Circuit decompositions of binary matroids

Bryce Frederickson[†] Lukas Michel[‡]

24 June 2023

Abstract

Given a simple Eulerian binary matroid M, what is the minimum number of disjoint circuits necessary to decompose M? We prove that $|M|/(\operatorname{rank}(M)+1)$ many circuits suffice if $M = \mathbb{F}_2^n \setminus \{0\}$ is the complete binary matroid, for certain values of n, and that $\mathcal{O}(2^{\operatorname{rank}(M)}/(\operatorname{rank}(M)+1))$ many circuits suffice for general M. We also determine the asymptotic behaviour of the minimum number of circuits in an odd-cover of M.

1 Introduction

Erdős and Gallai conjectured that the edge set of any graph on n vertices can be decomposed into $\mathcal{O}(n)$ edge-disjoint cycles and edges [Erd83]. Equivalently, this says that any Eulerian graph can be decomposed into $\mathcal{O}(n)$ edge-disjoint cycles. Despite receiving a lot of attention, the Erdős-Gallai Conjecture remains a major open problem in the area of graph decompositions. While a straightforward greedy argument that iteratively removes largest cycles yields a decomposition of size $\mathcal{O}(n \log n)$, it was only in 2014 that Conlon, Fox, and Sudakov [CFS14] improved this upper bound to $\mathcal{O}(n \log \log n)$. More recently, Bucić and Montgomery [BM22] showed that $\mathcal{O}(n \log^\star n)$ cycles suffice, where $\log^\star n$ is the iterated logarithm function.

Due to the difficulty of this problem, many variations of it have been considered. For example, if cycles can share edges, Fan proved that $\lfloor (n-1)/2 \rfloor$ cycles suffice to cover the edges of any Eulerian graph [Fan03]. In fact, the cover can be chosen so that every edge is covered an odd number of times. In a similar vein, Pyber proved that any graph can be covered by $n-1$ cycles and edges [Pyb85].

In this note, we consider a matroid analogue of the cycle decomposition question: what is the minimum number of disjoint circuits necessary to decompose a matroid? We focus on (simple) matroids representable over the finite field $\mathbb{F}_2$. Up to isomorphism, such matroids are equivalent to *(simple) binary matroids*, which are subsets $M \subseteq \mathbb{F}_2^n \setminus \{0\}$ for some $n \geq 1$. In this setting, M is *Eulerian* if $\sum_{x \in M} x = 0$, and a subset $N \subseteq M$ is a *circuit* if N is a minimal non-empty Eulerian subset of M with respect to inclusion.

We want to construct a circuit decomposition of M, that is, a small collection of disjoint circuits whose union is M. Observe that M admits a circuit decomposition if and only

[†]Department of Mathematics, Emory University, Atlanta, Georgia, 30322 (bfrede4@emory.edu).
[‡]Mathematical Institute, University of Oxford, United Kingdom (michel@maths.ox.ac.uk).

if M is Eulerian. In this case, we denote by $c(M)$ the minimum number of circuits in such a decomposition.

To obtain a lower bound on $c(M)$, note that every proper subset of a circuit in M is linearly independent. For any binary matroid M, the *rank* of M, denoted by $\operatorname{rank}(M)$, is the size of a largest linearly independent subset of M. Thus, any circuit in M can have size at most $\operatorname{rank}(M) + 1$, which implies that $c(M) \geq |M|/(\operatorname{rank}(M) + 1)$. For an Eulerian binary matroid M of size $\Theta(2^{\operatorname{rank}(M)})$, this lower bound gives $c(M) \geq \Theta(2^{\operatorname{rank}(M)}/(\operatorname{rank}(M) + 1))$. We prove a matching upper bound.

