Frobenius's degree formula and Toda's polynomials

Jin-Yi Cai *

Abstract

We discuss a connection between the degree formula of Frobenius in group representation theory and a family of polynomials used by Toda in his proof of the containment $PH \subseteq P^{\#P}$. The connection gives us a construction and proof of a generalized family of Toda polynomials.

1 Introduction

The theory of group representations and group characters is a powerful invention (discovery?) of Frobenius in 1896. One of the great achievements of Frobenius is to find all the characters of the symmetric group S_n for all n [3]. The celebrated *degree formula* of Frobenius gives the degree of an arbitrary character of S_n in a closed-form formula, corresponding to a partition p of n [5, 2].

One particular step in the derivation of Frobenius's degree formula is the evaluation of a certain determinant. We will make use of this determinant and some easy generalizations in a new construction and proof of a family of polynomials that generalizes those polynomials discovered by Toda in complexity theory.

In 1989, Toda proved one of the most exciting theorems in complexity theory, namely the power of Polynomial-time Hierarchy is subsumed by the power of counting, $PH \subseteq P^{\#P}$ [7]. There are two ingredients to Toda's proof. The first is an adaptation of an idea due to Valiant and Vazirani [8],

*Department of Computer Science, SUNY at Buffalo, Buffalo, NY 14260. Research supported in part by NSF grants CCR 9057486 and CCR 9319093, and an Alfred P. Sloan Fellowship. cai@cs.buffalo.edu

who showed that there is a probabilistic polynomial-time reduction from SAT to Unique Satisfiability. The Valiant-Vazirani reduction has become one of the most successfully applied tools in complexity theory in the past few years, for example [6, 9].

The second ingredient in the proof is entirely due to Toda. The proof calls for a construction which, in a sense, "amplifies" the power of a prime modulus. More precisely, Toda constructed a family of polynomials $\{f_n(x)\}$ with non-negative integral coefficients, such that, if $a = 0 \bmod p$, then $f_n(a) = 0 \bmod p^n$, and if $a = -1 \bmod p$, then $f_n(a) = -1 \bmod p^n$.

While Toda's polynomials have been recognized as an ingenious idea, and useful in some other applications, it is fair to say that they have not found wide spread applications as the first idea in his proof.

The original construction of Toda was a bit *ad hoc* and somewhat mysterious. To me, he sort of pulled a rabbit out of the hat. It was later realized, and pointed out by Yao, and by Beigel and Tauri, that the restriction that the coefficients be non-negative was not really necessary in the specific application Toda intended, and better constructions including an optimal construction without such restrictions were given later, see [10, 1]. Toda's polynomials have been useful in simulations of ACC circuits by constant depth quasi-polynomial size threshold circuits [10]. The better constructions were useful in obtaining better simulations [1]. In this paper we will be faithful to the original requirements of Toda, including non-negative coefficients, and try to "demystify" his constructions.

We give a generalization to Toda's polynomials. Our proof makes it plain a connection between Toda's polynomials and the degree formula of Frobenius. Assuming a closed form for a determinant used in the degree formula, our proof becomes quite straightforward.

2 The degree formula of Frobenius

Let S_n denote the symmetric group on n letters. A group representation of S_n over the complex numbers $\mathbf{C}$ is a homomorphism $R : S_n \to GL(d, \mathbf{C})$, where $GL(d, \mathbf{C})$ denotes the general linear group of dimension d. A group character $\chi : S_n \to \mathbf{C}$ is the trace of some representation R, $\chi(\pi) = \mathbf{tr}R(\pi)$. The degree of a character χ, denoted by $\deg(\chi)$, is the dimension d of the representation.

If a representation R has a non-trivial invariant subspace V, then it is called reducible. Maschke's theorem says that, in this case, the representation R can be completely broken up into a direct sum of two representations. The character becomes the sum of two constituent characters. Thus the irreducible representations and their characters (called simple characters) are the essential ones.

It is an elementary fact that each conjugacy class of S_n is uniquely determined by the cycle structure of a permutation, which in turn is in one-to-one correspondence with the partitions of n. The theory of group characters implies that there are exactly one irreducible representation for each partition of n.

