

On the distribution of coefficients of powers of positive polynomials

LÁSZLÓ MAJOR

*Institute of Mathematics
Tampere University of Technology
PL 553, 33101 Tampere
Finland
laszlo.major@tut.fi*

Abstract

Using the formalism of polynomials with positive coefficients, the fact that exactly half of all subsets of a finite set have even cardinality can be generalized asymptotically.

The well-known fact that every finite nonempty set has as many subsets of even cardinality as of odd cardinality can be restated as follows. If d denotes the particular integer 2, then for any integers $0 \leq j \leq d - 1$, $n \geq 1$ and the standard expansion $c_{n,0} + c_{n,1}x + c_{n,2}x^2 + \cdots$ of the polynomial $(\frac{1}{2} + \frac{1}{2}x)^n$ we have

$$\sum_{k \equiv j \pmod{d}} c_{n,k} = \frac{1}{d}.$$

For $n = 0$ this obviously fails. It also fails in general if $d \geq 3$. We will show however, that it remains asymptotically true for all $d \geq 2$ and not only for the polynomial $\frac{1}{2} + \frac{1}{2}x$, but for any polynomial with positive coefficients summing to 1 (Theorem 1). In particular, this will imply that summing up every d^{th} entry in the n^{th} row in Pascal's triangle asymptotically yields $2^n/d$.

Questions of distribution about powers of polynomials with positive coefficients, in connection with binomial and multinomial coefficients in particular, have been studied both by classical and contemporary authors. When Euler (1765) was investigating the properties of the trinomial coefficients (see Andrews [1]), he obtained a unimodal distribution of the coefficients by expanding the n^{th} power of the polynomial $1 + x + x^2$. In the analogous case of the polynomial $1 + x$ the corresponding unimodal distribution is the n^{th} row of Pascal's triangle. Further results and references concerning the powers of the polynomial $1 + x$ can be found in Marcus and Tuncel [6]. In general the distribution of the coefficients of the n^{th} power of the polynomial $p = p_0 + p_1x + \cdots + p_mx^m$ with nonnegative real coefficients is not necessarily

unimodal, but some sufficient conditions for unimodality of powers of polynomials are given by Odlyzko and Richmond [7] and by De Angelis [2]. In this paper we are concerned with a question of equidistribution of coefficients. The main result is Theorem 1. The lemmas and corollary provide background and an extension.

Let $d \geq 2$ be a fixed positive integer. Let $r(p)$ denote the remainder of the division of the polynomial p by $x^d - 1$, i.e. that unique polynomial of degree less than d for which the polynomial p is congruent to $r(p)$ modulo $x^d - 1$. A polynomial with positive (nonnegative) real coefficients is said to be *positive (nonnegative)* polynomial. The following Lemma provides a sufficient condition for the powers of a nonnegative polynomial p to have positive remainder by $x^d - 1$.

Lemma 1 *Let $p \in \mathbb{R}[x]$ be a nonnegative, nonzero polynomial. For any $q \in \mathbb{R}[x]$ and $i \in \mathbb{N}$ let q_i denote the coefficient of x^i in q . If there exist $k, l \in \{0, \dots, d-1\}$ such that $r(p)_k > 0$, $r(p)_l > 0$ and $\gcd(d, k-l) = 1$, then $r(p^n)$ is a positive polynomial for all integer $n > d-1$.*

Proof: It can be assumed that $k < l$. Let us denote the difference $l - k$ by h . It is easy to see that if $r((x^k + x^l)^{d-1})$ is positive then also $r(p^{d-1})$ is positive. In addition, $r((x^k + x^l)^{d-1}) = r(x^{k(d-1)}(1 + x^h)^{d-1})$ is positive if $r((1 + x^h)^{d-1})$ is positive, so let us concentrate on the polynomial $r((1 + x^h)^{d-1})$. We expand the expression $(1 + x^h)^{d-1}$ in the polynomial ring $\mathbb{R}[x]$ by using the Binomial Theorem:

$$(1 + x^h)^{d-1} = \sum_{i=0}^{d-1} \binom{d-1}{i} (x^{hi}). \quad (0.1)$$

Let us assume that the following congruence holds for some $i, j \in \{0, \dots, d-1\}$:

$$\binom{d-1}{i} (x^{hi}) \equiv \binom{d-1}{j} (x^{hj}) \pmod{x^d - 1}. \quad (0.2)$$

From the equation (0.2) it follows that $hi - hj$ is divisible by d . But it was assumed that $\gcd(h, d) = 1$, so consequently $i = j$. Therefore $r((1 + x^h)^{d-1})$ has exactly d different nonzero coefficients, so in other words it is positive and consequently $r(p^{d-1})$ is also positive.

