EFFECTIVE VERSIONS OF TWO THEOREMS OF RADO

JASON BELL, DARYL FUNK, BYOUNG DU KIM, AND DILLON MAYHEW

Abstract. Let M be a representable matroid on n elements. We give bounds, in terms of n, on the least positive characteristic and smallest field over which M is representable.

Our starting point is given by the following two theorems of Rado [5].

Theorem 1 (Rado, 1957)**.** *Let M be a matroid representable over a field K. Then M is representable over a simple algebraic extension of the prime field of K.*

Theorem 2 (Rado, 1957)**.** *Let K be an extension field of $\mathbb{Q}$ of degree N, and let M be a matroid representable over K. Then there is a positive integer c such that given any prime $p > c$ there is a positive integer $k = k(p) \leq N$ such that M is representable over $GF(p^k)$. For infinitely many p, $k(p) = 1$.*

Together, these two theorems say that if a matroid is linearly representable, then it is representable over a finite field. We ask, given a representable matroid on n elements, how large must such a field be? That is, given an n-element representable matroid M, what bound, depending just on n, can we place on the size of a field required to represent M?

To that end, let $\mathcal{M}_n$ be the set of all representable matroids on n elements. For a matroid M, let $c(M)$ be the least positive characteristic of a field over which M is representable. For each positive integer n, define

$$c(n) = \max\{c(M) : M \in \mathcal{M}_n\}.$$

Let $f(M)$ be the order of the smallest field over which M is representable. For each positive integer n, define

$$f(n) = \max\{f(M) : M \in \mathcal{M}_n\}.$$

By Rado's Theorems 1 and 2 above, $c(n)$ exists and $f(n)$ is finite for all n. Note that $c(n) \leq f(n)$ for all n, and that, since adding a loop to an n-element matroid yields a matroid on $n + 1$ elements representable over exactly the same fields, c and f are non-decreasing. A result of Brylawski [1] provides a lower bound for c (and thus for f; see Section 4). We ask for upper bounds on $c(n)$ and $f(n)$. For matroids on at most 8 elements, Table 1 summarises the data (the fact that $f(8) = 11$ is courtesy G. Royle [personal communication].

Funk and Mayhew were supported by a Rutherford Discovery Fellowship, administered by the Royal Society of New Zealand.

n	$c(n)$	$f(n)$
1	2	2
2	2	2
3	2	2
4	2	3
5	2	4
6	2	5
7	3	7
8	?	11

TABLE 1

We obtain the following bounds.

Theorem 3. *For all positive integers n,*

$$\log_2 \log_2 c(n) \leq n^5 \quad \textit{and} \quad \log_2 \log_2 \log_2 f(n) \leq n^3.$$

The following fact falls out of the proof of Theorem 3.

Theorem 4. *Let M be an n-element matroid representable over a field of characteristic 0, and let p be a prime satisfying*

$$\log_2 \log_2 \log_2 p > n^5.$$

Then M is representable over $\mathrm{GF}(p)$.

We consider the cases of representability over only positive characteristic (Theorem 2.1) and representability over characteristic 0 (Theorem 3.1) separately. Theorem 3 then follows immediately from these results.

By Table 1, we may assume throughout the rest of the paper that $n > 7$.

1. Bounding the degree of a field extension

Our first step is to prove an effective version of Rado's Theorem 1:

Theorem 1.1. *Let M be a matroid on n elements representable over a field K. Then M is representable over a simple algebraic extension of the prime field of K of degree at most $2^{2^{2n^2}}$.*

1.1. **A system of polynomials arising from a matroid.** Our approach is a standard one in studies of representability of matroids over fields. We assign to an n-element, rank-r matroid M an $r \times n$ matrix A whose entries are indeterminates $x_1, \ldots, x_t$, where $t = rn$. Each element of the matroid is represented by a column of the matrix. From this matrix we obtain a system of polynomial equations in $\mathbb{Z}[x_1, \ldots, x_t]$ as follows. For each r-element subset X of the ground set of M, there is a corresponding $r \times r$ submatrix of A whose columns are those representing the elements in X. Setting the determinants of $r \times r$ submatrices corresponding to dependent sets to zero, and demanding that the determinants of those $r \times r$ submatrices that correspond

to bases be nonzero, yields a system of polynomials. The latter conditions may be expressed by multiplying each polynomial f_i obtained from a basis by a new dummy variable z_i and subtracting 1 to form the polynomial equation $z_i f_i - 1 = 0$. Alternatively, these conditions may be expressed by the single polynomial obtained by taking the product of all determinants corresponding to bases, then multiplying by a single dummy variable and subtracting 1. Writing f_i for the polynomials obtained by taking the $r \times r$ determinants of A, and B for the index set of determinants given by $r \times r$ submatrices whose columns correspond to bases of M, this gives the equation $z \prod_{i \in B} f_i - 1 = 0$. This is more expensive in terms of the degree of the resulting polynomial, but cheaper in terms of the number of new variables added to the system. We therefore prefer this second formulation. In either case, the system can be interpreted in any field F by extending the canonical homomorphism $\mathbb{Z} \to F$ to a map $\mathbb{Z}[x_1, \ldots, x_t] \to F[x_1, \ldots, x_t]$ in the natural way. Those fields over which M is representable are exactly the fields over which the corresponding system of polynomials has a solution.

Given a system of polynomials $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_t]$ arising in this way from a rank-r, n-element matroid, we will require bounds on four parameters, described in the following lemma. Let $\deg f$ denote the total degree of the polynomial f; set $d = \max_i \deg f_i$. The *height* $H(f)$ of a polynomial f is the maximum absolute value of a coefficient in f; set $H = \max_i H(f_i)$.

Lemma 1.2. *Let $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_t]$ be a system of polynomials arising as described above from a rank-r, n-element matroid. Then*

- $s \leq 2^n$,
- $t \leq n^2 + 1$.
- $d \leq n2^n$, *and*
- $H \leq n^{n2^n}$.

Proof. It is straightforward to see that $s \leq \binom{n}{r} \leq 2^n$, $t \leq nr + 1 \leq n^2 + 1$, and $d = r \cdot \binom{n}{r} + 1 \leq n2^n$. A bound on H is less obvious, but no more difficult. Since the polynomials in our system corresponding to non-bases have height one, the maximum height of a polynomial in our system will be that of the polynomial obtained by taking the product of all $r \times r$ determinants corresponding to bases of M. Since this polynomial is obtained as the product of at most $\binom{n}{r} \leq 2^n$ polynomials given by determinants, each of which has $r! < n^n$ terms, the number of terms in the product, before summing identical monomials, is at most $(n^n)^{2^n}$. Hence the height of this polynomial is certainly at most n^{n2^n}. Thus for our system, $H \leq n^{n2^n}$. □

1.2. **Algebraic tools.** Before proceeding, we summarise the algebraic notions we require. A system of polynomials $f_1, \ldots, f_s \in F[x_1, \ldots, x_t]$ is *consistent* if it has a solution in the algebraic closure $\overline{F}$ of F; that is, there is an assignment of values $x_i = \alpha_i \in \overline{F}$, for $i \in \{1, \ldots, t\}$, so that for each $j \in \{1, \ldots, s\}$, $f_j(\alpha_1, \ldots, \alpha_t) = 0$. By Hilbert's Nullstellensatz, a system of polynomials P in the ring of polynomials $F[x_1, \ldots, x_t]$ is consistent if and

only if the ideal generated by P in $F[x_1, \ldots, x_t]$ does not contain 1 (one reference is [2, Chapter 30]).