As mentioned earlier, it is one of the most remarkable achievements of Frobenius to obtain all the simple characters of S_n, one for each partition p of n. Let

$$p : p_1 \geq p_2 \geq \ldots \geq p_n \geq 0; \quad \sum_{i=1}^{n} p_i = n,$$

be a partition of n. Then Frobenius asserts that the simple character associated with the partition p has degree

$$\deg(\chi^{(p)}) = \frac{n! \cdot \prod_{1\leq i<j\leq n}(p_i - p_j + j - i)}{\prod_{i=1}^{n}(p_i + n - i)!}.$$

This is the celebrated degree formula of Frobenius.

There is another way of expressing this formula. Associated with any partition p of n is a strictly decreasing sequence of non-negative integers

$$\ell : \ell_1 > \ell_2 > \ldots > \ell_n \geq 0,$$

where $\ell_i = p_i + n - i$. Thus $\sum_{i=1}^{n} \ell_i = n(n+1)/2$. The map from p to ℓ is a one-to-one correspondence, i.e., given a strictly decreasing sequence $\{\ell_i\}$ with $\sum_{i=1}^{n} \ell_i = n(n+1)/2$, we obtain a partition of n by letting $p_i = \ell_i - n + i$.

In terms of $\{\ell_i\}$, the degree formula of Frobenius can be written as

$$\deg(\chi^{(\ell)}) = \frac{n! \cdot \prod_{1\leq i<j\leq n}(\ell_i - \ell_j)}{\ell_1!\ell_2!\ldots\ell_n!}.$$

Let $e_i = n - i$, for $1 \leq i \leq n$. An important step in the derivation of Frobenius's degree formula is the evaluation of the following determinant

$$\det\left(\frac{\ell_i!}{(\ell_i - e_j)!}\right).$$

This was shown to have the value $\prod_{1\leq i<j\leq n}(\ell_i - \ell_j)$. For completeness sake, we will give a brief sketch of the proof of this determinant in the next section. A slight generalization will be given that will lead to our new proof of Toda's polynomials.

3 The determinant

Proposition 3.1 (Frobenius) *For any sequence of integers $\ell_1, \ell_2, \ldots, \ell_n$,*

$$\det\left(\frac{\ell_i!}{(\ell_i - e_j)!}\right) = \prod_{i<j}(\ell_i - \ell_j),$$

where $e_j = n - j$.

The idea of the proof is simple but elegant. Let

$$f_i(z) = a_{i1}z^{n-1} + a_{i2}z^{n-2} + \ldots + a_{in}, \quad i = 1, 2, \ldots, n,$$

be n polynomials of degree at most $n-1$. Then

$$\begin{aligned}
\det\left(f_i(x_j)\right) &= \det\begin{pmatrix} f_1(x_1) & f_1(x_2) & \ldots & f_1(x_n) \\ f_2(x_1) & f_2(x_2) & \ldots & f_2(x_n) \\ \vdots & \vdots & \vdots & \vdots \\ f_n(x_1) & f_n(x_2) & \ldots & f_n(x_n) \end{pmatrix} \\
&= \det\left(\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}\begin{pmatrix} x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \\ x_1^{n-2} & x_2^{n-2} & \ldots & x_n^{n-2} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & \ldots & 1 \end{pmatrix}\right) \\
&= \det(a_{ij}) \cdot V(x),
\end{aligned}$$

where $V(x)$ is the determinant of the Vandermonde matrix, which has value $\prod_{i<j}(x_i - x_j)$.

If we choose $f_i(z)$ to be a polynomial of degree $n-i$, then the matrix (a_{ij}) is upper triangular. This will be the case if we set

$$f_i(z) = \prod_{0 \le k < n-i}(z - k),$$

i.e., $f_i(z) = z \cdot (z-1) \cdots (z - (n-i-1))$, for $1 \le i \le n-1$, and $f_n(z) = 1$. In this case, the matrix (a_{ij}) not only is upper triangular, but also has 1's on the diagonal, thus $\det(a_{ij}) = 1$, and we get

$$\det\left(f_i(x_j)\right) = \prod_{i<j}(x_i - x_j).$$

Note that $f_i(\ell_j) = \ell_j!/(\ell_j - e_i)!$. The Proposition follows by taking the transpose.