It can be shown without difficulty that for any $n \geq d-1$, the remainder $r(p^n)$ is positive if $r(p^{d-1})$ is positive. \square

In order to be able to deal more efficiently with powers of polynomials we need the concept and some useful properties of *circulant matrices*. For a classical reference see e.g. Davis [3]. Let $v = (v_0, v_1, \dots, v_{d-1})$ be a row vector in \mathbb{R}^d . The permutation $\rho: \mathbb{R}^d \rightarrow \mathbb{R}^d$ given by

$$\rho(v_0, v_1, \dots, v_{d-1}) = (v_{d-1}, v_0, \dots, v_{d-2})$$

is called a *cyclic permutation*. The *circulant matrix* associated to the vector v is the $d \times d$ matrix whose i^{th} row is $\rho^{i-1}(v)$, $i = 1, \dots, d$ and it is denoted by

$$C = \text{circ}(v_0, v_1, \dots, v_{d-1}) = \text{circ}(v).$$

The product of two circulant matrices is circulant, therefore any positive integer power of a circulant matrix is circulant. We shall use the connection between powers of circulant matrices and the powers of residue polynomials. If $a = (a_0, a_1, \dots, a_{d-1})$ is the coefficient vector of some polynomial $r(p) \in \mathbb{R}[x]$, then the first row of $(\text{circ}(a))^n$ is the coefficient vector of $r(p^n)$. Lally and Fitzpatrick [5] give a general overview in this subject.

A matrix is called *positive (nonnegative)* if all its entries are positive (nonnegative) real numbers. A $d \times d$ nonnegative matrix M is said to be *doubly stochastic* if the sum of the entries in each row and in each column equals 1. The product of doubly stochastic matrices is doubly stochastic. The following lemma follows from a general result on eigenvectors of positive matrices, Theorem 8.2.8 in Horn and Johnson [4]. Here we provide a direct proof. A matrix whose entries are all ones will be denoted by U .

Lemma 2 *If M is a $d \times d$ positive doubly stochastic matrix, then*

$$\lim_{n \rightarrow \infty} M^n = \frac{1}{d}U. \tag{0.3}$$

Proof: Let us denote the doubly stochastic matrix $\frac{1}{d}U$ by J . If $M = J$, then the statement is trivial. Otherwise the matrix M can be given in the following form:

$$M = \lambda J + (1 - \lambda)M_0, \tag{0.4}$$

where $0 < \lambda < 1$ and M_0 is a doubly stochastic matrix. Let us write the n^{th} power of M by using the Binomial Theorem and the fact that $JD = DJ = J$ for all doubly stochastic matrix D ,

$$\begin{aligned} M^n &= \sum_{i=0}^n \binom{n}{i} (\lambda J)^{n-i} ((1 - \lambda)M_0)^i = (1 - \lambda)^n M_0^n + J \sum_{i=0}^{n-1} \binom{n}{i} \lambda^{n-i} (1 - \lambda)^i \\ &= (1 - \lambda)^n M_0^n + J(1 - (1 - \lambda)^n) = (1 - \lambda)^n (M_0^n - J) + J \end{aligned}$$

From the above expression follows our statement, because $0 < 1 - \lambda < 1$ and consequently $\lim_{n \rightarrow \infty} (1 - \lambda)^n = 0$. □

In order that the Lemma 2 could be applied for the powers of polynomials, we shall restrict our attention to polynomials p whose coefficients sum to 1 ($p(1) = 1$). We may do this without loss of generality, because all polynomials can be written in the form $p = p(1) \cdot p'$, where p' has the mentioned property. It can also be said that the coefficients of p' form a *stochastic vector*. Clearly the sum of the coefficients of $(p')^n$ is also 1 and the sum of the coefficients of p^n is equal to $p(1)^n$. By using Lemma 1, Lemma 2 and the connection between powers of circulant matrices and the powers of residue polynomials we obtain the following theorem:

Theorem 1 *Let p be a nonconstant polynomial with positive real coefficients summing to 1 and $d \geq 2$ a fixed integer. Then for all $0 \leq j \leq d - 1$*

$$\lim_{n \rightarrow \infty} \sum_{k \equiv j \pmod d} (p^n)_k = \frac{1}{d} \tag{0.5}$$

where $(p^n)_0 + (p^n)_1x + (p^n)_2x^2 + \dots$ is the standard expansion of p^n . □

The restriction that p is positive is quite strong. Theorem 1 can be extended to larger classes of polynomials. For instance the following corollary applies Lemma 1 so as to provide such an extension.