Given a field extension $E \supseteq F$, E can be viewed as a vector space V over F. The *degree* of the extension is the dimension of this vector space, denoted $[E : F]$. Given an element $\alpha \in E$, the map $m_\alpha \colon E \to E$ defined by multiplication by α is an F-linear transformation. When $[E : F]$ is finite, the map m_α is given by a matrix, with respect to a chosen basis for V; different bases yield different but similar matrices for m_α. The *norm* of α, denoted $\mathrm{Norm}_{E/F}\,\alpha$, is the determinant of a matrix corresponding to the linear transformation m_α. The norm is a map $E \to F$ satisfying $\mathrm{Norm}_{E/F}(\alpha\beta) = \mathrm{Norm}_{E/F}\,\alpha \cdot \mathrm{Norm}_{E/F}\,\beta$.

A nonzero polynomial $f \in F[X]$ is said to *split* in F if each of its irreducible factors has degree 1. A *splitting field* for a polynomial $f \in F[X]$ of degree d, is a field extension E of F, in which f splits

$$f(x) = \prod_{i=1}^{d} (x - \alpha_i)$$

such that E is generated over F by the roots $\alpha_i \in E$ of f.

Lemma 1.3 ([2], Theorem 17.18, Lemma 17.20, Corollary 17.21)**.** *Let $f \in F[X]$ be a nonzero polynomial. There exists a field $L \supseteq F$ such that f splits over L, and L contains a unique splitting field E for f over F.*

A polynomial $f \in F[X]$ of degree d has *distinct roots* if f has d different roots in every splitting field $E \supseteq F$ for f. A nonzero polynomial $f \in F[X]$ is *separable* over F if each irreducible factor of f in $F[X]$ has distinct roots; otherwise f is *inseparable*.

For any field extension $F \subseteq E$, the *Galois group* $\mathrm{Gal}(E/F)$ of E over F is the subgroup of the group of automorphisms of E consisting of those automorphisms that fix all elements of F. Given an arbitrary subgroup H of the group of automorphisms of E, define $\mathrm{Fix}(H) = \{\alpha \in E : \sigma(\alpha) = \alpha$ for all $\sigma \in H\}$. Then $\mathrm{Fix}(H)$ is a subfield of E. A field extension $E \supseteq F$ is *Galois* if $[E : F]$ is finite and $F = \mathrm{Fix}(\mathrm{Gal}(E/F))$.

Lemma 1.4 ([2], Theorem 18.13)**.** *Let $E \supseteq F$ be a field extension of finite degree. The following are equivalent.*

1. *E is a splitting field over F for some separable polynomial over F.*
2. *E is a Galois extension of F.*

Lemma 1.5 ([2], Lemmas 18.3, 18.19, Corollary 23.10)**.** *Let $E \supseteq F$ be a Galois extension, and let G be the Galois group of E over F. Let $f \in F[X]$ be nonzero, and let $\Omega = \{\alpha \in E : f(\alpha) = 0\}$ be nonempty. Then*

1. *$|G| = [E : F]$.*
2. *The action of G on E permutes the elements of Ω.*
3. *If f is irreducible and E is a splitting field over F for some polynomial in $F[X]$, then G acts transitively on Ω.*

(4) *For $\alpha \in E$,*

$$\mathrm{Norm}_{E/F}\,\alpha = \prod_{\sigma \in G} \sigma(\alpha).$$

We also use Gauss's Lemma:

Lemma (Gauss's Lemma; [2], Lemma 16.19)**.** *Let R be a unique factorisation domain and F its field of fractions. A nonzero polynomial in $R[X]$ is irreducible in $R[X]$ if and only if it is irreducible in $F[X]$.*

Let $f_1, \ldots, f_s \in F[x_1, \ldots, x_t]$ be a system of polynomials with coefficients in the field F. For each index $i \in \{1, \ldots, t\}$, let $\mathbf{x} - i$ denote the set of indeterminates $\{x_1, \ldots, x_t\} \setminus \{x_i\}$. For each pair of indices i, j, we may regard f_j as a single-variable polynomial in x_i with coefficients in the field $F(\mathbf{x} - i)$.

By Gauss's Lemma, it is sufficient that f be irreducible in $F[x_1, \ldots, x_t]$ to guarantee that f be irreducible in $F(\mathbf{x} - i)[x_i]$ for any i.

In order to take advantage of the tools of Galois Theory, we will want to select a polynomial f_j from our system that has an irreducible factor with distinct roots, when viewed as a polynomial in $F(\mathbf{x} - i)[x_i]$ for some $i \in \{1, \ldots, t\}$. We need to deal with the possibility that every polynomial in our system, when viewed as a polynomial in the polynomial ring $F(\mathbf{x}-i)[x_i]$, for every i, is inseparable. The following lemma describes the situation in this rather special case.

Lemma 1.6 ([2], Corollary 19.6)**.** *Let F be a field. Let $f \in F[X]$ be an irreducible polynomial that does not have distinct roots. Then the characteristic of F is a prime p and $f(X) = g(X^p)$ for some irreducible polynomial $g \in F[X]$.*

1.3. **Reduced systems of polynomials.** We need one more notion before we can state the two main results of this section. Denote by $\deg(f, x)$ the degree of the polynomial f in indeterminate x. Let $S = \{f_1, \ldots, f_s\}$ be a system of polynomials in indeterminates $x_1, \ldots, x_t$ with coefficients in the field K. The *leading indeterminate* of S is the unique indeterminate x_l satisfying:

- for some polynomial $f \in S$, $\deg(f, x_l) > 0$;
- for all polynomials $f \in S$, and for all $i > l$, $\deg(f, x_i) = 0$.

Write each polynomial $f \in S$ as a sum of monomials each consisting a single power x_l^d of the leading indeterminate x_l of the system, together with a coefficient $a_d \in F[x_1, \ldots, x_{l-1}]$, where each power of x_l appears in no more than one term; that is, write $f = a_n x_l^n + a_{n-1} x_l^{n-1} + \cdots + a_1 x_l + a_0$. The *leading coefficient* of f is the coefficient $a_n \in F[x_1, \ldots, x_{l-1}]$ of its highest power x_l^n of the leading indeterminate x_l of the system, where both n and a_n are nonzero. Thus a polynomial having no term containing the leading indeterminate has no leading coefficient.

Let $P = \sqrt{\langle S \rangle}$ be the radical ideal of the ideal generated by $f_1, \ldots, f_s$ in $F[x_1, \ldots, x_t]$. The system $f_1, \ldots, f_s \in F[x_1, \ldots, x_t]$ is *reduced* over F if

- each of $f_1, \ldots, f_s$ is irreducible,
- x_t is the leading indeterminate of the system,
- no leading coefficient is in P.

The *variety* defined by the polynomials $f_1, \ldots, f_s \in F[x_1, \ldots, x_t]$ is the set of all tuples $(\gamma_1, \ldots, \gamma_t) \in \overline{F}^t$ that are solutions to the system $f_1 = 0, \ldots, f_s = 0$, and is denoted $V(f_1, \ldots, f_s)$.

Lemma 1.7. *Let $h_1, \ldots, h_r \in F[x_1, \ldots, x_u]$ be a consistent system of polynomials, with $\deg(h_i, x_j) \leq D$ for each i, j. Then there is a consistent reduced system of polynomials $f_1, \ldots, f_s \in F[x_1, \ldots, x_t]$ with $\deg(f_j, x_i) \leq D$ for each i, j, and with $V(f_1, \ldots, f_s) \subseteq V(h_1, \ldots, h_r)$.*

If $h'_1, \ldots, h'_r$ is a system of polynomials chosen so that for each $j \in \{1, \ldots, r\}$, polynomial h'_j is an irreducible factor of h_j, and the system $h'_1, \ldots, h'_r$ is consistent, then we say $h'_1, \ldots, h'_r$ is a *valid choice of factors* of $h_1, \ldots, h_r$. Clearly, every consistent system of polynomials has a valid choice of factors.

