RANDOM GF(q)-REPRESENTABLE MATROIDS ARE NOT (b, c)-DECOMPOSABLE

JORN VAN DER POL

Abstract. We show that a random subset of the rank-n projective geometry PG(n − 1, q) is, with high probability, not (b, c)-decomposable: if k is its colouring number, it does not admit a partition of its ground set into classes of size at most ck, every transversal of which is b-colourable. This generalises recent results by Abdolazimi, Karlin, Klein, and Oveis Gharan [AKKOG21] and by Leichter, Moseley, and Pruhs [LMP22], who showed that PG(n − 1, 2) is not (1, c)-decomposable, resp. not (b, c)-decomposable.

1. Introduction

A matroid $M = (E, I)$, with ground set $E$ and independent sets $I$ is $k$-colourable (also $k$-coverable) if its ground set can be partitioned into $k$ independent sets. The smallest such $k$ is called the colouring number of $M$, for which we write $\text{col}(M)$. The colouring number of a matroid was studied by Edmonds [Edm65], who provided the following characterisation.

Theorem 1 (Edmonds’ Characterisation). $\text{col}(M) = \max_{X \subseteq E, r(X) > 0} \left\lceil \frac{|X|}{r(X)} \right\rceil$.

A $k$-colourable matroid $M$ is $(1, c)$-decomposable if its ground set can be partitioned into an arbitrary number of classes, each of which has cardinality at most $ck$, such that every transversal of the classes is independent. Equivalently, for such a matroid there exists a partition matroid $N$ on the same ground set, all of whose capacities are 1, such that every independent set in $N$ is independent in $M$ (in other words, the identity function is a weak map from $M$ to $N$). The notion of $(1, c)$-decomposition was introduced by Bérczi, Schwarz, and Yamaguchi [BSY21], who called it a $ck$-colourable partition reduction of $M$; the definition was subsequently extended to $(b, c)$-decomposability by Im, Moseley, and Pruhs [IMP21].

Definition. A $k$-colourable matroid is $(b, c)$-decomposable if there is a partition $E = E_1 \cup E_2 \cup \ldots \cup E_\ell$, called a $(b, c)$-decomposition, such that

(i) $|E_i| \leq ck$ for all $i \in [\ell]$, and

(ii) every transversal $Y = \{y_1, y_2, \ldots, y_\ell\}$ with $y_i \in E_i$ for all $i \in [\ell]$ is $b$-colourable.

Bérczi, Schwarz, and Yamaguchi [BSY21 Conjecture 1.10] conjectured that every matroid is $(1, 2)$-decomposable. This was disproved by Abdolazimi, Karlin, Klein, and Oveis Gharan [AKKOG21], who showed that, for sufficiently large $n$, the rank-$n$ binary projective geometry PG(n − 1, 2) is not $(1, c)$-decomposable. Recently, Leichter, Moseley, and Pruhs [LMP22] showed that the same matroid is not even $(b, c)$-decomposable, again provided that $n$ is sufficiently large.

Theorem 2 ([LMP22]). For sufficiently large $n$, the rank-$n$ binary projective geometry PG(n − 1, 2) admits no $(b, c)$-decomposition.
With minor modifications, their proof can be generalised to projective geometries over arbitrary finite fields.

**Theorem 3.** Let \( q \geq 2 \) be a prime power. For sufficiently large \( n \), the rank-\( n \) \( q \)-ary projective geometry \( PG(n-1, q) \) admits no \((b, c)\)-decomposition.

The crux in the argument of [LMP22] is an analysis of flats of large (depending on \( b \)) rank in \( PG(n-1, q) \). On the one hand, the number of such flats grows rapidly as \( n \) grows. On the other hand, if \( PG(n-1, q) \) is \((b, c)\)-decomposable, such flats have large colouring number, and therefore their number can be bounded from above. For large \( n \), this leads to a contradiction.

Let \( PG_p(n-1, q) \) be the random binary matroid obtained by restricting the full projective geometry \( PG(n-1, q) \) to a random subset \( E \) whose elements are chosen independently with probability \( p \). The main contribution of the current note is that the contradiction leading to the result of [LMP22] still holds with high probability in the random submatroid \( PG_p(n-1, q) \), and thus that a random GF\((q)\)-representable matroid is not \((b, c)\)-decomposable.

