Periodicity in quasipolynomial convolution

Thomas Zaslavsky*

Department of Mathematical Sciences
Binghamton University of SUNY
Binghamton, NY 13902-6000, U.S.A.
zaslav@math.binghamton.edu

Submitted: Jul 15, 2004; Accepted: Nov 12, 2004; Published: Nov 22, 2004
Mathematics Subject Classifications:
Primary 39A12, 44A35; *Secondary* 05A15, 11D04, 11D45, 15A18, 52B20
Keywords: quasipolynomial, convolution, period, degree, circulant matrix, null space, semimagic square, Frobenius coin problem.

Abstract

The leading term of a convolution of quasipolynomials with periods p and q is periodic with period $\gcd(p, q)$, smaller than expected. The degree of the convolution is usually $d+e+1$; we characterize the exceptions. To do this we need to characterize the null space of a circulant matrix.

We wish to point out a simple yet unexpected property of quasipolynomial calculus. A *quasipolynomial* is a function of positive integers that is given by a cyclically repeating sequence of polynomials; that is,

$$f(t) = \sum_{k=0}^{d} a_{t,k} t^k \qquad \text{for } t = 1, 2, 3, \dots,$$

where the coefficient $a_{t,k}$ is a periodic function of t for each k. Suppose $a_{t,k}$ cycles with period p_k; then $p := \operatorname{lcm}(p_0, p_1, \dots, p_d)$ is the *period* of f, meaning that $f(t) = f_t(t)$ where $f_1, f_2, \dots$ is a sequence of polynomials, $f_{t+p} = f_t$ for all t, and p is the smallest positive number for which that is so. The *degree* of f is the largest degree of any f_t. A quasipolynomial function extends to all integers, but we shall not need that fact. It is well known that a quasipolynomial is a function of positive integers whose generating function

$$\mathbf{G}_f(x) := \sum_{t \geq 1} f(t) x^t$$

*Research supported by the SGPNR.

is a rational function with denominator $(1-x^p)^{d+1}$ and with numerator of the form $x\varphi(x)$ where $\deg(\varphi) < p(d+1)$. (See [7, Section 4.4]; slight adjustments are needed because Stanley's quasipolynomials are defined for $t \geq 0$.)

We are interested in concocting a new function F by what might be called discrete integration or, in general, convolution. Here is a simple example:

$$F(t) := f(t-q) + f(t-2q) + \cdots = \sum_{\substack{0<s<t \\ s\equiv t \bmod q}} f(s). \tag{1}$$

This example arises in the course of counting semimagic squares [3, 4]. Another example, from counting the same squares in a different way, has the form

$$F(t) := \sum_{0<s<t} (t-s-1)f(s). \tag{2}$$

These are examples of convolution of quasipolynomials:

$$F(t) := \sum_{0<s<t} f(s)g(t-s). \tag{3}$$

In (1), g is the function 1_q defined by $1_q(r) := 1$ if $q \mid r$ and 0 if not, while in (2), $g(r) = r-1$.

It is obvious that F has degree at most $d+e+1$ where $d := \deg f$ and $e := \deg g$, and that the period of F divides the least common multiple $l := \operatorname{lcm}(p,q)$ of the periods p of f and q of g; for letting

$$\mathbf{G}_f(x) = \frac{x\varphi(x)}{(1-x^p)^{d+1}} \text{ and } \mathbf{G}_g(x) = \frac{x\psi(x)}{(1-x^q)^{e+1}} \ ,$$

then

$$\mathbf{G}_F(x) = \mathbf{G}_f(x)\mathbf{G}_g(x) = \frac{x^2\varphi(x)\psi(x)}{(1-x^p)^{d+1}(1-x^q)^{e+1}} = \frac{x\Phi(x)}{(1-x^l)^{d+e+2}}$$

where Φ is a polynomial of degree less than $(d+e+2)l$.

It is not as obvious, and seems not to have been noticed before, that the coefficient of t^{d+e+1} in F has period that divides the greatest common divisor $\gcd(p,q)$. (That is not necessarily so for lower coefficients.) We formulate this in a slightly stronger way as a theorem. Additional notation:

$$g(t) = \sum_{k=0}^{e} b_{t,k}t^k, \qquad F(t) = \sum_{k=0}^{d+e+1} c_{t,k}t^k,$$

and $q_k :=$ period of $b_{t,k}$, $P_k :=$ period of $c_{t,k}$, as functions of t with k held fixed.

