ODD CIRCUITS IN DENSE BINARY MATROIDS

JIM GEELEN AND PETER NELSON

Abstract. We show that, for each real number $\alpha > 0$ and odd integer $k \geq 5$ there is an integer c such that, if M is a simple binary matroid with $|M| \geq \alpha 2^{r(M)}$ and with no k-element circuit, then M has critical number at most c. The result is an easy application of a regularity lemma for finite abelian groups due to Green.

1. Introduction

We prove the following:

Theorem 1.1. *For each real number $\alpha > 0$ and odd integer $k \geq 5$, there exists $c \in \mathbb{Z}$ such that, if M is a simple binary matroid M with $|M| \geq \alpha 2^{r(M)}$ and with no k-element circuit, then M has critical number at most c.*

The restriction to excluding *odd* circuits from a *binary* matroid here is natural. The geometric density Hales-Jewett theorem [2] implies that dense GF(q)-representable matroids with sufficiently large rank necessarily contain arbitrarily large affine geometries over GF(q), which contain all even circuits when $q = 2$ and all circuits when $q > 2$. So dense k-circuit free GF(q)-representable matroids of large rank only exist when $q = 2$ and k is odd.

Our main theorem (Theorem 3.1) is somewhat more general than Theorem 1.1; it bounds the critical number of any sufficiently dense binary matroid whose elements are each contained in at most $o(2^{(k-2)r})$ circuits of size k. Note that each element of PG$(r-1, 2)$ is contained in at most $2^{(k-2)r}$ circuits of size k, so our result is best possible up to a constant factor. We obtain the theorem as an easy application of Green's regularity lemma for finite abelian groups [3], which we review in Section 2.

Date: March 7, 2014.

1991 *Mathematics Subject Classification.* 05B35.

Key words and phrases. matroids, regularity.

This research was partially supported by a grant from the Office of Naval Research [N00014-10-1-0851].

Recall that, if M is a simple rank-r binary matroid considered as a restriction of the binary projective geometry $G \cong \mathrm{PG}(r-1,2)$, then the *critical number* of M is the minimum $c \in \mathbb{Z}_0^+$ such that G has a rank-$(r-c)$ flat disjoint from $E(M)$. Equivalently, the critical number is the minimum number of "cocycles" needed to cover $E(M)$, where by a cocycle we mean a disjoint union of cocircuits. Thus cocycles correspond to cuts in a graph and, hence, critical number is a geometric analog of chromatic number.

Theorem 1.1 is analogous to the following theorem due to Thomassen [6].

Theorem 1.2. *For each real number $\alpha > 0$ and odd integer $k \geq 5$, there exists $c \in \mathbb{Z}$ such that every simple graph on n vertices with minimum degree at least αn and no k-cycle has chromatic number at most c.*

Theorem 1.2 does not extend to the case that $k = 3$; for each $\varepsilon > 0$, Hajnal (see [1]) gave examples of triangle-free graphs G with minimum degree at least $(\frac{1}{3} - \varepsilon)|V(G)|$ and with arbitrarily large chromatic number. Nevertheless, we conjecture that Theorem 1.1 also holds for $k = 3$. That is:

Conjecture 1.3. *For each real number $\alpha > 0$ there exists $c \in \mathbb{Z}$ such that, if M is a simple triangle-free binary matroid with $|M| \geq \alpha 2^{r(M)}$, then M has critical number at most c.*

Green's regularity lemma gives a weaker outcome:

Theorem 1.4. *For each real number $\varepsilon > 0$ there exists $c \in \mathbb{Z}$ such that, if M is a triangle-free restriction of a binary projective geometry $G \cong \mathrm{PG}(r-1,2)$, then there is a flat F of G such that $r(F) \geq r(G) - c$ and $|F \cap E(M)| \leq \varepsilon 2^{r(F)}$.*

2. Regularity

We will largely use the standard notation of matroid theory [4], but it will also be convenient to think of a rank-r binary matroid as a subset of the vector space $V = \mathrm{GF}(2)^r$. This change is purely notational; if $X \subseteq V$ then we write $M(X)$ for the binary matroid on X represented by a binary matrix with column set X. If $0 \notin X$ then $M(X)$ is simple. We define the *critical number* of X to be the critical number of $M(X)$; that is, the minimum codimension of a subspace of V disjoint from X.

