Counting bases of representable matroids

Michael Snook

School of Mathematics, Statistics and Operations Research
Victoria University of Wellington
Wellington, New Zealand

michael.snook@msor.vuw.ac.nz

Submitted: May 31, 2012; Accepted: Nov 18, 2012; Published: Dec 13, 2012
Mathematics Subject Classifications: 05b35, 68r05

Abstract

We show that it is #P-complete to count the number of bases of matroids representable over a fixed infinite field or fields of fixed characteristic.

Keywords: matroid bases, complexity, #P-complete.

In this paper we consider the difficulty of counting bases of representable matroids. We note that given a rank or independence oracle or a matrix representation, finding a basis of a matroid is easy. However, in many cases counting the bases of a matroid is #P-complete. For example, it is #P-complete to count the number of bases of transversal matroids or bircircular matroids ([2] and [3]). Representable matroids are an important class of matroids and it is only natural to consider the difficulty of counting the bases for the class of representable matroids. The obvious goal would be a theorem that answers Question 1.

Question 1. *Is it #P-complete to count the number of bases of a representable matroid over any fixed field.*

Vertigan proved this to be #P-complete in 1991 [2, 8]. However, no publication was ever produced. This feels like a substantial hole in the literature and should be remedied. One of the surprising things about this result is the fact that it is easy to count bases of graphic matroids while Vertigan's result implies that it is hard to count the number of bases of binary matroids.

While we do not resolve Question 1, in this paper we prove several similar results. In particular, it will be shown that it is #P-complete to count bases of representable matroids over
(i) fixed infinite fields and
(ii) finite fields of a fixed characteristic.

At the very least, these results provide a large amount of evidence that it is #P-complete to count the number of bases of matroids representable over any fixed field.

We will begin with some preliminaries on the complexity class #P. This class is the counting version of the class NP of decision problems. For example the decision problem could be: is there a vertex cover of size k? While the corresponding enumeration problem would be: how many vertex covers of size k are there? The complexity class #P was introduced by Valiant in 1979 by showing that the problem of calculating the permanent of a matrix is #P-complete [6]. We begin our definition of #P with a *counting Turing Machine*. This is just a standard non-deterministic Turing Machine with additional output that prints the number of accepting paths. The time complexity is that of the longest accepting path. The class #P is the class of problems that can be solved in polynomial time on a counting Turing Machine. Thus the class NP is contained in #P as any problem that can be verified in polynomial time by a non-deterministic Turing Machine can be solved in polynomial time by a counting Turing Machine. The notion of NP-completeness carries over to the class #P. Much as NP-complete problems are the hardest problems in NP, #P-complete problems are the hardest problems in #P. The enumeration version of a number of NP-complete problems are known to be #P-complete. However, it is certainly not known that the enumeration versions of all NP-complete problems are #P-complete. As an example of this, consider the problem of deciding if a graph has a Hamiltonian subgraph. The decision problem is NP-complete while the problem of enumerating the number of Hamiltonian subgraphs is believed to not be in #P. The reason for this is to know you have a Hamiltonian subgraph you would need to find a Hamiltonian circuit of the subgraph. However, the number of possible Hamiltonian circuits of subgraphs is not the number of Hamiltonian subgraphs. For more details of this and the class #P see [9].

The method of showing that a problem is #P-complete is similar to that of showing that a problem is NP-complete. We take a known #P-complete problem and show that by performing a polynomial number of reductions to our problem, we can extract the solution to the known #P-complete problem from the solutions of our problem. The major difference here is that we are allowed to perform multiple reductions as long as there is only a polynomial number of reductions performed and each reduction can be done in polynomial time.

It is worth pointing out that some decision problems that are in P have corresponding enumeration problems that are #P-complete. Examples of these include counting forests of a graph or perfect matchings in bipartite graphs ([4] and [7]). Counting forests of a graph will be of particular use to us in this paper as the proofs of our main results will be reductions from the problem of counting forests in a graph.