Theorem 1.1. *For every Eulerian binary matroid $M \subseteq \mathbb{F}_2^n \setminus \{0\}$ it holds that*

$$c(M) = \mathcal{O}\left(\frac{2^{\operatorname{rank}(M)}}{\operatorname{rank}(M) + 1}\right).$$

In fact, for certain values of n, we show that $M = \mathbb{F}_2^n \setminus \{0\}$, which we call the *complete binary matroid* of dimension n,[1] can be decomposed into exactly $|M|/(\operatorname{rank}(M) + 1)$ many circuits, where $|M| = 2^n - 1$ and $\operatorname{rank}(M) = n$.

Theorem 1.2. *Let p be an odd prime for which the multiplicative order of 2 modulo p is $p - 1$, and let $M \subseteq \mathbb{F}_2^{p-1} \setminus \{0\}$ be the complete binary matroid of dimension $p - 1$. Then*

$$c(M) = \frac{2^{p-1} - 1}{p}.$$

For arbitrary Eulerian binary matroids, we prove the following upper bound on the size of a circuit decomposition.

Theorem 1.3. *For every Eulerian binary matroid $M \subseteq \mathbb{F}_2^n \setminus \{0\}$ it holds that*

$$c(M) \leq (1 + o(1)) \frac{|M| \log(\operatorname{rank}(M))}{\log|M|} \quad \text{as} \quad |M| \to \infty.$$

This bound is the correct order of magnitude for certain sparse binary matroids. For instance, if M consists of k independent copies of $\mathbb{F}_2^2 \setminus \{0\}$, then $c(M) = k$ and

$$\frac{|M| \log(\operatorname{rank}(M))}{\log|M|} = \frac{3k \log(2k)}{\log(3k)} = (3 + o(1))k.$$

In addition to circuit decompositions, we will also consider circuit odd-covers. For a graph G, an odd-cover is a collection of graphs on the same vertex set that covers each edge of G an odd number of times and each non-edge of G an even number of times. As mentioned above, every n-vertex Eulerian graph has an odd-cover with $\lfloor (n-1)/2 \rfloor$ cycles. More recently, Borgwardt, Buchanan, Culver, Frederickson, Rombach, and Yoo [BBC+23] proved that every Eulerian graph of maximum degree Δ has an odd-cover with Δ cycles. Odd-covers were introduced by Babai and Frankl [BF88] and were also studied in [BPR22] and [BCC+22].

[1] This is equivalent to the projective geometry $PG(n-1, 2)$ in the literature [Oxl92].

A *circuit odd-cover* of a binary matroid M is a collection of circuits $C_1, \dots, C_t \subseteq \mathbb{F}_2^n$ such that $C_1 \oplus \cdots \oplus C_t = M$ where $A \oplus B$ denotes the symmetric difference of A and B. In such an odd-cover, the elements of M are covered an odd number of times while the elements of $\mathbb{F}_2^n \setminus M$ are covered an even number of times. Note that, similar to the decomposition setting, the condition that M is Eulerian is necessary and sufficient for the existence of a circuit odd-cover of M.

We denote by $c_2(M)$ the minimum number of circuits in a circuit odd-cover of M. Since every circuit decomposition is also a circuit odd-cover, we have $c_2(M) \leq c(M)$. We can obtain the following natural lower bound for $c_2(M)$.

Proposition 1.4. *For every Eulerian binary matroid $M \subseteq \mathbb{F}_2^n \setminus \{0\}$ it holds that*

$$c_2(M) \geq \max_{N \subseteq M} \left\lceil \frac{|N|}{\operatorname{rank}(N) + 1} \right\rceil.$$

Proof. Consider a circuit odd-cover $C_1, \dots, C_t$ of M. For every subset $N \subseteq M$, each C_i intersects N in at most $\operatorname{rank}(N) + 1$ elements since every proper subset of C_i is linearly independent. The elements of N must each be covered by $C_1, \dots, C_t$ an odd number of times, so in particular, they must each be covered at least once. This implies that $t \cdot (\operatorname{rank}(N) + 1) \geq |N|$. □

