Formal Power Series and Algebraic Combinatorics
Séries Formelles et Combinatoire Algébrique
Vancouver 2004

Cyclic Resultants

Christopher J. Hillar

Abstract. *Let k be a field of characteristic zero and let $f \in k[x]$. The m-th cyclic resultant of f is $r_m = Res(f, x^m - 1)$. We characterize polynomials having the same set of nonzero cyclic resultants. Generically, for a polynomial f of degree d, there are exactly 2^{d-1} distinct degree d polynomials with the same set of cyclic resultants as f. However, in the generic monic case, degree d polynomials are uniquely determined by their cyclic resultants. Moreover, two reciprocal ("palindromic") polynomials giving rise to the same set of nonzero r_m are equal. The reciprocal case was stated many years ago (for $k = \mathbb{R}$) and has many applications stemming from such disparate fields as dynamics, number theory, and Lagrangian mechanics. In the process, we also prove a unique factorization result in semigroup algebras involving products of binomials.*

1. Introduction

Let k be a field of characteristic zero and let $f(x) = a_0x^d + a_1x^{d-1} + \cdots + a_d \in k[x]$. The m-th *cyclic resultant* of f is $r_m(f) = \text{Res}(f, x^m - 1)$. We are primarily interested here in the fibers of the map $r : k[x] \to k^{\mathbb{N}}$ given by $f \mapsto (r_m)_{m=0}^{\infty}$. In particular, what are the conditions for two polynomials to give rise to the same set of cyclic resultants? For technical reasons, we will only consider polynomials f that do not have a root of unity as a zero. With this restriction, a polynomial will map to a set of all nonzero cyclic resultants.

One motivation for the study of cyclic resultants comes from the theory of dynamical systems. Sequences of the form r_m arise as the cardinalities of sets of periodic points for toral endomorphisms. Let f be monic of degree d with integral coefficients and let $X = \mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$ denote the d-dimensional additive torus. Then, the companion matrix A_f of f acts on X by multiplication mod 1; that is, it defines a map $T : X \to X$ given by

$$T(\mathbf{x}) = A_f\mathbf{x} \mod 1.$$

Let $\text{Per}_m(T) = \{\mathbf{x} \in \mathbb{T}^d : T^m(\mathbf{x}) = \mathbf{x}\}$ be the set of points fixed under the map T^m. Under the ergodicity condition that no zero of f is a root of unity, it follows (see [**3**]) that $|\text{Per}_m(T)| = |\det(A_f^m - I)|$, in which I is the d-by-d identity matrix, and both of these quantities are given by $|r_m(f)|$. As a consequence of our results, we characterize when the sequence $|\text{Per}_m(T)|$ determines the spectrum of the linear map $A : \mathbb{R}^d \to \mathbb{R}^d$ that lifts T.

In connection with number theory, such sequences were also studied by Pierce and Lehmer [**3**] in the hope of using them to produce large primes. As a simple example, the polynomial $f(x) = x - 2$ gives the Mersenne sequence $M_m = 2^m - 1$. Indeed, we have $M_m = |\det(A_f^m - I)|$, and these numbers are precisely

Key words and phrases. cyclic resultant, binomial factorization, group rings.

This work is supported under a National Science Foundation Graduate Research Fellowship.

the cardinalities of the sets $\mathrm{Per}_m(T)$ for the map $T(x) = 2x \mod 1$. Further motivation comes from knot theory [**9**] and Lagrangian mechanics [**6, 7**].

The principal result in the direction of our main characterization theorem was discovered by Fried [**4**] although certain implications of Fried's result were known to Stark [**2**]. One of our motivations for this work was to present a complete and satisfactory proof of this result. Fried's argument in [**4**], while elegant, is difficult to read and not as complete as one would like. Given a polynomial f of degree d, the *reversal* of f is the polynomial $x^d f(1/x)$. Additionally, f is called *reciprocal* if $a_i = a_{d-i}$ for $0 \le i \le d$ (sometimes such a polynomial is called *palindromic*). Alternatively, f is reciprocal if it is equal to its own reversal. Fried's result may be stated as follows.

Theorem 1.1 (Fried)**.** *Let $p(x) = a_0x^d + \cdots + a_{d-1}x + a_d \in \mathbb{R}[x]$ be a real reciprocal polynomial of even degree d with $a_0 > 0$, and let r_m be the m-th cyclic resultants of p. Then, $|r_m|$ uniquely determine this polynomial of degree d as long as the r_m are never 0.*

2. Statement of Results

As far as we know, the general (non-reciprocal) case has not received much attention. We begin by stating our main characterization theorem for cyclic resultants.

Theorem 2.1. *Let k be a field of characteristic zero, and let f and g be polynomials in $\overline{k}[x]$. Then, f and g generate the same sequence of nonzero cyclic resultants if and only if there exist $u, v \in \overline{k}[x]$ with $deg(u)$ even, $u(0) \neq 0$, and nonnegative integers $l_1 \equiv l_2 \pmod 2$ such that*

$$f(x) = x^{l_1} v(x) u(x^{-1}) x^{deg(u)}$$
$$g(x) = x^{l_2} v(x) u(x).$$

Although the theorem statement appears somewhat technical, we present a natural interpretation of the result. Suppose that $g(x) = x^{l_2}v(x)u(x)$ is a factorization of a polynomial g with nonzero cyclic resultants. Then, another polynomial f giving rise to this same sequence of resultants is obtained from v by multiplication with the reversal of u and a factor x^{l_1} in which $l_1 \in \mathbb{N}$ has the same parity as l_2. In other words, $f(x) = x^{l_1}v(x)u(x^{-1})x^{\deg(u)}$, and all such f must arise in this manner.

