Cyclotomic Polytopes and Growth Series of Cyclotomic Lattices

Matthias Beck & Serkan Hoşten San Francisco State University

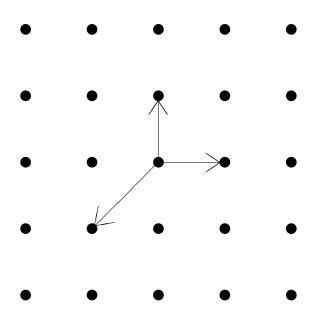
math.sfsu.edu/beck

Math Research Letters

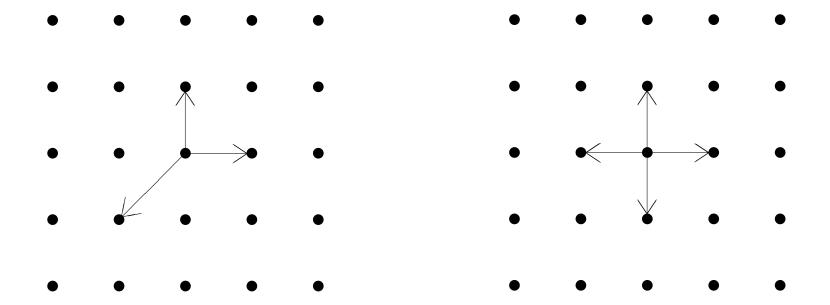
 $\mathcal{L} \subset \mathbb{R}^d$ — lattice of rank rM – subset that generates $\mathcal L$ as a monoid

```
\mathcal{L} \subset \mathbb{R}^d – lattice of rank r
M – subset that generates \mathcal{L} as a monoid
S(n) – number of elements in \mathcal{L} with word length n (with respect to M)
G(x) := \sum_{n \ge 0} S(n) x^n – growth series of (\mathcal{L}, M)
G(x) = \frac{h(x)}{(1-x)^r} where h is the coordinator polynomial of (\mathcal{L}, M)
```

```
\mathcal{L} \subset \mathbb{R}^d – lattice of rank r
M – subset that generates \mathcal{L} as a monoid
S(n) – number of elements in \mathcal{L} with word length n (with respect to M)
G(x) := \sum_{n \ge 0} S(n) x^n – growth series of (\mathcal{L}, M)
G(x) = \frac{h(x)}{(1-x)^r} where h is the coordinator polynomial of (\mathcal{L}, M)
```



```
\mathcal{L} \subset \mathbb{R}^d — lattice of rank r M — subset that generates \mathcal{L} as a monoid S(n) — number of elements in \mathcal{L} with word length n (with respect to M) G(x) := \sum_{n \geq 0} S(n) \, x^n — growth series of (\mathcal{L}, M) G(x) = \frac{h(x)}{(1-x)^r} where h is the coordinator polynomial of (\mathcal{L}, M)
```



Cyclotomic Lattices

```
\mathcal{L} = \mathbb{Z}[e^{2\pi i/m}] \cong \mathbb{Z}^{\varphi(m)}
M – all m^{\mathsf{th}} roots of unity (suitably identified in \mathbb{R}^{arphi(m)})
h_m – coordinator polynomial of \mathbb{Z}[e^{2\pi i/m}]
Initiated by Parker, motivated by error-correcting codes and random walks
```

Cyclotomic Lattices

```
\mathcal{L} = \mathbb{Z}[e^{2\pi i/m}] \cong \mathbb{Z}^{\varphi(m)}
M – all m^{\mathsf{th}} roots of unity (suitably identified in \mathbb{R}^{arphi(m)})
h_m – coordinator polynomial of \mathbb{Z}[e^{2\pi i/m}]
Initiated by Parker, motivated by error-correcting codes and random walks
```

Theorem (Kløve–Parker) The coordinator polynomial of $\mathbb{Z}[e^{2\pi i/p}]$, where p is prime, equals $h_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$.