We will assume that the reader is familiar with basic matroid theory. For an introduction to matroid theory see [5]. We will be using the operation of truncation for several of the reductions that follow. A problem with using truncation on representable matroids is that truncation of a representable matroid does not always produce a matroid representable over the same field. Even if truncating produces a matroid representable over the same field, it may be hard to construct a representation of the resulting matroid. Thus we need to find a way of producing an appropriate representation of a matroid created by

truncation. There are ways of getting around this though. The operation of truncation is equivalent to adding an element freely and then contracting it. It is often easier to create a representation of the matroid obtained by adding elements freely than it is to create the representation of a truncated matroid. This is partly due to the fact that to add elements freely, we only need to create a few columns of the matrix while to create the truncated representation we need to create a matrix representation almost from scratch. This is why, if we want to truncate a representable matroid, we will often add elements freely and then contract them. We can do this because contraction preserves representability. Therefore if we can find a representation of the matroid obtained by adding elements freely, we can obtain a representation of the truncated matroid.

Our approach to proving that counting bases is #P-complete for matroids representable over fixed infinite fields and fields of fixed characteristic will be similar. We will begin by adding elements freely to a given representable matroid. We will then construct a representation over an appropriate field for the matroid obtained and contract the added elements. This will allow us to create representations for truncations of the given matroid. We will then use this construction of the truncated matroid in a reduction from the known #P-complete problem of counting forests of a graph.

#Forests
INSTANCE: A graph G.
QUESTION: How may forests does G have?

In all our reductions from #Forests, we will need to construct a totally unimodular representation of the cycle matroid of the graph G in polynomial time. We can do this in the following fashion ([5], Chapter 5). Take the graph G and arbitrarily direct each edge to form the directed graph $D(G)$. Then the totally unimodular representation of G is the incidence matrix of $D(G)$. For the rest of this paper, we will assume that all representations of graphic matroids are constructed by this method. Thus they are all totally unimodular.

In the reductions that follow, we will need to be able to add elements freely to the matrices produced by the above method to produce matroids representable over certain fields. To do so, we will make use of a special type of matrix. An $n \times n$ Vandermonde matrix V is a matrix of the following form.

$$V = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix}$$

For the Vandermonde matrix V, $\det(V) = \prod_{i<j}(\alpha_j - \alpha_i)$. Therefore if $\alpha_1, \ldots, \alpha_n$ are all distinct, then $\det(V) \neq 0$. Otherwise, $\det(V) = 0$. In the following arguments we will be using a special matrix that is very similar to a Vandermonde matrix. We will say an $m \times n$ matrix X with entries in $\mathbb{Z}[x]$ is an *r-polynomial Vandermonde matrix* if $X_{i,j} = p_i(x^{k_j})$, where p_i is a monic polynomial such that $\deg(p_1) < \deg(p_2) < \ldots < \deg(p_m) \leqslant r$ and

$0 \leqslant k_1 < k_2 < \ldots < k_n \leqslant r$. Note that if we let $p_i(x) = x^i$ and $k_j = j - 1$, then the r-polynomial Vandermonde matrix is also a Vandermonde matrix with $\alpha_i = x_i$.

Lemma 2. *Let X be a $n \times n$ r-polynomial Vandermonde matrix. Then $\det(X)$ is a non-zero monic polynomial with degree less than r^3.*

Proof. The determinant of an $n \times n$ matrix X can be evaluated as $\sum_{\sigma \in S_n} sgn(\sigma) \prod_{i=1}^{n} X_{i,\sigma(i)}$ where $sgn(\sigma) = 1$ if σ is even and -1 otherwise. We will show that for the matrix X, there is a single product of maximum degree in this sum and thus there can be no cancellation of products and therefore the determinant cannot be 0. Moreover, this product of maximum degree will happen when σ is the identity permutation e.

