J Algebr Comb (2014) 39:141–152
DOI 10.1007/s10801-013-0442-0

# On the evaluation at $(-\iota, \iota)$ of the Tutte polynomial of a binary matroid

**R.A. Pendavingh**

Received: 6 March 2012 / Accepted: 29 March 2013 / Published online: 20 April 2013

**Abstract** Vertigan has shown that if $M$ is a binary matroid, then $|T_M(-\iota, \iota)|$, the modulus of the Tutte polynomial of $M$ as evaluated in $(-\iota, \iota)$, can be expressed in terms of the bicycle dimension of $M$. In this paper, we describe how the argument of the complex number $T_M(-\iota, \iota)$ depends on a certain $\mathbb{Z}/4\mathbb{Z}$-valued quadratic form that is canonically associated with $M$. We show how to evaluate $T_M(-\iota, \iota)$ in polynomial time, as well as the canonical tripartition of $M$ and further related invariants.

**Keywords** Matroid · Binary matroid · Tutte polynomial · Computational complexity

## 1 Introduction

The *Tutte polynomial* of a matroid $M = (E, \mathcal{I})$ with rank function $r$ is

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

Extending the work of Jaeger, Vertigan, and Welsh [7], Vertigan investigates the complexity of $\tau^0(\mathcal{M}_{\mathbb{F}}, x, y)$, the problem of evaluating $T_M(x, y)$ given $x, y$ and a matroid $M$ that is linearly represented over $\mathbb{F}$ [14]. Let $\iota$ denote the imaginary unit, let $\omega := e^{\iota\frac{2\pi}{3}}$ denote a complex third root, and let $\mathbb{A}$ be the algebraic closure of $\mathbb{Q}$.

**Theorem 1** (Vertigan, 1998) *Let $\mathbb{F}$ be a finite field and $(x, y) \in \mathbb{A}^2$ be a pair other than $(0, 0)$, $(1, 1)$, and such that $(x-1)(y-1) \neq 1$. Then the problem $\tau^0(\mathcal{M}_{\mathbb{F}}, x, y)$ is #P-complete, except when*

(1) $|\mathbb{F}| = 2$, *and* $(x, y)$ *is one of* $(-1, -1)$, $(0, -1)$, $(-1, 0)$, $(\iota, -\iota)$, $(-\iota, \iota)$;

R.A. Pendavingh (✉)
Eindhoven Technical University, Den Dolech 2, 5600MB Eindhoven, The Netherlands
e-mail: rudi@win.tue.nl

(2) $|\mathbb{F}| = 3$, *and* $(x, y)$ *is one of* $(\omega, \omega^2)$, $(\omega^2, \omega)$; *or*
(3) $|\mathbb{F}| = 4$, *and* $(x, y)$ *is* $(-1, -1)$.

In the present paper we derive, for a binary matroid $M$, an explicit expression for $T_M(-\iota, \iota)$ that can be evaluated in polynomial time.

To the best of our knowledge, the complexity status of $\tau^0(\mathcal{M}_{\mathbb{F}}, 1, 1)$ is open. Otherwise, the above theorem is now complemented by explicit, polynomial-time computable expressions for the value of the Tutte polynomial on each of the special points:

(1) If $(x, y) = (0, 0)$ or if $(x - 1)(y - 1) = 1$, it is trivial to compute $T_M(x, y)$ for any matroid $M$;
(2) for binary matroids $M$, $|T_M(-\iota, \iota)|$ was determined by Vertigan [14]; below, we derive an explicit expression for $T_M(-\iota, \iota)$;
(3) for ternary matroids $M$, Jaeger [8] has determined $|T_M(\omega, \omega^2)|$, and Gioan and Las Vergnas [3] found $T_M(\omega, \omega^2)$;
(4) for quaternary matroids $M$, $T_M(-1, -1)$ was found by Vertigan [14], extending a result for graphic/binary matroids by Rosenstiehl and Read [12].

The original motivation for this research was a computational problem that arose when writing a matroid package for Sage [13]. Testing whether two matroids are isomorphic can be made more efficient in practice by comparing matroid invariants, avoiding more involved computation if the values of the invariants do not match. For general matroids, there are few such invariants that are polynomial-time computable. For binary, ternary, and quaternary matroids, however, the values of the Tutte polynomial in the above-mentioned special points are clearly the kind of isomorphism invariant we can use for this purpose. With this objective in mind, we shall prove that computing $T_M(-\iota, \iota)$ as well as several related invariants takes $O(r(M)^2|E|)$ time altogether.

## 2 Preliminaries

### 2.1 Matroids

We assume familiarity with matroid theory. In our use of matroid terminology we generally follow Oxley [10]. There, a linear matroid $M(A)$ on ground set $E$ is defined from a $k \times E$ matrix $A$. For the present purposes, it will be convenient to also define a linear matroid from a linear subspace, as follows.

