Polynomials and fields with large degree and small discriminant

(General survey with new material in cases where the Galois group is required to be the symmetric group S_n)

David P. Roberts
University of Minnesota, Morris

Background on discriminants. We will work with monic separable polynomials in $\mathbf{Z}[x]$,

$$\begin{aligned} f(x) &= x^n + a_1 x^{n-1} + \cdots + a_n \\ &= (x-\alpha_1)\cdots(x-\alpha_n). \end{aligned}$$

The associated absolute discriminant is the positive integer

$$D_f = \prod_{i<j} |\alpha_i - \alpha_j|^2.$$

If f is irreducible one has the field $F = \mathbf{Q}[x]/f(x)$ with discriminant D_F satisfying

$$D_F = D_f / C_f^2$$

with C_f a positive integer.

We will generally renormalize to *root discriminants*:

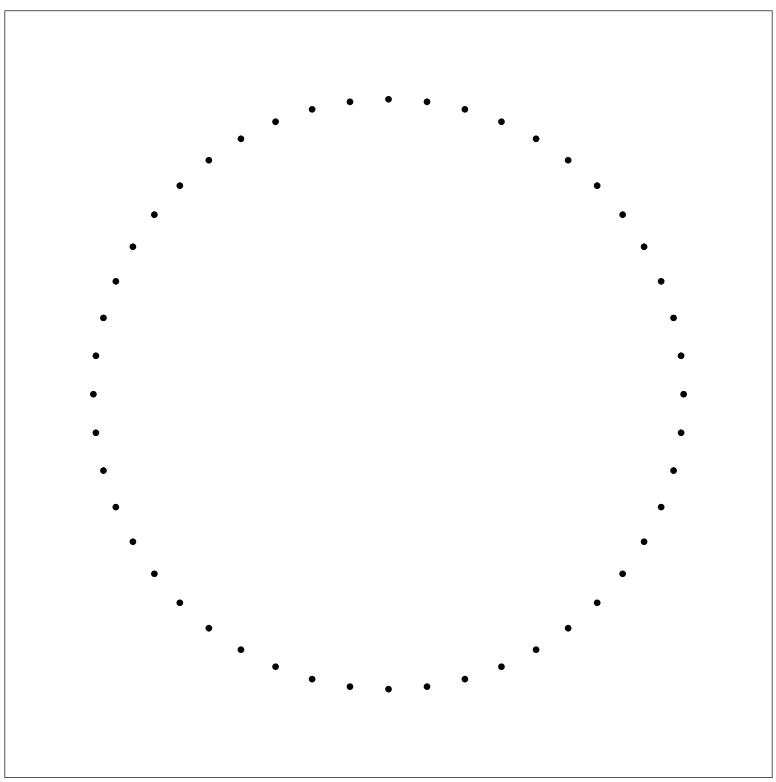
$$d_f = D_f^{1/n} \qquad d_F = D_F^{1/n}.$$

One advantage is that if L/F is unramified then $d_L = d_F$.

A non-standard renormalization: score. We define the *score* of a degree n polynomial with root discriminant d_f to be $s_f = d_f/n$. Similarly for a degree n field F, $s_F = d_F/n$. An advantage of score is the formula

$$s_{f(x^d)} = |f(0)|^{1/n - 1/dn} s_{f(x)}.$$

Example. The polynomial $x^n - 1$ has discriminant $D = n^n$, root discriminant $d = n$, and score $s = 1$. Root plot of $x^{48} - 1$:



Polynomial quantities. Let

- a_n be the minimal root discriminant of a degree n polynomial;

- b_n be the minimal root discriminant of an *irreducible* degree n polynomial;

- c_n be the minimal root discriminant of a *generic* degree n polynomial, meaning a polynomial with Galois group all of S_n.

Of course,

$$a_n \leq b_n \leq c_n.$$

Field quantities. Let

- d_n be the minimal root discriminant of a degree n field;

- e_n be the minimal root discriminant of a degree n field $F = \mathbf{Q}[x]/f(x)$ with f generic;

- f_n be the minimal root discriminant of the degree $n!$ splitting field $K_f \subset \mathbf{C}$ of a degree n generic polynomial f.

One has

$$a_n \;\le\; b_n \;\le\; c_n$$

$$d_n \;\le\; e_n \;\le\; f_n$$

The problem is to understand the asymptotic behavior of these six quantities as $n \to \infty$.