Green used Fourier-analytic techniques to prove his regularity lemma for abelian groups and to derive applications in additive combinatorics; these techniques are discussed in greater detail in the book of Tao and Vu [5, Chapter 4]. Fortunately, although this theory has many technicalities, the group $\mathrm{GF}(2)^n$ is among its simplest applications.

Let $V = \mathrm{GF}(2)^r$ and let $X \subseteq V$. Note that, if H is a codimension-1 subspace of V, then $|H| = |V \setminus H|$. We say that X is *ε-uniform* if for each codimension-1 subspace H of V we have

$$\big|\, |H \cap X| - |X \setminus H| \,\big| \leq \varepsilon |V|.$$

In Lemma 2.2 we will see that, for small ε, the ε-uniform sets are 'pseudorandom'.

Let H be a subspace of V. For each $v \in V$, let $H_v(X) = \{h \in H : h + v \in X\}$. For $\varepsilon > 0$, we say H is *ε-regular* with respect to V and X if $H_v(X)$ is ε-uniform in H for all but $\varepsilon|V|$ values of $v \in V$.

Regularity captures the way that X is distributed among the cosets of H in V. For $v \in V$, we let $X + v = \{x + v : x \in X\}$; thus $X + v$ is a translation of X. Note that $X + v$ is ε-uniform if and only if X is. Also note that $H_v(X) + v = X \cap H'$ where $H' = H + v$ is the coset of H in V that contains v. Therefore, if $u, v \in H'$, then $H_u(X)$ and $H_v(X)$ are translates of one another. So H is ε-regular if, for all but an ε-fraction of cosets H' of H, the set $(H' \cap X) + v$ is ε-uniform in H for some $v \in H'$.

The following result of Green [3] guarantees a regular subspace of bounded codimension. Here $W(t)$ denotes an exponential tower of 2's of height $\lceil t \rceil$.

Theorem 2.1 (Green's regularity lemma)**.** *Let $V = \mathrm{GF}(2)^n$, $X \subseteq V$, and let $\varepsilon > 0$ be a real number. Then there is a subspace H of v that is ε-regular with respect to X and V and has codimension at most $W(\varepsilon^{-3})$ in V.*

Let $A \subseteq V$ with $|A| = \alpha|V|$. For $x \in V$ and $k \in \mathbb{Z}$, we let $S(A, k; x)$ denote the set of k-tuples in A^k with sum equal to x. Clearly $|S(A, k; x)| \leq \alpha^{k-1}|V|^{k-1}$. If A were a random subset of V, we would expect around a $|V|^{-1}$-fraction of the tuples in A^k to sum to x, which would give $|S(A, k; x)| \approx \alpha^k |V|^{k-1}$; the next lemma, a corollary of [5, Lemma 4.13], bounds the error in such an estimate when A is uniform.

Lemma 2.2. *Let $V = \mathrm{GF}(2)^n$, let $x \in V$, and let $A \subseteq V$ with $|A| = \alpha|V|$. For each integer $k \geq 3$ and real $\varepsilon > 0$, if A is ε-uniform, then*

$$|S(A, k; x)| \geq (\alpha^k - \varepsilon^{k-2})|V|^{k-1}.$$

Observe that, if $x \in A$ and $\{x, a_1, \ldots, a_{k-1}\}$ is a k-element circuit in $M(A)$ that contains x, then $(a_1, \ldots, a_{k-1}) \in S(A, k-1; x)$. However the converse need not be true; if $(a_1, \ldots, a_{k-1}) \in S(A, k-1; x)$ then $\{x, a_1, \ldots, a_{k-1}\}$ is a k-element circuit unless some proper sub-tuple of $(a_1,\ldots,a_{k-1})$ sums to zero. We let $S_0(A,k;x)$ denote the set of k-tuples in $S(A,k;x)$ having some proper nonempty sub-tuple with sum 0. We argue that $S_0(A,k;x)$ is small.