Let P be some product $\prod_{i=1}^{n} X_{i,\sigma(i)}$ such that $\sigma \neq e$. Then P must contain some element $X_{i,j}$ where $i \neq j$. Take the greatest i such that $\sigma(i) \neq i$. Then P must also contain $X_{l,i}$ for some $l \neq i$ as σ is a permutation. As i has been chosen to be maximum, $i > j$ and $i > l$. Then as X is a r-polynomial Vandermonde matrix, $\deg(X_{i,i}) = \deg(p_i)k_i$, $\deg(X_{l,j}) = \deg(p_l)k_j$, $\deg(X_{i,j}) = \deg(p_i)k_j$ and $\deg(X_{l,i}) = \deg(p_l)k_i$. Let P' be a new product given by

$$P' = \frac{PX_{i,i}X_{l,j}}{X_{i,j}X_{l,i}}.$$

Note that

$$\deg(p_i)k_i + \deg(p_l)k_j - \deg(p_i)k_j - \deg(p_l)k_i = (\deg(p_i) - \deg(p_l))(k_i - k_j) > 0,$$

as $\deg(p_i) > \deg(p_l)$ and $k_i > k_j$. Thus $\deg(P') > \deg(P)$. Therefore by changing σ so that it fixes more elements we increase the degree. Hence we obtain the maximum degree only when σ is the identity permutation. As all $X_{i,j}$ are monic polynomials, any product of them must also be a monic polynomial. Thus the determinant of X is a non-zero monic polynomial. Now consider the product $\prod_{i=1}^{n} X_{i,i}$. This product will be a subproduct of $\prod_{i=1}^{r} X'_{i,i}$ which is a degree $\sum_{i=1}^{r} i^2$ monic polynomial. Thus

$$\deg(\det(X)) \leqslant \sum_{i=1}^{r} i^2 < r^3.$$

□

Lemma 3. *Let $A = [D|X]$ be a square matrix such that D is totally unimodular with non-zero determinant and X is an r-polynomial Vandermonde matrix. Then by row reductions and row swapping on A, we can get the following matrix*

$$A' = \left[\begin{array}{c|c} D' & X_t \\ \hline 0 & X_b \end{array}\right]$$

that has the following properties:

1. $|\det(A)| = |\det(A')|$,

2. *D' is a square matrix in upper triangular form with non-zero entries on the diagonal and*

3. *The matrix X_b is an r-polynomial Vandermonde matrix.*

Proof. This will be proven by induction on the number of columns in D. Suppose D no columns. Then A is already in the required form.

Now suppose this holds for matrices A where D has no more than k columns and take a matrix such that D has at most $k+1$ columns. For $i < l$, consider the matrix X'' obtained from X by adding row i to row l α times. Then $X''_{l,j} = p_l(x^{k_j}) + \alpha p_i(x^{k_j})$. As $i < l$, this is a monic polynomial with the same degree as $X_{l,j}$. Thus X'' is also an r-polynomial Vandermonde matrix.

Now the columns of D are all linearly independent, so there must be a non-zero entry in the first column. Choose the first non-zero entry in the first column. Use row reductions so that below this non-zero element, the column is only zeros. Because in the row reduction, rows have only had rows added/subtracted to them from above, we see that the matrix X' obtained by the row operations is still an r-polynomial Vandermonde matrix. Now delete the first column and the row with the non-zero entry. Call the resulting matrix A''. It now follows from the induction hypothesis that we can create a matrix in the required form from A''. We can then add the deleted row back in as the first row and put a column of zeros under the non-zero element from the deleted row. This has the same effect as moving the deleted row to the top of the matrix. The resulting matrix will be in the desired form. Again as the only operations performed are adding or subtracting rows from one another and row swaps, the absolute value of of the determinant has not changed. Thus $|\det(A)| = |\det(A')|$.

□

We know that the determinant of any r-polynomial Vandermonde matrix is a non-zero monic polynomial. We want a similar result for the determinant of a square submatrix of matrices of the form $[A|X]$ where A is a submatrix of a totally unimodular matrix and X is an r-polynomial Vandermonde matrix. As A is a submatrix of a totally unimodular matrix, we can no longer guarantee that $\det([A|X])$ is a monic polynomial. However, as we will see in Lemma 4, if $\det([A|X])$ is not a monic polynomial, then its leading coefficient is -1. In light of this, we will define an *absolutely monic polynomial* to be a polynomial with leading coefficient 1 or -1.