Lower bounds. Odlyzko's zeta-function-based theory gives a lower bound d'_n on d_n. If one assumes the generalized Riemann hypothesis one gets a larger lower bound d''_n on d_n. In small degrees (say $n \leq 100$) it is known that d_n/d''_n is small, typically less that 1.02.

The d'_n and d''_n are each increasing with

$$\lim_{n\to\infty} d'_n = 4e^{\gamma}\pi \approx 22.3816$$
$$\lim_{n\to\infty} d''_n = 8e^{\gamma}\pi \approx 44.7632$$

Since

$$d_n \leq b_n, c_n, e_n, f_n$$

Odlyzko's theory gives lower bounds on b_n, c_n, e_n, and f_n too. **No better lower bounds are known!**

Upper bounds on d_n. An old "cherished dream of Artin and Hasse" was that $d_n \to \infty$. Golod and Shafarevich (1964) destroyed this dream when they found infinite class field towers

$$F = H_0 \subset H_1 \subset H_2 \subset \cdots$$

with H_k unramified over H_{k-1} and hence all H_k having root discriminant the same as F.

Martinet (1978) showed that even the degree 20 field $\mathbf{Q}(\cos(2\pi/11), \sqrt{2}, \sqrt{-23})$ has an infinite class field 2-tower. Thus

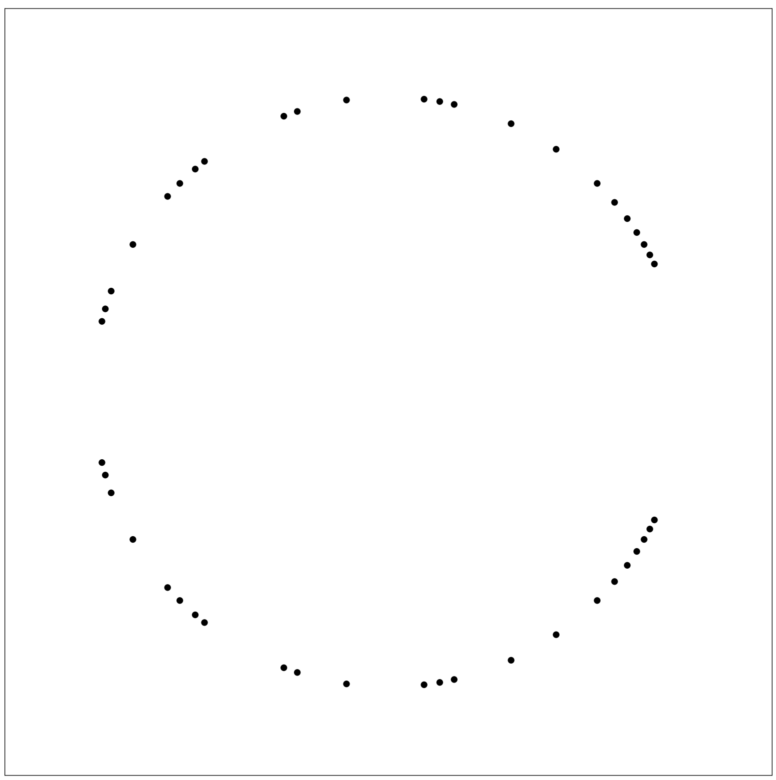
$$d_n \leq 11^{4/5} 2^{3/2} 23^{1/2} \approx 92.4$$

for n of the form $5 \cdot 2^j$. By working with slightly ramified towers, Hajir and Maire (2001) showed $d_n < 83.9$ for n of the form $3 \cdot 2^j$.

Upper bounds on a_n (Simon 1999). The polynomial $f_n = \Phi_{m+1}\Phi_{m+2}\cdots\Phi_{2m-1}\Phi_{2m}$ has root discriminant of the form

$$\lambda\sqrt{n} + O((\log n)^2)$$

with $\lambda = \frac{\pi}{3e}2^{4/3}\prod p^{1/(p^2-1)} \approx 0.507$.