Corollary 3.1 *For any sequence of integers $a_1, a_2, \ldots, a_n$,*

$$\det\left(\binom{a_i}{n-j}\right)_{1\le i,j\le n} = \frac{\prod_{i<j}(a_i-a_j)}{0!1!\cdots(n-1)!}, \tag{1}$$

and

$$\det\left(\binom{a_i}{j}\right)_{1\le i\le n, 0\le j\le n-1} = \frac{\prod_{i>j}(a_i-a_j)}{0!1!\cdots(n-1)!}. \tag{2}$$

Note that $\binom{a_i}{n-j} = \frac{a_i!}{(a_i-e_j)!e_j!}$, as $e_j = n-j$. Equality (1) follows. The matrix in the second equality (2) is just an involution of all the columns in the matrix of (1) (with respect to the central vertical line).

Corollary 3.2 *For any sequence of integers $a_0, a_1, \ldots, a_{n-1}$, and integer $c \ge 0$,*

$$\det\left(\binom{a_j}{c+i}\right)_{0\le i,j\le n-1} = \det\left(\binom{a_i}{c+j}\right)_{0\le i,j\le n-1} \tag{3}$$

$$= \binom{a_0}{c}\cdots\binom{a_{n-1}}{c}\frac{(c!)^n}{c!\cdots(c+n-1)!}\prod_{i>j}(a_i-a_j), \tag{4}$$

The proof is a simple induction, using the fact that $\binom{a}{b} = \frac{a}{b}\binom{a-1}{b-1}$, for $b > 0$.

4 Generalized Toda Polynomials

In [7], Toda proved the following:

Theorem 4.1 (Toda) *For all $k \ge 1$, there exists a polynomial $f(x) \in \mathbf{Z}[x]$ of degree 4^k, such that,*

1. *all coefficients of $f(x)$ are non-negative integers;*
2. *$f(x) \in (x^{2^k})$, the ideal generated by x^{2^k}; in other words, all coefficients of x^j in $f(x)$ vanish, for $j < 2^k$.*
3. *if we write $f(x)+1 = g(x+1)$, then $g(x) \in (x^{2^k})$; thus all coefficients of x^j in $g(x)$ vanish, for $j < 2^k$.*

Toda obtained his polynomials by self-composing k times the polynomial $3x^4 + 4x^3$. We show the following generalization:

Theorem 4.2 *For all $k \geq 1$, there exists a polynomial $f(x) \in \mathbf{Z}[x]$ of degree $2k$, such that,*

1. *all coefficients of $f(x)$ are non-negative integers;*
2. *$f(x) \in (x^k)$, the ideal generated by x^k; in other words, all coefficients of x^j in $f(x)$ vanish, for $j < k$.*
3. *if we write $f(x) + 1 = g(x+1)$, then $g(x) \in (x^k)$; thus all coefficients of x^j in $g(x)$ vanish, for $j < k$.*

This f has the following modulus amplification property.

Corollary 4.1 *For all integers n, m and $\ell \geq 1$, if $n \equiv 0 \bmod m^\ell$ then $f(n) \equiv 0 \bmod m^{k\ell}$. And similarly, if $n \equiv -1 \bmod m^\ell$ then $f(n) \equiv -1 \bmod m^{k\ell}$.*

We now give a proof of the theorem.

Write $g(x) = a_0 x^k + \cdots + a_k x^{2k}$. Let's collect the coefficients of x^j in

$$\begin{aligned} g(x+1) - 1 &= \sum_{i=0}^{k} a_i (x+1)^{k+i} - 1 \\ &= \sum_{i=0}^{k} a_i \sum_{j=0}^{k+i} \binom{k+i}{j} x^j - 1 \\ &= \sum_j \left(\sum_{i=0}^{k} \binom{k+i}{j} a_i \right) x^j - 1 \end{aligned}$$

(We take the convention that $\binom{n}{x} = 0$ if $x < 0$ or $x > n$.)