Example 2.2. One can check that the polynomials

$$f(x) = x^3 - 10\,x^2 + 31\,x - 30$$
$$g(x) = 15\,x^5 - 38\,x^4 + 17\,x^3 - 2\,x^2$$

both generate the same cyclic resultants. This follows from the factorizations

$$f(x) = (x-2)\left(15x^2 - 8x + 1\right)$$
$$g(x) = x^2(x-2)\left(x^2 - 8x + 15\right).$$

The following is a direct corollary of our main theorem to the generic case.

Corollary 2.3. *Let k be a field of characteristic zero and let g be a generic polynomial in $k[x]$ of degree d. Then, there are exactly 2^{d-1} distinct degree d polynomials with the same set of cyclic resultants as g.*

Proof. If g is generic, then g will not have a root of unity as a zero nor will $g(0) = 0$. Theorem 2.1, therefore, implies that any other degree d polynomial $f \in \overline{k}[x]$ giving rise to the same set of cyclic resultants is determined by choosing an even cardinality subset of the roots of g. Such polynomials will be distinct since g is generic. Since there are 2^d subsets of the roots of g and half of them have even cardinality, the theorem follows. □

Example 2.4. Let $g(x) = (x-2)(x-3)(x-5) = x^3 - 10\,x^2 + 31\,x - 30$. Then, there are $2^{3-1} - 1 = 3$ other degree 3 polynomials with the same set of cyclic resultants as g. They are:

$$15\,x^3 - 38\,x^2 + 17\,x - 2$$

$$10\,x^3 - 37\,x^2 + 22\,x - 3$$
$$6\,x^3 - 35\,x^2 + 26\,x - 5.$$

If one is interested in the case of generic monic polynomials, then Theorem 2.1 also implies the following uniqueness result.

Corollary 2.5. *Let k be a field of characteristic zero and let g be a generic monic polynomial in $k[x]$ of degree d. Then, there is only one monic, degree d polynomial with the same set of cyclic resultants as g.*

Proof. Again, since g is generic, it will not have a root of unity as a zero nor will $g(0) = 0$. Theorem 2.1 forces a constraint on the roots of g for there to be a different polynomial f with the same set of cyclic resultants as g. Namely, a subset of the roots of f has product 1, a non-generic situation. □

As to be expected, there are analogs of Theorem 2.1 and Corollary 2.5 to the real case involving absolute values.

Theorem 2.6. *Let f and g be polynomials in $\mathbb{R}[x]$. If f and g generate the same sequence of nonzero cyclic resultant absolute values, then there exist $u, v \in \mathbb{C}[x]$ with $u(0) \neq 0$ and nonnegative integers l_1, l_2 such that*

$$f(x) = \pm x^{l_1} v(x) u(x^{-1}) x^{deg(u)}$$
$$g(x) = x^{l_2} v(x) u(x).$$

Corollary 2.7. *Let g be a generic monic polynomial in $\mathbb{R}[x]$ of degree d. Then, g is the only monic, degree d polynomial in $\mathbb{R}[x]$ with the same set of cyclic resultant absolute values as g.*

The generic real case without the monic assumption is somewhat more subtle than that of Corollary 2.3. The difficulty is that we are restricted to polynomials in $\mathbb{R}[x]$. However, there is the following

Corollary 2.8. *Let g be a generic polynomial in $\mathbb{R}[x]$ of degree d. Then there are exactly $2^{\lceil d/2 \rceil + 1}$ distinct degree d polynomials in $\mathbb{R}[x]$ with the same set of cyclic resultant absolute values as g.*

Proof. If d is even, then genericity implies that all of the roots of g will be nonreal. In particular, it follows from Theorem 2.6 (and genericity) that any other degree d polynomial $f \in \mathbb{R}[x]$ giving rise to the same set of cyclic resultant absolute values is determined by choosing a subset of the $d/2$ pairs of conjugate roots of g and a sign. This gives us a count of $2^{d/2+1}$ distinct real polynomials. When d is odd, g will have exactly one real root, and a similar counting argument gives us $2^{\lceil d/2 \rceil + 1}$ for the number of distinct real polynomials in this case. This proves the corollary. □

A surprising consequence of this result is that the number of polynomials with equal sets of cyclic resultant absolute values is significantly smaller than the number predicted in Corollary 2.3.

Example 2.9. Let $g(x) = (x-2)(x+i+2)(x-i+2) = x^3 + 2\,x^2 - 3\,x - 10$. Then, there are $2^{\lceil 3/2 \rceil + 1} - 1 = 7$ other degree 3 real polynomials with the same set of cyclic resultant absolute values as g. They are:

$$-x^3 - 2\,x^2 + 3\,x + 10$$
$$\pm(-2\,x^3 - 7\,x^2 - 6\,x + 5)$$
$$\pm(5\,x^3 - 6\,x^2 - 7\,x - 2)$$
$$\pm(-10\,x^3 - 3\,x^2 + 2\,x + 1).$$

It is important to realize that while

$$\begin{aligned} f(x) =& (1-2x)(1+(i+2)x)(x-i+2) \\ =& (-4-2\,i)\,x^3 - (10-i)\,x^2 + (2+2\,i)\,x + 2 - i \end{aligned}$$

has the same set of actual cyclic resultants (by Theorem 2.1), it does not appear in the count above since it is not in $\mathbb{R}[x]$.

As an illustration of the usefulness of Theorem 2.1, we prove a uniqueness result involving cyclic resultants of reciprocal polynomials. Fried's result also follows in the same way using Theorem 2.6 in place of Theorem 2.1.

