Proof of a conjecture by Đoković on the Poincaré series of the invariants of a binary form

A. Blokhuis*, A. E. Brouwer, T. Szőnyi†

Abstract

Đoković [3] gave an algorithm for the computation of the Poincaré series of the algebra of invariants of a binary form, where the correctness proof for the algorithm depended on an unproven conjecture. Here we prove this conjecture.

1 Introduction

In [3] Đoković gave an algorithm for the computation of the Poincaré series of the algebra of invariants of a binary form, depending on the following conjecture.

Let $n \geq 3$ be an integer. If n is odd, define integers s and m and polynomials $p_n(z,t)$ and $q_n(z,t)$ and $r_n(t)$ by $n = 2s-1$ and $m = s^2$ and

$$p_n(z,t) = \prod_{i=1}^{s}(1 - tz^{2i-1}), \quad q_n(z,t) = \prod_{i=1}^{s}(z^{2i-1} - t), \quad r_n(t) = \prod_{i=2}^{n-1}(1 - t^{2i}).$$

If n is even, let $n = 2s$ and $m = s(s+1)$ and

$$p_n(z,t) = \prod_{i=1}^{s}(1 - tz^{2i}), \quad q_n(z,t) = \prod_{i=1}^{s}(z^{2i} - t), \quad r_n(t) = (1+t)\prod_{i=2}^{n-1}(1 - t^{i}).$$

Let $\phi_n(z,t) = z^{m-2}(z^2-1)r_n(t)$.

*The first author was partly supported by the ERC project No. 227701 DISCRETECONT.

†The third author gratefully acknowledges the financial support of NWO, including the support of the DIAMANT and Spinoza projects. He was partly supported by OTKA Grant NK 105645.

Conjecture 1.1 ([3], Conjecture 3.1) *There exist polynomials $a_n, b_n \in \mathbb{Z}[z,t]$ of z-degree $m-2$ such that $\phi_n = a_n q_n + b_n p_n$.*

Here we prove a slightly stronger and more precise result. Keep the above definition of $r_n(t)$ for odd n and for $n = 2$ (that is, $r_2(t) = 1+t$), but define for even $n \geq 4$:

$$r_n(t) = (1+t)^2 \prod_{i=3}^{n-1}(1-t^i) \quad \text{or} \quad r_n(t) = (1+t)^2 \prod_{i=3}^{n-1}(1-t^i) \,/\, (1+t^{\frac{1}{2}n-1})$$

when $n \equiv 2 \pmod 4$ or $n \equiv 0 \pmod 4$, respectively. Again put $\phi_n(z,t) = z^{m-2}(z^2-1)r_n(t)$. Then

Proposition 1.2 *There exist polynomials $a_n, b_n \in \mathbb{Z}[z,t]$ of z-degree $m-2$ such that $\phi_n = a_n q_n + b_n p_n$. Conversely, if $\psi_n = a_n q_n + b_n p_n$, where $a_n, b_n \in \mathbb{Z}[z,t]$ and $\psi_n = z^{m-2}(z^2-1)h(t)$ for some $h \in \mathbb{Z}[t]$, then $r_n | h$.*

Unrelated to the computation of Poincaré series was a further conjecture:

Conjecture 1.3 ([3], Conjecture 3.2) *Let $I_n = \langle p_n, q_n \rangle$ be the ideal of $\mathbb{Z}[z,t]$ generated by p_n and q_n. Then $I_n \cap \mathbb{Z}[t]$ is the principal ideal of $\mathbb{Z}[t]$ generated by the polynomial*

$$(1-t^2)\prod_{i=1}^{n-1}(1-t^{2i}), \quad (1+t)\prod_{i=1}^{n-1}(1-t^i), \quad \prod_{i=1}^{n-1}(1-t^i),$$

according as to whether n is odd, congruent to 2 modulo 4, or divisible by 4.