The lower bound given in Proposition 1.4 is closely related to the *arboricity* of M, denoted $a(M)$, which is the minimum t such that M can be expressed as the union (or equivalently, as the symmetric difference) of t linearly independent sets. In the case of graphic matroids, a decomposition of the matroid into independent sets coincides with a decomposition of the edge set of a corresponding graph into forests, whence the name arboricity. A celebrated theorem of Edmonds [Edm65] asserts that

$$a(M) = \max_{\varnothing \neq N \subseteq M} \left\lceil \frac{|N|}{\operatorname{rank}(N)} \right\rceil.$$

Since $|N| \leq 2^{\operatorname{rank}(N)}$, we have by Proposition 1.4 that

$$c(M) \geq c_2(M) \geq (1 + o(1))a(M) \quad \text{as} \quad a(M) \to \infty. \tag{1}$$

For $c(M)$, we cannot hope to attain this lower bound. For instance, if $M \subseteq \mathbb{F}_2^n \setminus \{0\}$ consists of k independent copies of $\mathbb{F}_2^s \setminus \{0\}$, then $c(M) \geq k$ but the arboricity of M is only $a(M) = \lceil (2^s - 1)/s \rceil$. However, for $c_2(M)$, we show that the lower bound is tight.

Theorem 1.5. *For every Eulerian binary matroid $M \subseteq \mathbb{F}_2^n \setminus \{0\}$ it holds that*

$$c_2(M) \leq \frac{4}{3} a(M) \qquad \textit{and} \qquad c_2(M) = (1 + o(1))a(M) \quad \textit{as} \quad a(M) \to \infty.$$

The rest of the paper is organized as follows. In Section 2 we construct circuit decompositions for arbitrary binary matroids and prove Theorems 1.1 and 1.3. We then specialise to the complete binary matroid and provide a proof of Theorem 1.2 in Section 3. Theorem 1.5 is proven in Section 4, and we conclude in Section 5 with some open problems.

2 Decomposing arbitrary binary matroids into circuits

To decompose any binary matroid M into circuits, our main method is to greedily remove the largest circuit in M that we can find. The following lemma gives an implicit lower bound on the size of such a circuit.

Lemma 2.1. *Let $M \subseteq \mathbb{F}_2^n \setminus \{0\}$ be a binary matroid and $c \geq 2$ be an integer. If M contains no circuit of size larger than c, then*

$$|M| \leq \sum_{i=1}^{c-1} \binom{\operatorname{rank}(M)}{i}.$$

Proof. Let $r = \operatorname{rank}(M)$ and let $B = \{b_1, \ldots, b_r\} \subseteq M$ be a basis of M. For every $m \in M \setminus B$, there exists a unique nonempty subset $I \subseteq [r]$ such that $m = \sum_{i \in I} b_i$.

We claim that $C = \{m\} \cup \{b_i : i \in I\}$ is a circuit. Indeed, $m + \sum_{i \in I} b_i = 0$. Moreover, if $\varnothing \neq D \subseteq C$ with $\sum_{x \in D} x = 0$, it cannot hold that $D \subseteq B$ since B is an independent set. Hence, $D = \{m\} \cup \{b_j : j \in J\}$ for some set $J \subseteq I$. This implies that m is in the span of $\{b_j : j \in J\}$. So, by uniqueness of I, we must have $J = I$ and thus $D = C$. This shows that C is a circuit.

Because M contains no circuit of size larger than c, we know that $|I| + 1 = |C| \leq c$ and thus $|I| \leq c - 1$. As $m \notin B \cup \{0\}$, we also know that $|I| \geq 2$. Moreover, the set I entirely determines m. Therefore,

$$|M| = |B| + |M \setminus B| \leq r + \sum_{i=2}^{c-1} \binom{r}{i} = \sum_{i=1}^{c-1} \binom{r}{i}. \qquad \square$$

If we now apply the greedy algorithm that always removes the largest circuit of M, whose size we lower bound by the preceding lemma, we can prove Theorem 1.3.

