ON THE IRREDUCIBILITY AND MONODROMY OF TUTTE POLYNOMIALS

ANDREW GOODALL, FLORENT JOUVE, AND JEAN-SÉBASTIEN SERENI

Abstract. We study algebraic properties of the Tutte polynomial of a matroid and its generalizations to other combinatorially defined bivariate polynomial invariants. Merino, de Mier and Noy showed that the Tutte polynomial of a connected matroid is irreducible, and Bohn, Cameron and Müller conjectured the stronger property that the Galois/monodromy group of the Tutte polynomial of a connected matroid of rank r is isomorphic to the full symmetric group on r letters. First, we generalize the result of Merino–de Mier–Noy to the context of general ranked sets by exploiting a recent translation of the Brylawski relations, satisfied by the coefficients of the Tutte polynomial, into a functional identity. Second, we give the first confirmation of the conjecture of Bohn–Cameron–Müller for infinite families of connected matroids, including the cycle graphs and the uniform matroids. Moreover, we apply the large sieve to obtain a probabilistic statement showing that suitable linear combinations of coprime Tutte polynomials generically satisfy the conjecture.

1. Introduction

The Tutte polynomial is a bivariate polynomial invariant of finite graphs that includes many important specializations, such as the chromatic polynomial, reliability polynomial, partition function of the Potts model in statistical physics, and the Jones polynomial of an alternating knot (encoded as a plane graph). The Tutte polynomial is more generally defined as an invariant of finite matroids and in this guise has served to bridge disparate areas of combinatorics (such as hyperplane arrangements and coding theory) and appears in various disciplines (such as the random cluster model in physics and DNA sequencing in biology). Beyond matroids, the definition of the Tutte polynomial extends further to ranked sets [22] where the rank function does not need satisfy all the axioms for a matroid rank function (see Section 2 below for a precise definition).

In the present work we continue the study initiated in [19] of "generic" properties of Tutte polynomials among bivariate $\mathbf{Z}$-polynomials. While [19] focuses on linear algebraic aspects (what is the dimension of the linear span of natural finite families of Tutte polynomials?), here we seek to understand the expected algebro–geometric structure of such polynomials.

Let us recall that for $M = (E, \mathrm{r})$ a matroid on groundset E and with rank function r, its *Tutte polynomial* is defined by

$$T_M(x, y) = \sum_{A \subseteq E} (x-1)^{\mathrm{r}(E)-\mathrm{r}(A)} (y-1)^{|A|-\mathrm{r}(A)}.$$

It is an element of $\mathbf{Z}[x, y]$ with $\deg_x T_M(x, y) = \mathrm{r}(M)$ and $\deg_y T_M(x, y) = |E| - \mathrm{r}(M)$, where $\mathrm{r}(M) \coloneqq \mathrm{r}(E)$. If M is the cycle matroid of a graph $G = (V, E)$ with $c(G)$ connected

2020 *Mathematics Subject Classification.* 05C31, 11R32, 11N36, 20B10.

Key words and phrases. Tutte polynomials, matroids, Galois theory, monodromy, permutation groups.

components then $\mathrm{r}(M) = |V| - c(G)$. The chromatic polynomial of G coincides (up to sign and a factor of $x^{c(G)}$) with the specialization $T_M(1-x, 0)$.

Given a matroid $M = (E, \mathrm{r})$, its Tutte polynomial $T_M(x, y)$ naturally defines a plane algebraic curve over $\mathbf{Q}$. We will work in the slightly more general context where R is a fixed unique factorization domain (UFD) with field of fractions k and where $T_M(x, y)$ is seen as an element of $R[x, y]$ through the application of the canonical ring homomorphism $\phi\colon \mathbf{Z} \to R$ (sending 1 to 1) to its coefficients. In this framework we will denote by C_M/k the plane affine curve attached to T_M, and by $\mathbb{A}^1_k$ the affine line over k. Our main focus in the present work is on properties of the k-morphism $\pi\colon C_M \to \mathbb{A}^1_k$ of degree $\mathrm{r}(M)$ defined for any extension K/k on K-rational points (x, y) of C_M by $\pi(x, y) = y$. In the case where C_M/k is irreducible, two groups are naturally associated with the morphism π (see [24, §1]):

- the Galois group of the (normal closure of the) field extension defined using the induced inclusion $\pi^*\colon k(\mathbb{A}^1_k) = k(y) \to k(C_M)$,
- the monodromy group corresponding to the topological unbranched cover $V \to U$ obtained by restricting π to suitable Zariski open subsets U and V of $\mathbb{A}^1_k$ and C_M, respectively.

In the above setting Harris shows ([24, §1, Proposition]) that these two groups coincide, a fact that has been exploited for geometric purposes ([24, 30, 40]). In the sequel we will denote by $G_{k,y}(T_M(x, y))$ (or $G_{k,y}(T_M)$ for brevity) the Galois/monodromy group attached to T_M via the morphism π in the way described above. This group can be seen as a permutation group on $\mathrm{r}(M)$ letters and equals the Galois group of the splitting field of $T_M(x, y)$ inside a fixed separable closure of $k(y)$. The irreducibility assumption on C_M/k corresponds to the transitive action of $G_{k,y}(T_M)$ seen as a permutation group, and this group is known to be a transitive subgroup of $\mathfrak{S}_{\mathrm{r}(M)}$ when M is a connected matroid ([33]) as long as $\mathrm{char}(k)$ does not divide the constant term of the monomial of degree 1 of the x-polynomial $T_M(x, y)$. One might wonder what finer properties than transitivity might be satisfied by the permutation group $G_{k,y}(T_M)$, such as its action being primitive or doubly transitive, and whether these properties correspond to a structural property of M like transitivity does to connectivity. However, the following conjecture of Bohn–Cameron–Müller [4, Conj. 9] directs us rather to consider whether $G_{k,y}(T_M)$ when transitive in fact coincides as a permutation group with the full symmetric group $\mathfrak{S}_{\mathrm{r}(M)}$:

Conjecture 1.1 (Bohn–Cameron–Müller)**.** *Let $M = (E, \mathrm{r})$ be a connected matroid on finite groundset E with $\mathrm{r}(M) > 0$, and let K be a field of characteristic zero. Then $G_{K,y}(T_M)$ is maximal* i.e *it is isomorphic to the symmetric group on $\mathrm{r}(M)$ letters.*

The conjecture has been computationally confirmed [4] for connected graphic matroids M such that $\mathrm{r}(M) \leqslant 10$. However, prior to the present work the conjecture has not as far as we know been proved for any infinite family of connected matroids. In [4] the analogue of Conjecture 1.1 is proved for the multivariate Tutte polynomial of a matroid ([4, Th. 1] in which there are as many variables as elements in the groundset). On the other hand, specializing the Tutte polynomial at combinatorially meaningful values to obtain a univariate polynomial is not expected to lead to analogous behaviour. Indeed part of the motivation for stating and studying Conjecture 1.1 comes from structural aspects of the chromatic polynomial. Once divided by the product of linear factors corresponding to its chromatic number, does the remaining "interesting" part of the chromatic polynomial of a graph resemble a random

integer polynomial? For instance does it generically have maximal Galois group (as is the case for random integer polynomials [3])? It turns out that this does not seem to be the case (as theoretical and computational evidence obtained in [7, 34] indicate). In this sense, the bivariate Tutte polynomial of a matroid is currently believed to lie at the frontier of polynomial matroid invariants whose Galois group is almost surely maximal.

In another direction, to prove that the Galois group of the Tutte polynomial of a connected matroid is transitive we need only use the Brylawski relations satisfied by the coefficients and the fact that a matroid is connected if and only if the coefficient of x in its Tutte polynomial (Crapo's beta invariant [10]) is non-zero. The class of bivariate polynomials satisfying Brylawski's relations includes not just Tutte polynomials of matroids but also rank-nullity polynomials of ranked sets generally. Drawing on a recent alternative derivation [1] of Brylawski's relations via the simplification the Tutte polynomial undergoes on the hyperbola $(x-1)(y-1)=1$, we prove in Section 2.2 that a large class of bivariate polynomials satisfying Brylawski's relations and with non-zero coefficient of x are irreducible, among which are the known cases of the Tutte polynomial of a connected matroid [33] or connected delta matroid [15]. For some classes of ranked sets, the coefficient of x in the rank-nullity polynomial being non-zero is – in a similar way to matroids – a necessary and sufficient condition for not being a direct sum of smaller ranked sets (e.g. for delta matroids [15]), but for others the condition is only sufficient (e.g. for greedoids, see Remark 2 below). We also exhibit an infinite family of ranked sets whose Tutte polynomial is irreducible but does not have maximal Galois group.

The paper is organized as follows. In §2, we study irreducibility properties of the Tutte polynomial in the broader context of ranked sets. Inspired by the recent work of Beke et al. [1], we introduce the notion of a *Brylawski polynomial*, which includes the rank-nullity polynomials of a ranked set as a special case, and establish analogous criteria for the irreducibility of a Brylawski polynomial to that established for the Tutte polynomial of a matroid [33]. Next we prove in §3 a probabilistic statement (which is, to a large extent, of independent interest) showing that particular $\mathbf{Z}[x]$-linear combinations of pairs of coprime bivariate polynomials that are monic of the same degree seen as x-polynomials (*e.g.* the respective, and distinct, Tutte polynomials of two connected matroids of the same size and rank) generically satisfy Conjecture 1.1. We do so by first generalizing a sieve result of Gallagher towards van der Waerden's Conjecture. We conclude by showing in §4 that Conjecture 1.1 might be extended to some, but not all, more general ranked sets and that it holds for some infinite families of connected matroids (including cycle graphs and uniform matroids).

2. The Tutte polynomial of a ranked set

Definition 1. For a finite set E, a *rank function* on E is an integer-valued function $\mathrm{r}\colon 2^E \to \mathbf{Z}$ satisfying

$$\mathrm{r}(\varnothing) = 0, \quad \mathrm{r}(A) \leqslant \mathrm{r}(E), \quad \text{and} \quad \mathrm{r}(A) \leqslant |A|, \quad \text{for all } A \subseteq E.$$

The pair $S = (E, \mathrm{r})$ is called a *ranked set*, and E is its *groundset*.

While $0 = \mathrm{r}(\varnothing) \leqslant \mathrm{r}(E)$, the rank function r may take negative values on proper subsets of E, although when r is monotone, which is the case for matroids, antimatroids and greedoids, it takes nonnegative values on all subsets [21].[1]

To a ranked set $S = (E, \mathrm{r})$ we associate the bivariate polynomial

$$T_S(x, y) = \sum_{A \subseteq E} (x-1)^{\mathrm{r}(E)-\mathrm{r}(A)} (y-1)^{|A|-\mathrm{r}(A)}, \tag{1}$$

which we call the corank-nullity polynomial of S, better known as the Tutte polynomial when S is a matroid. Along the hyperbola $(x-1)(y-1) = 1$ the polynomial T_S simplifies considerably to a polynomial dependent only on the size and rank of the groundset E.

Proposition 2.1. *For a ranked set $S = (E, \mathrm{r})$,*

$$(y-1)^{\mathrm{r}(E)} T_S\Big(\frac{y}{y-1}, y\Big) = y^{|E|}. \tag{2}$$

In other words,

$$T_S(x, y) \equiv x^{\mathrm{r}(E)} y^{|E|-\mathrm{r}(E)} \pmod{xy - x - y}.$$

Proof. By the definition of T_S, the left-hand side of (2) equals

$$\sum_{A \subseteq E} \Big(\frac{y-(y-1)}{y-1}\Big)^{\mathrm{r}(E)-\mathrm{r}(A)} (y-1)^{\mathrm{r}(E)+|A|-\mathrm{r}(A)} = \sum_{A \subseteq E} (y-1)^{|A|} = y^{|E|}.$$

□

Suppose $S_1 = (E_1, \mathrm{r}_1)$ and $S_2 = (E_2, \mathrm{r}_2)$ in which r_1 and r_2 are rank functions on disjoint sets E_1 and E_2, respectively. Then the *direct sum* $S_1 \oplus S_2 = (E_1 \cup E_2, \mathrm{r})$ has rank function on $E = E_1 \cup E_2$ defined by $\mathrm{r}(A_1 \cup A_2) = \mathrm{r}_1(A_1) + \mathrm{r}_2(A_2)$, where $A_1 \subseteq E_1$ and $A_2 \subseteq E_2$. Then $T_{S_1 \oplus S_2}(x, y) = T_{S_1}(x, y) T_{S_2}(x, y)$. In other words, if S can be expressed as the direct sum of ranked sets on non-empty groundsets, then $T_S(x, y)$ is a reducible polynomial. When S is a matroid, Merino et al. [33] showed that if $T_S(x, y)$ is reducible, then there are non-empty matroids S_1 and S_2 such that $S = S_1 \oplus S_2$, i.e. S is not connected. They use the fact that

[1] A rank function r on E defines a *matroid* if additionally it satisfies the following properties:

(i) Submodularity:
$$\mathrm{r}(A \cup B) + \mathrm{r}(A \cap B) \leqslant \mathrm{r}(A) + \mathrm{r}(B),$$
for $A, B \subseteq E$;

(ii) Adding an element cannot decrease the rank (monotonicity), and any increase is by at most 1:
$$\mathrm{r}(A) \leqslant \mathrm{r}(A \cup \{e\}) \leqslant \mathrm{r}(A) + 1,$$
for $A \subseteq E$ and $e \in E$.

For the rank function of a *greedoid* the additional conditions are weaker versions of those for a matroid:

(i) Local submodularity: If $r(A) = r(A \cup \{e\}) = r(A \cup \{f\})$, then $r(A \cup \{e, f\}) = r(A)$, for $A \subseteq E$ and $e, f \in E$;

(ii) Monotonicity:
$$r(A) \leqslant r(A \cup \{e\}),$$
for $A \subseteq E$ and $e \in E$.

Item (ii) implies that r takes nonnegative values. Antimatroids are special types of greedoids, variation in item (i) more complicated to state.

when $|E| \geqslant 2$ the matroid S is connected if and only if the coefficient of x in $T_S(x,y)$ is non-zero (a result due to Crapo [10]).[2] For greedoids (ranked sets generally) there are examples of S not expressible as the direct sum of greedoids (ranked sets) on non-empty groundsets such that $T_S(x,y)$ is reducible, and examples of S such that $T_S(x,y)$ is irreducible but the coefficient of x is zero. (For the latter, see Remark 2 below.)

Definition 2. Let $S = (E, \mathrm{r})$ where E is a finite set and r is a rank function on E. The dual rank function r^* is defined by

$$\mathrm{r}^*(A) = |A| + \mathrm{r}(E \setminus A) - \mathrm{r}(E),$$

for $A \subseteq E$, and we write $S^* = (E, \mathrm{r}^*)$ for the corresponding ranked set.

The dual r^* of a rank function is again a rank function because $\mathrm{r}^*(\varnothing) = 0 = \mathrm{r}(\varnothing)$; the condition $\mathrm{r}^*(A) \leqslant |A|$ is satisfied for all $A \subseteq E$ as $\mathrm{r}^*(A) = |A| - [\mathrm{r}(E) - \mathrm{r}(E \setminus A)] \leqslant |A|$ since $\mathrm{r}(E \setminus A) \leqslant \mathrm{r}(E)$; and $\mathrm{r}^*(A) = |A| + \mathrm{r}(E \setminus A) - \mathrm{r}(E) \leqslant |A| + |E \setminus A| - \mathrm{r}(E) = |E| - r(E) = \mathrm{r}^*(E)$. The dual of the dual rank function satisfies $(\mathrm{r}^*)^*(A) = |A| + |E \setminus A| + \mathrm{r}(A) - \mathrm{r}(E) - [|E| - \mathrm{r}(E)] = \mathrm{r}(A)$. Thus $(S^*)^* = S$, and it is routine to verify the duality formula $T_{S^*}(x,y) = T_S(y,x)$.

