index in I is in $\{1, 2, \ldots, 2t-1\}$.

Suppose that exactly l indices in I are in $\{1, 2, \ldots, 2t-1\}$. Relabeling if necessary, we may suppose that $1, 2, \ldots, l$ are those indices. Let $J = I \backslash \{1, 2, \ldots, l\}$. Then

$$A_1 + A_2 + \cdots + A_l + \sum_{j:j\in J} A_j = 0.$$

If l is even, then $A_1 + A_2 + \cdots + A_l = 0$ and $\{A_j : j \in J\}$ is an even non-empty subset of columns in the $2t$-sharp submatrix A' summing to zero, a contradiction. If l is odd, then $A_1 + A_2 + \cdots + A_l = A_{2t}$. If $l < 2t - 1$ and $2t \notin J$, then A_{2t} and the columns A_j, $j \in J$ form a non-empty even subset of columns in A' summing to zero, a contradiction. If $l < 2t - 1$ and $2t \in J$, then $\{A_j : j \in J, j \neq 2t\}$ is a non-empty even subset summing to zero, a contradiction. Finally, if $l = 2t - 1$, then J is a single-element set $\{j\}$ and $A_j = A_{2t}$. Since $j \geqslant 2t$ and the columns in A' are distinct, we conclude that $j = 2t$ and $e[I] = e[1, 2, \ldots, 2t]$. $\square$

Theorem 2.3. *The matroid* $W(4, f(4,k,2^r)+3)$ *is a minimal k-block over* $\mathrm{GF}(2^r)$.

Proof. By Theorem 2.2, it suffices to show that $W(4, f(4,k,2^r)+3)$ is a k-block, or, equivalently, in every $k \times (f(4,k,2^r)+3)$ matrix A, there exist four columns summing to zero. If the number of distinct columns in A is strictly greater than $f(4,k,2^r)$, then some four columns sum to zero. Thus we can assume that there are at most $f(4,k,2^r)$ distinct columns in A. Since there are at least three more columns than the number of distinct columns in A, there exist (a) four or more columns, all equal to each other, (b) three columns, all equal to each other, and disjoint from the triple, a dyad, (c) two disjoint dyads. In all three cases, we can extract four columns summing to zero. $\square$

The next theorem shows that for a given integer k greater than 2, $W(2t, f(2t,k,2^r)+2t-1)$ is a minimal k-block for all sufficiently large t.

Theorem 2.4. *Suppose that*

$$f(2t,k,2^r)+2t-1 \geqslant 2^{rk}+1$$

and

$$2t+2 \geqslant f(4,k,2^r).$$

Then, the matroid $W(2t, f(2t,k,2^r)+2t-1)$ *is a minimal k-block over* $\mathrm{GF}(2^r)$.

Proof. By Theorem 2.1, it suffices to show that $W(2t, f(2t,k,2^r)+2t-1)$ is a k-block. Let A be a $k \times (f(2t,k,2^r)+2t-1)$ matrix over $\mathrm{GF}(2^r)$ with columns indexed by I. If α is a vector in $\mathrm{GF}(2^r)^k$, let $I_\alpha = \{i : i \in I \text{ and } A_i = \alpha\}$ and let

$$\mathscr{O} = \{\alpha \in \mathrm{GF}(2^r)^k : |I_\alpha| \text{ is odd}\}.$$

If $|I_\alpha|$ is even, then the columns equal to α can be paired into $|I_\alpha|/2$ disjoint dyads. If $|I_\alpha|$ is odd, then we can choose $|I_\alpha|-1$ columns equal to α and pair them into $(|I_\alpha|-1)/2$ disjoint dyads, leaving one *single* column unpaired. The total number of dyads obtained is

$$\frac{2t-1+f(2t,k,2^r)-|\mathscr{O}|}{2} \tag{2}$$

and there are $|\mathscr{O}|$ single columns left over. The single columns are, of course, distinct.

From the set of single columns left over from the pairing, choose a maximum-size even subset of columns which sum to zero. Let this subset of columns be indexed by J. We claim that

$$|J| > |\mathscr{O}| - f(2t,k,2^r). \tag{3}$$

[Otherwise, there would be at least $f(2t,k,2^r)$ single columns not in J. These columns are distinct and by definition of $f(2t,k,2^r)$, there exist $2s$ single columns not in J summing to zero. We can add these $2s$ columns to the columns already chosen, obtaining a bigger even subset of columns summing to zero.] Combining formula (2) and inequality (3), we conclude that the number of dyads is at least $(2t-|J|)/2$.