This is true when n is odd, or $n \equiv 2 \pmod 4$, or $n = 4$, but false when $4|n$, $n > 4$. Here we prove

Proposition 1.4 *Let $I_n = \langle p_n, q_n \rangle$ be the ideal of $\mathbb{Z}[z,t]$ generated by p_n and q_n. Then $I_n \cap \mathbb{Z}[t]$ is the principal ideal of $\mathbb{Z}[t]$ generated by the polynomial*

$$(1-t^2)\prod_{i=1}^{n-1}(1-t^{2i}), \quad (1+t)\prod_{i=1}^{n-1}(1-t^i), \quad (1+t)\prod_{i=1}^{n-1}(1-t^i)/(1+t^{\frac{1}{2}n-1}),$$

according as to whether n is odd, congruent to 2 modulo 4, or divisible by 4.

The generator here is $(1-t^2)^2 r_n(t)$ when n is odd, $(1-t)r_n(t)$ when $n=2$, and $(1-t)^2 r_n(t)$ for even $n > 2$.

2 Relation with the denominator of the Poincaré function

Consider the Poincaré series $P(t) = \sum_k d_k t^k$ of the (graded) ring of invariants of a binary form of degree n, where $d_k = \dim I_k$ is the vector space dimension of the degree k part. Then $P(t)$ is a rational function given by the integral

$$P(t) = \frac{1}{2\pi i}\int_{|z|=1} f_n(z,t)\frac{dz}{z}$$

where

$$f_n(z,t) = \frac{1-z^{-2}}{\prod_{k=0}^{n}(1-tz^{n-2k})}.$$

If n is odd, then the denominator of $f_n(z,t)$ is $z^{-m}p_nq_n$. If n is even, it is $(1-t)z^{-m}p_nq_n$. Let $I_n = \langle p_n, q_n\rangle$ be the ideal of $\mathbb{Z}[z,t]$ generated by p_n and q_n. Let $g(t) \in \mathbb{Z}[t]$ be such that $\psi(z,t) := z^{m-2}(z^2-1)g(t) \in I_n$. Then $\psi = a_nq_n + b_np_n$ for certain $a_n, b_n \in \mathbb{Z}[z,t]$, where b_n has z-degree at most $m-1$, so that (omitting subscripts) $\frac{\psi}{pq} = \frac{a}{p} + \frac{b}{q}$. If n is odd, then

$$g(t)P(t) = \frac{1}{2\pi i}\int_{|z|=1}\left(\frac{a_n(z,t)}{p_n(z,t)} + \frac{b_n(z,t)}{q_n(z,t)}\right)\frac{dz}{z}.$$

Take $|t| < 1$. The contribution of the second term vanishes, since all poles are inside the unit circle, and the residue at ∞ is 0. The first term has all poles outside the unit circle, and contributes its residue at 0, which is $a_n(0,t)$. We find $P(t) = a_n(0,t)/g(t)$, so that $g(t)$ is a denominator of $P(t)$. Similarly, if n is even, $(1-t)g(t)$ is a denominator of $P(t)$.

Conjecturally (Dixmier's Conjecture 1 in [2]), the denominator of lowest degree of $P(t)$ is $r_n(t)$ when n is odd, and $(1-t)r_n(t)$ when n is even, and Dixmier proved that this is a denominator. The above discussion reproves his result (but does not prove his conjecture) since we may take $g(t) = r_n(t)$ by Proposition 1.2. A related result was proved in Derksen [1].

3 Proof — Preliminaries

The proofs of Propositions 1.2 and 1.4 are given simultaneously. The two main parts say that (i) certain specified functions are in the ideal I_n, and (ii) all elements of I_n have certain properties. Proposition 1.2 makes an additional claim about degrees. Let us settle that first, and make some other useful observations.

We drop the index n. Note that each of p, q, ϕ has z-degree m, and that $q(z,t) = z^m p(z^{-1},t)$ and $p(z,t) = z^m q(z^{-1},t)$ and $\phi(z,t) = -z^{2m-2}\phi(z^{-1},t)$.