Proof of Lemma 1.7. Set $P_0 = \sqrt{\langle h_1, \ldots, h_r \rangle}$. Let $h'_1, \ldots, h'_r$ be a valid choice of factors of $h_1, \ldots, h_r$. Set $S = \{h'_1, \ldots, h'_r\}$ and $P = \sqrt{\langle S \rangle}$. Then $V(P) \subseteq V(P_0)$. Let x_l be the leading indeterminate of S. If no polynomial h'_k has a leading coefficient in P_1, we are done: S is a reduced system of polynomials in $F[x_1, \ldots, x_l]$. Otherwise, put $s = r$, and for each polynomial $h'_j \in S$, put $p_j = h'_j$. Repeat the following step as many times as necessary.

Choose a polynomial $p = a_d x_l^d + \cdots + a_1 x_l + a_0 \in S$, where each $a_i \in K[x_1, \ldots, x_{l-1}]$, and $a_d \in P$. Then $a_d^m = g_1 p_1 + \cdots + g_s p_s$ for some positive integer m and some polynomials $g_1, \ldots, g_s \in F[x_1, \ldots, x_l]$, and a_d^m evaluates to 0 at every point in $V(P)$. Hence a_d vanishes at every point in $V(P)$. Let $f = a_{d-1} x_t^{d-1} + \cdots + a_0$. Then f also vanishes at every point in $V(P)$, so $V(\sqrt{\langle S \setminus \{p\} \cup \{f, a_d\} \rangle}) = V(P)$. Hence by Hilbert's strong Nullstellensatz, $\sqrt{\langle S \setminus \{p\} \cup \{f, a_d\} \rangle} = P$. Let S_1 be a system of polynomials $p'_1, \ldots, p'_{s'}$ obtained by a valid choice of factors of $S \setminus \{p\} \cup \{f, a_d\}$. Let $P_1 = \sqrt{\langle S_1 \rangle}$. Then $V(P_1) \subseteq V(P)$. Let $x_{l'}$ be the leading indeterminate of the new system S_1. If no polynomial in S_1 has a leading coefficient in P_1, we are done: we have a reduced system in $F[x_1, \ldots, x_{l'}]$. Otherwise, update by setting $l = l'$, $s = s'$, $S = S_1$ as a system of polynomials in $F[x_1, \ldots, x_l]$, and $P = P_1$; and repeat.

In each step, we replace a polynomial p with two polynomials each of strictly smaller degree: $\deg(f, x_l) < \deg(p, x_l)$ and $\deg(a_d, x_l) = 0$. Since r and u are finite, this process must eventually terminate. Since each step ends with a system S_1 consisting of irreducible polynomials, and the only reason we are unable to continue is that none of these polynomials have a leading coefficient in P_1, when the process terminates we must have obtained a reduced system. Moreover, valid choices of factors in each step ensure that the variety remains non-empty, so the final reduced system is consistent. $\square$

1.4. **Proof of Theorem 1.1.** Theorem 1.1 follows from Lemmas 1.8 and 1.9, which in turn require the more technical Lemma 1.10.

Lemma 1.8. *Let K be a field of characteristic 0, and let $f_1, \ldots, f_s$ be polynomials in the ring $K[x_1, \ldots, x_t]$ of polynomials over K. Assume that the system is consistent, and that $\deg(f_j, x_i) \leq D$ for each i, j. Then there is a solution $(\gamma_1, \ldots, \gamma_t) \in \overline{K}^t$ to $f_1 = 0, \ldots, f_s = 0$ such that*

$$[K(\gamma_1, \ldots, \gamma_t) : K] \leq 2^{2^t - t - 1} D^{2^t - 1}.$$

Lemma 1.9. *Let K be a field of characteristic $p > 0$, and let $f_1, \ldots, f_s$ be polynomials in the ring $K[x_1, \ldots, x_t]$ of polynomials over K. Assume that the system is consistent, and that $\deg(f_j, x_i) \leq D$ for each i, j. Then there is a solution $(\gamma_1, \ldots, \gamma_t) \in \overline{K}^t$ to $f_1 = 0, \ldots, f_s = 0$ such that*

$$[K(\gamma_1, \ldots, \gamma_t) : K] \leq 2^{3 \cdot 2^{t-1} - 2t - 1} D^{3 \cdot 2^{t-1} - 2}.$$

The proofs of Lemmas 1.8 and 1.9 are by induction on t. Lemma 1.10 below provides the required tool for the inductive step.

Each polynomial f_j may be considered as a single-variable polynomial in x_t with coefficients in the field $K(x_1, \ldots, x_{t-1})$. Writing $K_0 = K(x_1, \ldots, x_{t-1})$ for this field, we have $f_j \in K_0[x_t]$. Assume f_s is irreducible and separable over K_0. Let K_1 be the splitting field in $\overline{K_0}$ for f_s over K_0. Suppose $\deg(f_s, x_t) = d$ and a_d is the leading coefficient of f_s. Let $f = (1/a_d) f_s$. Then f splits over K_1; that is,

$$f = \prod_{i=1}^{d} (x_t - \alpha_i)$$

for some elements α_i in K_1, and the α_i are the roots of both f and f_s in K_1. It will be important for us that these roots α_i are distinct. Take $\alpha = \alpha_1$. Substituting $x_t = \alpha$ in each polynomial $f_j(x_1, \ldots, x_t)$ yields a polynomial $f_j(x_1, \ldots, x_{t-1}, \alpha)$, which is an element of K_1. Applying the norm to each of these elements, we obtain an element of K_0,

$$\mathrm{Norm}_{K_1/K_0} f_j(x_1, \ldots, x_{t-1}, \alpha) = \frac{g_j(x_1, \ldots, x_{t-1})}{h_j(x_1, \ldots, x_{t-1})} \in K_0$$

for some polynomials $g_j, h_j \in K[x_1, \ldots, x_{t-1}]$. Place an order on monomials —say, reverse lexicographic— and insist that g_j and h_j share no common factor, and that g_j be monic with respect to this order. As $K_0[x_t]$ is a unique factorisation domain, this guarantees that the expression g_j/h_j is unique. Denote by $N(\alpha, f_j)$ the polynomial $g_j \in K[x_1, \ldots, x_{t-1}]$ obtained in this way. Note that $N(\alpha, f_s)$ is the zero polynomial.

Lemma 1.10. *Let $f_1, \ldots, f_s \in K[x_1, \ldots, x_t]$ be a consistent reduced system of polynomials. Let $K_0 = K(x_1, \ldots, x_{t-1})$, and assume f_s, considered as a polynomial in x_t with coefficients in K_0, is separable over K_0. Let K_1 be the splitting field in $\overline{K_0}$ for f_s over K_0, and let $\alpha \in K_1$ be a root of f_s.*

Then the system of polynomials $N(\alpha, f_1), \ldots, N(\alpha, f_{s-1}) \in K[x_1, \ldots, x_{t-1}]$ *is consistent.*

Proof. Let $P = \sqrt{\langle f_1, \ldots, f_s \rangle}$ be the radical ideal of the ideal generated by $f_1, \ldots, f_s$ in $K[x_1, \ldots, x_t]$. Let $f_s = a_d x_t^d + \cdots + a_1 x_t + a_0$, where each $a_i \in K[x_1, \ldots, x_{t-1}]$. Since the system is reduced, f_s is irreducible and $a_d \notin P$. Let $f_s' = (1/a_d) f_s$. Polynomials f_s and f_s' have the same roots $\alpha_1, \ldots, \alpha_k \in K_1$. Put $\alpha = \alpha_1$.

