CYCLOTOMIC POLYTOPES AND GROWTH SERIES OF CYCLOTOMIC LATTICES

Matthias Beck and Serkan Hoşten

ABSTRACT. The coordination sequence of a lattice $\mathcal{L}$ encodes the word-length function with respect to M, a set that generates $\mathcal{L}$ as a monoid. We investigate the coordination sequence of the cyclotomic lattice $\mathcal{L} = \mathbb{Z}[\zeta_m]$, where ζ_m is a primitive m^{th} root of unity and where M is the set of all m^{th} roots of unity. We prove several conjectures by Parker regarding the structure of the rational generating function of the coordination sequence; this structure depends on the prime factorization of m. Our methods are based on unimodular triangulations of the mth cyclotomic polytope, the convex hull of the m roots of unity in $\mathbb{R}^{\phi(m)}$, with respect to a canonically chosen basis of $\mathcal{L}$.

1. Introduction

Let $\mathcal{L} \subset \mathbb{R}^d$ be a lattice of rank r, and let M be a subset that generates $\mathcal{L}$ as a monoid. The *coordination sequence* $(S(n))_{n \geq 0}$ of $(\mathcal{L}, M)$ is given by $S(n)$, the number of elements in $\mathcal{L}$ with *word length* n with respect to M, that is, the number of lattice elements that are expressed as a sum from M with a minimal number of n terms [7]. The *growth series* G of $(\mathcal{L}, M)$ is the generating function of $S(n)$:

$$G(x) := \sum_{n \geq 0} S(n)\, x^n.$$

Benson [3] proved that $G(x) = \frac{h(x)}{(1-x)^r}$ where $h(x)$, the *coordinator polynomial* of $\mathcal{L}$, is a polynomial of degree $\leq r$. Consequently, $S(n)$ is a polynomial of degree $r - 1$. The rationality of $G(x)$ when $\mathcal{L} \cong \mathbb{Z}^r$ is an easy by-product of our approach we present below (see also [25]).

Now let $\zeta_m := e^{2\pi i/m}$. We denote by $\Phi_m(x)$ the mth cyclotomic polynomial; its degree is $\phi(m)$, the Euler totient function. The ring of integers in the cyclotomic field of order m, $\mathbb{Z}[\zeta_m]$, is a lattice of full rank in $\mathbb{Z}[\zeta_m] \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^{\phi(m)}$ and hence isomorphic to $\mathbb{Z}^{\phi(m)}$. For the remainder of the paper, we let M be the set of all m^{th} roots of unity, and we let $h_m(x)$ be the corresponding coordinator polynomial. The study of the coordination sequence of $\mathbb{Z}[\zeta_m]$ with respect to M was initiated by Parker, who was motivated by applications to error-correcting codes and random walks. His article [16] includes Kløve's proof of the following result, previously conjectured by Parker.

Theorem 1 (Kløve–Parker). *The coordinator polynomial $h_p(x)$ of $\mathbb{Z}[\zeta_p]$, where p is prime, equals*

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1 \ .$$

Kløve's proof uses a counting argument that relates elements of $\mathbb{Z}[\zeta_p]$ to ordered partitions.

Parker [16] offered several conjectures. We call a degree-d polynomial $c_d x^d + c_{d-1} x^{d-1} + \cdots + c_0$ *palindromic* if $c_k = c_{d-k}$.

Conjecture 1 (Parker). *The coordinator polynomial $h_m(x)$ of $\mathbb{Z}[\zeta_m]$ equals $\left(h_{\sqrt{m}}(x)\right)^{m/\sqrt{m}}$, where $\sqrt{m}$ is the squarefree part of m. Furthermore, $h_{\sqrt{m}}(x)$ is a palindromic polynomial of degree $\phi(\sqrt{m})$.*

Conjecture 2 (Parker). *The coordinator polynomial of $\mathbb{Z}[\zeta_{2p}]$, where p is an odd prime, equals*

$$
\begin{aligned}
h_{2p}(x) &= \sum_{k=0}^{\frac{p-3}{2}} \left(x^k + x^{p-1-k}\right) \sum_{j=0}^{k} \binom{p}{j} + x^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{j} \\
&= \sum_{k=0}^{\frac{p-3}{2}} \left(x^k + x^{p-1-k}\right) \sum_{j=0}^{k} \binom{p}{j} + 2^{p-1} x^{\frac{p-1}{2}} \ .
\end{aligned}
$$

Conjecture 3 (Parker). *The coordinator polynomial of $\mathbb{Z}[\zeta_{15}]$ equals*

$$h_{15}(x) = \left(1 + x^8\right) + 7\left(x + x^7\right) + 28\left(x^2 + x^6\right) + 79\left(x^3 + x^5\right) + 130 x^4.$$

Patras and Solé studied Theorem 1 and Parker's conjectures from the viewpoint of Ehrhart polynomials of the *cyclotomic polytope* of $\mathbb{Z}[\zeta_m]$ (which we will define below). Their article [17] includes an alternate proof of Theorem 1 and a computation of $h_{2p}(x)$ that gave further credence to Conjecture 2.

In this paper we prove Conjectures 2 and 3, and we partly confirm Conjecture 1, in form of the following two theorems.

Theorem 2. *For any positive integer m, the coordinator polynomial of $\mathbb{Z}[\zeta_m]$ equals $\left(h_{\sqrt{m}}(x)\right)^{m/\sqrt{m}}$.*

Theorem 3. *Suppose the positive integer m is one of the following:*
  (i) $m = p^\alpha$ *where p is prime,*
  (ii) $m = p^\alpha q^\beta$ *where p and q are distinct primes, or*
  (iii) $m = 2^\alpha p^\beta q^\gamma$ *where p and q are distinct odd primes.*
Then the coordinator polynomial $h_m(x)$ of $\mathbb{Z}[\zeta_m]$ is of the form $h(x)^{m/\sqrt{m}}$, where $h(x)$ is the h-polynomial of a simplicial polytope, and hence it is palindromic, unimodal, and has nonnegative integer coefficients.

Our methods are based on unimodular triangulations of the cyclotomic polytope $\mathcal{C}_m$, which we introduce in Section 2. We show how one can compute $\mathcal{C}_m$ from $\mathcal{C}_{p_1}, \ldots, \mathcal{C}_{p_k}$ where $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. In Section 3 we study the Hilbert series of $\mathcal{C}_m$ and its connection to the growth series $G(x)$, and prove Theorem 2. We further show that when m is as in one of the cases of Theorem 3, the cyclotomic polytope $\mathcal{C}_m$ is totally unimodular. In Section 4 we review toric initial ideals of $\mathcal{C}_m$ and the

Dehn–Sommerville relations, and prove Theorem 3. In Section 5 we compute the face numbers of $\mathcal{C}_p$, $\mathcal{C}_{2p}$, and $\mathcal{C}_{15}$, and prove Conjectures 2 and 3. When p, q, r are distinct odd primes then the cyclotomic polytope for $m = pqr$ is *not* totally unimodular. This might be seen as an evidence that Conjecture 1 may not be true in general. In fact, in Section 5 we present and support the conjecture that $h_{105}(x)$ is *not* palindromic.

We would like to point out the recent paper [14] which studies the matroid defined by vertices of the cyclotomic polytope $\mathcal{C}_m$ and its dual matroid, in order to give an upper bound for the number of bases of this matroid. In the cases described in Theorem 3, this upper bound gives the exact count. Theorem 18 below establishes a polytope duality between $\mathcal{C}_m$ and certain multidimensional transportation polytopes and implies that $\mathcal{C}_{pq}$ is simplicial.