Corollary 2.10. *Let f and g be reciprocal polynomials with equal sets of nonzero cyclic resultants. Then, $f = g$.*

PROOF. Let f and g be reciprocal polynomials having the same set of nonzero cyclic resultants. Applying Theorem 2.1, it follows that $d = \deg(f) = \deg(g)$ and that

$$f(x) = v(x)u(x^{-1})x^{\deg(u)}$$
$$g(x) = v(x)u(x)$$

($l_1 = l_2 = 0$ since $f(0), g(0) \neq 0$). But then,

$$\begin{aligned} \frac{u(x^{-1})}{u(x)}x^{\deg(u)} &= \frac{f(x)}{g(x)} \\ &= \frac{x^d f(x^{-1})}{x^d g(x^{-1})} \\ &= \frac{u(x)}{u(x^{-1})}x^{-\deg(u)}. \end{aligned}$$

In particular, $u(x) = \pm u(x^{-1})x^{\deg(u)}$. If $u(x) = u(x^{-1})x^{\deg(u)}$, then $f = g$ as desired. In the other case, it follows that $f = -g$. But then $\text{Res}(f,x-1) = \text{Res}(g,x-1) = -\text{Res}(f,x-1)$ is a contradiction to f having all nonzero cyclic resultants. This completes the proof. $\square$

We now switch to the seemingly unrelated topic of binomial factorizations in semigroup algebras. The relationship to cyclic resultants will become clear later. Let A be a finitely generated abelian group and let $a_1, \ldots, a_n$ be distinguished generators of A. Let Q be the semigroup generated by $a_1, \ldots, a_n$. If k is a field, the *semigroup algebra* $k[Q]$ is the k-algebra with vector space basis $\{\mathbf{s}^a : a \in Q\}$ and multiplication defined by $\mathbf{s}^a \cdot \mathbf{s}^b = \mathbf{s}^{a+b}$. Let L denote the kernel of the homomorphism $\mathbb{Z}^n$ onto A. The *lattice ideal* associated with L is the following ideal in $S = k[x_1, \ldots, x_n]$:

$$I_L = \langle x^u - x^v \ : \ u, v \in \mathbb{N}^n \text{ with } u - v \in L\rangle.$$

It is a well-known fact that $k[Q] \cong S/I_L$ (e.g. see [**8**]). We are primarily concerned here with certain kinds of factorizations in $k[Q]$.

Question 2.11. When is a product of binomials in $k[Q]$ equal to another product of binomials?

The answer to this question is turns out to be fundamental for the study of cyclic resultants. Our main result in this direction is a certain kind of unique factorization of binomials in $k[Q]$.

Theorem 2.12. *Let k be a field of characteristic zero and let $\alpha \in k$. Suppose that*

$$\boldsymbol{s}^a \prod_{i=1}^{e} (\boldsymbol{s}^{u_i} - \boldsymbol{s}^{v_i}) = \alpha \boldsymbol{s}^b \prod_{i=1}^{f} (\boldsymbol{s}^{x_i} - \boldsymbol{s}^{y_i})$$

are two factorizations of binomials in the ring $k[Q]$. Furthermore, suppose that for each i, $u_i - v_i$ ($x_i - y_i$) has infinite order as an element of A. Then, $\alpha = \pm 1$, $e = f$, and up to permutation, for each i, there are elements $c_i, d_i \in Q$ such that $\boldsymbol{s}^{c_i}(\boldsymbol{s}^{u_i} - \boldsymbol{s}^{v_i}) = \pm \boldsymbol{s}^{d_i}(\boldsymbol{s}^{x_i} - \boldsymbol{s}^{y_i})$.

Of course, when each side has a factor of zero, the theorem fails. There are other obstructions, however, that make necessary the supplemental hypotheses concerning order. For example, take $k = \mathbb{Q}$, and let $A = \mathbb{Z}/2\mathbb{Z}$. Then, $k[Q] = k[A] \cong \mathbb{Q}[s]/\langle s^2 - 1\rangle$, and we have that

$$(1 - s)(1 - s) = 2(1 - s).$$

This theorem also fails when the characteristic is not 0.

Example 2.13. $L = \{0\}$, $I_L = \langle 0 \rangle$, $A = \mathbb{Z}$, $Q = \mathbb{N}$, $k = \mathbb{Z}/3\mathbb{Z}$,

$$(1 - t^3) = (1 - t)(1 - t)(1 - t).$$

One might wonder what happens when the binomials are not of the form $\mathbf{s}^u - \mathbf{s}^v$. The following example exhibits some of the difficulty in formulating a general statement.

Example 2.14. $L = \{(0, b) \in \mathbb{Z}^2 : b \text{ is even}\}$, $I_L = \langle s^2 - 1 \rangle \subseteq k[s, t]$, $A = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $Q = \mathbb{N} \oplus \mathbb{Z}/2\mathbb{Z}$, $k = \mathbb{Q}(i)$. Then,

$$(1 - t^4) = (1 - st)(1 + st)(1 - ist)(1 + ist) = (1 - st^2)(1 + st^2)$$

are three different binomial factorizations of the same semigroup algebra element.

Example 2.15. $L = \{0\}$, $I_L = \langle 0 \rangle$, $A = \mathbb{Z}$, $Q = \mathbb{N}$, $k = \mathbb{C}$. If

$$\prod_{i=1}^{r} (1 - t^{m_i}) = \prod_{i=1}^{s} (1 - t^{n_i})$$

for positive integers m_i,n_i, then $r = s$ and up to permutation, $m_i = n_i$ for all i.

