THE TUTTE POLYNOMIAL OF A FINITE PROJECTIVE SPACE

MICHAEL BARANY AND VICTOR REINER

Abstract. We compute a p-exponential generating function collating the Tutte polynomials for the family of matroids coming from finite projective spaces.

1. The generating function

Fix a prime power p, and consider the arrangement $\mathcal{A}(p,n)$ consisting of all $[n]_p := \frac{p^n-1}{p-1}$ possible hyperplanes in $\mathbb{F}_p^n$. Alternatively, these hyperplanes have normal vectors given by the columns of an $n \times [n]_p$ matrix, containing one vector from each line in $\mathbb{F}_p^n$. The point of these notes is to compute a compact generating function for the Tutte polynomials $T_{\mathcal{A}(p,n)}(x,y)$; an explicit formula for each $T_{\mathcal{A}(p,n)}(x,y)$, equivalent to (3) below was computed by Mphako [5].

The generating function is p-exponential, and uses some of these basic hypergeometric notations:

$$\begin{aligned}
(x;p)_n &:= (1-x)(1-px)(1-p^2x)\cdots(1-p^{n-1}x)\\
(x;p)_\infty &:= (1-x)(1-px)(1-p^2x)\cdots\\
[n]_p &:= 1+p+p^2+\cdots+p^{n-1} = \frac{1-p^n}{1-p}\\
[n]!_p &:= [n]_p[n-1]_p\cdots[2]_p[1]_p\\
\begin{bmatrix} n \\ \ell \end{bmatrix}_p &:= \frac{(p;p)_n}{(p;p)_\ell (p;p)_{n-\ell}} = \frac{[n]!_p}{[\ell]!_p[n-\ell]!_p}
\end{aligned}$$

Theorem 1.

$$\sum_{n\geq 0} T_{\mathcal{A}(p,n)}(x,y)\frac{u^n(y-1)^n}{(p;p)_n} = \frac{(u;p)_\infty}{((x-1)(y-1)u;p)_\infty}\sum_{k\geq 0} y^{[k]_p}\frac{u^k}{(p;p)_k}.$$

Date: May 2005.

Key words and phrases. Tutte polynomial, finite projective space, finite field method.

This work was inspired by the C code for computing Tutte polynomials produced by the first author as their Spring 2005 UROP project, sponsored by the Univ. of Minnesota Undergraduate Research Opportunities Program, and available at `www.math.umn.edu/ reiner`. Second author supported by NSF grant DMS-0245379.

Proof. We employ the *finite field method* exposed in [1, §3]. Here one computes instead the equivalent *coboundary polynomial*

$$\overline{\chi}_{\mathcal{A}(p,n)}(q,t) := \sum_{x \in \mathbb{F}_q^n} t^{h(x)}$$

where $q = p^r$ is some power of p, so that $\mathbb{F}_q$ is a field extension of $\mathbb{F}_p$, and where $h(x)$ is the number of hyperplanes in $\mathcal{A}(p,n)$ on which the vector $x \in \mathbb{F}_q^n$ lies. This $\overline{\chi}_{\mathcal{A}}(q,t)$ will be a polynomial in q and t, related to the Tutte polynomial as follows[1]:

$$T_{\mathcal{A}}(x,y) = \frac{1}{(y-1)^{\mathrm{rank}(\mathcal{A})}} \overline{\chi}_{\mathcal{A}}((x-1)(y-1), y). \tag{1}$$

To compute $\overline{\chi}_{\mathcal{A}(p,n)}(q,t)$, we take advantage of the $\mathbb{F}_p$-vector space isomorphism $\mathbb{F}_q \cong \mathbb{F}_p^r$ to represent a vector $x = (x_1, \ldots, x_n)$ as an $r \times n$ matrix over $\mathbb{F}_p$, whose i^{th} column represents x_i. If this matrix has rank ℓ, then x represents a vector that will lie on exactly $[n-\ell]_p = h(x)$ hyperplanes in $\mathcal{A}(p,n)$.

Consequently, if we can count the number of $r \times n$ matrices over $\mathbb{F}_p$ having rank ℓ, we can assemble the coefficients of $\overline{\chi}_{\mathcal{A}(p,n)}(q,t)$. It turns out that there are

$$\begin{aligned} \begin{bmatrix} n \\ \ell \end{bmatrix}_p \prod_{i=0}^{\ell-1} (p^{r-i} - 1) &= \begin{bmatrix} n \\ \ell \end{bmatrix}_p \prod_{i=0}^{\ell-1} (qp^{-i} - 1) \\ &= \begin{bmatrix} n \\ \ell \end{bmatrix}_p q^{\ell} (q^{-1}; p)_{\ell}. \end{aligned} \tag{2}$$

such matrices, using the fact that $GL_r(\mathbb{F}) \times GL_n(\mathbb{F})$ acts transitively on them, and calculating the stabilizer subgroup of a typical rank ℓ matrix.