We have $\deg_x T_S = \mathrm{r}(E) - \min_A \mathrm{r}(A) \geqslant \mathrm{r}(E)$ with equality if and only if r takes just non-negative values; and, noting that $|A| - \mathrm{r}(A) = \mathrm{r}^*(E) - \mathrm{r}^*(E \setminus A)$, $\deg_y T_S = \mathrm{r}^*(E) - \min_A \mathrm{r}^*(A) \geqslant |E| - \mathrm{r}(E)$, with equality if and only if r^* takes just non-negative values.

2.1. **Brylawski polynomials.**

Definition 3. A bivariate polynomial $U(x,y)$ over a commutative ring R such that $(y-1)^r U(\frac{y}{y-1}, y) = cy^n$ for some non-negative integer n, integer r, and non-zero constant $c \in R$ is called an (n,r)-*Brylawski polynomial* (with constant c). Equivalently, $(x-1)^{n-r} U(x, \frac{x}{x-1}) = cx^n$.

In Definition 3, we may have $r < 0$: for example, $U(x,y) = (y-1)^\ell$ is a $(0,-\ell)$-Brylawski polynomial (with constant $c = 1$). Similarly, we may have $r > n$: for example, $(x-1)^k$ is a $(0,k)$-Brylawski polynomial (with constant $c = 1$). By Proposition 2.1, the corank-nullity polynomial $T_S(x,y)$ of a ranked set $S = (E, \mathrm{r})$ is an $(|E|, \mathrm{r}(E))$-Brylawski polynomial (with constant $c = 1$). Here $0 \leqslant r = \mathrm{r}(E) \leqslant n = |E|$.

More generally, polynomials of the form $c_0 x^{k_1} y^{\ell_1} (x-1)^{k_2} (y-1)^{\ell_2}$, with $c_0 \in R \setminus \{0\}$, $k_i, \ell_j \in \mathbf{Z}_{\geqslant 0}$, are clear instances of Brylawski polynomials (for the choice $(n,r) = (k_1+\ell_1, k_1+k_2-\ell_2)$).

If $U(x,y)$ is an (n,r)-Brylawski polynomial and $V(x,y)$ is an (m,s)-Brylawski polynomial, then $U(x,y)V(x,y)$ is an $(n+m, r+s)$-Brylawski polynomial. (Lemma 2.5 below gives the converse.) In particular, if $U(x,y)$ is an (n,r)-Brylawski polynomial then $x^{k_1} y^{\ell_1} (x-1)^{k_2} (y-1)^{\ell_2} U(x,y)$ is an $(n + k_1 + \ell_1, r + k_1 + k_2 - \ell_2)$-Brylawski polynomial.

For a polynomial $U(x,y) = \sum u_{i,j} x^i y^j \in R[x,y]$, we set $\deg_x U = \max\{i : \exists j \;\; u_{i,j} \neq 0\}$ and $\deg_y U = \max\{j : \exists i \;\; u_{i,j} \neq 0\}$.

[2] The proof of this depends on the fact that for a connected matroid S and $e \in E$ either $S \backslash e$ or S/e is also connected [43, §6.5] (see also [10, p. 410]); that $t_{1,0}$, like all the coefficients of the Tutte polynomial, is non-negative (as is easily seen by induction using its deletion-contraction recurrence); and finally that $t_{1,0}$ satisfies the deletion-contraction recurrence for the Tutte polynomial. These properties do not extend to ranked sets generally.

Proposition 2.2. *If $U(x,y)$ is an (n,r)-Brylawski polynomial of $R[x,y]$, then $\deg_x U \geqslant r$ and $\deg_y U \geqslant n-r$.*

Moreover if R is a UFD then univariate factors of $U(x,y)$ are necessarily of the form $a(x-1)^k x^\ell$ or $b(y-1)^k y^\ell$, for $a,b \in R \setminus \{0\}$ and $k,\ell \in \mathbf{Z}_{\geqslant 0}$.

Proof. Let $U(x,y) = \sum u_{i,j} x^i y^j$ and $d \coloneqq \deg_x$. Since $\sum_{i,j} u_{i,j}(y-1)^{d-i} y^{i+j} = c(y-1)^{d-r} y^n$ is a polynomial identity, the degree d satisfies $d \geqslant r$. Moreover, if $d > r$, then, by setting $y = 1$ in this identity, $\sum_j u_{d,j} = 0$, while if $d = r$ then $\sum_j u_{d,j} = c$. Likewise, as the identity $(y-1)^r U(\frac{y}{y-1}, y) = cy^n$ is equivalent to the identity $(x-1)^{n-r} U(x, \frac{x}{x-1}) = cx^n$, a similar argument shows that $\deg_y U \geqslant n-r$.

We turn to the second statement. If $U(x,y)$ is a Brylawski polynomial divisible by a polynomial $V(x)$ (independent of y), then there exists $U_0(x,y) \in R[x,y]$ such that

$$(x-1)^{n-r} U(x, \tfrac{x}{x-1}) = V(x)(x-1)^{n-r} U_0(x, \tfrac{x}{x-1}) = cx^n.$$

By unique factorization in $R[x]$ the only potential irreducible factors of $V(x)$ are x and $x-1$. We reach the analogous conclusion for factors of $U(x,y)$ of type $V(y) \in R[y]$ by using the identity $(y-1)^r U(\frac{y}{y-1}, y) = cy^n$. □

Remark 1. We can say a little more in Proposition 2.2 when $U(x,y)$ is the corank-nullity polynomial $T_S(x,y)$ of a ranked set $S = (E, \mathrm{r})$. As already mentioned, T_S is an $(|E|, \mathrm{r}(E))$-Brylawski polynomial (by Proposition 2.1), and we have equality in $\deg_x T_S \geqslant \mathrm{r}(E)$ if and only if $\mathrm{r}(A) \geqslant 0$ for each $A \subseteq E$, and equality in $\deg_y T_S \geqslant |E| - \mathrm{r}(E)$ if and only if $\mathrm{r}^*(A) \geqslant 0$ for each $A \subseteq E$.

Moreover the only possible univariate factors of $T_S(x,y)$ are of the form ax^ℓ and by^ℓ. For suppose $x-1$ divides $T_S(x,y)$. Then

$$T_S(1,y) = \sum_{\substack{A \subseteq E \\ \mathrm{r}(A) = \mathrm{r}(E)}} (y-1)^{|A| - \mathrm{r}(E)} = 0,$$

which cannot hold as the sum contains leading term $(y-1)^{|E| - \mathrm{r}(E)}$, and so is monic as a polynomial in y. Dually, supposing $y-1$ divides $T_S(x,y)$ yields

$$T_S(x,1) = \sum_{\substack{A \subseteq E \\ \mathrm{r}(A) = |A|}} (x-1)^{\mathrm{r}(E) - |A|} = 0,$$

and the sum is a monic polynomial in x (from the term contributed by $A = \varnothing$).

When $S = (E, \mathrm{r})$ is a matroid, if x^ℓ divides $T_S(x,y)$ then S is the direct sum of a smaller ranked set and $S_1 = (E_1, \mathrm{r}_1)$, in which $|E_1| = \ell$ and $\mathrm{r}_1(A) = |A|$ for each $A \subseteq E_1$ (i.e., S_1 is the matroid of ℓ coloops, for which $T_{S_1}(x,y) = x^\ell$); dually, if y^ℓ divides $T_S(x,y)$ then S is the direct sum of a smaller ranked set and $S_1^* = (E_1, \mathrm{r}_1^*)$, in which $|E_1| = \ell$ and $\mathrm{r}_1^*(A) = 0$ for each $A \subseteq E_1$ (i.e., S_1^* is the matroid of ℓ loops, for which $T_{S_1^*}(x,y) = y^\ell$).

The motivation for the name "Brylawski polynomial" lies in the following key proposition and its consequence for corank-nullity polynomials of ranked sets (Corollary 2.4).

Proposition 2.3 ([1, proof of Theorem 1.1]). *If $U(x,y)$ is an (n,r)-Brylawski polynomial with constant c then its coefficients $u_{i,j}$ satisfy* [3]

$$\sum_{\substack{i,j\\ i+j\leqslant h}} (-1)^j \binom{h-i}{j} u_{i,j} = c\cdot(-1)^{n-r}\binom{h-r}{h-n}, \quad \text{for any integer } h \geqslant 0.$$

In particular, $u_{0,0} = 0$ if $n > 0$, and $u_{1,0} = u_{0,1}$ if $n > 1$. Proposition 2.3 contains the following special case.

Corollary 2.4. *Let $S = (E, \mathrm{r})$ be a ranked set with $|E| = n$, $\mathrm{r}(E) = r$, and $T_S(x,y) = \sum_{i,j} t_{i,j}x^i y^j$. Then, for any integer $h \geqslant 0$,*

$$\sum_{\substack{i,j\\ i+j\leqslant h}} (-1)^j \binom{h-i}{j} t_{i,j} = (-1)^{n-r}\binom{h-r}{h-n}. \tag{3}$$

The linear relations given by Corollary 2.4 for $0 \leqslant h < n$ were established by Brylawski [5] for matroid rank functions, and extended to greedoid and antimatroid rank functions by Gordon [22], who also established the affine relation for $h = n$. Although the proof of Corollary 2.4 given by Beke *et al* [1] assumes that r takes non-negative values, it is easily extended to include the case of rank functions taking negative values as well. In fact [1, Th. 1.1] is really Corollary 2.4 above once extended from **N**- to **Z**-valued rank functions: Beke *et al* do not explicitly state the generalization to Brylawski polynomials, although their argument depends only property defining a Brylawski polynomial (Definition 3) and not on being the Tutte polynomial of a rank function.

A constant not equal to 1 in Definition 3 of an (n,r)-Brylawski polynomial features in [2, Lemma 7.6, Theorem 8.2]. For our purposes, allowing an arbitrary constant serves as a technical convenience (and we do not usually need to specify the constant) enabling one to prove stability properties of the class of Brylawski polynomials. While it is straightforward to see that the product of two Brylawski polynomials is again a Brylawski polynomial, the following lemma asserts that the converse holds over any UFD.

Lemma 2.5. *Let R be a UFD. Suppose that $T(x,y)$ is an (n,r)-Brylawski polynomial in $R[x,y]$ with factorization $T(x,y) = U(x,y)V(x,y)$ in $R[x,y]$. Then there are integers m, s such that $U(x,y)$ is an $(n-m, r-s)$-Brylawski polynomial and $V(x,y)$ is an (m,s)-Brylawski polynomial, where $0 \leqslant m \leqslant n$.*

Proof. For simplicity write $T(x,y) = T(x)$, meaning that it is considered as a polynomial in x with coefficients in $R[y]$. Likewise write $T(x) = U(x)V(x)$ the given factorization of T over $R[y]$. As T is an (n,r)-Brylawski polynomial, there is non-zero $c \in R$ such that

$$cy^n = (y-1)^r T\Big(\frac{y}{y-1}\Big) = (y-1)^{r-s}U\Big(\frac{y}{y-1}\Big)\cdot(y-1)^s V\Big(\frac{y}{y-1}\Big), \tag{4}$$

where s is chosen to be the minimal integer such that $(y-1)^s V(\frac{y}{y-1})$ is a polynomial in y. This then forces $(y-1)^{r-s}U(\frac{y}{y-1})$ to be a polynomial in y, for otherwise it is a ratio of a polynomial in y and a power of $y-1$, and this implies that $y-1$ divides $(y-1)^s V(\frac{y}{y-1})$ as

[3] We use the convention $\binom{a}{b} = 0$ if $b < 0$ or $b > a$.

the product on the right-hand side of (4) is the polynomial cy^n on the left-hand side, which contradicts minimality of s.

By unique factorization in $R[y]$, this implies that

$$(y-1)^s V\big(\frac{y}{y-1}\big) = by^m, \quad \text{and } (y-1)^{r-s} U\big(\frac{y}{y-1}\big) = ay^{n-m},$$

for some $a, b \in R$ such that $ab = c$ and some integer m satisfying $0 \leqslant m \leqslant n$. □

2.2. **Irreducibility of Brylawski polynomials.** The main result of this section is the following.

Theorem 2.6. *Let R be a UFD and let $T(x,y) = \sum_{i,j} t_{i,j} x^i y^j \in R[x,y]$ be an (n,r)-Brylawski polynomial, where n, r are integers with $r \geqslant 1$ and $n - r \geqslant 1$. Suppose that* (i) *neither $x-1$ nor $y-1$ divide $T(x,y)$;* (ii) *$t_{1,0} \neq 0$ and* (iii) *$\deg_x T + \deg_y T \in \{n, n+1\}$. If $T(x,y) = U(x,y)V(x,y)$ in $R[x,y]$ then $U(x,y)$ or $V(x,y)$ is constant (in R). In particular $T(x,y)$ is irreducible in $k[x,y]$ where k is the fraction field of R; moreover if $\gcd_{i,j}\{t_{i,j}\} = 1$ then $T(x,y)$ is irreducible in $R[x,y]$.*

By Proposition 2.2, condition (iii) is equivalent to $\deg_x T + \deg_y T \leqslant n+1$.

Proof of Theorem 2.6. Suppose that $T(x,y)$ is an (n,r)-Brylawski polynomial and $T(x,y) = U(x,y)V(x,y)$, where U, V are not constants (in R). By assumption (i), and the fact that under assumption (ii) neither x nor y divide $T(x,y)$ (noting that $t_{0,1} = t_{1,0}$ by Proposition 2.3 as $n \geqslant 2$), Proposition 2.2 implies neither $U(x,y)$ nor $V(x,y)$ is univariate. By Lemma 2.5 there are integers m, s such that $U(x,y)$ is an $(n-m, r-s)$-Brylawski polynomial and $V(x,y)$ is an (m,s)-Brylawski polynomial, where $0 \leqslant m \leqslant n$. We also have $\deg_x U + \deg_x V = \deg_x T$ and $\deg_y U + \deg_y V = \deg_y T$. By definition, there is $c \in R$ such that

$$(y-1)^r T(\frac{y}{y-1}, y) = cy^n.$$

We may assume that $0 < \deg_x U, \deg_x V < \deg_x T$ and $0 < \deg_y U, \deg_y V < \deg_y T$. For otherwise $T(x,y)$ admits a univariate factor in $R[x,y]$ and we reach a contradiction.

As $U(x,y)$ is an $(n-m, r-s)$-Brylawski polynomial and $V(x,y)$ is a (m,s)-Brylawski polynomial where $0 \leqslant m \leqslant n$, by Proposition 2.2 we have $s \leqslant \deg_x V < \deg_x T$ and $m - s \leqslant \deg_y V < \deg_y T$. These inequalities imply that $m \leqslant \deg_x T + \deg_y T - 2 \leqslant n-1$. Similarly, $r - s \leqslant \deg_x U < \deg_x T$ and $n - m - (r-s) \leqslant \deg_y U < \deg_y T$ imply that $n - m \leqslant \deg_x T + \deg_y T - 2 \leqslant n-1$. Hence $m \geqslant 1$ and $n - m \geqslant 1$, and the first of Brylawski's relations gives $v_{0,0} = 0 = u_{0,0}$.

But then $t_{1,0} = u_{0,0}v_{1,0} + u_{1,0}v_{0,0} = 0$, contrary to assumption (ii). □

When $T = T_S$ is the corank-nullity polynomial of a ranked set $S = (E, \mathrm{r})$ in which both r and its dual r^* take nonnegative values (which holds for rank functions of matroids, but not necessarily of greedoids [21]), we have $\deg_x T_S = \mathrm{r}(E)$ and $\deg_y T_S = |E| - \mathrm{r}(E)$ and so, with $\deg_x T_S + \deg_y T_S = |E|$, condition (iii) in Theorem 2.6 holds for the $(|E|, \mathrm{r}(E))$-Brylawski polynomial $T_S(x,y)$. But if either r or r^* take negative values, then condition (iii) fails for T_S unless only one of these rank functions takes negative values and moreover the only negative value this one takes is -1. We therefore deduce the following particular case of Theorem 2.6, first shown by Merino, de Mier and Noy [33].