Degrees. Assume that $\phi = aq + bp$ for certain polynomials $a = a(z,t)$ and $b = b(z,t)$. Since q has z-degree m, we may assume that b has z-degree at most $m-1$, and then also a has. The equalities just observed yield

$$(z^{m-2}a(z^{-1},t) + b(z,t))\, p(z,t) + (z^{m-2}b(z^{-1},t) + a(z,t))\, q(z,t) = 0.$$

Since p and q have no common factor, $z^{m-1}a(z^{-1},t) + zb(z,t) = Aq(z,t)$ and $z^{m-1}b(z^{-1},t) + za(z,t) = -Ap(z,t)$ for some A. Now $Az^m q(z^{-1},t) = z^{m-1}b(z^{-1},t) + za(z,t) = -Ap(z,t) = -Az^m q(z^{-1},t)$, and we must have $A = 0$. It follows that a and b are polynomials of z-degree at most $m-2$. That the degrees cannot be smaller follows by comparing both sides of $\phi = aq + bp$ upon substitution of $t = 0$.

Polynomials. Let $I = \langle p, q\rangle$ be the ideal of $\mathbb{Z}[z,t]$ generated by p and q. Since $z \,|\, (p-1)$, it follows that if $zf \in I$, then also $f \in I$. In particular, if $\phi = aq + bp$ where a, b are rational functions with no poles other than $z = 0$, so that $z^e\phi \in I$ for some $e \geq 0$, then also $\phi \in I$.

The case $n = 2$. If $n = 2$, then $s = 1$, $m = 2$ and $p = 1 - tz^2$, $q = z^2 - t$, and $r = 1 + t$. Proposition 1.2 claims $(z^2-1)(1+t) \in I$, which holds since $(z^2-1)(1+t) = q - p$. And that if $(z^2-1)h(t) \in I$ for some $h \in \mathbb{Z}[t]$, then $h(-1) = 0$. But $p(z,-1) = q(z,-1) = 1 + z^2$, so $(z^2-1)h(-1)$ has a factor $z^2 + 1$, and hence $h(-1) = 0$. Proposition 1.4 claims that $I \cap \mathbb{Z}[t] = (1 - t^2)$, and that is clear.

4 Proof — Existence

Next we show the existence of a, b in the various cases. Below, n is fixed and no longer written as index to $p = p_n$ and $q = q_n$, so that we can use indices to p and q with a different meaning. Now $p = p(z,t) = \prod_{i=0}^{s-1}(1 - tz^{n-2i})$ and $q = q(z,t) = \prod_{i=0}^{s-1}(z^{n-2i} - t)$, where $n = 2s-1$ or $n = 2s$.

Let $\psi \in \mathbb{Z}[z,t]$ be given. (It will be the function claimed to be in I in Proposition 1.2 or 1.4.) In order to show $\psi = aq + bp$ for some $a, b \in \mathbb{Z}[z,t]$, we rewrite this equation as

$$\frac{\psi}{pq} = \frac{a}{p} + \frac{b}{q}$$

and split this into partial fractions.

For some rational functions $a_h(z), b_h(z)$ and $c(z,t)$, where $c(z,t)$ is a polynomial in t, we have

$$\frac{\psi}{pq} = \sum_{h=0}^{s-1} \frac{a_h}{1 - tz^{n-2h}} + \sum_{h=0}^{s-1} \frac{b_h}{z^{n-2h} - t} + c$$

The a_h, b_h follow by multiplying by $1 - tz^{n-2h}$ resp. $z^{n-2h} - t$ and substituting $t = z^{2h-n}$ resp. $t = z^{n-2h}$. Thus,

$$a_h = \left.\frac{\psi}{p_h q}\right|_{t=z^{2h-n}} \quad \text{and} \quad b_h = \left.\frac{\psi}{p q_h}\right|_{t=z^{n-2h}},$$

where $p_h = p/(1 - tz^{n-2h})$ and $q_h = q/(z^{n-2h} - t)$.