If $E$ is a finite set, $\mathbb{F}$ is any field and $V$ is a linear subspace of $\mathbb{F}^E$, then $V$ determines a matroid $M(V)$ on $E$ with set of independent sets

$$\mathcal{I}(V) := \bigl\{F \subseteq E \mid \text{there is no } v \in V \text{ such that } \operatorname{supp}(v) \subseteq F\bigr\},$$

where $\operatorname{supp}(v) := \{e \in E \mid v_e \neq 0\}$. The relation to the standard definition of linear matroid is that if $A$ is a $k \times E$ matrix and $V = \ker(A)$, then $M(A) = M(V)$.

We will denote

$$V/e := \{v_{|E-e} \mid v \in V\},$$

so that $M(V/e) = M(V)/e$.

## 2.2 The bicycle dimension

Let $V$ be a linear subspace of $\mathbb{F}^E$, where $|\mathbb{F}|$ is one of $2, 3, 4$. The *bicycle dimension* of $V$ is defined by

$$d(V) := \dim\bigl(V \cap V^\perp\bigr).$$

Here $V^\perp := \{w \in \mathbb{F}^E \mid \langle w, v\rangle = 0 \text{ for all } v \in V\}$ as usual, where we take $\langle w, v\rangle := \sum_i w_i v_i$ if $\mathbb{F} = \mathrm{GF}(2)$ or $\mathrm{GF}(3)$ and $\langle w, v\rangle := \sum_i w_i^* v_i$ if $\mathbb{F} = \mathrm{GF}(4)$, where $^* : \mathrm{GF}(4) \to \mathrm{GF}(4)$ is the unique nontrivial field automorphism (i.e. $x^* = x^2$ for each $x \in \mathrm{GF}(4)$).

Vertigan [14] shows that if $V$ is a linear subspace of $\mathbb{F}^E$ and $|\mathbb{F}|$ is one of $2, 3, 4$, then $d(V)$ depends only on $M(V)$.

## 2.3 Quadratic forms

Let $V$ be a finite-dimensional linear space over a field $\mathbb{F}$. Let $b : V \times V \to \mathbb{F}$ be a bilinear form. Then $q : V \to \mathbb{F}$ is a *quadratic form associated with $b$* if

$$q(\lambda x + \mu y) = \lambda^2 q(x) + \mu^2 q(y) + \lambda\mu b(x, y)$$

for all $\lambda, \mu \in \mathbb{F}$ and $x, y \in V$.

A bilinear form is *non-degenerate* if there is no $w \in V$ such that $b(v, w) = 0$ for all $v \in V$. A quadratic form is *nonsingular* if the associated bilinear form is non-degenerate. A basis $v_1, \dots, v_k$ of $V$ is *orthogonal* with respect to $b$ if

$$b(v_i, v_j) = 0 \quad \text{if } i \neq j.$$

The following is well-known.

**Lemma 1** *If $b : V \times V \to \mathbb{F}$ is a non-degenerate bilinear form and the field $\mathbb{F}$ has characteristic other than 2, then there exists a basis of $V$ that is orthogonal with respect to $b$.*

Two quadratic forms $q, q'$ on $V$ are *isomorphic* if there is some linear bijection $L : V \to V$ such that $q(v) = q'(L(v))$ for all $v \in V$. If $v_1, \dots, v_k$ and $w_1, \dots, w_k$ are $b$-orthogonal bases of $V$ and $q$ is a quadratic form associated with $b$, then $\prod_i q(v_i)$ is a quadratic residue if and only if $\prod_i q(w_i)$ is a quadratic residue. Let $\chi(q)$ be 1 or $-1$ depending on whether the product is a quadratic residue or nonresidue.

**Theorem 2** *If $q, q'$ are nonsingular quadratic forms on $V$ over a field of characteristic other than 2, then $q$ is isomorphic to $q'$ if and only if $\chi(q) = \chi(q')$.*

The case when the characteristic is 2 is somewhat more involved. A basis $v_1, \dots, v_{2m}$ of $V$ is *alternating* with respect to $b$ if

$$b(v_i, v_j) = \begin{cases} 1 & \text{if } \{i, j\} = \{k, k+m\} \text{ for some } k \in \{1, \dots, m\}, \\ 0 & \text{otherwise.} \end{cases}$$

**Lemma 2** *If $b : V \times V \to \mathbb{F}$ is a non-degenerate bilinear form and the field $\mathbb{F}$ has characteristic* 2, *then exactly one of the following holds*:

(1) *$V$ has a basis that is orthogonal with respect to $b$*, *or*
(2) *$V$ has a basis that is alternating with respect to $b$.*

Brown [1] generalizes quadratic forms over GF(2) to $\mathbb{Z}/4\mathbb{Z}$-*valued quadratic forms* $q : V \mapsto \mathbb{Z}/4\mathbb{Z}$, satisfying

$$q(x+y) = q(x) + q(y) + \alpha\bigl(b(x,y)\bigr),$$

where $b : V \times V \mapsto \mathrm{GF}(2)$ is a bilinear mapping, and $\alpha : \mathrm{GF}(2) \to \mathbb{Z}/4\mathbb{Z}$ is the additive group homomorphism such that $\alpha(0) = 0$ and $\alpha(1) = 2$. Such a quadratic form $q$ is *non-degenerate* resp. *alternating* if and only if the associated bilinear function $b$ is.

