

Polynomials with Rational Roots that Differ by a Non-zero Constant

Philip Gibbs

The problem of finding two polynomials $P(x)$ and $Q(x)$ of a given degree n in a single variable x that have all rational roots and differ by a non-zero constant is investigated. It is shown that the problem reduces to considering only polynomials with integer roots. The cases $n < 4$ are solved generically. For $n = 4$ the case of polynomials whose roots come in pairs $(a, -a)$ is solved. For $n = 5$ an infinite number of inequivalent solutions are found with the ansatz $P(x) = -Q(-x)$. For $n = 6$ an infinite number of solutions are also found. Finally for $n = 8$ we find solitary examples. This also solves the problem of finding two polynomials of degree n that fully factorise into linear factors with integer coefficients such that the difference is one.

Generalities

Let $P(x)$ and $Q(x)$ be two polynomials of degree n such that all roots of $P(x)$ and $Q(x)$ are rational. For which degrees n can we find two such polynomials which differ only by a non-zero constant independent of x ?

Since all roots are rational we can factorise both polynomials

$$P(x) = a \prod_{i=1}^n (x - r_i)$$

$$Q(x) = b \prod_{i=1}^n (x - s_i)$$

Where r_i and s_i are the rational roots. For $n > 0$, if the difference $P(x) - Q(x) = c$ is a constant independent of x then we must have $a = b$ and without loss of generality we can assume $a = b = 1$.

Conditions on the roots

The condition for a solution can be written in terms of the roots

$$\sum_{i=1}^n r_i^k = \sum_{i=1}^n s_i^k, \text{ for } 1 \leq k < n$$

$$\prod_{i=1}^n r_i \neq \prod_{i=1}^n s_i$$

Equivalence to problems over integers

Take N to be the multiple of the denominators of all roots for both equations then

$$P'(x) = N^n P(x/N) = \prod_{i=1}^n (x - Nr_i)$$

So $P'(x)$ is a polynomial with integer roots. Similarly for $Q'(x) = N^n Q(x/N)$. But $P'(x) - Q'(x) = N^n c$ is constant. It follows that if we can find a solution with rational roots then we can also find one with

integer roots. The converse is trivial. Therefore we need only search for polynomials with integer roots r_i and s_i .

This problem is also equivalent to finding two polynomials of degree n that can be fully factorised into linear factors with integer coefficients and that differ by one. If we have two such polynomials then they have rational roots. Conversely, if we have two polynomials $P(x)$ and $Q(x)$ with integer roots that differ by a constant $P(x) - Q(x) = c$, then substitute $x' = x - s_1$ where s_1 is a root of $Q(x)$ so that $Q'(x') = Q(x' + s_1)$ has a factor of x' and therefore the product of the roots of $P'(x') = P(x' + s_1)$ is c . Now make a second substitution to define $P''(x'') = (1/c)P'(cx'')$ and $Q''(x'') = (1/c)Q'(cx'')$. It can be verified that $P''(x'')$ and $Q''(x'')$ factorise into linear factors with integer coefficients and that $P''(x'') - Q''(x'') = 1$

No coincident roots

If a root r of $P(x)$ were also a root of $Q(x)$ then $x-r$ would be a factor of $P(x)-Q(x)$ which could then not be constant. It follows that none of the roots of $P(x)$ can coincide with roots of $Q(x)$.

Transformations and dualities

Given one solution as roots r_i and s_i , another can be formed by translating using an integer constant translation $r'_i = r_i + t$, $s'_i = s_i + t$, or by multiplying by a constant $r'_i = k.r_i$, $s'_i = k.s_i$. Solutions which differ by combinations of such transformations will be regarded as equivalent. When a solution is equivalent to itself under a non-trivial transformation we call it self-dual. This can happen in essentially two ways;

- (1) $r_i = t - r_j$ and $s_i = t - s_j$
- (2) $r_i = t - s_j$

By using the transformations we can assume $t = 0$ in either case.

