Algebraic combinatorics and resultant methods for polynomial system solving

Anna Karasoulou

ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Μελέτη και επίλυση πολυωνυμικών συστημάτων με χρήση αλγεβρικών και συνδυαστικών μεθόδων

Άννα Ν. Καρασούλου

ΑΘΗΝΑ

Μάιος 2017

NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

SCHOOL OF SCIENCES
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATIONS

PROGRAM OF POSTGRADUATE STUDIES

PhD THESIS

Algebraic combinatorics and resultant methods for polynomial system solving

Anna N. Karasoulou

ATHENS

May 2017

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Μελέτη και επίλυση πολυωνυμικών συστημάτων με χρήση αλγεβρικών και συνδυαστικών μεθόδων

Άννα Ν. Καρασούλου

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Ιωάννης Ζ. Εμίρης, Καθηγητής ΕΚΠΑ

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:

Ιωάννης Ζ. Εμίρης, Καθηγητής ΕΚΠΑ

Ευάγγελος Ράπτης, Καθηγητής ΕΚΠΑ

Bernard Mourrain, Διευθυντή ερευνών Ινστιτούτο INRIA Sophia Antipolis - Méditerranée

ΕΠΤΑΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Ιωάννης Ζ. Εμίρης,
Καθηγητής ΕΚΠΑ

Ευάγγελος Ράπτης,
Καθηγητής ΕΚΠΑ

Bernard Mourrain,
Διευθυντή ερευνών Ινστιτούτο INRIA Sophia Antipolis - Méditerranée

Βασίλειος Ζησιμόπουλος,
Καθηγητής ΕΚΠΑ

Νικόλαος Μισυρλής,

Καθηγητής ΕΚΠΑ

Μιχαήλ Ν. Βραχάτης,
Καθηγητής Πανεπιστήμιο Πατρών

Ilias S. Kotsireas,
Καθηγητής Πανεπιστημίο Wilfrid Laurier

Ημερομηνία Εξέτασης: 31 Μαΐου 2017

PhD THESIS

Algebraic combinatorics and resultant methods for polynomial system solving

Anna N. Karasoulou

SUPERVISOR: Ioannis Z. Emiris, Professor NKUA

THREE-MEMBER ADVISORY COMMITTEE:

Ioannis Z. Emiris, Professor NKUA

Evangelos Raptis, Professor NKUA

Bernard Mourrain, Director of Research INRIA Sophia Antipolis - Méditerranée

SEVEN-MEMBER EXAMINATION COMMITTEE

Ioannis Z. Emiris,
Professor NKUA

Evangelos Raptis,
Professor NKUA

Bernard Mourrain,
Director of Research INRIA Sophia Antipolis - Méditerranée

Vassilis Zissimopoulos,
Professor NKUA

Nikolaos Missirlis,

Professor NKUA

Michael N. Vrahatis,
Professor University of Patras

Ilias S. Kotsireas,
Professor Wilfrid Laurier University

Examination Date: May 31, 2017

ΠΕΡΙΛΗΨΗ

Η διδακτορική διατριβή της Άννας Καρασούλου επικεντρώνεται στην επίλυση πολυωνυμικών συστημάτων χρησιμοποιώντας εργαλεία από την αλγεβρική και την συνδυαστική γεωμετρία. Η χρήση συνδυαστικών μεθόδων κατέστη απαραίτητη για την εκμετάλλευση της δομής και της αραιότητας των πολυωνυμικών εξισώσεων. Περιγράφονται επίσης γεωμετρικοί αλγορίθμοι για την διάσπαση πολυτόπων κατά Minkowski, με απώτερη εφαρμογή την παραγοντοποίηση των αντίστοιχων πολυωνύμων στο πλαίσιο της εκμετάλλευσης της αραιότητάς τους. Η κ. Άννα Καρασούλου αντιμετώπισε με επιτυχία ορισμένα μη τετριμμένα προβλήματα, τα οποία επιγραμματικά αναφέρουμε εδώ και τα αναλύουμε στην συνέχεια.

Το πρώτο πρόβλημα είναι ο υπολογισμός τύπου της αραιής απαλοίφουσας (sparse resultant) και της αραιής διακρίνουσας (sparse discriminant) [14], [29], [39], με χρήση της δομής των εξισώσεων. Επιπλέον μελετήθηκε και βρέθηκε κλειστός τύπος για τον βαθμό της διακρίνουσας και της απαλοίφουσας πολυωνυμικών εξισώσεων καθώς και η μεταξύ τους σχέση.

Ειδικότερα, διενεργήθηκε μελέτη τύπων για τον βαθμό της αραιής (μεικτής) διακρίνουσας και της αραιής απαλοίφουσας πολυωνυμικών εξισώσεων. Ο σκοπός της μελέτης αυτής είναι να διερευνηθεί ο τρόπος υπολογισμού της αραιής διακρίνουσας ενός καλώς ορισμένου συστήματος μέσω ενός τύπου που την συνδέει με την αραιή απαλοίφουσα ενός υπερπροσδιορισμένου πολυωνυμικού συστήματος, εξετάζοντας τα αραιά πολυώνυμα μέσω της θεωρίας των πολυτόπων του Νεύτωνα. Στα πλαίσια της μελέτης αυτής προέκυψαν δύο ερευνητικές εργασίες [39], [29], οι οποίες περιγράφονται αναλυτικά στα κεφάλαια 4 και 6. Στο κεφάλαιο 4 μελετάται η σχέση της αραιής διακρίνουσας και της απαλοίφουσας με έμφαση στις εφαρμογές της διακρίνουσας. Μελετάται η σχέση της αραιής διακρίνουσας με την αραιή απαλοίφουσα του συστήματος των πολυωνύμων επαυξημένου με τον Τορικό Ιακωβιανό πίνακα του συστήματος. Η σχέση αυτή οδηγεί σε έναν τύπο για την αραιή διακρίνουσα, ο οποίος επιτρέπει τον υπολογισμό της αποτελεσματικά, χωρίς την εισαγωγή νέων μεταβλητών, όπως γίνεται με τη μέθοδο του Cayley. Δίνεται επίσης μία απόδειξη για τον συνολικό βαθμό της αραιής διακρίνουσας 2 πολυωνύμων, καθώς και ένας τύπος για την αραιή διακρίνουσα όταν ένα εκ των πολυωνύμων παραγοντοποιείται, χρησιμοποιώντας τα πολύτοπα του Νεύτωνα.