2. Cyclotomic polytopes

We will now define the mth *cyclotomic polytope* $\mathcal{C}_m$ associated to $\mathbb{Z}[\zeta_m]$. To this end, we will choose a specific lattice basis of $\mathbb{Z}[\zeta_m]$ consisting of certain powers of ζ_m. These powers will correspond to the standard unit vectors of $\mathbb{R}^{\phi(m)}$. The other powers are integer linear combinations of this basis; hence they are lattice vectors in $\mathbb{R}^{\phi(m)}$. The mth cyclotomic polytope $\mathcal{C}_m$ is the convex hull of all of these m lattice points in $\mathbb{R}^{\phi(m)}$ which correspond to the mth roots of unity. We give this construction first when m is prime, then for a prime power m, and finally when m is the product of two relatively prime integers. These three cases will define $\mathcal{C}_m$ for any positive integer m.

When $m = p$ is a prime number we fix the $\mathbb{Z}$-basis $1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}$ of the lattice $\mathbb{Z}[\zeta_p]$. Since $\zeta_p^{p-1} = -\sum_{i=0}^{p-2} \zeta_p^i$, these p elements form a monoid basis for $\mathbb{Z}[\zeta_p]$. We identify them with $e_0, e_1, \ldots, e_{p-2}, -\sum_{i=0}^{p-2} e_i$ in $\mathbb{Z}^{p-1}$. Hence we obtain:

Proposition 4. *The cyclotomic polytope $\mathcal{C}_p \subset \mathbb{R}^{p-1}$, for p prime, is the simplex*

$$\mathcal{C}_p \quad = \quad \mathrm{conv}\left(e_0, e_1, \ldots, e_{p-2}, -\sum_{i=0}^{p-2} e_i\right).$$

The only interior lattice point of $\mathcal{C}_p$ is the origin.

In order to describe $\mathcal{C}_m$ for general m we need two operations on polytopes. The first one is the *direct sum* (sometimes called *free sum*; see [12, 15, 18]). Let $P \subset \mathbb{R}^{d_1}$ and $Q \subset \mathbb{R}^{d_2}$ be two polytopes each of which contains the origin in its interior. Then we define

$$P \circ Q := \mathrm{conv}\left(P \times \mathbf{0}_{d_2}, \mathbf{0}_{d_1} \times Q\right) \subset \mathbb{R}^{d_1+d_2}.$$

Here $\mathbf{0}_d$ denotes the origin in $\mathbb{R}^d$. The polytope $P \circ Q$ contains $\mathbf{0}_{d_1+d_2}$ in its interior and its dimension is the sum of the dimensions of P and Q. We denote the k-fold direct sum $P \circ \cdots \circ P$ by $P^{\circ k}$.

For a prime p and an integer $\alpha \geq 2$, let $\zeta := \zeta_{p^\alpha}$ be a primitive $(p^\alpha)^{\text{th}}$ root of unity. The powers $\zeta^{k+jp^{\alpha-1}}$, where $0 \leq k \leq p^{\alpha-1} - 1$ and $0 \leq j \leq p - 2$, form a lattice basis of $\mathbb{Z}[\zeta_{p^\alpha}]$, and we will identify them with the standard unit vectors in $\mathbb{Z}^{\phi(p^\alpha)} = \mathbb{Z}^{p^{\alpha-1}(p-1)}$. When we do the identification as $\zeta^{k+jp^{\alpha-1}} \longleftrightarrow e_{k(p-1)+j}$, the

cyclotomic polytope $\mathcal{C}_{p^\alpha}$ is

$$\mathcal{C}_{p^\alpha} = \mathrm{conv}\left(e_{k(p-1)+0}, e_{k(p-1)+1}, \ldots, e_{k(p-1)+p-2}, -\sum_{n=0}^{p-2} e_{k(p-1)+n} : k = 0, \ldots, p^{\alpha-1}-1\right).$$

Proposition 5. *The cyclotomic polytope $\mathcal{C}_{p^\alpha}$, where p is prime, is equal to $\mathcal{C}_p^{\circ p^{\alpha-1}}$. This polytope is a simplicial polytope of dimension $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ and the origin is the only interior lattice point.*

Proof. As above, let $\zeta := \zeta_{p^\alpha}$ be a primitive $(p^\alpha)^{\mathrm{th}}$ root of unity. Since $\Phi_p\left(\zeta^{p^{\alpha-1}}\right) = 0$ we have

$$-1 - \zeta^{p^{\alpha-1}} - \zeta^{2p^{\alpha-1}} - \cdots - \zeta^{(p-2)p^{\alpha-1}} = \zeta^{(p-1)p^{\alpha-1}}.$$

By multiplying this expression with ζ^k for $k = 0, \ldots, p^{\alpha-1} - 1$ we get

$$-\zeta^k - \zeta^{k+p^{\alpha-1}} - \zeta^{k+2p^{\alpha-1}} - \cdots - \zeta^{k+(p-2)p^{\alpha-1}} = \zeta^{k+(p-1)p^{\alpha-1}}.$$

The roots of unity that appear on the left-hand side are all distinct and they are ζ^j for $j = 0, \ldots, (p-1)p^{\alpha-1} - 1$. This is our chosen lattice basis of $\mathbb{Z}[\zeta]$.

By Proposition 4, $\mathcal{C}_{p^\alpha}$ is precisely $\mathcal{C}_p^{\circ p^{\alpha-1}}$. It follows that $\mathcal{C}_{p^\alpha}$ is simplicial since $P \circ Q$ is simplicial if P and Q are: the facets of $P \circ Q$ are the sets of the form $\mathrm{conv}\,(F_1 \times \mathbf{0}_{d_2}, \mathbf{0}_{d_1} \times F_2)$, where F_1 is a facet of P and F_2 is a facet of Q. Furthermore, if F_1 and F_2 are simplices, so is $\mathrm{conv}\,(F_1 \times \mathbf{0}_{d_2}, \mathbf{0}_{d_1} \times F_2)$. $\qquad\square$

Example (The cyclotomic polytope $\mathcal{C}_9$)**.** To clarify the proof of Proposition 5 we treat the case $m = 9 = 3^2$. Since $\Phi_3(x) = 1 + x + x^2$ we get

$$-1 - \zeta^3 = \zeta^6, \quad -\zeta - \zeta^4 = \zeta^7, \quad -\zeta^2 - \zeta^5 = \zeta^8,$$

where $\zeta = \zeta_9$ is a primitive 9th root of unity. So

$$\mathcal{C}_9 = \mathrm{conv}\,(e_0,\ e_1,\ -e_0 - e_1,\ e_2,\ e_3,\ -e_2 - e_3,\ e_4,\ e_5,\ -e_4 - e_5),$$

and this is exactly $\mathcal{C}_3 \circ \mathcal{C}_3 \circ \mathcal{C}_3$.

We now recursively construct a lattice basis for $\mathbb{Z}[\zeta_m]$ and the cyclotomic polytope $\mathcal{C}_m$, by factoring $m = m_1 m_2$, where m_1 and m_2 are relatively prime, and assuming that bases for $\mathbb{Z}[\zeta_{m_1}]$ and $\mathbb{Z}[\zeta_{m_2}]$ and the cyclotomic polytopes $\mathcal{C}_{m_1}$ and $\mathcal{C}_{m_2}$ in these bases are already constructed.