Brown also defines an invariant $\sigma(q)$ such that

$$\sum_{x \in V} \iota^{q(x)} = \sqrt{2}^{\dim(V)} e^{\frac{\pi \iota \sigma(q)}{4}}. \tag{2}$$

Wood [15] has classified the $\mathbb{Z}/4\mathbb{Z}$-valued quadratic forms as follows:

**Theorem 3** (Wood, 1993) *If $q, q'$ are nonsingular $\mathbb{Z}/4\mathbb{Z}$-valued quadratic forms on $V$*, *then $q$ is isomorphic to $q'$ if and only if*

(1) $\sigma(q) = \sigma(q')$, *and*
(2) *$q$ is alternating $\Leftrightarrow$ $q'$ is alternating.*

## 3 A special point of the Tutte polynomial

### 3.1 Characterization of $T_M(-\iota, \iota)$

Let $V$ be a linear subspace of $\mathrm{GF}(2)^E$, and let $q_V : V \to \mathbb{Z}/4\mathbb{Z}$ be defined by

$$q_V(x) := \bigl|\mathrm{supp}(x)\bigr| \mod 4$$

for all $x \in V$. Then $q_V(x+y) = q_V(x) + q_V(y) + \alpha(b(x,y))$ taking $b(x,y) = \sum_i x_i y_i$, so that $q_V$ is a $\mathbb{Z}/4\mathbb{Z}$-valued quadratic form on $V$.

If $q_V(y) = 0$ for all $y \in V \cap V^\perp$, then for all $x \in V$ and all $y \in V \cap V^\perp$, we have

$$q_V(x+y) = q_V(x) + q_V(y) + \alpha\bigl(b(x,y)\bigr) = q_V(x)$$

and then we may define $\tilde{q}_V : V/(V \cap V^\perp) \to \mathrm{GF}(2)$ by setting

$$\tilde{q}_V\bigl(x + V \cap V^\perp\bigr) = q_V(x). \tag{3}$$

Then $\tilde{q}$ is nonsingular by construction.

We have arrived at the main result of this paper, a characterization of $T_M(-\iota, \iota)$ for binary matroids $M$ in terms of the bicycle dimension and Brown's invariant.

**Theorem 4** *Let $V$ be a linear subspace of* $\mathrm{GF}(2)^E$ *and let* $M := M(V)$. *Then*

$$T_M(-\iota, \iota) = e^{\frac{\pi\iota}{4}(\sigma(\tilde{q}_V)+|E|-3r(E))}\sqrt{2}^{d(V)} \tag{4}$$

*if* $q_V(x) = 0$ *for all* $x \in V \cap V^\perp$, *and* $T_M(-\iota, \iota) = 0$ *otherwise.*

*Proof* By an application of Greene's formula [5] (as in [14, p. 390]), we have

$$\sum_{x\in V} \iota^{q_V(x)} = \iota^{r(E)}(1-\iota)^{|E|-r(E)}T_M(-\iota, \iota).$$

Rewriting, we obtain

$$T_M(-\iota, \iota) = \sqrt{2}^{-|E|+r(E)} e^{\frac{\pi\iota}{4}(|E|-3r(E))} \sum_{x\in V} \iota^{q_V(x)}. \tag{5}$$

If $y \in V \cap V^\perp$, then $V = V + y$ and $b(x, y) = 0$ for all $x \in V$, so that $q_V(x + y) = q_V(x)$ for all $x \in V$. Hence if $q_V(y) = 2$ for such an $y \in V \cap V^\perp$, then

$$\sum_{x\in V} \iota^{q_V(x)} = \sum_{x\in V} \iota^{q_V(x+y)} = \iota^{q_V(y)} \sum_{x\in V} \iota^{q_V(x)} = -\sum_{x\in V} \iota^{q_V(x)}.$$

It follows that then $\sum_{x\in V} \iota^{q_V(x)} = 0$ and hence $T_M(-\iota, \iota) = 0$.