Consequently,

$$\overline{\chi}_{\mathcal{A}(p,n)}(q,t) = \sum_{\ell=0}^{n} \begin{bmatrix} n \\ \ell \end{bmatrix}_p q^{\ell} (q^{-1}; p)_{\ell} \, t^{[n-\ell]_p}. \tag{3}$$

[1]We are lying slightly here: the finite field method exposed in [1, §3] assumes an arrangement of hyperplanes with normal vectors in $\mathbb{Z}^d$, and considers a counting problem for the reduced arrangement in $\mathbb{F}_q^d$ for various primes powers q. However, it applies equally well to an arrangement of hyperplanes in $\mathbb{F}_p^d$ for a prime power p, which one then considers as an arrangement in $\mathbb{F}_q^d$ for various powers $q = p^r$; this is the context of Crapo and Rota's "critical problem" [3, §16].

This assembles nicely into a p-exponential generating function.

$$\begin{aligned}\sum_{n\geq 0}\overline{\chi}_{\mathcal{A}(p,n)}(q,t)\frac{u^n}{(p;p)_n} &= \sum_{n\geq 0}\left(\sum_{\ell=0}^{n}\begin{bmatrix}n\\ \ell\end{bmatrix}_p q^\ell (q^{-1};p)_\ell\; t^{[n-\ell]_p}\right)\frac{u^n}{(p;p)_n}\\ &= \sum_{n\geq 0}\sum_{\ell=0}^{n}\frac{q^\ell (q^{-1};p)_\ell\, u^\ell}{(p;p)_\ell}\cdot\frac{t^{[n-\ell]_p}\, u^{n-\ell}}{(p;p)_{n-\ell}}\\ &= \sum_{\ell\geq 0}\frac{(q^{-1};p)_\ell\,(qu)^\ell}{(p;p)_\ell}\sum_{k\geq 0}t^{[k]_p}\frac{u^k}{(p;p)_k}.\end{aligned}$$

The first sum on the last line can be evaluated as an infinite product by the p-binomial theorem

$$\sum_{\ell\geq 0}\frac{(a;p)_\ell\, x^\ell}{(p;p)_\ell} = \frac{(ax;p)_\infty}{(x;p)_\infty}.$$

Hence taking $a = q^{-1}$ and $x = qu$, one obtains

$$\sum_{n\geq 0}\overline{\chi}_{\mathcal{A}(p,n)}(q,t)\frac{u^n}{(p;p)_n} = \frac{(u;p)_\infty}{(qu;p)_\infty}\sum_{k\geq 0}t^{[k]_p}\frac{u^k}{(p;p)_k}. \tag{4}$$

According to (1), we should now substitute $q = (x-1)(y-1)$ and $t = y$. After noting that $\mathrm{rank}(\mathcal{A}(p,n)) = n$, the theorem follows. □

2. Known specializations

Here are two well-known specializations of the foregoing calculations.

2.1. The characteristic polynomial. Setting $t = 0$ in (3) (or equivalently, setting $\ell = n$ in (2)) yields the number of vectors in $\mathbb{F}_q^n$ that lie on none of the hyperplanes in $\mathcal{A}(p,n)$, which is equivalent (up to rescaling) to the *characteristic polynomial* of the matroid of $\mathcal{A}(p,n)$:

$$q^n(q^{-1};p)_n = (q-1)(q-p)(q-p^2)\cdots(q-p^{n-1}).$$

2.2. Dual Hamming and Hamming codes. The theorem can be used to derive the weight enumerator $A(z)$ for the *dual Hamming code*, whose code vectors consist of the n-dimensional row-space in $\mathbb{F}_p^{[n]_p}$ for the $n\times[n]_p$ matrix that represents the matroid $\mathcal{A}(p,n)$. Greene [4] showed that the weight enumerator is related to the Tutte polynomial by

$$A(z) = (1-z)^n z^{[n]_p - n}T_{\mathcal{A}(p,n)}\left(\frac{1+(p-1)z}{1-z},\frac{1}{z}\right).$$

He computes [4, Example 3.4] that the dual Hamming code has the extremely simple weight enumerator

$$A(z) = 1 + (p^n - 1)z^{p^{n-1}}. \tag{5}$$

Indeed this follows from the theorem with a little algebra, noting that the specialization $x = \frac{1+(p-1)z}{1-z}$ and $y = \frac{1}{z}$ leads to the relation $(x-1)(y-1) = p$, and using the fact that

$$\frac{(u;p)_\infty}{(pu;p)_\infty} = 1 - u.$$

One can, of course, also deduce from the theorem the weight enumerator for the *Hamming code* itself, rather than its dual. But this also follows from (5) via the MacWilliams identity (see [4]).