So assume that $\omega_1, \ldots, \omega_{\phi(m_1)}$ form a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta_{m_1}]$, and together with $\omega_{\phi(m_1)+1}, \ldots, \omega_{m_1}$ they form a monoid basis. Then

$$\mathcal{C}_{m_1} = \mathrm{conv}\,\left(e_1, \ldots, e_{\phi(m_1)}, v_{\phi(m_1)+1}, \ldots, v_{m_1}\right) \subset \mathbb{R}^{\phi(m_1)}.$$

Similarly, we assume that $\rho_1, \ldots, \rho_{\phi(m_2)}$ form a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta_{m_2}]$, and together with $\rho_{\phi(m_2)+1}, \ldots, \rho_{m_2}$ they form a monoid basis. Now

$$\mathcal{C}_{m_2} = \mathrm{conv}\,\left(f_1, \ldots, f_{\phi(m_2)}, w_{\phi(m_2)+1}, \ldots, w_{m_2}\right) \subset \mathbb{R}^{\phi(m_2)}.$$

For the cyclotomic lattice $\mathbb{Z}[\zeta_m]$ the set of mth roots $\{\omega_i \rho_j \ : \ 1 \leq i \leq \phi(m_1),\ 1 \leq j \leq \phi(m_2)\}$ is a basis, and the pairwise product of the lattice points in $\mathbb{R}^{\phi(m)}$ corresponding to *all* of the m_1^{th} and m_2^{th} roots is a monoid basis of $\mathbb{Z}[\zeta_m]$. We define the cyclotomic polytope $\mathcal{C}_m$ to be the convex hull of the vectors in this monoid basis.

This construction motivates the second polytope operation we need, namely the tensor product of two polytopes. Let $P \subset \mathbb{R}^{d_1}$ and $Q \subset \mathbb{R}^{d_2}$ be two polytopes with vertices $v_1, \ldots, v_s$ and $w_1, \ldots, w_t$, respectively. Then $P \otimes Q \subset \mathbb{R}^{d_1 d_2}$ is the polytope

$$P \otimes Q := \mathrm{conv}\,(v_i \otimes w_j \,:\, 1 \leq i \leq s, \ 1 \leq j \leq t)\,.$$

Our construction of $\mathcal{C}_m$ immediately implies:

Proposition 6. *Let* $m = m_1 m_2$ *where* $m_1, m_2 > 1$ *are relatively prime. Then the cyclotomic polytope* $\mathcal{C}_m$ *is equal to* $\mathcal{C}_{m_1} \otimes \mathcal{C}_{m_2}$.

Propostions 4, 5, and 6 allow us to describe the cyclotomic polytope $\mathcal{C}_m$ for any positive integer m. Moreover, $\mathcal{C}_m$ is determined by $\mathcal{C}_{\sqrt{m}}$.

Theorem 7. *The cyclotomic polytope* $\mathcal{C}_m$ *is equal to* $\mathcal{C}_{\sqrt{m}}^{\circ(m/\sqrt{m})}$ *where* $\sqrt{m}$ *is the squarefree part of* m.

Proof. Let $m = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. Propositions 5 and 6 imply that $\mathcal{C}_m = \bigotimes_{i=1}^{n} \mathcal{C}_{p_i}^{\circ p^{\alpha_i - 1}}$. If we let V_i be the matrix whose columns are the vertices of $\mathcal{C}_{p_i}$, then the polytope $\mathcal{C}_{p_i}^{\circ p^{\alpha_i - 1}}$ is equal to $\mathrm{conv}\left(V_i \otimes I_{p^{\alpha_i - 1}}\right)$, where I_k denotes a $k \times k$ identity matrix. Therefore

$$\mathcal{C}_m = \mathrm{conv}\left(\bigotimes_{i=1}^{n}(V_i \otimes I_{p^{\alpha_i - 1}})\right) = \mathrm{conv}\left(\bigotimes_{i=1}^{n} V_i \otimes \bigotimes_{i=1}^{n} I_{p^{\alpha_i - 1}}\right).$$

The last expression is precisely $\mathcal{C}_{\sqrt{m}}^{\circ(m/\sqrt{m})}$. $\square$

Lemma 8. *Let* $m = p_1 p_2 \cdots p_k$, *where* $p_1, p_2, \ldots, p_k$ *are distinct primes. Then the vertices of* $\mathcal{C}_m$ *have coordinates in* $\{0, +1, -1\}$, *and they are precisely the tensor products of the vertices of* $\mathcal{C}_{p_1}, \ldots, \mathcal{C}_{p_k}$. *The only other lattice point in* $\mathcal{C}_m$ *is the origin, which is in the interior of* $\mathcal{C}_m$.

Proof. The vertices of $\mathcal{C}_m$ have coordinates in $\{0, +1, -1\}$ by construction. It is clear that none of the tensor products of the vertices of $\mathcal{C}_{p_1}, \ldots, \mathcal{C}_{p_k}$ is a convex combination of the others, so they are all vertices. It remains to prove that the origin is the only other lattice point in $\mathcal{C}_m$. If m is prime, Proposition 4 says that there is no other lattice point aside from the origin and the vertices. Now let $m = np$ where n is squarefree, not divisible by p, and p is prime. By induction, $\mathcal{C}_n$ does not contain any lattice point other than the origin and its vertices. Let A_m be the matrix whose columns are the vertices of $\mathcal{C}_m$, then

$$A_m = \begin{bmatrix} A_n & & & -A_n \\ & A_n & & -A_n \\ & & \ddots & \vdots \\ & & A_n & -A_n \end{bmatrix}.$$

(This matrix has p column blocks and $p-1$ row blocks.) Now suppose there is a nonzero lattice point $u \in \mathcal{C}_m$ that is a nontrivial convex combination of the vertices. The point u is a $0, \pm 1$ vector, and we may assume that it has first coordinate 1. Then u has to be a convex combination of vertices of $\mathcal{C}_m$ that have 1 as the first coordinate. This means that u is a convex combination of such vectors coming from the first A_n-block of A_m and the top $(-A_n)$-block. By looking at the coordinates of the first

row of the second block of A_n's in A_m, we see that the corresponding coordinate of u is strictly between 0 and 1 if in the convex combination vectors from both the first A_n and the top $(-A_n)$-block were used. Hence u must be a convex combination of the first n columns of A_m, which contradicts our induction hypothesis.   □

Corollary 9. *The cyclotomic polytope $\mathcal{C}_m$ is a $\{0, +1, -1\}$-polytope with only one lattice point other than its vertices. This lattice point is the origin and it is in the interior of $\mathcal{C}_m$.*

Proof. This follows from Theorem 7 and Lemma 8.   □

We will return to the combinatorial structure of $\mathcal{C}_m$ in Section 4.

3. Hilbert series and unimodular triangulations

Let $\mathcal{L} \subset \mathbb{Z}^d$ be a lattice, let M be a minimal set of monoid generators, and let K be an arbitrary field. The monoid (semigroup) algebra $K[M']$, where $M' = \{(u, 1) : u \in M \cup \{0\}\}$, is a finitely generated graded K-algebra where each monomial in $K[M']$ corresponds to (v, k) where $v = \sum_{u_i \in M \cup \{0\}} n_i u_i$ with nonnegative integer coefficients n_i such that $\sum n_i = k$. Such an element has degree k in $K[M']$. In this setting the *Hilbert series* of $K[M']$ is

$$H(K[M']; x) := \sum_{k \geq 0} \dim_K \left(K[M']_k\right) x^k,$$

where $K[M']_k$ denotes the vector space of elements of degree k in this graded algebra. It is a standard result of commutative algebra that

$$H(K[M']; x) = \frac{h(x)}{(1-x)^{d+1}}$$

where $h(x)$ is a polynomial of degree at most d [1, Chapter 11]. When $\mathcal{L} \cong \mathbb{Z}^d$, it is clear that the number of elements in $\mathcal{L}$ of length exactly k (with respect to M) is equal to $\dim_K(K[M']_k) - \dim_K(K[M']_{k-1})$, and therefore the growth series is

$$G(x) = (1-x)H(K[M']; x) = \frac{h(x)}{(1-x)^d},$$

and this reproves the rationality of $G(x)$ in this case.