If we expand b_h as a formal power series in z, we only get integer coefficients, since all factors in the denominator (other than powers of z) are $\pm(1 - z^k)$ for some k. So if we show that fb_h is a polynomial, for some $f \in \mathbb{Z}[z]$, then in fact it is in $\mathbb{Z}[z]$.

We show that a_h and b_h have no other poles than 0 and ± 1, and that a and b can be taken to be polynomials. There are 6 cases: n odd, $n \equiv 2 \pmod 4$, $n \equiv 0 \pmod 4$ in Proposition 1.2, where $\psi(z,t) = z^{m-2}(z^2 - 1)r(t)$, and in Proposition 1.4, where $\psi(z,t)$ is the polynomial claimed to generate the ideal I. In all cases $\psi(z,t)$ is divisible by $r(t)$. We assume $n \geq 3$.

Poles of b_h

The denominator $p(z, z^{n-2h})q_h(z, z^{n-2h})$ of b_h has zeros that are roots of unity or 0. Let ω be a primitive d-th root of unity, $d > 2$. We show that ω is not a pole of b_h. The multiplicity of ω as a root of the denominator is the number of elements of the sequence $-2h, -2h+2, \ldots, -2, 2, \ldots, 2n-2h$ other than $n-2h$ that is divisible by d, at most $\lfloor (n-h)/e \rfloor + \lfloor h/e \rfloor \leq \lfloor n/e \rfloor$, where $e = d$ when d is odd, and $e = d/2$ when d is even. The multiplicity of ω as a root of the numerator is at least its multiplicity as root of $r(t)$. If n is odd, this latter multiplicity is at least $\lfloor (n-1)/e \rfloor$, and hence is greater, unless perhaps e divides both h and $n-h$, so that d divides $2n - 4h$, and ω is root of each of the $n-2$ factors of $r(z^{n-2h})$. Since $n - 2 \geq \lfloor n/e \rfloor$ this settles the claim in case n is odd.

Now suppose $n \equiv 2 \pmod 4$. In the numerator we have a factor $r(z^{n-2h})$ which has a factor $\prod_{i=3}^{n-1}(1 - z^{2i})$, which has ω as a root of multiplicity $\lfloor (n-1)/e \rfloor$ if $e \geq 3$. Again we conclude that ω can be a pole of b_h only when e divides h and $n-h$ and d does not divide the omitted number $n-2h$. Now ω is a root of $(z^{2(n-2h)} - 1)/(z^{n-2h} - 1) = z^{n-2h} + 1$, and we are saved by the additional factor $t + 1$ in $r(t)$. The same holds for $d = 4$, $e = 2$ since the other additional factor $t + 1$ in $r(t)$ helps for odd h.

If $n \equiv 0 \pmod 4$, $n > 4$, then the same holds, except that in $r(t)$ a factor $1 - t^{2s-2}$ was replaced by $1 - t^{s-1}$, so that the numerator of b_h lost a factor $(1-z^{2(s-1)(n-2h)})/(1-z^{(s-1)(n-2h)})$. So we may suppose that $d \,|\, 2(s-1)(n-2h)$ and $d \nmid (s-1)(n-2h)$, so that d is even and $d \nmid n - 2h$. Now ω is a root of $z^{n-2h} + 1$ if and only if it is a root of $z^{2(n-2h)} - 1$. The multiplicity of ω as a root of the numerator is at least the number of integers $i(n-2h)$ divisible by d, where $i \in \{1, 2, \ldots, n-3, n-1\}$, that is the number of such $i(s-h)$ divisible by e. If $g = \gcd(e, s-h) > 1$, this number is at least $\lfloor g(n-1)/e \rfloor - 1$, which is not smaller than $\lfloor n/e \rfloor$, as desired. So, we may assume $\gcd(e, s-h) = 1$, so that $e \,|\, 2(s-1)$, $e \nmid (s-1)(s-h)$ and e is even, h is odd. Now $e \nmid h$ and $e \nmid n-h$ and the multiplicity of ω as root of the denominator equals $\lfloor (h-1)/e \rfloor + \lfloor (n-h-1)/e \rfloor$. Its multiplicity as root of the numerator is at least $\lfloor (n-3)/e \rfloor$, so if ω is a pole, then $e|(h-1)$ and $e|(n-h-1)$, so $e|n-2h$, so $e = 2$ and we are saved by the additional factor $1 + z^{n-2h}$ in the numerator.