Corollary 2.7. *Let M be a connected matroid on groundset E of size $\geqslant 2$ and with Tutte polynomial $T_M(x,y) = \sum_{i,j} t_{i,j} x^i y^j$. Let R be any UFD and let $\varphi\colon \mathbf{Z} \to R$ be the natural ring homomorphism whose kernel is generated by the characteristic κ of R. Assuming that $\kappa \nmid t_{1,0}$, then T_M, seen as an element of $R[x,y]$ by applying φ to its coefficients, is irreducible.*

For a connected matroid $S = (E, \mathrm{r})$ with $|E| \geqslant 2$, we have $t_{1,0} = t_{0,1} \neq 0$, ensuring that $r = \mathrm{r}(E) \geqslant 1$ and $n - r = |E| - \mathrm{r}(E) \geqslant 1$ as required for Theorem 2.6.

Corollary 2.7 extends to delta matroids in which the rank function r used in the definition of the Tutte polynomial is the function σ defined in [15, p. 1341, eq. (3)] (obtained by averaging the ranks of two associated matroids). By Theorem 4.7 of the paper just cited, the coefficient $t_{1,0}$ is non-zero if and only if the delta matroid is connected; that paper's Theorem 1.2 is then a consequence of the general phenomenon recorded in our Theorem 2.6.

Remark 2. Assumptions (ii) and (iii) in Theorem 2.6 are not necessary conditions for irreducibility. (As already mentioned, for matroids assumption (ii) is in fact necessary as well as sufficient for connectivity, and accordingly necessary and sufficient for irreducibility [33].)

The polynomial $x^3 + 2x^2 + y^2 + 3xy$ (see [22, p. 23]) is a $(5,3)$-Brylawski polynomial, equal to the corank-nullity polynomial

$$T_S(x,y) = (x-1)^3 + 5(x-1)^2 + 10(x-1) + 7 + 3(x-1)(y-1) + 5(y-1) + (y-1)^2,$$

where $S = (E, \mathrm{r})$, in which $|E| = 5$ and r is defined by $\mathrm{r}(\varnothing) = 0$; $\mathrm{r}(A) = 1$ for each A of size 1; $\mathrm{r}(A) = 2$ for each A of size 2; $\mathrm{r}(A) = 3$ for 7 subsets A of size 3, and $\mathrm{r}(A) = 2$ for the remaining 3 subsets of size 3; $\mathrm{r}(A) = 3$ for each A of size 4; and $\mathrm{r}(E) = 3$. The polynomial $T_S(x,y)$ shares with the Tutte polynomial of a matroid the properties of being monic as a polynomial in x (considering $T_S(x,y)$ over $\mathbf{Z}[y]$) and monic as a polynomial in y (considering $T_S(x,y)$ over $\mathbf{Z}[x]$). This polynomial is irreducible (as a quadratic in y, its discriminant is $x^2(1-4x)$) but does not satisfy assumption (ii) of Theorem 2.6. Irreducibility of $T_S(x,y)$ implies the ranked set S cannot be expressed as the direct sum of smaller ranked sets.[4]

[4] Gordon [20] exhibits in his Example 2.1 a greedoid that is not decomposable as a direct sum of smaller greedoids and yet has $t_{1,0} = 0$. Let $E = \{a,b,c\}$ and $\mathcal{F} = \{\varnothing, \{a\}, \{b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$. The greedoid rank function is defined for $A \subseteq E$ by

$$\mathrm{r}(A) = \max\{|F| : F \in \mathcal{F}, F \subseteq A\}.$$

Then $S = (E, \mathrm{r})$ has corank-nullity polynomial

$$\begin{aligned} T_S(x,y) &= (x-1)^3 + 2(x-1)^2 + (x-1)^3(y-1) + 2(x-1) + (x-1)^2(y-1) + 1 \\ &= x[x + (x-1)^2 y] \end{aligned}$$

The first factor is the Tutte polynomial of a single isthmus, i.e. of the ranked set $S_1 = (E_1, \mathrm{r}_1)$, where $E_1 = \{c\}$ and r_1 is defined by $\mathrm{r}_1(\varnothing) = 0, \mathrm{r}(\{c\}) = 1$. While the second factor is not the Tutte polynomial of a greedoid, it is equal to

$$(x-1)^2(y-1) + (x-1)^2 + x - 1 + 1$$

which is the corank-nullity polynomial of $S_2 = (E_2, \mathrm{r}_2)$ in which $E_2 = \{a,b\}$ and r_2 is defined by

$$\mathrm{r}_2(\varnothing) = 0,\ \mathrm{r}_2(\{a\}) = 0,\ \mathrm{r}_2(\{b\}) = 1,\ \mathrm{r}_2(\{a,b\}) = 2.$$

Not only do we have then

$$T_S(x,y) = T_{S_1}(x,y) T_{S_2}(x,y),$$

but $S = S_1 \oplus S_2$ even though as a greedoid S cannot be expressed as a sum of smaller greedoids.

Assumption (iii), while automatic for corank-nullity polynomials of matroids, as noted after the statement of the theorem, is not necessary either, as the following example shows. We define the ranked set $S = (E, \mathrm{r})$ for integers $a > b > 0$, in which $|E| \geqslant b$, by setting

$$\mathrm{r}(A) = \begin{cases} 0 & A = \varnothing, \\ |A| - a & \varnothing \subsetneq A \subsetneq E, \\ |E| - b & A = E. \end{cases}$$

Then

$$T_S(x,y) = (x-1)^{|E|-b} + \sum_{\varnothing \subsetneq A \subsetneq E} (x-1)^{|E|-b-|A|+a}(y-1)^{|A|-|A|+a} + (y-1)^{|E|-|E|+b}$$

$$= (x-1)^{|E|-b} + (x-1)^{a-b}(y-1)^a \sum_{0<i<|E|} \binom{|E|}{i} (x-1)^i + (y-1)^b.$$

Also,

$$\mathrm{r}^*(A) = \begin{cases} 0 & A = \varnothing, \\ b - a & \varnothing \subsetneq A \subsetneq E, \\ b & A = E. \end{cases}$$

Writing $X = x - 1$, $Y = y - 1$, $|E| = n$,

$$T_S(X,Y) = X^{n-b} + X^{a-b}Y^a \sum_{0<i<n} \binom{n}{i} X^i + Y^b.$$

This has X-degree $n + (a - b - 1) \geqslant n \geqslant r(E) = n - b$ and Y-degree a, so that $\deg_x T_S + \deg_y T_S = n + 2a - b - 1 \geqslant n + a$. Thus for $a > 1$ the assumption (iii) fails. The Newton polygon of $T_S(X,Y)$ has vertices $(0,b)$, $(n-b,0)$, and $(a-b+i,a)$ for $i \in \{n-1,\ldots,1\}$, and is readily seen not to be reducible as a Minkowski sum of smaller polygons. (Its sides have direction vectors $(n-b,-b)$, $(a-1,a)$, $(-1,0)$ ($n-2$ times), and $(b-a-1,b-a)$; since $a, b, a-b > 0$, all the sides of one of the smaller polygons would be forced to have direction vectors $(-1,0)$.) Hence $T_S(X,Y)$ is irreducible ([18, p. 507]).

The example in Remark 2 in which assumption (ii) of Theorem 2.6 fails is accommodated by the following irreducibility criterion, derived by a similar proof to that of Theorem 2.6.

Theorem 2.8. *Let $T(x,y) = \sum_{i,j} t_{i,j} x^i y^j$ be an (n,r)-Brylawski polynomial over R, a UFD, where n, r are integers with $r \geqslant 1$ and $n - r \geqslant 1$. Let $\varphi\colon \mathbf{Z} \to R$ be the canonical ring homomorphism and suppose that* (i) *none of $x-1, y-1, x, y$ divide $T(x,y)$;* (ii) *$\varphi(2) \nmid t_{1,1}$; and* (iii) *$\deg_x T + \deg_y T = n$. Then $T(x,y)$ is irreducible in $k[x,y]$ where k denotes the fraction field of R; moreover if $\gcd_{i,j}\{t_{i,j}\} = 1$ in R then $T(x,y)$ is irreducible in $R[x,y]$.*

Proof. Suppose that $T(x,y) = U(x,y)V(x,y)$ is factorization of $T(x,y)$ in $R[x,y]$ with both U and V non constant. Assumption (iii) (together with Proposition 2.2) implies $\deg_x U + \deg_x V = \deg_x T = r$ and $\deg_y U + \deg_y V = \deg_y T = n - r$, and as $T(x,y)$ is an (n,r)-Brylawski polynomial, there is $c \in R$ such that

$$(y-1)^r T\left(\frac{y}{y-1}, y\right) = cy^n.$$

As in the proof of Theorem 2.6, we may assume that $0 < \deg_x U, \deg_x V < \deg_x T$ and $0 < \deg_y U, \deg_y V < \deg_y T$ (needing (i); note that assuming that neither x nor y are factors of $T(x,y)$ replaces the condition that $t_{1,0} \neq 0$ assumed in the earlier theorem), and, using Lemma 2.5, the polynomial $U(x,y)$ is an $(n-m, r-s)$-Brylawski polynomial and $V(x,y)$ is a (m,s)-Brylawski polynomial for some integers m, s with $0 \leqslant m \leqslant n$. We invoke Proposition 2.2 and see that the inequalities $s \leqslant \deg_x V < \deg_x T$ and $m - s \leqslant \deg_y V < \deg_y T$ imply that $m \leqslant \deg_x T + \deg_y T - 2 = n-2$; and $r-s \leqslant \deg_x U < \deg_x T$ and $n-m-(r-s) \leqslant \deg_y U < \deg_y T$ imply $n - m \leqslant \deg_x T + \deg_y T - 2 = n-2$. Hence $m \geqslant 2$ and $n - m \geqslant 2$, and the first two Brylawski relations (Proposition 2.3) give $v_{0,0} = 0 = u_{0,0}$ and $u_{1,0} = u_{0,1}$ and $v_{1,0} = v_{0,1}$.

But then $t_{1,1} = u_{0,0}v_{1,1} + u_{1,1}v_{0,0} + u_{1,0}v_{0,1} + u_{0,1}v_{1,0} = \varphi(2)u_{0,1}v_{0,1}$, contradicting (ii). □

We close this section with two examples of ranked sets for which our general criteria for irreducibility in Theorems 2.6 and 2.8 are not satisfied, but which we can prove are irreducible by considering their Newton polygons (again applying [18, p. 507]). Each example involves a rank function taking non-negative values, but whose dual takes negative values. In Section 4.1.1 we show that the Galois group of the corank-nullity polynomial in Example 1 as a polynomial in x is not the full symmetric group of degree r (see Proposition 4.2; this is the only example we know where Conjecture 1.1 does not extend from matroids to ranked sets generally). In Section 4.1.2 we exhibit an infinite number of instances of the corank-nullity polynomial in Example 2 for which its Galois group as a polynomial in x is the symmetric group of degree $|E|$ (see Corollary 4.4).

Example 1. Let E be a finite set and let $r \in \mathbf{Z}$ be such that $|E| \geqslant r \geqslant 1$. Consider $\mathrm{r}\colon 2^E \to \mathbf{Z}$ the rank function defined by $\mathrm{r}(E) = r$ and $\mathrm{r}(A) = 0$ for $A \subsetneq E$. The corank-nullity polynomial of the ranked set $S = (E, \mathrm{r})$ is

$$T_S(x,y) = (y-1)^{|E|-r} + (y^{|E|} - (y-1)^{|E|})(x-1)^r,$$

which is an $(|E|, r)$-Brylawski polynomial with $\deg_x T_S = r = \mathrm{r}(E)$ and $\deg_y T_S = |E| - 1 \geqslant |E| - \mathrm{r}(E)$. As $\deg_x T_S + \deg_y T_S = n + r - 1$, assumption (iii) of Theorem 2.6 is not satisfied if $r > 2$.

The dual rank function r^* is defined by $\mathrm{r}^*(\varnothing) = 0$, and $\mathrm{r}^*(A) = |A| - r$ for $\varnothing \subsetneq A \subseteq E$.

The Newton polygon of the polynomial $Y^{|E|-r} + X^r[(Y+1)^{|E|} - Y^{|E|}]$ is the convex hull of vertices $(0, |E| - r)$ and (r, i) for $i \in \{0, 1, \ldots, |E| - 1\}$ and this clearly cannot be expressed as a Minkowski sum of smaller polygons (the direction vectors of the segments forming the convex hull — a triangle — are $(r, -|E| + r)$, $(0, 1)$ with multiplicity $|E| - 1$, and $(-r, 1 - r)$). Hence $T_S(x,y)$ is irreducible.

Example 2. Let E be a non-empty finite set and for $A \subset E$ define the rank function r by

$$\mathrm{r}(A) = \begin{cases} 0 & A = \varnothing \\ 1 & \varnothing \subsetneq A \subsetneq E \\ |E| & A = E. \end{cases}$$

The Tutte polynomial of $S = (E, \mathrm{r})$ is

$$T_S(x,y) = (x-1)^{|E|} + \sum_{\varnothing \subsetneq A \subsetneq E} (x-1)^{|E|-1}(y-1)^{|A|-1} + 1$$
$$= (x-1)^{|E|} + (x-1)^{|E|-1}\left(\frac{y^{|E|} - 1 - (y-1)^{|E|}}{y-1}\right) + 1.$$

Here $\deg_x T_S = |E| = \mathrm{r}(E)$ and $\deg_y T_S = |E| - 2 \geqslant |E| - \mathrm{r}(E) = 0$. As $\deg_x T_S + \deg_y T_S = 2|E| - 2$ assumption (iii) of Theorem 2.6 fails when $|E| > 3$. The dual rank function is defined by

$$\mathrm{r}^*(A) = \begin{cases} 0 & A = \varnothing \\ 1 - |E \setminus A| & \varnothing \subsetneq A \subsetneq E \\ 0 & A = E. \end{cases}$$

The Newton polygon of the polynomial $X^{|E|} + X^{|E|-1}\frac{(Y+1)^{|E|}-1-Y^{|E|}}{Y} + 1$ is the convex hull of vertices $(|E|, 0)$, $(0,0)$ and $(|E|-1, i)$ for $i \in \{0, 1, \ldots, |E|-2\}$ (again this is a triangle and the direction vectors of the sides are $(-1, |E|-2)$, $(-|E|+1, -|E|+2)$ and $(|E|, 0)$). This clearly cannot be expressed as a Minkowski sum of smaller polygons. Hence $T_S(x,y)$ is irreducible.

3. Probabilistic approach: generic Galois maximality

In this section, which is to a large extent of independent interest, we approach Conjecture 1.1 from a probabilistic point of view: within suitable families of polynomials equipped with a "height function" and originating from well identified rank functions (such as rank functions associated to connected matroids) we aim at obtaining an upper bound on the size of the set of "pathological" elements (those having a non maximal Galois group) in the family as the height grows. This is achieved through Kowalski's sieve framework [28] with a crucial appeal to Cohen's work [8]. In the first subsection below we state and prove a generalized form of a uniform sieve bound due to Gallagher [17] towards the celebrated (and recently solved [3]) conjecture of van der Waerden [44] from 1936.