If on the other hand $q_V(x) = 0$ for all $x \in V \cap V^\perp$, then by (3) we have

$$\sum_{x\in V} \iota^{q_V(x)} = \sum_{w\in V\cap V^\perp} \sum_{v\in\tilde{V}} \iota^{q_V(v+w)} = \sum_{w\in V\cap V^\perp} \sum_{v\in\tilde{V}} \iota^{\tilde{q}_V(v+V\cap V^\perp)}$$

where $\tilde{V}$ is any subspace of $V$ so that $V = (V \cap V^\perp) \oplus \tilde{V}$. The summation over $V \cap V^\perp$ amounts to a factor $2^{d(V)}$, and using (2) on the non-degenerate form $\tilde{q}_V$ we obtain

$$\sum_{x\in V} \iota^{q_V(x)} = 2^{d(V)}\sqrt{2}^{\dim(\tilde{V})} e^{\frac{\pi\iota}{4}\sigma(\tilde{q}_V)}.$$

Substituting this expression in (5), and using

$$|E| - r(M) = \dim(V) = d(V) + \dim(\tilde{V}),$$

we obtain (4). □

For comparison, we state the characterization of $T(\omega, \omega^2)$ for ternary matroids due to Gioan and Las Vergnas [3] in similar terms. For a subspace $V \subseteq \mathrm{GF}(3)^E$, let $q_V : V \to \mathrm{GF}(3)$ be defined by

$$q_V : x \mapsto \left|\mathrm{supp}(x)\right| \mod 3,$$

and let $\tilde{q}_V : V/(V \cap V^\perp) \to \mathrm{GF}(3)$ be defined by $\tilde{q}_V(x + V \cap V^\perp) = q_V(x)$.

**Theorem 5** *Let $V \subseteq \mathrm{GF}(3)^E$ be a linear subspace and $M := M(V)$. Then*

$$T_M\bigl(\omega, \omega^2\bigr) = (-1)^{\frac{1-\chi(\tilde{q}_V)}{2}} \omega^{2|E|-r(M)} (\iota\sqrt{3})^{d(V)}.$$

### 3.2 Complexity of computing $T_M(-\iota, \iota)$

In what follows, let $V \subseteq \mathrm{GF}(2)^E$ be a linear subspace of dimension $k$. A *$q$-basis* is a basis $v_1, \ldots, v_k$ of $V$ such that

(1) $v_1, \ldots, v_{k-d(V)}$ is an orthogonal or alternating basis of some subspace $\tilde{V}$ such that $V = \tilde{V} \oplus (V \cap V^{\perp})$;
(2) $v_{k-d(V)+1}, \ldots, v_k$ is a basis of $V \cap V^{\perp}$; and
(3) $q_V(v_{k-d(V)+1}) = 0, \ldots, q_V(v_{k-1}) = 0$.

Standard linear algebra techniques yield:

**Lemma 3** *Given any basis of $V$, computing a $q$-basis takes $O(\mathrm{dim}(V)^2|E|)$ time.*

The following is straightforward from the definition of $q$-basis and (2).

**Lemma 4** *Let $v_1, \ldots, v_k$ be a $q$-basis of $V$. Then $q_V(v) = 0$ for all $v \in V \cap V^{\perp}$ if and only if $d(V) = 0$ or $q_V(v_k) = 0$. If so, then*

(1) *if $v_1, \ldots, v_{k-d(V)}$ is orthogonal, then*

$$\sigma(\tilde{q}_V) = \#\bigl\{i \mid q_V(v_i) = 1\bigr\} - \#\bigl\{i \mid q_V(v_i) = 3\bigr\} \mod 8,$$

*and*

(2) *if $v_1, \ldots, v_{k-d(V)}$ is alternating, then*

$$\sigma(\tilde{q}_V) = 4\#\bigl\{i \in \{1, \ldots, m\} \mid q_V(v_i) = q_V(v_{i+m})\bigr\} \mod 8,$$

*where $m = \frac{k-d(V)}{2}$.*

**Theorem 6** *Let $V \subseteq \mathrm{GF}(2)^E$ be a linear subspace. Given any basis of $V$, the evaluation of $T_{M(V)}(-\iota, \iota)$ takes $O(\mathrm{dim}(V)^2|E|)$ time.*

*Proof* To compute $T_{M(V)}(-\iota, \iota)$, it suffices to determine $|E|$, $\mathrm{rank}(M(V)) = |E| - \mathrm{dim}(V)$, whether $q_V(v) = 0$ for all $v \in V \cap V^{\perp}$, and if so, $\sigma(\tilde{q}_V)$. Given a $q$-basis of $V$, this takes in $O(\mathrm{dim}(V)|E|)$ time. □

As $\mathrm{dim}(V) = |E| - r(M(V)) = r^*(M(V))$, this amounts to a complexity bound of $O(r^*(M(V))^2|E|)$ for evaluating $T_{M(V)}(-\iota, \iota)$ from a basis of $V$. We note that as in general $T_M(x, y) = T_{M^*}(y, x) = \overline{T_{M^*}(\overline{y}, \overline{x})}$, we have

$$T_{M(V)}(-\iota, \iota) = \overline{T_{M(V^{\perp})}(-\iota, \iota)}.$$

We may determine the latter in $O(\mathrm{dim}(V^{\perp})^2|E|) = O(r(M(V))^2|E|)$ time from any basis of $V^{\perp}$.