Let $P_\alpha = \{g(x_1, \ldots, x_{t-1}, \alpha) : g \in P\}$. Then P_α is an ideal of $K[x_1, \ldots, x_{t-1}][\alpha]$. Let $Q = P_\alpha \cap K[x_1, \ldots, x_{t-1}]$. Let $S = \{a_d^k : k \in \mathbb{Z}_{\geq 0}\}$, and let $S^{-1}P_\alpha$ be the ideal

$$\left\{ \frac{p_\alpha}{s} : p_\alpha \in P_\alpha, s \in S \right\}$$

in the ring

$$S^{-1}K[x_1, \ldots, x_{t-1}][\alpha] = \left\{ \frac{f}{s} : f \in K[x_1, \ldots, x_{t-1}][\alpha], s \in S \right\}.$$

If $E \supseteq F$ is a field extension, and $A \subseteq E$, denote by $\operatorname{Norm}_{E/F} A$ the set $\{b \in F : b = \operatorname{Norm}_{E/F} a \text{ for some } a \in A\}$.

Claim. $\operatorname{Norm}_{K_1/K_0} S^{-1}P_\alpha \subseteq S^{-1}P_\alpha \cap S^{-1}K[x_1, \ldots, x_{t-1}]$.

Proof of claim. Write

$$\begin{aligned} f_s'(x_t) &= (x_t - \alpha_1)(x_t - \alpha_2) \cdots (x_t - \alpha_d) \\ &= x_t^d + \epsilon_{d-1}(\alpha_1, \ldots, \alpha_d) x_t^{d-1} + \epsilon_{d-2}(\alpha_1, \ldots, \alpha_d) x_t^{d-2} + \\ &\qquad \cdots + \epsilon_0(\alpha_1, \ldots, \alpha_d) \end{aligned}$$

where each ϵ_i is an elementary symmetric polynomial in $\alpha_1, \ldots, \alpha_d$. Comparing coefficients, we have $\epsilon_i(\alpha_1, \ldots, \alpha_d) = a_i/a_d$.

Let $F \in S^{-1}P_\alpha$. Then $F = g/s$ for some $g \in P_\alpha$ and $s \in S$. Since the norm respects multiplication (and $1/a_d^k \in K_0$ for all integers k), we just need consider $\operatorname{Norm}_{K_1/K_0} f$ where $f \in K[x_1, \ldots, x_{t-1}][\alpha]$ is an irreducible factor of the numerator of F. By Lemmas 1.4 and 1.5 we have

$$\operatorname{Norm}_{K_1/K_0} f = \prod_{\sigma \in \operatorname{Gal}(K_1/K_0)} \sigma(f)$$

Since each $\sigma \in \operatorname{Gal}(K_1/K_0)$ fixes K_0 and permutes $\alpha_1, \ldots, \alpha_d$, and $\operatorname{Gal}(K_1/K_0)$ acts transitively on $\alpha_1, \ldots, \alpha_d$, $\operatorname{Norm}_{K_1/K_0} f$ is given by

$$\prod_{\sigma \in \operatorname{Gal}(K_1/K_0)} f(x_1, \ldots, x_{t-1}, \sigma(\alpha))$$

and this expression is symmetric in $\alpha_1, \ldots, \alpha_d$. Hence $\operatorname{Norm}_{K_1/K_0} f$ can be written as a polynomial G in the elementary symmetric polynomials ϵ_i [8,

Theorem 1.12] and we have

$$\begin{aligned}\operatorname{Norm}_{K_1/K_0} f &= G\left(\epsilon_{d-1}(\alpha_1,\ldots,\alpha_d),\ldots,\epsilon_0(\alpha_1,\ldots,\alpha_d)\right)\\ &= G\left(\frac{a_{d-1}}{a_d},\ldots,\frac{a_0}{a_d}\right)\end{aligned}$$

where G is a polynomial in $K[x_1,\ldots,x_{t-1}][X_1,\ldots,X_d]$. This shows that $\operatorname{Norm}_{K_1/K_0} F \in S^{-1}K[x_1,\ldots,x_{t-1}]$. Since one of the automorphisms $\sigma \in G$ is the identity, it follows that $\operatorname{Norm}_{K_1/K_0} F \in S^{-1}P_\alpha$. △

Claim. $S^{-1}P_\alpha \cap S^{-1}K[x_1,\ldots,x_{t-1}] \subseteq S^{-1}Q$

Proof of claim. Let $f \in S^{-1}P_\alpha \cap S^{-1}K[x_1,\ldots,x_{t-1}]$. Then

$$f = \frac{g(x_1,\ldots,x_{t-1})}{a_d^k}$$

for some polynomial $g \in P_\alpha \cap K[x_1,\ldots,x_{t-1}]$ and some positive integer k. That is, $f \in S^{-1}(P_\alpha \cap K[x_1,\ldots,x_{t-1}]) = S^{-1}Q$. △

We now have $\operatorname{Norm}_{K_1/K_0} S^{-1}P_\alpha \subseteq S^{-1}Q$. Since for each j, $\operatorname{Norm}_{K_1/K_0} f_j \in \operatorname{Norm}_{K_1/K_0} S^{-1}P_\alpha$, this implies that $N(\alpha, f_j) \in Q$ (since by definition, $N(\alpha, f_j) \in K[x_1,\ldots,x_{t-1}]$).

Claim. Q is an ideal of $K[x_1,\ldots,x_{t-1}]$.

Proof of claim. Let $g,h \in Q = P_\alpha \cap K[x_1,\ldots,x_{t-1}]$ and let $r \in K[x_1,\ldots,x_{t-1}]$. Then $g,h \in P_\alpha$, so there are polynomials $g',h' \in P$ such that $g'(x_1,\ldots,x_{t-1},\alpha) = g$ and $h'(x_1,\ldots,x_{t-1},\alpha) = h$. Since P is an ideal of $K[x_1,\ldots,x_t]$, $g'+h' \in P$. Also $rg' \in P$, since $r,g' \in K[x_1,\ldots,x_t]$. Then $g'+h'$ and rg' when evaluated at $x_t = \alpha$ are in P_α; that is, $g+h$ and rg are in P_α. Since $g,h \in K[x_1,\ldots,x_{t-1}]$, also $g+h, rg \in K[x_1,\ldots,x_{t-1}]$. Hence $g+h$ and rg are both in $P_\alpha \cap K[x_1,\ldots,x_{t-1}] = Q$. △

Hence if $1 \notin Q$, then 1 is not in the ideal generated by the system of polynomials $N(\alpha,f_1),\ldots,N(\alpha,f_{s-1})$, and so by the weak Nullstellensatz, the system $N(\alpha,f_1),\ldots,N(\alpha,f_{s-1})$ is consistent. So suppose, for a contradiction, that $1 \in Q$. This occurs if and only if $1 \in P_\alpha$. Then there is a polynomial $f \in P$ with $f(x_1,\ldots,x_{t-1},\alpha) = 1$. We have

$$P_\alpha \subseteq K[x_1,\ldots,x_{t-1}][\alpha] \subseteq K(x_1,\ldots,x_{t-1})(\alpha) \cong K[x_1,\ldots,x_t]/\langle f_s'\rangle$$

and so

$$f(x_1,\ldots,x_{t-1},x_t) - 1 \in \langle f_s'\rangle.$$

Hence there is a polynomial $g \in K[x_1,\ldots,x_t]$ such that $f-1 = gf_s'$. Choose a point $\gamma \in V(P)$. Now

$$f(\gamma) - 1 = g(\gamma)f_s'(\gamma)$$

implies $-1 = 0$, a contradiction. □

Proof of Lemma 1.8. We proceed by induction on t. The result clearly holds for $t = 1$. As in the proof of Lemma 1.10, let $P = \sqrt{\langle f_1, \dots, f_s \rangle}$ be the radical ideal of the ideal generated by $f_1, \dots, f_s$ in $K[x_1, \dots, x_t]$. Applying Lemma 1.7, we may assume that f_s is irreducible, has leading indeterminate x_t, and has leading coefficient $a_d \in K[x_1, \dots, x_{t-1}] \notin P$. As in the proof of Lemma 1.10, write $f_s = a_d x_t^d + \cdots + a_0$, and let K_0, K_1, and α be as in Lemma 1.10. As in the proof of the first claim in the proof of Lemma 1.10, we have, for each $j \in \{1, \dots, s\}$,