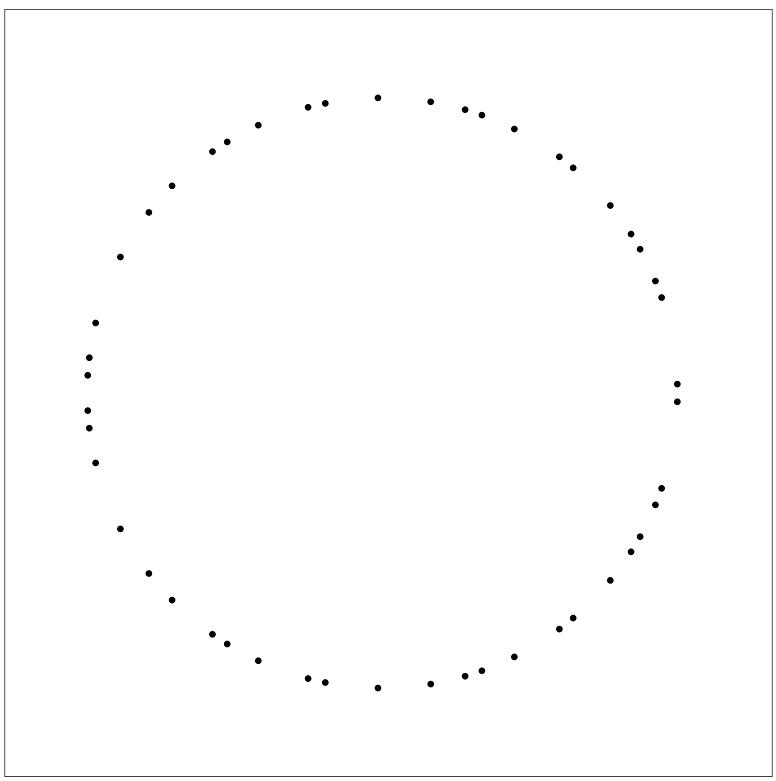


(Example of $\Phi_8\Phi_9\Phi_{10}\Phi_{11}\Phi_{12}\Phi_{13}\Phi_{14}$: $n = 46$, $d \approx 6.31$; $d/\sqrt{n} \approx 0.93$, $s = d/n \approx 0.14$)

Upper bounds on b_n (Scholz 1938; Simon 1999). The polynomial $g_n = \Phi_{2\cdot3\cdot5\cdot7\cdots p_k}$ has root discriminant asymptotic to

$$e^{2\gamma} n \frac{\log\log n}{\log n}.$$

These are the best current upper bounds on b_n.

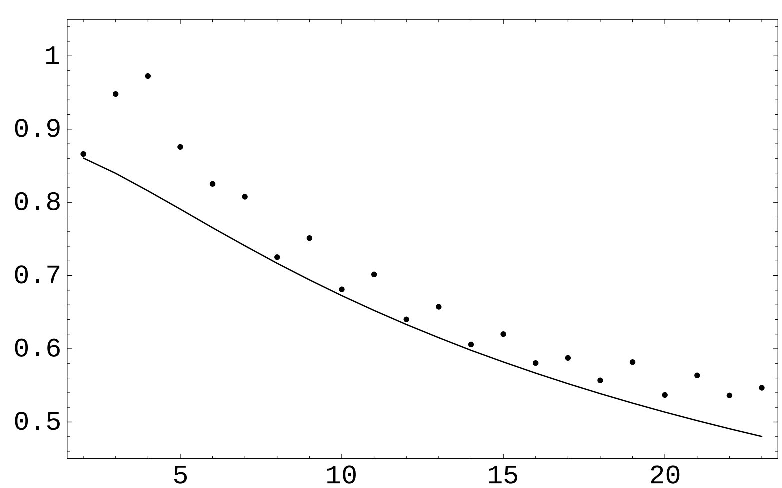


(Example of Φ_{210}: $n = 48$, $d \approx 29.31$, $d/\sqrt{n} \approx 4.23$, and $s = d/n \approx 0.61$.)

Results on c_n and e_n for small n. For $n \leq 7$, generic polynomials simultaneously giving the smallest polynomial root discriminant c_n and smallest field root discriminant e_n:

n	$f(x)$	D_f	d_f	s_f
2	$x^2 - x - 1$	3	1.73	0.87
3	$x^3 - x^2 - 1$	23	2.84	0.95
4	$x^4 - x^3 - 1$	229	3.89	0.97
5	$x^5 - x^4 - x^3 + x^2 - 1$	1609	4.38	0.88
6	$x^6 - x^5 + x^3 - x^2 + 1$	14731	4.95	0.83
7	$1, -1, -1, 0, 1, 1, -1, -1$	184607	5.65	0.81

In degrees 8-23, the current records (Simon 1999) towards c_n and e_n again agree and compare with Odylzko lower bounds as follows:



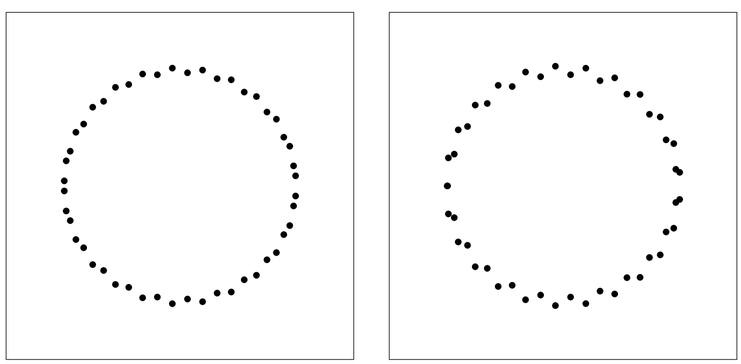
Upper bounds on c_n and e_n from trinomials. Let

$$f(x) = x^n + ax^m + b.$$

If n and m are relatively prime then

$$D_f = |n^n b^{n-1} - (-1)^n m^m (n-m)^{n-m} a^n b^{m-1}|.$$

As we are looking for small discriminants, we take $b = \pm 1$. Taking $a = \pm 1$ then makes the first term larger in absolute value and in large degrees scores become very close to 1. Taking $a = \pm 2$ gives smaller scores, but non-generic polynomials.

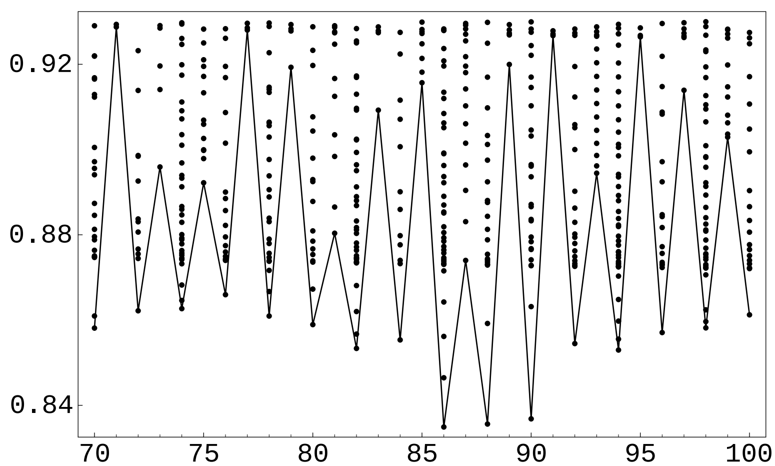


($x^{48}+x^{23}+1$ with score 0.99999999999999992 and $x^{48} + 2x^{23} + 1$ with score 0.93, but reducible.)

Upper bounds on c_n and e_n from quadrinomials. Consider

$$f(x) = x^n + ax^m + bx^r + c.$$

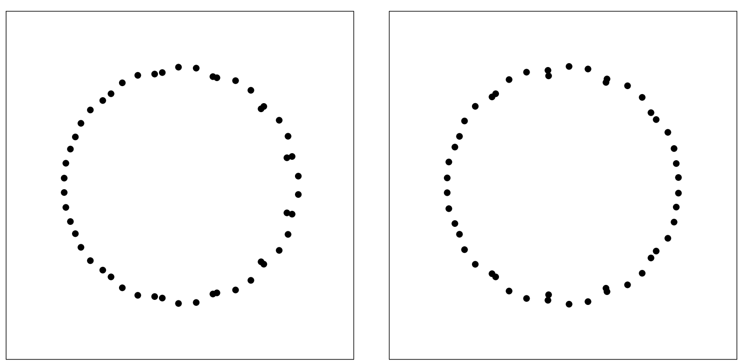
with $n > m > r > 0$ and $a, b, c \in \{-1, 1\}$. Scores tend to be near 1. All scores < 0.93 arising in degrees $70 \leq 100$, with the lowest scores for each degree connected by straight lines:



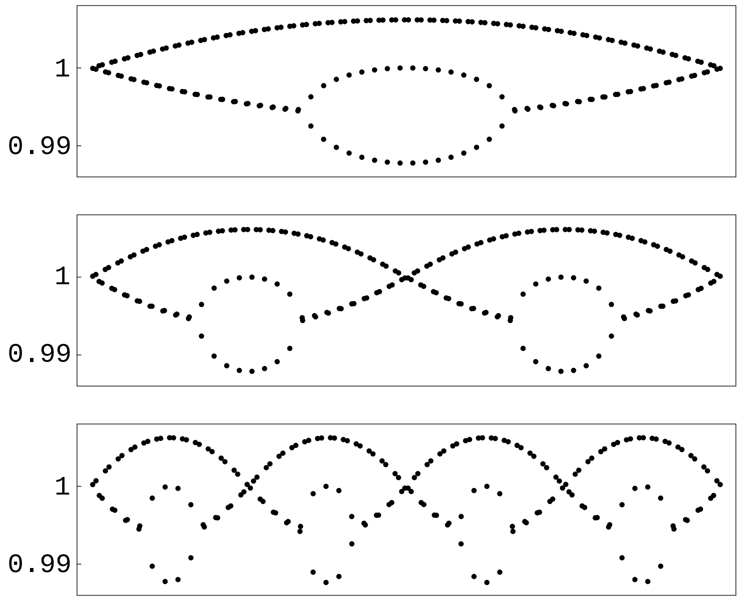
Polynomials $q_n(x)$ giving rise to the lowest scores in even degrees have one of three forms:

$x^{4k+2} + x^{k+1} + x^k + 1$ if $n = 4k + 2$
$x^{4k} + x^{k+1} - x^{k-1} + 1$ if $n = 4k$ with k even
$x^{4k} + x^{k+2} - x^{k-2} + 1$ if $n = 4k$ with k odd

Roots of the Case 1 polynomial $q_{50}(x) = x^{50} + x^{13} + x^{12} + 1$ on the left, with score 0.870919. Note that for $|\theta|$ near 0 there are four pairs of close roots with very close arguments θ; for $|\theta|$ near $\pi/2$ there are similarly close roots, but now with very close moduli r. For $|\theta|$ near π the roots are equally spaced.



Roots of the Case 2 polynomial $q_{48}(x) = x^{48} + x^{13} - x^{11} + 1$ on the right, with score 0.871762. Here what happened over the θ-interval $[-\pi, \pi]$ for q_{50} happens for q_{48} over $[-\pi, 0]$ and again over $[0, \pi]$.



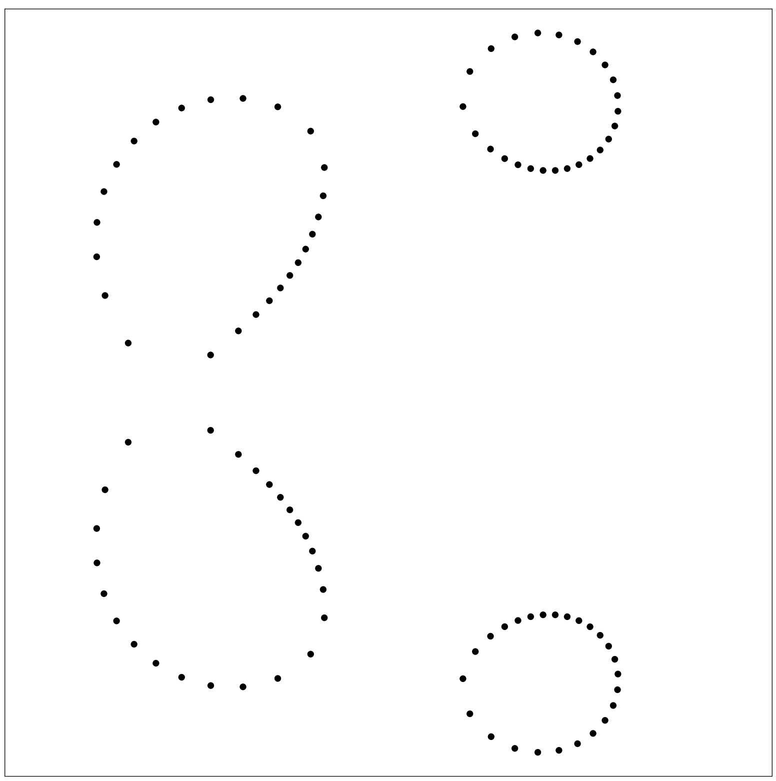
The root plots correspond to q_{198}, q_{200}, q_{196} which belong to Cases 1, 2, and 4 respectively. Points (r, θ) with r the modulus of a root and $\theta \in [-\pi, \pi]$ the argument of the same root are plotted. To make distances approximately correct, each root plot should be compressed vertically by a factor of 80.

From computations out through degree 1200, it seems that the scores of q_n converge to a constant near 0.84674.

Upper bounds on c_n and e_n from perturbing singular polynomials. Example:

$$(x^4 + x^3 + x^2 + x + 1)^m - x^{2m-1}$$

seems to have scores tending to $5^{3/4}/4 \approx 0.835$ Root plot with $m = 25$ so that $n = 100$ and $s = d/n = 0.841738$.