We now are in a position to outline our strategy for characterizing those polynomials f and g having the same set of nonzero cyclic resultants (this strategy is similar to the one employed in [**4**]). Given a polynomial f and its sequence of r_m, we construct the generating function $E_f(z) = \exp\left(-\sum_{m \geq 1} r_m \frac{z^m}{m}\right)$. This series turns out to be rational with coefficients depending explicitly on the roots of f. Since f and g are assumed to have the same set of r_m, it follows that their corresponding rational functions E_f and E_g are equal. Let G be the (multiplicative) group of units in the algebraic closure of k. Then, the divisors of these two rational functions are group ring elements in $\mathbb{Z}[G]$ and their equality forces a certain binomial group ring factorization that is analyzed explicitly. The results above follow from this final analysis.

3. Binomial Factorizations in Semigroup Algebras

To prove our factorization result, we will pass to the full group algebra $k[A]$. As above, we represent elements $\tau \in k[A]$ as $\tau = \sum_{i=1}^{m} \alpha_i \mathbf{s}^{g_i}$, in which $\alpha_i \in k$ and $g_i \in A$. The following lemma is quite well-known.

Lemma 3.1. *If $\alpha \in k^*$ and $g \in A$ has infinite order, then $1 - \alpha \mathbf{s}^g \in k[A]$ is not a 0-divisor.*

Proof. Let $\alpha \in k^*, g \in A$ and $\tau = \sum_{i=1}^{m} \alpha_i \mathbf{s}^{g_i} \neq 0$ be such that

$$\tau = \alpha \mathbf{s}^g \tau = \alpha \mathbf{s}^{2g} \tau = \alpha \mathbf{s}^{3g} \tau = \cdots.$$

Suppose that $\alpha_1 \neq 0$. Then, the elements $\mathbf{s}^{g_1}, \mathbf{s}^{g_1+g}, \mathbf{s}^{g_1+2g}, \ldots$ appear in τ with nonzero coefficient, and since g has infinite order, these elements are all distinct. It follows, therefore, that τ cannot be a finite sum, and this contradiction finishes the proof. $\square$

Since the proof of the main theorem involves multiple steps, we record several facts that will be useful later. The first result is a verification of the factorization theorem for a generalization of the situation in Example 2.15.

Lemma 3.2. *Let k be a field of characteristic zero and let C be an abelian group. Let $k[C]$ be the group algebra with k-vector space basis given by $\{\boldsymbol{s}^c : c \in C\}$ and set $R = k[C][t, t^{-1}]$. Suppose that $c_1, \ldots, c_e, d_1, \ldots, d_f, b \in C$, $m_1, \ldots, m_e, n_1, \ldots, n_f$ are nonzero integers, $q \in \mathbb{Z}$, and $z \in k$ are such that*

$$\prod_{i=1}^{e} (1 - \boldsymbol{s}^{c_i} t^{m_i}) = z \boldsymbol{s}^b t^q \prod_{i=1}^{f} (1 - \boldsymbol{s}^{d_i} t^{n_i})$$

holds in R. Then, $e = f$ and after a permutation, for each i, either $\boldsymbol{s}^{c_i} t^{m_i} = \boldsymbol{s}^{d_i} t^{n_i}$ or $\boldsymbol{s}^{c_i} t^{m_i} = \boldsymbol{s}^{-d_i} t^{-n_i}$.

PROOF. Let $\operatorname{sgn} : \mathbb{Z} \setminus \{0\} \to \{-1, 1\}$ denote the standard sign map $\operatorname{sgn}(n) = n/|n|$ and set $\gamma = z\mathbf{s}^b t^q$. Rewrite the left-hand side of the given equality as:

$$\prod_{i=1}^{e} (1 - \mathbf{s}^{c_i} t^{m_i}) = \prod_{\operatorname{sgn}(m_i)=-1} -\mathbf{s}^{c_i} t^{m_i} \prod_{i=1}^{e} \left(1 - \mathbf{s}^{\operatorname{sgn}(m_i)c_i} t^{|m_i|}\right).$$

Similarly for the right-hand side, we have:

$$\prod_{i=1}^{f} (1 - \mathbf{s}^{d_i} t^{n_i}) = \prod_{\operatorname{sgn}(n_i)=-1} -\mathbf{s}^{d_i} t^{n_i} \prod_{i=1}^{f} \left(1 - \mathbf{s}^{\operatorname{sgn}(n_i)d_i} t^{|n_i|}\right).$$

Next, set

$$\eta = \gamma \prod_{\operatorname{sgn}(m_i)=-1} -\mathbf{s}^{-c_i} t^{-m_i} \prod_{\operatorname{sgn}(n_i)=-1} -\mathbf{s}^{d_i} t^{n_i}$$

so that our original equation may be written as

$$\prod_{i=1}^{e} \left(1 - \mathbf{s}^{\operatorname{sgn}(m_i)c_i} t^{|m_i|}\right) = \eta \prod_{i=1}^{f} \left(1 - \mathbf{s}^{\operatorname{sgn}(n_i)d_i} t^{|n_i|}\right).$$

Comparing the lowest degree term (with respect to t) on both sides, it follows that $\eta = 1$. It is enough, therefore, to prove the claim in the case when

$$\prod_{i=1}^{e} (1 - \mathbf{s}^{c_i} t^{m_i}) = \prod_{i=1}^{f} (1 - \mathbf{s}^{d_i} t^{n_i}) \tag{3.1}$$

and the m_i, n_i are positive. Without loss of generality, suppose the lowest degree nonconstant term on both sides of (3.1) is t^{m_1} with coefficient $-\mathbf{s}^{c_1} - \cdots - \mathbf{s}^{c_u}$ on the left and $-\mathbf{s}^{d_1} - \cdots - \mathbf{s}^{d_v}$ on the right. Here, u (v) corresponds to the number of m_i (n_i) with $m_i = m_1$ ($n_i = m_1$).