Lemma 2.3. *Let $V=\mathrm{GF}(2)^n$, let k be an integer, let $x\in V$, and let $A\subseteq V$. Then $|S_0(A,k;x)|\le 2^k|A|^{k-2}$.*

Proof. If some subtuple has sum 0 then its complementary tuple has sum x. Summing over all possible nonempty sub-tuples, we have

$$\begin{aligned}|S_0(A,k;x)| &\le \sum_{i=1}^{k-1}\binom{k}{i}|S(A,i;0)||S(A,k-i;x)|\\ &\le \sum_{i=1}^{k-1}\binom{k}{i}|A|^{i-1}|A|^{k-i-1}\\ &\le 2^k|A|^{k-2}.\end{aligned}$$

□

3. The Main Result

Theorem 3.1. *For every real number $\alpha>0$ and odd integer $k\ge 5$, there exists a real number $\beta>0$ and integer c such that, if M is a simple binary matroid with $|M|\ge\alpha 2^{r(M)}$, then either M has critical number at most c, or some element of M is contained in at least $\beta 2^{(k-2)r(M)}$ distinct k-element circuits of M.*

Proof. Let $\alpha>0$ be real and let $k\ge 5$ be an odd integer. Choose $\varepsilon>0$ so that

$$(\alpha-\varepsilon)^{k-1}-\varepsilon^{k-3}>0,$$

let $\alpha_0=\alpha-\varepsilon$, and then choose $r_0\in\mathbb{Z}$ so that

$$\alpha_0^{k-1}-\varepsilon^{k-3}-2^{k-1+W(\varepsilon^{-3})-r_0}>0.$$

Let $s_0=W(\varepsilon^{-3})$, let $c=\max(r_0,s_0)$ and let

$$\beta=\frac{2^{(2-k)s_0}}{(k-1)!}\left(\alpha_0^{k-1}-\varepsilon^{k-3}-2^{k-1+s_0-r_0}\right).$$

By our choice of r_0, we have $\beta>0$.

Let M be a simple rank-r binary matroid with $|M|\ge\alpha 2^r$. Let $V=\mathrm{GF}(2)^r$ and let $X\subseteq V$ such that $M\cong M(X)$. By Green's regularity lemma, there is an ε-regular subspace H of V with codimension $s\le c$.

Claim 1. *There is some $a\in V$ such that $H_a(X)$ is ε-uniform in H and satisfies $|H_a(X)|\ge\alpha_0|H|$.*

Proof of claim: Let V_0 be the set of $v \in V$ for which $H_v(X)$ is not ε-uniform; we have $|V_0| \le \varepsilon|V|$ by regularity. In summing $|H_v(X)|$ over all $v \in V$, we count each $x \in X$ with multiplicity $|H|$, so

$$\sum_{v \in V} |H_v(X)| = |X||H| \ge \alpha|V||H|.$$

On the other hand, $\sum_{v \in V_0} |H_v(X)| \le \varepsilon|V||H|$. Thus there exists an element $a \in V \backslash V_0$ with

$$|H_a(X)| \ge \tfrac{\alpha|V||H| - \varepsilon|V||H|}{|V \backslash V_0|} \ge (\alpha - \varepsilon)|H| = \alpha_0|H|,$$

as required. □

Since $|H_a(X)|$ is constant as a ranges over each coset of H, we may choose $a = 0$ if $a \in H$. Let $A = H_a(X)$. We may assume that M has critical number greater than c and, hence, there exists $x \in H \cap X$.

Claim 2. $|S(A, k-1; x) \backslash S_0(A, k-1; x)| \ge \beta(k-1)!\ 2^{(k-2)r}$.