Proof of Theorem 1.3. We assume that M is nonempty. Let $r = \operatorname{rank}(M) \geq 2$. We claim that if $N \subseteq M$ is Eulerian and nonempty, then N contains a circuit of size at least $\log|N| / \log r$. If not, this value would have to be larger than three since N contains some circuit and every circuit has size at least three. But then N would contain no circuit of size larger than $c = \lfloor \log|N| / \log r \rfloor \geq 3$ and so Lemma 2.1 would imply that

$$\begin{aligned} |N| &\leq \sum_{i=1}^{c-1} \binom{\operatorname{rank}(N)}{i} \leq \sum_{i=1}^{c-1} \binom{r}{i} \leq \sum_{i=1}^{c-1} r^i \\ &= \frac{r^c - r}{r - 1} < r^c \leq |N|, \end{aligned}$$

giving a contradiction.

To decompose M into circuits, we start with $N = M$ and repeatedly remove a maximum circuit from N until N is empty. During this process, N remains Eulerian. While N satisfies $|N| \geq |M| / \log^2|M|$, we know from the discussion above that N contains a circuit of size at least

$$\frac{\log|N|}{\log r} \geq \frac{\log|M| - 2\log\log|M|}{\log r}.$$

Hence, after at most

$$\frac{|M|}{\frac{\log|M|-2\log\log|M|}{\log r}} = (1+o(1))\frac{|M|\log r}{\log|M|}$$

many steps, N will satisfy $|N| \leq |M|/\log^2|M|$. Note that

$$|N| \leq \frac{|M|}{\log^2|M|} \leq \frac{2|M|\log r}{\log^2|M|} = o(1)\frac{|M|\log r}{\log|M|}.$$

Hence, by decomposing N into at most $|N|/3$ circuits, we decompose M into at most

$$(1+o(1))\frac{|M|\log r}{\log|M|}$$

many circuits, as required. □

Next, we want to prove Theorem 1.1. If M has size $\mathcal{O}(2^{\operatorname{rank}(M)}/\log(\operatorname{rank}(M)))$, Theorem 1.3 already tells us that $c(M) = \mathcal{O}(2^{\operatorname{rank}(M)}/(\operatorname{rank}(M)+1))$. Thus, it suffices to prove this bound if M is very dense, meaning that its size is close to $2^{\operatorname{rank}(M)}$.

In this setting, we still want to use the greedy algorithm to decompose M into circuits. However, the lower bound on the circuit size used in the preceding proof will no longer be sufficient. Instead, if M is dense, we need to show that there are circuits of size $\Theta(\operatorname{rank}(M))$ to obtain the desired result. To this end, we use the following standard entropy bound on the sum of binomial coefficients. Here, we denote the binary entropy function by $H(\alpha) = -\alpha\log_2\alpha - (1-\alpha)\log_2(1-\alpha)$.

Lemma 2.2. *Let r be a positive integer. Then for any $\alpha \in [0, 1/2]$ we have*

$$\sum_{i=0}^{\lfloor \alpha r \rfloor} \binom{r}{i} \leq 2^{H(\alpha)r}.$$

Proof. Note that $\alpha \leq 1-\alpha$ and therefore

$$\begin{aligned}\sum_{i=0}^{\lfloor \alpha r \rfloor} \binom{r}{i} &\leq \sum_{i=0}^{\lfloor \alpha r \rfloor} \binom{r}{i}\left(\frac{1-\alpha}{\alpha}\right)^{\alpha r - i} \\ &= \frac{1}{\alpha^{\alpha r}(1-\alpha)^{(1-\alpha)r}} \sum_{i=0}^{\lfloor \alpha r \rfloor} \binom{r}{i}(1-\alpha)^{r-i}\alpha^i \\ &\leq \frac{1}{\alpha^{\alpha r}(1-\alpha)^{(1-\alpha)r}} = 2^{H(\alpha)r}.\end{aligned}$$

□

By combining this entropy bound with Lemma 2.1, we can now prove that every dense binary matroid M has circuits of size $\Theta(\operatorname{rank}(M))$ and can therefore be decomposed into $\mathcal{O}(|M|/(\operatorname{rank}(M)+1))$ many circuits.