Lemma 4. *For $k < r$, let A be a rank k $r \times k$ totally unimodular matrix and X be a $r \times (r-k)$ r-polynomial Vandermonde matrix. Then* $\det[A|X]$ *is a non-zero absolutely monic polynomial of degree $\leqslant r^3$ and coefficients of absolute value no greater than $r!m^r$ where m is the value of the largest coefficient in X'.*

Proof. By Lemma 3, we know we can get $[A|X']$ in the form

$$A' = \left[\begin{array}{c|c} D' & X_t \\ \hline 0 & X_b \end{array}\right]$$

where

1. $|\det([A|X])| = |\det(A')|$,
2. D' is a square matrix in upper triangular form with non-zero entries on the diagonal and
3. The matrix X_b is an r-polynomial Vandermonde matrix.

Note that $\det(A') = \det(D') \cdot \det(X_b)$ and $|\det(D')| = 1$ as A is totally unimodular. Thus $\det(A') = 0$ if and only if $\det(X_b) = 0$. As X_b is an r-polynomial Vandermonde matrix, it follows by Lemma 2 that $\det(X_b)$ is a non-zero monic polynomial with degree no greater than r^3. Thus $\det(A')$ is a non-zero absolutely monic polynomial of degree no greater than r^3.

Now consider the coefficients in the determinant of $[A|X]$. The determinant is a sum of $r!$ products of r polynomials. As m is the maximum size of a coefficient in $[A|X]$, the absolute value of a coefficient in each product can be no greater than m^r. As there are $r!$ products, the maximum size of a coefficient in $\det[A'|X]$ can therefore be no greater than $r!m^r$. □

We now have all we need to move on to specific cases of the basis counting problem. We will begin with showing it is #P-complete to count the number of bases of matroids representable over fields of characteristic 0. That is the following problem.

Char-0 #Bases
INSTANCE: A representation of a matroid M over a fixed field of characteristic 0.
QUESTION: How many bases does M have?

We need to add one caveat to this as not all fields of characteristic 0 can be worked with in polynomial time by a Turing machine. For example, certain real numbers may require an infinite binary string to represent them and thus cannot be used as input. Moreover, if the field operations are not polynomial time, then even deciding if a set of columns is a basis will likely be hard.

Note that all fields of characteristic 0 contain the rationals as a subfield. Suppose it is #P-complete to count bases of matroids representable over some subfield of a field F. Then it follows that it is #P-hard to count bases of matroids representable over F. Thus, if it is #P-complete to count bases of matroids representable over the rationals, then it is #P-hard to count bases of matroids representable over any fixed field with characteristic 0. Furthermore, if F can be described to a Turing machine and operations are in polynomial time, then it is #P-complete to count bases of matroids representable over F.

Lemma 5. *Assume M is a rational representable matroid with a totally unimodular representation $M[A]$ where $A = [I_r|C]$. Let X be an $r \times r$ r-polynomial Vandermonde matrix where $X_{i,j} = x^{ij}$. Furthermore, let X' be the matrix obtained by substituting x with the rational number $(r! + 1)$. Then $M' = M[A|X']$ is the rational representable matroid obtained by adding r elements freely to M.*

Proof. Let $[A'|X'']$ be an $r \times r$ submatrix of $[A|X]$, where A' is a linearly independent subset of columns of A and X'' is a subset of columns of X. From Lemma 4 we know that $\det[A'|X'']$ is a non-zero absolutely monic polynomial of degree less than r^3 and coefficients of absolute size no greater than $n = r!m^r = r!$ as all coefficients in X are 1. Note that $\sum_{i=1}^{k} n \cdot (n+1)^k = (n+1)^{k+1} - 1$ for all $k \in \{1, 2, \ldots, r^3\}$. Thus if we substitute $x = n + 1$ into the polynomial corresponding to the determinant of $[A'|X'']$, then the absolute value of the largest power is larger than the rest of the polynomial. Thus there can be no cancellation and therefore the determinant of any $r \times r$ submatrix of $[A|X']$ is non-zero if the columns from A are linearly independent. Therefore $M' = M[A|X']$ is a rational representation of the matroid obtained by adding r elements freely to M. □

Lemma 6. *The matrix M' in Lemma 5 can be constructed in polynomial time given the totally unimodular matrix $A = [I_r|C]$.*