3.1. Generalizing a uniform version of a Theorem of Gallagher.

Gallagher [17] considers, for fixed $r \geqslant 1$ and for a growing parameter $N \in \mathbf{N}_{\geqslant 1}$, the set

$$E_r(N) := \left\{ f(x) = x^r + \sum_{i=0}^{r-1} a_i x^i \colon a_i \in \mathbf{Z},\ |a_i| \leqslant N,\ |\operatorname{Gal}_{\mathbf{Q}}(f)| < r! \right\}$$

of polynomials f for which the Galois group of a splitting field over $\mathbf{Q}$ (denoted $\operatorname{Gal}_{\mathbf{Q}}(f)$ in the above definition of $E_r(N)$) is not maximal. A uniform version of the large sieve result of Gallagher [17] states that $|E_r(N)|/(2N+1)^r \ll r^3 \log N \cdot N^{-1/2}$ (for all $N \geqslant 2$, all $r \geqslant 1$, and with an absolute implied constant, see [28, Th. 4.2]). The starting point of Gallagher's method is the identification of the set of monic $\mathbf{Z}$-polynomials of degree r with $\mathbf{Z}^r$ through fixing the canonical basis $(1, x, \ldots, x^{r-1})$ of $\mathbf{Q}$-polynomials of degree $< r$.

We extend Gallagher's approach to more general linearly independent families of polynomials. Our result (Theorem 3.1) gives the same type of uniform upper bound on the proportion of pathological elements (still meant in the sense that the Galois group is not maximal) as in [28, Th. 4.2].

For $s \in \mathbf{N}$, consider a family $(F_0, \dots, F_s)$ of monic polynomials in $\mathbf{Z}[x]$ with $\deg F_s < \max\{\deg F_i \colon i \leqslant s-1\} =: r$. For p an element in a set of prime numbers $\mathcal{P}(r)$ of positive density (the definition of $\mathcal{P}(r)$ may depend on r only and we assume that its density admits a positive lower bound uniform in r), let $(F_{0,p}, \dots, F_{s,p})$ be the reduction of $(F_0, \dots, F_s)$ modulo p (meaning that we reduce the coefficients of the polynomials F_i modulo p). For any prime $p \in \mathcal{P}(r)$, assume the following assumptions hold:

(H1) the polynomials $F_{i,p}$ are relatively prime for $i \in \{0, \dots, s\}$, and $(F_{0,p}, \dots, F_{s,p})$ is linearly independent over $\mathbf{F}_p$ (in particular $s \leqslant r$),

(H2) the family $(F_{i,p} - \beta_i F_{s,p})_{0 \leqslant i \leqslant s-1}$ has *normal* gcd for all $(\beta_i) \in \mathbf{F}_p^s$ in the sense of Cohen [8, p. 95] (*i.e.* the gcd of this family has at most one multiple irreducible factor which, if it exists, has multiplicity 2 and degree 1) and $(F_{i,p})_{0 \leqslant i \leqslant s}$ is *not totally composite* in the sense of [8, (2.2)] (a family $(f_0, \dots, f_s) \in \mathbf{F}_p[x]^{s+1}$ is *totally composite* if there exists $\psi = N/D \in \mathbf{F}_p(x)$, written in lowest degree terms, and $(g_j)_{0 \leqslant j \leqslant s} \in \mathbf{F}_p[x]^{s+1}$, such that $\deg N > \deg D + 1$, $\ell := \max_j \deg g_j > 1$ and $f_i = D^\ell \cdot (g_i \circ \psi)$ for all $i \in \{0, \dots, s\}$).

The main result of this subsection is the following extension of the uniform version of Gallagher's Theorem ([28, Th. 4.2]).

Theorem 3.1. *With notation and assumptions as above, one has:*

$$\frac{\left|\left\{(n_i)_{1 \leqslant i \leqslant s} \in [-N, N]^s \colon |\operatorname{Gal}_{\mathbf{Q}}\left(F_0 + \sum_{i=1}^s n_i F_i\right)| < r!\right\}\right|}{(2N+1)^s} \ll r^2 \Big(1 + \frac{1}{\log r}\Big)^{2s} \frac{\log N}{\sqrt{N}},$$

for every integers $s \geqslant 1$, $r \geqslant 2$, every $N \gg_r 1$ and with an absolute implied constant.

As already mentioned above, the proof proceeds by a sieving argument using primes in the set $\mathcal{P}(r)$. Before proving Theorem 3.1, we introduce the necessary objects and outline the sieve setup.

For a prime number p, we let $\pi_p \colon \mathbf{Z}^s \to \mathbf{F}_p^s$ be the reduction modulo p morphism that acts coordinate-wise. Let λ be a *factorisation pattern* for polynomials of degree r: given a partition λ of r (*i.e.* $\lambda = (a_1, \dots, a_r) \in \mathbf{Z}_{\geqslant 0}^r$ with $\sum_{i=0}^r i a_i = r$), a polynomial f of degree r has factorisation pattern λ if it has exactly a_i distinct irreducible factors of degree i, for each $i \in \{0, \dots, r\}$ (in particular such an $\mathbf{F}_p$-polynomial is squarefree). For a prime number p and for $\boldsymbol{\lambda} = \{\lambda_i\}_i$ a set of partitions of r, define the following subset of $\mathbf{F}_p^s$:

$$\Omega_{\boldsymbol{\lambda},p} = \Big\{(\beta_i)_{1 \leqslant i \leqslant s} \in \mathbf{F}_p^s \colon F_{0,p} + \sum_{i=1}^s \beta_i F_{i,p} \text{ has factorisation pattern } \lambda \in \boldsymbol{\lambda} \text{ in } \mathbf{F}_p[x]\Big\}.$$

(We will simply write $\Omega_{\lambda,p}$ if $\boldsymbol{\lambda} = \{\lambda\}$ contains a single partition.) In the spirit of [28, §4.2], we fix (for now) an auxiliary parameter L (to be eventually optimized) and consider the *sieving problem* of finding an upper bound for the cardinality of

$$S(N, \boldsymbol{\lambda}, L) := \{(n_i)_{1 \leqslant i \leqslant s} \in [-N, N]^s \colon \forall p \in \mathcal{P}(r) \cap [1, L],\ \pi_p((n_i)) \notin \Omega_{\boldsymbol{\lambda},p}\}.$$

As explained in [28, §4.2], if the reduction modulo a prime number p of $F = F_0 + \sum_{i=1}^s n_i F_i$ (corresponding to $(\pi_p(n_i))_{1 \leqslant i \leqslant s}$) has factorisation pattern λ over $\mathbf{F}_p$, then at least one permutation of cycle type λ (*i.e.* a product of a_1 fixed points, a_2 disjoint transpositions, etc...) belongs to $\operatorname{Gal}_{\mathbf{Q}}(F)$. Consequently if a polynomial $F = F_0 + \sum_{i=1}^s n_i F_i$ has a Galois group

over $\mathbf{Q}$ not intersecting the conjugacy invariant subset $c_{\boldsymbol{\lambda}}$ of $\mathfrak{S}_r$ consisting of permutations of cycle type $\lambda \in \boldsymbol{\lambda}$, then the s-tuple $(n_i)_{1\leqslant i\leqslant s}$ belongs to $S(N, \boldsymbol{\lambda}, L)$. In other words,

$$\Big|\big\{(n_i)_{1\leqslant i\leqslant s} \in [-N, N]^s\colon \operatorname{Gal}_{\mathbf{Q}}(F_0 + \sum_{i=1}^{s} n_i F_i) \text{ does not intersect } c_{\boldsymbol{\lambda}} \text{ in } \mathfrak{S}_r \big\}\Big| \leqslant \big|S(N, \boldsymbol{\lambda}, L)\big|.$$

Moreover, if $(c_{\boldsymbol{\lambda}_j})$ is a set of conjugacy invariant subsets such that no proper subgroup of $\mathfrak{S}_r$ intersects every $c_{\boldsymbol{\lambda}_j}$ then

$$\Big|\Big\{(n_i)_{1\leqslant i\leqslant s} \in [-N, N]^s\colon |\operatorname{Gal}_{\mathbf{Q}}(F_0 + \sum_{i=1}^{s} n_i F_i)| < r!\Big\}\Big| \leqslant \sum_j \big|S(N, \boldsymbol{\lambda}_j, L)\big|. \tag{5}$$

The following *sieve inequality* is a key ingredient to the proof of Theorem 3.1.

Proposition 3.2. *Let $s \geqslant 1$ be an integer and let $(F_0, \dots, F_s)$ be a $(s+1)$-tuple of monic polynomials in $\mathbf{Z}[x]$ with $\deg F_s < \max\{\deg F_i\colon i \leqslant s-1\} =: r \geqslant 2$. Let $\boldsymbol{\lambda}$ be a set of partitions of r and let $\mathcal{P}(r)$ be a set of primes depending only on r. For any positive integers N, L, there exists constants $\Delta(N, L)$ and $H(L, \boldsymbol{\lambda})$ depending only on (N, L) and $(L, \boldsymbol{\lambda})$, respectively, satisfying*

$$\big|S(N, \boldsymbol{\lambda}, L)\big| \leqslant \Delta(N, L) \cdot H(L, \boldsymbol{\lambda})^{-1}.$$

Moreover one has the bounds

$$\Delta(N, L) \leqslant (\sqrt{2N+1} + L)^{2s} \quad \text{and} \quad H(L, \boldsymbol{\lambda}) \geqslant \sum_{p\in\mathcal{P}(r)\cap[1,L]} \frac{|\Omega_{\boldsymbol{\lambda},p}|}{|\mathbf{F}_p^s|}.$$

Proof. Formally the first inequality as well as the lower bound on H are applications of Kowalski's sieve statement [28, Prop. 3.5] (where the constants Δ and H are also properly defined in a general context). The upper bound on Δ is due to Huxley [25]; see also [28, Th. 4.1]. □

In view of Proposition 3.2, our next task is to estimate the lower bound on $H(L, \lambda)$. To this purpose we appeal to a result of Cohen [8, Th. 3].

Lemma 3.3 (Cohen)**.** *Keeping the notation as in 3.2, assume that (H1) and (H2) hold for $(F_0, \dots, F_s)$. Then for every $p \in \mathcal{P}(r) \cap (r, \infty)$,*

$$\frac{|\Omega_{\lambda,p}|}{|\mathbf{F}_p^s|} = T(\lambda) + O_r(p^{-1/2}),$$

where $T(\lambda)$ is the proportion of elements of the symmetric group $\mathfrak{S}_r$ of cycle type $\lambda = (a_1, \dots, a_r)$ the partition of r with i contributing a_i times for all $i \in \{1, \dots, r\}$ (precisely[5] $T(\lambda) = (\prod_i i^{a_i} a_i!)^{-1}$).

Note that the assumption $p > r$ enables us to simplify some of the requirements in Cohen's work. Indeed, for such a p, linear independence over $\mathbf{F}_p$ is equivalent to linear independence over $\mathbf{F}_p(x^p)$, as explained by Cohen [8, p. 95], and also F_s is automatically *tame* (which means that no zero of F_s has multiplicity divisible by p [8, statement of Th. 3]).

We are now ready to prove Theorem 3.1 (the argument follows closely the proof of [28, Th. 4.2]).

[5]For example the partition λ_{irr} corresponding to irreducible polynomials is $(a_1, \dots, a_r) = (0, \dots, 0, 1)$ and one has $T(\lambda_{\mathrm{irr}}) = 1/r$.

Proof of Theorem 3.1. Imposing $L \geqslant r^2$, say, we start by applying Lemma 3.3. First we have for any partition λ of r,

$$\sum_{p\in\mathcal{P}(r)\cap[1,L]} \frac{|\Omega_{\lambda,p}|}{|\mathbf{F}_p^s|} \geqslant \sum_{p\in\mathcal{P}(r)\cap(r,L]} \frac{|\Omega_{\lambda,p}|}{|\mathbf{F}_p^s|} = T(\lambda)\Big(|\mathcal{P}(r)\cap(r,L]|\Big) + O_r\Big(\sum_{p\leqslant L}\frac{1}{\sqrt{p}}\Big),$$

where, in the error term, the sum extends to primes up to L. Moreover, summation by parts yields the following upper bound:

$$\sum_{p\leqslant L}\frac{1}{\sqrt{p}} \leqslant \frac{\sqrt{L}}{\log L}.$$

Let $\boldsymbol{\lambda}$ be a finite set of partitions of r and let $T(\boldsymbol{\lambda}) = \sum_{\lambda\in\boldsymbol{\lambda}} T(\lambda)$. By Proposition 3.2 we deduce, invoking the Prime Number Theorem (which implies $|\mathcal{P}(r)\cap(r,L]| \gg L/\log L$ since $L \geqslant r^2$), that we have for some constant $C_r > 0$ depending only on r and as soon as $\sqrt{L} > \max(r, C_r/T(\boldsymbol{\lambda}))$,

$$H(L,\boldsymbol{\lambda})^{-1} \gg T(\boldsymbol{\lambda})|\mathcal{P}(r)\cap(r,L]| - C_r\frac{\sqrt{L}}{\log L} \gg T(\boldsymbol{\lambda})\frac{L}{\log L}\Big(1-\frac{C_r}{T(\boldsymbol{\lambda})\sqrt{L}}\Big),$$

with absolute implied constants. In turn we obtain

$$|S(N,\boldsymbol{\lambda},L)| \ll (\sqrt{2N+1}+L)^{2s}\cdot(T(\boldsymbol{\lambda}))^{-1}\frac{\log L}{L}\Big(1-\frac{C_r}{T(\boldsymbol{\lambda})\sqrt{L}}\Big)^{-1}.$$

Now for $N \gg \max(T(\boldsymbol{\lambda})^{-2}r^4, T(\boldsymbol{\lambda})^{-3}C_r^4)$, we choose $L = T(\boldsymbol{\lambda})\sqrt{2N+1}$. We obtain

$$|S(N,\boldsymbol{\lambda},L)| \ll T(\boldsymbol{\lambda})^{-2}(1+T(\boldsymbol{\lambda}))^{2s}N^{s-\frac{1}{2}}\log N. \tag{6}$$

To conclude we follow the end of the proof of [28, Th. 4.2] by invoking [17, Lemma p. 98]: no proper transitive subgroup of $\mathfrak{S}_r$ contains both a transposition and a q-cycle of prime length $q > r/2$. Therefore it is enough to consider the following families of factorization patterns:

- λ_{irr} the trivial partition $(a_1,\dots,a_r)$ of r with $a_r = 1$, which detects the transitivity of the Galois action,
- $\boldsymbol{\lambda}_{\mathrm{tr}}$ the set of partitions $(a_1,\dots,a_r)$ of r satisfying $a_2 = 1$ and $a_{2i} = 0$ for $i \neq 1$, which detects an element of the Galois group acting as a transposition,
- $\boldsymbol{\lambda}_{\mathrm{prime}}$ the set of partitions $(a_1,\dots,a_r)$ of r with $a_q = 1$ for some prime number $q > r/2$, which detects an element of the Galois group acting as a q-cycle.