$$\begin{aligned}
\operatorname{Norm}_{K_1/K_0} f_j &= \prod_{\sigma \in \operatorname{Gal}(K_1/K_0)} f_j(x_1, \dots, x_{t-1}, \sigma(\alpha)) \\
&= G_j\left(\epsilon_{d-1}(\alpha_1, \dots, \alpha_d), \dots, \epsilon_0(\alpha_1, \dots, \alpha_d)\right) \\
&= G_j\left(\frac{a_{d-1}}{a_d}, \dots, \frac{a_0}{a_d}\right)
\end{aligned}$$

where G_j is a polynomial in $K[x_1, \dots, x_{t-1}][X_1, \dots, X_d]$. Since the degree in $\operatorname{Norm}_{K_1/K_0} f_j$ of each root α_k is at most D, and the degree of each α_k in the symmetric polynomials is 1, the degree of each X_i in $G(X_1, \dots, X_k)$ is at most D. Since the degree of each indeterminate in each coefficient of G is at most D^2, and the degree of each x_i in each coefficient a_i of f_j is at most D, the degree of each indeterminate in the numerator of $\operatorname{Norm}_{K_1/K_0} f_j$ is at most $2D^2$. Thus the system

$$N(\alpha, f_1), \dots, N(\alpha, f_{s-1}) \in K[x_1, \dots, x_{t-1}]$$

has no indeterminate x_i of degree more than $2D^2$. By Lemma 1.10, it is consistent. By induction, this system has a solution $(\gamma_1, \dots, \gamma_{t-1}) \in \overline{K}^{t-1}$ with $[K(\gamma_1, \dots, \gamma_{t-1}) : K]$ at most

$$2^{2^{t-1}-(t-1)-1}(2D^2)^{2^{t-1}-1}.$$

Since $K[x_1, \dots, x_{t-1}] \subseteq K(x_1, \dots, x_{t-1})(\alpha) \cong K[x_1, \dots, x_t]/\langle f_s' \rangle$, for each j, viewing $N(\alpha, f_j)$ as a polynomial in $K[x_1, \dots, x_t]/\langle f_s' \rangle$ and evaluating $N(\alpha, f_j)$ at $(\gamma_1, \dots, \gamma_{t-1})$ yields a polynomial $n_j \in \langle f_s' \rangle \subseteq K[x_1, \dots, x_t]$. Thus the system

$$N(\alpha, f_1), \dots, N(\alpha, f_{s-1})$$

yields a system of polynomials of the form

$$m_1 f_s', \dots, m_{s-1} f_s' \in K[x_1, \dots, x_t]$$

where $n_j = m_j f_s'$. Evaluating f_s' at $(\gamma_1, \dots, \gamma_{t-1})$ yields the single-variable polynomial $f_s'^{\gamma}(x_t) \in K(\gamma_1, \dots, \gamma_{t-1})[x_t]$. Since $f_s'^{\gamma}$ has degree at most D in x_t, it has a root $\gamma_t \in \overline{K}$ with $[K(\gamma_1, \dots, \gamma_t) : K(\gamma_1, \dots, \gamma_{t-1})] \leq D$. Hence

$$\begin{aligned}
[K(\gamma_1, \dots, \gamma_t) : K] &= [K(\gamma_1, \dots, \gamma_t) : K(\gamma_1, \dots, \gamma_{t-1})][K(\gamma_1, \dots, \gamma_{t-1} : K] \\
&= D \cdot 2^{2^{t-1}-(t-1)-1}(2D^2)^{2^{t-1}-1} \\
&= 2^{2^t-t-1} D^{2^t-1}.
\end{aligned}$$

□

We now apply the same induction argument in the case that the field K has positive characteristic p. We just require an additional step in order to deal with the possibility that the polynomials in our system are all inseparable over $K(\mathbf{x}-i)[x_i]$, for every i. By Lemma 1.6, if this is the case, then the exponent on every indeterminate in every term of every polynomial in the system is a multiple of p.

Proof of Lemma 1.9. We proceed by induction on t. The result clearly holds for $t = 1$. Applying Lemma 1.7, we may assume that the system is reduced.

Let q be the largest multiple of p that is a common factor of all exponents of x_t among all terms of $f_1, \ldots, f_s$, so that for each j, $f_j = g_j(x_t^q)$, where $g_j \in K[x_1, \ldots, x_{t-1}][x_t]$ is irreducible. Let $z = x_t^q$, and consider the system of polynomials $g_1, \ldots, g_s \in K[x_1, \ldots, x_{t-1}, z]$ obtained by replacing each polynomial f_j with $g(z)$. We may assume (renaming polynomials if necessary) that g_s has at least one term in which the exponent on z not a multiple of p. We now have a system $g_1, \ldots, g_s \in K[x_1, \ldots, x_{t-1}, z]$, in which (by Lemma 1.6) g_s is separable over $K(x_1, \ldots, x_{t-1})$.

Write $g_s = a_d z^d + \cdots + a_0$. Since each g_j is obtained from f_j by just replacing x_t^q with z, and $a_d \notin \sqrt{\langle f_1, \ldots, f_s\rangle}$, we have that $a_d \notin \sqrt{\langle g_1, \ldots, g_s\rangle}$. Let $P = \sqrt{\langle g_1, \ldots, g_s\rangle}$, let $K_0 = K(x_1, \ldots, x_{t-1})$, let K_1 be the splitting field in $\overline{K_0}$ for g_s over K_0, and let $\alpha \in K_1$ be a root of g_s, as in Lemma 1.10. Again as in the proof of the first claim in the proof of Lemma 1.10, we have

$$\begin{aligned}\operatorname{Norm}_{K_1/K_0} g_j &= \prod_{\sigma \in \operatorname{Gal}(K_1/K_0)} g_j(x_1, \ldots, x_{t-1}, \sigma(\alpha)) \\ &= G_j\left(\epsilon_{d-1}(\alpha_1, \ldots, \alpha_d), \ldots, \epsilon_0(\alpha_1, \ldots, \alpha_d)\right) \\ &= G_j\left(\frac{a_{d-1}}{a_d}, \ldots, \frac{a_0}{a_d}\right)\end{aligned}$$

for some polynomial $G_j \in K[x_1, \ldots, x_{t-1}][X_1, \ldots, X_d]$. Just as in the proof of Lemma 1.8, the system

$$N(\alpha, g_1), \ldots, N(\alpha, g_{s-1}) \in K[x_1, \ldots, x_{t-1}]$$

is consistent by Lemma 1.10, and has no indeterminate x_i of degree more than $2D^2$. By induction, this system has a solution $(\gamma_1, \ldots, \gamma_{t-1})$ with $[K(\gamma_1, \ldots, \gamma_{t-1}) : K]$ at most

$$[K(\gamma_1, \ldots, \gamma_{t-1}) : K] \leq 2^{3 \cdot 2^{t-2} - 2(t-1) - 1} (2D^2)^{3 \cdot 2^{t-2} - 2}.$$

Hence the system $g_1, \ldots, g_s \in K[x_1, \ldots, x_{t-1}, z]$ has a solution $(\gamma_1, \ldots, \gamma_{t-1}, \gamma_z)$ with

$$[K(\gamma_1, \ldots, \gamma_{t-1}, \gamma_z) : K] \leq [K(\gamma_1, \ldots, \gamma_{t-1}) : K] \cdot D.$$

