ON THE COGIRTH OF BINARY MATROIDS

CAMERON CRENSHAW AND JAMES OXLEY

Abstract. The cogirth, $g^*(M)$, of a matroid M is the size of a smallest cocircuit of M. Finding the cogirth of a graphic matroid can be done in polynomial time, but Vardy showed in 1997 that it is NP-hard to find the cogirth of a binary matroid. In this paper, we show that $g^*(M) \leq \frac{1}{2}|E(M)|$ when M is binary, unless M simplifies to a projective geometry. We also show that, when equality holds, M simplifies to a Bose-Burton geometry, that is, a matroid of the form $PG(r-1,2) - PG(k-1,2)$. These results extend to matroids representable over arbitrary finite fields.

1. Introduction

For an arbitrary graph G, the well-known fact that the degree sum of G is twice the number of edges of G implies that

$$\frac{|E(G)|}{\delta(G)} \geq \frac{1}{2}|V(G)|,$$

where $\delta(G)$ is the minimum degree of G. In a matroid M of nonzero rank, the *cogirth*, $g^*(M)$, of M is the size of a smallest cocircuit of M. As $U_{r,n}$ shows, $\frac{|E(M)|}{g^*(M)}$ can be arbitrarily close to 1 even for simple matroids, although it is bounded below by $\frac{1}{2}(r(M)+1)$ when M is graphic.

In this paper, we show that, when M is binary,

$$\frac{|E(M)|}{g^*(M)} \geq 2$$

unless M simplifies to a projective geometry. We also characterize the matroids that achieve equality in this bound. Both of these results are special cases of results for matroids representable over arbitrary finite fields.

The terminology used here will follow Oxley [6] with the following addition. We will often use P_r and A_r to denote $PG(r-1,q)$ and $AG(r-1,q)$, respectively, where q should be clear from the context. The next two results are the main results of the paper.

Date: May 25, 2022.

Key words and phrases. binary matroid, representable matroid, cogirth.

Theorem 1.1. *For $r \geq 1$, let M be a rank-r matroid representable over $GF(q)$ whose simplification is not P_r. Then*

$$\frac{|E(M)|}{g^*(M)} \geq \frac{q}{q-1}.$$

Moreover, equality holds if and only if M is loopless and, for a fixed embedding of $\mathrm{si}(M)$ *in P_r,*

(i) *the complement of* $\mathrm{si}(M)$ *in P_r is isomorphic to P_k for some k with $1 \leq k < r$; and*

(ii) *if P is a copy of P_{k+1} in P_r containing the complement of* $\mathrm{si}(M)$*, then the parallel classes of the elements in $E(M) \cap E(P)$ all have the same size; and*

(iii) $|E(N)| \geq (q-1)|E(M) - E(N)|$ *for every restriction N of M that simplifies to A_r.*

This theorem excludes the matroids M for which $\mathrm{si}(M) \cong PG(r-1, q)$. These excluded matroids are covered by the next result.

Proposition 1.2. *For $r \geq 1$, let M be a matroid that simplifies to $PG(r-1, q)$. Then*

$$\frac{|E(M)|}{g^*(M)} \geq \frac{q^r - 1}{q^{r-1}(q-1)}.$$

Moreover, equality holds if and only if M is loopless and all its parallel classes have the same size.

Condition (i) in Theorem 1.1 says that M simplifies to a *Bose-Burton geometry* [3], that is, a matroid that is obtained from $PG(r-1, q)$ by deleting some $PG(k-1, q)$ where $1 \leq k < r$. In each of our results, the bound on $\frac{|E(M)|}{g^*(M)}$ is relatively easy to obtain. The core of each proof involves characterizing when equality holds in the bound. The proofs appear in Section 3.

Our results have implications for linear codes. A *linear code* of *length* n and *rank* k is a k-dimensional subspace of the n-dimensional vector space over $GF(q)$. Such a code C is also known as a *q-ary code* (see, for example, [5]). The minimum distance d of C is the minimum number of coordinates in which two vectors in C differ or, equivalently, the minimum number of non-zero coordinates in a non-zero vector in C. The *relative distance* of C is d/n. A *generator matrix* for C is a $k \times n$ matrix A over $GF(q)$ such that C equals the row space of A. Let M be $M[A]$, the vector matroid of A. Then the cocircuits of M coincide with the minimal non-empty supports of the vectors in C. Thus the cogirth of M is the minimum distance of C, and $g^*(M)/|E(M)|$ is the relative distance, d/n, of C.

