

# Computing Higher Polynomial Discriminants

Erich L. Kaltofen

Dept. of Mathematics, North Carolina State University  
Raleigh, North Carolina, USA  
kaltofen@ncsu.edu

Dept. of Computer Science, Duke University  
Durham, North Carolina, USA

## ABSTRACT

In <https://arxiv.org/abs/1609.00840> (see also <https://doi.org/10.1007/s11425-018-1594-2>), Dongming Wang and Jing Yang in 2016 have posed the problem how to compute the “third” discriminant of a polynomial  $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ ,

$$\delta_3(f) = \prod_{1 \leq i < j < k < l \leq n} ((\alpha_i + \alpha_j - \alpha_k - \alpha_l)(\alpha_i - \alpha_j + \alpha_k - \alpha_l)(\alpha_i - \alpha_j - \alpha_k + \alpha_l)),$$

from the coefficients of  $f$ ; note that  $\delta_3$  is a symmetric polynomial in the  $\alpha_i$ . For complex roots,  $\delta_3(f) = 0$  if the mid-point (average) of 2 roots is equal the mid-point of another 2 roots. Iterated resultant computations yield the square of the third discriminant. We apply a symbolic homotopy by Kaltofen and Trager [JSC, vol. 9, nr. 3, pp. 301–320 (1990)] to compute its squareroot. Our algorithm uses polynomially many coefficient field operations in the degree of  $f$ .

## CCS CONCEPTS

• **Mathematics of computing** → **Computations on polynomials**; Computations in finite fields; • **Computing methodologies** → **Algebraic algorithms**.

## KEYWORDS

symmetric functions; polynomial resultant; Orlando polynomial; symbolic homotopy;

## ACM Reference Format:

Erich L. Kaltofen. 2021. Computing Higher Polynomial Discriminants. In *Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation (ISSAC '21), July 18–23, 2021, Virtual Event, Russian Federation*. ACM, New York, NY, USA, 7 pages. <https://doi.org/10.1145/3452143.3465543>

## 1 INTRODUCTION

Let  $K$  be a field and consider the polynomial

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).  
ISSAC '21, July 18–23, 2021, Virtual Event, Russian Federation

© 2021 Copyright held by the owner/author(s). Publication rights licensed to ACM.  
ACM ISBN 978-1-4503-8382-0/21/07...\$15.00  
<https://doi.org/10.1145/3452143.3465543>

$$F(x) = (x - y_1) \cdots (x - y_n) = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad \text{where } a_i \in K[y_1, \dots, y_n], \quad (1)$$

and  $y_i$  are fresh variables. Note that the  $a_i$  are plus/minus the elementary symmetric functions in  $y_i$ . The discriminant of  $F$  is defined as

$$\Delta_1(y_1, \dots, y_n) = \prod_{1 \leq i < j \leq n} ((y_i - y_j)(y_j - y_i)), \quad (2)$$

which is a symmetric polynomial in the  $y_i$ , that is, there is a polynomial  $D_1(z_0, \dots, z_{n-1}) \in K[z_0, \dots, z_{n-1}]$  ( $z_i$  fresh variables) such that  $\delta_1(F, x) = D_1(a_0, \dots, a_{n-1}) = \Delta_1(y_1, \dots, y_n)$ . If  $K$  is a field of characteristic  $\neq 2$ , then  $D_1$  is absolutely irreducible, that is an irreducible polynomial over the algebraic closure of  $K$  (see the paragraph below the Proof of Lemma 1.1). Note our notation:  $\Delta_1$  is the discriminant polynomial in variables for the roots,  $D_1$  is the discriminant polynomial in variables for the coefficients (except the leading 1), and  $\delta_1$  is a corresponding function with a univariate polynomial argument whose variable is the second argument. For a polynomial  $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in K[x]$  we write  $\delta_1(f) = D_1(c_0, \dots, c_{n-1})$ ; because there is a single variable  $x$ , we omit that second argument. Each symbol denotes a family of  $n$ -variate polynomials, where  $n$  is the degree of  $F$ . All our discriminant formulas will be identities on multivariate polynomials into which actual roots and coefficients can be substituted. For instance, the formula for the discriminant as the Sylvester resultant of  $F$  and its derivative  $\partial F / \partial x$ ,

$$D_1(a_0, \dots, a_{n-1}) = \det \begin{pmatrix} 1 & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & 1 & a_{n-1} & \ddots & & a_0 & & \vdots \\ \vdots & & & \ddots & & & & \vdots \\ 0 & 0 & & & 1 & a_{n-1} & a_{n-2} & \cdots & a_0 \\ n & (n-1)a_{n-1} & \cdots & & 2a_2 & a_1 & 0 & \cdots & 0 \\ 0 & n & (n-1)a_{n-1} & \cdots & 2a_2 & a_1 & \ddots & & \vdots \\ \vdots & & & & & & & & \vdots \\ 0 & \cdots & & & 0 & n & (n-1)a_{n-1} & \cdots & 2a_2 & a_1 \end{pmatrix}, \quad (3)$$

is an identity in  $K[y_1, \dots, y_n]$  over any field  $K$ , even those whose characteristic divides  $n$ .<sup>1</sup>

For fields  $K$  of characteristic 2,  $D_1$  is the square of the Orlando polynomial

$$\widehat{\Delta}_1 = \prod_{1 \leq i < j \leq n} (y_i + y_j) \quad (4)$$

<sup>1</sup>Note that if the discriminant is defined as  $\prod_{i < j} (x_i - x_j)^2$  one multiplies (3) by  $(-1)^{n(n-1)/2}$ .

whose corresponding  $\widehat{D}_1$  is again is an absolutely irreducible polynomial in the coefficient variables  $z_i$  (see Lemma 1.1). A corresponding determinantal expression is Luciano Orlando's 1911 formula (5) of Figure 1.

**Figure 1:** Luciano Orlando's 1911 Formula [4], [2, Eq. (1.37)].

$$\widehat{D}_1(a_0, \dots, a_{n-1}) = (-1)^{n(n-1)/2} \det \begin{pmatrix} a_{n-1} & a_{n-3} & a_{n-5} & \dots & \dots & a_{-(n-3)} & a_{-(n-1)} \\ 1 & a_{n-2} & a_{n-4} & \dots & \dots & a_{-(n-4)} & a_{-(n-2)} \\ a_{n+1} & a_{n-1} & a_{n-3} & a_{n-5} & \dots & a_{-(n-5)} & a_{-(n-3)} \\ a_{n+2} & 1 & a_{n-2} & a_{n-4} & \dots & a_{-(n-6)} & a_{-(n-4)} \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ a_{2n-3} & \dots & \dots & \dots & \dots & a_1 & a_{-1} \\ a_{2n-2} & \dots & \dots & \dots & \dots & a_2 & a_0 \end{pmatrix},$$

where  $a_i = 0$  for all  $i > n$  and  $i < 0$ . (5)

In [5, 6] higher discriminants are introduced. One forms a product of linear combinations of the roots  $y_i$  that lead to symmetric polynomials. For fields  $K$  of characteristic  $\neq 2$  and  $\neq 3$  [5] define

$$\Delta_2 = \prod_{1 \leq i < j < k \leq n} \left( (2y_i - y_j - y_k)(2y_j - y_i - y_k)(2y_k - y_i - y_j) \right) \quad (6)$$

and the corresponding  $D_2(z_0, \dots, z_{n-1})$  as the second discriminant, which is absolutely irreducible over  $K$  (see Lemma 1.1). Wang and Yang [2016] give determinantal representations of  $\Delta_2$  in terms of the coefficients of  $f$  in analogy to (3.5). The corresponding higher Orlando polynomial is

$$\widehat{\Delta}_2 = \prod_{1 \leq i < j < k \leq n} (y_i + y_j + y_k), \quad (7)$$

which is defined for any characteristic and where the corresponding  $\widehat{D}_2$  is absolutely irreducible (see Lemma 1.1).