Since the set of distinct monomials $\{\mathbf{s}^c : c \in C\}$ is a k-vector space basis for the ring $k[C]$, equality of the t^{m_1} coefficients above implies that $u = v$ and that up to permutation, $\mathbf{s}^{c_j} = \mathbf{s}^{d_j}$ for $j = 1, \ldots, u$ (recall that the characteristic of k is zero). Using Lemma 3.1 and induction completes the proof. □

Lemma 3.3. *Let $P = (p_{ij})$ be a d-by-n integer matrix such that every row has at least one nonzero integer. Then, there exists $\boldsymbol{v} \in \mathbb{Z}^n$ such that the vector $P\boldsymbol{v}$ does not contain a zero entry.*

PROOF. Let P be a d-by-n integer matrix as in the hypothesis of the lemma, and for $h \in \mathbb{Z}$, let $\mathbf{v}_h = (1, h, h^2, \ldots, h^{n-1})^T$. Assume, by way of contradiction, that $P\mathbf{v}$ contains a zero entry for all $\mathbf{v} \in \mathbb{Z}^n$. Then, in particular, this is true for all $\mathbf{v}_h$ as above. By the (infinite) pigeon-hole principle, there exists an infinite set of $h \in \mathbb{Z}$ such that (without loss of generality) the first entry of $P\mathbf{v}_h$ is zero. But then,

$$f(h) := \sum_{i=1}^{n} p_{1i} h^{i-1} = 0$$

for infinitely many values of h. It follows, therefore, that $f(h)$ is the zero polynomial, contradicting our hypothesis and completing the proof. □

Lemma 3.3 will be useful in verifying the following fact.

Lemma 3.4. *Let A be a finitely generated abelian group and $a_1, \ldots, a_d$ elements in A of infinite order. Then, there exists a homomorphism $\phi : A \to \mathbb{Z}$ such that $\phi(a_i) \neq 0$ for all i.*

Proof. Write $A = B \oplus C$, in which C is a finite group and B is free of rank n. If $n = 0$, then there are no elements of infinite order; therefore, we may assume that the rank of B is positive. Since $a_1, \ldots, a_d$ have infinite order, their images in the natural projection $\pi : A \to B$ are nonzero. It follows that we may assume that A is free and a_i are nonzero elements of A.

Let $e_1, \ldots, e_n$ be a basis for A, and write

$$a_t = p_{t1}e_1 + \cdots + p_{tn}e_n$$

for (unique) integers $p_{ij} \in \mathbb{Z}$. To determine a homomorphism $\phi : A \to \mathbb{Z}$ as in the lemma, we must find integers $\phi(e_1), \ldots, \phi(e_n)$ such that

$$\begin{aligned} 0 &\neq p_{11}\phi(e_1) + \cdots + p_{1n}\phi(e_n) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ 0 &\neq p_{d1}\phi(e_1) + \cdots + p_{dn}\phi(e_n). \end{aligned} \tag{3.2}$$

This, of course, is precisely the consequence of Lemma 3.3 applied to the matrix $P = (p_{ij})$, finishing the proof. □

Recall that a *trivial unit* in the group ring $k[A]$ is an element of the form $\alpha\mathbf{s}^a$ in which $\alpha \in k^*$ and $a \in A$. The main content of Theorem 2.12 is contained in the following result. The technique of embedding $k[A]$ into a Laurent polynomial ring is also used by Fried in [**4**].

Lemma 3.5. *Let A be an abelian group and let k be a field of characteristic 0. Two factorizations in $k[A]$,*

$$\prod_{i=1}^{e} (1 - \boldsymbol{s}^{g_i}) = \eta \prod_{i=1}^{f} \left(1 - \boldsymbol{s}^{h_i}\right),$$

in which η is a trivial unit and $g_i, h_i \in A$ all have infinite order are equal if and only if $e = f$ and there is some nonnegative integer p such that, up to permutation,

(1) $g_i = h_i$ *for* $i = 1, \ldots, p$
(2) $g_i = -h_i$ *for* $i = p + 1, \ldots, e$
(3) $\eta = (-1)^{e-p}\boldsymbol{s}^{g_{p+1}+\cdots+g_e}$.

Proof. The if-direction of the claim is a straightforward calculation. Therefore, suppose that one has two factorizations as in the lemma. It is clear we may assume that A is finitely generated. By Lemma 3.4, there exists a homomorphism $\phi : A \to \mathbb{Z}$ such that $\phi(g_i), \phi(h_i) \neq 0$ for all i. The ring $k[A]$ may be embedded into the Laurent ring, $R = k[A][t, t^{-1}]$, by way of

$$\psi\left(\sum_{i=1}^{m} \alpha_i \mathbf{s}^{a_i}\right) = \sum_{i=1}^{m} \alpha_i \mathbf{s}^{a_i} t^{\phi(a_i)}.$$

Write $\eta = \alpha\mathbf{s}^b$. Then, applying this homomorphism to the original factorization, we have

$$\prod_{i=1}^{e} \left(1 - \mathbf{s}^{g_i} t^{\phi(g_i)}\right) = \alpha \mathbf{s}^b t^{\phi(b)} \prod_{i=1}^{f} \left(1 - \mathbf{s}^{h_i} t^{\phi(h_i)}\right).$$

Lemma 3.2 now applies to give us that $e = f$ and there is an integer p such that up to permutation,

(1) $g_i = h_i$ for $i = 1, \ldots, p$
(2) $g_i = -h_i$ for $i = p + 1, \ldots, e$.