One has $T(\lambda_{\mathrm{irr}}) = r^{-1}$ and the asymptotics ([17, p. 99]):

$$T(\boldsymbol{\lambda}_{\mathrm{tr}}) \sim \frac{\log 2}{\log r}, \qquad T(\boldsymbol{\lambda}_{\mathrm{prime}}) \sim \frac{1}{\sqrt{2\pi r}} \qquad (r\to\infty).$$

In particular $\max(T(\lambda_{\mathrm{irr}})^{-2}, T(\boldsymbol{\lambda}_{\mathrm{tr}})^{-2}, T(\boldsymbol{\lambda}_{\mathrm{prime}})^{-2}) \ll r^2$. Combining this with (5) and (6) the proof is complete. □

3.2. **Application to linear combinations of Tutte polynomials of connected matroids.** We restrict to the case $s = 2$: let $T_{M_1}(x, y)$ and $T_{M_2}(x, y)$ be distinct Tutte polynomials of connected matroids M_1, M_2 of rank $r \geqslant 2$ and size $n \geqslant r + 1$. By Corollary 2.7 (originally [33] in this case) T_{M_1} and T_{M_2} are irreducible in $\mathbf{Z}[x, y]$. The fact that T_{M_1} and T_{M_2} are distinct is equivalent to their $\mathbf{Q}$-linear independence. From [19, §5] the conditions $r \geqslant 2$ and $n \geqslant r+1$ guarantee that the dimension of the $\mathbf{Q}$-span of Tutte polynomials of connected matroids of size n and rank r is at least 2 and therefore one can indeed pick two linearly independent Tutte polynomials of connected matroids of size n and rank r. Consequently T_{M_1} and T_{M_2} are distinct irreducible elements of $\mathbf{Z}[x, y]$. We will state and prove the main result of this section (Theorem 3.1) in the more general setting where we only require that T_1 and T_2 be copime squarefree in $\mathbf{Z}[x, y]$ and monic of the same degree as x-polynomials with coefficients in $\mathbf{Z}[y]$.

We start by establishing the following result explaining that suitable specializations of T_1 and T_2 at integral values of y yield triples (F_0, F_1, F_2) satisfying assumptions (H1) and (H2) of §3.1.

Proposition 3.4. *Let $r \in \mathbf{N}_{\geqslant 2}$ and let $T_1(x, y)$ and $T_2(x, y)$ be elements of $\mathbf{Z}[x, y]$ that are coprime, squarefree, and monic of the same degree r seen as x-polynomials with coefficients in $\mathbf{Z}[y]$. For big enough $t \in \mathbf{Z}$ (depending only on (T_1, T_2)) there exists a constant $C(T_1, T_2, t)$ (depending only on (T_1, T_2, t)) so that for every prime $p \geqslant C(T_1, T_2, t)$ the polynomials $T_{1,p}(x, t_p)$ and $T_{2,p}(x, t_p)$ are squarefree and coprime (where $t_p = t \bmod p$ and, for any $g \in \mathbf{Z}[x, y]$, we define g_p to be the element of $\mathbf{F}_p[x, y]$ obtained by reducing the coefficients of g modulo p). Moreover, setting*

$$F_1(x, y) = T_1(x, y)\,, \qquad F_2(x, y) = T_1(x, y) - T_2(x, y)\,, \qquad F_0(x, y) = xF_2(x, y),$$

then for every $p \geqslant C(T_1, T_2, t)$, the triple $(F_{i,p}(x, t_p))_{0\leqslant i\leqslant 2}$ satisfies assumptions (H1) and (H2) of §3.1.

Proof. We consider $P(x, y) = T_1(x, y)T_2(x, y)$, the product of T_1 and T_2. Since T_1 and T_2 are distinct and irreducible in the UFD $\mathbf{Z}[x, y]$, the polynomial $P(x, y)$ is squarefree in $\mathbf{Z}[x, y]$ (and also in $(\mathbf{Q}(y))[x]$) and so its x-discriminant (an element of $\mathbf{Z}[y]$) is non zero. Therefore for big enough $t \in \mathbf{Z}$ (depending only on (T_1, T_2)), the specialization $P(x, t)$ is squarefree; in other words $T_1(x, t)$ and $T_2(x, t)$ are coprime and squarefree. For every such t the discriminant of the x-polynomial $T_1(x, t)T_2(x, t)$ is non zero and therefore for every big enough prime p (depending only on (T_1, T_2, t)), this discriminant is non zero modulo p, meaning that $T_{1,p}(x, t_p)$ and $T_{2,p}(x, t_p)$ are squarefree and coprime.

Below we will write $F_{i,p}$ as shorthand for $F_{i,p}(x, t_p)$ $(0 \leqslant i \leqslant 2)$ for brevity. We can now check that assumptions (H1) and (H2) are satisfied by the relevant triples $(F_{i,p})_{0\leqslant i\leqslant 2}$.

(H1) Since $T_{1,p}(x, t_p)$ and $T_{2,p}(x, t_p)$ are coprime, then $\gcd(F_{1,p}, F_{2,p}) = 1$ and therefore $(F_{i,p})_{0\leqslant i\leqslant 2}$ is a family of relatively prime polynomials.

Let us check that the linear independence assumption is satisfied. Since $F_{1,p}$ and $F_{2,p}$ are coprime, they are not colinear. Assume by contradiction that for some $\alpha, \beta \in \mathbf{F}_p$ one has

$$F_{0,p} = \alpha F_{1,p} + \beta F_{2,p}.$$

Recombining, we obtain

$$(x - (\alpha + \beta))T_{1,p}(x, t_p) = (x - \beta)T_{2,p}(x, t_p).$$

This contradicts the fact that $T_{1,p}(x,t_p)$ and $T_{2,p}(x,t_p)$ are coprime, squarefree, and have degree $r \geqslant 2$.

(H2) We first check the *normality* assumption. For any $(\beta_0,\beta_1) \in \mathbf{F}_p^2$, we have

$$\begin{aligned}\gcd(F_{0,p}-\beta_0F_{2,p}, F_{1,p}-\beta_1F_{2,p}) &= \gcd((x-\beta_0)F_{2,p}, F_{1,p}-\beta_1F_{2,p})\\ &= \gcd(x-\beta_0, F_{1,p}-\beta_1F_{2,p}),\end{aligned}$$

where, for the last step, we use the fact that $F_{2,p}$ and $F_{1,p}$ are coprime. This implies that the gcd considered is normal.

Finally, assume by contradiction that $(F_{i,p})_{0\leqslant i\leqslant 2}$ is totally composite, then in particular there exists polynomials g_0 and g_2 in $\mathbf{F}_p[x]$ and a rational function $\psi \in \mathbf{F}_p[x]$ of positive degree such that

$$F_{0,p} = xF_{2,p} = D^\ell g_0(\psi)\,, \qquad F_{2,p} = D^\ell g_2(\psi).$$

This leads to

$$x = (h\circ\psi)(x)$$

where $h = g_0/g_2$. Taking degrees, we obtain $1 = (\deg h)(\deg\psi)$. However both factors on the right hand side are integers and $\deg\psi \geqslant 2$ by assumption; a contradiction.

□

We are now ready to draw the following consequence of Theorem 3.1 and Proposition 3.4. This establishes in particular that, generically degree one $\mathbf{Z}[x]$-linear combinations of two linearly independent Tutte polynomials of connected (n,r)-matroids have maximal Galois group over $\mathbf{Q}(y)$.

Theorem 3.5. *Let $T_1(x,y)$ and $T_2(x,y)$ be elements of $\mathbf{Z}[x,y]$ that are coprime, squarefree, and monic of the same degree $r \geqslant 2$ seen as x-polynomials with coefficients in $\mathbf{Z}[y]$ (for example one can take $T_1(x,y)$ and $T_2(x,y)$ to be distinct Tutte polynomials of connected (n,r)-matroids with $r \geqslant 2$ and $n \geqslant r+1$). Then one has*

$$\frac{\Big|\big\{(n_1,n_2)\in\{-N,\dots,N\}^2 \colon |G_{\mathbf{Q},y}\big((x+n_1)T_1-(x+n_2)T_2\big)|<r!\big\}\Big|}{(2N+1)^2} \ll r^2\frac{\log N}{\sqrt{N}},$$

for all $N \gg_r 1$ and with an absolute implied constant.

Proof. As in Proposition 3.4 set $F_0(x,y) = x(T_1(x,y)-T_2(x,y))$, $F_1(x,y) = T_1(x,y)$, and $F_2(x,y) = T_1(x,y)-T_2(x,y)$. Picking t big enough (again in the sense of Proposition 3.4) the assumptions of Theorem 3.1 (with $s=2$) are satisfied for the choice $\mathcal{P}(r) = \{p \text{ prime}\colon p \geqslant \max(C(T_1,T_2,t), r+1)\}$ which depends on (T_1,T_2,t) only and has density 1. We conclude by applying Theorem 3.1 and a specialization argument (Proposition 4.1, where one additionally notes that if $f(x,y)\in\mathbf{Z}[x,y]$ has x-degree d and if $t,p\in\mathbf{Z}$ are such that p is prime and $f(x,t) \bmod p$ is irreducible of degree d in $\mathbf{F}_p[x]$, then $f(x,y)$ is irreducible seen as an x-polynomial with coefficients in $\mathbf{Q}(y)$). □

4. Monodromy computations for some ranked sets and specific families of 2-connected graphs

In this section we first consider possible extensions of Conjecture 1.1 to general ranked sets, and next we prove that the conjecture holds for some families of connected matroids.

4.1. **Examples of monodromy group of Tutte polynomials of ranked sets.** In order to prove that Conjecture 1.1 holds in a number of cases, we will use the same strategy as for the proof of Theorem 3.1 by showing that the Galois group considered, seen as a permutation group, contains elements having a certain cycle type. Typically the final step of the proof relies on a classical specialization argument (also used in the proof of Theorem 3.1). We state the version, restricted to a UFD, of [4, Prop. 4], itself a simplified form of [29, VII, Th. 2.9]).

Proposition 4.1. *Let R be a UFD equipped with a ring homomorphism $\psi\colon R \to L$ to a field L. Let $f(X) \in R[X]$ be monic irreducible and assume that $\psi(f)$ (the element of $L[X]$ obtained by mapping ψ to the coefficients of f) is separable. Then $\mathrm{Gal}_L(\psi(f))$ is a subgroup of $\mathrm{Gal}_k(f)$, where k denotes the field of fractions of R.*

Remark 3. Let K/k be an algebraic field extension. Let $T(x,y) \in k[x,y]$ be squarefree and non constant as an x-polynomial with coefficients in $k[y]$. Fix an algebraic closure $\overline{K(y)}$ of $K(y)$; this is also an algebraic closure of $k(y)$. Let $(\alpha_i)_{1\leqslant i\leqslant r}$ be the roots of T in $\overline{K(y)}$. Then $k(y)((\alpha_i)_i)$ (resp. $K(y)((\alpha_i)_i)$) is a splitting field of T over $k(y)$ (resp. $K(y)$) and one has an injective group morphism

$$\begin{array}{ccc} \mathrm{Gal}_{K(y)}(T) & \longrightarrow & \mathrm{Gal}_{k(y)}(T) \\ \sigma & \longmapsto & \sigma_{|k(y)((\alpha_i)_i)}. \end{array}$$

As a consequence the maximality of $\mathrm{Gal}_{K(y)}(T)$ (meaning it has order $r!$) implies the maximality of $\mathrm{Gal}_{k(y)}(T)$. Moreover, if K/k has finite degree, then $\mathrm{Gal}_{k(y)}(T) \simeq \mathrm{Gal}_{K(y)}(T)$. Therefore, in the sequel, even though we fix, at times, the field of constants that we work over (*e.g.* $\mathbf{Q}$ or $\mathbf{C}$), one should keep in mind that under the above assumptions the statements still hold after a finite constant field extension or by considering a subfield over which the base field is algebraic.

In the remainder of §4.1, we give examples showing that Conjecture 1.1 extends to some but not all general rank functions.

Remark 4. To give a first low degree example in the case $R = \mathbf{Z}$, we go back to the first example in Remark 2. Specializing the Tutte polynomial $T_S(x,y) = x^3 + 2x^2 + y^2 + 3xy$ (see [22, p. 23]) at $y = 1$ and reducing modulo 5, we obtain the product of irreducibles $(x+1)(x^2+3)$ in $\mathbf{F}_5[x]$. We deduce that the Galois group of $T_S(x,y)$ over $\mathbf{Q}(y)$ is isomorphic to $\mathfrak{S}_3$ (up to isomorphism, it is the unique transitive permutation group of degree 3 that contains a transposition).

The first example below corresponds to a rank function assuming 2 values only. In this case the Galois group is not maximal (generically it has index $\geqslant 3$ inside the relevant symmetric group). The second example corresponds to a rank function assuming 3 values. In this case we exhibit subfamilies for which we show that the Galois group is maximal.

4.1.1. *A rank function assuming two values.* Example 1 gives an example of a rank function whose dual takes negative values, and whose corank-nullity polynomial is the polynomial

$$T_{n,r}(x,y) = (y-1)^{n-r} + (y^n - (y-1)^n)(x-1)^r,$$

where $n \geqslant r \geqslant 1$. Let R be a UFD and let $\varphi\colon \mathbf{Z} \to R$ be the natural ring homomorphism the kernel of which is generated by the characteristic of R. Applying φ to the coefficients, we consider the polynomial T as an element of $R[x, y]$. We let k be the fraction field of R.

Proposition 4.2. *As a polynomial in x, $T_{n,r}(x, y)$ is irreducible over $k(y)$. Assuming moreover that the characteristic of R does not divide r, the Galois group $G_{k,y}(T_{n,r})$ has order at most $r\varphi(r)$. If $r \geqslant 4$, then the index of $G_{k,y}(T_{n,r})$ in $\mathfrak{S}_r$ is at least 3. In particular $G_{k,y}(T_{n,r})$ is neither isomorphic to $\mathfrak{S}_r$ nor to $\mathfrak{A}_r$ as soon as $r \geqslant 4$.*

Proof. By invariance of the Galois group structure (and in particular reducibility properties) when factoring out a non-zero constant term, taking the reciprocal or performing linear transformations, we can replace $T_{n,r}(x, y)$ by

$$U_{n,r}(x, y) = x^r - \frac{(y-1)^n - y^n}{(y-1)^{n-r}}.$$

The polynomial $U_{n,r}$ has coefficients in $k(y)$ and its constant term is not a constant multiple of any $g(y)^\ell$ for some $g(y) \in k(y)$ and $\ell \in \mathbf{N}_{\geqslant 2}$. Indeed the numerator of such a $g(y)^\ell$ has multiple roots, which is not the case for $(y-1)^n - y^n$ as one checks by computing the y-derivative. Applying [29, Chap. 6, Th. 9.1], we deduce that $U_{n,r}$ is irreducible over $k(y)$.

Furthermore [29, Chap. 6, §9, Ex. 2] constructs, under the stated assumptions, an injective morphism from $G_{k,y}(U_{n,r})$ to

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : b \in \mathbf{Z}/r\mathbf{Z},\ a \in (\mathbf{Z}/r\mathbf{Z})^\times \right\},$$

which concludes the proof. □

4.1.2. *A rank function assuming three values.* The ranked set of Example 2 has corank-nullity polynomial equal to

$$T_n(x, y) = (x-1)^n + (x-1)^{n-1}\left(\frac{y^n - 1 - (y-1)^n}{y-1}\right) + 1,$$

where $n \geqslant 1$.

Setting $X = x - 1$ we obtain

$$T_n(X, y) = X^n + \left(\frac{y^n - 1 - (y-1)^n}{y-1}\right) X^{n-1} + 1.$$

For a suitable factorization of n, the following statement asserts the maximality of the Galois group of T_n over $\mathbf{Q}(y)$.

Proposition 4.3. *Let $n = p_1 p_2$ be the product of two odd primes such that the (multiplicative) order of 2 modulo p_i does not divide $p_j - 1$ (for any $i \neq j$). Then the Galois group of the splitting field of $T_n(X, 2)$ over $\mathbf{Q}$ is isomorphic to $\mathfrak{S}_n$ and therefore $G_{\mathbf{Q},y}(T_n(x, y)) \simeq \mathfrak{S}_n$.*

Proof. First note that

$$T_n(X, 2) = X^n + (2^n - 2)X^{n-1} + 1.$$

By assumption, one has $n \geqslant 15$ and therefore [23, Th. 1] implies that $T_n(X, 2)$ is irreducible over $\mathbf{Q}$. In particular $T_n(X, y)$ is irreducible over $\mathbf{Q}(y)$.