Wang and Yang [5, Section 8] further define third discriminants. For fields  $K$  of characteristic  $\neq 2$ , they define

$$\Delta_3 = \prod_{1 \leq i < j < k < \ell \leq n} \left( (y_i + y_j - y_k - y_\ell)(y_i - y_j + y_k - y_\ell)(y_i - y_j - y_k + y_\ell) \right) \quad (8)$$

and the corresponding  $D_3(z_0, \dots, z_{n-1})$  as the third discriminant, which is absolutely irreducible over  $K$ . Over fields of characteristic 2 we have  $\Delta_3 = \widehat{\Delta}_3^3$  (see (12)). By expressing the lexicographically leading term with variable order  $y_1 > y_2 > \dots > y_n$  in (8) as the leading term in a symmetric product,

$$y_1^{3 \binom{n-1}{3}} y_2^{3 \binom{n-2}{3}} \dots y_{n-3}^{3 \binom{3}{3}} = \text{lead-term} \left( a_{n-1}^{3 \binom{n-2}{2}} a_{n-2}^{3 \binom{n-3}{2}} \dots a_3^{3 \binom{2}{2}} \right),$$

where the  $a_i$ 's are defined in (1), we obtain the total degree

$$\deg_{z_0, \dots, z_{n-1}}(D_3) = 3 \binom{n-1}{3}.$$

In Section 4 we give the polynomial for  $D_3(z_0, \dots, z_4)$  ( $n = 5$ ) whose leading monomial is  $-z_4^9 z_3^3$ . Note that the variables  $z_i$  correspond to the coefficients  $c_i$  of  $f$ , not the elementary symmetric functions in the roots of  $f$ : In (1) we have  $a_i = (-1)^{n-i} \sigma_{n-i}(y_1, \dots, y_n)$  with  $\sigma_k(y_1, \dots, y_n) = \sum_{1 \leq j_1 < \dots < j_k \leq n} y_{j_1} \dots y_{j_k}$ .

Wang and Yang [2016] also consider factors of the form  $3y_i - y_j -$

$y_k - y_\ell$ . The geometric interpretation of  $D_2$  and  $D_3$  is as follows. Let  $f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0 \in K[x]$ , where  $K$  is a field of characteristic  $\neq 2$  and  $\neq 3$  and  $n \geq 4$ . If  $D_2(c_0, \dots, c_{n-1}) = 0$  then the average of 2 roots is a third root, and if  $D_3(c_0, \dots, c_{n-1}) = 0$  then the average of 2 roots is = the average of another 2 roots. Over the complex numbers  $K = \mathbb{C}$  the average is the mid-point between the two complex roots on the complex plane.

One can generalize the construction to the factors being weighted linear forms  $w_1 y_{i_1} + w_2 y_{i_2} + \dots + w_\nu y_{i_\nu}$  with  $\nu \geq 2$  and  $n \geq \nu$  and weights  $w_1 = 1$ ,  $w_\mu \in K$  for  $2 \leq \mu \leq \nu$ . Then for a set  $P \subseteq S_\nu$  of permutations on  $(1, \dots, \nu)$ , where  $S_\nu$  is the set of all permutations on  $(1, \dots, \nu)$ , we define

$$\Delta_{\nu-1, \vec{w}, P} = \prod_{1 \leq i_1 < \dots < i_\nu \leq n} \prod_{\sigma \in P} (w_{\sigma(1)} y_{i_1} + w_{\sigma(2)} y_{i_2} + \dots + w_{\sigma(\nu)} y_{i_\nu}). \quad (9)$$

By reordering the weights we may assume that the identity permutation  $\in P$ . We shall require from  $P$  that  $\Delta_{\nu-1, \vec{w}, P}$  in (9) is a symmetric polynomial in  $y_1, \dots, y_n$  whose corresponding polynomial  $D_{\nu-1, \vec{w}, P}(z_0, \dots, z_{n-1})$  in the coefficient variables of  $F$  is absolutely irreducible over  $K$ . A sufficient condition for  $P$  is the following:

LEMMA 1.1. *Suppose the following conditions are satisfied for  $P \subseteq S_\nu$ :*

1. *For all permutations  $\pi \in S_n$  on  $(1, \dots, n)$  we have: if  $\{\pi(i_1), \dots, \pi(i_\nu)\} = \{j_1, \dots, j_\nu\}$  with  $j_1 < j_2 < \dots < j_\nu$  then*

$$\prod_{\sigma \in P} (w_{\sigma(1)} y_{\pi(i_1)} + w_{\sigma(2)} y_{\pi(i_2)} + \dots + w_{\sigma(\nu)} y_{\pi(i_\nu)}) = \prod_{\sigma \in P} (w_{\sigma(1)} y_{j_1} + w_{\sigma(2)} y_{j_2} + \dots + w_{\sigma(\nu)} y_{j_\nu}). \quad (10)$$

*Note that if  $(w_{\sigma(1)}, \dots, w_{\sigma(\nu)})_{\sigma \in P}$  is a list of all distinct reorderings of the weights, condition (10) is true. If there are  $\kappa$  distinct weights of multiplicity  $m_1, m_2, \dots, m_\kappa$ ,  $\nu = m_1 + \dots + m_\kappa$ , there are  $\nu! / (m_1! \dots m_\kappa!)$  such reorderings.*

2. *For all permutations  $\sigma, \tau \in P$  with  $\sigma \neq \tau$ :  $(w_{\sigma(1)}, w_{\sigma(2)}, \dots, w_{\sigma(\nu)})$  is not a scalar multiple of  $(w_{\tau(1)}, w_{\tau(2)}, \dots, w_{\tau(\nu)})$ .*

*Then  $\Delta_{\nu-1, \vec{w}, P}$  is a symmetric polynomial and  $D_{\nu-1, \vec{w}, P}$  is absolutely irreducible over  $K$ .*

PROOF. By Item 1 a permutation  $\pi$  maps an inner product polynomial of (9) to another inner product polynomial, which establishes symmetry. Item 2 establishes that all linear forms in (9) are relatively prime to one another. Now let  $E(z_0, \dots, z_{n-1})$  be an absolutely irreducible factor of  $D_{\nu-1, \vec{w}, P}(z_0, \dots, z_{n-1})$  such that  $w_1 y_1 + \dots + w_\nu y_\nu$  divides  $E(a_0, \dots, a_{n-1})$ . Because  $E$  on evaluation is symmetric in the  $y_i$ ,  $w_1 y_{\pi(1)} + \dots + w_\nu y_{\pi(\nu)}$  must also divide  $E(a_0, \dots, a_{\nu-1})$  for all  $\pi \in S_n$ . Now for all  $1 \leq i_1 < \dots < i_\nu \leq n$  and all  $\sigma \in P$  let  $\pi(\mu) = i_{\sigma^{-1}(\mu)}$  for  $1 \leq \mu \leq \nu$ . Then  $w_1 y_{\pi(1)} + \dots + w_\nu y_{\pi(\nu)} = w_{\sigma(1)} y_{i_1} + \dots + w_{\sigma(\nu)} y_{i_\nu}$ , and therefore all (relatively prime) factors of (9) divide  $E(a_0, \dots, a_{\nu-1})$ , implying that  $E = D_{\nu-1, \vec{w}, P}$ .  $\square$