Proof. To show this, all we need is that the size of $(r!m^r + 1)^{r^2}$ is polynomial in terms of $\max(r + |C|, \log(m))$ where C is the number of columns in C. The size of $(r!m^r + 1)^{r^2}$ is

$$\log((r!m^r + 1)^{r^2}) = r^2 \log(r!m^r + 1) < r^2 \log((rm)^r + 1) < r^2 \log((2rm)^r) = r^3 \log(2rm)$$

which is clearly polynomial in $\max(r + |C|, \log(m))$. Therefore the matrix $[A|X']$ can be constructed in polynomial time. □

Theorem 7. *It is #P-complete to count the number of bases of a matroid representable over the rationals.*

Proof. This will be done from a reduction of #Forests. Let G be a graph for which you want to count the number of forests. Without loss of generality we can assume that G is connected. We can construct a totally unimodular representation A of the rank $r = |V|-1$ cycle matroid M of G in polynomial time. Then the number of forests of G is the sum of the number of independent sets of size k for $k = \{0, \ldots, r\}$ of M. Now construct the matrix M' from Lemma 5.

Let M_k be the matroid obtained from M by $k \in \{0, \ldots, r\}$ truncations. Note that $M_0 = M$. Representations for these matroids can be constructed from M' by simply contracting the first k columns of X' in M' and deleting the remaining $r - k$ columns of X'. Then the number of independent sets of size k in M is the number of bases of the matroid M_{r-k}. From Lemma 5, we know that a rational representation of M' and thus M_k can be obtained in polynomial time. Therefore it is #P-complete to count bases of matroids representable over the rationals. □

Corollary 8. *Char-0 #Bases is #P-hard.*

Proof. As any field of characteristic 0 contains the rationals as a subfield, it follows that the basis counting problem on matroids representable over a fixed field of characteristic 0 is #P-hard. □

Note that if the fixed field in question can be described to a Turing machine and worked with in polynomial time, then we can replace #P-hard with #P-complete.

If we are working over a finite field of large enough size then the above reduction may still work. However we cannot fix a finite field and then use the above result as there will always be cases where the fixed finite field is not big enough to add elements freely by the above method.

This covers the case of counting bases in matroids representable over fixed fields of characteristic 0. We now move on to the case of counting bases in matroids representable over fields of fixed characteristic.

Fixed Char-p #Bases
INSTANCE: A representation of a matroid M over some field of characteristic p.
QUESTION: How many bases does M have?

Our method for showing that this problem is #P-complete will be similar to the one used to show that Char-0 #Bases is #P-complete. We will modify the matrix X where $X_{i,j} = x^{ij}$ in a way that creates a representation for a matroid obtained by adding elements freely to a representable matroid. Using this construction, we can then produce a reduction from the forest counting problem to the problem Fixed Char-p #Bases. To do this, our construction must produce a matroid representable over an appropriate field. The required construction will be given by Lemma 9.

We will treat elements of the fields $\mathrm{GF}(p^k)$ as polynomials in the variable x with coefficients in $\mathrm{GF}(p)$ and maximum degree $k-1$ modulo some irreducible polynomial of degree k. If $f \in \mathrm{GF}(p^k)$, then $\deg(f)$ is the degree of f when considered as a polynomial. For example, the elements of $\mathrm{GF}(4)$ are $\{0, 1, x, x+1\}$ modulo $x^2 + x + 1$. We will be interested in the fields $\mathrm{GF}(p^{r^3})$. Let $g_{p,r}(x)$ be the degree r^3 polynomial such that multiplication in $\mathrm{GF}(p^{r^3})$ is reduced modulo $g_{p,r}(x)$. Moreover, let $\phi_{p,r} : \mathbb{Z}[x] \to \mathrm{GF}(p^{r^3})$ be the homomorphism

$$\begin{aligned}\phi_{p,r}(\alpha_0 + \alpha_1 x^1 \quad + \quad \ldots + \alpha_n x^n) = \\ ((\alpha_0 \bmod p) + (\alpha_1 \bmod p)x^1 + \ldots + (\alpha_n \bmod p)x^n) \bmod g_{p,r}(x).\end{aligned}$$

Lemma 9. *Let $A = [I_r|C]$ be a totally unimodular matrix over $\mathbb{Z}[x]$ and let X be the $r \times r$ r-polynomial Vandermonde matrix where $X_{i,j} = x^{ij}$. If $M = M[A]$, then $\phi_{p,r}([A|X])$ is the $\mathrm{GF}(p^{r^3})$ representation of the matroid obtained by adding r elements freely to M.*