Theorem 1 *P_{d+e+1} divides $\gcd(p_d, q_e)$, and in general*

$$P_k \mid \operatorname{lcm}\big\{p_{k+1},\dots,p_d,q_{k+1},\dots,q_e,\gcd(p_l,q_m) : l+m=k \text{ with } 0\leq l\leq d,\ 0\leq m\leq e\big\}.$$

Proof. For the first part it suffices to consider quasipolynomials $f(t) = a_t t^d$ and $g(t) = b_t t^e$ with periods p and q, respectively. The coefficient c_{d+e+1} is easily seen to be a positive constant times

$$\gamma_t := \sum_{\sigma=0}^{l-1} a_\sigma b_{t-\sigma}$$

(taking subscripts modulo l). An obvious period of γ_t is q. Another is p, since

$$\sum_\sigma a_\sigma b_{t+p-\sigma} = \sum_\sigma a_{\sigma-p} b_{t-(\sigma-p)} = \sum_\sigma a_\sigma b_{t-\sigma}.$$

Thus, $\gcd(p, q)$ is a period.

The second part follows by routine calculations. ∎

Thus, for example, in F the coefficient of t^{d+e+1} is constant if g is a polynomial, or if f has constant leading coefficient, as when f is the Ehrhart quasipolynomial of a rational polytope [7, Section 4.6, pp. 235ff.].

One might call c_{d+e+1} the *generic leading coefficient* of F because, although in general it is the leading coefficient, it could be identically zero. We give two simple criteria for this to occur. In $\mathbb{C}^n$ let

$$\eta_n^{(j)} := (1, \omega^j, \omega^{2j}, \ldots, \omega^{(n-1)j})$$

where ω is a primitive nth root of unity. The *circulant matrix* of $a \in \mathbb{C}^n$ is

$$\mathrm{Circ}(a) := \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & \cdots & a_{n-2} \\ \vdots & \vdots & & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}.$$

Theorem 2 *Let n be any multiple of $\mathrm{lcm}(p_d, q_e)$ and let $k := \gcd(p_d, q_e)$. The following properties of F are equivalent:*

(i) F has degree less than $d + e + 1$.

(ii) $a := (a_{d,1}, a_{d,2}, \ldots, a_{d,n})$ and $b := (b_{e,1}, b_{e,2}, \ldots, b_{e,n})$ belong to subspaces generated by complementary subsets of $\{\eta_n^{(j)}\}_{j=0}^{n-1}$ in $\mathbb{C}^n$.

(iii) $\hat{a} := (\hat{a}_{d,1}, \hat{a}_{d,2}, \ldots, \hat{a}_{d,k})$ and $\hat{b} := (\hat{b}_{e,1}, \hat{b}_{e,2}, \ldots, \hat{b}_{e,k})$ belong to subspaces generated by complementary subsets of $\{\eta_k^{(j)}\}_{j=0}^{k-1}$ in $\mathbb{C}^k$, where

$$\hat{a}_j := a_j + a_{j+k} + \cdots + a_{j+(p-k)} \quad \text{and} \quad \hat{b}_j := b_j + b_{j+k} + \cdots + b_{j+(q-k)}.$$

Proof. We apply Lemma 3 to deduce equivalence of (i) and (ii). The proof that (i) and (iii) are equivalent is similar but it begins by noting that $(\mathrm{Circ}\, b^*)a^{\mathrm{T}} = 0 \iff (\mathrm{Circ}\, \hat{b}^*)\hat{a}^{\mathrm{T}} = 0$ due to Theorem 1. ∎

If $b = (b_0, b_1, \ldots, b_{n-1}) \in \mathbb{C}^n$, define

$$b^* := (b_{n-1}, \ldots, b_1, b_0).$$

Also, from now on $\eta^{(j)}$ denotes $\eta_n^{(j)}$.

Lemma 3 *For vectors $a, b \in \mathbb{C}^n$, and taking subscripts modulo n, we have $a^{\mathrm{T}} \in \operatorname{Nul} \operatorname{Circ}(b^*)$ $\iff$ $b^{\mathrm{T}} \in \operatorname{Nul} \operatorname{Circ}(a^*)$ $\iff$ $\sum_{\sigma=0}^{n-1} a_\sigma b_{\tau-\sigma} = 0$ for all $\tau = 0, 1, \ldots, n-1$ $\iff$ a and b belong to subspaces generated by complementary subsets of $\{\eta^{(j)}\}_{j=0}^{n-1}$.*