When $\frac{d}{n} > 1 - \frac{1}{q}$, the Plotkin bound [7] for q-ary codes [1, 2, 4] asserts that $|C| \leq \frac{qd}{qd-(q-1)n}$. Moreover, when $q = 2$ and $\frac{d}{n} = \frac{1}{2}$, Plotkin showed that $|C| \leq 4d$. Theorem 1.1 describes the matroids that do not simplify to $PG(r-1, q)$ for which the relative distance of the corresponding linear code equals $1 - \frac{1}{q}$.

2. Preliminaries

In a matroid M of rank at least one, a loop contributes to $|E(M)|$ but not to $g^*(M)$. Since our concern here is on bounding $\frac{|E(M)|}{g^*(M)}$ below, we shall focus on matroids without loops. It will be convenient here to deal with the parallel classes in such a matroid M by assigning, to each element of $\mathrm{si}(M)$, a *weight* $w(e)$ that is equal to the cardinality of the parallel class of M that contains e. Thus we deal with simple matroids with associated weight functions that take a positive-integer value on each element. For a set X in such a matroid N, we write $w(X)$ for $\sum_{x \in X} w(x)$ and write $w(N)$ for $w(E(N))$. The weight function of $N \backslash Y$ is the restriction of the weight function of N to $E(N) - Y$. When Y is contracted from N, we replace each parallel class P by a single element e_P whose weight in the contraction is $w_N(P)$. We will call this weighted simple matroid the *weighted contraction* of Y and denote it by N/Y, even though the underlying matroid is actually $\mathrm{si}(N/Y)$. The cogirth of a weighted matroid is the minimum weight of a cocircuit.

3. The Proofs

We begin with a lemma that serves as the base case for both of the inductive arguments that prove the inequalities in the main results.

Lemma 3.1. *Let M be a simple, rank-2 matroid, and let w be a weight function on M. Then*
$$\frac{w(M)}{g^*(M)} \geq \frac{|E(M)|}{|E(M)|-1},$$
with equality if and only if w is constant.

Proof. Let $w_1 \leq w_2 \leq \cdots \leq w_n$ be the weights of the elements of M. Because the cocircuits of M coincide with the complements of the parallel classes in the rank-2 matroid M, we deduce that $g^*(M) = w_1 + w_2 + \cdots + w_{n-1}$. Thus, the desired inequality is equivalent to
$$(n-1)(w_1 + w_2 + \cdots + w_n) \geq n(w_1 + w_2 + \cdots + w_{n-1}).$$
Subtracting $(n-1)(w_1 + w_2 + \cdots + w_{n-1})$ from each side, we obtain
$$(n-1)w_n \geq w_1 + w_2 + \cdots + w_{n-1}, \tag{3.1}$$
which is true since $w_n \geq w_i$ for all i. Note that equality holds in (3.1) if and only if $w_i = w_n$ for all i. □

The following is the main result of the paper. It is equivalent to Theorem 1.1 and is stated here in terms of weights.

Theorem 3.2. *Let M be a simple, rank-r matroid representable over $GF(q)$, and let w be a weight function on M. Suppose $M \not\cong P_r$. Then*
$$\frac{w(M)}{g^*(M)} \geq \frac{q}{q-1}.$$

Moreover, equality holds if and only if, for a fixed embedding of M in P_r,

(i) *the complement of M is isomorphic to P_k, with $1 \leq k < r$; and*
(ii) *if P is a copy of P_{k+1} containing the complement of M in P_r, then w is constant on P; and*
(iii) *$w(N) \geq (q-1)w(E(M) - E(N))$ for every A_r-restriction N of M.*