Στο κεφάλαιο 5 περιγράφεται η μελέτη που διενεργήθηκε , πάνω στην διακρίνουσα των ομογενών συμμετρικών πολυωνύμων, δηλαδή των αναλλοίωτων συστημάτων κάτω από την δράση της συμμετρικής ομάδας. Αναζητήθηκε και βρέθηκε κλειστός τύπος για τον υπολογισμό της απαλοίφουσας και της διακρίνουσας τέτοιου συστήματος.

Το δεύτερο πρόβλημα το οποίο αντιμετώπισε είναι το NP-δύσκολο πρόβλημα του υπολογισμού της διάσπασης πολυτόπων κατά Minkowski με χρήση προσεγγιστικών [41] και αλγορίθμων ακριβείας [36], καθώς και η μελέτη του προβλήματος του αθροίσματος υποσυνόλων (subset sum) σε αυθαίρετη διάσταση [41].

Στο κεφάλαιο 7 μελετάται και προτείνεται αλγόριθμος για τον υπολογισμό όλων των μη τετριμμένων, ανάγωγων διασπάσεων κατά Minkowski, ενός οποιουδήποτε κυρτού πολυτόπου διάστασης d, το οποίο έχει κορυφές με ακέραιες συντεταγμένες. Για τον υπολογισμό αυτό μελετήθηκε ο κώνος όλων των συνδυαστικά ισοδύναμων πολυτόπων. Η υλοποίηση δίνεται σε Sage.

Στο κεφάλαιο 8 μελετώνται δύο NP-δύσκολα προβλήματα: το πρόβλημα της διάσπασης κατά Minkowski των ακέραιων πολυτόπων στο επίπεδο και το πρόβλημα του αθροίσματος υποσυνόλων (Subset sum) σε αυθαίρετη διάσταση (kD-SS). Στο πρόβλημα απόφασης δίνεται ένα σύνολο S από διανύσματα διάστασης k, ένα διάνυσμα στόχος t και πρέπει να αποφασιστεί αν υπάρχει ένα υποσύνολο του S το οποίο αθροίζει στο t. Στο αντίστοιχο πρόβλημα βελτιστοποίησης ζητείται υποσύνολο ώστε το αντίστοιχο άθροισμα να προσεγγίζει το διάνυσμα στόχο. Αποδεικνύουμε μέσω αναγωγής από το Set Cover ότι για γενική διάσταση k το αντίστοιχο πρόβλημα βελτιστοποίησης kD-SS-opt δεν είναι APX παρόλο που το κλασικό πρόβλημα $1D$-SS-opt έχει PTAS. Η προσέγγισή μας σχετίζει το kD-SS με το πρόβλημα του Closest Vector. Παρουσιάζουμε έναν $O(n^3/\epsilon^2)$ προσεγγιστικό αλγόριθμο για το $2D$-SS-opt, όπου n είναι ο πληθάριθμος του S και $\epsilon > 0$ φράσσει το αθροιστικό σφάλμα και σχετίζεται με μία ιδιότητα του δοθέντος αντικειμένου από τον χρήστη. Μετά από μία αναγωγή από το πρόβλημα βελτιστοποίησης της διάσπασης κατά Minkowski στο $2D$-SS-opt προσεγγίζουμε το εξής: Δοθέντος ενός πολυγώνου Q και μίας παραμέτρου $\epsilon > 0$, υπολογίζουμε τα δύο πολύτοπα της διάσπασης και , όπου $Q' = A + B$ είναι τέτοιο ώστε το Q και το Q' διαφέρουν κατά $O(\epsilon D)$, όπου D η διάμετρος του Q, ή η Hausdorff απόσταση του Q από το Q' είναι $O(\epsilon D)$. Η υλοποίηση διατίθεται στο Github.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Αλγεβρικοί Αλγόριθμοι, Υπολογιστική Γεωμετρία και Αλγεβρική Συνδυαστική

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Διακρίνουσα, Απαλοίφουσα, Διάσπαση, Πολύτοπα, Πολυδιάστατο Πρόβλημα Αθροίσματος Υποσυνόλων, Προσεγγιστικοί Αλγόριθμοι

ABSTRACT

The contribution of the thesis is threefold. We worked on Problems in the areas of algebraic algorithms, computational geometry and algebraic combinatorics. The first Problem is computing the discriminant, when the system's dimension varies. Thus solving polynomial equations and systems by exploiting the structure and sparseness of them have been studied. Specifically, closed formulas for the degree of the sparse (mixed) discriminant and the sparse resultant of polynomial equations have been studied, as well as relationships between them. Closed formulas when one of the polynomials factors in the context of the theory of sparse elimination using the Newton polytope have been proposed. The main purpose is to facilitate the computation of the sparse (or mixed) discriminant of a well-constrained polynomial system and to generalize the formula that connects the mixed discriminant with the sparse resultant. The results of this work are presented in Chapter 4 and 6 of the thesis and have been published in [39] and [29] . In Chapter 5 we are given a system of $n \geqslant 2$ homogeneous polynomials in n variables which is equivariant with respect to the symmetric group of n symbols. We then prove that its resultant can be decomposed into a product of several resultants that are given in terms of some divided differences. As an application, we obtain a decomposition formula for the discriminant of a multivariate homogeneous symmetric polynomial. The results of this work have been published in [14].