The case $n = 4$ follows by a simple direct check.

This shows that b_h has no other poles than perhaps 0 and ± 1. The multiplicity of ± 1 as a root of the denominator is $n-1$, and as a root of the numerator $n-2$ in the case of Proposition 1.2 and at least $n-1$ in the case of Proposition 1.4. Define $b(z,t) = \sum_h b_h(z) q_h(z,t)$. We show that $b(z,t)$ has no poles other than perhaps $z = 0$. The only other possible poles are simple ones at $z = \pm 1$ in the case of Proposition 1.2. If $n \equiv 2 \pmod 4$, the residue of $b_h q_h$ at $z = 1$ is

$$R_h = (-1)^h 2^{2-n} (n-2h)^{n-2} (1-t)^{s-1} \frac{(n-1)!}{h!(n-h)!} = C \cdot (-1)^h (n-2h)^{n-2} \binom{n}{h},$$

where C is independent of h. These residues add up to zero. Indeed

$$\sum_{h=0}^{s-1} R_h = \frac{1}{2} C \cdot \sum_{h=0}^{n} (-1)^h \binom{n}{h} (n-2h)^{n-2}.$$

This sum equals the $(n-2)$-nd derivative of $(e^z - e^{-z})^n$ evaluated at $z = 0$. But since $n - 2 < n$ this derivative is still divisible by $e^z - e^{-z}$ and hence the sum is zero. If $n \equiv 0 \pmod 4$ or n is odd, the residues differ from the above by a factor 2^{-1} or 2^{n-3}, respectively, and again sum to zero. The residues at $z = -1$ are the same, up to a sign independent from h, and also sum to zero. So, indeed, $b(z,t)$ has no other poles than possibly at $z = 0$.

For $a = \sum a_h p_h$ the computation is the same since a_h and b_h, and also p_h and q_h, have the same residue at $z = \pm 1$ (up to a sign independent of h).

It follows that for sufficiently large N we may write $z^N\psi = aq + bp + cpq$ where a, b, c are polynomials. We can replace a by $a+cp$ to get $z^N\psi = aq+bp$. It follows that $\psi \in I$. □

5 Proof of Proposition 1.4 — Part 2

Next, we show that no lower degree polynomials are in $I \cap \mathbb{Z}[t]$.

Lemma 5.1 *Let $f(x) \in \mathbb{R}[x]$ be such that $f(x) = u$ for a positive and $f(x) = v$ for b negative x. Then f is constant or has degree at least $a + b - 1$.*

Proof: $f'(x)$ has (at least) $a - 1$ positive and $b - 1$ negative zeros. □

The next lemma describes a way to get lower bounds for the degree of nonzero elements in $I \cap \mathbb{Z}[t]$.