Proof. We begin by proving the displayed inequality by induction on r. Lemma 3.1 gives the result when $r = 2$ since $|E(M)| < |E(P_2)| = q + 1$. Suppose $r \geq 3$. If there is an e in $E(M)$ with $M/e \ncong P_{r-1}$, then, by induction,

$$(q-1)w(M) > (q-1)w(M/e) \geq qg^*(M/e) \geq qg^*(M).$$

Thus we may assume that $M/e \cong P_{r-1}$ for all e in $E(M)$. Take a line of P_r that meets both $E(M)$ and $E(P_r) - E(M)$. Let X be the set of elements of M on this line and e be a maximum-weight element of X. Let $Y = X - e$. Note that $|Y| \leq q - 1$, so

$$w(Y) \leq w(e)(q-1). \tag{3.2}$$

Observe that $M\backslash Y/e$ has rank $r-1$ but is not isomorphic to P_{r-1} so, by the induction assumption,

$$(q-1)w(M\backslash Y/e) \geq qg^*(M\backslash Y/e).$$

Now

$$w(M\backslash Y/e) = w(M) - w(e) - w(Y),$$

and

$$g^*(M\backslash Y/e) \geq g^*(M) - w(Y).$$

Thus

$$(q-1)w(M) \geq qg^*(M) + w(e)(q-1) - w(Y),$$

so, by (3.2),

$$(q-1)w(M) \geq qg^*(M)$$

as desired.

Next we characterize when equality is achieved in the last bound. Let M^c be the complement of the fixed embedding of M in P_r. When $M^c \cong P_k$ for $1 \leq k < r$, a hyperplane of P_r either contains this P_k or meets it in a P_{k-1}. Thus a cocircuit of M is isomorphic to either A_r or $A_r - A_k$. We call these *type-I* and *type-II cocircuits*, respectively, noting that there are no type-I cocircuits when $k = r - 1$.

3.2.1. *Suppose M satisfies (i) and (ii). If C^* is a type-II cocircuit of M, then*

$$w(C^*) = \frac{q-1}{q}w(M).$$

As M satisfies (i), $M^c \cong P_k$. Since C^* is a type-II cocircuit, there is a restriction A of P_r isomorphic to A_r such that A meets M^c and $C^* = E(M) \cap E(A)$. Let H be the hyperplane of P_r that is the complement of A.

Now, P_r consists of $\frac{q^{r-k}-1}{q-1}$ copies of P_{k+1} containing M^c, and the pairwise intersection of these copies is M^c. Thus M is the disjoint union of $\frac{q^{r-k}-1}{q-1}$ copies of A_{k+1}. By (ii), the elements in each A_{k+1} have the same weight. To complete the proof of 3.2.1, we show that C^* contains exactly $\frac{q-1}{q}$ of the elements of each A_{k+1}.

Consider the complementary A_{k+1} to M^c in a fixed P_{k+1}. Note that P_{k+1} consists of $q+1$ copies of P_k, including M^c, that contain $H \cap E(M^c)$, which is isomorphic to P_{k-1}. Therefore, this A_{k+1} is the disjoint union of q copies of A_k. Now H meets P_{k+1} at a P_k distinct from M^c. Thus A meets P_{k+1} in a set that is the union of q disjoint copies of A_k, one of which is in M^c. This implies that $C^* \cap A_{k+1}$ is the disjoint union of $q-1$ copies of A_k, and 3.2.1 follows.

Now assume that $\frac{w(M)}{g^*(M)} = \frac{q}{q-1}$. Then equality holds in (3.2) so $|Y| = q-1$ and $w(y) = w(e)$ for all $y \in Y$. The former implies that every line of P_r that meets both M and M^c contains exactly q points of M. This means that every line that contains two points of M^c lies entirely in M^c. Thus M^c is a flat of P_r, proving (i).

As $w(y) = w(e)$ for all $y \in Y$, it follows that w is constant on each line of P_r that meets both M and M^c. Since a P_k contained in a P_{k+1} meets every line of the P_{k+1}, (ii) is satisfied. It now follows from 3.2.1 that $\frac{w(M)}{g^*(M)} = \frac{q}{q-1}$ if and only if M satisfies (i) and (ii), and the type-I cocircuits of M have weight at least $\frac{q-1}{q}w(M)$. It is straightforward to check that this third condition is equivalent to (iii), so the theorem holds. □

The reader may find condition (iii) of Theorem 3.2 unsatisfying, and the next proposition offers a potential replacement, (iii)$'$. The example that follows Proposition 3.3 shows that conditions (i), (ii), and (iii)$'$ do not guarantee $\frac{w(M)}{g^*(M)} = \frac{q}{q-1}$ for a matroid M meeting the hypotheses of Theorem 3.2. In addition, the example illustrates the potential difficulty of finding a satisfactory replacement for (iii).