The second Problem is computing the Minkowski decomposition of a polytope and the third one was the problem of Multidimensional Subset Sum (kD-SS) in arbitrary dimension.

Firstly, we present an algorithm for computing all Minkowski Decompositions (MinkDecomp) of a given convex, integral d-dimensional polytope, using the cone of combinatorially equivalent polytopes. An implementation is given in sage. The results of this work are presented in Chapter 7 of the thesis and have been published in [36] .

Secondly, we consider the approximation of two NP-hard problems: Minkowski Decomposition (MinkDecomp) of lattice polygons in the plane and the closely related problem of Multidimensional Subset Sum (kD-SS) in arbitrary dimension. In kD-SS, a multiset S of k-dimensional vectors is given, along with a target vector t, and one must decide whether there exists a subset of S that sums up to t. We prove, through a gap-preserving reduction from Set Cover that, for general dimension k, the corresponding optimization problem kD-SS-opt is not in APX, although the classic $1D$-SS-opt has a PTAS. Our approach relates kD-SS with the well studied Closest Vector Problem. On the positive side, we present a $O(n^3/\epsilon^2)$ approximation algorithm for $2D$-SS-opt, where n is the cardinality of the multiset and $\epsilon > 0$ bounds the additive error in terms of some property of the input. We state two variations of this algorithm, which are more suitable for implementation. Employing a reduction of the optimization version of MinkDecomp to $2D$-SS-opt we approximate the former: For an input polygon Q and parameter $\epsilon > 0$, we compute summand polygons A and B, where $Q' = A + B$ is such that some geometric function differs on Q and Q' by

$O(\epsilon D)$, where D is the diameter of Q, or the Hausdorff distance between Q and Q' is also in $O(\epsilon D)$. We conclude with experimental results based on our implementations. The results of this work are presented in Chapter 8 of the thesis and have been published in [41],[40].

Finally, in Chapter 9 we provide extensions and open problems.

SUBJECT AREA: Algebraic Algorithms, Computational Geometry and Algebraic Combinatorics

KEYWORDS: Discriminant, Resultant, Decomposition, Polytopes, Multidimensional Subset Sum, Approximation Algorithms

ΣΥΝΟΠΤΙΚΗ ΠΑΡΟΥΣΙΑΣΗ ΤΗΣ ΔΙΔΑΚΤΟΡΙΚΗΣ ΔΙΑΤΡΙΒΗΣ

Η διδακτορική διατριβή της Άννας Καρασούλου επικεντρώνεται στην επίλυση πολυωνυμικών συστημάτων χρησιμοποιώντας εργαλεία από την αλγεβρική και την συνδυαστική γεωμετρία. Η χρήση συνδυαστικών μεθόδων κατέστη απαραίτητη για την εκμετάλλευση της δομής και της αραιότητας των πολυωνυμικών εξισώσεων. Περιγράφονται επίσης γεωμετρικοί αλγορίθμοι για την διάσπαση πολυτόπων κατά Minkowski, με απώτερη εφαρμογή την παραγοντοποίηση των αντίστοιχων πολυωνύμων στο πλαίσιο της εκμετάλλευσης της αραιότητάς τους.

Το πρόβλημα του υπολογισμού της αραιής απαλοίφουσας και της αραιής διακρίνουσας:

Οι πολυωνυμικές εξισώσεις και τα αντίστοιχα συστήματά τους εμφανίζονται σε πλειάδα επιστημονικών και τεχνολογικών εφαρμογών και η επίλυσή τους αποτελεί θεμελιώδες πρόβλημα της Υπολογιστικής Άλγεβρας. Η απαλοίφουσα ενός συστήματος πολυωνυμικών εξισώσεων είναι ένα νέο πολυώνυμο στους συντελεστές του συστήματος, ο μηδενισμός του οποίου αποτελεί αναγκαία και επαρκή συνθήκη ύπαρξης ριζών. Η διακρίνουσα αποτελεί ένα θεμελιώδες εργαλείο στην εξέταση των πολυωνυμικών συστημάτων. Η σχέση της με την απαλοίφουσα είναι άρρηκτη. Για παράδειγμα, η διακρίνουσα ενός πολυωνύμου σε μία μεταβλητή αντιστοιχεί στην απαλοίφουσα του πολυωνύμου και της παραγώγου του.

Η θεωρία αραιής αλγεβρικής απαλοιφής ασχολείται με τη μελέτη της απαλοίφουσας (και της διακρίνουσας), για τη μελέτη και τον υπολογισμό των ριζών πολυωνυμικών συστημάτων σε τορικές ποικιλότητες (varieties). Αυτή η θεωρία έχει τις απαρχές της στην δουλειά των Gel'fand, Kapranov και Zelevinsky. Οι μέθοδοι που χρησιμοποιούμε εκμεταλλεύονται την στενή σχέση αλγεβρικής και συνδυαστικής γεωμετρίας, όπως αυτή εκφράζεται μέσω του πολύτοπου του Νεύτωνα ενός πολυωνύμου. Η κ. Καρασούλου μελέτησε συστήματα πολλών μεταβλητών αραιών πολυωνύμων.