### 3.3 Computing the canonical tripartition

Let $V \subseteq \mathrm{GF}(2)^E$. We consider

$$F_i := \{e \in E \mid d(V/e) = d(V) + i\}.$$

**Lemma 5** *Let $v_1, \dots, v_k$ be a $q$-basis of $V$. Then*

(1) $F_{-1} = \bigcup_{i=k-d(V)+1}^{k} \mathrm{supp}(v_i)$;
(2) $F_1 = \mathrm{supp}(\sum_{i=1}^{k-d(V)} v_i) \setminus F_{-1}$ *if the $q$-basis is orthogonal*, $F_1 = \emptyset$ *otherwise*; *and*
(3) $F_0 = E \setminus (F_{-1} \cup F_1)$.

*In particular*, $F_i = \emptyset$ *for any* $i \notin \{-1, 0, 1\}$.

In what follows, we write $A[X, Y]$ for the restriction of a matrix $A$ to the rows indexed by $X$ and the columns indexed by $Y$.

*Proof* Let $A$ be any $k \times E$ matrix over GF(2) such that $V = \mathrm{rowspace}(A)$. Then $V^\perp = \mathrm{kernel}(A)$, and $d(V) = \dim(V \cap V^\perp) = k - \mathrm{rank}(AA^T)$. If we write

$$A^e := A\bigl[\{1, \dots, k\}, E - e\bigr] \quad \text{and} \quad a^e := A\bigl[\{1, \dots, k\}, e\bigr]$$

for $e \in E$, then $V/e = \mathrm{rowspace}(A^e)$ and $d(V/e) = k - \mathrm{rank}(A^e(A^e)^T)$. Thus

$$d(V/e) - d(V) = \mathrm{rank}\bigl(AA^T\bigr) - \mathrm{rank}\bigl(AA^T + a^e\bigl(a^e\bigr)^T\bigr).$$

Now consider the matrix $A$ whose rows are the given $q$-basis of $V$.

If $e \in \mathrm{supp}(v_i)$ for some $i > k - d(V)$, so $a_i^e \neq 0$, then consider the matrix $B$ that arises by adding the $i$th row of $A$ to the rows $j \in \mathrm{supp}(a^e) - \{i\}$. Then the rows of $B$ again form a $q$-basis of $V$, $b^e$ is a unit vector, and hence $d(V/e) - d(V) = \mathrm{rank}(BB^T) - \mathrm{rank}(BB^T + b^e(b^e)^T) = -1$.

If $a_i^e = 0$ for all $i > k - d(V)$, then $d(V/e) - d(V) = \mathrm{rank}(AA^T) - \mathrm{rank}(AA^T + a^e(a^e)^T) = \mathrm{rank}(BB^T) - \mathrm{rank}(BB^T + b^e(b^e)^T)$ where $B = A[\{1, \dots, k - d(V)\}, E]$. So without loss of generality, we may assume $d(V) = 0$.

In case the rows of $A$ are orthogonal, let $B := A[\mathrm{supp}(a^e), E]$. Then $d(V/e) - d(V) = \mathrm{rank}(AA^T) - \mathrm{rank}(AA^T + a^e(a^e)^T) = \mathrm{rank}(BB^T) - \mathrm{rank}(BB^T + b^e(b^e)^T) = \mathrm{rank}(I) - \mathrm{rank}(I + J)$, where $J$ denotes the square all-one matrix with rows and columns indexed by $\mathrm{supp}(a^e)$. Then the rank of $I + J$ depends only on the parity of $|\mathrm{supp}(a^e)|$, and we have

$$d(V/e) - d(V) = \begin{cases} 1 & \text{if } |\mathrm{supp}(a^e)| \text{ is even,} \\ 0 & \text{otherwise.} \end{cases}$$

In case the rows of $A$ are alternating, it remains to show that $d(V/e) - d(V) = 0$, i.e. that $AA^T + a^e(a^e)^T$ is nonsingular. If not, there is a nonzero vector $x \in \mathrm{GF}(2)^k$

so that $(AA^T + a^e(a^e)^T)x = 0$, or equivalently, $AA^Tx = a^e(a^e)^Tx$. As $AA^Tx \neq 0$, we must have $(a^e)^Tx = 1$ and hence $AA^Tx = a^e$. As

$$AA^Tx = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix} x = (x_{k/2+1}, \dots, x_k, x_1, \dots, x_{k/2})^T,$$

this implies that $(a^e)^Tx = 0$, a contradiction. □

The triple $(F_{-1}, F_0, F_1)$ is known as the *canonical tripartition* of $V$. Originally this notion was developed for graphs by Rosenstiehl and Read [12], but the generalization to binary spaces is straightforward. As is clear from the lemma, the determination of the canonical tripartition takes $O(\dim(V)|E|)$ time given a $q$-basis of $V$.

### 3.4 A projection

We describe another invariant of subspaces $V \subseteq \mathrm{GF}(2)^E$. The description of this invariant is simpler in the case that $V \cap V^\perp$ is trivial. Therefore, we consider this more restricted setting first. Following Godsil and Royle [4], we call a subspace $V \subseteq \mathrm{GF}(2)^E$ *pedestrian* if the 'bicycle space' $V \cap V^\perp$ is trivial, i.e. if $d(V) = 0$.