Proof. From Lemma 2, we see that $\det[X]$ is a non-zero monic polynomial with degree less than r^3. Thus $\phi_{p,r}(\det[X])$ is a non-zero element of $\mathrm{GF}(p^{r^3})$ and therefore the columns in X are all linearly independent. Let $N' = [A'|X']$ be some $r \times r$ square submatrix of $[A|X]$ where A' is a linearly independent subset of columns of A and X' is a submatrix of X. It follows from Lemma 4 that $\det(N')$ is a non-zero absolutely monic polynomial of degree less than r^3. Thus $\phi_{p,r}(\det[N'])$ is a non-zero element of the field $\mathrm{GF}(p^{r^3})$. As this holds for all possible N' and $\phi_{p,r}(\det[X]) \neq 0$, we see that $\phi_{p,r}([A|X])$ is the $\mathrm{GF}(p^{r^3})$ representation of the matroid obtained by adding r elements freely to M. □

We now have a method of creating representations for matroids obtained by adding elements freely to representable matroids such that the created representation is over a field with the same characteristic. We will now use this in a similar reduction to that of Theorem 7 to show that Fixed Char-p #Bases is #P-complete.

Theorem 10. *Fixed Char-p #Bases is #P-complete.*

Proof. Let G be an instance of the forest counting problem on graphs and let M be the rank r cycle matroid of G. Suppose we can count bases of matroids representable over fields of characteristic p. We can create a totally unimodular representation A of M over the field $\mathbb{Z}[x]$ in polynomial time. Now create the $\mathbb{Z}[x]$ matrix $[A|X]$ where $X_{i,j} = x^{ij}$. By Lemma 9, the matroid M' represented by the $\mathrm{GF}(p^{r^3})$ matrix $\phi_{p,r}([A|X])$ is isomorphic to the matroid obtained by adding r elements freely to M.

Now by contracting k columns of $\phi_{p,r}(X)$ and deleting the remaining $r-k$ columns of $\phi_{p,r}(X)$ for $k \in \{0,\ldots,r\}$ from M', we obtain a representation of a matroid whose number of bases is the same as the number of independent sets of M of size $r-k$. This is just truncating M k times. Thus by doing this for $k=0$ to $k=r$ we can count all the independent sets of M and thus the forests of G. Note that the field $\mathrm{GF}(p^l)$ has the same characteristic as $\mathrm{GF}(p)$ for all positive integers l. Thus it is #P-complete to count the number of bases of a representable matroid over fields of fixed characteristic. □

By using the same argument as in Theorem 10, we can show that the following problem is #P-complete.

Infinite Char P #Bases
INSTANCE: A representation of a matroid M over a fixed infinite field of non-zero characteristic p.
QUESTION: How many bases does M have?

Note that for this problem, we assume that we have some way of describing the infinite field to our Turing Machine. Furthermore, because the problem is defined for a fixed field, we can assume that we know all the properties of the field. In particular, we know whether or not it has a transcendental element.

Lemma 11. *Let F be an infinite field with non-zero characteristic that has a transcendental element α. Then it is #P-complete to count bases of matroids representable over F.*

Proof. Because α is transcendental, we can make a matrix X similar to the one from Theorem 10 with $\phi(X_{i,j}) = \alpha^{ij}$. We can then use the reduction from Theorem 10 to show that this is #P-complete. □

A *Steinitz number* is a number of the form $N = p_1^{x_1} \cdot p_2^{x_2} \cdot \cdots = \prod_{i=1}^{\infty} p_i^{x_i}$ where p_i is the *ith* prime and $x_i \in \{0,1,2,\ldots,\infty\}$ [1]. This is a generalization of integers that allows for infinite numbers. For some Steinitz number N, $\mathrm{GF}(p^N) = \bigcup_{d|N} \mathrm{GF}(p^d)$ where $d \in \mathbb{Z}$.