If $|J| \leqslant 2t$, then we can choose $(2t-|J|)/2$ dyads and add the columns in them to the columns indexed by J to get $2t$ columns summing to zero.

To deal with the case when $|J| > 2t$, we need to use the two technical hypotheses. Since $|J| \geqslant 2t+2 \geqslant f(4,k,2^r)$, the columns in J contain four columns, indexed by F, say, summing to zero. Since the columns indexed by J sum to zero, the columns in the complement $J \backslash F$ also sum to zero. Repeating this procedure, we obtain a subset H of J so that the columns in H sum to zero and $|H|$ equals $2t$ or $2t-2$, depending on whether $|J|-2t$ is congruent to 0 or 2 modulo 4. In the first case, H is a set of $2t$ columns summing to zero. In the second case, the hypothesis $f(2t,k,2^r)+2t-1 \geqslant 2^{rk}+1$ implies that there exists at least one dyad. Adding any dyad to H yields a set of $2t$ columns summing to zero. □

3. Two bounds and an example

Although Theorem 2.4 shows that $W(2t,\ f(2t,k,2^r)+2t-1)$ is a k-block for all but finitely many t, the technical hypotheses are there only to make the proof work. To remove them, we need to know, for example, whether $f(2t,k,2^r)+2t-1$ *distinct* columns always contain $2t$ columns summing to zero. Knowing more about the values of $f(2t,k,2^r)$ would certainly help.

We begin with an upper bound obtained with the pigeonhole principle.

Lemma 3.1. *Let s be an integer satisfying $1 \leqslant s \leqslant t$. If*

$$\binom{N}{s} > 2^{rk}, \tag{4}$$

then

$$f(2t,k,2^r) \leqslant N-1.$$

In particular,

$$f(4,k,2^r) \leqslant \lceil 2^{(rk+1)/2} \rceil.$$

Proof. Let N satisfy the inequality (4) and let A be a $k \times N$ matrix over $\mathrm{GF}(2^r)$. We will show that A is not $2t$-sharp. Consider the function on the collection of s-subsets of columns of A sending a subset of t columns to the sum of those columns. Since there are 2^{rk} distinct columns, inequality (4) implies that two s-subsets of columns, indexed by I and J, have the same sum. Hence, the columns indexed by the symmetric difference $I \,\Delta\, J$ sum to zero. Since $|I \,\Delta\, J|$ equals the positive even integer $2t-2|I \cap J|$, the matrix A is not $2t$-sharp. □

From Theorem 2.4, Lemma 3.1, and the lower bound $f(2t,k,2^r) \geqslant k+1$, we obtain the following corollary.

Corollary 3.2. *If $2t \geqslant 2^{rk}-k+1$, then the matroid $W(2t,\ f(2t,k,2^r)+2t-1)$ is a minimal k-block over* $\mathrm{GF}(2^r)$.

A companion to Lemma 3.1 is the following lower bound, suggested by the close similarity between sharp matrices and parity check matrices of codes.

Lemma 3.3. *A $k \times N$ $2t$-sharp matrix with no column equal to the zero vector exists over* $\mathrm{GF}(2^r)$ *if*

$$\binom{N-1}{1}+\binom{N-1}{3}+\cdots+\binom{N-1}{2t-1} < 2^{rk}-1.$$

Proof. Use the argument in the proof of the Gilbert–Varshamov bound in coding theory (see, for example, [2, Chapter 1]). $\square$

The lower bound implied by Lemma 3.3 is not very useful for small k or large t. However, the upper bound given in Lemma 3.1 is often the true value for small k.

Lemma 3.4. *For all integers t greater than* 1, $f(2t, 3, 2) = 4$.

Proof. By Lemma 3.1, $f(4, 3, 2) \leqslant 4$. Up to row operations and column permutations, there are two 3×4 4-sharp matrices. They are

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

We conclude that $f(4, 3, 2) = 4$. Since these two matrices are $2t$-sharp for $t \geqslant 3$, we also have $f(2t, 3, 2) = 4$ for those values of t. $\square$

Theorems 2.1, 2.4, and Lemma 3.4 imply the following result.