**Theorem 4.** Let \( q \geq 2 \) be a prime power and let \( p \in (0, 1/2] \). Let \( b, c \geq 1 \). With high probability \( \mathbb{P} \), \( PG_p(n-1, q) \) is not \((b, c)\)-decomposable.

Note that Theorems 2 and 3 can be recovered from Theorem 4 by choosing \( p = 1 \).

Finally, we compare the situation for random GF\((q)\)-representable matroids with the situation for random \( n \)-element matroids. While Theorem 4 with \( p = 1/2 \) implies that the random GF\((q)\)-representable matroid is, with high probability, not \((b, c)\)-decomposable, it is likely that a random matroid on \( n \) elements is decomposable: It is believed that almost every matroid is paving [CR70, MNWW11, PvdP15], and Bérczi, Schwarz, and Yamaguchi [BSY21] showed that paving matroids of rank at least 2 are \((1, 2)\)-decomposable. The following probabilistic version of the original conjecture by Bérczi, Schwarz, and Yamaguchi still seems likely.

**Conjecture 5.** With high probability, the random matroid on ground set \([n]\) is \((1, 3/2)\)-decomposable.

This conjecture is weaker than the original conjecture because it allows for a small number of matroids that are not \((b, c)\)-decomposable. At the same time, the conclusion for the remaining matroids is stronger, as \( 3/2 < 2 \). The improved constant can be explained as follows. The random matroid on a ground set with \( n \) elements has, with high probability, rank asymptotic to \( n/2 \) [OSW13, Corollary 2.3]; a paving matroid of rank \( r \sim n/2 \) is \( k \)-colourable [BSY21, Lemma 3.5] and has a \( \lceil \frac{r}{k} \rceil \)-colourable partition reduction [BSY21, Theorem 1.6] for some \( k \in \{2, 3\} \).

Finally, for \( k \in \{2, 3\} \) and \( r \) sufficiently large we have \( \lceil \frac{r}{k} \rceil = k + 1 \leq \frac{3}{2}k \).

The remainder of this note is structured as follows. In Section 2 we introduce some of the tools we require. Then, in Section 3 we prove Theorem 4.

---

1A sequence of events \( \mathcal{E}_n \), indexed by \( n \), occurs with high probability when \( \lim_{n \to \infty} P(\mathcal{E}_n) = 1 \), or equivalently, \( \lim_{n \to \infty} P(\mathcal{E}_n^c) = 0 \).
2. Preliminaries

We require two probabilistic bounds. The first estimates tail probabilities for nonnegative random variables, and the second is a concentration bound for sums of independent random variables.

**Lemma 6** (Markov inequality). Let $X$ be a nonnegative random variable and let $\mu = \mathbb{E}[X]$. Then for all $x > 0$

$$P(X \geq x) \leq \frac{\mu}{x}.$$  

**Lemma 7** (Chernoff bound). Let $X_1, X_2, \ldots, X_N$ be independent random variables taking values in $\{0, 1\}$. Let $X = \sum_{i=1}^{N} X_i$ and let $\mu = \mathbb{E}[X]$. For all $0 \leq \delta \leq 1$,

$$P(X \geq (1 + \delta)\mu) \leq \exp\left(-\frac{1}{3}\delta^2 \mu\right)$$

and

$$P(X \leq (1 - \delta)\mu) \leq \exp\left(-\frac{1}{2}\delta^2 \mu\right).$$

We write $\binom{n}{d}_q$ for $q$-binomial coefficients; that is, for $0 \leq d \leq n$ and $q > 1$

$$\binom{n}{d}_q = \frac{1}{q - 1} \prod_{j=0}^{d-1} q^n - q^j - 1.$$  

When $q \geq 2$ is a prime power, $\binom{n}{d}_q$ counts the number of rank-$d$ flats in $PG(n-1, q)$. The following standard bounds are useful for estimating $q$-binomial coefficients.