Corollary 1 *Let $d \geq 2$ a fixed integer. If the nonnegative polynomial p satisfies the conditions of Lemma 1 and its coefficients sum to 1, then the convergence (0.5) holds for p , or equivalently, for all $0 \leq j \leq d - 1$*

$$\lim_{n \rightarrow \infty} r(p^n)_j = \frac{1}{d},$$

where $r(p^n)_j$ denotes the coefficient of x^j in the remainder of p^n modulo $x^d - 1$.

Proof: Let p be a polynomial satisfying the conditions of Lemma 1 and let $p(1) = 1$. Let us denote the coefficient vector of $r(p)$ by c and the circulant matrix $\text{circ}(c)$ by C . By Lemma 1 if $m \geq d - 1$ then C^m is a positive matrix. We use J to denote the $d \times d$ matrix in which every entry is $\frac{1}{d}$. By Lemma 2, $\lim_{n \rightarrow \infty} C^{(d-1)n} = J$. We may also express this fact by using the max norm of matrices:

$$\lim_{n \rightarrow \infty} \|C^{(d-1)n} - J\| = 0.$$

We show that for all $0 \leq i \leq d - 1$, $\lim_{n \rightarrow \infty} C^{(d-1)n+i} = J$. We recall that $J C^i = J$, so we have

$$\|C^{(d-1)n} C^i - J\| = \|C^{(d-1)n} C^i - J C^i\| \leq \|C^{(d-1)n} - J\| \cdot \|C^i\|. \tag{0.6}$$

Because $\|C^i\|$ is a constant, we obtain that $\lim_{n \rightarrow \infty} C^{(d-1)n+i} = J$ for all $0 \leq i \leq d - 1$, consequently $C^m \rightarrow J$ as m tends to infinity. □

Application to Pascal’s triangle For any $d \geq 2$ we can extract from the n^{th} row of Pascal’s triangle $\binom{n}{0}, \dots, \binom{n}{n}$, d disjoint subsequences, one for each $j = 0, \dots, d - 1$:

$$\binom{n}{j}, \binom{n}{j+d}, \binom{n}{j+2d}, \dots$$

It follows from Theorem 1 that the d different sums $\binom{n}{j} + \binom{n}{j+d} + \binom{n}{j+2d} + \dots$ are asymptotically equal to $2^n/d$ as $n \rightarrow \infty$.

Acknowledgement

I would like to express my sincere gratitude to the referee for the remarks and for the valuable advice concerning the references.

References

- [1] G.E. ANDREWS, Euler's "Exemplum Memorabile Inductionis Fallacis" and q -Trinomial Coefficients, *J. Amer. Math. Soc.* **3** (1990), 653–669.
- [2] V. DE ANGELIS, Asymptotic expansions and positivity of coefficients for large powers of analytic functions, *Int. J. Math. Math. Sc.* **2003** (16) (2003), 1003–1025.
- [3] P.J. DAVIS, *Circulant Matrices*, John Wiley and Sons, 1979.
- [4] R.A. HORN AND C.R. JOHNSON, *Matrix Analysis*, Cambridge University Press, 1991.
- [5] K. LALLY AND P. FITZPATRICK, Algebraic Structure of Quasicyclic Codes, *Discrete Appl. Math.* **111** (2001), 157–175.
- [6] B. MARCUS AND S. TUNCEL, Matrices of polynomials, positivity, and finite equivalence of Markov chains, *J. Amer. Math. Soc.* **6** (1993), 131–147.
- [7] M. ODLYZKO AND L.B. RICHMOND, On the unimodality of high convolutions of discrete distributions, *Ann. Probab.* **13** (1985), 299–306.

(Received 5 July 2010; revised 4 Nov 2010)