Cyclotomic Lattices

$$\mathcal{L} = \mathbb{Z}[e^{2\pi i/m}] \cong \mathbb{Z}^{\varphi(m)}$$

M – all m^{th} roots of unity (suitably identified in $\mathbb{R}^{arphi(m)}$)

 h_m – coordinator polynomial of $\mathbb{Z}[e^{2\pi i/m}]$

Initiated by Parker, motivated by error-correcting codes and random walks

Theorem (Kløve-Parker) The coordinator polynomial of $\mathbb{Z}[e^{2\pi i/p}]$, where p is prime, equals $h_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$.

Conjectures (Parker)

(1) $h_m(x) = g(x)^{\frac{m}{\sqrt{m}}}$ for a palindromic polynomial g of degree $\varphi(\sqrt{m})$.

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

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

Conjectures (Parker)

(1) $h_m(x) = g(x)^{\frac{m}{\sqrt{m}}}$ for a palindromic polynomial g of degree $\varphi(\sqrt{m})$.

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

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

Theorem (MB-Hoşten) Suppose m is divisible by at most two odd primes.

(1)
$$h_m(x) = h_{\sqrt{m}}(x)^{\frac{m}{\sqrt{m}}}$$

Conjectures (Parker)

(1) $h_m(x) = g(x)^{\frac{m}{\sqrt{m}}}$ for a palindromic polynomial g of degree $\varphi(\sqrt{m})$.

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

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

Theorem (MB-Hoşten) Suppose m is divisible by at most two odd primes.

(1)
$$h_m(x) = h_{\sqrt{m}}(x)^{\frac{m}{\sqrt{m}}}$$

(2) $h_{\sqrt{m}}(x)$ is the h-polynomial of a simplicial polytope.

Conjectures (Parker)

(1) $h_m(x) = g(x)^{\frac{m}{\sqrt{m}}}$ for a palindromic polynomial g of degree $\varphi(\sqrt{m})$.

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

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

Theorem (MB-Hoşten) Suppose m is divisible by at most two odd primes.

(1)
$$h_m(x) = h_{\sqrt{m}}(x)^{\frac{m}{\sqrt{m}}}$$

(2) $h_{\sqrt{m}}(x)$ is the h-polynomial of a simplicial polytope.

Corollary If m is divisible by at most two odd primes, then $h_{\sqrt{m}}(x)$ is palindromic, unimodal, and has nonnegative integer coefficients.

Conjectures (Parker)

(1) $h_m(x) = g(x)^{\frac{m}{\sqrt{m}}}$ for a palindromic polynomial g of degree $\varphi(\sqrt{m})$.

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

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

Theorem (MB-Hoşten) Suppose m is divisible by at most two odd primes.

(1)
$$h_m(x) = h_{\sqrt{m}}(x)^{\frac{m}{\sqrt{m}}}$$

(2) $h_{\sqrt{m}}(x)$ is the h-polynomial of a simplicial polytope.

Corollary If m is divisible by at most two odd primes, then $h_{\sqrt{m}}(x)$ is palindromic, unimodal, and has nonnegative integer coefficients.

Theorem (MB-Hoșten) Parker's Conjectures (2) & (3) are true.

We choose a specific basis for $\mathbb{Z}[e^{2\pi i/m}]$ consisting of certain powers of $e^{2\pi i/m}$ which we then identify with the unit vectors in $\mathbb{R}^{arphi(m)}$. The other powers of $e^{2\pi i/m}$ are integer linear combinations of this basis; hence they are lattice vectors in $\mathbb{Z}[e^{2\pi i/m}] \subset \mathbb{R}^{\varphi(m)}$. The m^{th} cyclotomic polytope \mathcal{C}_m is the convex hull of all of these m lattice points in $\mathbb{R}^{\varphi(m)}$, which correspond to the m^{th} roots of unity.

We choose a specific basis for $\mathbb{Z}[e^{2\pi i/m}]$ consisting of certain powers of $e^{2\pi i/m}$ which we then identify with the unit vectors in $\mathbb{R}^{arphi(m)}$. The other powers of $e^{2\pi i/m}$ are integer linear combinations of this basis; hence they are lattice vectors in $\mathbb{Z}[e^{2\pi i/m}]\subset \mathbb{R}^{\varphi(m)}$. The m^{th} cyclotomic polytope \mathcal{C}_m is the convex hull of all of these m lattice points in $\mathbb{R}^{\varphi(m)}$, which correspond to the m^{th} roots of unity. We will do this recursively in three steps:

- (1) m is prime
- (2) m is a prime power
- (3) m is the product of two coprime integers.