Pedestrian spaces are not rare. Fixing a subspace $W \subseteq \mathrm{GF}(2)^E$ of dimension $k$, there are exactly $2^k$ distinct subspaces $V \subseteq \mathrm{GF}(2)^{E+e}$ such that $\dim(V) = k$ and $V/e = W$. Of these spaces $V$, exactly $2^k - 2^{k-d(W)}$ satisfy $d(V) = d(W) - 1$. From the remaining $2^{k-d(V)}$, exactly half has $d(V) = d(W)$, half has $d(V) = d(W) + 1$. A straightforward analysis shows that if $|E|$ tends to infinity, slightly less than 3/7th of the subspaces $V \subseteq \mathrm{GF}(2)^E$ of dimension $k$ will be pedestrian.

If $V \subseteq \mathrm{GF}(2)^E$ is a pedestrian subspace then $\mathrm{GF}(2)^E = V \oplus V^\perp$, i.e. any vector $x \in \mathrm{GF}(2)^E$ can be uniquely written as $x = v + w$, where $v \in V$ and $w \in V^\perp$. Hence there is a unique linear map $\pi_V : \mathrm{GF}(2)^E \to V$ so that $\pi_V(x) \in V$ and $x - \pi_V(x) \in V^\perp$ for all $x \in \mathrm{GF}(2)^E$. The matrix $Q_V$ so that $\pi_V(x) = Q_Vx$ is textbook material in linear algebra; it is

$$Q_V = A^T\left(AA^T\right)^{-1}A \tag{6}$$

where $A$ is any matrix with independent rows such that $\mathrm{rowspace}(A) = V$. That $AA^T$ is invertible follows from our assumption that $V$ is pedestrian, that $Q_V \in \mathrm{rowspace}(A) = V$ is clear, and we have $x - Q_Vx \in \mathrm{kernel}(A) = V^\perp$ since

$$A(x - Q_Vx) = A\left(x - A^T\left(AA^T\right)^{-1}Ax\right) = Ax - AA^T\left(AA^T\right)^{-1}Ax = 0.$$

It is not difficult to determine $Q_V$ from a $q$-basis of $V$.

**Lemma 6** *Let $V \subseteq \mathrm{GF}(2)^E$ be a pedestrian linear subspace, and let $v_1, \dots, v_k$ be a $q$-basis of $V$. Then*

$$Q_V = \sum_{i=1}^{k} v_iv_i^T \quad or \quad Q_V = \sum_{i=1}^{k/2} v_iv_{i+k/2}^T + v_{i+k/2}v_i^T$$

*if the basis is orthogonal or alternating, respectively.*

*Proof* Let $A$ be the matrix whose rows are $v_1, \dots, v_k$. Then

$$AA^T = I \quad \text{or} \quad AA^T = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}$$

depending on whether the $q$-basis is orthogonal or alternating. The result now follows from (6). □

Let $G_V$ be the support graph of the $E \times E$ matrix $Q_V$, so $V(G_V) = E$ and

$$E(G_V) = \bigl\{ef \mid (Q_V)_{ef} \neq 0\bigr\}.$$

**Theorem 7** *If $V \subseteq \mathrm{GF}(2)^E$ and $V' \subseteq \mathrm{GF}(2)^{E'}$ are pedestrian binary spaces, then $M(V)$ is isomorphic to $M(V')$ if and only if $G_V$ is isomorphic to $G_{V'}$.*

Binary matroid isomorphism may thus be reduced to graph isomorphism in the time it takes to construct $G_V$, which is $O(\dim(V)|E|^2)$.

If we do not assume that $V$ is pedestrian, then we may still write

$$\bigl(V + V^\perp\bigr)/\bigl(V \cap V^\perp\bigr) = V/\bigl(V \cap V^\perp\bigr) \oplus V^\perp/\bigl(V \cap V^\perp\bigr).$$

Hence there is a unique linear map $\tilde{\pi}_V : (V + V^\perp)/(V \cap V^\perp) \to V/(V \cap V^\perp)$ such that

$$\tilde{\pi}_V(x) \in V/\bigl(V \cap V^\perp\bigr) \quad \text{and} \quad x - \tilde{\pi}_V(x) \in V^\perp/\bigl(V \cap V^\perp\bigr)$$

for all $x \in (V + V^\perp)/(V \cap V^\perp)$. Clearly, $\tilde{\pi}_V$ coincides with $\pi_V$ if $V$ is pedestrian.