Lemma 1.1 applies to all the above discriminants except the classical discriminant  $D_1$ . Item 2 in Lemma 1.1 is not satisfied for  $\Delta_1$  in (2): the weight vectors of the linear forms have  $(1, -1) = -(-1, 1)$ . In the proof of Lemma 1.1 we then get that  $\prod_{i < j} (y_i - y_j)$

divides  $E(a_0, \dots, a_{n-1})$  and possibly the evaluated polynomial cofactor. In the latter case,  $E(a_0, \dots, a_{n-1}) = c \prod_{i < j} (y_i - y_j)$  for some  $c \in K$ , which changes sign under transposing  $(y_1, y_2)$  and would therefore not be symmetric over characteristic  $\neq 2$ . For fields  $K$  of characteristic 2, the classical discriminant  $D_1$  is the square of the Orlando polynomial (4).

The validity of Item 1 in Lemma 1.1 is proven for  $\Delta_3$  in (8) by observing that if  $\pi(j)$  becomes the smallest of  $\pi(i), \pi(j), \pi(k), \pi(\ell)$ , for example, then

$$\begin{aligned} & (y_{\pi(i)} + y_{\pi(j)} - y_{\pi(k)} - y_{\pi(\ell)}) (y_{\pi(i)} - y_{\pi(j)} + y_{\pi(k)} - y_{\pi(\ell)}) \\ & \quad \times (y_{\pi(i)} - y_{\pi(j)} - y_{\pi(k)} + y_{\pi(\ell)}) = \\ & (y_{\pi(i)} + y_{\pi(j)} - y_{\pi(k)} - y_{\pi(\ell)}) (-1) (y_{\pi(i)} - y_{\pi(j)} + y_{\pi(k)} - y_{\pi(\ell)}) \\ & \quad \times (-1) (y_{\pi(i)} - y_{\pi(j)} - y_{\pi(k)} + y_{\pi(\ell)}), \quad (11) \end{aligned}$$

and  $y_{\pi(j)}$  has positive sign in all factors. Note that we have  $D_3 = D_{3, (1,1,-1,-1), P_3}$  where  $P_3 = \{\text{id}, \binom{1,2,3,4}{1,3,2,4}, \binom{1,2,3,4}{1,4,2,3}\} \subset S_4$ . There is another  $\tilde{D}_3 = D_{3, (-1,-1,1,1), P_3} = (-1) \binom{n}{4} D_{3, (1,1,-1,-1), P_3}$ .

The objective of our paper is for a given  $f \in K[x]$  to compute  $\delta_{v-1, \vec{w}, P}(f)$  for fixed  $v, \vec{w}$  and  $P$  in polynomially many field operations in  $\text{deg}(f)$ .

## 2 COMPUTING HIGHER ORLANDO POLYNOMIALS

For  $v \geq 2$  we shall write

$$\begin{aligned} \widehat{\Delta}_{v-1} &= \prod_{1 \leq i_1 < i_2 < \dots < i_v \leq n} (y_{i_1} + y_{i_2} + \dots + y_{i_v}) \\ &\in K[y_1, \dots, y_n], \quad K \text{ a field.} \quad (12) \end{aligned}$$

The polynomial  $\widehat{\Delta}_{v-1}$  of total degree  $\binom{n}{v}$  is symmetric in the  $y_i$  and therefore a polynomial in the elementary symmetric functions. We let  $\widehat{D}_{v-1} \in K[z_0, \dots, z_{n-1}]$  be the polynomial in coefficient variables  $z_i$  such that for  $F(x) = (x - y_1) \dots (x - y_n) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ , where  $a_i \in K[y_1, \dots, y_n]$  (1), we have  $\widehat{D}_{v-1}(a_0, \dots, a_{n-1}) = \widehat{\Delta}_{v-1}$ . For  $f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0 \in K$  we define

$$\widehat{\delta}_{v-1}(f) \stackrel{\text{def}}{=} \widehat{D}_{v-1}(c_0, \dots, c_{n-1}) \in K. \quad (13)$$

We now give algorithms that compute  $\widehat{\delta}_{v-1}$  from input  $f$ . For  $v = 2$  one can use Orlando's Formula (5). Our algorithms will show that  $\widehat{D}_{v-1}$  is an integer polynomial in the  $z_i$  (taking the coefficients modulo the characteristic for fields of characteristic  $< \infty$ ).

We consider  $v = 3$  (7). Let  $G(x) = v_m x^m + v_{m-1} x^{m-1} + \dots + v_0 \in (K[v_0, \dots, v_m])[x]$ , where  $v_i$  are fresh variables, and let  $R = \text{res}(F, G, x)$  be the Sylvester resultant of  $F$  and  $G$  in the variable  $x$ ,

$$R = \det \begin{pmatrix} 1 & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & \dots & 0 \\ 0 & 1 & a_{n-1} & \dots & a_0 & \dots & \dots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{n-1} & a_{n-2} & \dots & a_0 \\ v_m & v_{m-1} & \dots & v_1 & v_0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & v_m & v_{m-1} & \dots & v_1 & v_0 & \dots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & v_m & v_{m-1} & \dots & v_1 & v_0 \end{pmatrix} = \prod_{i=1}^n G(y_i). \quad (14)$$

Note that the Sylvester matrix in (14) is of dimensions  $n+m$  and that the product identity in (14) is in the polynomial ring  $K[y_1, \dots, y_n]$ ,

$v_0, \dots, v_m]$ , which yields an algorithm for  $\widehat{\delta}_{v-1}$ , which we describe now.

Let  $f(x) = x^n + c_{n-1}x^{n-1} + \dots + c_0 = \prod_{i=1}^n (x - \alpha_i) \in K[x]$  where  $\alpha_i \in \overline{K}$ , where  $\overline{K}$  is the algebraic closure of  $K$ . We may assume that  $c_0 \neq 0$ , because we have for monic  $f \in K[x]$  with  $f(0) \neq 0$ :

$$\begin{aligned} \widehat{\delta}_2(xf(x)) &= \widehat{\delta}_1(f) \widehat{\delta}_2(f), \quad \widehat{\delta}_2(x^2 f(x)) = f(0) \widehat{\delta}_1(f)^2 \widehat{\delta}_2(f), \\ \widehat{\delta}_2(x^k f(x)) &= 0 \text{ for } k \geq 3. \quad (15) \end{aligned}$$

Note that  $\widehat{\delta}_1(f) = \prod_{i < j} (\alpha_i + \alpha_j)$  can be computed by Orlando's Formula (5). Then by (14) we have

$$\begin{aligned} f^{[i,j]}(x) &\stackrel{\text{def}}{=} \text{res}(\underbrace{(-1)^n f(-u+x)}_{\prod (u - (x - \alpha_i))}, f(u), u) \\ &= \prod_{1 \leq i, j \leq n} (x - (\alpha_i + \alpha_j)) \in K[x]. \quad (16) \end{aligned}$$