We are therefore left with verifying statement (3) of the lemma. Using Lemma 3.1, we may cancel equal terms in our original factorization, leaving us with the following equation:

$$\begin{aligned}\prod_{i=p+1}^{e}(1-\mathbf{s}^{g_i}) &= \eta\prod_{i=p+1}^{e}(1-\mathbf{s}^{-g_i})\\ &= \eta(-1)^{e-p}\prod_{i=p+1}^{e}\mathbf{s}^{-g_i}\prod_{i=p+1}^{e}(1-\mathbf{s}^{g_i}).\end{aligned}$$

Finally, one more application of Lemma 3.1 gives us that $\eta=(-1)^{e-p}\mathbf{s}^{g_{p+1}+\cdots+g_e}$ as desired. This finishes the proof. □

We may now prove Theorem 2.12.

Proof of Theorem 2.12. Let

$$\mathbf{s}^a\prod_{i=1}^{e}(\mathbf{s}^{u_i}-\mathbf{s}^{v_i})=\alpha\mathbf{s}^b\prod_{i=1}^{f}(\mathbf{s}^{x_i}-\mathbf{s}^{y_i})$$

be two factorizations in the ring $k[Q]$. View this expression in $k[A]$ and factor each element of the form $(\mathbf{s}^u-\mathbf{s}^v)$ as $\mathbf{s}^u(1-\mathbf{s}^{v-u})$. By assumption, each such $v-u$ has infinite order. Now, apply Lemma 3.5, giving us that $\alpha=\pm1$, $e=f$, and that after a permutation, for each i either $\mathbf{s}^{v_i-u_i}=\mathbf{s}^{y_i-x_i}$ or $\mathbf{s}^{v_i-u_i}=\mathbf{s}^{x_i-y_i}$. It easily follows from this that for each i, there are elements $c_i,d_i\in Q$ such that $\mathbf{s}^{c_i}(\mathbf{s}^{u_i}-\mathbf{s}^{v_i})=\pm\mathbf{s}^{d_i}(\mathbf{s}^{x_i}-\mathbf{s}^{y_i})$. This completes the proof of the theorem. □

4. Cyclic Resultants and Rational Functions

We begin with some preliminaries concerning cyclic resultants. Let $f(x)=a_0x^d+a_1x^{d-1}+\cdots+a_d$ be a degree d polynomial over k, and let the companion matrix for f be given by:

$$A=\begin{bmatrix}0 & 0 & \cdots & 0 & -a_d/a_0\\ 1 & 0 & \cdots & 0 & -a_{d-1}/a_0\\ 0 & 1 & \cdots & 0 & -a_{d-2}/a_0\\ 0 & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \cdots & 1 & -a_1/a_0\end{bmatrix}.$$

Also, let I denote the d-by-d identity matrix. Then, we may write [**1**, p. 77]

$$r_m=a_0^m\det(A^m-I). \tag{4.1}$$

Extending to a splitting field of f, this equation can also be expressed as,

$$r_m=a_0^m\prod_{i=1}^{d}(\alpha_i^m-1), \tag{4.2}$$

in which $\alpha_1,\ldots,\alpha_d$ are the roots of $f(x)$.

Let $e_i(y_1,\ldots,y_d)$ be the i-th elementary symmetric function in the variables $y_1,\ldots,y_d$ (we set $e_0=1$). Then, we know that $a_i=(-1)^ia_0e_i(\alpha_1,\ldots,\alpha_d)$ and that

$$r_m=a_0^m\sum_{i=0}^{d}(-1)^ie_{d-i}(\alpha_1^m,\ldots,\alpha_d^m). \tag{4.3}$$

We first record an auxiliary result.

Lemma 4.1. *Let* $F_k(z) = \prod_{1 \le i_1 < \cdots < i_k \le d} (1 - a_0\alpha_{i_1} \cdots \alpha_{i_k} z)$ *with* $F_0(z) = 1 - a_0 z$*. Then,*

$$\sum_{m=1}^{\infty} a_0^m e_k\left(\alpha_1^m, \ldots, \alpha_n^m\right) z^m = -z \cdot \frac{F_k'}{F_k},$$

in which F_k' *denotes* $\frac{dF_k}{dz}$*.*

Proof. For $k = 0$, the equation is easily verified. When $k > 0$, the calculation is still fairly straightforward:

$$\begin{aligned}
\sum_{m=1}^{\infty} a_0^m e_k\left(\alpha_1^m, \ldots, \alpha_d^m\right) z^m &= \sum_{m=1}^{\infty} \sum_{i_1 < \cdots < i_k} a_0^m \alpha_{i_1}^m \cdots \alpha_{i_k}^m \cdot z^m \\
&= \sum_{i_1 < \cdots < i_k} \sum_{m=1}^{\infty} a_0^m \alpha_{i_1}^m \cdots \alpha_{i_k}^m \cdot z^m \\
&= \sum_{i_1 < \cdots < i_k} \frac{a_0\alpha_{i_1} \cdots \alpha_{i_k} z}{1 - a_0\alpha_{i_1} \cdots \alpha_{i_k} z} \\
&= \frac{-z \cdot \frac{d}{dz}\left[\prod_{i_1 < \cdots < i_k} (1 - a_0\alpha_{i_1} \cdots \alpha_{i_k} z)\right]}{\prod_{i_1 < \cdots < i_k} (1 - a_0\alpha_{i_1} \cdots \alpha_{i_k} z)} \\
&= -z \cdot \frac{F_k'}{F_k}.
\end{aligned}$$

□

We may now state and prove the rationality result mentioned in the introduction.

Lemma 4.2. $R_f(z) = \sum_{m=1}^{\infty} r_m z^m$ *is a rational function in* z*.*

Proof. We simply compute that

$$\begin{aligned}
\sum_{m=1}^{\infty} r_m z^m &= \sum_{m=1}^{\infty} \sum_{i=0}^{d} (-1)^i a_0^m e_{d-i}\left(\alpha_1^m, \ldots, \alpha_d^m\right) \cdot z^m \\
&= \sum_{i=0}^{d} (-1)^i \sum_{m=1}^{\infty} a_0^m e_{d-i}\left(\alpha_1^m, \ldots, \alpha_d^m\right) \cdot z^m \\
&= -z \cdot \sum_{i=0}^{d} (-1)^i \cdot \frac{F_{d-i}'}{F_{d-i}}.
\end{aligned}$$

□

Let us remark at this point that Lemma 4.2 implies the following curious determinantal identity.