Lemma 10. *Let $K[M']$ be the monoid algebra corresponding to the cyclotomic polytope $\mathcal{C}_m$. Let N be the lattice points in $\mathcal{C}_m \circ \mathcal{C}_m$ and $K[N']$ be the corresponding monoid algebra. Then*

$$H(K[N']; x) = H(K[M']; x) \cdot H(K[M']; x).$$

Proof. This follows from

$$\dim_K \left(K[N']_k\right) = \sum_{s+t=k} \dim_K \left(K[M']_s\right) \dim_K \left(K[M']_t\right).$$

□

The statement of Theorem 2, namely that $h_m(x) = \left(h_{\sqrt{m}}(x)\right)^{m/\sqrt{m}}$, follows now immediately from Theorem 7 and Lemma 10:

Proof of Theorem 2. Let $N = \mathcal{C}_m \cap \mathbb{Z}^{\phi(m)}$ and $M = \mathcal{C}_{\sqrt{m}} \cap \mathbb{Z}^{\phi(\sqrt{m})}$, and let $K[N']$ and $K[M']$ be the corresponding monoid algebras. Theorem 7 implies $\mathcal{C}_m = \mathcal{C}_{\sqrt{m}}^{\circ(m/\sqrt{m})}$ and Lemma 10 implies that

$$H(K[N']; x) = \left(H(K[M']; x)\right)^{m/\sqrt{m}}.$$

This means that $h_m(x) = \left(h_{\sqrt{m}}(x)\right)^{m/\sqrt{m}}$. $\qquad\square$

Now let $\mathcal{P}_M \subset \mathbb{R}^d$ be the convex hull of M. Suppose that the set of lattice points $\mathcal{P}_M \cap \mathbb{Z}^d$ is equal to $M \cup \{0\}$. Corollary 9 implies that $\mathcal{C}_m$ has this property. In general, the monoid generated by M' and the monoid of the lattice points in the cone generated by M' are not equal. In the case of the equality we call M', $\mathcal{P}_M$, and $K[M']$ *normal*. We give a necessary condition for the normality of these objects below. Note that when $\mathcal{P}_M$ is normal then the set of lattice points in $\text{cone}(M') \cap \{x : x_{d+1} = k\}$ is in bijection with the set of lattice points in $k\mathcal{P}_M$, the kth dilate of $\mathcal{P}_M$.

A simplex with vertices $v_0, v_1, \ldots, v_d \subset \mathbb{Z}^d$ is *unimodular* if $\mathbb{Z}^d$ is generated by $\{v_1 - v_0, v_2 - v_0, \ldots, v_d - v_0\}$. This is equivalent to $|\det(v_1 - v_0, v_2 - v_0, \ldots, v_d - v_0)| = 1$. A *unimodular triangulation* of a polytope $\mathcal{P}$ is a triangulation into unimodular simplices with vertices in $\mathcal{P} \cap \mathbb{Z}^d$.

Lemma 11. *If $\mathcal{P}_M$ has a unimodular triangulation then $\mathcal{P}_M$ is normal.*

Proof. For each unimodular simplex $\sigma = \{v_0, v_1, \ldots, v_r\}$ in this triangulation we consider

$$\text{cone}(\sigma) = \text{cone}\left(\begin{pmatrix} 1 \\ v_0 \end{pmatrix}, \begin{pmatrix} 1 \\ v_1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 \\ v_r \end{pmatrix}\right)$$

These cones cover $\text{cone}(M')$ and the absolute value of the determinant of their generators is one. If $z \in \text{cone}(M')$ then z is in one of the $\text{cone}(\sigma)$, and if it has integer coordinates, Cramer's Rule implies that z is a nonnegative integer linear combination of the generators of this cone. This shows that M' is normal. $\qquad\square$

Definition. A matrix with $0, +1, -1$ entries is called *totally unimodular* if every square submatrix has determinant $0, +1,$ or -1. We say that a polytope $\mathcal{P}$ is *totally unimodular* if the matrix whose columns are the lattice points in $\mathcal{P}$ is totally unimodular.

If $\mathcal{P}$ contains the origin in its interior and is totally unimodular, then any triangulation of $\mathcal{P}$ that is a cone with apex the origin is unimodular. We will show that the polytope $\mathcal{C}_m$, where m is an integer described in Theorem 3, is totally unimodular. We will use the following characterization of totally unimodular matrices.

Theorem 12. [19, Theorem 19.3] *A matrix A with $0, +1, -1$ entries is totally unimodular if and only if each collection of columns of A can be split into two parts so that the sum of the columns in one part minus the sum of the columns in the other part is a vector with entries only $0, +1,$ and -1.*

Theorem 13. *The polytope $\mathcal{C}_m$ is totally unimodular for all m described in Theorem 3.*

Proof. Given $\mathcal{C}_m$, we let A_m be the matrix of its vertices. By Corollary 9 this matrix has $0, +1, -1$ entries. The matrix $\begin{bmatrix} B & 0 \\ 0 & C \end{bmatrix}$ is totally unimodular if and only if B and C are. By Theorem 7, we may assume that m is squarefree, that is, m is prime, the product of two primes, or $m = 2pq$, where p and q are odd primes.

In the first case $A_p = [I_{p-1} \ -\mathbf{1}]$ where $\mathbf{1}$ is a column of all ones. This matrix is clearly totally unimodular.

The matrix for the case $m = pq$ is

$$
A_{pq} = \begin{bmatrix} A_p & & & -A_p \\ & A_p & & -A_p \\ & & \ddots & \vdots \\ & & A_p & -A_p \end{bmatrix}.
$$

Now we use Theorem 12 and split the columns of A_{pq} into two parts. Given a subset of the columns of A_{pq} we put all the columns in the last block into the first part. The sum of these columns is a vector with entries either 0 and -1 only, or 0 and $+1$ only, depending on whether the last column of this block (a $+\mathbf{1}$) is included or not. We treat the second case, and the first case can be dealt with similarly. We put all the columns that involve $-\mathbf{1}$ also in the first part. Now the sum of all these columns is a vector with $0, +1$, and -1 only. The remaining columns are columns of $I_{(p-1)(q-1)}$, and we can arrange them to be put in the two parts so that the resulting vector has only $0, +1$, and -1 entries.

Finally, the matrix A_{2pq} equals $[A_{pq} \ -A_{pq}]$, and we immediately conclude that A_{2pq} is also totally unimodular. $\qquad\square$

Remark. Total unimodularity breaks down already in the case of $\mathcal{C}_{3pq}$, where p and q are distinct primes > 3. Here

$$
A_{3pq} = \begin{bmatrix} A_{pq} & & -A_{pq} \\ & A_{pq} & -A_{pq} \end{bmatrix},
$$

and the columns

$$
\begin{pmatrix} \mathbf{0}_{(p-1)(q-1)} \\ \mathbf{1}_{(p-1)(q-1)} \end{pmatrix}, \quad \begin{pmatrix} 1 \\ \mathbf{0}_{p-2} \\ \vdots \\ 1 \\ \mathbf{0}_{p-2} \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} \mathbf{1}_{p-1} \\ \mathbf{0}_{(p-1)(q-2)} \\ \mathbf{1}_{p-1} \\ \mathbf{0}_{(p-1)(q-2)} \end{pmatrix}
$$

violate the condition of Theorem 12. When $m = pqr$ for primes $p, q, r > 3$, the polytope $\mathcal{C}_m$ is also not totally unimodular. This follows from the non-normality of the monoid algebra of the three-dimensional $(p-1) \times (q-1) \times (r-1)$ transportation polytope [24, p. 77]. Hence $\mathcal{C}_m$ is not totally unimodular when m is divisible by three or more odd primes.

4. Palindromy

The monoid algebra $K[M']$ is a finitely generated graded K-algebra, and hence $K[M']$ is isomorphic to $K[x_1, \ldots, x_n]/I_M$ where $n = |M'|$ and I_M is a homogeneous *toric ideal* [22]. For the results in this section we need the notion of *initial ideals*.