**Lemma 7** *Let $V \subseteq \mathrm{GF}(2)^E$ be a linear space and let $\tilde{V}$ be any subspace of $V$ such that $V = \tilde{V} + (V \cap V^\perp)$. Then $\tilde{\pi}_V(x + (V \cap V^\perp)) = \pi_{\tilde{V}}(x) + (V \cap V^\perp)$ for any $x \in V + V^\perp$.*

*Proof* Let $x \in V + V^\perp$. If $\tilde{W} \subseteq V^\perp$ is such that $V^\perp = \tilde{W} \oplus (V \cap V^\perp)$, then $V + V^\perp = \tilde{V} \oplus \tilde{W} \oplus (V \cap V^\perp)$ and we may write $x = v + w + z$, where $v \in \tilde{V}$, $w \in \tilde{W}$, $z \in V \cap V^\perp$. Then

$$\tilde{\pi}_V\bigl(x + \bigl(V + V^\perp\bigr)\bigr) = v + \bigl(V \cap V^\perp\bigr) = \pi_{\tilde{V}}(x) + \bigl(V \cap V^\perp\bigr)$$

as required. □

And so we have

$$\tilde{\pi}_V\bigl(x + \bigl(V \cap V^\perp\bigr)\bigr) = Q_{\tilde{V}}x + \bigl(V \cap V^\perp\bigr)$$

for any $\tilde{V}$ such that $V = \tilde{V} + (V \cap V^\perp)$. Such a $\tilde{V}$ is determined as the span of the first $k - d(V)$ vectors of a $q$-basis of $V$.

If $(F_{-1}, F_0, F_1)$ is the canonical tripartition of $V$, then from Lemma 5 we have

$$F_{-1} = \bigcup \bigl\{\mathrm{supp}(v) \mid v \in V \cap V^\perp\bigr\}.$$

Then $(Q_{\tilde{V}})_{ef}$ is independent of the choice of $\tilde{V}$ if $e, f \in F := E \setminus F_{-1}$, since then

$$\big\langle e_e + \big(V \cap V^{\perp}\big), \tilde{\pi}_V\big(e_f + \big(V \cap V^{\perp}\big)\big)\big\rangle = e_e^T Q_{\tilde{V}} e_f = (Q_{\tilde{V}})_{ef}.$$

Let $\tilde{G}_V$ denote the support graph of $Q_{\tilde{V}}[F, F]$. Then $\tilde{G}_V = G_V$ if $V$ is pedestrian. Theorem 7 thus extends to non-pedestrian spaces in a weaker form:

**Theorem 8** *If $V \subseteq \mathrm{GF}(2)^E$ and $V' \subseteq \mathrm{GF}(2)^{E'}$ are binary spaces, then $M(V)$ is isomorphic to $M(V')$ only if $\tilde{G}_V$ is isomorphic to $\tilde{G}_{V'}$.*

## 4 Some remarks and conjectures

### 4.1 Counting bases

As was mentioned in the introduction, the complexity of $\tau^0(\mathcal{M}_{\mathbb{F}}, 1, 1)$ appears to be open. Vertigan announced that this problem is #P-complete for any fixed field $\mathbb{F}$ in [14], but his result remains unpublished.

It is straightforward from the definition of the Tutte-polynomial (1) that

$$T_M(1,1) = \big|\big\{F \subseteq E \mid r_M(E) = r_M(F) = |F|\big\}\big|,$$

i.e. that $T_M(1,1)$ equals the number of bases of $M$. Thus for any fixed field $\mathbb{F}$, the complexity of the following problem is open:

**given**: a basis of a subspace $V \subseteq \mathbb{F}^E$
**find**: the number of bases of $M(V)$

For regular matroids, however, counting bases is easy: if $A$ is a totally unimodular matrix with independent rows, then the number of bases of $M(A)$ equals $\det(AA^T)$. For the case of graphs, this is known as Kirchhoff's Matrix-Tree Theorem—the proof is a direct application of the Cauchy–Binet Formula for $\det(AB)$ in linear algebra. Thus computing the number of bases of $M(A)$ clearly takes polynomial time given the totally unimodular matrix $A$. This result generalizes to sixth-root-of-unity matroids and even quaternionic-unimodular matroids. See [11] for the extension of the Matrix-Tree Theorem to quaternionic matroids, as well as a noteworthy use of the matrix $Q_V$ in relation to counting bases in minors of $M(V)$. We conjecture that the following related problem may also be solved in polynomial time:

**given**: a dyadic matrix $A$
**find**: the number of bases of $M(A)$

Here, a rational matrix $A$ is *dyadic* if $\det(B) \in \{(-1)^a 2^b \mid a, b \in \mathbb{Z}\} \cup \{0\}$ for each square submatrix $B$ of $A$, and a matroid $M$ is *dyadic* if $M = M(A)$ for some dyadic matrix $A$.

The class of matroids representable over a fixed field has exponential growth rate, but the regular matroids, the sixth-root-of-unity matroids and the dyadic matroids each have a *quadratic growth rate* (see [2]). A bold conjecture one might make is that any minor-closed class of matroids of quadratic growth rate is such that the number of bases of a matroid in the class is computable in polynomial time from some succinct description of the matroid. To be more specific about the nature of this succinct description, we conjecture: if $\mathbb{P}$ is a partial field (see [11] for a definition) so that the class of matroids representable over $\mathbb{P}$ has quadratic growth rate, then it takes polynomial time to compute the number of bases of $M(A)$, given any $\mathbb{P}$-matrix $A$.