Now $(\gamma_1, \ldots, \gamma_{t-1}, \sqrt[q]{\gamma_z})$ is a solution to our original system. The minimal polynomial of $\sqrt[q]{\gamma_z}$ over $K(\gamma_1, \ldots, \gamma_{t-1}, \gamma_z)$ divides $X^q - \gamma_z$, and $q \leq D$, so

we have

$$\begin{aligned}
&[K(\gamma_1,\dots,\gamma_{t-1},\gamma_z,\sqrt[q]{\gamma_z}):K]=\\
&[K(\gamma_1,\dots,\gamma_{t-1},\gamma_z,\sqrt[q]{\gamma_z}):K(\gamma_1,\dots,\gamma_{t-1},\gamma_z)]\cdot[K(\gamma_1,\dots,\gamma_{t-1},\gamma_z):K]\\
&\quad\le D\cdot[K(\gamma_1,\dots,\gamma_{t-1}):K]\cdot D\le 2^{3\cdot 2^{t-2}-2(t-1)-1}(2D^2)^{3\cdot 2^{t-2}-2}\cdot D^2\\
&\qquad\qquad = 2^{3\cdot 2^{t-1}-2t-1}D^{3\cdot 2^{t-1}-2}.
\end{aligned}$$

Hence, taking $\gamma_t=\sqrt[q]{\gamma_z}$, certainly also

$$[K(\gamma_1,\dots,\gamma_{t-1},\gamma_t):K]\le 2^{3\cdot 2^{t-1}-2t-1}D^{3\cdot 2^{t-1}-2}. \qquad \square$$

Proof of Theorem 1.1. Together, Lemmas 1.8 and 1.9 guarantee that given an arbitrary system of polynomials over a field K, in t variables, with each variable of degree at most D, there is always an algebraic extension of K of degree at most

$$2^{3\cdot 2^{t-1}-2t-1}D^{3\cdot 2^{t-1}-2} \tag{1}$$

in which we can find a solution to the system.

Given a rank-r matroid on n elements, an associated system of polynomials has, in each polynomial coming from a determinant, every variable of degree at most 1, and at most $\binom{n}{r}$ determinantal polynomials. Hence we have $t\le nr+1\le n^2+1$ and $\deg(f_i,x_j)\le\binom{n}{r}\le 2^n$ for each i, j. Hence the bound given in (1) yields (for $n\ge 2$)

$$\begin{aligned}
2^{3\cdot 2^{t-1}-2t-1}D^{3\cdot 2^{t-1}-2} &\le 2^{3\cdot 2^{n^2}-2(n^2+1)-1}(2^n)^{3\cdot 2^{n^2}-2}\\
&= 2^{3n2^{n^2}+3\cdot 2^{n^2}-2n^2-2n-3}\\
&< 2^{3n2^{n^2}+1}<2^{2^{2n^2}}. \qquad \square
\end{aligned}$$

2. Positive characteristic

Let $c_{>0}(n)=\max\{c(M): M \text{ is representable only over a field of positive characteristic}\}$ and let $f_{>0}(n)=\max\{f(M): M \text{ is representable only over a field of positive characteristic}\}$. We obtain the following bounds.

Theorem 2.1. *For all positive integers n,*

$$\log_2\log_2 c_{>0}(n)<n^4 \quad \textit{and} \quad \log_2\log_2\log_2 f_{>0}(n)<n^3.$$

Theorem 2.1 just combines the statements of Theorems 2.2 and 2.4 below. Let M be a representable matroid, but not over characteristic 0. Applying a result of Krick, Pardo, and Sombra [4] gives the following bound on $c(M)$.

Theorem 2.2. *Let M be an n-element matroid representable only over strictly positive characteristic. Then*

$$\log_2\log_2 c(M)<n^4.$$

We obtain this bound as follows. Let $F \subseteq \mathbb{Z}[x_1, \ldots, x_t]$ be the system of polynomials given by M as described at the beginning of Section 1. Denote by $\langle F \rangle$ the ideal in $\mathbb{Z}[x_1, \ldots, x_t]$ generated by the polynomials in F. Let K be a field, and denote by F_K the system of polynomials F viewed over the polynomial ring $K[x_1, \ldots, x_t]$, and by $\langle F_K \rangle$ the ideal generated by F_K in $K[x_1, \ldots, x_t]$. Hilbert's weak Nullstellensatz says that F_K is solvable over some extension field of K if and only if $1 \notin \langle F_K \rangle$. If $1 \in \langle F \rangle$, then also $1 \in \langle F_K \rangle$ for all fields K, so M is not representable over any field. But suppose $\langle F \rangle$ contains an integer $a > 1$. Then the system F_K is solvable in K only if the characteristic of K divides a. In other words, if M can be represented over K, then the characteristic of K divides a. Thus a provides an upper bound on $c(M)$.

One way to state Hilbert's Nullstellensatz is the following.

Theorem (Hilbert's Nullstellensatz)**.** *Let $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_t]$ be polynomials such that the system $f_1 = 0, \ldots, f_s = 0$ has no solution in $\mathbb{C}^t$. Then there is a positive integer $a \in \langle f_1, \ldots, f_s \rangle$.*

The result of Krick, Pardo, and Sombra we use is the following effective version of Hilbert's Nullstellensatz. For a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_t]$, let $\deg f$ denote its total degree, and let $h(f) = \log H(f)$ denote the logarithm of the maximum absolute value of its coefficients.

Theorem 2.3 ([4])**.** *Let $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_t]$ be polynomials such that the system $f_1 = 0, \ldots, f_s = 0$ has no solution in $\mathbb{C}^t$. Set $d = \max_i \deg f_i$ and $h = \max_i h(f_i)$. Then there is a positive integer $a \in \langle f_1, \ldots, f_s \rangle$ satisfying*

$$\log a \leq 4t(t+1)d^t \left(h + \log s + (t+7)\log(t+1)\, d\right).$$

Proof of Theorem 2.2. By Lemma 1.2, for our system $F \subseteq \mathbb{Z}[x_1, \ldots, x_t]$ we have $s \leq 2^n$, $d \leq n2^n$, $t \leq n^2 + 1$, and $H \leq n^{n2^n}$. Hence

$$h \leq \log n^{n2^n} < n2^n \log_2 n \leq n2^n \log_2 2^n = n^2 2^n \leq 2^n 2^n = 2^{2n}.$$

Substituting these values into the result of Theorem 2.3 we obtain a positive integer $a \in \langle f_1, \ldots, f_s \rangle$ satisfying

$$\begin{aligned}
\log a &\leq 4(n^2+1)(n^2+2)(n2^n)^{n^2+1}\left(2^{2n} + \log 2^n + (n^2+8)\log(n^2+2)\, n2^n\right) \\
&\leq (4n^4 + 12n^2 + 8)(n^{n^2+1}2^{n^3+n})(2^n n(n^2+8)\log(n^2+2) + n\log 2 + 2^{2n}) \\
&\leq (4n^4 + 12n^2 + 8)(n^{n^2+1}2^{n^3+n})\left(2^n\left(n(n^2+8)\log(n^2+2) + n\right) + 2^{2n}\right).
\end{aligned}$$

Using the facts $n^{n^2+1} \leq 2^{n^3}$, $n(n^2+8)\log(n^2+2) + n \leq n^4$, $(4n^4 + 12n^2 + 8)(n^4+1) \leq n^9$, and $n^9 \leq 2^{4n}$, we obtain

$$\begin{aligned}
\log a &\leq (4n^4 + 12n^2 + 8)(2^{2n^3+n})(2^{2n}(n^4+1)) \\
&\leq n^9 2^{2n^3+3n} \leq 2^{4n} 2^{2n^3+3n} = 2^{2n^3+7n}.
\end{aligned}$$

Hence

$$\log_2 a < 2 \cdot \log a < 2 \cdot 2^{2n^3+7n} = 2^{2n^3+7n+1} \leq 2^{n^4}. \qquad \square$$

Theorem 2.4. *Let M be an n-element matroid representable only over strictly positive characteristic. Then*

$$\log_2 \log_2 \log_2 f(M) < n^3.$$

Proof. By Theorem 2.2, M is representable over a field of characteristic p, where p is a prime of size at most $2^{2^{n^4}}$. Hence by Theorem 1.1, M is representable over a simple algebraic extension of $\mathrm{GF}(p)$ of degree at most $N = 2^{2^{2n^2}}$. That is, M is representable over a field of size at most p^N. So

$$f(M) \leq (2^{2^{n^4}})^{2^{2^{2n^2}}} = 2^{2^{n^4}+2^{2n^2}} \leq 2^{2^{2^{n^3}}}. \qquad \square$$

3. Characteristic zero

Let $c_0(n) = \max\{c(M) : M \text{ is representable over a field of characteristic } 0\}$ and let $f_0(n) = \max\{f(M) : M \text{ is representable over a field of characteristic } 0\}$. We obtain the following bounds.