Moreover $\gcd(n, 2^n - 2) = 1$. Indeed, for $\{i, j\} = \{1, 2\}$, one has

$$2^n - 2 = (2^{p_i})^{p_j} - 2 \equiv 2(2^{p_j - 1} - 1) \not\equiv 0 \bmod p_i,$$

since the order of 2 modulo p_i does not divide $p_j - 1$, by assumption. We conclude that the Galois group of the splitting field of $T_n(X, 2)$ over $\mathbf{Q}$ is isomorphic to $\mathfrak{S}_n$ by invoking [37, Th. 1]. We finish the proof by applying Proposition 4.1. □

From Proposition 4.3 we can deduce that there are infinitely many values of n for which the Tutte polynomial of the ranked set in Example 2 has maximal Galois group over $\mathbf{Q}(y)$. The following statement gives a strong form of this fact.

Corollary 4.4. *For large enough $t \geqslant 2$, one has the following lower bound (that holds with an absolute implied constant):*

$$\#\{n \leqslant t \colon G_{\mathbf{Q},y}(T_n(x,y)) \simeq \mathfrak{S}_n\} \gg \frac{t^{0.16}}{\log t}.$$

Proof. By Proposition 4.3, a lower bound for the quantity investigated is

$$\#\{n = p_1 p_2 \leqslant t \colon \mathrm{ord}_{p_i}(2) \nmid (p_j - 1) \text{ for } \{i,j\} = \{1,2\}\}, \tag{7}$$

where p_1, p_2 are odd prime numbers and $\mathrm{ord}_{p_i}(2)$ denotes the multiplicative order of 2 modulo p_i. Modulo a prime at least 5, we know that 2 cannot have order 2. Also, by Fermat, $\mathrm{ord}_{p_i}(2) \mid (p_i - 1)$ for any odd prime p_i, and therefore (7) is bounded from below by

$$\#\{n = p_1 p_2 \leqslant t \colon p_i \neq 3\,, p_i \equiv 3 \bmod (4),\ (i = 1, 2),\ \gcd(p_1 - 1, p_2 - 1) = 2\}.$$

We rewrite this quantity as follows:

$$\sum_{\substack{7 \leqslant p_1 \leqslant t \\ p_1 \equiv 3 \bmod 4}} \#\{7 \leqslant p_2 \leqslant t/p_1 \colon p_2 \not\equiv 1 \bmod q \text{ if } q = 4 \text{ or } q \mid (p_1 - 1),\ q \text{ odd prime}\}. \tag{8}$$

To estimate the general term of this sum we need to count, for given p_1, the prime numbers p_2 that are less than t/p_1 and satisfy a linear system of type $\{p_2 \equiv a_i \bmod q_i,\ \forall i \in \{0, \ldots, r\}\}$ where $q_0 = 4$, $q_1, \ldots, q_r$ are the distinct odd prime divisors of $p_1 - 1$ and a_i is an invertible class distinct from 1 modulo q_i for $i \geqslant 1$. By the Chinese Remainder Theorem each such system is equivalent to a single congruence $p_2 \equiv a \bmod (q_0 \cdots q_r)$. One knows [45, Th. 1.1] that there exists a prime number $p_2 \ll (q_1 \cdots q_r)^{5.18}$ satisfying such a congruence (with an absolute effectively computable implied constant). This means that if one restricts the sum in (8) to primes $p_1 \leqslant t^{1/6.2}$, for big enough t, then there is a suitable prime $p_2 \leqslant t/p_1$. In particular the sum (8) is bounded from below, for big enough t, by

$$\pi(t^{1/6.2}; 4, 3),$$

the count of prime numbers that are 3 modulo 4 and less than $t^{1/6.2}$. We conclude by invoking the Prime Number Theorem in arithmetic progressions and the fact that $1/6.2 \simeq 0.1613$. □

In the rest of Section 4, we prove that Conjecture 1.1 holds for several families of 2-connected graphs. In some cases we do not prove the full force of the maximality result predicted by the conjecture but we obtain information about the Galois action that goes beyond the transitivity granted by our irreducibility statement (Corollary 2.7).

4.2. **The case of an n-cycle.** Let $n \geqslant 3$ and let C_n be the cycle on n vertices, a 2-connected graph (the associated matroid is connected) with Tutte polynomial given by

$$T_{C_n}(x,y) = \sum_{i=1}^{n-1} x^i + y.$$

In this section, we prove the conjecture of Bohn–Cameron–Müller for the graphic matroid associated with the n-cycle C_n where $n \geqslant 3$.

Theorem 4.5. *Let $n \geqslant 3$ and let k be a field of characteristic 0 or $p \nmid n(n-1)$. We have $G_{k,y}(T_{C_n}) \simeq \mathfrak{S}_{n-1}$. In particular Conjecture 1.1 holds for C_n.*

Below we give a proof valid over any field satisfying the assumptions of the statement. For the case $k = \mathbf{Q}$ (and therefore, over any number field by Remark 3) we will derive an independent proof as a consequence of Lemma 4.10. Before proving Theorem 4.5 we consider a slight modification of T_{C_n} better suited for computing its Galois group over $k(y)$ with k as in the statement of Theorem 4.5.

Lemma 4.6. *For n and k as in Theorem 4.5, let $p(x) = (x^n - 1)/(x-1) \in k[x]$. Then, setting $P(x,y) = p(x) - y$, we have $G_{k,y}(P) \simeq \mathfrak{S}_{n-1}$.*

Proof of Lemma 4.6. We present the argument given by N. Elkies [14]. It uses a result that goes back to Hilbert ([39, Th. 4.4.1]) under the generalized form proved in Serre's book [39, Th. 4.4.5] and which asserts the following. Let $f \in k[x]$ be of degree d, and suppose the roots $x_1, \ldots, x_{d-1}$ of the derivative f' are pairwise distinct and that the images $y_j := f(x_j)$ are also pairwise distinct (*i.e.* f is a so-called *Morse function*), then the Galois group of $f(x) - y$ over $k(y)$ is isomorphic to $\mathfrak{S}_d$.

To see that this holds for $p(x)$ as in the statement, note that the discriminant of $p(x) - y$ with respect to x has precisely the y_j's as roots (this is seen *e.g.* by using the defining formula for the discriminant which is, up to sign, the resultant of a polynomial and its derivative). In fact the computation

$$\frac{\mathrm{d}}{\mathrm{d}x}\big((x-1)(p(x)-y)\big) = (p(x)-y) + (x-1)p'(x)$$

shows that $(x-1)(p(x)-y)$ and its x-derivative have a common root if and only if y is one of the y_j's, or $y = n$ (in the latter case the common root is $x_0 = 1$). Thus if one wants to detect multiplicities in the y_j's by using the formula for the discriminant of a trinomial (see *e.g.* [41, Th. 2])

$$\mathrm{disc}_x((x-1)(p(x)-y)) = \mathrm{disc}_x(x^n - yx - 1 + y) = \pm((n-1)^{n-1}y^n - n^n(y-1)^{n-1}),$$

one first has to divide this y-polynomial by the highest power of $(y-n)$ that it is a multiple of. One easily sees that this maximal power is $(y-n)^2$ and we deduce that the roots of

$$q(y) := \frac{(n-1)^{n-1}y^n - n^n(y-1)^{n-1}}{(y-n)^2}$$

are the y_j's counted with multiplicity. To finish the proof one computes the discriminant of the polynomial q and checks that it does not vanish. Elkies computes ([14]) this discriminant and shows that, up to sign, it equals $2\Delta_n\Delta_{n-1}$ (here, for any positive integer m we define $\Delta_m = m^{(m-1)(m-3)}$) which is non zero by our assumption on the characteristic of k. □

Proof of Theorem 4.5. In the notation of Lemma 4.6, one has $P(x,1-y)=T_{C_n}(x,y)$ and therefore we deduce that $G_{k,1-y}(P)=G_{k,y}(T_{C_n})\simeq\mathfrak{S}_{n-1}$ since $k(y)=k(1-y)$. □

4.3. **The case of uniform matroids.** Let $U_{a,b}$ be the uniform matroid, which is defined on groundset $\{1,\dots,b\}$ and has bases all subsets of size a: the rank of $A\subseteq\{1,\dots,b\}$ is equal to $|A|$ if $|A|\leqslant a$ and equal to a if $a<|A|\leqslant b$. The Tutte polynomial of $U_{a,b}$ is then given by

$$T_{U_{a,b}}(x,y)=\sum_{i=0}^{a}\binom{b}{i}(x-1)^{a-i}+\sum_{j=a+1}^{b}\binom{b}{j}(y-1)^{j-a}.$$

Assume further that $0<a<b$, for which $U_{a,b}$ is connected (Brylawski [5, Cor. 7.14] showed that the coefficient of x in $T_{U_{a,b}}(x,y)$ is equal to $\binom{b-2}{a-1}$).

Theorem 4.7. *Assume $a\geqslant 2$.*

(1) *One has $G_{\mathbf{Q},y}(T_{U_{a,b}})\simeq\mathfrak{S}_a$ if b is big enough in terms of a.*
(2) *If $b=a+p$ for some prime number $p>a$ then $G_{\mathbf{Q},y}(T_{U_{a,b}})$ acts as a primitive permutation group on the roots of $T_{U_{a,b}}$ in a fixed algebraic closure of $\mathbf{Q}(y)$. If in addition a is composite, then the action of $G_{\mathbf{Q},y}(T_{U_{a,b}})$ is doubly transitive.*

Remark 5. The reason why the second statement of Theorem 4.7 is included in addition to the first one is because of uniformity issues. As we explain in the proof below, Theorem 4.7(1) is quite directly deduced from work of Filaseta and Moy [16] (recently complemented by Klahn and Technau [27]), however no explicit growth rate for b as a function of a is made explicit in [16, 27] and it does not seem clear how to extract this information from their approach. Celebrated results (see *e.g* [11, Chap. 4 and §7.7]) in group theory show that primitivity (and all the more so for, double transitivity) is not a property shared by many subgroups of the symmetric group.

Proof of Theorem 4.7. (1) We note that

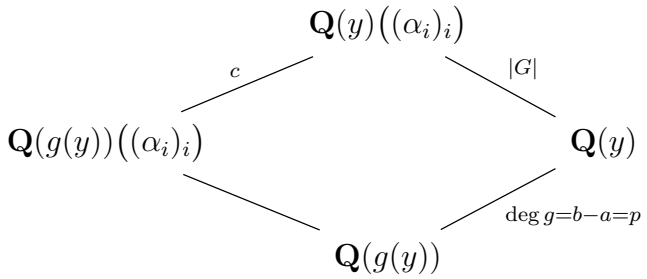
$$q^{\star}_{a,b}(x-1):=T_{U_{a,b}}(x,1)=\sum_{i=0}^{a}\binom{b}{i}(x-1)^{a-i}.$$

This polynomial is the reciprocal evaluated at $x-1$ of the polynomial denoted $q_{a,b}(x)$ in [16, p. 295]. For fixed $a\geqslant 2$, one can apply [16, Theorem 1] (complemented, for $a=6$, by [27, Th. 2]) which asserts that for big enough b (as a function of a), the Galois group of $q_{a,b}(x-1)$ over $\mathbf{Q}$ is isomorphic to $\mathfrak{S}_a$. The same holds for $q^{\star}_{a,b}(x)$, and we conclude by Proposition 4.1.

(2) Let $\alpha_1,\dots,\alpha_a$ be the roots of $T_{U_{a,b}}$ in an algebraic closure of $\mathbf{Q}(y)$. By definition $G_{\mathbf{Q},y}(T_{U_{a,b}})\simeq\mathrm{Gal}(\mathbf{Q}(y)((\alpha_i)_i)/\mathbf{Q}(y))$. For simplicity this group will be denoted G and we will write

$$f(x):=\sum_{i=0}^{a}\binom{b}{i}(x-1)^{a-i},\qquad g(y):=\sum_{j=a+1}^{b}\binom{b}{j}(y-1)^{j-a},$$

so that $T_{U_{a,b}}(x,y) = f(x) + g(y)$. The following diagram summarizes the situation.



Let $K = \mathbf{Q}(y)$, $K_g = \mathbf{Q}(g(y))$ and $c = [K((\alpha_i)_i) : K_g(\alpha_i)_i]$. The fact that $[K : K_g] = \deg g$ comes from [9, Prop. 7.5.5, p. 176] since g is non constant. The extension $K_g((\alpha_i)_i)/K_g$ is Galois since $K_g((\alpha_i)_i)$ is a splitting field of $T_{U_{a,b}}$ over K_g. Let H denote its Galois group. As easily seen in the above diagram, $c \cdot |H| = |G| \cdot \deg g$.

Any automorphism of $K((\alpha_i)_i)$ fixing K restricts to an automorphism of $K_g((\alpha_i)_i)$ fixing K_g (indeed, g has rational coefficients). This induces an injective group morphism $G \hookrightarrow H$.

Since g is a non constant polynomial with rational coefficients, one has $H \simeq \mathrm{Gal}_{\mathbf{Q}(Y)}(f(x)+Y)$, where Y is an indeterminate over $\mathbf{Q}$ and the Galois group is understood as that of the splitting field of $f(x) + Y$ over $\mathbf{Q}(Y)$. We invoke a result of Dujella, Gusić and Tichy [12, Cor. 1], that asserts that the polynomial with integer coefficients

$$f(x+1) = x^a + bx^{a-1} + \cdots$$

is indecomposable (meaning that if $f = f_1 \circ f_2$ for some integral polynomials f_1, f_2 then either f_1 or f_2 has degree 1; note also that regarding $f(x+1)$ as an element of $\mathbf{Z}[x]$ or $\mathbf{Q}[x]$ does not affect indecomposability, by [42, Cor. 2.3]) since, by assumption, b is coprime to a. In turn the polynomial f is indecomposable and by virtue of [42, Lem. 3.1], the group H acts as a primitive permutation group on the roots (seen in a fixed algebraic closure $\overline{\mathbf{Q}(Y)}$ of $\mathbf{Q}(Y)$) of the x-polynomial $f(x) + Y$. In case a is composite, we can further combine [42, Lem. 3.3, Lem. 4.4]. The former statement guarantees that H contains an a-cycle while the latter infers that in this case a composite implies that H is doubly transitive as a permutation group of the roots in $\overline{\mathbf{Q}(Y)}$ of the x-polynomial $f(x) + Y$.

Finally we prove that $G \simeq H$. It relies on the following classical property of the compositum of a field extension with a Galois extension (see *e.g.* [13, §14.4]).

Lemma 4.8. *Let Ω/k be a field extension and let L and M be subextensions such that L/k is finite Galois. Then the compositum LM (inside Ω) is finite Galois over M and* $\mathrm{Gal}(LM/M) \simeq \mathrm{Gal}(L/(L \cap M))$.

In order to apply the lemma to our situation, note that $K((\alpha_i)_i))$ is the compositum of K and $K_g((\alpha_i)_i)$ (inside $\overline{\mathbf{Q}(y)}$). The lemma implies that

$$G = \mathrm{Gal}(K\big((\alpha_i)_i\big)/K) \simeq \mathrm{Gal}\left(K_g\big((\alpha_i)_i\big)/(K \cap K_g\big((\alpha_i)_i\big))\right).$$

However $K \cap K_g\big((\alpha_i)_i\big)$ is a subextension of K/K_g which, by assumption, has prime degree. Therefore $K \cap K_g\big((\alpha_i)_i\big)$ is either K or K_g. By contradiction, assume that this intersection is K; then we have a tower $K_g\big((\alpha_i)_i\big)/K/K_g$ which would imply that $p \mid [K_g\big((\alpha_i)_i\big) : K_g]$.