Proposition 3.3. *Let M be a simple, rank-r matroid representable over $GF(q)$, and let w be a weight function on M. Suppose that $M \ncong P_r$ and that $\frac{w(M)}{g^*(M)} = \frac{q}{q-1}$. Then*

(iii)$'$ *$q^{r-1}w(e) \leq w(M)$ for all e in $E(M)$.*

Proof. By Theorem 3.2, $M^c = P_k$. If $k = r-1$, then Theorem 3.2(ii) implies that (iii)$'$ holds with equality. Thus we may assume that $k < r-1$. Extend the weight function of M to P_r by assigning each element of M^c a weight of one. Then contract M^c from P_r to form a weighted matroid $M' \cong P_{r-k}$. Fix an element e in $E(M)$, and let e' be the image of e in M'. Note that

$w(M') = w(M)$ and $w(e') = q^k w(e)$ under this transformation. Moreover, the type-I cocircuits of M correspond to the cocircuits of M', so the weight of each cocircuit of M' equals the weight of the corresponding type-I cocircuit of M.

Let C^* be a cocircuit of M' that avoids e' and let H be the complementary hyperplane to C^* in M'. Since $\frac{w(M)}{g^*(M)} = \frac{q}{q-1}$, it follows that

$$\frac{q}{q-1} w(C^*) \geq w(M'),$$

and subtracting $w(C^*)$ from each side produces

$$\frac{1}{q-1} w(C^*) \geq w(H). \tag{3.3}$$

Note that (3.3) holds for an arbitrary cocircuit of M' avoiding e', so we have such an inequality for every such cocircuit. Moreover, C^* and H partition $E(M')$ so, for a fixed $f \in E(M' \backslash e')$, its weight contributes to exactly one side of each inequality. Now, there are $\frac{q^{r-k-1}-1}{q-1}$ total inequalities as this is the number t of hyperplanes of M' containing e'. Similarly, $w(f)$ contributes to the right-hand side of exactly $\frac{q^{r-k-2}-1}{q-1}$ of these inequalities as this is the number s of hyperplanes of M' containing both e' and f. Hence $w(f)$ contributes to the left-hand side of $t-s$ of these inequalities. Summing these inequalities gives

$$\frac{t-s}{q-1} w(M' \backslash e') \geq s w(M' \backslash e') + t w(e'),$$

and this simplifies to

$$w(M') \geq q^{r-k-1} w(e').$$

Finally, we substitute $w(M)$ for $w(M')$ and $q^k w(e)$ for $w(e')$ to obtain

$$w(M) \geq q^{r-1} w(e)$$

as desired. □

Example 3.4. Let $q = 2$ and let $M = P_4 - p$ for some $p \in E(P_4)$. Then $M \cong P_4 - P_1$. Take a hyperplane H of P_4 containing p, and note that H has $|P_3|$ elements. Then $H - p$ is a hyperplane of M and the corresponding cocircuit C^* is type-I and has $|A_4|$ elements.

Assign the weight 2 to each element of $H - p$ and the weight 1 to each element of C^*. Then

$$w(M) = 2(|P_3| - 1) + 1 \cdot |A_4| = 2(6) + 8 = 20.$$

Observe that conditions (i) and (ii) of Theorem 3.2 hold and, since, for all e in $E(M)$,

$$q^{r-1} w(e) \leq 2^3(2) < 20 = w(M),$$

so does (iii)$'$. However, $w(C^*) = 8$, so the equation

$$\frac{w(M)}{g^*(M)} = \frac{q}{q-1} \tag{3.4}$$

fails.

Now, in P_4, take a line in $C^* \cup p$ and another in H that each meet in $\{p\}$. Swap the weights 1 and 2 on the elements of M on these lines. Note that (i), (ii), and (iii)$'$ continue to hold, and $w(M)$ is unchanged. However, it is straightforward to check that the weights of the type-I cocircuits of M are at least 10, so (3.4) holds by Theorem 3.2. Thus, characterizing the matroids for which equality holds in Theorem 3.2 requires not only restricting the weights themselves, but also controlling their distribution.

Finally, we prove a proposition equivalent to Proposition 1.2 stated here in terms of weights.