Lemma 12. *Let F be an infinite field with non-zero characteristic p that has no transcendental element α. Then it is #P-complete to count bases of matroids representable over F.*

Proof. Let G be a graph for which we want to count the number of forests and r be the rank of the cycle matroid of G. We will prove this by showing that there is a set of subfields of F such that it is #P-complete to count bases of matroids representable over them. This will imply that it is #P-complete to count the number of bases representable over F. If F is infinite with no transcendental element, every element must be algebraic. Thus it must be a subfield of the algebraic closure of $\mathrm{GF}(p)$, denoted $\overline{\mathrm{GF}(p)}$. Brawley and Schnibben showed that all sub fields of $\overline{\mathrm{GF}(p)}$ are of the form $\mathrm{GF}(p^N)$ for some Steinitz number N [1]. If F is infinite, then either there must be some power $x_i = \infty$ in N or there is an infinite number of x_i's that are not equal to zero. First, suppose we have some $x_i = \infty$. Then choose some k such that $p_i^k > r^3$. This gives a subfield $F' = \mathrm{GF}(p^{p_i^k}) \subset F$. We can now work over F' and use the reduction from Theorem 10. Thus it is #P-complete to count the number of bases of matroids representable over fields of the form $\mathrm{GF}(p^{p_i^k})$ for some positive integer k.

Now suppose that N has an infinite number of primes p_i with $x_i \neq 0$. Let P be the set of all such primes. When given G, we can now work over the field $\mathrm{GF}(p^{p_i})$ where $p_i \in P$ and $p_i > r^3$. We can then apply that same reduction used in Theorem 10. This shows that it is #P-complete to count the number of bases of matroids representable over the fields $\mathrm{GF}(p^{p_i})$ where $p_i \in P$.

In either case, we have a family of subfields of F such that it is #P-complete to count the number of bases of matroids representable over them. Thus it is #P-complete to count the number of bases of matroids representable over F. □

Theorem 13. *Infinite Char P #Bases is #P-complete*

Proof. An infinite field F of non-zero characteristic p either has a transcendental element or is a subfield of $\overline{\mathrm{GF}(p)}$. Recall that as the problem is for fixed fields, we know if we have a transcendental element. If F has a transcendental element, then Lemma 11 shows that Infinite Char P #Bases is #P-complete. Alternatively, if F is a subfield of $\overline{\mathrm{GF}(p)}$, then it follows from Lemma 12 that it is #P-complete to count bases of matroids representable over F. Therefore Infinite Char P #Bases is #P-complete. □

Combining Theorems 7 and 13 we see that it is #P-complete to count the number of bases for matroids representable over any fixed infinite field. This just leaves the finite case. Theorem 10 provides a partial answer for this case. However, there is still work to be done to resolve Question 1.

Acknowledgements

I would like to thank Dillon Mayhew for his help and support while writing this paper. I would also like to thank the referee for their very quick responses and for simplifying the presentation by suggesting replacing several Lemmas with Lemma 4. Also for simplifying the definition of an r-polynomial Vandermonde matrix.

References

[1] Joel V. Brawley and George E. Schnibben, *Infinite algebraic extensions of finite fields*, American Mathematical Soc., 1989.

[2] Charles J. Colbourn, J. Scott Provan, and Dirk Vertigan, *The complexity of computing the Tutte polynomial on transversal matroids*, Combinatorica, (1995).

[3] Omer Giménez and Marc Noy, *On the complexity of computing the Tutte polynomial of bicircular matroids*, Comb. Probab. Comput., 15 (2006), pp. 385–395.

[4] F. Jaeger, D. L. Vertigan, and D. J. A. Welsh, *On the computational complexity of the jones and tutte polynomials*, Math. Proc. Camb. Phil. Soc., (1990).

[5] J. G. Oxley, *Matroid theory*, Oxford University Press, 2 ed., 2011.

[6] Leslie G Valiant, *The complexity of computing the permanent*, Theoretical Computer Science, 8 (1979).

[7] ——, *The complexity of enumeration and reliability problems*, SIAM Journal on Computing, 8 (1979), pp. 410–421.

[8] Dirk L. Vertigan, *Bicycle dimension and special points of the tutte polynomial*, J. Comb. Theory, Ser. B, 74 (1998).

[9] Dominic Welsh, *Complexity: Knots, Colourings and Counting*, Cambridge University Press, 1993.