Theorem 2.3. *For any $\varepsilon > 0$, there exist $r_0 \in \mathbb{N}$ and $\delta > 0$ such that every Eulerian binary matroid $M \subseteq \mathbb{F}_2^n \setminus \{0\}$ with $\operatorname{rank}(M) \geq r_0$ and $|M| \geq 2^{(1-\delta)\operatorname{rank}(M)}$ satisfies*

$$c(M) \leq (2+\varepsilon)\frac{|M|}{\operatorname{rank}(M)+1}.$$

Proof. Let $\alpha = 1/(2+\varepsilon/2)$ and $\delta = (1-H(\alpha))/2$. It is easily verified that $H(x)$ is strictly increasing on $[0,1/2]$ with $H(1/2) = 1$, and so we have $\delta > 0$. Let M be an Eulerian binary matroid with $r = \operatorname{rank}(M)$ and $|M| \geq 2^{(1-\delta)r}$. By Lemma 2.2,

$$\sum_{i=1}^{\lfloor \alpha r \rfloor} \binom{r}{i} \leq 2^{H(\alpha)r} = 2^{(1-2\delta)r} < |M|,$$

so we know by Lemma 2.1 that M contains a circuit of size at least αr. We remove circuits of this size until the remaining Eulerian binary matroid N has size $|N| \leq 2^{(1-2\delta)r}$. The number of circuits removed so far is at most $|M|/(\alpha r)$, and N can be decomposed into at most $|N|/3$ circuits. Now,

$$\frac{|N|}{3} \leq \frac{2^{(1-2\delta)r}}{3} \leq \frac{2^{-\delta r}|M|}{3} = o\left(\frac{|M|}{r+1}\right).$$

Thus we have

$$\begin{aligned} c(M) &\leq \frac{|M|}{\alpha r} + o\left(\frac{|M|}{r+1}\right) \\ &= \left(\frac{r+1}{r}(2+\varepsilon/2) + o(1)\right)\frac{|M|}{r+1} \\ &\leq (2+\varepsilon)\,\frac{|M|}{r+1} \end{aligned}$$

for r sufficiently large. □

In particular, if M is dense, this result implies that $c(M)$ is within a factor of $2+o(1)$ of the lower bound $|M|/(\operatorname{rank}(M)+1)$ from the introduction. Theorem 1.1 is now an easy consequence.

Proof of Theorem 1.1. Let δ and r_0 be as in Theorem 2.3 with $\varepsilon = 1/2$. If $\operatorname{rank}(M) \geq r_0$ and $|M| \geq 2^{(1-\delta)\operatorname{rank}(M)}$, the theorem implies $c(M) \leq \mathcal{O}(2^{\operatorname{rank}(M)}/(\operatorname{rank}(M)+1))$. Otherwise, M can be decomposed into at most $|M|/3$ circuits, and

$$\frac{|M|}{3} \leq 2^{(1-\delta)\operatorname{rank}(M)} = \frac{2^{\operatorname{rank}(M)}}{2^{\delta \operatorname{rank}(M)}} = o\left(\frac{2^{\operatorname{rank}(M)}}{\operatorname{rank}(M)+1}\right). \qquad \square$$

3 Decomposing complete binary matroids into circuits

In this section we prove Theorem 1.2, so we decompose the complete binary matroid M into circuits. We will construct the circuits of this decomposition as orbits under a particular group action on M. This special structure allows us to show that M can be decomposed into exactly $|M|/(\operatorname{rank}(M)+1)$ many circuits, as required.

Proof of Theorem 1.2. For $i \in \mathbb{Z}_p$, we write $e_i \in \mathbb{F}_2^p$ for the i-th standard basis vector of $\mathbb{F}_2^p$. For $x \in \mathbb{F}_2^p$, we denote by $x_i = \langle x, e_i \rangle$ the i-th coordinate of x. Define

$$N = \left\{ x \in \mathbb{F}_2^p \setminus \{0\} \;\middle|\; \sum_{i \in \mathbb{Z}_p} x_i = 0 \right\}.$$

Note that N is isomorphic to M since $\operatorname{rank}(N) = p-1$ and $|N| = 2^{\operatorname{rank}(N)} - 1$.