Theorem 3.1. *For all positive integers n,*

$$\log_2 \log_2 c_0(n) < n^5 \quad \textit{and} \quad \log_2 \log_2 \log_2 f_0(n) < n^3.$$

We use the following two results. The first combines and paraphrases a result of Kollár [3] and a result of Sombra [7] giving bounds on the degree of polynomials in Bézout's identity.

Theorem 3.2 ([3, 7])**.** *Let K be a field, and let $f_1, \ldots, f_s \in K[x_1, \ldots, x_t]$ be polynomials each of total degree at least 1 and at most d. Suppose $f_1, \ldots, f_s$ have no common zero in $\overline{K}^t$. Then there exist polynomials $g_1, \ldots, g_s \in K[x_1, \ldots, x_t]$ satisfying*

$$g_1 f_1 + \cdots + g_s f_s = 1$$

where each g_i has total degree at most d^t.

The second gives a lower bound on the product of the primes that are at most a given integer.

Theorem 3.3. *Let a be a positive integer. The product of the primes at most a is greater than 2^{a-3}.*

Proof. By [6, Theorem 10], $\prod_{p \leq a} p > e^{0.84a}$ for $a \geq 101$. Since $e^{0.84} > 2$, $\prod_{p \leq a} p > 2^a$ for $x \geq 101$. It is straightforward to check by direct calculation that the inequality $\prod_{p \leq a} p > 2^{a-3}$ holds for $a \leq 100$. $\square$

We also use Hadamard's inequality, a well-known bound on the determinant of a matrix:

Lemma (Hadamard's inequality)**.** *Let A be an $n \times n$ matrix with entries in $\mathbb{C}$. If every entry A_{ij} of A satisfies $|A_{ij}| \leq B$, then $|\det(A)| \leq B^n n^{n/2}$.*

The *height* $H(f)$ of a polynomial f is the maximum of the absolute values of its coefficients. Theorem 3.1 is a corollary of the following theorem.

Theorem 3.4. *Let $f_1, \dots, f_s \in \mathbb{Z}[x_1, \dots, x_t]$ be polynomials of total degree at least 1 and at most d, and of height at most H, and assume $f_1, \dots, f_s$ share a common zero in $\mathbb{C}^t$. Let $L = s\binom{d^t+t}{t}$. Then there is a prime p satisfying*

$$p < 6 + 2L \log_2 H + L \log_2 L$$

such that $\mathbb{Z}[x_1, \dots, x_t]/\langle p, f_1, \dots, f_s\rangle$ is nonzero. Moreover, for all $p > H^L \sqrt{L}^L$ the ring $\mathbb{Z}[x_1, \dots, x_t]/\langle p, f_1, \dots, f_s\rangle$ is nonzero.

Proof. Note that for a commutative ring R, the collection of polynomials of degree at most d^t in $R[x_1, \dots, x_t]$ is a free R-module on the generators

$$S := \{x_1^{i_1} \cdots x_t^{i_t} : i_1 + \cdots + i_t \le d^t\}.$$

The size of S is the number of ways to write d^t as a sequence of $t+1$ non-negative integers (there is a 1-1 correspondence between the sequences of length t whose sum is at most d^t and sequences of length $t+1$ whose sum is exactly d^t, obtained by truncating each of the latter sequences at t terms). So $|S|$ is the number of weak compositions of d^t into $t+1$ parts; that is, $|S| = \binom{d^t+t}{t}$.

Now let $S = \{m_1, m_2, \dots, m_{|S|}\}$. Let $\{z_{i,j} : 1 \le i \le |S|, 1 \le j \le s\}$ be a set of indeterminates; this collection has size L. Define

$$g_j = \sum_{i=1}^{|S|} z_{i,j} m_i \in \mathbb{Z}[x_1, \dots, x_t][z_{i,j} : 1 \le i \le |S|, 1 \le j \le s].$$

Now consider the equation

$$1 - g_1 f_1 + \cdots + g_s f_s = 0. \tag{2}$$

By Theorem 3.2 there is an assignment of values from a field K to the indeterminates $z_{i,j}$ satisfying (2) if and only if $1 \in \langle f_1, \dots, f_s\rangle_K$. Let $t\colon \mathbb{Z}[x_1, \dots, x_t][z_{i,j}] \to K[x_1, \dots, x_t]$ be an assignment of values in K to the indeterminates $z_{i,j}$. Expand (2) and set $t(z_{i,j}) = t_{i,j} \in K$. Consider the coefficient of a monomial $m \in S$ appearing in this equation. Each such coefficient yields an equation of the form

$$\delta_{m,1} - \sum_{i=1}^{|S|} \sum_{j=1}^{s} t_{i,j} c_{i,m,j} = 0$$

where $c_{i,m,j}$ is a coefficient of f_j, and hence is at most H in absolute value (and where $\delta_{m,1} = 1$ if $m = 1$ and is otherwise 0).

Now write equation (2) as a matrix equation $A\vec{z} = \vec{b}$, where A is a $|S| \times s|S|$ integer matrix (with rows indexed by the monomials in S and columns by the $s|S| = L$ variables z_{ij} that are the components of $\vec{z}$). The entries of A are at most H in absolute value and $\vec{b}$ has one entry equal to one and the rest equal to zero. Observe that, for a field K, $A\vec{z} = \vec{b}$ has a solution in $\overline{K}^t$ if and only if $1 \in \langle f_1, \dots, f_s\rangle_K$. Since 1 is not in the ideal $\langle f_1, \dots, f_n\rangle_{\mathbb{Q}}$, we see that this equation $A\vec{z} = \vec{b}$ has no solutions in $\mathbb{C}^t$. Let r denote the

rank of A. Then there is an $(r+1)\times(r+1)$ minor of the matrix $(A|\vec{b})$ that does not vanish. Since $r \leq L-1$ and the entries of $(A|\vec{b})$ are at most H, by Hadamard's inequality this minor is bounded by $(H\sqrt{L})^L$. Let D denote this minor. Then $|D| \leq H^L\sqrt{L}^L$.

On the other hand, if p is prime and $1 \in \langle f_1,\ldots,f_s\rangle_{\mathrm{GF}(p)}$ (taking reductions of the f_i modulo p) then $A\vec{z}=\vec{b}$ has a solution modulo p. Since A has rank at most $r \mod p$, then $(A|\vec{b})$ must have rank at most r mod p and so D must vanish modulo p.

In particular, this means that if $p > H^L\sqrt{L}^L$ then, as D does not vanish modulo p, $A\vec{z}=\vec{b}$ does not have a solution modulo p. Thus $1 \notin \langle f_1,\ldots,f_s\rangle_{\mathrm{GF}(p)}$. In other words, $f_1,\ldots,f_s$ share a common zero in $\overline{\mathrm{GF}(p)}^t$.