For an integer  $\lambda \in \mathbb{Z}$  with  $\lambda \geq 2$  we define

$$f^{[\lambda i]}(x) \stackrel{\text{def}}{=} \prod_{i=1}^n (x - \lambda \alpha_i) = \begin{cases} x^n & \text{if } \lambda \bmod \text{char}(K) = 0, \\ \lambda^n f(x/\lambda) & \text{if } \lambda \bmod \text{char}(K) \neq 0, \end{cases} \quad (17)$$

We compute

$$f^{[i \neq j]}(x) \stackrel{\text{def}}{=} \frac{f^{[i,j]}(x)}{f^{[2i]}(x)} = \prod_{1 \leq i, j \leq n, i \neq j} (x - \alpha_i - \alpha_j). \quad (18)$$

We next compute, over fields of characteristic  $\neq 2$ , by power series expansion (Hensel lifting with multiplicities—see Appendix A) the squareroot of (18), which is

$$f^{[i < j]}(x) \stackrel{\text{def}}{=} \prod_{1 \leq i < j \leq n} (x - \alpha_i - \alpha_j) = f^{[i \neq j]}(x)^{1/2}. \quad (19)$$

If  $K$  has characteristic = 2, we assume to have a squareroot algorithm in  $K$ . For example, for  $K = \mathbb{F}_{2^k}$ , we have  $(c^2)^{2^{k-1}} = c \in \mathbb{F}_{2^k}$  (the squareroots are unique). Then the squareroot of a squared polynomial is  $(x^{2d} + b_{d-1}^2 x^{2(d-1)} + \dots + b_0^2)^{1/2} = x^d + b_{d-1} x^{d-1} + \dots + b_0$ . Note that if the field  $K$  has characteristic  $\neq 2$ , one may use (5) to compute  $f^{[i < j]}(x)$ : If  $f(u + x/2) = u^n + b_{n-1} u^{n-1} + \dots + b_0$  with  $b_i \in K[x]$ , then  $f^{[i < j]}(x) = (-1)^{n(n-1)/2} \widehat{D}_1(b_0, \dots, b_{n-1})$ .

Again by (14) we have

$$\begin{aligned} f^{[-, 2i, -, j]}(x) &\stackrel{\text{def}}{=} \text{res}(f^{[2i]}(u-x), (-1)^n f(-u), u) \\ &= \prod_{1 \leq i, j \leq n} (x + 2\alpha_i + \alpha_j) \in K[x], \quad (20) \end{aligned}$$

where  $\text{deg}(f^{[-, 2i, -, j]}) = n^2$ ,

$$\begin{aligned} f^{[-, i < j, -, k]}(x) &\stackrel{\text{def}}{=} \text{res}(f^{[i < j]}(u-x), (-1)^n f(-u), u) \\ &= \prod_{\substack{1 \leq i < j \leq n \\ 1 \leq k \leq n}} (x + \alpha_i + \alpha_j + \alpha_k) \in K[x], \quad (21) \end{aligned}$$

where  $\text{deg}(f^{[-, i < j, -, k]}) = n \binom{n}{2}$ ,

$$\begin{aligned} f_{\text{orl}}^{[\text{cbd}]}(x) &\stackrel{\text{def}}{=} \frac{(-1)^n f^{[-, i < j, -, k]}(x)}{f^{[-, 2i, -, j]}(x) / f^{[3i]}(-x)} \\ &= \prod_{1 \leq i < j < k \leq n} (x + \alpha_i + \alpha_j + \alpha_k)^3 \in K[x], \quad (22) \end{aligned}$$

where  $\deg(f_{\text{orl}}^{[\text{cbd}]}) = n \binom{n}{2} - n^2 + n = 3 \binom{n}{3}$ . If  $K$  has characteristic  $\neq 3$ , we compute  $f_{\text{orl}}(x) \stackrel{\text{def}}{=} \prod_{1 \leq i < j < k \leq n} (x + \alpha_i + \alpha_j + \alpha_k)$  as the cube root of  $f_{\text{orl}}^{[\text{cbd}]}(x)$  (see Appendix A). The Orlando value  $\widehat{\delta}_2(f)$  (13) is then the constant coefficient of  $f_{\text{orl}}$ . For fields  $K$  of characteristic 3 we again must assume that one can compute cube roots of elements in  $K$ . For example, for  $K = \mathbb{F}_{3^k}$  we have  $(c^3)^{3^{k-1}} = c \in \mathbb{F}_{3^k}$  (the cube root is unique).

One reviewer has pointed out that in [1] a different algorithm is presented for computing  $f_{\text{orl}}(x)$  from  $f(x)$ , which is based on using the Newton-identities for the sums of the powers of the roots of a polynomial in terms of symmetric functions. That algorithm is presented to iterate to arbitrary  $v$ , which is also possible for our algorithm above. The algorithm in [1] requires the field  $K$  to have 0 or a large characteristic, as divisions by factorials occur.

One may avoid the computation of the polynomial  $f^{[-,i<j,-,k]}$  in (21) whose degree grows cubically in  $n$ , using a symbolic homotopy. We construct the symbolic homotopical polynomial (cf. [3])

$$f_{\text{hom}}(x) = tf(x) + (1-t)f_{\text{known}}(x) \in (K[t])[x], \quad (23)$$

where

$$f_{\text{known}}(x) = (x-r_1) \cdots (x-r_n) \in K[x] \quad (24)$$

is computed for such values of the roots  $r_i \in K$  that we have

$$0 \neq \widehat{\delta}_2(f_{\text{known}}) \prod_{1 \leq i < j \leq n} (2r_i + r_j) \\ \text{where } \widehat{\delta}_2(f_{\text{known}}) = \prod_{1 \leq i < j < k \leq n} (r_i + r_j + r_k). \quad (25)$$

Since  $r_n$  as a variable in (25) has degree  $n-1 + \binom{n-1}{2}$ , this is always possible if the cardinality of  $K$  is  $\geq n + \binom{n-1}{2}$ . For smaller finite fields we can algebraically extend  $K$  to sufficiently large cardinality.