### 4.2 Isomorphism testing for binary matroids

We consider the problem:

**given**: bases for subspaces $V \subseteq \mathrm{GF}(2)^E$, $V' \subseteq \mathrm{GF}(2)^{E'}$
**decide**: if $M(V)$ is isomorphic to $M(V')$

This problem properly contains isomorphism testing for 3-connected graphs, and by a simple reduction the general graph isomorphism problem. The complexity of the latter problem remains open to this day. In practice, one may use a canonical labeling algorithm as was described and implemented by McKay [9] for solving such graph isomorphism problems.

We described three isomorphism invariants that one could compute from a basis of $V$ in just $O(\dim(V)|E|^2)$ time:

(1) $T_{M(V)}(-\iota, \iota)$;
(2) the cardinalities of the $F_i$ in the canonical tripartition $(F_{-1}, F_0, F_1)$; and
(3) the number of edges of $\tilde{G}_V$, $\tilde{G}[F_0]$ and $\tilde{G}[F_1]$.

In a random selection of 10,000 subspaces of $\mathrm{GF}(2)^{30}$ of dimension 10, all but 324 of the pairs of were revealed as non-isomorphic by a comparison of these invariants, or were identified as isomorphic by an application of Theorem 7. This means that in less than 1 in 100,000 cases, it was necessary to revert to other methods for testing isomorphism. In a forthcoming Sage package for matroid computation, this technique has been implemented to speed up the isomorphism test for binary matroids, and similar methods have been implemented for ternary and quaternary matroids.

Haggard, Pearce, and Royle [6] describe a practical algorithm to compute the Tutte polynomial of a graph, which makes extensive use of graph isomorphism testing to reduce the overall computational effort. A possible application of our isomorphism test would be the extension of their method to an algorithm for computing the Tutte polynomial of binary matroids of moderate size, where the more straightforward methods can only handle small matroids.

**Acknowledgements** We thank Judith Keijsper for a stimulating conversation on the nature of orthogonal projection in binary spaces. We also thank two anonymous referees for their constructive comments.

## References

1. Brown, E.H. Jr.: Generalizations of the Kervaire invariant. Ann. Math. (2) **95**, 368–383 (1972)
2. Geelen, J., Kung, J.P.S., Whittle, G.: Growth rates of minor-closed classes of matroids. J. Comb. Theory, Ser. B **99**(2), 420–427 (2009)

3. Gioan, E., Las Vergnas, M.: On the evaluation at $(j, j^2)$ of the Tutte polynomial of a ternary matroid. J. Algebr. Comb. **25**(1), 1–6 (2007)
4. Godsil, C., Royle, G.: Algebraic Graph Theory. Graduate Texts in Mathematics, vol. 207. Springer, New York (2001)
5. Greene, C.: Weight enumeration and the geometry of linear codes. Stud. Appl. Math. **55**(2), 119–128 (1976)
6. Haggard, G., Pearce, D.J., Royle, G.: Computing Tutte polynomials. ACM Trans. Math. Softw. **37**(3), Art. 24, 17 (2010)
7. Jaeger, F., Vertigan, D.L., Welsh, D.J.A.: On the computational complexity of the Jones and Tutte polynomials. Math. Proc. Camb. Philos. Soc. **108**(1), 35–53 (1990)
8. Jaeger, F.: Tutte polynomials and bicycle dimension of ternary matroids. Proc. Am. Math. Soc. **107**(1), 17–25 (1989)
9. McKay, B.D.: Practical graph isomorphism. In: Proceedings of the Tenth Manitoba Conference on Numerical Mathematics and Computing, vol. I, Winnipeg, Man., 1980, vol. 30, pp. 45–87 (1981)
10. Oxley, J.: Matroid Theory, 2nd edn. Oxford Graduate Texts in Mathematics, vol. 21. Oxford University Press, Oxford (2011)
11. Pendavingh, R.A., van Zwam, S.H.M.: Skew partial fields, multilinear representations of matroids, and a matrix tree theorem. Adv. Appl. Math. **50**(1), 201–227 (2013)
12. Rosenstiehl, P., Read, R.C.: On the principal edge tripartition of a graph. Ann. Discrete Math. **3**, 195–226 (1978)
13. Stein, W.A., et al.: Sage Mathematics Software (Version 4.8.0). The Sage Development Team, 2012. http://www.sagemath.org
14. Vertigan, D.: Bicycle dimension and special points of the Tutte polynomial. J. Comb. Theory, Ser. B **74**(2), 378–396 (1998)
15. Wood, J.A.: Witt's extension theorem for mod four valued quadratic forms. Trans. Am. Math. Soc. **336**(1), 445–461 (1993)