Theorem 3.5. *For all $t \geqslant 2$, the matroids $W(2t, 2t + 3)$ are binary minimal* 3*-blocks.*

The cases $k = 2$ and 3 are by no means typical. The case $k = 4$ shows what complications may occur in general.

Lemma 3.6. $f(4, 4, 2) = 6$. *When $t \geqslant 3$,* $f(2t, 4, 2) = 5$.

Proof. By Lemma 3.1, $f(4, 4, 2) \leqslant 6$. Up to row operations and column permutations, there are two 4×6 4-sharp matrices. They are

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Hence, $f(4, 4, 2) = 6$. Now suppose that $t \geqslant 3$. Then these two matrices given above are not $2t$-sharp, but 4×5 $2t$-sharp matrices are obtained when any one column is deleted. Using Lemma 3.1 and inequality (1), we conclude that $f(2t, 4, 2) = 5$. $\square$

Theorems 2.1, 2.4, and Lemma 3.6 imply that $W(4, 9)$ and $W(2t, 2t + 4)$ for $t \geqslant 6$ are minimal 4-blocks. The three remaining matroids $W(6, 10)$, $W(8, 12)$, $W(10, 14)$ can be shown to be 4-blocks by case analysis.

We briefly describe how to do this for $W(6, 10)$ in three steps. (1) By Lemma 3.1, every 10 distinct columns contain six columns summing to zero. (2) If the number of distinct columns is between 6 and 9, then either there are six distinct columns summing to zero or there are four distinct columns summing to zero and a dyad disjoint from them. (3) If there are five or fewer of distinct columns, then there are at least three disjoint dyads.

Theorem 3.7. *The matroids $W(4, 9)$ and $W(2t, 2t + 4)$, $t \geqslant 3$, are binary minimal* 4*-blocks.*

Next, we state the results of three more calculations without proof.

Lemma 3.8

(a) $f(4, 5, 2) = 7$, *and for* $t \geqslant 3$, $f(2t, 5, 2) = 6$.
(b) $9 \leqslant f(4, 6, 2) \leqslant 11$, $f(6, 6, 2) = 8$, *and for* $t \geqslant 4$, $f(2t, 6, 2) = 7$.
(c) $10 \leqslant f(4, 7, 2) \leqslant 16$, $f(6, 7, 2) = 10$, $f(8, 7, 2) = 9$, *and for* $t \geqslant 5$, $f(2t, 7, 2) = 8$.

Knowing sufficiently many small cases, we can now answer the question: does Theorem 2.4 hold unconditionally for all triples $2t, k, 2^r$? The disappointing answer is "no". When $2t = 6$, $k = 7$, and $r = 1$, the matroid $W(2t, f(6, 7, 2) + 2t - 1)$ is not a binary 7-block.

We begin by checking that $f(6, 7, 2)$ is indeed 10. To do so, observe that Lemma 3.1 implies $f(6, 7, 2) \leqslant 10$. In addition, a 7×10 6-sharp matrix can be constructed by taking a 7×7 identity matrix and adding the columns

$$(1, 1, 1, 1, 1, 1, 1)^{\mathrm{T}}, \quad (1, 1, 1, 1, 0, 0, 0)^{\mathrm{T}}, \quad (0, 0, 0, 1, 1, 1, 1)^{\mathrm{T}}.$$

Proposition 3.9. *$W(6, 15)$ is not a binary 7-block.*

To prove Proposition 3.9, consider the 7×16 "echeloned" matrix A

$$\begin{pmatrix} A_1 & A_2 & 0 \\ 0 & 0 & A_3 \end{pmatrix},$$

where A_1 is the 4×4 identity matrix, A_2 is the 4×4 matrix made by putting together all four 4-dimensional weight-3 column vectors, and A_3 is the 3×8 matrix made from all eight 3-dimensional column vectors.

Lemma 3.10. *The matrix A contains no six columns summing to zero.*

Proof. Divide the matrix into two parts, the first part consisting of the first eight columns and the second the remaining seven columns. Suppose that six columns sum to zero. Then, noting that there is only one zero column (in the second part) and no two columns sum to zero, one of the following four cases holds.

(a) Five columns, summing to zero, come from the first part, and the remaining column is the zero column from the second.
(b) Both parts contain three columns each.
(c) All six columns are in the first part.
(d) All six columns are in the second part.