One computes  $\widehat{\delta}_2(f_{\text{hom}})^3 \in K[t]$  as follows (writing  $f_{\text{hom}}(x) = \prod_i (x - \alpha_i^h)$ ):

$$d^{[i<j,k]}(t) \stackrel{\text{def}}{=} \text{res}(f_{\text{hom}}^{[i<j]}(u), (-1)^n f_{\text{hom}}(-u), u) \\ = \prod_{\substack{1 \leq i < j \leq n \\ 1 \leq k \leq n}} (\alpha_i^h + \alpha_j^h + \alpha_k^h) \in K[t], \quad (26)$$

$$d^{[2i,j]}(t) \stackrel{\text{def}}{=} \text{res}(f_{\text{hom}}^{[2i]}(u), (-1)^n f_{\text{hom}}(-u), u) \\ = \prod_{1 \leq i,j \leq n} (2\alpha_i^h + \alpha_j^h) \in K[t], \quad (27)$$

$$d^{[2i,j,i \neq j]}(t) \stackrel{\text{def}}{=} \begin{cases} \frac{d^{[2i,j]}(t)}{(-3)^n f_{\text{hom}}(0)} & \text{if } 3 \bmod \text{char}(K) \neq 0, \\ \delta_1(f, x) \text{ (cf. (3))} & \text{if } 3 \bmod \text{char}(K) = 0, \end{cases} \quad (28)$$

$$d^{[\text{cbd}]}(t) \stackrel{\text{def}}{=} \frac{d^{[i<j,k]}(t)}{d^{[2i,j,i \neq j]}(t)} \\ = \prod_{1 \leq i < j < k \leq n} (\alpha_i^h + \alpha_j^h + \alpha_k^h)^3 = \widehat{\delta}_2(f_{\text{hom}})^3 \in K[t]. \quad (29)$$

The divisions in (28 and 29) are by non-zero polynomials because  $f_{\text{hom}}(0)$  evaluates at  $t=1$  to  $f(0)$ , which is non-zero by an earlier assumption (15), and  $d^{[2i,j,i \neq j]}(0) \neq 0$  by the second factor in (25).

We first prove that if  $d^{[\text{cbd}]}$  is a constant polynomial  $\in K$ , then

$\widehat{\delta}_2(f) = \widehat{\delta}_2(f_{\text{known}})$ , which has been computed while choosing the  $r_i$ . Suppose  $\widehat{\delta}_2(f) \neq \widehat{\delta}_2(f_{\text{known}})$ . The polynomial  $\widehat{\delta}_2(f_{\text{hom}}) \in K[t]$  then cannot be a constant polynomial because for  $t=0$  and  $t=1$  it evaluates to different values. Therefore its third power,  $d^{[\text{cbd}]}(t)$ , is not constant. Note that  $d^{[\text{cbd}]}$  may be constant even if the coefficients of  $f_{\text{hom}}$  depend on  $t$ .

In case  $d^{[\text{cbd}]}(t)$  has degree  $\geq 3$  in  $t$  (it is the third power of a non-constant polynomial) we compute the monic cube root polynomial of its monic associate,  $h(t)^3 = \frac{1}{c} d^{[\text{cbd}]}(t)$ , where  $c$  is the leading coefficient of  $d^{[\text{cbd}]}(t)$  in  $t$ . Because  $d^{[\text{cbd}]}(0) = \widehat{\delta}_2(f_{\text{known}})^3 \neq 0$  by (25) we must have  $h(0) \neq 0$ . Then the homotopy (23) yields  $\widehat{\delta}_2(f_{\text{hom}}) = \widehat{\delta}_2(f_{\text{known}})/h(0)h(t)$  and  $\widehat{\delta}_2(f) = \widehat{\delta}_2(f_{\text{known}})h(1)/h(0)$ .

### 3 COMPUTING HIGHER DISCRIMINANTS

Let

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \\ = \prod_{i=1}^n (x - \alpha_i), \quad n \geq 4, \quad c_i \in K, \quad \alpha_i \in \overline{K}, \quad (30)$$

where  $K$  is a field and  $\overline{K}$  its algebraic closure. We can compute the second discriminant  $\delta_2(f) \stackrel{\text{def}}{=} D_2(c_0, \dots, c_{n-1})$  = the constant coefficient of (33) (see (6)) as follows:

$$f^{[-,2i,j<k]}(x) \stackrel{\text{def}}{=} \text{res}(f^{[2i]}(u-x), f^{[i<j]}(u), u) \\ = \prod_{\substack{1 \leq i \leq n \\ 1 \leq j < k \leq n}} (x + 2\alpha_i - \alpha_j - \alpha_k), \quad (31)$$

where  $f^{[2i]}$  is (17) for  $\lambda=2$  and  $f^{[i<j]}$  is (19),

$$f^{[i,-,j,i \neq j]}(x) \stackrel{\text{def}}{=} \frac{\text{res}(f(u-x), f(u), u)}{x^n} \\ = \prod_{1 \leq i,j \leq n, i \neq j} (x + \alpha_i - \alpha_j), \quad (32)$$

$$f_{\text{sec-discr}}(x) \stackrel{\text{def}}{=} \frac{f^{[2i,-,j<k]}(x)}{f^{[i,-,j,i \neq j]}(x)} \\ = \prod_{\substack{1 \leq j < k \leq n \\ 1 \leq i \leq n, i \neq j, i \neq k}} (x + 2\alpha_i - \alpha_j - \alpha_k). \quad (33)$$

One may continue to the next higher polynomial:

$$f^{[i<j<k]}(x) \stackrel{\text{def}}{=} (-1)^{\binom{n}{3}} f_{\text{orl}}(-x) \\ = \prod_{1 \leq i < j < k \leq n} (x - \alpha_i - \alpha_j - \alpha_k), \quad (34)$$

where  $f_{\text{orl}}$  is defined in the text below (22),

$$\frac{\text{res}(f^{[3i]}(u-x), f^{[i<j<k]}(u), u)}{f_{\text{sec-discr}}(x)} \\ = \prod_{\substack{1 \leq i < j < k \leq n \\ 1 \leq \ell \leq n, \ell \neq i, \ell \neq j, \ell \neq k}} (x + 3\alpha_\ell - \alpha_i - \alpha_j - \alpha_k), \quad (35)$$

whose constant coefficient is one version of the third discriminant in [5] (see (41) below).

One can avoid the nested resultants by computing the square-free decomposition of  $f$ . Let  $f = \prod_{i=1}^k f_i^{f_i}$  where  $f_i$  are squarefree,  $n_k \stackrel{\text{def}}{=} \deg(f_k) \geq 1$  and  $\text{GCD}(f_i, f_j) = 1$  for all  $1 \leq i < j \leq k$ . If  $k \geq 3$  then  $\delta_2(f) = 0$  because there is a root of multiplicity 3. We have for a squarefree polynomial  $f_1$ :

$$\delta_2(f_1) = \text{res}(f_1^{[2i]}(x), f_1^{[i<j]}(x), x) / \delta_1(f_1), \quad (36)$$

where  $f_1^{[2i]}$  is (17) for  $f = f_1$  and  $\lambda = 2$  and  $f_1^{[i<j]}$  is (19) for  $f = f_1$ , and for the square of a squarefree polynomial  $f_2$ :

$$\delta_2(f_2^2) = 2^{2n_2(n_2-1)} \delta_1(f_2)^6 \delta_2(f_2)^8, \quad n_2 = \deg(f_2). \quad (37)$$