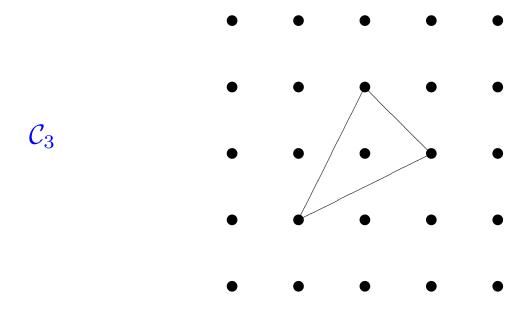
We choose a specific basis for $\mathbb{Z}[e^{2\pi i/m}]$ consisting of certain powers of $e^{2\pi i/m}$ which we then identify with the unit vectors in $\mathbb{R}^{\varphi(m)}$. The other powers of $e^{2\pi i/m}$ are integer linear combinations of this basis; hence they are lattice vectors in $\mathbb{Z}[e^{2\pi i/m}] \subset \mathbb{R}^{\varphi(m)}$. The m^{th} cyclotomic polytope \mathcal{C}_m is the convex hull of all of these m lattice points in $\mathbb{R}^{\varphi(m)}$, which correspond to the m^{th} roots of unity. We will do this recursively in three steps:

- (1) m is prime
- (2) m is a prime power
- (3) m is the product of two coprime integers.

When m=p is a prime number, let $\zeta=e^{2\pi i/p}$ and fix the \mathbb{Z} -basis $1,\zeta,\zeta^2,\ldots,\zeta^{p-2}$ of the lattice $\mathbb{Z}[\zeta]$. Together with $\zeta^{p-1}=-\sum_{j=0}^{p-2}\zeta^j$, these p elements form a monoid basis for $\mathbb{Z}[\zeta]$. We identify them with $e_0,e_1,\ldots,e_{p-2},-\sum_{j=0}^{p-2}e_j$ in \mathbb{R}^{p-1} and define the cyclotomic polytope $\mathcal{C}_p\subset\mathbb{R}^{p-1}$ as the simplex

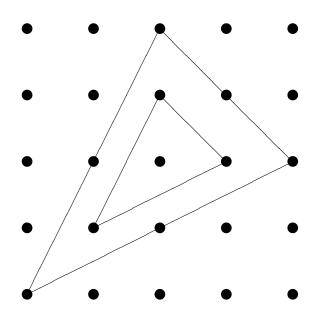
$$C_p = \text{conv}\left(e_0, e_1, \dots, e_{p-2}, -\sum_{i=0}^{p-2} e_i\right).$$

$$C_p = \text{conv}\left(e_0, e_1, \dots, e_{p-2}, -\sum_{i=0}^{p-2} e_i\right).$$



$$C_p = \text{conv}\left(e_0, e_1, \dots, e_{p-2}, -\sum_{i=0}^{p-2} e_i\right).$$

 \mathcal{C}_3

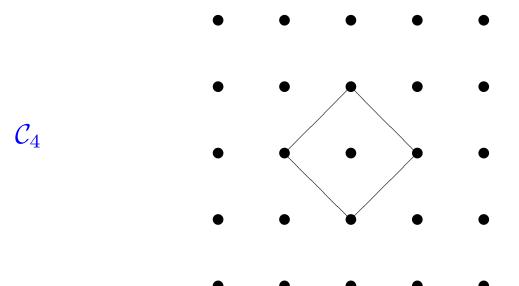


For two polytopes $P \subset \mathbb{R}^{d_1}$ and $Q \subset \mathbb{R}^{d_2}$, each containing the origin in its interior, we define the direct sum $P \circ Q := \operatorname{conv}(P \times \mathbf{0}_{d_2}, \mathbf{0}_{d_1} \times Q)$. For a prime p, we define the cyclotomic polytope

$$\mathcal{C}_{p^{lpha}} = \underbrace{\mathcal{C}_p \circ \mathcal{C}_p \circ \cdots \circ \mathcal{C}_p}_{p^{lpha-1} ext{ times}}$$
 .