Lemma 5.2 *Let z_0, t_0 be complex numbers such that $p(z_0, t_0) = q(z_0, t_0) = 0$. Let $0 \neq h \in I \cap \mathbb{Z}[t]$. Then the multiplicity e of t_0 as zero of h is at least the number of factors of pq of which (z_0, t_0) is a zero, minus one.*

Proof: Let $0 \neq h(t) = a(z, t)q(z, t) + b(z, t)p(z, t)$. Apply the linear transformation $z = z_0(1 + \bar{z})$ and $t = t_0(1 + \bar{t})$ to the polynomials involved, and define $\bar{f} \in \mathbb{C}[\bar{z}, \bar{t}]$ by $\bar{f}(\bar{z}, \bar{t}) = f(z, t)$ for $f \in \mathbb{Z}[z, t]$. Since $p(0, t) = p(z, 0) = 1$, the numbers z_0, t_0 are nonzero, and this linear transformation preserves degrees. We find $\bar{h}(\bar{t}) = \bar{a}(\bar{z}, \bar{t})\bar{q}(\bar{z}, \bar{t}) + \bar{b}(\bar{z}, \bar{t})\bar{p}(\bar{z}, \bar{t})$.

For any (nonzero) polynomial f, let f_0 be the term of f having lowest total degree. If $f = gh$ then $f_0 = g_0h_0$, and if $f + g + h = 0$, then either $f_0 + g_0 + h_0 = 0$ or two of f_0, g_0, h_0 sum to zero while the third has higher degree.

Apply this to the equality $\bar{h} = \bar{a}\bar{q} + \bar{b}\bar{p}$. Let $q = \prod_{i \in K}(z^i - t)$ and $p = \prod_{j \in L}(1 - tz^j)$. Let $K_0 = \{i \in K \mid z_0^i = t_0\}$ and $L_0 = \{j \in L \mid t_0 z_0^j = 1\}$. A factor $z^i - t$ of q transforms to $z_0^i(1+\bar{z})^i - t_0(1+\bar{t})$. If $z_0^i \neq t_0$ then this has a nonzero constant term, but if $z_0^i = t_0$ its lowest degree term is $t_0(i\bar{z} - \bar{t})$. So we find that $\bar{q}_0$ (and hence $(\bar{a}\bar{q})_0$) is divisible by $\prod_{i \in K_0}(i\bar{z} - \bar{t})$. Similarly, the lowest degree part of $\bar{b}\bar{p}_0$ is divisible by $\prod_{j \in L_0}(\bar{t} + j\bar{z})$. The lowest degree part of $\bar{h}$ is $\bar{t}^e$ for some exponent e which is the multiplicity of t_0 as zero of h, and we conclude that $c\bar{t}^e = \bar{a}_0\bar{q}_0 + \bar{b}_0\bar{p}_0$, where $c = 0$ when e is larger than the degree of $\bar{a}_0\bar{q}_0$. (Note that $\bar{h}$ is a function of $\bar{t}$ only, while $\bar{q}_0$ and $\bar{p}_0$ depend on $\bar{z}$, so $\bar{a}_0\bar{q}_0$ and $\bar{b}_0\bar{p}_0$ have the same degree.)

Put $\bar{t} = 1$ to dehomogenize the system and look at the polynomial $\bar{a}_0(\bar{z}, 1)\bar{q}_0(\bar{z}, 1)$. It has zeros at $\bar{z} = 1/i$ for $i \in K_0$, and equals c for

$\bar{z} = -1/j$ where $j \in L_0$. Now apply the previous lemma to the real part of $s\bar{a}_0(\bar{z},1)\bar{q}_0(\bar{z},1)$, where $s \in \mathbb{C}$ is chosen such that this real part is not identically zero, to find a lower bound for e. □

Let $g(t)$ be the polynomial claimed to generate $I \cap \mathbb{Z}[t]$. Below we shall find for each zero t_0 of $g(t)$ a z_0 such that this lower bound for the multiplicity e of t_0 as zero of h equals the multiplicity of t_0 as zero for g. It will follow that h is a multiple of g.