Now for  $g(x) = \prod_{i=1}^d (x - \beta_i) \in \mathbb{K}[x]$  and  $h(x) = \prod_{j=1}^e (x - \gamma_j) \in \mathbb{K}[x]$  we define

$$\begin{aligned} \chi_{0,1}(g, h) &\stackrel{\text{def}}{=} \text{res}(\underbrace{\text{res}(g(u), g^{[2i]}(u+x), u) / g(x), h, x)}_{=\prod_{i \neq j} (x - (2\beta_i - \beta_j))}) \\ &= \prod_{1 \leq i \neq j \leq d, 1 \leq k \leq e} (2\beta_i - \beta_j - \gamma_k), \end{aligned} \quad (38)$$

where  $g^{[2i]}$  is (17) for  $f = g$  and  $\lambda = 2$ ,

$$\begin{aligned} \chi_{0,2}(g, h) &\stackrel{\text{def}}{=} \text{res}(g^{[2i]}(x), h^{[i<j]}(x), x) \\ &= \prod_{1 \leq i \leq d, 1 \leq j < k \leq e} (2\beta_i - \gamma_j - \gamma_k), \end{aligned} \quad (39)$$

where  $h^{[i<j]}$  is (19) for  $f = h$ . We then have

$$\begin{aligned} \delta_2(f_1 f_2^2) &= \delta_2(f_1) \delta_2(f_2^2) \times \\ &\quad \chi_{1,1}(f_1, f_2^2) \chi_{0,2}(f_1, f_2^2) \chi_{1,1}(f_2^2, f_1) \chi_{0,2}(f_2^2, f_1). \end{aligned} \quad (40)$$

Similarly, one may compute over fields of characteristic  $\neq 2$  and  $\neq 3$  the constant coefficient of (35),

$$\begin{aligned} \widetilde{\delta}_3(f, x) &\stackrel{\text{def}}{=} \prod_{\substack{1 \leq i < j < k \leq n \\ 1 \leq \ell \leq n, \ell \neq i, \ell \neq j, \ell \neq k}} (3\alpha_\ell - (\alpha_i + \alpha_j + \alpha_k)) \\ &= \frac{\text{res}(f^{[3i]}(x), f^{[i<j<k]}(x), x)}{\delta_2(f)}, \end{aligned} \quad (41)$$

provided that  $\delta_2(f) \neq 0$  ( $f^{[i<j<k]}$  is defined in (34)). If  $\delta_2(f) = 0$  for an already squarefree polynomial  $f$ , one computes a further refined factorization of  $f$  by

$$\begin{aligned} f^{[2i; \text{gcd}; i < j]}(x) &\stackrel{\text{def}}{=} \text{GCD}(f^{[2i]}(x), f^{[i < j]}(x)) \\ &= \prod_{1 \leq i \leq n, \exists j, k, j \neq k: 2\alpha_i = \alpha_j + \alpha_k} (x - 2\alpha_i), \end{aligned} \quad (42)$$

where  $f^{[i < j]}$  is computed in (19) (the characteristic of  $\mathbb{K}$  is  $\neq 2$ ). Then  $2^{-d} f^{[2i; \text{gcd}; i < j]}(2x)$  ( $d = \deg(f^{[2i; \text{gcd}; i < j]})$ ) divides  $f(x)$ . For  $\mathbb{K} = \mathbb{C}$  the division is non-trivial because not all roots of the squarefree  $f$  can be midpoints of roots in the complex plane. For fields of characteristic  $p \geq 5$ , the GCD in (42) can be  $= f^{[2i]}(x)$ , for example for  $f(x) = x^{p-1} - 1$ . Then no refinement of the squarefree factorization is possible, and (35) is used.

Because of an additional symmetry (11) the above approach does

not seem to yield an algorithm for the third discriminant (8) directly. A difficulty is that the factorization  $G(x^2) = F(x)F(-x)$  is not unique, unlike the monic squareroot of  $G(x) = F(x)^2$ : for instance,  $(x^2 + 3x + 2)(x^2 - 3x + 2) = (x^2 + x - 2)(x^2 - x - 2)$ . We now show how to compute, by using a symbolic homotopy, the third discriminant  $\delta_3(f)$ , which is defined as

$$\delta_3(f) = \prod_{1 \leq i < j < k < \ell \leq n} \left( (\alpha_i + \alpha_j - \alpha_k - \alpha_\ell)(\alpha_i - \alpha_j + \alpha_k - \alpha_\ell) \times (\alpha_i - \alpha_j - \alpha_k + \alpha_\ell) \right) \in \mathbb{K}. \quad (43)$$

We construct the symbolic homotopical polynomial (cf. [3])

$$f_{\text{hom}}(x) = t f(x) + (1-t) f_{\text{known}}(x) \in \mathbb{K}[t][x], \quad (44)$$

where

$$f_{\text{known}}(x) = (x - r_1) \cdots (x - r_n) \in \mathbb{K}[x] \quad (45)$$

is computed for such values of the roots  $r_i \in \mathbb{K}$  that we have

$$\delta_1(f_{\text{known}}) \delta_3(f_{\text{known}}) \neq 0. \quad (46)$$

Since  $r_n$  as a variable in (46) has degree  $n - 1 + 3 \binom{n-1}{3}$ , this is always possible if the cardinality of  $\mathbb{K}$  is  $\geq n + 3 \binom{n-1}{3}$ . For smaller finite fields we can algebraically extend  $\mathbb{K}$  to sufficiently large cardinality.

One computes  $\delta_3(f_{\text{hom}})^2 \in \mathbb{K}[t]$  as follows (writing  $f_{\text{hom}}(x) = \prod_i (x - \alpha_i^h)$ ):

$$\begin{aligned} d^{[i < j, -k < \ell]}(t) &\stackrel{\text{def}}{=} \delta_1(f_{\text{hom}}^{[i < j]}(x), x) \\ &= \prod_{\substack{1 \leq i < j \leq n \\ 1 \leq k < \ell \leq n}} (\alpha_i^h + \alpha_j^h - \alpha_k^h - \alpha_\ell^h) \in \mathbb{K}[t], \end{aligned} \quad (47)$$

where  $f_{\text{hom}}^{[i < j]}$  is (19) for  $f = f_{\text{hom}}$ ,

$$\begin{aligned} d^{[\text{sqd}]}(t) &\stackrel{\text{def}}{=} (-1)^3 \binom{n}{4} \frac{d^{[i < j, -k < \ell]}(t)}{\delta_1(f_{\text{hom}})^{n-2}} \\ &= \prod_{\substack{1 \leq i < j \leq n, 1 \leq k < \ell \leq n \\ i < k, j \neq k, j \neq \ell}} (\alpha_i^h + \alpha_j^h - \alpha_k^h - \alpha_\ell^h)^2 \\ &= \delta_3(f_{\text{hom}})^2 \in \mathbb{K}[t]. \end{aligned} \quad (48)$$

The division in (48) is by a non-zero polynomial because  $\delta_1(f_{\text{hom}})$  evaluates at  $t = 0$  to  $\delta_1(f_{\text{known}})$ , which by (46) is  $\neq 0$ . The exponent  $n - 2$  in (48) arises because for each  $(\alpha_r^h - \alpha_s^h)(\alpha_s^h - \alpha_r^h)$  in  $\delta_1(f_{\text{hom}})$  there are  $n - 2$  indices for the  $\alpha_q^h$  which has cancelled by virtue of  $q = i = k$  or  $q = i = \ell$  or  $q = j = k$  or  $q = j = \ell$  in (47). For  $3 \binom{n}{4}$  of the linear factors in  $d^{[i < j, -k < \ell]}(t) / \delta_1(f_{\text{hom}})^{n-2}$  we have  $k < i$ .