In the polynomial ring $R = K[x_1, \ldots, x_n]$, we abbreviate the monomial $x_1^{u_1} \cdots x_n^{u_n}$ by x^u. A *term order* $\prec$ is a well ordering of all the monomials in R (with the minimum element $x^0 = 1$) that is compatible with multiplication; that is, $x^u \prec x^v$ implies that $x^w x^u \prec x^w x^v$ for any monomial x^w. Given a nonzero polynomial f and a term order $\prec$, we let $\mathsf{in}_\prec(f)$, the *initial term* of f, be the largest monomial of f with respect to $\prec$. If I is an ideal, the *initial ideal* of I with respect to the term order $\prec$ is the monomial ideal generated by all the initial terms of polynomials in I:

$$\mathsf{in}_\prec(I) = \langle \mathsf{in}_\prec(f) \ : \ f \in I \rangle.$$

Proposition 14. [9, Chapter 15] *Let I be a homogeneous ideal in R and $\prec$ any term order. Then for all k, $(R/I)_k$ and $(R/\mathsf{in}_\prec(I))_k$ are isomorphic K-vector spaces, and therefore $H(R/I; x) = H(R/\mathsf{in}_\prec(I); x)$.*

The following result follows from Corollary 8.4 and Corollary 8.9 in [22]. The regular triangulation $\Delta_\prec$ of M is obtained by lifting each point in M by ω_i where $\omega = (\omega_1, \ldots, \omega_n)$ is a weight vector so that $\mathsf{in}_\prec(I_M) = \mathsf{in}_\omega(I_M)$, and then by taking the convex hull of these lifted points. The facets of the lower hull of this convex hull form $\Delta_\prec$; see [22, Chapter 8] for more details.

Theorem 15. *Let $K[M']$ be a monoid algebra and I_M be the corresponding toric ideal. The initial ideal $\mathsf{in}_\prec(I_M)$ is squarefree if and only if the regular triangulation $\Delta_\prec$ of M induced by $\prec$ is unimodular. In this case $\mathsf{in}_\prec(I_M)$ is the Stanley-Reisner ideal of $\Delta_\prec$ viewed as a simplicial complex.*

The *f-vector* $(f_{-1}, f_0, \ldots, f_{d-1})$ of the d-polytope $\mathcal{P}$ consists of its face numbers, so $f_{-1} = 1$ (corresponding to the empty face), f_0 is the number of vertices of $\mathcal{P}$, f_1 the number of edges, and so on, up to f_{d-1}, the number of facets. Closely related is the *h-vector* $(h_0, h_1, \ldots, h_d)$ of $\mathcal{P}$, defined through

$$\sum_{j=0}^{d} h_j x^j = \sum_{k=0}^{d} f_{k-1} (x-1)^{d-k} .$$

The left-hand side is the *h-polynomial* of $\mathcal{P}$. Explicitly, h_j is given by

$$h_j = \sum_{k=0}^{j} (-1)^{j-k} \binom{d-k}{j-k} f_{k-1} .$$

The famous *Dehn–Sommerville Relations* assert that, for a simplicial polytope, $h_j = h_{d-j}$.

We are now ready to prove Theorem 3, namely that the coordinator polynomial of $\mathbb{Z}[\zeta_m]$, when m is divisible by at most two odd primes, is of the form $h(x)^{m/\sqrt{m}}$, where $h(x)$ is the h-polynomial of a simplicial polytope. This implies that $h(x)$ is palindromic, unimodal, and has nonnegative integer coefficients.

Proof of Theorem 3. Theorem 2 reduces the discussion to the case when m is square-free. By Theorem 13 the polytope $\mathcal{C}_m$ is totally unimodular. Corollary 9 implies that any triangulation of $\mathcal{C}_m$ induced by a triangulation of its boundary (by coning over the boundary triangulation using the origin as the apex) is unimodular. Now we can use a *pulling* (*reverse lexicographic* [22, Chapter 8]) triangulation of the boundary of $\mathcal{C}_m$

to obtain such a unimodular *regular* triangulation $\Delta_\prec$. We note that this boundary triangulation is the boundary of a simplicial polytope $Q_\prec$ of the same dimension as $\mathcal{C}_m$ (see [20] for the construction of such a triangulation). By Theorem 15 the initial ideal $\text{in}_\prec(I_M)$ is squarefree and it is the Stanley-Reisner ideal of $\Delta_\prec$. Proposition 14 implies that $H(K[M']; x) = H(R/\text{in}_\prec(I_M)); x)$ and this rational function's numerator is the h-polynomial of $Q_\prec$ [21, Theorem II.1.4]. Now the Dehn–Sommerville relations imply palindromy of the numerator of the growth series. Unimodality and nonnegativity follow from [21, Theorem III.1.1]. $\square$

Corollary 16. *If $\mathcal{C}_m$ is a simplicial polytope then the coordinator polynomial of $\mathbb{Z}[\zeta_m]$ equals the h-polynomial of $\mathcal{C}_m$.*

Proof. As in the above proof, we use the unimodular regular triangulation $\Delta_\prec$ obtained by coning over the boundary of $\mathcal{C}_m$ using the origin as the apex. $\square$

Example. (The coordinator polynomial of $\mathbb{Z}[\zeta_{180}]$). Since $m = 180 = 2^2 \cdot 3^2 \cdot 5$ the coordinator polynomial is of the form $p(x)^6$ where $p(x)$ is the coordinator polynomial of $\mathbb{Z}[\zeta_{30}]$. Using the software `4ti2` [11] we computed a reverse lexicographic initial ideal of the toric ideal I_M where $M = \mathcal{C}_{30} \cap \mathbb{Z}^8$. This initial ideal has 615 squarefree minimal generators. Then we used the computer algebra system `CoCoA` [6] to compute the Hilbert series from this monomial ideal to obtain

$$p(x) = x^8 + 22x^7 + 208x^6 + 874x^5 + 1480x^4 + 874x^3 + 208x^2 + 22x + 1.$$

Remark. The polytope $\mathcal{C}_m$ is not simplicial in general. For example, when $m = 30$ the polytope $\mathcal{C}_{30}$ is a non-simplicial polytope of dimension 8 with 810 facets. This polytope has two types of facets: 450 of them are simplicial, and the rest of them are facets with 10 vertices. Proposition 4, Proposition 5, and Theorem 7 together with Proposition 17 below imply that the other candidates for non-simplicial $\mathcal{C}_m$ for $m < 30$ are $m = 15$ and $m = 21$. However, in these cases the two polytopes are simplicial; $\mathcal{C}_{15}$ has 360 facets and $\mathcal{C}_{21}$ has 4410 facets. Hence $\mathcal{C}_{30}$ is the smallest non-simplicial cyclotomic polytope. We have also checked that $\mathcal{C}_{33}$ and $\mathcal{C}_{35}$ are simplicial with 554400 and 1134000 facets, respectively. This led us to the following result whose proof was suggested by Robin Chapman [5].