Corollary 4.3. *Let* d *be a positive integer and set* $n = 2^d + 1$*. Then,*

$$A = \left(\prod_{l=1}^{d} \left(\alpha_l^{n+i-j} - 1\right)\right)_{i,j=1}^{n}$$

has determinant 0*.*

PROOF. Let $r_m = \prod_{l=1}^{d}(\alpha_l^m - 1)$ for $m \in \{1, 2, \ldots\}$. From above, $\sum_{m=1}^{\infty} r_m z^m$ is a rational function of z with numerator and denominator each having degree at most 2^d. This implies a linear recurrence for the r_m of length at most 2^d, and therefore it follows that $\det(A) = 0$. $\square$

Manipulating the expression for $R_f(z)$ occurring in Lemma 4.2, we also have the following fact.

Corollary 4.4. *If d is even, let $G_d = \frac{F_d F_{d-2} \cdots F_0}{F_{d-1} F_{d-3} \cdots F_1}$ and if d is odd, let $G_d = \frac{F_d F_{d-2} \cdots F_1}{F_{d-1} F_{d-3} \cdots F_0}$. Then,*

$$\sum_{m=1}^{\infty} r_m z^m = -z \frac{G_d'}{G_d}.$$

In particular, it follows that

$$\exp\left(-\sum_{m=1}^{\infty} r_m \frac{z^m}{m}\right) = G_d. \tag{4.4}$$

Example 4.5. Let $f(x) = x^2 - 5x + 6 = (x-2)(x-3)$. Then, $r_m = (2^m - 1)(3^m - 1)$ and $F_0(z) = 1 - z$, $F_1(z) = (1-2z)(1-3z)$, $F_2(z) = 1 - 6z$. Thus,

$$R_f(z) = -z\left(\frac{F_2'}{F_2} - \frac{F_1'}{F_1} + \frac{F_0'}{F_0}\right) = \frac{6z}{1-6z} - \frac{2z}{1-2z} - \frac{3z}{1-3z} + \frac{z}{1-z}$$

and

$$\exp\left(-\sum_{m=1}^{\infty} r_m \frac{z^m}{m}\right) = \frac{(1-6z)(1-z)}{(1-2z)(1-3z)}.$$

Following [**4**], we discuss how to deal with absolute values in the $k = \mathbb{R}$ case. Let $f \in \mathbb{R}[x]$ have degree d such that the r_m as defined above are all nonzero. We examine the sign of r_m using equation (4.2). First notice that a complex conjugate pair of roots of f does not affect the sign of r_m. A real root α of f contributes a sign factor of $+1$ if $\alpha > 1$, -1 if $-1 < \alpha < 1$, and $(-1)^m$ if $\alpha < -1$. Let E be the number of zeroes of f in $(-1, 1)$ and let D be the number of zeroes in $(-\infty, -1)$. Also, set $\epsilon = (-1)^E$ and $\delta = (-1)^D$. Then, it follows that

$$\frac{r_m}{|r_m|} = \epsilon \cdot \delta^m.$$

In particular,

$$|r_m| = \epsilon (\delta a_0)^m \prod_{i=1}^{d} (\alpha_i^m - 1). \tag{4.5}$$

In other words, the sequence of $|r_m|$ is obtained by multiplying each cyclic resultant of the polynomial $\tilde{f} := \delta f = \delta a_0 x^d + \delta a_1 x^{d-1} + \cdots + \delta a_d$ by ϵ. Denoting by $\widetilde{G}_d$ the rational function determined by $\tilde{f}$ as in (4.4), it follows that

$$\exp\left(-\sum_{m=1}^{\infty} |r_m| \frac{z^m}{m}\right) = \left(\widetilde{G}_d\right)^{\epsilon}. \tag{4.6}$$

5. Proofs of the Main Theorems

Let G be the multiplicative group generated by the nonzero roots $\alpha_1, \ldots, \alpha_d$ of f. Vector space basis elements of the group ring $k[G]$ will be represented by $[\alpha]$, $\alpha \in G$. The divisor (in $k[G]$) of the rational function G_d defined by Corollary 4.4 is

$$(-1)^{d+1}\left(\sum_{k \text{ odd}} \sum_{i_1 < \cdots < i_k} \left[(a_0 \alpha_{i_1} \cdots \alpha_{i_k})^{-1}\right] - \sum_{k \text{ even}} \sum_{i_1 < \cdots < i_k} \left[(a_0 \alpha_{i_1} \cdots \alpha_{i_k})^{-1}\right]\right) \tag{5.1}$$

$$= [a_0^{-1}] \prod_{i=1}^{d} \left([\alpha_i^{-1}] - [1]\right).$$

Let us remark that for ease of presentation above, when $k = 0$, we have assigned

$$\sum_{i_1 < \cdots < i_k} \left[(a_0 \alpha_{i_1} \cdots \alpha_{i_k})^{-1}\right] = [a_0^{-1}],$$

which corresponds to the factor of $F_0(z) = 1 - a_0 z$ in G_d. With this computation in hand, we now prove our main theorems.