We first prove that if  $d^{[\text{sqd}]}$  is a constant polynomial  $\in \mathbb{K}$ , then  $\delta_3(f) = \delta_3(f_{\text{known}})$ , which has been computed while choosing the  $r_i$ . Suppose  $\delta_3(f) \neq \delta_3(f_{\text{known}})$ . The polynomial  $\delta_3(f_{\text{hom}}) \in \mathbb{K}[t]$  then cannot be a constant polynomial because for  $t = 0$  and  $t = 1$  it evaluates to different values. Therefore its square,  $d^{[\text{sqd}]}$ , is not constant. Note that  $d^{[\text{sqd}]}$  may be constant even if the coefficients of  $f_{\text{hom}}$  depend on  $t$ .

In case  $d^{[\text{sqd}]}(t)$  has degree  $\geq 2$  in  $t$  (it is the square of a non-constant polynomial) we compute the monic squareroot polynomial of its monic associate,  $h(t)^2 = \frac{1}{c} d^{[\text{sqd}]}(t)$ , where  $c$  is the leading coefficient of  $d^{[\text{sqd}]}(t)$  in  $t$ . Note that  $\Delta_3$  (8) is defined for fields  $\mathbb{K}$  of characteristic  $\neq 2$ . Because  $d^{[\text{sqd}]}(0) = \delta_3(f_{\text{known}})^2 \neq 0$  by (46) we must have  $h(0) \neq 0$ . Then the homotopy (44) yields

$$\delta_3(f_{\text{hom}}) = \delta_3(f_{\text{known}})/h(0)h(t) \text{ and } \delta_3(f) = \delta_3(f_{\text{known}})h(1)/h(0).$$

#### 4 THIRD DISCRIMINANTS FOR DEGREES $N = 4$ AND $N = 5$

The third discriminant for  $n = 4$  in coefficients is  $D_3(z_0, \dots, z_3) = -z_3^3 + 4z_3z_2 - 8z_1$ , which does not depend on  $z_0$ , because the product (8) has 3 linear factors and therefore does not contain the constant coefficient  $a_0 = y_1 \cdots y_4$  of  $F(x)$  in (1).

The third discriminant for  $n = 5$  in coefficients is shown in Figure 2, which can be copied-and-pasted into a worksheet, for instance, into Maple. Note that  $D_5$  could still be computed from the

Figure 2:  $D_3$  for  $n = 5$ .

$$\begin{aligned} D_3(z_0, \dots, z_4) = & -z_4^9 z_3^3 + 4z_4^{10} z_3^2 z_2 - 8z_4^{11} z_1 \\ & + 12z_4^{17} z_3^4 - 49z_4^{18} z_3^2 z_2 - 4z_4^{19} z_3^2 z_2^2 \\ & + 108z_4^{19} z_3^3 z_1 + 8z_4^{20} z_0 \\ & - 48z_4^{25} z_3^5 + 180z_4^{26} z_3^3 z_2 + 141z_4^{27} z_3^2 z_2^2 \\ & - 523z_4^{27} z_3^2 z_1 - 192z_4^{28} z_3 z_2 z_1 - 100z_4^{28} z_3^3 z_0 \\ & + 64z_4^{33} z_3^6 - 112z_4^{34} z_3^4 z_2 - 952z_4^{35} z_3^2 z_2^2 \\ & - 91z_4^{36} z_3^2 z_1^3 + 1052z_4^{35} z_3^3 z_1 \\ & + 1750z_4^{36} z_3^3 z_2 z_1 + 124z_4^{37} z_3 z_1^2 \\ & + 431z_4^{36} z_3^2 z_2^2 z_0 + 184z_4^{37} z_3 z_2 z_0 \\ & - 320z_4^{42} z_3^5 z_2 + 1680z_4^{43} z_3^3 z_2^2 \\ & + 1448z_4^{44} z_3^3 z_2^3 - 720z_4^{43} z_3^2 z_1^4 z_0 \\ & - 4696z_4^{44} z_3^2 z_2 z_1 - 1531z_4^{45} z_3^2 z_2^2 z_1 \\ & - 1051z_4^{45} z_3^3 z_1^2 - 692z_4^{44} z_3^3 z_3 z_0 \\ & - 1542z_4^{45} z_3^3 z_2 z_0 - 136z_4^{46} z_3 z_1 z_0 \\ & + 512z_4^{43} z_3^4 z_2^2 - 4400z_4^{42} z_3^2 z_2^3 \\ & - 688z_4^{43} z_3^2 z_4 + 64z_4^{43} z_3^5 z_1 + 3104z_4^{42} z_3^3 z_2 z_1 \\ & + 7248z_4^{43} z_3^3 z_2^2 z_1 + 2420z_4^{43} z_3^2 z_1^2 z_0 \\ & + 1967z_4^{44} z_3 z_2 z_1^2 + 208z_4^{42} z_3^4 z_0 \\ & + 3504z_4^{43} z_3^2 z_2 z_0 + 1415z_4^{44} z_3 z_2^2 z_0 \\ & + 1014z_4^{44} z_3 z_1 z_0 + 12z_4^{45} z_0^2 \\ & - 256z_3^3 z_2^3 + 4608z_4^{43} z_3^3 z_2^4 - 128z_3^4 z_2^2 z_1 \\ & - 4112z_4^{43} z_3^2 z_2^2 z_1 - 4056z_4^{42} z_3^2 z_3 z_1 \\ & - 800z_4^{43} z_3^3 z_1^2 - 8340z_4^{42} z_3^2 z_2 z_1^2 \\ & - 625z_4^{43} z_3^3 z_1^3 + 64z_3^5 z_0 - 1120z_4^{43} z_3^3 z_2 z_0 \\ & - 5960z_4^{42} z_3^2 z_2^2 z_0 - 1680z_4^{42} z_3^2 z_1 z_0 \\ & - 2230z_4^{43} z_3 z_2 z_1 z_0 - 75z_4^{43} z_3^3 z_0^2 \\ & - 1728z_2^5 + 1440z_3 z_2^3 z_1 + 1600z_3^2 z_2 z_1^2 \\ & + 7800z_4 z_2^2 z_1^2 + 2500z_4 z_3 z_1^3 \\ & + 1200z_3^2 z_2^2 z_0 + 3600z_4 z_2^3 z_0 - 800z_3^3 z_1 z_0 \\ & + 8800z_4 z_3 z_2 z_1 z_0 - 625z_4^2 z_1^2 z_0 \\ & + 375z_4^2 z_2 z_0^2 \\ & - 5000z_2 z_1^3 - 9000z_2^2 z_1 z_0 + 2500z_3 z_1^2 z_0 \\ & - 1875z_4 z_1 z_0^2 \\ & + 3125z_0^3; \end{aligned}$$

expansion (8) with the standard algorithm for computing symmetric representations. We have computed the polynomial by interpolating the third discriminants for values for the  $z_i$ 's. The square of the third discriminant  $d^{\text{[sqd]}}(t)$  (48) of the  $f_{\text{hom}}$  for each of the 8064 polynomials with scalar coefficients was also computed by interpolating  $t$  at values in  $K$  at which the discriminant of the evaluated

$f_{\text{hom}}$  is  $\neq 0$ . In such a way, the entire computation would be highly parallelizable. We used  $f_{\text{known}}(x) = (x - 11)(x - 7)x(x + 1)(x + 3)$  with  $\delta_3(f_{\text{known}}) = 9608341743000$ .