Κατά το διάστημα 2011-2013 έγινε μελέτη πάνω στην επίλυση πολυωνυμικών εξισώσεων και συστημάτων με εκμετάλλευση της δομής και της αραιότητάς τους. Ειδικότερα, διενεργήθηκε μελέτη τύπων για τον βαθμό της αραιής (μεικτής) διακρίνουσας και της αραιής απαλοίφουσας πολυωνυμικών εξισώσεων. Ο σκοπός της μελέτης αυτής είναι να διερευνηθεί ο τρόπος υπολογισμού της αραιής διακρίνουσας ενός καλώς ορισμένου συστήματος μέσω ενός τύπου που συνδέει την αραιή διακρίνουσα με την αραιή απαλοίφουσα ενός υπερπροσδιορισμένου πολυωνυμικού συστήματος, εξετάζοντας τα αραιά πολυώνυμα μέσω της θεωρίας των πολυτόπων του Νεύτωνα. Στα πλαίσια της μελέτης αυτής προέκυψαν δύο ερευνητικές εργασίες. Η εργασία με τίτλο «Plane mixed discriminants and toric Jacobians» [29], παρουσιάστηκε στο συνέδριο SIAM Conference on Applied Algebraic Geometry, Colorado, USA. Στην εργασία με τίτλο «Sparse Discriminants and Applications» [39] περιγράφεται η σχέση της αραιής διακρίνουσας και της απαλοίφουσας με έμφαση στις εφαρμογές της διακρίνουσας. Μελετάται η σχέση της αραιής διακρίνουσας με την αραιή απαλοίφουσα του συστήματος των πολυωνύμων επαυξημένου με τον Τορικό Ιακωβιανό πίνακα του

συστήματος. Η σχέση αυτή οδηγεί σε έναν τύπο για την αραιή διακρίνουσα, ο οποίος επιτρέπει τον υπολογισμό της αποτελεσματικά, χωρίς την εισαγωγή νέων μεταβλητών, όπως γίνεται με τη μέθοδο του Cayley. Δίνεται επίσης μία απόδειξη για τον συνολικό βαθμό της αραιής διακρίνουσας δύο πολυωνύμων, καθώς και ένας τύπος για την αραιή διακρίνουσα όταν ένα εκ των πολυωνύμων παραγοντοποιείται, χρησιμοποιώντας τα πολύτοπα του Νεύτωνα.

Το διάστημα 2014-2016 η κ. Άννα Καρασούλου επισκέφθηκε δύο φορές το INRIA Sophia-Antipolis στην Γαλλία και διενεργήθηκε μελέτη, πάνω στην διακρίνουσα των ομογενών συμμετρικών πολυωνύμων πολλών μεταβλητών και βρέθηκε κλειστός τύπος για τον υπολογισμό της και της διάσπασής της. Επιπλέον μελετήθηκαν συστήματα n ομογενών πολυωνύμων n μεταβλητών, τα οποία είναι αναλλοίωτα κάτω από την δράση της συμμετρικής ομάδας n στοιχείων. Αναζητήθηκε και βρέθηκε κλειστός τύπος για τον υπολογισμό της απαλοίφουσας τέτοιου συστήματος. Αποδείχθηκε ότι η απαλοίφουσα μπορεί να διασπαστεί ως γινόμενο απαλοιφουσών, οι οποίες δίνονται σε όρους πηλίκα διαφορών. Επιπλέον βρέθηκε συνδυαστικός τύπος για τον ακριβή υπολογισμό των πολλαπλοτήτων των παραγόντων που εμφανίζονται στην διάσπαση. Μία πρώτη έκδοση της εργασίας αυτής παρουσιάστηκε στο συνέδριο Applications of Real Algebraic Geometry (ARAG), Aalto University, Finland. Στην συνέχεια δημοσιεύτηκε η ερευνητική εργασία με τίτλο «Resultant of an equivariant polynomial system with respect to the symmetric group» [14], η οποία παρουσιάστηκε επίσης στο διεθνές Εργαστήριο Applications of Computer Algebra (ACA), Kalamata, Greece.

Το πρόβλημα της διάσπασης ενός κυρτού πολυγώνου με ακέραιες κορυφές και προβλήματα βελτιστοποίησης:

Δοθέντος ενός κυρτού πολυγώνου με ακέραιες κορυφές εξετάζουμε αλγορίθμους που μας επιτρέπουν να το διασπάσουμε σε δύο άλλα κυρτά πολύγωνα τέτοια ώστε το διανυσματικό άθροισμά τους, ή άθροισμα Minkowski, να ισούται με το αρχικό πολύγωνο. Υπό το πρίσμα της αλγεβρικής γεωμετρίας τα (κυρτά) πολύτοπα χαρακτηρίζουν με μεγαλύτερη ακρίβεια ένα πολυώνυμο από ό,τι ο συνολικός του βαθμός. Για το λόγο αυτό αποτελούν ένα θεμελιώδες αντικείμενο μελέτης στην θεωρία αραιής αλγεβρικής απαλοιφής. Η βασική κατασκευή πολυτόπων είναι το πολύτοπο του Νεύτωνα που ορίζεται για κάθε πολυώνυμο και εκφράζει την αραιότητα του πολυωνύμου. Το πρόβλημα της διάσπασης των πολυτόπων συνδέεται με την παραγοντοποίηση του πολυτόπου του Νεύτωνα ενός πολυωνύμου, το οποίο είναι θεμελιώδες πρόβλημα στην μελέτη και των υπολογισμό των πολυωνυμικών συστημάτων με πολλές μεταβλητές.

Το διάστημα 2015-2017 πραγματοποιήθηκε μελέτη για την διάσπαση των πολυτόπων κατά Minkowski. Στα πλαίσια της μελέτης αυτής προέκυψαν οι ακόλουθες ερευνητικές εργασίες.