Consider the following group action of $\mathbb{Z}_p$ on N defined for $j \in \mathbb{Z}_p$ by the linear map

$$\phi_j(x) = \sum_{i \in \mathbb{Z}_p} x_i e_{i+j} = (x_{p-j}, x_{p-j+1}, \ldots, x_{p-1}, x_0, x_1, \ldots, x_{p-j-1}).$$

We claim that the orbits in N under this action are circuits of size p, which gives us a decomposition of N into such circuits.

Consider an orbit $O = \{\phi_j(x) \mid j \in \mathbb{Z}_p\}$ for some $x \in N$. By definition of N, $\sum_{i \in \mathbb{Z}_p} x_i = 0$, and so because p is odd we must have $x_i \neq x_{i+1}$ for some i. This implies that $\phi_1(x) \neq x$ and therefore $|O| \geq 2$. Since $|O|$ divides p by the Orbit-Stabilizer Theorem and because p is prime, it follows that $|O| = p$.

It remains to show that O is a circuit. First, we show that since 2 has multiplicative order $p-1$ in $\mathbb{Z}_p$, the polynomial $(t^p - 1)/(t-1) = t^{p-1} + \cdots + t + 1$ is irreducible over $\mathbb{F}_2$. Let $\omega \neq 1$ be a p-th root of unity over $\mathbb{F}_2$, and let $g(t)$ be its minimal polynomial over $\mathbb{F}_2$. Recall that $g(t)$ is irreducible over $\mathbb{F}_2$ and has the form $\prod_{i=1}^{k}(t - \omega_i)$ over the splitting field K of ω, where $\omega_1, \ldots, \omega_k \in K$ are the distinct Galois conjugates of ω over $\mathbb{F}_2$. Repeated application of the Frobenius automorphism $\alpha \mapsto \alpha^2$ in K gives $p-1$ distinct Galois conjugates of ω, namely $\omega, \omega^2, \omega^{2^2}, \ldots, \omega^{2^{p-2}}$. Thus $\deg g(t) = k \geq p-1$, so $g(t) = (t^p - 1)/(t-1)$ is irreducible over $\mathbb{F}_2$.

Now, let $\phi = \sum_{i \in \mathbb{Z}_p} x_i \phi_i = \sum_{i \in \mathbb{Z}_p} x_i \phi_1^i$, where we identify $\mathbb{Z}_p$ with $\{0, \ldots, p-1\}$. Note that O can be rewritten as

$$O = \left\{ \sum_{i \in \mathbb{Z}_p} x_i e_{i+j} \;\middle|\; j \in \mathbb{Z}_p \right\} = \left\{ \sum_{i \in \mathbb{Z}_p} x_i \phi_i(e_j) \;\middle|\; j \in \mathbb{Z}_p \right\} = \{\phi(e_j) \mid j \in \mathbb{Z}_p\}.$$

Therefore, a linear dependence in O is of the form

$$0 = \sum_{j \in \mathbb{Z}_p} \mu_j \phi(e_j) = \phi(y)$$

where $y = \sum_{j \in \mathbb{Z}_p} \mu_j e_j$. To show that O is a circuit, it suffices to show that the kernel of ϕ is generated by $\sum_{i \in \mathbb{Z}_p} e_i$. Here, we follow the approach of [met19]. To this end, let $f(t) = \sum_{i \in \mathbb{Z}_p} x_i t^i$. Since $f(1) = \sum_{i \in \mathbb{Z}_p} x_i = 0$, we know that $t-1$ divides $f(t)$, and because $(t^p - 1)/(t-1)$ is irreducible, we must have $\gcd(f(t), t^p - 1) = t - 1$. By properties of the gcd, there exist polynomials $h(t), u(t), v(t) \in \mathbb{F}_2[t]$ such that

$$\begin{aligned} f(t) &= h(t)(t-1); \\ t - 1 &= u(t)f(t) + v(t)(t^p - 1). \end{aligned}$$