Proposition 17. *The cyclotomic polytope $\mathcal{C}_{pq}$, where p and q are prime, is simplicial.*

The result follows from a polytope duality between $\mathcal{C}_m$ and certain multidimensional transportation polytopes. We first introduce these polytopes. Let $p_1, \ldots, p_k$ be positive integers. A *multidimensional table* is a $p_1 \times \cdots \times p_k$ array of real numbers. We will denote the entries of such a table $\mathbf{x}$ by $x_{i_1 \ldots i_k}$. Now suppose for each $i = 1, \ldots, k$ there is a $(k-1)$-dimensional table $\mathbf{b^i}$ of size $p_1 \times \cdots \times \widehat{p_i} \times \cdots \times p_k$ with nonnegative real entries. Then

$$P\left(\mathbf{b^1}, \ldots, \mathbf{b^k}\right) :=$$
$$\left\{ \mathbf{x} \in \mathbb{R}_{\geq 0}^{\prod p_i} : \begin{array}{ll} \sum_{j=1}^{p_1} x_{j\, i_2 \ldots i_k} = b^1_{i_2 \ldots i_k} & \forall\, (i_2, \ldots, i_k) \in [p_2] \times \cdots \times [p_k] \\ \sum_{j=1}^{p_2} x_{i_1\, j\, i_3 \ldots i_k} = b^2_{i_1 i_3 \ldots i_k} & \forall\, (i_1, i_3, \ldots, i_k) \in [p_1] \times [p_3] \cdots \times [p_k] \\ \quad\vdots & \\ \sum_{j=1}^{p_k} x_{i_1 \ldots i_{k-1} j} = b^k_{i_1 \ldots i_{k-1}} & \forall\, (i_1, \ldots, i_{k-1}) \in [p_1] \times \cdots \times [p_{k-1}] \end{array} \right\}$$

is a *multidimensional transportation polytope* defined by the tables $\mathbf{b^1}, \ldots, \mathbf{b^k}$. We will be concerned with a very particular type of transportation polytopes, namely, given integers $p_1, \ldots, p_k$ we let $\mathbf{b^i}$ be the table all whose entries are equal to p_i. Such a transportation polytope will be denoted by $P(p_1, \ldots, p_k)$. For instance, when $k = 2$, $P(p_1, p_2)$ is the "usual" transportation polytope consisting of nonnegative $p_1 \times p_2$ matrices with all row sums equal to p_2 and all column sums equal to p_1. Now we can state the duality theorem.

Theorem 18. *Let $m = p_1 p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are distinct primes. Then the cyclotomic polytope $\mathcal{C}_m$ and the transportation polytope $P(p_1, \ldots, p_k)$ are dual to each other.*

Proof. We will show that the face lattice of $\mathcal{C}_m$ and $P(p_1, \ldots, p_k)$ are dual to each other. First we show that there is a bijection between the facets of $\mathcal{C}_m$ and the vertices of $P(p_1, \ldots, p_k)$. Each facet of $\mathcal{C}_m$ is defined by a linear form $f(x) = 1$. Now let $\mathbf{y}$ be the $p_1 \times \cdots \times p_k$ table where $y_{i_1 \ldots i_k} = f(v_{i_1}^1 \otimes v_{i_2}^2 \otimes \cdots \otimes v_{i_k}^k)$ where $v_{i_j}^j$ is a vertex of $\mathcal{C}_{p_j}$. The entries of $\mathbf{y}$ are at most 1, and those entries that are equal to 1 are in bijection with the vertices on the facet defined by $f(x) = 1$. Since the sum of the vertices of each C_{p_j} is the origin, we conclude that

$$\sum_{j=1}^{p_1} y_{j\, i_2 \ldots i_k} = 0 \qquad \forall\, (i_2, \ldots, i_k) \in [p_2] \times \cdots \times [p_k]$$

$$\sum_{j=1}^{p_2} y_{i_1\, j\, i_3 \ldots i_k} = 0 \qquad \forall\, (i_1, i_3, \ldots, i_k) \in [p_1] \times [p_3] \cdots \times [p_k]$$

$$\vdots$$

$$\sum_{j=1}^{p_k} y_{i_1 \ldots i_{k-1} j} = 0 \qquad \forall\, (i_1, \ldots, i_{k-1}) \in [p_1] \times \cdots \times [p_{k-1}].$$

Now we define a new table $\mathbf{x}$ where $x_{i_1 \cdots i_k} = 1 - y_{i_1 \cdots i_k}$. This table is a point of the transportation polytope $P(p_1, \ldots, p_k)$. A facet F of $\mathcal{C}_m$ corresponds to a table in this transportation polytope whose zero entries are in bijection with the vertices of $\mathcal{C}_m$ that are on F. On the other hand, a vertex of $P(p_1, \ldots, p_k)$ is defined by setting some of the entries to zero. This implies that $\mathbf{x}$ has to be a vertex of $P(p_1, \ldots, p_k)$, since otherwise there would be a vertex with more zero entries which in turn give more vertices of $\mathcal{C}_m$ incident to F. This contradiction shows the bijection between the facets of $\mathcal{C}_m$ and the vertices of $P(p_1, \ldots, p_k)$.

To extend this bijection to all faces we make the following observation: If F is a face of $\mathcal{C}_m$ that is the intersection of the facets $F_1, \ldots, F_t$ defined by the linear forms $f_1, \ldots, f_t$, then $f = \sum_{i=1}^{t} \lambda_i f_i$ such that $\lambda_i > 0$ and $\sum_{i=1}^{t} \lambda_i = 1$ can be taken to be a supporting hyperplane of F which is not a supporting hyperplane of faces strictly containing F. Such an f gives rise to $\mathbf{x} = \sum_{i=1}^{t} \lambda_i \mathbf{x^i}$ where the $\mathbf{x^i}$'s are the vertices of $P(p_1, \ldots, p_k)$ corresponding to the facets $F_1, \ldots, F_t$. All such $\mathbf{x}$ form the relative interior of a face G of $P(p_1, \ldots, p_k)$ defined by setting those entries of $\mathbf{x}$ corresponding to the vertices on F equal to zero. The vertices of G are precisely $\mathbf{x^1}, \ldots, \mathbf{x^t}$, since any extra vertex will translate into one more vertex on F. $\qquad \square$

Proof of Proposition 17. The points in $P(p,q)$ are in bijection with nonnegative edge assignments of the complete bipartite graph $K_{p,q}$ with the node partition V_1 and V_2. The edge assignments sum to q at each node in V_1 and to p at each node in V_2 (see, e.g., [4]). If p and q are distinct primes, the vertices of $P(p,q)$ correspond to spanning trees of $K_{p,q}$ that satisfy the same conditions on the edge assignments. The edges of such a spanning tree are in bijection with the positive entries of the vertex $\mathbf{x}$. Hence there are exactly $p+q-1$ such positive entries and exactly $(p-1)(q-1)$ zero entries. Using the bijection established in the above proof we conclude that each facet of $\mathcal{C}_{pq}$ has exactly $(p-1)(q-1)$ vertices. Since the dimension of $\mathcal{C}_{pq}$ is equal to $(p-1)(q-1)$, each facet must be a simplex.   □

5. Explicit computations and a conjectural counterexample

We start with the case of $m = p$, a prime. The vertices of the cyclotomic polytope $\mathcal{C}_p \subset \mathbb{R}^{p-1}$ are the unit vectors $e_1, e_2, \ldots, e_{p-1}$, and $-\mathbf{1} = -\sum_j e_j$. (We apologize for the change of notation from Section 2.) This simplex has the apparent unimodular triangulation

$$\{\mathrm{conv}\,(\mathbf{0}, e_1, e_2, \ldots, e_{p-1}), \mathrm{conv}\,(\mathbf{0}, e_1, \ldots, e_{p-2}, -\mathbf{1}), \ldots, \mathrm{conv}\,(\mathbf{0}, e_2, \ldots, e_{p-1}, -\mathbf{1})\},$$

the only triangulation that uses the origin. Hence Kløve–Parker's Theorem 1 is an immediate consequence of Corollary 16 and the fact that the h-vector of a simplex is $(1, 1, \ldots, 1)$:

$$G(x) = \frac{h_{\mathcal{C}_p}(x)}{(1-x)^p} = \frac{x^{p-1} + x^{p-2} + \cdots + 1}{(1-x)^p} \ .$$

The second case is $m = 2p$ for an odd prime p. $\mathcal{C}_{2p}$ is totally unimodular, and so the facets are supported by hyperplanes of the form

$$(1) \qquad\qquad\qquad a_1 x_1 + \cdots + a_{p-1} x_{p-1} = 1 \ .$$

Furthermore, since $A_{2p} = [I_{p-1} \ -\mathbf{1} \ -I_{p-1} \ \mathbf{1}]$ the a_j's are all 0 or ± 1. Let us call two vertices v_1, v_2 of $\mathcal{C}_{2p}$ *opposite* if $v_2 = -v_1$. A facet cannot contain two opposite vertices because otherwise the right-hand side of (1) would be 0.