Δημοσιεύτηκε η ερευνητική εργασία με τίτλο «Approximate subset sum and Minkowski decomposition of polytopes» [41], [40]. Στην εργασία αυτήν μελετάμε δύο NP-δύσκολα προβλήματα: το πρόβλημα της διάσπασης κατά Minkowski των ακέραιων πολυτόπων στο επίπεδο και το πρόβλημα του αθροίσματος υποσυνόλων (Subset sum) σε αυθαίρετη διάσταση (kD-SS). Στο πρόβλημα απόφασης δίνεται ένα σύνολο S από διανύσματα διάστα-

σης k, ένα διάνυσμα στόχος t και πρέπει να αποφασιστεί αν υπάρχει ένα υποσύνολο του S το οποίο αθροίζει στο t. Στο αντίστοιχο πρόβλημα βελτιστο-ποίησης ζητείται υποσύνολο ώστε το αντίστοιχο άθροισμα να προσεγγίζει το διάνυσμα στόχο. Αποδεικνύουμε μέσω αναγωγής από το Set Cover ότι για γενική διάσταση k το αντίστοιχο πρόβλημα βελτιστοποίησης kD-SS-opt δεν είναι APX παρόλο που το κλασικό πρόβλημα $1D$-SS-opt έχει PTAS. Η προσέγγισή μας σχετίζει το kD-SS με το πρόβλημα του Closest Vector. Παρουσιάζουμε έναν $O(n^3/\epsilon^2)$ προσεγγιστικό αλγόριθμο για το $2D$-SS-opt, όπου n είναι ο πληθάριθμος του S και $\epsilon > 0$ φράσσει το αθροιστικό σφάλμα και σχετίζεται με μία ιδιότητα του δοθέντος αντικειμένου από τον χρήστη. Μετά από μία αναγωγή από το πρόβλημα βελτιστοποίησης της διάσπασης κατά Minkowski στο $2D$-SS-opt προσεγγίζουμε το εξής: Δοθέντος ενός πολυγώνου Q και μίας παραμέτρου $\epsilon > 0$, υπολογίζουμε τα δύο πολύτοπα της διάσπασης και , όπου $Q' = A + B$ είναι τέτοιο ώστε το Q και το Q' διαφέρουν κατά $O(\epsilon D)$, όπου D η διάμετρος του Q, ή η Hausdorff απόσταση του Q από το Q' είναι $O(\epsilon D)$. Η υλοποίηση διατίθεται στο Github.

Παράλληλα πραγματοποιήθηκε μελέτη και προτείνεται αλγόριθμος για τον υπολογισμό όλων των μη τετριμμένων, ανάγωγων διασπάσεων κατά Minkowski, ενός οποιουδήποτε κυρτού πολυτόπου διάστασης d, το οποίο έχει κορυφές με ακέραιες συντεταγμένες. Για τον υπολο-γισμό αυτό μελετήθηκε ο κώνος όλων των συνδυαστικά ισοδύναμων πολυτόπων. Η υλοποίηση δίνεται σε Sage. Η εργασία με τίτλο « On the space of Minkowski summands of a convex polytope » [36].

Γενικεύσεις και ανοιχτά προβλήματα

Από την διατριβή αυτήν προκύπτουν κάποια ανοιχτά προβλήματα τα οποία παραθέτουμε στην συνέχεια. Από την σκοπιά της Υπολογιστικής Άλγεβρας και της Συνδυαστικής ένα πρόβλημα θα ήταν η γενίκευση του κλειστού τύπου για την απαλοίφουσα ενός συστήματος n ομογενών πολυωνύμων σε n μεταβλητές τα οποία μένουν αναλλοίωτα κάτω από την δράση άλλης ομάδας συμμετρίας ή να μελετηθεί το ίδιο αποτέλεσμα, αλλά για πολλαπλά συμμετρικά πολυώνυμα. Όμοια θα μπορούσε να γενικευτεί και ο κλειστός τύπος της διακρίνουσας του κεφαλαίου 5. Επιπλέον ένα άλλο πρόβλημα θα ήταν η γενίκευση των τύπων της διακρίνουσας του κεφαλαίου 6 για οποιονδήποτε αριθμό μεταβλητών. Από την σκοπιά της Υπολογιστικής Γεωμετρίας και των Αλγεβρικών Αλγορίθμων υπάρχουν κάποια προβλήματα που προκύπτουν από τα κεφάλαια 7 και 8. Το πρώτο είναι δοθέντος ενός πίνακα $A \in \mathbb{Z}^{m\times d}$ and $b \in \mathbb{Z}^m$ τέτοιου ώστε $Ax \leqslant b$ είναι η H-αναπαράσταση του κυρτού ακεραίου πολυτόπου P_b, να οριστούν και να υπολογιστούν οι ακέραιοι προσεγγιστικοί προσθεταίοι του. Το δεύτερο πρόβλημα είναι να εφαρμόσουμε αυτές τις μεθόδους σε αλγεβρικά προβλήματα όπως η προσεγγιστική παραγοντοποίηση των πολυωνύμων ή τον έλεγχο της παραγοντοποίησης.

To my Family for their continues love and support
and especially to my husband Konstantinos Lentzos and my son Nikolaos Lentzos.

ACKNOWLEDGEMENTS

This dissertation could not have been completed without the great support that I have received from so many people over the years. I wish to offer my most heartfelt thanks. Without their cooperation I would not have been able to conduct this analysis. My sincere gratitude to my supervisor Prof. Ioannis Z. Emiris for teaching me all the aspects of research and generously offering me his advice.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

PREFACE

This dissertation is submitted for the degree of Doctor of Philosophy at the Department of Informatics and Telecommunications of National and Kapodistrian University of Athens.

The research questions were formulated by my supervisor, Prof. Ioannis Z. Emiris, who supported and inspired me in all stages during my PhD. The research was sophisticated, but conducting extensive investigation has allowed me to answer all the questions that we identified. I would like to thank him again for being my supervisor, for the trust he has shown to me from the very first day of our collaboration, helping me to pursue research on topics for which I am truly passionate and achieve those high impact results. His office door was always open and his email available anytime, even late at night or during holidays.

Fortunately, both Prof. Evangelos Raptis and Dr. Bernard Mourrain were always helping me, supporting me and encouraging me to continue to the next big step. Thank you for all of the meetings and chats over the years. I would also like to thank Dr. Bernard Mourrain for the funding of my two internships at INRIA Sophia Antipolis - Méditerranée. Many thanks to my tutors Prof. Ilias S. Kotsireas, for his enthusiasm, encouragement and advices and also Prof. Vassilis Zissimopoulos, Prof. Nikolaos Missirlis, and Prof. Michael N. Vrahatis for always being available and willing to answer my queries and guiding me through the project.