Note that $\phi_1^p = \phi_0$, which is the identity on $\mathbb{F}_2^p$, so we have

$$\begin{aligned} f(\phi_1) &= h(\phi_1)(\phi_1 - \phi_0); \\ \phi_1 - \phi_0 &= u(\phi_1)f(\phi_1). \end{aligned}$$

Thus $\phi = f(\phi_1)$ and $\phi_1 - \phi_0$ have the same kernel, which is easily seen to be spanned by $\sum_{i \in \mathbb{Z}_p} e_i$. This proves that O is a circuit, so we've successfully decomposed N into circuits of size p. □

We note that the technical conditions of Theorem 1.2 are necessary for our proof. For example, our method fails for $p = 7$, where the orbit of $e_0 + e_1 + e_2 + e_4$ decomposes into two circuits. Perhaps a different construction could give the same bound, up to rounding, for arbitrary complete binary matroids.

4 Odd-covers of binary matroids

In this section, we consider circuit odd-covers and prove Theorem 1.5. Again, as for circuit decompositions, our strategy will be to greedily find a large circuit C, but instead of removing C from M, we instead replace M by $M \oplus C$. This means that C can also use elements outside of M and it is only important that $M \oplus C$ is much smaller than M so that the greedy algorithm finishes quickly. To find a suitable circuit C, we simply pick a maximal independent set of M and complete it to a circuit. This leads to the following bound.

Lemma 4.1. *For every Eulerian binary matroid $M \subseteq \mathbb{F}_2^n \setminus \{0\}$ it holds that*

$$c_2(M) \leq (1 + o(1)) \frac{|M|}{\log_2 |M|}.$$

Proof. We start with $N = M$ and repeatedly replace N with $N \oplus C$ for some circuit $C \subseteq \mathbb{F}_2^n \setminus \{0\}$. This retains that N is Eulerian. We obtain C by taking a maximal linearly independent subset I of N and completing it to a circuit $C := I \cup \{x\}$ where $x = \sum_{y \in I} y$. Since $\operatorname{rank}(N) \geq \log_2 |N|$, we reduce the size of N by at least $\log_2 |N| - 1$ at every step. As long as $|N| \geq |M| / \log^2 |M|$, we have

$$\log_2 |N| - 1 \geq \log_2 |M| - 2 \log_2 \log |M| - 1.$$

Once $|N| < |M| / \log^2 |M|$, we can decompose N into at most $|N|/3$ circuits of size at least 3. In total, the number of circuits used is at most

$$\frac{|M|}{\log_2 |M| - 2 \log_2 \log |M| - 1} + \frac{|M|}{3 \log^2 |M|} = (1 + o(1)) \frac{|M|}{\log_2 |M|}. \qquad \square$$

We now establish the exact asymptotics of $c_2(M)$ in the regime where $a(M) \to \infty$.

Proof of Theorem 1.5. We have $c_2(M) \geq (1 + o(1)) a(M)$ already from (1). To prove the upper bounds, let $M = I_1 \cup \cdots \cup I_t$ be a decomposition of M into $t = a(M)$ linearly independent sets. For each I_i, the set $C_i := I_i \cup \{x_i\}$ where $x_i = \sum_{y \in I_i} y$ is a circuit. Now, the matroid $N := M \oplus C_1 \oplus \cdots \oplus C_t \subseteq \{x_1, \ldots, x_t\}$ is Eulerian of size at most t, so N can be decomposed into at most $t/3$ circuits, implying that $c_2(M) \leq (4/3)t$. But actually, by Lemma 4.1, N is the symmetric difference of at most $(1 + o(1))(t / \log_2 t)$ circuits, giving

$$c_2(M) \leq t + (1 + o(1)) \frac{t}{\log_2 t} = (1 + o(1)) a(M). \qquad \square$$

5 Open problems

We showed that for certain values of n, the complete n-dimensional binary matroid M can be decomposed into exactly $(2^{\text{rank}(M)} - 1)/((\text{rank}(M) + 1))$ many circuits. We conjecture that this is an upper bound for the minimum size of a circuit decomposition of any Eulerian binary matroid.