Even n

Let $n = 2s$. Recall that $g(t) = (1+t)\prod_{i=1}^{n-1}(1-t^i)$ for odd s, while $g(t) = (1+t)\prod_{i=1}^{n-1}(1-t^i)/(1+t^{\frac{1}{2}n-1})$ for even s. Renormalize, replacing z^2 by z, so that $p = p_n(z,t) = \prod_{i=1}^{s}(1-tz^i)$ and $q = q_n(z,t) = \prod_{i=1}^{s}(z^i - t)$. Let $g(t_0) = 0$, where t_0 is a primitive d-th root of unity. Given t_0, we find z_0 such that the lower bound given by the above lemma for the multiplicity e of t_0 as zero of h equals the multiplicity of t_0 as zero of g. Suitable pairs (z_0, t_0) must satisfy $z_0^i = t_0$ for some $1 \le i \le s$ and $z_0^j t_0 = 1$ for some $1 \le j \le s$.

For $t_0 = 1$ take $z_0 = 1$, then both $z_0^i = t_0$ and $z_0^j t_0 = 1$ have s solutions, and we find $e \ge 2s-1 = n-1$. For $t_0 = -1$ take $z_0 = -1$, then both $z_0^i = t_0$ and $z_0^i t_0 = 1$ are true for all odd i, $\lfloor (s+1)/2 \rfloor$ values, and we find $e \ge s$ if s is odd and $e \ge s-1$ if s is even, as desired.

For $t_0^d = 1$, $d > 2$, we take $z_0 = t_0^a$ such that the equations $ai \equiv 1 \pmod{d}$ and $aj \equiv -1 \pmod{d}$ in total have as many solutions with $1 \le i \le s$ and $1 \le j \le s$ as possible. If the solutions for i are $i_0, i_0+d, \ldots$, then for j we get $d - i_0, 2d - i_0, \ldots$. Let $s = md + r$ with $0 \le r < d$ and first try $i_0 = 1$. If $r = 0$ we find m i's, m j's, and $e \ge 2m-1$. If $r > 0$ we find $m+1$ i's and at least m j's, so $e \ge 2m$. We can get the inequality $e \ge 2m+1$ if i_0 can be chosen in such a way that there are $m+1$ i's and $m+1$ j's, that is, if i_0 can be chosen with $d - r \le i_0 \le r$, and coprime to d. This requires $r > \frac{1}{2}d$, and then for odd d the choice $i_0 = \frac{1}{2}(d+1)$ works. If $4|d$, then the choice $i_0 = \frac{1}{2}d+1$ works. If $d \equiv 2 \pmod{4}$, then the choice $i_0 = \frac{1}{2}d+2$ works, unless $r = \frac{1}{2}d+1$, that is, unless $d|n-2$, $d \nmid s-1$. Since this corresponds precisely to the additional factor in the denominator of $g(t)$ when $4|n$, we showed in all cases that e is at least the multiplicity of the root t_0 of $g(t)$.

Odd n

Now let $n = 2s-1$, and $g(t) = (1-t^2)\prod_{i=1}^{n-1}(1-t^{2i})$. Put $p = p_n(z,t) = \prod_{i=1}^{s}(1-tz^{2i-1})$, $q = q_n(z,t) = \prod_{i=1}^{s}(z^{2i-1}-t)$.

Let t_0 be a primitive d-th root of unity. Put $\delta = d$ if d is odd, and $\delta = d/2$ if d is even. The multiplicity of t_0 as a root of g is n for $t_0 = \pm 1$,

and $\lfloor (n-1)/\delta \rfloor$ for $d > 2$. Suitable pairs (z_0, t_0) must satisfy $z_0^{2i-1} = t_0$ for some $1 \le i \le s$ and $z_0^{2j-1} t_0 = 1$ for some $1 \le j \le s$. For $t_0 = \pm 1$ take $z_0 = t_0$, then both $z_0^{2i-1} = t_0$ and $z_0^{2j-1} t_0 = 1$ have s solutions, and we find $e \ge 2s - 1 = n$. For $d > 2$ take $z_0 = t_0^a$ for suitable a. Then we want i, j such that $a(2i-1) \equiv 1 \pmod{d}$ and $a(2j-1) \equiv -1 \pmod{d}$. We find solutions $i_0, i_0 + \delta, i_0 + 2\delta, \ldots$ and $j_0, j_0 + \delta, j_0 + 2\delta, \ldots$ where $j_0 = \delta + 1 - i_0$. Let $s = m\delta + r$ with $0 \le r < \delta$. In every interval of length δ we find an i and a j. If $r = 0$ we get $e \ge 2m - 1$. If $r \ge 1$ we get $e \ge 2m$. If $(\delta+1)/2 < r < \delta$ we may take $i_0 = \delta/2$ if δ is even and $(\delta-1)/2$ if δ is odd, and find $e \ge 2m + 1$.
$\square$