I would like to thank my co-authors and tutors Dr. Laurent Busé, Prof. Alicia Dickenstein, Prof. Ioannis Z. Emiris, Dr. Evelyne Hubert, Prof. Gregory Karagiorgos and Prof. Günter Rote, whom I consider myself fortunate to meet, and whose pieces of advise have been priceless.

I would like to thank my co-authors and friends Dr. Eleni Tzanaki, Charilaos Tzovas, Dr. Zafeirakis Zafeirakopoulos for productive collaboration.

I would like to warmly thank my colleagues from the ΕρΓΑ laboratory, Galaad and Aromath team for their enthusiasm, collaboration, encouragement It was always helpful to share ideas and knowledge about my research. Specially thanks to Evangelos Anagnostopoulos, Dr. Vissarion Fisikopoulos, Dr. Christos Konaxis, Ioannis Psarros and Dr. Elias Tsigaridas for their advices.

I would like to thank Prof. Dimitris Achlioptas, Dr. Ioannis Chamodrakas, Prof. Ioannis Z. Emiris, Prof. Aggelos Kiayias and Prof. Evangelos Raptis for their trust and tutoring me as assistant.

I would like to thank Antigoni Galanaki and Tatiana Kyrou for helping me with the paperwork.

My sincere gratitude to Prof. Evangelos Raptis, Prof. Korina Rozi and Prof. Dimitrios Varsos for their continuous support and for being my tutors from my early stages until now.

I also benefitted from my friends who kept me motivated. Many thanks to Theodosia Antonellou, Spyros Argiroiliopoulos, Kostas Athanasiou, Aimilia Basilaki, Xrisanthi Chimona, Mr. Charalampos and Ms. Mairy Christoforatos, Manousos Damorakis, Nikos Grivokostopoulos, Thalia Ioannou, Ifigeneia Makariti, Zacharias Mpikos, Baggelis Ntaloukas, Charilaos Vougioukas and their families for their continues support and love.

I would like to express my gratitude and appreciation to my big family Karasoulos, Boutidis, Kapogiannis, Xiarchopoulos, Lentzos, Bouloukos, Kalabesios, Ronald and Sara Wildford, Antoni and Basiliki Kourtikaki, Ourania Kalpaxi, Irini and Nikianna Kapogianni, Anastasios and Nikolaos Giannakopoulos, Theodoros Kapogiannis, Christina Kapogianni, Dimitrios and Eleni Karasoulos, Nikolaos and Anna Kapogianni, Panagiota and Sotiria Zoumpou, Christina Lentzou, Nikolaos and Anastasia Lentzos for being by my side and for their love.

My parents Nikolaos and Theophanie Karasoulou and my brother Dimitrios Karasoulos deserve a particular note of thanks: your wise advise and kind words have, as always, served me well. Thank you for your infinite support and love. Without you I wouldn't finish even the first classes of school, of piano Academy, of ballet Academy, of tennis Academy, of .... and most of all of becoming the person that I am today.

My love to my son Nikolaos Lentzos. Thank you for your infinite love and for making my life beautiful. Special thanks to my close family for looking after you while I was doing my research and writing this thesis and for providing funding for the early and the last years of my studies.

Finally, I seize this opportunity to express my love to my husband Konstantinos Lentzos and say a very very big thank you for bearing me in my worst, loving me, encouraging me and supporting me.

I hope you enjoy your reading.

Anna Karasoulou

Athens, May 31, 2017

1. INTRODUCTION

In this thesis we worked on problems in the areas of algebraic algorithms, computational geometry and algebraic combinatorics. The first problem is computing the discriminant of a well-constrained sparse polynomial system. The second one is computing the Minkowski decomposition (MinkDecomp) of lattice polytopes and the third one is the problem of Multidimensional Subset Sum (kD-SS) in arbitrary dimension k.

Solving polynomial equations and systems by exploiting the structure and sparseness of them have been studied. The polynomial equations and their respective systems are shown on a various scientific and technological applications . Their solution is the fundamental problem of Computational Algebra and Computational Algebraic Geometry. Specifically, closed formulas for the degree of the sparse (mixed) discriminant and the sparse resultant of polynomial equations have been studied, as well as relationships between them.

Closed formulas when one of the polynomials factors in the context of the theory of sparse elimination using the Newton polytope have been proposed. The main purpose is to facilitate the computation of the sparse (or mixed) discriminant of a well-constrained polynomial system and to generalize the formula that connects the mixed discriminant with the sparse resultant. The above led to two research papers [39] and [29] .

The paper [39] describes the sparse (or mixed) discriminant and its applications. It also relates it to the sparse resultant of an overconstrained polynomial system, considering the sparse polynomials via the theory of Newton polytopes.

Especially we present our main results relating the mixed discriminant with the sparse resultant of two bivariate Laurent polynomials with fixed support and their toric Jacobian. On our way, we deduced a general multiplicativity formula for the mixed discriminant when one polynomial factors as $f = f' \cdot f''$. This formula occurred as a consequence of our main result, Theorem 6.3.3, and generalized known formulas in the homogeneous case to the sparse setting. Furthermore, we obtained a new proof of the bidegree formula for planar mixed discriminants. This work is described in Chapter 4.

In [14] we are given a system of $n \geqslant 2$ homogeneous polynomials in n variables which is equivariant with respect to the symmetric group of n symbols. We then prove that its resultant can be decomposed into a product of several resultants that are given in terms of some divided differences. As an application, we obtain a decomposition formula for the discriminant of a multivariate homogeneous symmetric polynomial.

Discriminant is a very useful tool, but also very hard to compute. The factorization formula that we propose, in the case of symmetric polynomials, reduces the computations significantly. Taking advantage of the polynomial symmetries, the idea is that we gather together the same factors by using combinatorial exponents in the appearing resultants. This work is described in Chapter 5.