Proof of Theorem 2.1. Examining the statement of the theorem, we may assume that k is algebraically closed. Let f and g be polynomials in $k[x]$ such that the multiplicity of 0 as a root of f (g) is l_1 (l_2). Then, $f(x) = x^{l_1}(a_0 x^{d_1} + \cdots + a_{d_1})$ and $g(x) = x^{l_2}(b_0 x^{d_2} + \cdots + b_{d_2})$ in which a_0 and b_0 are not 0. Let $\alpha_1, \ldots, \alpha_{d_1}$ and $\beta_1, \ldots, \beta_{d_2}$ be the nonzero roots of f and g, respectively, and let G be the multiplicative group generated by these elements. Since $f(x)$ and $g(x)$ both generate the same sequence of cyclic resultants, it follows that the divisor (in the group ring $k[G]$) of their corresponding rational functions (see (4.4)) are equal. By above, such divisors factor, giving us that

$$(-1)^{d_1}[a_0^{-1}] \prod_{i=1}^{d_1} \left([1] - [\alpha_i^{-1}]\right) = (-1)^{d_2}[b_0^{-1}] \prod_{i=1}^{d_2} \left([1] - [\beta_i^{-1}]\right).$$

Since we have assumed that f and g generate a set of nonzero cyclic resultants, neither of them can have a root of unity as a zero. Therefore, Lemma 3.5 applies to give us that $d := d_1 = d_2$ and that up to a permutation, there is a nonnegative integer p such that

(1) $\alpha_i = \beta_i$ for $i = 1, \ldots, p$
(2) $\alpha_i = \beta_i^{-1}$ for $i = p+1, \ldots, d$
(3) $(-1)^{d-p} = 1$, $a_0 b_0^{-1} = \beta_{p+1} \cdots \beta_d$.

Set $u(x) = (x - \beta_{p+1}) \cdots (x - \beta_d)$, which has even degree, and let $v(x) = b_0(x - \beta_1) \cdots (x - \beta_p)$ (note that if $p = 0$, then $v(x) = b_0$) so that $g(x) = x^{l_2} v(x) u(x)$. Now,

$$u(x^{-1}) x^{\deg(u)} = (-1)^{d-p} \beta_{p+1} \cdots \beta_d (x - \beta_{p+1}^{-1}) \cdots (x - \beta_d^{-1}),$$

and thus

$$\begin{aligned} f(x) &= x^{l_1} a_0 b_0^{-1} v(x)(x - \beta_{p+1}^{-1}) \cdots (x - \beta_d^{-1}) \\ &= x^{l_1} v(x) u(x^{-1}) x^{\deg(u)}. \end{aligned}$$

It remains only to argue that $l_1 \equiv l_2 \pmod 2$. However, from formula (4.2) with $m = 1$, it is easily seen that $(-1)^{l_1} = (-1)^{l_2}$. The converse is also straightforward from (4.2), and this completes the proof of the theorem. □

The proof of Theorem 2.6 is similar, employing equation (4.6) in place of (4.4).

Proof of Theorem 2.6. Since multiplication of a real polynomial by a power of x does not change the absolute value of a cyclic resultant, we may assume $f, g \in \mathbb{R}[x]$ have distinct roots. The result now follows from (4.6) and the argument used to prove the if-direction of Theorem 2.1. □

6. Algorithms Related to Cyclic Resultants

In the proof of Theorem 2.1, the multiplicative group generated by the roots of f played an important role; which leads us to the following natural question. Given a polynomial $f \in \mathbb{Z}[x]$ of degree d, can one devise an algorithm to determine the structure of the group G generated by the roots of f? Of course, G will be a direct sum of a free abelian group and a finite cyclic group, so one possible output would consist of two numbers: the rank of the free part and the order of the cyclic component. Another description would be to give generators for the lattice L, where L is the kernel of the homomorphism sending the generators of $\mathbb{Z}^d$ to the roots of f.

It turns out that an algorithm does indeed exist, however, it is exponential in d. The result is due to Ge [**5**], although our question is a special case of a more general problem he studied. Given a finite list of nonzero elements of an algebraic number field K, Ge has an algorithm that determines a generating set for the group of all multiplicative relations between those elements (and therefore the structure of the subgroup they generate). It would be nice to know if there is a better (polynomial) time procedure to solve our special case, however, we do not know of any work in this direction.

7. Acknowledgement

We would like to thank Bernd Sturmfels for bringing this problem to our attention and for the idea of reformulating Lemma 3.5 into the statement of Theorem 2.12.

References

[1] D. Cox, J. Little, D. O'Shea, *Using Algebraic Geometry*, Springer, New York, 1998.
[2] J.J. Duistermaat and V. Guillemin, *The spectrum of positive elliptic operators and periodic bicharacteristics*, Inv. Math. 25 (1975) 39-79.
[3] G. Everest and T. Ward. Heights of Polynomials and Entropy in Algebraic Dynamics. Springer-Verlag London Ltd., London, 1999.
[4] D. Fried, *Cyclic resultants of reciprocal polynomials*, in Holomorphic Dynamics (Mexico 1986), Lecture Notes in Math. 1345, Springer Verlag, 1988, 124-128.
[5] Guoqiang Ge, *Algorithms related to multiplicative representations of algebraic numbers*, PhD thesis, Math Dept, U. C. Berkeley, 1993.
[6] V. Guillemin, *Wave trace invariants*, Duke Math. J. 83 (1996), 287-352.
[7] A. Iantchenko, J. Sjöstrand, and M. Zworski, *Birkhoff normal forms in semi-classical inverse problems*, preprint.
[8] E. Miller and B. Sturmfels, *Combinatorial Commutative Algebra*, Springer, 2004.
[9] W. H. Stevens, *Recursion formulas for some abelian knot invariants*, Journal of Knot Theory and Its Ramifications, Vol. 9, No. 3 (2000) 413-422.

Department of Mathematics, University of California, Berkeley, CA 94720.
E-mail address: chillar@math.berkeley.edu