Questions: $\liminf c_n > 0$? $\liminf e_n > 0$??

Upper bounds on f_n from Borisov's (1998) abc-polynomials. For b, c, relatively prime positive integers put $a = b + c$ and

$$f_{a,b,c}(x) = \frac{bx^a - ax^b + c}{(x-1)^2}$$

so that the degree is $n = a-2$. The coefficients increase arithmetically from b by steps of b to bc and then decrease arithmetically by steps of c to c, e.g.

$$f_{8,1,7}(x) = \\ x^6 + 2x^5 + 3x^4 + 4x^3 + 5x^2 + 6x + 7$$

$$f_{8,3,5}(x) = \\ 3x^6 + 6x^5 + 9x^4 + 12x^3 + 15x^2 + 10x + 5$$

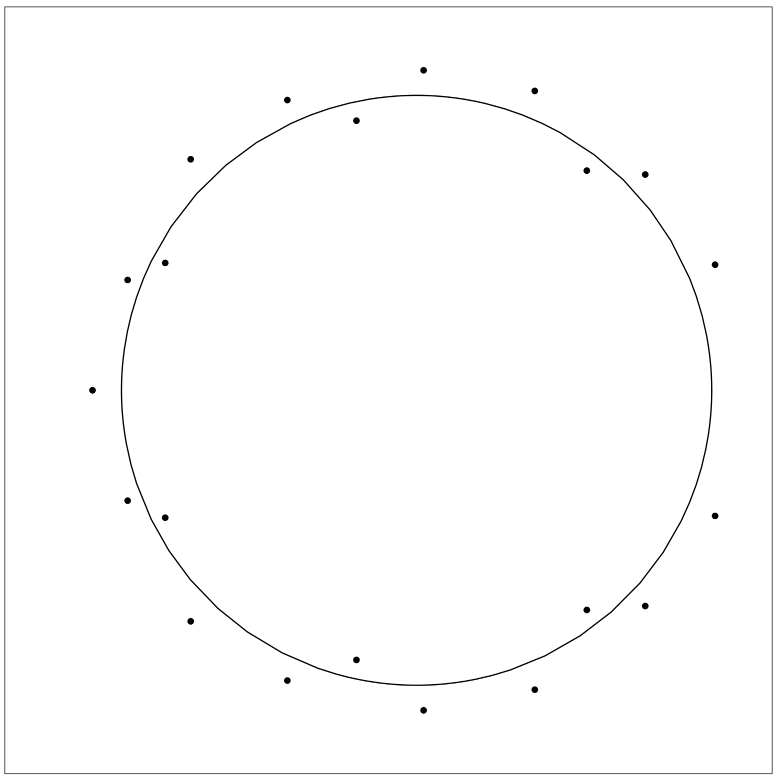
The polynomial discriminant is

$$D_{a,b,c} = 2a^{a-3}b^{a-4}c^{a-4}$$

so that a prime divides $D_{a,b,c}$ iff it divides abc. Galois root discriminants are small, e.g.

$$\begin{aligned} D_{8,1,7} &= 2^{11/4}7^{4/5} &&\approx 31.9088 \\ D_{8,3,5} &= 2^{11/4}3^{4/5}5^{2/3} &&\approx 47.3707 \end{aligned}$$

There are $b-1$ roots inside the unit circle and $c-1$ roots outside the unit circle. There is one real root if a is odd and no real roots if a is even. A root plot of $f_{23,7,16}$:



It follows that $\mathrm{Gal}(f_{a,b,c})$ is inside the alternating group iff either (a is twice an odd square) or (b and c are an odd square and twice an odd square). The only known cases of smaller Galois group are $\mathrm{Gal}(f_{8,b,c}) = PGL_2(5) \subset S_6$.

Ramification behaves very regularly. Suppose $p|abc$. The ramification at p is tame iff one of a, b, c is p. The next simplest case is when otherwise $\text{ord}_p(abc) = 1$. Then all wild slopes at p are $1 + 1/(p-1)$.

The only completely tame fields are for $\{a, b, c\}$ has the form $\{n+2, n, 2\}$ with $(n, n+2)$ a twin prime pair. For these the Galois root discriminant is

$$2^{1-1/n} n^{1-1/(2n-4)} (n+2)^{1-1/n} \approx 2n^2.$$

Even when wild ramification is allowed, $2n^2$ seems a sharp asymptotic minimum, and we haven't seen lower GRD's in other contexts. So,

Question: $\liminf f_n/n^2 = 2$?