Self-dual type (1) can only arise for even n since otherwise it requires a zero root for both polynomials. It is then equivalent to $P(x) = P(-x)$ and $Q(x) = Q(-x)$

Self-dual type (2) can arise for odd or even n . We then get $P(x) = (-1)^n Q(-x)$

When we impose self-duality on the solutions we automatically fulfil about half of the required conditions on the roots. This can help us in the search at higher values of n .

n = 2

General case

The quadratic case is simple to solve. Using the transformations we can assume that the roots are

$(r, -r)$ and $(s, -s)$ from polynomials $P(x) = x^2 - r^2$ and $Q(x) = x^2 - s^2$. This provides solutions when $r^2 \neq s^2$. All other solutions are equivalent to one of these.

n = 3

Type (2) self-dual

The cubic case is more challenging, but it is not difficult to find some type (2) self-dual solutions with

$$r_1 = -s_1, \quad r_2 = -s_2, \quad r_3 = -s_3$$

This automatically gives us that

$$r_1^2 + r_2^2 + r_3^2 = s_1^2 + s_2^2 + s_3^2$$

The remaining requirement is that

$$r_1 + r_2 + r_3 = 0$$

with none of the roots equal to zero. This is easy to satisfy, i.e. take $r_1 = a-b$, $r_2 = b-c$, $r_3 = c-a$, where a , b and c are any distinct integers. This includes an infinite number of inequivalent solutions e.g. by fixing a and b , then varying c .

General case

For $n = 3$ it is also possible to construct a more complete solution. To see this first set

$$r_1 = -s_1$$

This can be done without loss of generality since any solution is equivalent to one with this condition. Then we require just,

$$r_2^2 + r_3^2 = s_2^2 + s_3^2$$

$$2s_1 = r_2 + r_3 - s_2 - s_3$$

The first equation is well known with general solution in four parameters a, b, c, d , based on complex number norms is given by

$$r_2 = ab + cd, \quad r_3 = ad - bc, \quad s_2 = ab - cd, \quad s_3 = ad + bc,$$

Then we can complete the solution by solving the second equation with

$$s_1 = cd - bc, \quad r_1 = bc - cd$$

To ensure that the difference in the polynomials is non-zero, we need

$$r_1 r_2 r_3 - s_1 s_2 s_3 = bcd(b-d)(a-c)(a+c) \neq 0$$

Although this solution is complete up to translations it does not reflect the permutation symmetries of the original problem. To find a more symmetric solution, first examine the matrix of differences

$$\delta_{ij} = r_i - s_j$$

Each of these components factorises as follows

$$\Delta = \begin{pmatrix} 2c(b-d) & b(c-a) & -d(c+a) \\ b(a+c) & 2cd & (a-c)(b-d) \\ d(a-c) & (a+c)(d-b) & -2bc \end{pmatrix}$$

Rename the factors as follows

$$p = -2c, \quad q = c - a, \quad t = c + a, \quad u = d - b, \quad v = b, \quad w = -d$$

Then the matrix takes a more symmetric form

$$\Delta = \begin{pmatrix} pu & qv & tw \\ tv & pw & qu \\ qw & tu & pv \end{pmatrix}$$

With the extra conditions

$$p + q + t = u + v + w = 0$$

A further observation is that a solution can also be derived from this matrix form by taking

$$r_i = \sum_j \delta_{ij}, \quad s_j = \sum_i \delta_{ij}$$

It can then be verified that the required equations for the roots are satisfied without the extra conditions. To ensure that the difference is non-zero we require

$$r_1 r_2 r_3 - s_1 s_2 s_3 = (p-q)(p-t)(q-t)(u-v)(v-w)(u-w) \neq 0$$

n = 4

Type (1) self-dual

For quartic polynomials it is possible to find type (1) self-dual solutions using

$$r_3 = -r_1, \quad r_4 = -r_2, \quad s_3 = -s_1, \quad s_4 = -s_2$$

The remaining equality we need to satisfy is

$$r_1^2 + r_2^2 = s_1^2 + s_2^2$$

Which is solved using

$$r_1 = ab + cd, \quad r_2 = ad - bc, \quad s_1 = ab - cd, \quad s_2 = ad + bc,$$

From this we can generate an infinite number of inequivalent solutions.