First Proof. The set $\{\eta^{(j)}\}_{j=0}^{n-1}$ is a basis of $\mathbb{C}^n$. We can therefore write $a = \sum_{j=0}^{n-1} \alpha_j \eta^{(j)}$ and $b = \sum_{j=0}^{n-1} \beta_j \eta^{(j)}$. Then

$$\sum_\sigma a_\sigma b_{\tau-\sigma} = \sum_\sigma \sum_j \alpha_j \omega^{j\sigma} \sum_k \beta_k \omega^{k(\tau-\sigma)} = \sum_j \sum_k \alpha_j \beta_k \omega^{k\tau} \zeta(\omega^{j-k})$$

where $\zeta(x) := 1 + x + \cdots + x^{n-1}$. But $\zeta(\omega^m) = 0$ if $0 < m < n$, so

$$\sum_\sigma a_\sigma b_{\tau-\sigma} = n \sum_k \alpha_k \beta_k \omega^{k\tau}.$$

Now define the polynomial $\theta(x) := \sum_{k=0}^{n-1} \alpha_k \beta_k x^k$. We have shown that $\sum_\sigma a_\sigma b_{\tau-\sigma} = 0$ if and only if ω^τ is a zero of θ. It follows that, if $\sum_\sigma a_\sigma b_{\tau-\sigma} = 0$ for all τ, then θ is identically zero; that is, for each $k = 0, 1, \ldots, n-1$, either α_k or β_k equals 0; and the converse is obvious. That proves the lemma. ∎

Let $\Omega(a)$ be the smallest subset of $\{\eta^{(j)}\}_{j=0}^{n-1}$ required to span a and $\Omega^c(a)$ its complementary subset. That is, $\Omega^c(a) = \{\eta^{(j)} : a \cdot \eta^{(j)} = 0\}$, the dot denoting the standard Hermitian inner product. Then

$$\operatorname{Nul} \operatorname{Circ}(a^*) = \langle \Omega^c(a) \rangle, \tag{4}$$

the linear span of $\Omega^c(a)$, by Lemma 3.

Second Proof. The set $\{\eta^{(j)}\}_{j=0}^{n-1}$ is an orthogonal basis of eigenvectors of any circulant matrix of order n; see [5]. The fact that $\operatorname{Circ}(a)\eta^{(j)} = (a \cdot \eta^{(-j)})\eta^{(j)}$ shows that $\eta^{(j)}$ is an eigenvector of $\operatorname{Circ}(a)$ $\iff$ $a \cdot \eta^{(-j)} = 0$ $\iff$ $\eta^{(-j)} \in \Omega^c(a)$ $\iff$ $\eta^{(j)} \in \overline{\Omega^c(a)}$, the set of complex conjugates of vectors in $\Omega^c(a)$. Hence, $\langle \overline{\Omega^c(a)} \rangle \subseteq \operatorname{Nul} \operatorname{Circ}(a)$. The eigenvalues of $\operatorname{Circ}(a)$ being the numbers $a \cdot \eta^{(-j)}$, we see that $\dim \operatorname{Nul} \operatorname{Circ}(a) = |\Omega^c(a)|$, whence

$$\operatorname{Nul} \operatorname{Circ}(a) = \langle \overline{\Omega^c(a)} \rangle.$$

Now, $a^* \cdot \eta^{(j)} = \omega^{-j}(a \cdot \eta^{(-j)})$, so $\Omega^c(a^*) = \overline{\Omega^c(a)}$, thus (4) holds and the lemma follows. ∎

Suppose f fixed in the convolution (3), and fix n to be a multiple of p. Since $|\Omega(a)|$ is independent of n, in the vector space of quasipolynomials g of period dividing n, the subspace of those for which $\deg F \leq d + e$ has codimension $|\Omega(a)|$.

In some cases it is obvious without Theorem 2 that $\deg F = d + e + 1$. For instance, of the leading coefficients of f and g, one may be constant and the other nonnegative—as for instance in Equation (1) when f has constant leading term.

That is the situation in the enumeration of semimagic squares in [3]. Such a square is a $q \times q$ array of positive integers, all different, in which every row and column has the same sum, called the *magic sum*. Every semimagic square can be normalized by permuting rows and columns so that $x_{11} = \min x_{jk}$, the top row and left column are increasing, and (by a diagonal reflection if needed) $x_{21} > x_{12}$. By subtracting x_{11} from every entry we get a *supernomalized* square, which is positive except in the top left corner. Let $F(t)$ be the number of nomralized squares with magic sum t, and let $f(s)$ be the number of supernormalized squares with magic sum s, for $s, t > 0$. These functions satisfy (1). Therefore, if f has constant leading term, by Theorem 1 so does F. In fact, both f and F are generalized Ehrhart quasipolynomials. Let P be the polytope of normalized doubly stochastic matrices (normalized as above but with weak rather than strict inequalities) and Q the subpolytope of those in which $x_{11} = 0$. The normalized, or supernormalized, squares are the integral points inside the dilation tP, or sQ, that lie in no hyperplane of the form $x_{jk} = x_{lm}$; thus they are counted by an "inside-out" Ehrhart quasipolynomial (see [2]) whose leading coefficient is the volume of the polytope. (See [4].) The latter observation explains why f has constant leading coefficient; and it gives a geometrical explanation for the constancy of that of F, independent of the algebraic explanation supplied by Theorem 1. The geometrical interpretation here of Equation (1) is that P is dissected into slices of one less dimension that are translates of Q. This analysis makes it feasible to carry out an exact computation for $q = 3$ in [3, 4].