Proposition 3.5. *Let M be a matroid isomorphic to $PG(r-1, q)$ and w be a weight function on $E(M)$. Then*

$$\frac{w(M)}{g^*(M)} \geq \frac{q^r - 1}{q^{r-1}(q-1)}.$$

Moreover, equality holds if and only if w is constant.

Proof. We prove the inequality by induction on r. It is trivial when $r = 1$ and is true for $r = 2$ by Lemma 3.1, so suppose $r \geq 3$. Let C^* be a cocircuit of M of weight $g^*(M)$ and let H be the complementary hyperplane to C^* in M. Choose Z as a maximum-weight hyperplane of H. Then, letting Y be the complement of Z in H, we have

$$\frac{w(M)}{g^*(M)} = \frac{w(C^*) + w(Y) + w(Z)}{w(C^*)} = 1 + \frac{w(Y) + w(Z)}{w(C^*)}. \tag{3.5}$$

Observe that the weighted contraction of Z from M is isomorphic to P_2 so, by the inequality for $r = 2$, we get that

$$\frac{w(M/Z)}{g^*(M/Z)} \geq \frac{q+1}{q}.$$

Now, since C^* is also a minimum-weight cocircuit of M/Z, we rewrite this inequality as

$$\frac{w(Y) + w(C^*)}{w(C^*)} \geq \frac{q+1}{q}. \tag{3.6}$$

It follows that $qw(Y) \geq w(C^*)$. Substituting into (3.5), we obtain

$$\frac{w(M)}{g^*(M)} \geq 1 + \frac{1}{q} \cdot \frac{w(Y) + w(Z)}{w(Y)}. \tag{3.7}$$

Finally, the hyperplane H is isomorphic to P_{r-1}, and our choice of Z makes Y a minimum-weight cocircuit of H. Thus, by induction,

$$\frac{w(Y) + w(Z)}{w(Y)} \geq \frac{q^{r-1} - 1}{q^{r-2}(q-1)}. \tag{3.8}$$

Substituting (3.8) into (3.7) gives the desired inequality.

One easily checks that, when w is constant,

$$\frac{w(M)}{g^*(M)} = \frac{q^r - 1}{q^{r-1}(q-1)}. \tag{3.9}$$

We now use induction on r to prove that the elements of M have the same weight when (3.9) holds. When $r = 1$, this is trivial, and Lemma 3.1 handles the rank-2 case.

Suppose $r \geq 3$. Since (3.9) holds, equality holds in (3.6) and (3.8). It follows from the latter using the induction assumption that the weight function w on $E(M)$ is constant on the hyperplane H of M. From the former, we deduce that, in M/Z, every point has equal weight. It follows that every hyperplane H' of M containing Z has the same weight. Hence the cocircuit $E(M) - H'$ has the same weight as C^*. Replacing H by H', we deduce that w is constant on the elements of H'. Letting H' range over all of the hyperplanes of M containing Z, we deduce that w is constant on $E(M)$. □

Acknowledgements

The authors thank the referee for a number of helpful comments.

References

[1] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

[2] I. F. Blake and R. C. Mullin, An Introduction to Algebraic and Combinatorial Coding Theory, Academic Press, New York, 1976.

[3] R.C. Bose, R.C. Burton, A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and MacDonald codes, J. Combinatorial Theory 1 (1966), 96–104.

[4] V. Guruswami, Introduction to Coding Theory, Notes 4, Elementary Bounds on Codes, January, 2010. Retrieved May 23, 2022 from http://www.cs.cmu.edu/~venkatg/teaching/codingtheory/notes/notes4.pdf.

[5] R. Hill, A First Course in Coding Theory, Oxford University Press, New York, 1986.

[6] J. Oxley, Matroid Theory, Second edition, Oxford University Press, New York, 2011.

[7] M. Plotkin, Binary Codes with specified minimum distance, IRE Trans. IT-6 1960, 445–450.

[8] A. Vardy, The intractability of computing the minimum distance of a code, IEEE Trans. Inform. Theory 43 (1997), 1757–1766.

Mathematics Department, Louisiana State University, Baton Rouge, Louisiana, USA
Email address: ccrens5@lsu.edu

Mathematics Department, Louisiana State University, Baton Rouge, Louisiana, USA
Email address: oxley@math.lsu.edu