The theorem is equivalent to the existence of integer solutions $a_0, \ldots, a_k$ to the following system of equations and inequalities.

$$\begin{aligned} \sum_i a_i &= 1 \\ \sum_i \binom{k+i}{j} a_i &= 0 \qquad \text{if } 0 < j < k \\ \sum_i \binom{k+i}{j} a_i &\geq 0 \qquad \text{if } k \leq j < 2k \quad \text{and} > 0 \text{ if } j = 2k \end{aligned}$$

Let us consider the first k equations, on $a_0, \ldots, a_{k-1}$. The determinant of the coefficient matrix is

$$\det \begin{pmatrix} \binom{k}{0} & \binom{k+1}{0} & \cdots & \binom{k+k-1}{0} \\ \binom{k}{1} & \binom{k+1}{1} & \cdots & \binom{k+k-1}{1} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{k}{k-1} & \binom{k+1}{k-1} & \cdots & \binom{k+k-1}{k-1} \end{pmatrix}.$$

In Corollary 3.1 we set $n = k$ and $a_i = k + i$, we find

$$\det \left(\binom{k+i}{j} \right)_{0 \le i,j \le k-1} = 1.$$

The right hand side of the first k equations is

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} - a_k \begin{pmatrix} \binom{2k}{0} \\ \binom{2k}{1} \\ \vdots \\ \binom{2k}{k-1} \end{pmatrix}.$$

Hence, the solution in terms of a_k to the first k equations has the form $a_i = \alpha_i a_k + \beta_i$, $0 \le i < k$, where α_i and β_i are integers given by

$$\alpha_i = -\det \begin{pmatrix} \binom{k}{0} & \cdots & \binom{k+i-1}{0} & \binom{2k}{0} & \binom{k+i+1}{0} & \cdots & \binom{k+k-1}{0} \\ \binom{k}{1} & \cdots & \binom{k+i-1}{1} & \binom{2k}{1} & \binom{k+i+1}{1} & \cdots & \binom{k+k-1}{1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \binom{k}{k-1} & \cdots & \binom{k+i-1}{k-1} & \binom{2k}{0} & \binom{k+i+1}{k-1} & \cdots & \binom{k+k-1}{k-1} \end{pmatrix},$$

and

$$\beta_i = (-1)^i \det \begin{pmatrix} \binom{k}{1} & \cdots & \binom{k+i-1}{1} & \binom{k+i+1}{1} & \cdots & \binom{k+k-1}{1} \\ \binom{k}{2} & \cdots & \binom{k+i-1}{2} & \binom{k+i+1}{2} & \cdots & \binom{k+k-1}{2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \binom{k}{k-1} & \cdots & \binom{k+i-1}{k-1} & \binom{k+i+1}{k-1} & \cdots & \binom{k+k-1}{k-1} \end{pmatrix}.$$

For α_i we set $n = k$ and

$$a_i = k + 0, k + 1, \ldots, k + i - 1, 2k, k + i + 1, \ldots, 2k - 1$$

in Corollary 3.1; for β_i we set $n = k - 1$, $c = 1$ and

$$a_i = k + 0, k + 1, \ldots, k + i - 1, k + i + 1, \ldots, 2k - 1$$

in Corollary 3.2, respectively.

After collecting terms, we get

$$a_i = (-1)^{k+i}\binom{k}{i}a_k + (-1)^i \frac{k}{k+i}\binom{k-1}{i}\binom{2k-1}{k}, \quad 0 \leq i < k.$$

This formula is also valid for $i = k$.

We claim that, with these values of a_i,

$$\begin{aligned} \sum_{i=0}^{k} a_i &= 1, \\ \sum_{i=0}^{k}\binom{k+i}{j}a_i &= \binom{k}{j-k}\left[a_k + (-1)^{k-1}\binom{2k-1}{k}\frac{2k-j}{j}\right], \quad 0 < j \leq 2k. \end{aligned}$$

Note that $\binom{k}{j-k} = 0$ for $0 < j < k$. For $k \leq j < 2k$, the right hand sides are all nonnegative if $a_k \geq \binom{2k-1}{k}$, and positive for $j = 2k$.

The following formulae from [4] will be useful (p.188 (5.41) and p.169 (5.24)):

$$\sum_i \binom{n}{i}\frac{(-1)^i}{x+i} = \frac{1}{x \cdot \binom{x+n}{n}}, \quad x \neq 0, -1, \ldots, -n. \tag{5}$$

and

$$\sum_i \binom{\ell}{m+i}\binom{s+i}{n}(-1)^i = (-1)^{\ell+m}\binom{s-m}{n-\ell}, \quad \ell, m, n \text{ are integers}, \ell \geq 0. \tag{6}$$