Proposition 19. *Suppose p is an odd prime and $k \leq \frac{p-1}{2}$. Then every k-subset of $A_{2p} = [I_{p-1} \ -\mathbf{1} \ -I_{p-1} \ \mathbf{1}]$ that does not contain opposite vertices forms a $(k-1)$-face of $\mathcal{C}_{2p}$.*

Corollary 20. *Suppose p is an odd prime and $k \leq \frac{p-1}{2}$. Then $\mathcal{C}_{2p}$ has*

$$f_{k-1} = 2^k \binom{p}{k}$$

$(k-1)$-faces.

Proof of Proposition 19. Given a k-subset $S \subseteq A_{2p}$ without opposite vectors, we consider two cases, depending whether or not $\pm\mathbf{1} \in S$.

1. case: $\pm\mathbf{1} \notin S$.

First suppose $k \leq \frac{p-1}{2} - 1$. We choose n vectors from I_{p-1} and $m = k - n$ vectors from $-I_{p-1}$. Now, without loss of generality, suppose that these vectors are

$e_1, \ldots, e_n, -e_{n+1}, \ldots, -e_k$. Set $b = \frac{m-n}{p-1-k}$; note that $|b| < 1$ because $k \le \frac{p-1}{2} - 1$. Consider the hyperplane

$$x_1 + \cdots + x_n - x_{n+1} - \cdots - x_k + b\,(x_{k+1} + \cdots + x_{p-1}) = 1 \ .$$

Our k chosen vectors are on this hyperplane, and we claim that the remaining vectors in A_{2p} satisfy

$$(2) \qquad x_1 + \cdots + x_n - x_{n+1} - \cdots - x_k + b\,(x_{k+1} + \cdots + x_{p-1}) < 1 \ .$$

For the remaining unit vectors this follows from $|b| < 1$, and for $x = \pm\mathbf{1}$ (2) becomes the inequality $0 < 1$.

Now suppose $k = \frac{p-1}{2}$. Again we choose n vectors from I_{p-1} and $m = k - n$ vectors from $-I_{p-1}$. If $n \ne 0$ or k, the above proof goes through verbatim. If $n = k$, set $b = -1 + \frac{1}{2k}$ and continue the proof above. If $n = 0$, set $b = 1 - \frac{1}{2k}$ and continue the proof above.

2. case: $\mathbf{1} \in S$. (The case $-\mathbf{1} \in S$ is analogous, so that we will omit it here.)

Again we choose n vectors from I_{p-1} and $m = k - 1 - n$ vectors from $-I_{p-1}$. We may assume these vectors are $e_1, \ldots, e_n, -e_{n+1}, \ldots, -e_{k-1}$. Set $b = \frac{m-n+1}{p-k}$; note that $|b| \le \frac{k}{p-k} < 1$. Consider the hyperplane

$$x_1 + \cdots + x_n - x_{n+1} - \cdots - x_{k-1} + b\,(x_k + \cdots + x_{p-1}) = 1 \ .$$

Our k chosen vectors are on this hyperplane, and again one can easily check that the remaining vectors in A_{2p} satisfy

$$x_1 + \cdots + x_n - x_{n+1} - \cdots - x_{k-1} + b\,(x_k + \cdots + x_{p-1}) < 1 \ .$$

$\square$

Remark. One can use the correspondence of the facets of $\mathcal{C}_{2p}$ to the vertices of $P(2, p)$ described in the proof of Proposition 17 to show that $\mathcal{C}_{2p}$ has $p\binom{p-1}{\frac{p-1}{2}}$ facets. We do not know the number of facets for the more general cyclotomic polytopes $\mathcal{C}_{pq}$ for distinct primes p and q; it would be interesting if the correspondence to transportation polytopes could lead to this number.

Proposition 17 and Corollary 20 allow us to prove Parker's Conjecture 2:

Theorem 21. *The coordinator polynomial of $\mathbb{Z}[\zeta_{2p}]$, where p is an odd prime, equals*

$$h_{2p}(x) = \sum_{k=0}^{\frac{p-3}{2}} (x^k + x^{p-1-k}) \sum_{j=0}^{k} \binom{p}{j} + x^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{j}.$$

Proof. The cyclotomic polytope $\mathcal{C}_{2p}$ is simplicial by Proposition 17, so Corollary 16 applies. For $j \le \frac{p-1}{2}$, Corollary 20 gives

$$h_j = \sum_{k=0}^{j} (-1)^{j-k} \binom{p-1-k}{j-k} f_{k-1} = \sum_{k=0}^{j} (-1)^{j-k} \binom{p-1-k}{j-k} 2^k \binom{p}{k} = \sum_{k=0}^{j} \binom{p}{k},$$

as one easily checks that

$$\sum_{k=0}^{j} (-1)^{j-k} \binom{p-1-k}{j-k} 2^k \binom{p}{k} - \sum_{k=0}^{j-1} (-1)^{j-1-k} \binom{p-1-k}{j-1-k} 2^k \binom{p}{k} = \binom{p}{j}.$$

Palindromy of the h-vector gives h_j for $j > \frac{p-1}{2}$. $\square$

Going beyond $m = p$ or $2p$, next we prove Parker's Conjecture 3.

Corollary 22. *The coordinator polynomial of $\mathbb{Z}[\zeta_{15}]$ equals*

$$c_{\mathbb{Z}[\zeta_{15}]}(x) = (1 + x^8) + 7(x + x^7) + 28(x^2 + x^6) + 79(x^3 + x^5) + 130x^4.$$

Proof. By Proposition 6, the polytope $\mathcal{C}_{15}$ has vertices

$$A_{15} = \begin{bmatrix} I_4 & -\mathbf{1} & & -I_4 & \mathbf{1} \\ & & I_4 & -\mathbf{1} & -I_4 & \mathbf{1} \end{bmatrix},$$

and it is simplicial by Proposition 17. With this data, one can easily use the software
`polymake` [10] to check that $\mathcal{C}_{15}$ has the h-polynomial $x^8 + 7x^7 + 28x^6 + 79x^5 + 130x^4 + 79x^3 + 28x^2 + 7x + 1$. The result now follows with Corollary 16. $\square$

m	$h_{\mathbb{Z}[\zeta_m]}$
6	$x^2 + 4x + 1$
10	$x^4 + 6x^3 + 16x^2 + 6x + 1$
12	$(x^2 + 4x + 1)^2$
14	$x^6 + 8x^5 + 29x^4 + 64x^3 + 29x^2 + 8x + 1$
15	$x^8 + 7x^7 + 28x^6 + 79x^5 + 130x^4 + 79x^3 + 28x^2 + 7x + 1$
18	$(x^2 + 4x + 1)^3$
20	$(x^4 + 6x^3 + 16x^2 + 6x + 1)^2$
21	$x^{12} + 9x^{11} + 45x^{10} + 158x^9 + 432x^8 + 909x^7 + 1302x^6 + \cdots + 1$
22	$x^{10} + 12x^9 + 67x^8 + 232x^7 + 562x^6 + 1024x^5 + 562x^4 + 232x^3$ $\qquad + 67x^2 + 12x + 1$
24	$(x^2 + 4x + 1)^4$
26	$x^{12} + 14x^{11} + 92x^{10} + 378x^9 + 1093x^8 + 2380x^7 + 4096x^6 + \cdots + 1$
28	$(x^6 + 8x^5 + 29x^4 + 64x^3 + 29x^2 + 8x + 1)^2$
30	$x^8 + 22x^7 + 208x^6 + 874x^5 + 1480x^4 + 874x^3 + 208x^2 + 22x + 1$
33	$x^{20} + 13x^{19} + 91x^{18} + 444x^{17} + 1677x^{16} + 5187x^{15} + 13614x^{14}$ $\qquad + 31083x^{13} + 61422x^{12} + 100561x^{11} + 126214x^{10} + \cdots + 1$
34	$x^{16} + 18x^{15} + 154x^{14} + 834x^{13} + 3214x^{12} + 9402x^{11} + 21778x^{10}$ $\qquad + 41226x^9 + 65536x^8 + \cdots + 1$
35	$x^{24} + 11x^{23} + 66x^{22} + 286x^{21} + 1001x^{20} + 2996x^{19} + 7896x^{18}$ $\qquad + 18631x^{17} + 39671x^{16} + 76046x^{15} + 128726x^{14} + 185206x^{13}$ $\qquad + 212926x^{12} + \cdots + 1$
36	$(x^2 + 4x + 1)^6$
38	$x^{18} + 20x^{17} + 191x^{16} + 1160x^{15} + 5036x^{14} + 16664x^{13} + 43796x^{12}$ $\qquad + 94184x^{11} + 169766x^{10} + 262144x^9 + \cdots + 1$
39	$x^{24} + 15x^{23} + 120x^{22} + 667x^{21} + 2865x^{20} + 10068x^{19} + 29998x^{18}$ $\qquad + 77670x^{17} + 177966x^{16} + 363919x^{15} + 655692x^{14} + 1001649x^{13}$ $\qquad + 1214590x^{12} + \cdots + 1$
40	$(x^4 + 6x^3 + 16x^2 + 6x + 1)^4$