**Lemma 8.** $q^{d(n-d)} \leq \binom{n}{d}_q \leq q^{d(n-d)+1}$ for all $0 \leq d \leq n$ and $q > 1$.

Throughout, we use $o(1)$ to denote a quantity that tends to 0 as the parameter $n$ tends to infinity. We write $a = (1 \pm b)c$ as shorthand for $(1 - b)c \leq a \leq (1 + b)c$.

3. Proof of Theorem 4

3.1. Random subsets of projective geometries. We obtain a random submatroid of the projective geometry $PG(n-1, q)$ by retaining each of its elements independently with probability $p$. Writing $E_p$ for the resulting random set of points, we set $PG_p(n-1, q) = PG(n-1, q)|E_p$. This model of random $GF(q)$-representable matroids was first studied by Kelly and Oxley [KO82], who obtained results about rank, connectivity, and critical exponent in this model.

3.2. Size, rank, and colouring number of $PG_p(n-1, q)$. In the following three lemmas, we analyse the size, rank, and colouring number of the random matroid $PG_p(n-1, q)$.

**Lemma 9.** Let $q \geq 2$ be a prime power and let $p \in (0, 1]$. Let $\delta > 0$. With high probability, $|PG_p(n-1, q)| = (1 \pm \delta)p\frac{q^n}{q-1}$.

**Proof.** This follows immediately from the Chernoff bound, upon observing that $|PG_p(n-1, q)|$ is the sum of $\frac{q^n}{q-1} \sim \frac{q^n}{q-1}$ independent indicator random variables, each with expected value $p$. \[\square\]

The critical exponent is also known as the critical number.
The next lemma was proved in [KOS2] Theorem 4, where it was shown that with high probability \( \text{PG}_p(n-1, q) \) contains an \((n+1)\)-circuit of \( \text{PG}(n-1, q) \). Here, we provide an alternative proof.

**Lemma 10.** Let \( q \geq 2 \) be a prime power and let \( p \in (0, 1) \). With high probability, \( \text{PG}_p(n-1, q) \) is of full rank, that is \( r(\text{PG}_p(n-1, q)) = n \).

**Proof.** If \( \text{PG}_p(n-1, q) \) is not of full rank, then \( E_p \) is contained in a hyperplane of \( \text{PG}(n-1, q) \). By the union bound, this happens with probability at most

\[
\binom{n}{n-1} (1-p)^{n-1} = \frac{q^n - 1}{q-1} \frac{(1-p)^{n-1}}{(q-1)n} = o(1). 
\]

Thus, \((1)\) holds with high probability, which concludes the proof. \(\square\)

**Lemma 11.** Let \( q \geq 2 \) be a prime power and let \( p \in (0, 1) \). Let \( \delta > 0 \). With high probability, \( \text{col}(\text{PG}_p(n-1, q)) = (1 \pm \delta) p \frac{q^n}{(q-1)n} \).

**Proof.** We first prove the lower bound. By Lemma 9 and Lemma 10, with high probability, \( \text{PG}_p(n-1, q) \) has at least \((1 - \delta)p \frac{q^n}{(q-1)n}\) points and has rank \( n \). It follows from Edmonds’ characterisation of the colouring number that

\[
\text{col}(\text{PG}_p(n-1, q)) \geq \frac{(1 - \delta)p \frac{q^n}{(q-1)n}}{n}
\]

with high probability.

To prove the corresponding upper bound, it suffices to show that, with high probability,

\[
|E_p \cap F| \leq (1 + \delta)p \frac{q^n}{(q-1)n} r(E_p \cap F). \tag{1}
\]

We may assume that \( n \geq \frac{1}{(1+\delta)p} \).

Let \( F \) be a flat of \( \text{PG}(n-1, q) \) of rank \( t > 0 \). If \( t \leq n - 2 \log_q n \), then

\[
|F| = \frac{q^t - 1}{q-1} < \frac{q^n - 2 \log_q n}{q-1} = \frac{q^n}{(q-1)n} = (1 + \delta)p \frac{q^n}{(q-1)n},
\]

so \((1)\) holds for all flats \( F \) of rank at most \( n - 2 \log_q n \).