Conjecture 5.1. *For every Eulerian binary matroid $M \subseteq \mathbb{F}_2^n \setminus \{0\}$ it holds that*

$$c(M) \leq \left\lceil \frac{2^{\text{rank}(M)} - 1}{\text{rank}(M) + 1} \right\rceil.$$

In particular, we believe that the conclusion of Theorem 1.2 should hold, up to rounding, for any complete binary matroid, without the technical assumptions on p.

For odd-covers of binary matroids, we determined that $c_2(M) = (1 + o(1))a(M)$ as $a(M) \to \infty$. There are numerous matroids with $c_2(M) \geq a(M)$. For example, if M consists of two independent copies of $\mathbb{F}_2^s \setminus \{0\}$, it is easy to see that any circuit covers at most $\text{rank}(M)$ many elements of M and so $c_2(M) \geq a(M)$. The difference between this and the lower bound from Proposition 1.4 grows arbitrarily large as $s \to \infty$. However, we believe that there are no matroids which are worse than this, meaning that there should always be an odd-cover of size at most $a(M)$.

Conjecture 5.2. *For every Eulerian binary matroid $M \subseteq \mathbb{F}_2^n \setminus \{0\}$ it holds that*

$$c_2(M) \leq a(M).$$

Acknowledgements. We would like to thank Sang-il Oum, Alex Scott, David Wood, and Liana Yepremyan for organising the April 2023 MATRIX-IBS Structural Graph Theory Downunder III workshop where part of this research was performed.

References

[BBC+23] Steffen Borgwardt, Calum Buchanan, Eric Culver, Bryce Frederickson, Puck Rombach, and Youngho Yoo (Jun. 2023). Path odd-covers of graphs. arXiv:2306.06487. ↑2

[BCC+22] Calum Buchanan, Alexander Clifton, Eric Culver, Jiaxi Nie, Jason O'Neill, Puck Rombach, and Mei Yin (Feb. 2022). Odd covers of graphs. arXiv:2202.09822. ↑2

[BF88] László Babai and Péter Frankl (1988). Linear algebra methods in combinatorics (University of Chicago). ↑2

[BM22] Matija Bucić and Richard Montgomery (Nov. 2022). Towards the Erdős-Gallai Cycle Decomposition Conjecture. arXiv:2211.07689. ↑1

[BPR22] Calum Buchanan, Christopher Purcell, and Puck Rombach (2022). Subgraph complementation and minimum rank. *Electronic Journal of Combinatorics* **29**(1), Paper No. 1.38, 20. ↑2

[CFS14] David Conlon, Jacob Fox, and Benny Sudakov (2014). Cycle packing. *Random Structures & Algorithms* **45**(4), 608–626. ↑1

[Edm65] JACK EDMONDS (1965). Minimum partition of a matroid into independent subsets. *Journal of Research of the National Bureau of Standards. Section B* **69B**, 67–72. ↑3

[Erd83] P. ERDŐS (1983). On some of my conjectures in number theory and combinatorics. *Proceedings of the fourteenth Southeastern conference on combinatorics, graph theory and computing*, vol. 39, 3–19. ↑1

[Fan03] GENGHUA FAN (2003). Covers of Eulerian graphs. *Journal of Combinatorial Theory, Series B* **89**(2), 173–187. ↑1

[met19] METAMORPHY (Oct. 2019). Rank of circulant matrix with k ones per row. Mathematics Stack Exchange. ↑7

[Oxl92] JAMES G. OXLEY (1992). Matroid theory. Oxford Science Publications (The Clarendon Press, Oxford University Press, New York). ↑2

[Pyb85] L. PYBER (1985). An Erdős-Gallai conjecture. *Combinatorica* **5**(1), 67–79. ↑1