For two polytopes $P \subset \mathbb{R}^{d_1}$ and $Q \subset \mathbb{R}^{d_2}$, each containing the origin in its interior, we define the direct sum $P \circ Q := \operatorname{conv}(P \times \mathbf{0}_{d_2}, \mathbf{0}_{d_1} \times Q)$. For a prime p, we define the cyclotomic polytope

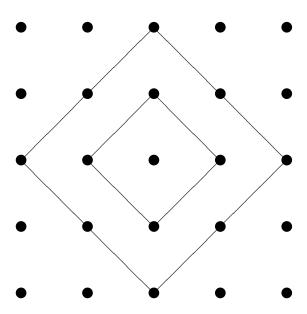
$$\mathcal{C}_{p^{lpha}} = \underbrace{\mathcal{C}_p \circ \mathcal{C}_p \circ \cdots \circ \mathcal{C}_p}_{p^{lpha-1} ext{ times}}$$
 .



For two polytopes $P \subset \mathbb{R}^{d_1}$ and $Q \subset \mathbb{R}^{d_2}$, each containing the origin in its interior, we define the direct sum $P \circ Q := \operatorname{conv}(P \times \mathbf{0}_{d_2}, \mathbf{0}_{d_1} \times Q)$. For a prime p, we define the cyclotomic polytope

$$\mathcal{C}_{p^{lpha}} = \underbrace{\mathcal{C}_p \circ \mathcal{C}_p \circ \cdots \circ \mathcal{C}_p}_{p^{lpha-1} ext{ times}}$$
 .

 \mathcal{C}_4



For two polytopes $P \subset \mathbb{R}^{d_1}$ and $Q \subset \mathbb{R}^{d_2}$, each containing the origin in its interior, we define the direct sum $P \circ Q := \operatorname{conv}(P \times \mathbf{0}_{d_2}, \mathbf{0}_{d_1} \times Q)$. For a prime p, we define the cyclotomic polytope

$$\mathcal{C}_{p^{lpha}} = \underbrace{\mathcal{C}_p \circ \mathcal{C}_p \circ \cdots \circ \mathcal{C}_p}_{p^{lpha-1} ext{ times}}$$
 .

For two polytopes $P = \operatorname{conv}(v_1, v_2, \dots, v_s)$ and $Q = \operatorname{conv}(w_1, w_2, \dots, w_t)$ we define their tensor product

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

For two polytopes $P \subset \mathbb{R}^{d_1}$ and $Q \subset \mathbb{R}^{d_2}$, each containing the origin in its interior, we define the direct sum $P \circ Q := \operatorname{conv}(P \times \mathbf{0}_{d_2}, \mathbf{0}_{d_1} \times Q)$. For a prime p, we define the cyclotomic polytope

$$\mathcal{C}_{p^{lpha}} = \underbrace{\mathcal{C}_p \circ \mathcal{C}_p \circ \cdots \circ \mathcal{C}_p}_{p^{lpha-1} ext{ times}}.$$

For two polytopes $P = \operatorname{conv}(v_1, v_2, \dots, v_s)$ and $Q = \operatorname{conv}(w_1, w_2, \dots, w_t)$ we define their tensor product

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

Our construction implies for $m=m_1m_2$, where $m_1,m_2>1$ are relatively prime, that the cyclotomic polytope \mathcal{C}_m is equal to $\mathcal{C}_{m_1} \otimes \mathcal{C}_{m_2}$.

For two polytopes $P \subset \mathbb{R}^{d_1}$ and $Q \subset \mathbb{R}^{d_2}$, each containing the origin in its interior, we define the direct sum $P \circ Q := \operatorname{conv}(P \times \mathbf{0}_{d_2}, \mathbf{0}_{d_1} \times Q)$. For a prime p, we define the cyclotomic polytope

$$\mathcal{C}_{p^{lpha}} = \underbrace{\mathcal{C}_p \circ \mathcal{C}_p \circ \cdots \circ \mathcal{C}_p}_{p^{lpha-1} ext{ times}}$$
 .