In the paper [29] the closed formula of sparse (or mixed) discriminant for Laurent poly-

nomials with fixed support is proved. The relationship between the sparse (or mixed) discriminant of two bivariate Laurent polynomials with fixed support, with the sparse resultant of these polynomials and their toric Jacobian is also given. This helps to obtain a new proof for the bidegree of the discriminant as well as to establish a multiplicativity formula of the mixed discriminant, when one of the polynomials is factorized. This work is described in Chapter 6.

In [36] we present an algorithm for computing all Minkowski Decompositions (MinkDecomp) of a given convex, integral d-dimensional polytope, using the cone of combinatorially equivalent polytopes. An implementation is given in sage. This work is described in Chapter 7.

In [41],[40] we consider the approximation of two NP-hard problems: Minkowski Decomposition (MinkDecomp) of lattice polygons in the plane and the closely related problem of Multidimensional Subset Sum (kD-SS) in arbitrary dimension k. In kD-SS, a multiset S of k-dimensional vectors is given, along with a target vector t, and one must decide whether there exists a subset of S that sums up to t. We prove, through a gap-preserving reduction from Set Cover that, for general dimension k, the corresponding optimization problem kD-SS-opt is not in APX, although the classic $1D$-SS-opt has a PTAS. Our approach relates kD-SS with the well studied Closest Vector Problem. On the positive side, we present a $O(n^3/\epsilon^2)$ approximation algorithm for $2D$-SS-opt, where n is the cardinality of the multiset and $\epsilon > 0$ bounds the additive error in terms of some property of the input. We state two variations of this algorithm, which are more suitable for implementation. Employing a reduction of the optimization version of MinkDecomp to $2D$-SS-opt we approximate the former: For an input polygon Q and parameter $\epsilon > 0$, we compute summand polygons A and B, where $Q' = A + B$ is such that some geometric function differs on Q and Q' by $O(\epsilon\, D)$, where D is the diameter of Q, or the Hausdorff distance between Q and Q' is also in $O(\epsilon\, D)$. We conclude with experimental results based on our implementations. This work is described in Chapter 8.

At the last Chapter we provide extensions and open problems.

2. BACKGROUND

In this chapter we are giving some definitions and describe some problems that we will refer to in later chapters.

2.1 Preliminaries

A formal definition of the *affine space* is given below, while Marcel Berger in [7] explains that , "An affine space is nothing more than a vector space whose origin we try to forget about, by adding translations to the linear maps".

Definition 2.1.1. An affine space is a set X that admits a free transitive action of a vector space V . That is, there is a map

$$X \times V \to X : (x, v) \to x + v,$$

called translation by the vector v, such that

1. Addition of vectors corresponds to composition of translations, i.e., for all $x \in X$ and $u, v \in V, x + (u + v) = (x + u) + v$.
2. The zero vector acts as the identity, i.e., for all $x \in X, x + 0 = x$.
3. The action is free, i.e., if for a given vector $v \in V$ exists a point $x \in X$ such that $x + v = x$ then $v = 0$.
4. The action is transitive, i.e., for all points $x, y \in X$ exists a vector $v \in V$ such that $y = x + v$.

The dimension of X is the dimension of the vector space of translations, V.

The vector v in Condition 4 that translates the point x to the point y is by Condition 3 unique, and is often written as $v = \overrightarrow{xy}$ or as $v = y - x$. We have in fact a unique map

$$X \times X \to V : (x, y) \to y - x$$

such that $y = x + (y - x)$ for all $x, y \in X$. It furthermore satisfies

1. For all $x, y, z \in X, z - x = (z - y) + (y - x)$.
2. For all $x, y \in X$ and $u, v \in V, (y + v) - (x + u) = (y - x) + v - u$.
3. For all $x \in X, x - x = 0$.
4. For all $x, y \in X, y - x = -(x - y)$.

Definition 2.1.2. 1. Let a, b be two points of $\mathbb{R}^n$. The set of all $x \in \mathbb{R}^n$ of the form

$$x = (1 - \lambda)a + \lambda b, \lambda \in \mathbb{R}$$

is called a line through a and b.

2. A subset M of $\mathbb{R}^n$ is called an *affine set (affine manifold)* if it contains every line through two point of it. An affine set which contains the origin is a subspace.

Proposition 2.1.3 (Prop 1.1[91])**.** *A nonempty set M is an affine set if and only if $M = a + L$, where $a \in M$ and L is a subspace.*

Definition 2.1.4. 1. The subspace L is said to be parallel to the affine set M and it is uniquely defined.

2. The dimension of the subspace L parallel to an affine set M is called the dimension of M. A point $a \in \mathbb{R}^n$ is an affine set of dimension 0, because the subspace parallel to $M = \{a\}$ is $L = \{0\}$. A line through two points a, b is an affine set of dimension 1, because the subspace parallel to it is the one-dimensional subspace $\{x = \lambda(b - a)|\lambda \in \mathbb{R}\}$. An $(n-1)-$ dimensional affine set is called a hyperplane or a plane for short.

Definition 2.1.5. Let $x_1, \ldots, x_n$ be vectors in a real vector space, and let $\lambda_1, \ldots, \lambda_n$ be non-negative scalars in $\mathbb{R}$. Then $\lambda_1 x_1 + \cdots + \lambda_n x_n$ is called a conic combination of the vectors $x_1, \ldots, x_n$. If, in addition, $\lambda_1 + \cdots + \lambda_n = 1$, then it is a convex combination of $x_1, \ldots, x_n$.

Definition 2.1.6. A polyhedron (plur: polyhedra), or polyhedral set in $\mathbb{R}^d$ is the intersection of a finite number of half-spaces.