Next, let \( t \geq n - 2 \log_q n \). If \( r(E_p \cap F) < t \), then \( F \) contains a rank-\((t-1)\) flat \( F' \) such that \( E_p \cap F' = \emptyset \). This happens with probability at most

\[
\left( \frac{t}{t-1} \right)_q (1-p)^{q^{t-1}} \leq q^t (1-p)^{q^{t-1}}
\]

By the Chernoff bound, the probability that \( |E_p \cap F| \) is larger than \((1 + \delta)p |F|\) is at most

\[
\exp \left( \frac{1}{3} \delta^2 p |F| \right) \leq \exp \left( \frac{1}{3} \delta^2 p q^{t-1} \right).
\]

It follows that for a flat \( F \) of rank \( t \), \((1)\) fails with probability at most

\[
q^t (1-p)^{q^{t-1}} + \exp \left( \frac{1}{3} \delta^2 p q^{t-1} \right).
\]

Summing over all flats of rank \( t \), it follows that \((1)\) fails with probability at most

\[
\sum_{t=n-2 \log_q n}^n \left( \binom{n}{t}_q \left( q^t (1-p)^{q^{t-1}} + \exp \left( \frac{1}{3} \delta^2 p q^{t-1} \right) \right) \right) = o(1).
\]

Thus, \((1)\) holds with high probability, which concludes the proof. \(\square\)
3.3. **Proof of the main theorem.** We now prove Theorem 4, which we restate here for convenience.

**Theorem 4.** Let $q \geq 2$ be a prime power and let $p \in (0, 1]$. Let $b, c \geq 1$. With high probability, $PG_p(n - 1, q)$ is not $(b, c)$-decomposable.

**Proof.** Let $d = \lceil \log \log n \rceil$ and let $n_0$ be so large that
\[
d \geq 3, \quad nq^{-d^2} > \frac{c^2 (1 + \delta)^2 p^2}{(q - 1)^2}, \quad \text{and} \quad \frac{1}{2} p \frac{q^d - 1}{q - 1} > b
\]
for all $n \geq n_0$. We may assume that $n \geq n_0$. Let $k = (1 + \delta) p \frac{q^n}{(q - 1)n}$. For convenience, write $M = PG_p(n - 1, q)$.

We say that a rank-$d$ flat of $M$ is dense if it contains at least $\frac{1}{2} p q^{d - 1}$ elements. Let $Z_d$ be the set of dense rank-$d$ flats of $M$.

**Claim 4.1.** $\text{col}(M|F) > b$ for all $F \in Z_d$.

**Proof of claim.** By Edmonds’ characterisation and density,
\[
\text{col}(M|F) \geq \frac{|F|}{d} \geq \frac{1}{2} p \frac{q^d - 1}{q - 1} > b.
\]

Consider the following three properties:

(i) $M$ has at least $\frac{1}{2} p q^{d - 1}$ elements.

(ii) $M$ is $k$-colourable.

(iii) $|Z_d| \geq \frac{1}{2} \binom{n}{d}$.

We will show that each of these properties holds with high probability, and that if the three properties hold then $M$ is not $(b, c)$-decomposable.

Property (i) holds with high probability by Lemma 9. Property (ii) holds with high probability by Lemma 11.