Proof of claim: By Lemma 2.2, we have

$$\begin{aligned} |S(A, k-1; x)| &\ge \left(\alpha_0^{k-1} - \varepsilon^{k-3}\right) |H|^{k-2} \\ &= \left(\alpha_0^{k-1} - \varepsilon^{k-3}\right) 2^{(k-2)(r-s)}. \end{aligned}$$

By Lemma 2.3 we have

$$\begin{aligned} |S_0(A, k-1; x)| &\le 2^{k-1}|A|^{k-3} \\ &\le 2^{k-1}|H|^{k-3} \\ &= 2^{k-1+s-r} 2^{(k-2)(r-s)} \end{aligned}$$

Combining these and using $r \ge r_0$ and $s \le s_0$, the claim follows. □

Let $w = (w_1, \ldots, w_{k-1}) \in S(A, k-1; x) \backslash S_0(A, k-1; x)$. The tuple $w' = (w_1 + a, w_2 + a, \ldots, w_{k-1} + a, x)$ is contained in X^k, sums to zero, and since no sub-tuple of w sums to zero, the elements of w' are distinct and have no sub-tuple summing to zero . (If $a = 0$ this is clear, and otherwise $a \notin H$ so the $w_i + a$ are distinct from x.) Therefore w' corresponds to a circuit of $M(X)$ containing x. Taking into account permutations of w, it follows that x is in at least $\beta 2^{(k-2)r}$ distinct k-element circuits of $M(X)$. □

4. Triangle-free binary matroids

Finally, to prove Theorem 1.4, we need a variation on Lemma 2.2, also following from [5, Lemma 4.13]. Let $V = \mathrm{GF}(2)^r$. For sets $A_1, A_2, A_3 \subseteq V$, let $T(A_1, A_2, A_3)$ be the set of triples in $A_1 \times A_2 \times A_3$ with sum zero.

Lemma 4.1. *Let $V \in \mathrm{GF}(2)^n$ and $\varepsilon > 0$. Let $A_1, A_2, A_3 \subseteq V$ with $|A_i| = \alpha_i|V|$. If A_1 is ε-uniform, then*

$$|T(A_1, A_2, A_3)| \geq (\alpha_1\alpha_2\alpha_3 - \varepsilon)|V|^2.$$

Proof of Theorem 1.4. Let $\varepsilon > 0$. Let δ be a real number such that $\varepsilon(\varepsilon - \delta)^2 > \delta > 0$, and let $c = W(\delta^{-3})$.

Let M be a simple rank-r triangle-free binary matroid. If $|M| \leq \varepsilon 2^r$ then the theorem holds, so we may assume for a contradiction that $|M| > \varepsilon 2^r$. Let $V = \mathrm{GF}(2)^r$ and $X \subseteq V$ be such that $M \cong M(X)$.

By Green's regularity lemma there is an δ-regular subspace H of V with codimension at most c. As in the first claim of the proof of Theorem 3.1, there is some $a \in Z$ such that $H_a(X)$ is δ-regular and satisfies $|H_a(X)| \geq \varepsilon - \delta$. We may choose a such that either $a = 0$ or $a \notin H$. Let $A = H_a(X)$.

If $|X \cap H| \leq \varepsilon|H|$, then the theorem holds. Otherwise, by Lemma 4.1, we have $|T(A, A, X \cap H)| \geq (\varepsilon(\varepsilon - \delta)^2 - \delta)|H|^2 > 0$, so there is some triple (x, y, z) with $x + y + z = 0$, where $x, y \in A$ and $z \in X \cap H$. Now $\{x + a, y + a, z\}$ is a triangle of $M(X)$, a contradiction. □

References

[1] P. Erdős, M. Simonovits, On a valence problem in extremal graph theory, Discrete Math. 5 (1973), 323-334.

[2] H. Furstenberg, Y. Katznelson, IP-sets, Szemerédi's Theorem and Ramsey Theory, Bull. Amer. Math. Soc. (N.S.) 14 no. 2 (1986), 275–278.

[3] B. Green, A Szemerédi-type regularity lemma in abelian groups, with applications, Geometric & Functional Analysis GAFA 15 (2005), 340–376.

[4] J. G. Oxley, Matroid Theory, Oxford University Press, New York (2011).

[5] T. C. Tao and V. H. Vu, Additive Combinatorics, Cambridge Studies in Advanced Mathematics, 105, Cambridge University Press, Cambridge (2006).

[6] C. Thomassen, On the chromatic number of pentagon-free graphs of large minimum degree, Combinatorica 27 (2007), 241–243.

Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Canada

Department of Mathematics, Statistics and Operations Research, Victoria University of Wellington, Wellington, New Zealand