For two polytopes $P = \text{conv}(v_1, v_2, \dots, v_s)$ and $Q = \text{conv}(w_1, w_2, \dots, w_t)$ we define their tensor product

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

Our construction implies for $m=m_1m_2$, where $m_1,m_2>1$ are relatively prime, that the cyclotomic polytope \mathcal{C}_m is equal to $\mathcal{C}_{m_1}\otimes\mathcal{C}_{m_2}$.

For general m,

$$\mathcal{C}_m = \underbrace{\mathcal{C}_{\sqrt{m}} \circ \mathcal{C}_{\sqrt{m}} \circ \cdots \circ \mathcal{C}_{\sqrt{m}}}_{\frac{m}{\sqrt{m}} \text{ times}},$$

a $0/\pm 1$ polytope with the origin as the sole interior lattice point.

 $\mathcal{L} \cong \mathbb{Z}^d$ a lattice, M a minimal set of monoid generators, K a field

The vectors in $M' = \{(u, 1) : u \in M \cup \{0\}\}$ encoded as monomials give rise to the monoid algebra K[M'], in which each monomial corresponds to (v,k) where $v=\sum_{u_i\in M\cup\{0\}}n_iu_i$ with nonnegative integer coefficients n_i such that $\sum n_i = k$.

 $\mathcal{L} \cong \mathbb{Z}^d$ a lattice, M a minimal set of monoid generators, K a field

The vectors in $M' = \{(u, 1) : u \in M \cup \{0\}\}$ encoded as monomials give rise to the monoid algebra K[M'], in which each monomial corresponds to (v,k) where $v=\sum_{u_i\in M\cup\{0\}}n_iu_i$ with nonnegative integer coefficients n_i such that $\sum n_i = k$. This grading gives rise to the Hilbert series

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

where $K[M']_k$ denotes the vector space of elements of degree k in this graded algebra.

 $\mathcal{L} \cong \mathbb{Z}^d$ a lattice, M a minimal set of monoid generators, K a field

The vectors in $M' = \{(u, 1) : u \in M \cup \{0\}\}$ encoded as monomials give rise to the monoid algebra K[M'], in which each monomial corresponds to (v,k) where $v=\sum_{u_i\in M\cup\{0\}}n_iu_i$ with nonnegative integer coefficients n_i such that $\sum n_i = k$. This grading gives rise to the Hilbert series

$$H(K[M'];x) := \sum_{k>0} \dim_K (K[M']_k) x^k = \frac{h(x)}{(1-x)^{d+1}},$$

where $K[M']_k$ denotes the vector space of elements of degree k in this graded algebra.

 $\mathcal{L} \cong \mathbb{Z}^d$ a lattice, M a minimal set of monoid generators, K a field

The vectors in $M' = \{(u,1) : u \in M \cup \{0\}\}$ encoded as monomials give rise to the monoid algebra K[M'], in which each monomial 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 $\sum n_i = k$. This grading gives rise to the Hilbert series

$$H(K[M'];x) := \sum_{k\geq 0} \dim_K (K[M']_k) x^k = \frac{h(x)}{(1-x)^{d+1}},$$

where $K[M']_k$ denotes the vector space of elements of degree k in this graded algebra. When $\mathcal{L} \cong \mathbb{Z}^d$, the number of elements in \mathcal{L} of length k (with respect to M) is equal to $\dim_K(K[M']_k) - \dim_K(K[M']_{k-1})$, and therefore the growth series of \mathcal{L} is

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

 $\mathcal{L} \cong \mathbb{Z}^d$ a lattice, M a minimal set of monoid generators, K a field

The vectors in $M' = \{(u,1) : u \in M \cup \{0\}\}$ encoded as monomials give rise to the monoid algebra K[M'], in which each monomial 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 $\sum n_i = k$. This grading gives rise to the Hilbert series

$$H(K[M'];x) := \sum_{k>0} \dim_K (K[M']_k) x^k = \frac{h(x)}{(1-x)^{d+1}},$$

where $K[M']_k$ denotes the vector space of elements of degree k in this graded algebra. When $\mathcal{L} \cong \mathbb{Z}^d$, the number of elements in \mathcal{L} of length k (with respect to M) is equal to $\dim_K(K[M']_k) - \dim_K(K[M']_{k-1})$, and therefore the growth series of \mathcal{L} is

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

In the conditions of our theorem, the Hilbert series of $C_m \circ C_m$ equals (1-x) times the square of the Hilbert series of C_m , whence $h_m(x) = h_{\sqrt{m}}(x)^{\frac{m}{\sqrt{m}}}$.