FIGURE 1. The coordinator polynomials of $\mathbb{Z}[\zeta_m]$ for $m \leq 41$.

For reference, we give in Figure 1 the first 41 coordinator polynomials. (In the table, we omitted $h_m(x)$ for prime powers m.) The results of this article could be used to compute the coordinator polynomials for $m \leq 104$, where $m = 105$ is the first non-trivial case that our results do not cover. Although in principal these coordinator polynomials could be computed, the feasible range seems to end with $m = 41$ with the current computational tools like `4ti2` [11] which we used for toric initial ideal computations, and `CoCoA` [6] which we used for Hilbert series computations. We offer the following conjecture for the first non-trivial case.

Conjecture 4. *The coordinator polynomial $h_{105}(x)$ is not palindromic.*

We conclude by giving some supporting evidence for this conjecture. We call a polytope $\mathcal{P} \subset \mathbb{R}^d$ *integral* is all its vertices are in $\mathbb{Z}^d$. An integral polytope $\mathcal{P} := \left\{ x \in \mathbb{R}^d : Ax \leq \mathbf{1} \right\}$ that contains the origin in its interior is called *reflexive* if A is an integral matrix [2]. The *Ehrhart series* of an integral d-polytope $\mathcal{P}$ is the rational generating function $\sum_{k \geq 0} \# \left(k\mathcal{P} \cap \mathbb{Z}^d \right) x^k$, which is of the form $\frac{f(x)}{(1-x)^{d+1}}$ for some polynomial f of degree at most d [8]. Hibi [13] proved that an integral polytope that contains the origin in its interior is reflexive if and only if the numerator of its Ehrhart series is palindromic. Since we proved that $\mathcal{C}_m$ is normal if m is divisible by at most two odd primes, Hibi's theorem implies that $\mathcal{C}_m$ is reflexive for these m.

On the other hand, Seth Sullivant [23] computed some of the facets of $\mathcal{C}_{105}$ and found that the defining matrix A is not integral, that is, $\mathcal{C}_{105}$ is *not* reflexive. If one could show that $\mathcal{C}_{105}$ is normal, then this would provide a counterexample to Parker's Conjecture 1.

Acknowledgements

References

[1] M. F. Atiyah and I. G. Macdonald, Introduction to commutative algebra, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[2] V. V. Batyrev, *Dual polyhedra and mirror symmetry for Calabi-Yau hypersurfaces in toric varieties*, J. Algebraic Geom. **3** (1994), no. 3, 493–535.

[3] M. Benson, *Growth series of finite extensions of $\mathbf{Z}^n$ are rational*, Invent. Math. **73** (1983), no. 2, 251–269.

[4] E. D. Bolker, *Simplicial geometry and transportation polytopes*, Trans. Amer. Math. Soc. **217** (1976) 121–142.

[5] R. Chapman, personal communication, August 2005.

[6] CoCoATeam, CoCoA*: a system for doing Computations in Commutative Algebra*, Available at `cocoa.dima.unige.it`.

[7] J. H. Conway and N. J. A. Sloane, *The cell structures of certain lattices*, Miscellanea mathematica, Springer, Berlin, 1991, pp. 71–107.

[8] E. Ehrhart, *Sur les polyèdres rationnels homothétiques à n dimensions*, C. R. Acad. Sci. Paris **254** (1962) 616–618.

[9] D. Eisenbud, Commutative algebra, Graduate texts in mathematics, vol. 150, Springer-Verlag, New York, 1995.

[10] E. Gawrilow and M. Joswig, *polymake: a framework for analyzing convex polytopes*, Polytopes—combinatorics and computation (Oberwolfach, 1997), DMV Sem., vol. 29, Birkhäuser, Basel, 2000, pp. 43–73. Available at `www.math.tu-berlin.de/polymake/`.

[11] R. Hemmecke and R. Hemmecke, *4ti2 version 1.1—computation of Hilbert bases, Graver bases, toric Gröbner bases, and more*, Available at `www.4ti2.de`, September 2003.

[12] M. Henk, J. Richter-Gebert, and G. M. Ziegler, *Basic properties of convex polytopes*, Handbook of Discrete and Computational Geometry (J. E. Goodman and J. O'Rourke, eds.), Chapman & Hall/CRC Press, Boca Raton, second ed., 2004, pp. 355–382.

[13] T. Hibi, *Dual polytopes of rational convex polytopes*, Combinatorica **12** (1992), no. 2, 237–240.

[14] J. Martin and V. Reiner, *Cyclotomic and simplicial matroids*, to appear in Israel J. Math.

[15] P. McMullen, *Constructions for projectively unique polytopes*, Discrete Math. **14** (1976), no. 4, 347–358.

[16] M. G. Parker, *Conjectures on the size of constellations constructed from direct sums of PSK kernels*, Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999), Lecture Notes in Comput. Sci., vol. 1719, Springer, Berlin, 1999, pp. 420–429.

[17] F. Patras and P. Solé, *The coordinator polynomial of some cyclotomic lattices*, to appear in European J. Combinatorics.

[18] M. A. Perles and G. C. Shephard, *Facets and nonfacets of convex polytopes*, Acta Math. **119** (1967) 113–145.

[19] A. Schrijver, *Theory of linear and integer programming*, Wiley-Interscience Series in Discrete Mathematics, John Wiley & Sons Ltd., Chichester, 1986, A Wiley-Interscience Publication.

[20] R. P. Stanley, *Linear Diophantine equations and local cohomology*, Invent. Math. **68** (1982), no. 2, 175–193.

[21] ———, *Combinatorics and commutative algebra*, second ed., Progress in Mathematics, vol. 41, Birkhäuser Boston Inc., Boston, MA, 1996.

[22] B.Sturmfels, *Gröbner bases and convex polytopes*, University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1996.

[23] S.Sullivant, personal communication, January 2006.

[24] M. Vlach, *Conditions for the existence of solutions of the three-dimensional planar transportation problem*, Discrete Appl. Math. **13** (1986), no. 1, 61–78.

[25] P. Wagreich, *The growth function of a discrete group*, Group actions and vector fields (Vancouver, B.C., 1981), Lecture Notes in Math., vol. 956, Springer, Berlin, 1982, pp. 125–144.

DEPARTMENT OF MATHEMATICS, SAN FRANCISCO STATE UNIVERSITY, SAN FRANCISCO, CA 94132
E-mail address: `[beck,serkan]@math.sfsu.edu`