#### ACKNOWLEDGMENTS

The subject of the paper was brought to the author's attention during the *Working Seminar on Algorithmic Intelligence* at the Suzhou Institute of Beihang University, which was organized by Dongming Wang on June 16, 2018. The author thanks Dongming Wang and Jing Yang for their comments on the work. Jing Yang has demonstrated the computation of  $D_3$  for 5 roots (see Section 4) via a Gröbner basis and has introduced the author to Orlando's Formula (5) at their meeting at Beihang University in Beijing in May 2019.

This research was supported by the National Science Foundation under Grant CCF-1717100.

#### REFERENCES

- [1] David Casperson and John McKay. 1994. Symmetric Functions, m-Sets, and Galois Groups. *Math. Comp.* 63, 208 (1994), 749–757. <http://www.jstor.org/stable/2153295>.
- [2] Olga Holtz and Mikhail Tyaglov. 2011. Structured matrices, continued fractions, and root localization of polynomials. *CoRR* 0912.4703 (March 2011). <https://arxiv.org/abs/0912.4703>.
- [3] E. Kaltofen and B. Trager. 1990. Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *J. Symbolic Comput.* 9, 3 (1990), 301–320. URL: <http://users.cs.duke.edu/~elk27/bibliography/90/KaTr90.pdf>.
- [4] Luciano Orlando. 1911. Sul problema di Hurwitz relativo alle parti reali delle radici di un'equazione algebrica. *Math. Ann.* 71 (1911), 233–245.
- [5] Dongming Wang and Jing Yang. 2016. The Second Discriminant of a Univariate Polynomial. *CoRR* abs/1609.00840 (Sept. 2016). <https://arxiv.org/abs/1609.00840>.
- [6] Dongming Wang and Jing Yang. 2019. The Second Discriminant of a Univariate Polynomial. *Science China Mathematics* (2019). Published Dec. 23, 2019; <https://doi.org/10.1007/s11425-018-1594-2>.

#### A APPENDIX: COMPUTING POLYNOMIAL ROOTS

We briefly describe how the polynomial  $\lambda$ -th root of a monic polynomial can be computed. Let  $g(x) = \hat{g}(x)x^{\lambda m} \in K[x]$  where  $\hat{g} = \hat{h}^\lambda$  is monic with  $\hat{h} \in K[x]$  monic and  $\hat{g}(0) \neq 0$ . One computes for  $d = \deg(\hat{h})$  the reverse polynomial  $h(x) = x^d \hat{h}(1/x)$  with  $h(0) = 1$  from the reverse  $\hat{g}_{\text{rev}}(x) = x^{\lambda d} \hat{g}(1/x)$  with  $\hat{g}_{\text{rev}}(0) = 1$ . The power series expansion of  $h(x)$  can be computed by quadratically convergent Newton iteration: Suppose  $h^{[i]} = (h \bmod x^{2^i})$  with  $h^{[0]} = 1$ . We obtain  $h^{[i+1]}(x) = h^{[i]}(x) + x^{2^i} \tilde{h}^{[i]}(x)$  from

$$h^{[i]}(x)^\lambda + \lambda h^{[i]}(x)^{\lambda-1} x^{2^i} \tilde{h}^{[i]}(x) \equiv \hat{g}_{\text{rev}}(x) \pmod{x^{2^{i+1}}}, \quad (49)$$

that is

$$\begin{aligned} \tilde{h}^{[i]}(x) = & \left( \frac{1}{\lambda} (h^{[i]}(x)^{-1})^{\lambda-1} \hat{g}_{\text{err}}^{[i]}(x) \bmod x^{2^i} \right) \\ \text{where } x^{2^i} \hat{g}_{\text{err}}^{[i]}(x) \stackrel{\text{def}}{=} & \hat{g}_{\text{rev}}(x) - h^{[i]}(x)^\lambda \pmod{x^{2^{i+1}}}. \quad (50) \end{aligned}$$

The power series expansion of  $h^{[i]}(x)^{-1}$  can again be computed by Newton iteration. As  $\lambda$ -th root, we have  $g(x) = (x^{d+m} h(1/x))^\lambda$ . Note that for a monic polynomial  $g \in D[x]$ , where  $D$  is a unique factorization domain of characteristic 0, the division by  $\lambda$  in (50) is exact and the root polynomial  $x^{d+m} h(1/x) \in D[x]$ .

## B APPENDIX: NOTATION

Notation (in alphabetic order):	
$a_i \in \mathbb{K}[y_1, \dots, y_n]$	$x^n + a_{n-1}x^{n-1} + \dots + a_0 \stackrel{\text{def}}{=} (x-y_1) \cdots (x-y_n)$
$D_1$	the discriminant = $D_{1,(1,-1),S_2}$ in coefficient variables (cf. (2)).
$D_2$	the second discriminant (in coefficient variables) = $D_{2,(2,-1,-1),P_2}$ with $P_2 = \{\text{id}, \binom{1,2,3}{2,1,3}, \binom{1,2,3}{2,3,1}\} \subset S_3$ (cf. (6)).
$D_3$	the third discriminant (in coefficient variables) = $D_{3,(1,1,-1,-1),P_3}$ with $P_3 = \{\text{id}, \binom{1,2,3,4}{1,3,2,4}, \binom{1,2,3,4}{1,4,2,3}\} \subset S_4$ (cf. (8)).
$D_{\nu-1,(w_1,\dots,w_\nu),P}$	the $(\nu-1)$ -st discriminant with root weights $w_i \in \mathbb{K}, 1 \leq i \leq \nu$ and permutation set $P$ (cf. (9)).
$\delta_\nu(f, x)$	the $\nu$ -th discriminants of a univariate polynomial $f$ in the variable $x$ .
$\Delta_\nu$	the $\nu$ -th discriminants in root variables

Notation continued (in alphabetic order):	
$\widehat{\Delta}_\nu$	the $\nu$ -th Orlando polynomial (12) in the roots.
$\widehat{D}_\nu$	the $\nu$ -th Orlando polynomials in the coefficients
$\widehat{\delta}_\nu(f, x)$	the $\nu$ -th Orlando polynomial of a univariate polynomial $f$ in the variable $x$ .
$\widetilde{\delta}_3(f, x)$	$\stackrel{\text{def}}{=} \prod_{\substack{1 \leq i < j < k \leq n \\ 1 \leq \ell \leq n, \ell \neq i, \ell \neq j, \ell \neq k}} (3\alpha_\ell - (\alpha_i + \alpha_j + \alpha_k))$ for $f(x) = \prod_{i=1}^n (x - \alpha_i)$ (see (41)).
$f_{\text{Orl}}(x)$	$\stackrel{\text{def}}{=} \prod_{1 \leq i < j < k \leq n} (x + \alpha_i + \alpha_j + \alpha_k)$ for $f(x) = \prod_{i=1}^n (x - \alpha_i)$ .
$f_{\text{sec-discr}}(x)$	$\stackrel{\text{def}}{=} \prod_{\substack{1 \leq j < k \leq n \\ 1 \leq i \leq n, i \neq j, i \neq k}} (x + 2\alpha_i - \alpha_j - \alpha_k)$ for $f(x) = \prod_{i=1}^n (x - \alpha_i)$ . (see (33)).
$S_n$	the set of permutations of $(1, \dots, n)$ .
$y_1, \dots, y_n$	the variables denoting the roots.
$z_0, \dots, z_{n-1}$	the variables denoting the coefficients.