A polytope \mathcal{P} is totally unimodular if every submatrix of the matrix consisting of the vertices of \mathcal{P} has determinant $0, \pm 1$.

Theorem (MB-Hoşten) If m is divisible by at most two odd primes then the cyclotomic polytope \mathcal{C}_m is totally unimodular.

A polytope \mathcal{P} is totally unimodular if every submatrix of the matrix consisting of the vertices of \mathcal{P} has determinant $0, \pm 1$.

Theorem (MB-Hoşten) If m is divisible by at most two odd primes then the cyclotomic polytope \mathcal{C}_m is totally unimodular.

Corollary If m is divisible by at most two odd primes then the cyclotomic polytope \mathcal{C}_m is normal, i.e., the monoid generated by M' and the monoid of the lattice points in the cone generated by M' are equal.

A polytope \mathcal{P} is totally unimodular if every submatrix of the matrix consisting of the vertices of \mathcal{P} has determinant $0, \pm 1$.

Theorem (MB-Hoşten) If m is divisible by at most two odd primes then the cyclotomic polytope \mathcal{C}_m is totally unimodular.

Corollary If m is divisible by at most two odd primes then the cyclotomic polytope \mathcal{C}_m is normal, i.e., the monoid generated by M' and the monoid of the lattice points in the cone generated by M' are equal.

Remark Total unimodularity breaks down already for \mathcal{C}_{3pq} for distinct primes p,q>3. This is an indication that Parker's Conjecture (1) might not be true in general.

Theorem (MB-Hoșten) Suppose m is divisible by at most two odd primes. (2) $h_{\sqrt{m}}(x)$ is the h-polynomial of a simplicial polytope.

. . . follows now because $C_{\sqrt{m}}$ has a unimodular triangulation, which induces a unimodular triangulation of the boundary of $\mathcal{C}_{\sqrt{m}}$. This boundary equals the boundary of a simplicial polytope $\mathcal Q$ (Stanley), and $h_{\sqrt{m}}$ is the hpolynomial of Q (which is palindromic, unimodal, and nonnegative).

Theorem (MB-Hoșten) Suppose m is divisible by at most two odd primes. (2) $h_{\sqrt{m}}(x)$ is the h-polynomial of a simplicial polytope.

. . . follows now because $C_{\sqrt{m}}$ has a unimodular triangulation, which induces a unimodular triangulation of the boundary of $\mathcal{C}_{\sqrt{m}}$. This boundary equals the boundary of a simplicial polytope Q (Stanley), and $h_{\sqrt{m}}$ is the hpolynomial of Q (which is palindromic, unimodal, and nonnegative).

Remark If \mathcal{C}_m is a simplicial polytope then the coordinator polynomial h_m equals the h-polynomial of \mathcal{C}_m . The polytope \mathcal{C}_m is simplicial, e.g., for m a prime power or the product of two primes (the latter was proved by R. Chapman and follows from the fact that \mathcal{C}_{pq} is dual to a transportation polytope with margins p and q).

Open Problems

Describe the face structure of C_m , e.g., in the case m=pq.

Open Problems

- Describe the face structure of C_m , e.g., in the case m=pq.
- ▶ Is \mathcal{C}_m normal for all m?

Open Problems

- Describe the face structure of \mathcal{C}_m , e.g., in the case m=pq.
- Is \mathcal{C}_m normal for all m?
- S. Sullivant computed that the dual of \mathcal{C}_{105} is not a lattice polytope, i.e., \mathcal{C}_{105} is not reflexive. If we knew that \mathcal{C}_{105} is normal, a theorem of Hibi would imply that the coordinator polynomial h_{105} is not palindromic, and hence that Parker's Conjecture (1) is not true in general.