This is impossible by our assumption on p and since $[K_g((\alpha_i)_i) : K_g] \leqslant a!$. We conclude that $K \cap K_g((\alpha_i)_i) = K_g$ and in turn that $G \simeq H$, since $K_g((\alpha_i)_i)/K_g$ is Galois of group isomorphic to H.

□

Remark 6. Note that [42, Lem. 3.3], used in the proof to derive double transitivity from primitivity in the case where a is composite, is a property specific to bivariate polynomials (it holds at least for polynomials of the form $f(x) - y$). In particular, contrary to many other arguments used in the present work, such a strong group-theoretic property on the Galois action is not established by a specialization argument. We will argue in the same way, using an approach specific to bivariate polynomials, in the next section when proving Theorem 4.5 over number fields. Monodromy groups of type $\mathrm{Gal}_{\mathbf{C}(y)}(f(x)-y)$ where $f \in \mathbf{Q}[x]$ is indecomposable have been classified [36]. Also note that similar monodromy computations are performed in [26, §7] in the context of curves over finite fields with defining equation of type $y^a = f(x)$.

4.4. **The case of an n-cycle with a "thick edge".**

Definition 4. Let $n, j \geqslant 1$ be integers. We define C_n^j to be the multigraph obtained from a path of length $n-1$ with endpoints u and v by adding j edges joining u and v in parallel.

Thus $C_n^1 = C_n$, the cycle of length n, and C_n^j has $n + j - 1$ edges and rank $n - 1$. The graph C_n^0 is P_n, the path on n vertices; the graph C_2^0 consists of a single bridge.

Using the deletion-contraction recurrence for the Tutte polynomial (*e.g.* [21, Th. 3.1]), a straightforward induction gives, for $n \geqslant 2$,

$$T(C_n^j; x, y) = x^{n-1} + (y + x + \cdots + x^{n-2}) \cdot (1 + y + \cdots + y^{j-1}). \tag{9}$$

The multigraph C_2^j consists of $j+1$ parallel edges joining two vertices, for which $T(C_2^j; x, y) = x + y + \cdots + y^j$, consistent with (9) with $n = 2$. The multigraph C_1^j consists of j loops on a vertex, and $T(C_1^j; x, y) = y^j$.

4.4.1. *The case where j is odd.* We prove the following extra case of Conjecture 1.1. One of the main ingredients here is specializing $T(C_n^j; x, y)$ at $y = -1$. Since $j \equiv 1 \bmod 2$ one has for $n \geqslant 2$

$$T(C_n^j; x, -1) = x^{n-1} + x^{n-2} + \cdots + x - 1. \tag{10}$$

Theorem 4.9. *Let $k/\mathbf{Q}$ be a finite field extension. Assume that $n \geqslant 3$ and that j is odd. We have:*

1. *the group $G_{k,y}(T(C_n^j; x, y))$ is isomorphic to a transitive subgroup of $\mathfrak{S}_{n-1}$ that contains a transposition;*
2. *assuming that n is odd, $G_{k,y}(T(C_n^j; x, y)) \simeq \mathfrak{S}_{n-1}$;*
3. *if $n-1$ is prime, then $G_{k,y}(T(C_n^j; x, y)) \simeq \mathfrak{S}_{n-1}$; in fact $\mathrm{Gal}_{\mathbf{Q}}(T(C_n^j; x, -1)) \simeq \mathfrak{S}_{n-1}$.*

As we will see in the proof, (3) of the statement is deduced from [32, Th. 3.4]. Recall also that Remark 3 explains why it is enough to prove the statement in the case $k = \mathbf{Q}$. We first state a preparatory result, and proceed by drawing a second proof of Theorem 4.5 in the case where k is a number field.

Lemma 4.10. *Let $n \in \mathbf{N}_{\geqslant 2}$ and let $f(x) = x^{n-1} + x^{n-2} + \cdots + x - 1 \in \mathbf{Z}[x]$. Let G_f denote the Galois group of a splitting field of f over $\mathbf{Q}$. Then the following hold:*

(1) *f is irreducible over $\mathbf{Q}$;*
(2) *if $n \geqslant 3$, then the discriminant of the polynomial f has an odd prime divisor (in other words, $|\operatorname{disc}(f)|$ is not a power of 2);*
(3) *if p is an odd prime divisor of $|\operatorname{disc}(f)|$ then the inertia subgroup at p (defined up to conjugation and seen as a permutation subgroup of the complex roots of f) is generated by a transposition, and*
(4) *assuming that n is odd, we have $G_f \simeq \mathfrak{S}_{n-1}$.*

Before proving the Lemma, we use it to give a second proof of Theorem 4.5 in the case where k is a number field (which reduces to the case $k = \mathbf{Q}$ by Remark 3).

Alternative proof of Theorem 4.5 for $k = \mathbf{Q}$. As mentioned after Definition 4 the case of an n-cycle corresponds to $j = 1$. Recall also that Corollary 2.7 guarantees that T_{C_n} is irreducible seen as an x-polynomial with coefficients in $\mathbf{Q}(y)$. Therefore, combining (10) with Proposition 4.1 and Lemma 4.10(2) and (3), the Galois group $\mathrm{Gal}_{\mathbf{Q}(y)}(T_{C_n})$ is isomorphic to a transitive subgroup of $\mathfrak{S}_{n-1}$ containing a transposition. Moreover, as mentioned in Remark 6, we may combine [12, Cor. 1] and [42, Lem. 3.1] to show that this Galois group acts as a primitive permutation group of degree $n-1$. A primitive permutation group of degree $n-1$ containing a transposition is necessarily isomorphic to $\mathfrak{S}_{n-1}$ (see [11, Th. 3.3A]). □

Proof of Lemma 4.10. For (1), we first set

$$g(x) = (x-1)f(x) = (x-1)\cdot\left(\frac{x^n-1}{x-1} - 2\right) = x^n - 2(x-1) - 1 = x^n - 2x + 1.$$

We then apply a result due to Perron (see *e.g.* [38, Th. 2]) asserting that $f(x)$ (*i.e.* the quotient of $g(x)$ by $x-1$) is irreducible over $\mathbf{Q}$.

Next we prove (2). Fix $n \geqslant 3$. The discriminant D of g is given by ([41, Th. 2]):

$$D = (-1)^{n(n-1)/2}\big(n^n - (n-1)^{n-1}2^n\big). \tag{11}$$

Moreover, recalling the definition of the discriminant of a polynomial in terms of the resultant of the polynomial and its derivative ([29, Chap. IV, Prop. 8.3 and 8.5]), we have:

$$\begin{aligned} D = (-1)^{\frac{n(n-1)}{2}}\operatorname{Res}(g,g') &= (-1)^{\frac{n(n-1)}{2}}\prod_{\alpha \text{ root of } g} g'(\alpha) \\ &= (-1)^{\frac{n(n-1)}{2}} f(1)\prod_{\alpha \text{ root of } f} f'(\alpha)\prod_{\alpha \text{ root of } f}(\alpha-1) \\ &= (-1)^{\deg f + \frac{n(n-1)}{2}}(f(1))^2\prod_{\alpha \text{ root of } f} f'(\alpha) = (f(1))^2\operatorname{disc}(f). \end{aligned} \tag{12}$$

Since $f(1) = n-2$, we obtain:

$$|\operatorname{disc}(f)| = \frac{|n^n - (n-1)^{n-1}2^n|}{(n-2)^2}.$$

If n is odd then the right hand side is odd as well and we are done[6]. Let us assume that $n = 2k'$ ($k' \geqslant 2$). Then, up to sign, we have

$$|\operatorname{disc}(f)| = \frac{|(2k')^{2k'} - (2k'-1)^{2k'-1}2^{2k'}|}{4(k'-1)^2} = 2^{2(k'-1)}\frac{|k'^{2k'} - (2k'-1)^{2k'-1}|}{(k'-1)^2}$$

If k' is even, then the right-most factor is odd[7] and we are done. Therefore we assume that $n = 2(2k+1)$ (*i.e.* $k' = 2k+1$) for some $k \geqslant 1$. We get

$$|\operatorname{disc}(f)| = 2^{4k}\frac{|(2k+1)^{2(2k+1)} - (4k+1)^{4k+1}|}{4k^2}$$

Let us investigate the parity of the second factor. By Newton's formula:

$$(2k+1)^{2(2k+1)} = \sum_{j=0}^{4k+2}\binom{4k+2}{j}(2k)^j, \qquad (4k+1)^{4k+1} = \sum_{i=0}^{4k+1}\binom{4k+1}{i}(4k)^i.$$

The contributions of the indices $i = j = 0$ are both 1. They subtract to 0. Moreover we see that the contributions of the indices:

(i) $j = 1$ and $i = 1$ are respectively $(2k+1)4k$ and $(4k+1)4k$. The difference subtracts to an integer divisible by $8k^2$.

(ii) $j = 2$ and $i = 2$ are respectively $4k^2(2k+1)(4k+1)$ and $16k^2 2k(4k+1)$ and the difference of these two terms is divisible par $4k^2 = 2^{2\ell+2}$ but not $8k^2$ since $(2k+1)(4k+1)$ is odd.

(iii) $j \geqslant 3$ and $i \geqslant 3$ are integers divisible by $8k^2$.

We conclude that

$$\frac{|(2k+1)^{2(2k+1)} - (4k+1)^{4k+1}|}{4k^2} \equiv |(4k+1)(2k+1-8k)| \equiv 1 \bmod 2. \tag{13}$$

Therefore, $|\operatorname{disc}(f)|$ admits an odd prime divisor as soon as the left-hand side of (13) is not equal to 1. We claim that indeed one has

$$(4k+1)^{4k+1} - (2k+1)^{2(2k+1)} > 4k^2.$$

Notice first that the inequality is true if $k \in \{1, 2\}$ by direct computation and suppose now that $k \geqslant 3$. It is enough to prove that

$$\frac{(4k+1)^{4k+1}}{(2k+1)^{4k+2}} > (4k+1)^2,$$

that is

$$\left(\frac{4k+1}{2k+1}\right)^{4k-1} > (2k+1)^3.$$

Taking the logarithm on both sides, we see that it suffices that

$$(4k-1)\ln(13/7) > 3\ln(2k+1),$$

[6]Note that $\operatorname{disc}(f) \neq \pm 1$ because f is irreducible and has degree > 1 and thus generates a ramified extension of the rationals.

[7]Here we note that the numerator of the fraction of the right-most member is $\geqslant k'^{2k'-1}$ for $k' \geqslant 2$ and therefore the fraction cannot be 1.

because $x \mapsto \frac{4x+1}{2x+1} = 1 + \frac{2x}{2x+1}$ is increasing as a function of x and we assumed that $k \geqslant 3$. This last inequality holds for all $k \geqslant 3$ as can be seen by a quick analysis of the function $x \mapsto (4x-1)\ln(13/7) - 3\ln(2x+1)$ for $x > 1$. We have proved that $|\operatorname{disc}(f)|$ is not a power of 2.

We turn to (3). Our method mimics the argument of Osada [37, Proof of Th. 1].

Let K be the splitting field (inside the complex numbers) of f (equivalently, of g) over $\mathbf{Q}$. Let p be a prime number ramified in $K/\mathbf{Q}$ and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying over p. We let $I(\mathfrak{p}/p)$ denote the inertia subgroup of G_f relative to p and $\mathfrak{p}$. Let σ be a non trivial element of $I(\mathfrak{p}/p)$; thus $\sigma(\alpha) \neq \alpha$ for some root α of f. Since $\sigma \in I(\mathfrak{p}/p)$, we have $\sigma(\alpha) \equiv \alpha (\mathrm{mod}\ \mathfrak{p})$, meaning that $\alpha \bmod \mathfrak{p}$ is a multiple root of the reduction of f modulo p. In particular $g(\mathrm{mod}\ p) \in \mathbf{F}_p[x]$ has a multiple root. Let us show that $g(\mathrm{mod}\ p)$ has at most one multiple root, and that in this case, its multiplicity is 2. We will deduce that for any root $\beta \in K$ of f, the necessary congruence $\sigma(\beta) \equiv \beta (\mathrm{mod}\ \mathfrak{p})$ implies $\sigma(\beta) = \beta$ and thus σ, seen as a permutation of the roots of f is the transposition, $(\alpha\sigma(\alpha))$.

Let r be a multiple root of $f(x)$ modulo some odd prime p ramified in $K/\mathbf{Q}$. It is also a multiple root of $g(x) = x^n - 2x + 1$, seen as an element of $\mathbf{F}_p[x]$. Then $r^n = 2r - 1$ and r is also a root of the derivative $nx^{n-1} - 2$ of g. Thus $nr^n = 2r$. In particular $p \nmid n$: indeed, by contradiction, if $p \mid n$, then $nr^n = 2r = 0$ which would imply $p = 2$ since $r \neq 0$. This contradicts the fact that p is odd. Hence $2r - 1 = 2r/n$ and in turn $2r(1 - 1/n) = 1$. In particular $p \nmid n - 1$. We conclude that $r = n/(2(n-1))$ is the only possible multiple root of $x^n - 2x + 1 \in \mathbf{F}_p[x]$. Finally the second derivative of g is $n(n-1)x^{n-2}$ which only vanishes at 0 (recall $p \nmid n$ and $p \nmid n - 1$). Thus r has mulitplicity < 3 as a root of g.

Finally we prove (4). Since $n \geqslant 2$ and n is odd, we have $n \geqslant 3$. First remark that the Galois group G_f of f over $\mathbf{Q}$ is the same as the Galois group of g over $\mathbf{Q}$. By (1), the group G_f is a transitive subgroup of $\mathfrak{S}_{n-1}$. By [37, Lemma 5], it suffices to show that G_f (seen as a subgroup of $\mathfrak{S}_{n-1}$) can be generated by transpositions to conclude that $G_f \simeq \mathfrak{S}_{n-1}$. To do so, we use the fact that G_f is generated by the union over prime numbers p of the inertia subgroups of G_f at p (a consequence of Galois theory combined with the fact that no non-trivial extension of $k = \mathbf{Q}$ is unramified).

Note that f does not have a multiple root modulo 2. Indeed, assume by contradiction that r is such a root; it is a multiple root of g and by the same computation as the one performed in the proof of (3), we have:

$$r^n = 2r - 1 = 1\,, \qquad nr^{n-1} = 0.$$

These two equalities are not compatible, since n is odd. This implies that all the ramified primes in the splitting field of f over $\mathbf{Q}$ are odd and by (3) all the non trivial inertia subgroups of G_f are generated by a transposition. This concludes the proof. □

We are now ready to prove Theorem 4.9; our argument combines Lemma 4.10 and Proposition 4.1.

Proof of Theorem 4.9. We first prove (1). Recall (10) and apply Proposition 4.1 for the choice $R = k[y]$, $f(x) = T(C_n^j; x, y)$ (irreducible over R by Corollary 2.7, and monic as a polynomial with coefficients in $k[y]$) and where the ring homomorphism we choose is reduction modulo $y + 1$. The image of the polynomial $T(C_n^j; x, y)$ by such a morphism is the $\mathbf{Q}$-polynomial on the right hand side of (10). We conclude by combining Lemma 4.10(1), (2) and (3).

The proof of (2) follows from the same specialization argument (Proposition 4.1) as in the proof of (1), combined this time with Lemma 4.10(4).