A different way of counting semimagic squares leads to an equation of the form (2). Instead of the magic sum, let t be a strict upper bound on the values of the numbers x_{jk}; that is, $0 < x_{jk} < t$. For normalized 3×3 squares, the largest entry is x_{13} [4]. Taking $F(t)$ to be the number of 3×3 semimagic squares with all $x_{jk} < t$, and $f(s)$ the number of supernormalized squares with $x_{33} = s$, Equation (2) holds. Again, geometry shows that f has constant leading coefficient and either algebra (an obvious case of Theorem 1) or geometry implies constancy of the leading coefficient of F; acording to Theorem 1 one reaches the same conclusion for every quasipolynomial f. We use this approach to evaluate $F(t)$ in [3, 4].

It was the combination of these two semimagic enumerations that suggested Theorem 1.

As a final example we consider (1) with an extremely simple quasipolynomial; we let $f = 1_p$. For positive t, $F(t)$ is the number of representations $t = jp + kq$ with j, k positive integers. The point of this example is to show that Theorem 1 is in some sense best possible, because the period of the second leading coefficient can be equal to $\operatorname{lcm}(p, q)$. For simplicity we assume p and q are relatively prime; then $l := \operatorname{lcm}(p, q) = pq$. By Theorem 1 we know that $F(t) = c_1 t + c_{t,0}$. From its definition, F takes integer values and $F(t) = F(t - l) + 1$ if $t > l$. It follows that F cannot have a period less than l; thus, $c_{t,0}$ has period l.

We show an exact formula for $c_{t,0}$. Let τ denote the least nonnegative residue of

$t \bmod l$. Then $F(t) = F(\tau) + \lfloor t/l \rfloor$. As $F(l) = 1$, we know $F(0) = 0$. Thus, $F(\tau) = 0$ or 1 for $0 \le \tau < l$ and

$$F(t) = \frac{1}{l}t + \left[F(\tau) - \frac{\tau}{l}\right]. \tag{5}$$

Some will recognize F as the counting function involved with the two-variable Frobenius coin problem when every coin denomination must be used at least once. (In the standard problem it is not obligatory to use every denomination. The problems are obviously equivalent. We call our counting function *strict*.) The strict function for the Frobenius problem with m coins of relatively prime denominations $p_1, \ldots, p_m$ (cognate to the standard counting function $p_{\mathcal{A}}$ of [1]) is the convolution of $1_{p_1}, \ldots, 1_{p_m}$, better known by its generating function $\prod \left[x^{p_j}/(1 - x^{p_j})\right]$. The formula (5) for the strict function of two variables should be compared to that of Popoviciu ([6]; or see [1]) for the standard 2-coin function, where nonpolynomiality is handled in a different way.

References

[1] Matthias Beck and Sinai Robins, A formula related to the Frobenius problem in two dimensions. In David Chudnovsky *et al.*, eds., *Number Theory: New York Seminar 2003*, pp. 17–23. Springer, New York, 2004.

[2] Matthias Beck and Thomas Zaslavsky, Inside-out polytopes. Submitted. Available on the Web at `arXiv.org`, paper ID math.CO/0309330.

[3] ——, An enumerative geometry for magic and magilatin labellings. In preparation. Available on the Web at `www.math.binghamton.edu/zaslav/Tpapers/`

[4] ——, An enumerative geometry for magic and magilatin labellings: Computational supplement. In preparation.

[5] Philip J. Davis, *Circulant Matrices*. Wiley, New York, 1979. MR 81a:15003. Zbl. 418.15017.

[6] Tiberiu Popoviciu, Asupra unei probleme de patitie a numerelor. *Acad. Rep. Pop. Romane, Filiala Cluj, Studii si cercetari stiintifice* **4** (1953), 7–58.

[7] Richard P. Stanley, *Enumerative Combinatorics*, Vol. 1. Wadsworth & Brooks/Cole, Monterey, Calif., 1986. MR 87j:05003. Zbl. 608.05001. Corrected reprint: Cambridge Stud. Adv. Math., Vol. 49. Cambridge University Press, Cambridge, 1997. MR 98a:05001. Zbl. 889.05001, 945.05006.