Type (2) self-dual

We can also look for type (2) self-dual solutions using

$$s_1 = -r_1, \quad s_2 = -r_2, \quad s_3 = -r_3, \quad s_4 = -r_4$$

This then requires

$$r_1 + r_2 + r_3 + r_4 = 0 \quad \text{and} \quad r_1^3 + r_2^3 + r_3^3 + r_4^3 = 0$$

the second equation gives

$$(r_1 + r_2)(r_1^2 - r_1 r_2 + r_2^2) + (r_3 + r_4)(r_3^2 - r_3 r_4 + r_4^2) = 0$$

Then using the second equation we get

$$r_1^2 - r_1 r_2 + r_2^2 = r_3^2 - r_3 r_4 + r_4^2$$

But we also have

$$(r_1 + r_2)^2 = (r_3 + r_4)^2$$

And combining the different quadratics we also get

$$(r_1 - r_2)^2 = (r_3 - r_4)^2$$

It quickly follows that the two polynomials must be equal, so no type (2) self-dual solutions are possible for $n = 4$.

n=5

Type (2) self-dual

In this case we set

$$r_1 = -s_1, \quad r_2 = -s_2, \quad r_3 = -s_3, \quad r_4 = -s_4, \quad r_5 = -s_5$$

Then the remaining equations to solve are

$$r_1 + r_2 + r_3 + r_4 + r_5 = 0 \quad \text{and} \quad r_1^3 + r_2^3 + r_3^3 + r_4^3 + r_5^3 = 0$$

This has an infinite number of inequivalent solutions e.g. from this sequence for z any positive integer.

$$r_1 = 1, \quad r_2 = 2z^2 + 3z, \quad r_3 = -(2z^2 + 4z + 1), \quad r_4 = -(2z^2 + 4z + 2), \quad r_5 = 2z^2 + 5z + 2$$

n=6

Type (1) self-dual

For degree six polynomials consider type (1) self-dual solutions using

$$r_4 = -r_1, \quad r_5 = -r_2, \quad r_6 = -r_3, \quad s_4 = -s_1, \quad s_5 = -s_2, \quad s_6 = -s_3$$

Then the remaining equations to solve are

$$r_1^2 + r_2^2 + r_3^2 = s_1^2 + s_2^2 + s_3^2 \quad \text{and} \quad r_1^4 + r_2^4 + r_3^4 = s_1^4 + s_2^4 + s_3^4$$

Again this has an infinite number of inequivalent solutions e.g. from this sequence.

$$r_1 = 0, \quad r_2 = r_3 = 3z^2 + 3z + 1, \quad s_1 = 2z + 1, \quad s_2 = 3z^2 + 2z, \quad s_3 = 3z^2 + 4z + 1$$

n=8

Type (1) self-dual

For n=8 a brute force numerical search has produced some example solutions the smallest of which is

$$\{ r_i \} = \{-24, -23, -14, -5, 5, 14, 23, 24\}$$

$$\{ s_i \} = \{-25, -21, -16, -2, 2, 16, 21, 25\}$$

Final Remarks

Solutions seem to be reasonably abundant up to degree 8 but there is no obvious pattern that allows us to find general solutions for arbitrarily high degree. As n increases the number of variables increases at twice the rate of the constraints, but the constraints are of increasingly high degree. It is therefore an interesting question as to whether solutions exist for all n .

Although this problem has been studied here for its own interest it may have applications to other problems where it is required to find systems of numbers with small differences that have many factors.