Finally we prove (3). This is deduced from [32, Th. 3.4] which asserts that the polynomial $T(C^j_{p+1}; x, -1)$ is irreducible modulo $p := n-1$. Let $h(x) = x^p - \sum_{i=0}^{p-1} x^i$. Note that for odd j, this is the opposite of the reciprocal of $T(C^j_{p+1}; x, -1)$ (see (10)). We further denote by $h_p(x) = x^p - \sum_{i=0}^{p-1} x^i \in \mathbf{F}_p[x]$ the reduction of h modulo p. It is enough to prove that h_p is irreducible to deduce the result. Indeed by virtue of (11) and (12) the prime p does not divide the discriminant of f (recall that a polynomial with non zero constant coefficient and its reciprocal have, up to sign and a power of the constant coefficient, the same discriminant), therefore if h_p is irreducible, the Galois group of h over $\mathbf{Q}$ contains a p-cycle and is a subgroup of $\mathfrak{S}_p$. It is therefore a transitive permutation group of prime degree, hence it is a primitive permutation group. Since it also contains a transposition (by Lemma 4.10(2) and (3)), we conclude that $\mathrm{Gal}_{\mathbf{Q}}(h) \simeq \mathfrak{S}_p$ by [11, Th. 3.3A]. Finally we apply once more Proposition 4.1. □

4.4.2. *Case $n-1 \in \{p, p^2\}$ and $-j$ nonsquare mod p.* We prove that Conjecture 1.1 holds for $T(C^j_n; x, y)$ for extra values of n and j. This time we proceed by specializing the Tutte polynomial at $y = 1$:

$$T(C^j_n; x, 1) =: h(x) = x^{n-1} + j \sum_{k=0}^{n-2} x^k.$$

Theorem 4.11. *Let $k/\mathbf{Q}$ be a finite field extension. If*

(1) *$n-1 \in \{p, p^2\}$ for some prime number $p \geqslant 5$,*
(2) *$-j$ is a nonsquare modulo p, and*
(3) *$\gcd(n, j-1) = 1$,*

then $G_{k,y}(T(C^j_n; x, y)) \simeq \mathfrak{S}_{n-1}$.

As before, it is enough, by Remark 3 to consider the case $k = \mathbf{Q}$. We will need the following preparatory result.

Lemma 4.12. *Let $a, b \in \mathbf{Q}$ and let $m > k > 0$ be integers such that $\gcd(m, k) = 1$. Consider the trinomial $f(x) = x^m + ax^k + b \in \mathbf{Q}[x]$. Let $h(x) \in \mathbf{Z}[x]$ be an irreducible factor of $f(x)$ and assume that*

(i) *D_f/D_h is a square in $\mathbf{Z}$ (here D_g denotes the discriminant of any $g \in \mathbf{Q}[x]$);*
(ii) *there exists a prime number p such that $v_p(D_f)$ (the p-adic valuation of D_f) is odd and $p \nmid ab$.*

Then the Galois group $\mathrm{Gal}_{\mathbf{Q}}(f)$ of the splitting field of f (seen as a permutation subgroup of the complex roots of f) over $\mathbf{Q}$ contains a transposition.

Proof. We use [41, Th. 2] to compute:

$$D_f = (-1)^{m(m-1)/2} b^{k-1} \big(m^m b^{m-k} + (-1)^{m+1} (m-k)^{m-k} k^k a^m \big).$$

Let θ be a complex root of h and denote by $d_{\mathbf{Q}(\theta)}$ the discriminant of the number field $\mathbf{Q}(\theta)$, then $D_h/d_{\mathbf{Q}(\theta)}$ is a square in $\mathbf{Z}$ (the square of the index of $\mathbf{Z}[\theta]$ in the ring of integers of K). By assumption (i), we deduce that $D_f/d_{\mathbf{Q}(\theta)} = (D_f/D_h) \cdot (D_h/d_{\mathbf{Q}(\theta)})$ is a square in $\mathbf{Z}$.

We deduce that if p is a prime number satisfying (ii) then p is ramified in $\mathbf{Q}(\theta)/\mathbf{Q}$ (*i.e.* it divides $d_{\mathbf{Q}(\theta)}$). Moreover, applying [35, Lemma 5] (which builds on [31, Th. 2]), the inertia

subgroup relative to any prime ideal $\mathfrak{p}$ above p in the splitting field K_h of h over $\mathbf{Q}$ is generated by a transposition. In turn $\mathrm{Gal}_{\mathbf{Q}}(f)$ contains a transposition. □

Our goal is to apply the above Lemma to the specialization $h(x)$ at $y=1$ of $T(C_n^j;x,y)$. Then $f(x)=(x-1)h(x)$ is a trinomial to which the Lemma can be applied if

(a) h is irreducible,

(b) one can find a prime p such that $v_p(D_f)$ is odd and $p\nmid j(j-1)$ (see the proof of Theorem 4.11 below).

To see that condition (a) holds we invoke [23, Th. 2] asserting the irreducibility in $\mathbf{Q}[x]$ of $T(C_n^j;x,1)$ for $j>1$.

Lemma 4.13 (Harrington)**.** *Assume $n\geqslant 2$. The specialization at $y=1$ of $T(C_n^j;x,y)$ is the $\mathbf{Q}$-polynomial:*

$$h(x)=x^{n-1}+j\sum_{k=0}^{n-2}x^k.$$

If $j>1$, then $h(x)$ is irreducible over $\mathbf{Q}$ except if $(n,j)=(3,4)$.

Proof of Theorem 4.11. Recall that $G=G_{\mathbf{Q},y}(T(C_n^j;x,y))$ seen as a permutation group is a transitive subgroup of $\mathfrak{S}_{n-1}$ by virtue of Corollary 2.7.

Next let us show that G contains a transposition. Let $h(x)$ be the specialization of $T(C_n^j;x,y)$ at $y=1$ and define $f(x):=(x-1)h(x)=x^n+(j-1)x^{n-1}-j$. Then, as shown in the proof of 4.10(2), the number D_f/D_h is a square in $\mathbf{Z}$. Furthermore, as seen in the proof of Lemma 4.12, one has

$$D_f=(-1)^{n(n-1)/2}(-j)^{n-1}D_0 \text{ where } D_0=(-j)n^n+(-1)^{n-1}(n-1)^{n-1}(j-1)^n.$$

We note that $D_0\equiv -j \bmod (n-1)$, therefore D_0 is a non-square modulo p. In particular D_0 is not a square in $\mathbf{Z}$. Let ℓ be a prime such that $v_\ell(D_0)$ is odd. Then $\ell\nmid j-1$, otherwise ℓ would divide either n or j contradicting the assumption $\gcd(n,j-1)=1$.

Also note that j is coprime to D_0 (in particular $\ell\nmid j$). Indeed a common prime divisor of j and D_0 would divide $n-1$ and so that prime divisor would be p. We would obtain $j\equiv 0 \bmod p$ which contradicts the fact that $-j$ is a nonsquare modulo p. Therefore D is a non-square in $\mathbf{Z}$.

Therefore since $v_\ell(D_f)=v_\ell(D_0)$ is odd and $\ell\nmid j(j-1)$ Lemma 4.12 applies and shows that $\mathrm{Gal}_{\mathbf{Q}}(f)$ seen as a permutation group of the complex roots of f contains a transposition. In particular G contains a transposition.

Finally we want to prove that G is a primitive subgroup of $\mathfrak{S}_{n-1}$, which is now enough to conclude by [11, Th. 3.3A]. The proof of primitivity is provided by Proposition 4.14 below.

In order to see that the assumptions of Proposition 4.14 are satisfied for $h(x)=T(C_n^j;x,1)$, we appeal to Lemma 4.13 and we set $\phi(x):=(x-1)h(x)=x^n+(j-1)x^{n-1}-j$ and so, in the notation of Proposition 4.14, one has $k=n$, $s=n-1$, $a=j-1$ and $b=-j$. One cheks that $\gcd((j-1)(n-1),-jn)=1$ since $(n-1)$ (resp. $j-1$) is coprime to both n and $-j$. □

Proposition 4.14. *Let $\phi(x)=x^k+ax^s+b\in\mathbf{Z}[x]$ for integers $k\geqslant 3$ and $s\in\{1,\dots,k-1\}$.*

Assume that $\gcd(as(k-s),kb)=1$ and $s\in\{p,p^2\}$ for some prime number p. If $\phi(x)=(x-\alpha)h(x)$ for some $\alpha\in\mathbf{Z}$ and an irreducible $h\in\mathbf{Z}[x]$, then the Galois group of the splitting field of ϕ over $\mathbf{Q}$ acts as a primitive permutation group on the set of complex roots of h.

Proof. The setting and the proof are slightly adapted from work [35] of Movahhedi–Salinier. Letting G_ϕ be the Galois group of the splitting inside $\mathbf{C}$ of ϕ over $\mathbf{Q}$, the assumptions imply that G_ϕ is isomorphic to a transitive subgroup of $\mathfrak{S}_{k-1}$. Moreover using a computation similar to (12) one has

$$\mathrm{disc}(\phi) = h(\alpha)^2 \mathrm{disc}(h)$$

and thus the analysis of [35, §2, §3] applies and we conclude by invoking [35, Cor. 1 to Th. 3]. □

Acknowledgements

F. Jouve benefited from the financial support of the ANR through project ETIENE (ANR-24-CE93-0016) and is grateful to its members for valuable remarks and comments after some of the above results were presented on the occasion of the first project meeting held in Jussieu in June 2025. A. Goodall was partially supported by the Czech Science Foundation (GAČR) grant 25-16627S.

References

[1] C. Beke, G. K. Csáji, P. Csikvári, and S. Pituk, *Short proof of a theorem of Brylawski on the coefficients of the Tutte polynomial*, European Journal of Combinatorics **110** (2023), 4.
[2] ———, *Permutation Tutte polynomial*, European Journal of Combinatorics **120** (2024), 28.
[3] M. Bhargava, *Galois groups of random integer polynomials and van der Waerden's Conjecture*, Ann. of Math. (2) **201** (2025), no. 2, 339–377.
[4] A. Bohn, P. J. Cameron, and P. Müller, *Galois groups of multivariate Tutte polynomials*, J. Algebraic Combin. **36** (2012), no. 2, 223–230.
[5] T. H. Brylawski, *A decomposition for combinatorial geometries*, Trans. Amer. Math. Soc. **171** (1972), 235–282.
[6] T. H. Brylawski and J. Oxley, *The Tutte polynomial and its applications*, Matroid applications, 1992, pp. 123–225.
[7] P. J. Cameron and K. Morgan, *Algebraic properties of chromatic roots*, Electron. J. Combin. **24** (2017), no. 1, Paper No. 1.21, 14.
[8] S. D. Cohen, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc. (2) **6** (1972), 93–102.
[9] D. A. Cox, *Galois theory*, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2012.
[10] H. H. Crapo, *A higher invariant for matroids*, J. Combinatorial Theory **2** (1967), 406–417.
[11] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer, Cham, 1996.
[12] A. Dujella, I. Gusić, and R. F. Tichy, *On the indecomposability of polynomials*, Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II **214** (2005), 81–88 (2006).
[13] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed., 2004.
[14] N. D. Elkies, *A family of polynomials with symmetric Galois group*, MathOverflow. URL: https://mathoverflow.net/q/75367 (version: 2011-10-01).
[15] J. A. Ellis-Monaghan, A. J. Goodall, I. Moffatt, S. D. Noble, and L. Vena, *Irreducibility of the Tutte polynomial of an embedded graph*, Algebr. Comb. **5** (2022), no. 6, 1337–1351.
[16] M. Filaseta and R. Moy, *On the Galois group over $\mathbb{Q}$ of a truncated binomial expansion*, Colloq. Math. **154** (2018), no. 2, 295–308.
[17] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), Proc. Sympos. Pure Math., vol. Vol. XXIV, Amer. Math. Soc., Providence, RI, 1973, pp. 91–101.
[18] S. Gao, *Absolute irreducibility of polynomials via Newton polytopes*, Journal of Algebra **237** (2001), no. 2, 501–520.

[19] A. J. Goodall, F. Jouve, and J.-S. Sereni, *Vector spaces spanned by Tutte polynomials*, preprint, available at https://hal.science/hal-04485620v1/.
[20] G. Gordon, *A β invariant for greedoids and antimatroids*, Electron. J. Combin. **4** (1997), no. 1, Research Paper 13, 13.
[21] ———, *On Brylawski's generalized duality*, Mathematics in Computer Science **6** (2012), no. 2, 135–146.
[22] ———, *Linear relations for a generalized Tutte polynomial*, Electron. J. Combin. **22** (2015), no. 1, Paper 1.79, 30.
[23] J. Harrington, *On the factorization of the trinomials $x^n + cx^{n-1} + d$*, Int. J. Number Theory **8** (2012), no. 6, 1513–1518.
[24] J. Harris, *Galois groups of enumerative problems*, Duke Math. J. **46** (1979), no. 4, 685–724.
[25] M. N. Huxley, *The large sieve inequality for algebraic number fields*, Mathematika **15** (1968), 178–187.
[26] N. M. Katz and Y. Nakayama, *Strange congruences*, preprint, available at https://web.math.princeton.edu/~nmk/KN8ter.pdf.
[27] B. Klahn and M. Technau, *Galois groups of $\binom{n}{0} + \binom{n}{1}X + \cdots + \binom{n}{6}X^6$*, International Journal of Number Theory **19** (2023), no. 10, 2443–2450.
[28] E. Kowalski, *The large sieve and its applications*, Cambridge Tracts in Mathematics, vol. 175, Cambridge University Press, Cambridge, 2008. Arithmetic geometry, random walks and discrete groups.
[29] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.
[30] A. Leykin and F. Sottile, *Galois groups of Schubert problems via homotopy computation*, Math. Comp. **78** (2009), no. 267, 1749–1765.
[31] P. Llorente, E. Nart, and N. Vila, *Discriminants of number fields defined by trinomials*, Acta Arith. **43** (1984), no. 4, 367–373.
[32] P. A. Martin, *The Galois group of $x^n - x^{n-1} - \cdots - x - 1$*, J. Pure Appl. Algebra **190** (2004), no. 1-3, 213–223.
[33] C. Merino, A. de Mier, and M. Noy, *Irreducibility of the Tutte polynomial of a connected matroid*, J. Combin. Theory Ser. B **83** (2001), no. 2, 298–304.
[34] K. Morgan, *Galois groups of chromatic polynomials*, LMS J. Comput. Math. **15** (2012), 281–307.
[35] A. Movahhedi and A. Salinier, *The primitivity of the Galois group of a trinomial*, J. London Math. Soc. (2) **53** (1996), no. 3, 433–440.
[36] P. Müller, *Primitive monodromy groups of polynomials*, Recent developments in the inverse Galois problem (Seattle, WA, 1993), Contemp. Math., vol. 186, Amer. Math. Soc., Providence, RI, 1995, pp. 385–401.
[37] H. Osada, *The Galois groups of the polynomials $X^n + aX^l + b$*, J. Number Theory **25** (1987), no. 2, 230–238.
[38] E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. **4** (1956), 287–302.
[39] J.-P. Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Damon; With a foreword by Darmon and the author.
[40] F. Sottile and J. White, *Double transitivity of Galois groups in Schubert calculus of Grassmannians*, Algebr. Geom. **2** (2015), no. 4, 422–445.
[41] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.
[42] G. Turnwald, *On Schur's conjecture*, J. Austral. Math. Soc. Ser. A **58** (1995), no. 3, 312–357.
[43] W. T. Tutte, *Connectivity in matroids*, Canadian J. Math. **18** (1966), 1301–1324.
[44] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatsh. Math. Phys. **43** (1936), no. 1, 133–147.
[45] T. Xylouris, *On the least prime in an arithmetic progression and estimates for the zeros of Dirichlet L-functions*, Acta Arith. **150** (2011), no. 1, 65–91.

Computer Science Institute (IÚUK), Faculty of Mathematics and Physics, Charles University, Malostranské nám. 25, 118 00 Praha 1, Czech Republic. andrew@iuuk.mff.cuni.cz

Université de Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France. florent.jouve@math.u-bordeaux.fr

Service public français de la recherche, Centre National de la Recherche Scientifique (ICube, CSTB), Strasbourg, France. jean-sebastien.sereni@cnrs.fr