It is easy to check that all four cases are impossible. For example, to rule out (b), observe that because A is echeloned, the three columns from the first part must sum to zero. Since all the columns in the first part have odd weight, this is not possible. □

The matrix A is bigger than we need. Any 15 columns from A give a 7×15 matrix whose null space is disjoint from $W(6, 15)$. We conclude that $W(6, 15)$ is not a 7-block.

4. Minimal blocks from graphs

This section is intended as an appendix. The new results are easy and should be known, but they do not seem to have been written down.

We begin with a construction due to Zaslavsky [10]. Let Γ be a simple graph with N vertices and q be a power of a prime. The *full* GF(q)*-expansion* $\Gamma(q)$ is the set

$$\{e_i - \omega e_j : \{i, j\} \text{ an edge in } \Gamma, \omega \in \mathrm{GF}(q)\}$$

of points in N-dimensional projective space PG$(N-1, q)$ with the coordinates indexed by the vertices of Γ. Two column vectors in GF$(q)^k$ are said to be *projectively equivalent* if one is a non-zero scalar multiple of the other. The relation between the critical problem for full expansions and colorings of the underlying graph is given by the following easy lemma.

Lemma 4.1. *Let $\Gamma(q)$ be the full expansion of the graph Γ over* GF(q)*. The null space of a matrix A with columns indexed by the vertices of Γ is disjoint from $\Gamma(q)$ if and only if the columns of A, under projective equivalence, give a coloring of Γ.*

Theorem 4.2. *Let*

$$h = \frac{q^k - 1}{q - 1} + 1,$$

the number of equivalence classes in GF$(q)^k$ *under projective equivalence. Then the full expansion $\Gamma(q)$ of a minimal $(h+1)$-chromatic graph is a minimal k-block.*

Proof. Since the number h is the number of projective equivalence classes in GF$(q)^k$, the matroid $\Gamma(q)$ is a k-block over GF(q). Minimality follows from the fact that for every edge $\{i, j\}$ in a minimal $(h+1)$-chromatic graph Γ, there exists an h-coloring such that $\{i, j\}$ is the only monochromatic edge. $\square$

Theorem 4.2 generalizes Tutte's odd circuit lemma in another direction. Recall that the odd cycle C_{2t+1} is a minimal 3-chromatic graph.

Corollary 4.3. *The full expansion $C_{2t+1}(q)$ is a minimal* 1*-block over* GF(q).

Note that $C_3(q)$ is the rank-3 jointless Dowling group geometry over the multiplicative group GF$(q)^{\times}$. These matroids are known to be tangential 1-blocks over GF(q) (see [9]). All the results in this section extend easily to the critical problem for submatroids of Dowling group geometries (see, for example, [9,10,4, Sections 4.5 and 8.11]).

References

[1] H.H. Crapo, G.-C. Rota, On the Foundations of Combinatorial Theory: Combinatorial Geometries, Preliminary ed., M.I.T. Press, Cambridge, MA, 1970.

[2] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-correcting Codes, North-Holland, Amsterdam, 1977.

[3] J.P.S. Kung, Extremal matroid theory, in: N. Robertson, P.D. Seymour (Eds.), Graph Structure Theory, Amer. Math. Soc., Providence, RI, 1993, pp. 21–62.

[4] J.P.S. Kung, Critical problems, in: J.E. Bonin, J.G. Oxley, B. Servatius (Eds.), Matroid Theory, Amer. Math. Soc., Providence, RI, 1996, pp. 1–127.

[5] J.P.S. Kung, Critical exponents, colines and projective geometries, Combin. Probab. Comput. 9 (2000) 355–362.

[6] J.G. Oxley, On a covering problem of Mullin and Stanton for binary matroids, Aequationes Math. 20 (1980) 104–112.
[7] J.G. Oxley, Matroid Theory, Oxford Univ. Press, Oxford, 1992.
[8] W.T. Tutte, On the algebraic theory of graph colorings, J. Combin. Theory 1 (1966) 15–50.
[9] G.P. Whittle, Dowling group geometries and the critical problem, J. Combin. Theory Ser. B 47 (1989) 80–92.
[10] T. Zaslavsky, Biased graphs. III. Chromatic and dichromatic invariants, J. Combin. Theory Ser. B 64 (1995) 17–88.