Let p' be the least prime for which $A\vec{z}=\vec{b}$ does not have a solution modulo p'; equivalently, let p' be the least prime for which $1 \notin \langle f_1,\ldots,f_s\rangle_{\mathrm{GF}(p')}$. Let q be the largest prime less than p'. Then D is a multiple of all primes $\leq q$. Hence, by Theorem 3.3 and Hadamard's Inequality,

$$2^{q-3} \leq \prod_{p\leq q} p \leq |D| \leq H^L\sqrt{L}^L$$

which implies

$$q \leq 3 + L\log_2 H + L/2\log_2 L.$$

Hence by Bertrand's postulate, $p' < 2q \leq 6 + 2L\log_2 H + L\log_2 L$. □

Now suppose our system of polynomials $f_1,\ldots,f_s \in \mathbb{Z}[x_1,\ldots,x_t]$ of Theorem 3.4 is a system arising from an n-element matroid M, of rank r, representable over a field of characteristic zero, as described in Section 1.1. By Theorem 3.4 there is a prime $p < 6 + 2\log_2 H + L\log_2 L$ such that $1 \notin \langle p, f_1,\ldots,f_s\rangle$. Since the polynomials $f_1,\ldots,f_s$, reduced modulo p share a common zero in $\overline{\mathrm{GF}(p)}^t$, M is representable over a field of characteristic p. Hence

$$c(M) \leq 6 + 2L\log_2 H + L\log_2 L.$$

To complete the proof of Theorem 3.1, we just need to write L and H in terms of n. By Lemma 1.2, for our system of polynomials $f_1,\ldots,f_s$, we have $s \leq 2^n$, $t \leq n^2+1$, $d \leq n2^n$, and $H \leq n^{n2^n}$. Hence

$$\begin{aligned} L = s\binom{d^t+t}{t} &\leq s2^{d^t+t} \leq 2^n 2^{(n2^n)^{n^2+1}+n^2+1} \\ &\leq 2^n 2^{(n^{n+1})^{n^2+1}+n^2+1} \leq 2^{n^{n^4}+n^2+n+1}. \end{aligned}$$

Observe that $H \leq n^{n2^n} \leq 2^{2^{2n}}$, which is a more convenient bound.

Proof of Theorem 3.1. Let M be an n-element matroid representable over a field of characteristic zero. By Theorem 3.4, and the above bounds for L

and H

$$\begin{aligned}
c(M) &\le 6 + 2L\log_2 H + L\log_2 L \\
&\le 6 + 2\cdot 2^{n^{n^4}+n^2+n+1}\log_2 2^{2^{2n}} + 2^{n^{n^4}+n^2+n+1}\log_2 2^{n^{n^4}+n^2+n+1} \\
&\le 6 + 2^{n^{n^4}+n^2+n+2}2^{2n} + 2^{n^{n^4}+n^2+n+1}\cdot(n^{n^4}+n^2+n+1) \\
&\le 6 + 2^{n^{n^4}+n^2+3n+2} + 2^{n^{n^4}+n^2+n+1}\cdot(n^{n^4}+n^2+n+1) \\
&\le 2\cdot 2^{n^{n^4}+n^2+3n+2}\cdot(n^{n^4}+n^2+n+1) \\
&\le 2^{n^{n^4}+n^2+3n+3}\cdot(n^{n^4}+n^2+n+1) \\
&\le 2^{n^{n^4}+n^2+3n+3}\cdot 2^{n^5} = 2^{n^{n^4}+n^5+n^2+3n+3} \le 2^{2^{n^5}}.
\end{aligned}$$

Hence by Theorem 1.1

$$f(M) \le (2^{2^{n^5}})^{2^{2^{2n^2}}} = 2^{2^{n^5}+2^{2n^2}} \le 2^{2^{2^{n^3}}}. \qquad \square$$

Proof of Theorem 4. If $p > H^L L^{L/2}$, then by Theorem 3.4 M is representable over GF(p). Substituting $2^{2^{2n}}$ for H and $2^{n^{n^4}+n^2+n+1}$ for L yields

$$\begin{aligned}
H^L L^{L/2} &\le (2^{2^{2n}})^{2^{n^{n^4}+n^2+n+1}}\cdot(2^{n^{n^4}+n^2+n+1})^{2^{-1}2^{n^{n^4}+n^2+n+1}} \\
&\le 2^{2^{n^{n^4}+n^2+3n+1}}\cdot 2^{(n^{n^4}+n^2+n+1)\cdot 2^{n^{n^4}+n^2+n}} \\
&\le 2^{2^{n^{n^4}+n^2+3n+1}}\cdot 2^{(2^{n^5})\cdot 2^{n^{n^4}+n^2+n}} \\
&\le 2^{2^{n^{n^4}+n^2+3n+1}}\cdot 2^{2^{n^{n^4}+n^5+n^2+n}} \\
&\le 2^{2\cdot 2^{n^{n^4}+n^5+n^2+n}} = 2^{2^{n^{n^4}+n^5+n^2+n+1}} \le 2^{2^{2^{n^5}}}.
\end{aligned}$$

$\square$

4. A lower bound

Using a result from [1], we obtain the following lower bound on $c(n)$.

Theorem 4.1. $\log_2 c(n) \ge (n-7)/2$

The result we use is the following.

Theorem 4.2 (Brylawski [1], Corollary 3.3)**.** *For any prime p there is a matroid M on at most $2\lfloor\log_2 p\rfloor + 6$ elements with $c(M) = p$.*

Proof of Theorem 4.1. For each positive integer $n \ge 7$, choose a prime p such that

$$2^{(n-7)/2} \le p \le 2^{(n-5)/2}.$$

By Bertrand's postulate, this is always possible. Since $\frac{n-5}{2}$ is $\frac{1}{2}$-integral, $\lfloor\log_2 p\rfloor + \frac{1}{2} \le \frac{n-5}{2}$, so

$$2\lfloor\log_2 p\rfloor + 6 \le n.$$

By Theorem 4.2, there is a matroid N on at most $2\lfloor \log_2 p \rfloor + 6$ elements with $c(N) = p$. Add to N as many loops as necessary to obtain a matroid M on exactly n elements with $c(M) = p$. □

Acknowledgement

We express our thanks to Gary Gordon for pointing out the results of Brylawski that enabled our lower bound, and to Gordon Royle for calculating $f(8)$.

References

[1] Tom Brylawski. Finite prime-field characteristic sets for planar configurations. *Linear Algebra Appl.*, 46:155–176, 1982.
[2] I. Martin Isaacs. *Algebra*. Brooks/Cole Publishing Co., Pacific Grove, CA, 1994. A graduate course.
[3] János Kollár. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1(4):963–975, 1988.
[4] Teresa Krick, Luis Miguel Pardo, and Martín Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Math. J.*, 109(3):521–598, 2001.
[5] R. Rado. Note on independence functions. *Proc. London Math. Soc. (3)*, 7:300–320, 1957.
[6] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.
[7] Martín Sombra. A sparse effective Nullstellensatz. *Adv. in Appl. Math.*, 22(2):271–295, 1999.
[8] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem*. A K Peters, Ltd., Natick, MA, third edition, 2002.

Department of Pure Mathematics, University of Waterloo, Canada
E-mail address: jpbell@uwaterloo.ca

School of Mathematics and Statistics, Victoria University of Wellington, New Zealand
E-mail address: daryl.funk@vuw.ac.nz

School of Mathematics and Statistics, Victoria University of Wellington, New Zealand
E-mail address: byoungdu.kim@vuw.ac.nz

School of Mathematics and Statistics, Victoria University of Wellington, New Zealand
E-mail address: dillon.mayhew@vuw.ac.nz