3. Alternate approach: p-cones

Lastly, we mention an alternate approach to the derivation of Theorem 1. In [2], the authors derive a nice formula expressing the Tutte polynomial $T_{M'}(x,y)$ for the *p-cone*[2] M' of a matroid M of rank r represented inside a finite projective space $\mathbb{P}^r_{\mathbb{F}_p}$, in terms of $T_M(x,y)$. Phrased instead in terms of the coboundary polynomials, their formula reads

$$\overline{\chi}_{M'}(q,t) = t\overline{\chi}_M\left(q,t^p\right) + p^r(q-1)\overline{\chi}_M\left(\frac{q}{p},t\right). \tag{6}$$

One can construct the tower of finite projective geometries $\mathbb{P}^n_{\mathbb{F}_p}$ by iterating this p-cone construction, beginning with the "seed" geometry $M_0 = \mathbb{P}^{-1}_{\mathbb{F}_p}$ of rank 0. Then the p-exponential generating function

$$F(q,t,u) := \sum_{n\geq 0} \overline{\chi}_{\mathcal{A}(p,n)}(q,t)\frac{u^n}{(p;p)_n}$$

obeys the following recurrence derived from (6):

$$F(q,t,u) - tuF(q,t^p,u) = u(q-1)F\left(\frac{q}{p},t,pu\right) + F(q,t,pu). \tag{7}$$

On the face of it, this recurrence looks hard to solve. However, with the hindsight of formula (4) which one hopes to derive for $F(q,t,u)$, it is better to rephrase this recurrence in terms of the generating function

$$\hat{F}(q,t,u) := \frac{(qu;p)_\infty}{(u;p)_\infty}F(q,t,u),$$

which we expect to (miraculously!) be independent of q. The recurrence (7) becomes

$$\hat{F}(q,t,u) - tu\hat{F}(q,t^p,u) = \frac{1}{1-u}\left[u(q-1)\hat{F}\left(\frac{q}{p},t,pu\right) + (1-qu)\hat{F}(q,t,pu)\right]. \tag{8}$$

[2]Here is a definition of the p-cone construction M', starting with a matroid M represented by points in $\mathbb{P}^r_{\mathbb{F}_p}$. First embed $\mathbb{P}^r_{\mathbb{F}_p}$ in $\mathbb{P}^{r+1}_{\mathbb{F}_p}$. Then choose an *apex* point a in $\mathbb{P}^{r+1}_{\mathbb{F}_p} - \mathbb{P}^r_{\mathbb{F}_p}$. Then let M' be the union of all lines spanned by a together with points of M.

One can use this last recurrence to prove that the coefficient of u^n in $\hat{F}(q,t,u)$ is independent of q by induction on n. With this knowledge in hand, the recurrence (8) then greatly simplifies to

$$\hat{F}(t,u) - tu\hat{F}(t^p,u) = \hat{F}\,(t,pu)\,. \tag{9}$$

This is easily solved (e.g. by writing down the recurrence it gives for the coefficient of $\frac{u^n}{(p;p)_n}$ on both sides), yielding

$$\hat{F}(q,t,u) = \sum_{k\geq 0} t^{[k]_p} \frac{u^k}{(p;p)_k},$$

in agreement with (4).

Acknowledgements

The authors thank Joe Bonin for pointing them to the reference [5] and suggesting that they pursue an approach as in Section 3. They also thank Dennis Stanton for useful discussions regarding the recurrence (7).

References

[1] F. Ardila, Computing the Tutte polynomial of a hyperplane arrangement. ArXiv preprint, 2004, math.CO/0409211.
[2] J.E. Bonin and H. Qin, Tutte polynomials of q-cones *Discrete Math.* **232** (2001), 95–103.
[3] H.H. Crapo and G.-C. Rota, On the foundations of combinatorial theory: Combinatorial geometries. Preliminary edition. M.I.T. Press, Cambridge, Mass.-London, 1970.
[4] C. Greene, Weight enumeration and the geometry of linear codes. *Studies in Appl. Math.* **55** (1976), 119–128.
[5] E.G. Mphako, Tutte polynomials of perfect matroid designs. *Combin. Probab. Comput.* **9** (2000), 363–367.

School of Mathematics, University of Minnesota, Minneapolis, MN 55455, USA
E-mail address: bara0051@umn.edu, reiner@math.umn.edu