6 Proof of Proposition 1.2 — Part 2

The last thing to be proved is the 'Conversely' part of Proposition 1.2. We already saw that $zf \in I$ if and only if $f \in I$, so the hypothesis here is that $(z^2 - 1)h(t) \in I$, and we hope to conclude that $r_n | h$.

The proof is very similar to the second half of the proof of Proposition 1.4. Again we apply the same linear transformation and take terms of lowest total degree.

If $n = 2s$ is even, rescale first, replacing z^2 by z. Then transform and take terms of lowest degree. The factor $(z-1)$ transforms to $z_0(1 + \bar{z}) - 1$ which has constant term of lowest degree, unless $z_0 = 1$, in which case the term of lowest degree is $\bar{z}$. Earlier we took for each t_0 that is a primitive d-th root of unity a z_0 that also is a primitive d-th root of unity. That is, for $t_0 \ne 1$ we have $z_0 \ne 1$ and the lower bound on the multiplicity of the root t_0 of $h(t)$ is the same as before.

It remains to estimate the multiplicity of 1 as a root of $h(t)$. From $c\bar{z}\bar{t}^e = \bar{a}_0\bar{q}_0 + \bar{b}_0\bar{p}_0$ we see that $\bar{a}_0(\bar{z}, 1)\bar{q}_0(\bar{z}, 1)$ has the property that for the s values $\bar{z} = 1/i$ with $1 \le i \le s$ it vanishes, while for the s values $\bar{z} = -1/j$ with $1 \le j \le s$ its values lie on the line $c\bar{z}$. For its derivative that means that there are $s - 1$ positive values where it vanishes and $s - 1$ negative values where it equals c, so that the derivative has degree at least $2s - 3 = n - 3$, and hence $\bar{a}_0\bar{q}_0$ has degree at least $n - 2$, and $e \ge n - 3$. This bound is two less than before, but $g(t) = (t-1)^2 r_n(t)$ so this suffices.

Now let $n = 2s - 1$ be odd. The factor $(z^2 - 1)$ transforms to $z_0^2(1 + \bar{z})^2 - 1$, which has constant term of lowest degree, unless $z_0^2 = 1$, in which case the term of lowest degree is $2\bar{z}$. All is as before, and we find the same lower bound on the multiplicity of the root t_0 of $h(t)$ as before, unless $t_0^2 = 1$ and $z_0 = t_0$. As in the case n even, we find $e \ge 2s - 3$, that is, $e \ge n - 2$. This bound is two less than before, but $g(t) = (t^2 - 1)^2 r_n(t)$ so this suffices. We proved everything. $\square$

References

[1] Harm Derksen, *Universal denominators of Hilbert series*, J. Algebra **285** (2005) 586–607.

[2] J. Dixmier, *Quelques résultats et conjectures concernant les séries de Poincaré des invariants des formes binaires*, pp. 127–160 in: Séminaire d'algèbre Paul Dubreil et Marie-Paule Malliavin (1983-1984), Springer Lecture Notes in Math. **1146**, 1985.

[3] Dragomir Ž. Đoković, *A heuristic algorithm for computing the Poincaré series of the invariants of binary forms*, Int. J. Contemp. Math. Sci. **1** (2006) 557–568.