For $j = 0$, we use (5),

$$\begin{aligned} \sum_{i=0}^{k} a_i &= \sum_{i=0}^{k}\left[(-1)^{k+i}\binom{k}{i}a_k + (-1)^i\frac{k}{k+i}\binom{k-1}{i}\binom{2k-1}{k}\right] \\ &= a_k\left[(-1)^k\sum_{i=0}^{k}(-1)^i\binom{k}{i}\right] + k\binom{2k-1}{k}\sum_{i=0}^{k}\binom{k-1}{i}\frac{(-1)^i}{k+i} \\ &= 0 + k\binom{2k-1}{k} \cdot \frac{1}{k \cdot \binom{k+k-1}{k-1}} \\ &= 1. \end{aligned}$$

For $0 < j \leq 2k$,

$$\sum_{i=0}^{k} \binom{k+i}{j} a_i = \sum_i \binom{k+i}{j} \left[(-1)^{k+i} \binom{k}{i} a_k + (-1)^i \frac{k}{k+i} \binom{k-1}{i} \binom{2k-1}{k} \right]$$

The coefficient of a_k is

$$(-1)^k (-1)^{k+0} \binom{k-0}{j-k} = \binom{k}{j-k},$$

by setting in (6) $\ell = k$, $s = k$, $m = 0$ and $n = j$.

The constant term is the product of $\binom{2k-1}{k}$ with

$$\begin{aligned} \sum_{i=0}^{k} \binom{k-1}{i} \binom{k+i}{j} (-1)^i \frac{k}{k+i} &= k \sum_i \binom{k-1}{i} \binom{k+i-1}{j-1} \frac{1}{j} (-1)^i \\ &= \frac{k}{j} (-1)^{k-1+0} \binom{(k-1)-0}{(j-1)-(k-1)} \\ &= \frac{k}{j} (-1)^{k-1} \binom{k-1}{j-k}, \end{aligned}$$

by setting in (6) $\ell = k-1$, $s = k-1$, $m = 0$ and $n = j-1$.

Finally note that $\binom{k-1}{j-k} = 0$ for $j < k$. For $k \leq j \leq 2k$,

$$\binom{k-1}{j-k} = \binom{k-1}{2k-j-1} = \binom{k}{2k-j} \frac{2k-j}{k} = \binom{k}{j-k} \frac{2k-j}{k},$$

so the constant term is always

$$\binom{k}{j-k} (-1)^{k-1} \binom{2k-1}{k} \frac{2k-j}{k},$$

for $0 < j \leq 2k$.

QED

We have found all solutions to the requirements of Theorem 4.2.

Acknowledgment

I thank Peter Hajnal, Ioan Macarie, Mitsu Ogihara, D. Sivakumar for interesting discussions.

References

[1] R. Beigel and J. Tauri, "On ACC", Proc. of the *32nd Annual Symposium on Foundations of Computer Science*, pp 783–792, 1991.

[2] W. Feit, *Characters of Finite Groups*, Benjamin, New York, 1967.

[3] G. Frobenius, "Über die Charaktere der symmetrischen Gruppe. Sitz. Ber. Preuss. Akad. Berlin (1900), 516–534.

[4] R. Graham, D. Knuth and O. Patashnik, *Concrete Mathematics*, Addison-Wesley Publishing Company. First Edition, third printing, May 1989.

[5] W. Ledermann, *Introduction to Group Characters*, Cambridge University Press, Cambridge, Second Edition, 1987.

[6] K. Mulmuley, U. Vazirani and V. Vazirani, "Matching is as Easy as Matrix Inversion", Proc. of the *19th Annual Symposium on Theory of Computing*, 1987, pp 345–354.

[7] S. Toda, "On the computational power of PP and $\oplus$ P", Proc. of the *30th Annual Symposium on Foundations of Computer Science*, pp 514–519, 1989.

[8] L. G. Valiant and V. V. Vazirani, "NP is as easy as detecting unique solutions", *Theoretical Computer Science*, 47, pp 85–93, 1986.

[9] A. Wigderson, "NL/poly $\subseteq$ $\oplus$L/poly", Proc. of the *Ninth Annual Conference of Structure in Complexity Theory*, pp 59–62.

[10] A. Yao, "On ACC and threshold circuits", Proc. of the *31th Annual Symposium on Foundations of Computer Science*, pp 619–627, 1990.