**Claim 4.2.** Property (iii) holds with high probability.

**Proof of claim.** Let $F$ be a flat of $PG(n - 1, q)$. For $F$ to survive as a dense rank-$d$ flat of $M$, $|E_p \cap F|$ must be large while $r(E_p \cap F) = d$. The probability that $|F \cap E_p| < \frac{1}{2} p q^{d - 1}$ is at most
\[
\exp \left( \frac{1}{2} p \frac{q^d - 1}{q - 1} \right) = o(1)
\]
by an application of the Chernoff bound, while the probability that $r(E_p \cap F) < d$ is at most
\[
\binom{d}{d - 1} q (1 - p)^{q^{d - 1}} \leq q^d (1 - p) q^{d - 1} = o(1).
\]
It follows that the expected number of flats of $F$ that do not survive as a dense rank-$d$ flat in $M$ is $o \left( \binom{n}{d} \right)$. By the Markov inequality, the probability that more than $\frac{1}{2} \binom{n}{d}$ rank-$d$ flats of $PG(n - 1, q)$ do not survive as dense rank-$d$ flats in $M$ is at most
\[
o \left( \binom{n}{d} \right) / \frac{1}{2} \binom{n}{d} q = o(1),
\]
and hence the probability that $|Z_d| < \frac{1}{2} \binom{n}{d}$ is $o(1)$. \qed
Finally, we show that if (i)–(iii) hold, then \( M \) is not \((b, c)\)-decomposable — the proof follows the argument used in [LMP22]. Suppose that (i)–(iii) hold; for the sake of contradiction, assume that \( M \) is \((b, c)\)-decomposable, and let \( \{E_1, E_2, \ldots, E_\ell\} \) be a \((b, c)\)-decomposition.

Let \( F \in \mathbb{Z}_d \). By Claim 4.1, \( M|F \) is not \( b \)-colourable. It follows that for every dense rank-\( d \) flat of \( M \) there is an index \( i \in [\ell] \) such that \( |F \cap E_i| \geq 2 \).

Every dense rank-\( d \) flat of \( M \) can therefore be specified by an element \( i \in [\ell] \), a pair of elements in \( E_i \), and \( d - 2 \) elements outside of \( E_i \) to complete a spanning subset of the flat. Thus, the number of dense rank-\( d \) flats in \( M \) is at most

\[
|Z_d| \leq \ell \binom{ck}{2} \binom{q^n}{d-2} < n \frac{(ck)^2}{2} q^{n(d-2)}
\]

\[
\leq \frac{c^2(1+\delta)^2 p^2}{2(q-1)^2 n} q^{nd-d^2} \leq \frac{1}{2} q^{nd-d^2} \leq \frac{1}{2} \binom{n}{d-2},
\]

where the penultimate inequality follows from \( n \geq n_0 \), and the final inequality follows from Lemma 8.

Equation (2) contradicts Property (iii), so \( M \) is not \((b, c)\)-decomposable. \( \square \)

References

[AKKOG21] Dorna Abdolazimi, Anna R. Karlin, Nathan Klein, and Shayan Oveis Gharan. Matroid partition property and the secretary problem, 2021. Preprint, arXiv:2111.12436v1

[BSY21] Kristóf Bérzsi, Tamás Schwarz, and Yutaro Yamaguchi. List coloring of two matroids through reduction to partition matroids. SIAM Journal on Discrete Mathematics, 35(3):2192–2209, 2021.

[CR70] Henry H. Crapo and Gian-Carlo Rota. On the foundations of combinatorial theory: Combinatorial geometries. The M.I.T. Press, 1970.

[Edm65] Jack Edmonds. Minimum partition of a matroid into independent subsets. Journal of Research of the National Bureau of Standards, 69B:67–72, 1965.

[IMP21] Sungjin Im, Benjamin Moseley, and Kirk Pruhs. The matroid intersection cover problem. Operations Research Letters, 49(1):17–22, 2021.

[KO82] Douglas G. Kelly and James G. Oxley. Asymptotic properties of random subsets of projective spaces. Mathematical Proceedings of the Cambridge Philosophical Society, 91(1):119–130, 1982.

[LMP22] Marina Leichter, Benjamin Moseley, and Kirk Pruhs. On the impossibility of decomposing binary matroids, 2022. Preprint, arXiv:2206.12896v2.

[LOSW13] Lisa Lowrance, James Oxley, Charles Semple, and Dominic Welsh. On properties of almost all matroids. Advanced in Applied Mathematics, 50:115–124, 2013.

[MNWW11] Dillon Mayhew, Mike Newman, Dominic Welsh, and Geoff Whittle. On the asymptotic proportion of connected matroids. European Journal of Combinatorics, 32(6):882–890, 2011.

[PvdP15] Rudi Pendavingh and Jorn van der Pol. On the number of matroids compared to the number of sparse-paving matroids. Electronic Journal of Combinatorics, 22(2):P2.51, 2015.