Rather than enumerating a list of n pairs (a_i, b_i) defining single inequalities, it is usual to define a $n \times d$ matrix A which has the different a_i as its n line vectors, and a vector $b \in \mathbb{R}^n$ with the b_i, so that it is possible to write the polyhedron as: $\{x|Ax \leqslant b\}$

Definition 2.1.7. Let $S_1, ..., S_r$ be sets of vectors. We define their Minkowski sum, or vector sum, as the set of vectors which can be written as the sum of a vector of each set. Namely:

$$S_1 + \cdots + S_r := \{x_1 + \cdots + x_r | x_i \in S_i, \forall i\}.$$

The Minkowski sum is commutative and associative.

Geometrically, the Minkowski sum is the set of points covered by any translation of one set by a vector in the other one.

Theorem 2.1.8. *(Minkowski-Weyl) Any polyhedron is the Minkowski sum of a finitely generated closed cone and a finitely generated convex set, and conversely. That is, P is a polyhedron if and only if there are vectors $v_1, \ldots, v_n, r_1, \ldots, r_m$ of $\mathbb{R}^d$ such that:*

$$P = \{\lambda_1 v_1 + \cdots + \lambda_n v_n + \mu_1 r_1 + \cdots + \mu_m r_m | \lambda_1 + \cdots + \lambda_n = 1, \lambda_i, \mu_i \geqslant 0\}.$$

As we can see, polyhedra can be described either as a set of inequalities or as a set of generators. These two representations are commonly called H-representation (for half-space) and V-representation (for vertex). If the representation is minimal, the vectors v_i and r_i in the V-representation presented here are called vertices and rays. There are two natural restrictions of this theorem, by excluding either of the conical and convex combinations.

Theorem 2.1.9. *(Minkowski-Weyl for cones) Any polyhedral cone is a finitely generated closed cone, and conversely. That is, P is a polyhedral cone if and only if there are vectors* $r_1, \ldots, r_m$ *of* $\mathbb{R}^d$ *such that:*

$$P = \{\mu_1 r_1 + \cdots + \mu_m r_m | \mu_i \geqslant 0\}.$$

Let us now define our main object of study:

Definition 2.1.10. A polytope is a bounded polyhedron.

In other words a polytope is the convex hull of a finite set in $\mathbb{R}^d$. If the finite set is $A = \{m_1, \ldots, m_l\} \subset \mathbb{R}^d$, then the polytope can be expressed as

$$Conv(A) = \{\lambda_1 m_1 + \cdots + \lambda_l m_l : \lambda_i \geqslant 0, \sum_{i=1}^{l} \lambda_i = 1\}.$$

Definition 2.1.11. A lattice polytope is a set of the form $Conv(A)$, where $A \subset \mathbb{Z}^d$ is finite. That is the convex hull of a set of points with integer coordinates.

Example 2.1.12. If the set of exponent vectors of all monomials of total degree at most b is $A_b = \{m \in \mathbb{Z}^d_{\geqslant 0} : |m| \leqslant b\}$, then the convex hull of A_b is a polytope (and it is also a simplex)

$$Q_b = \{(a_1, \ldots, a_d) \in \mathbb{R}^d : a_i \geqslant 0, \sum_{i=1}^{d} a_i \leqslant d\}.$$

Definition 2.1.13. A simplex is defined to be the convex hull of $d+1$ points $m_1, \ldots, m_{n+1}$ such that $m_2 - m_1, \ldots, m_{d+1} - m_1$ are a basis of $\mathbb{R}^d$.

We will now define the faces of a polytope $P \subset \mathbb{R}^d$. Let a non zero vector $v \in \mathbb{R}^d$.

Definition 2.1.14. An affine hyperplane is defined by an equation of the form $< m, v >= -a$ (the minus sing simplifies certain formulas).

Definition 2.1.15. If $a_p(v) = -\min_{m \in P}(< m, v >)$, then we call the equation $< m, v >= -a_P(v)$ a supporting hyperplane of P and we call v an inner pointing normal.

The supporting hyperplane has the property that the *face of* P *determined by* v is equal to

$$P_v = P \cap \{m \in \mathbb{R}^d :< m, v >= -a_P(v)\} \neq \emptyset$$

and P lies in the half-space

$$P \subset \{m \in \mathbb{R}^d :< m, v >\geqslant -a_P(v)\}.$$

An other approach could be the following: Let P be a polytope and a, x be vectors of $\mathbb{R}^d$, $a \neq 0$ and b a scalar. We say (a, b) is a valid inequality for P, if the inequality $< a, x >\leqslant b$ holds for any point $x \in P$.

Definition 2.1.16. For any valid inequality of a polytope, the subset of the polytope of vectors which are tight for the inequality is called a *face* of the polytope. That is, the set F is a face of the polytope P if and only if

$$F = \{x \in P| < a, x >= b\},$$

for some valid inequality (a, b) of P . The set of faces of a polytope P is denoted by $F(P)$.

Faces of polytopes can be partially ordered by inclusion, that is, some faces are contained in the others. The partially ordered set of faces of a polytope is called its *face lattice*.

Definition 2.1.17. Let P be a polytope. The face lattice of the polytope, $L(P)$, is the set of faces $F(P)$ partially ordered by inclusion. That is, for F and G in $L(P)$, we have $F \leqslant G$ if and only if $F \subset G$. When the term face lattice is used, it generally implies we are considering the faces as abstract elements ordered by inclusion, leaving aside geometrical notions.

Definition 2.1.18. If $L(P)$ is the face lattice of a polytope, a chain S is a subset of $L(P)$ which is totally ordered, that is, for any distinct $F, G \in S$, we have either $F \subset G$ or $G \subset F$. The length of a chain is its cardinality minus one. If $\{F_1, \ldots, F_n\}$ is a chain, there is an ordering $i_1, \ldots, i_n$ such that $F_{i_1} \subset \cdots \subset F_{i_n}$.

Theorem 2.1.19. *(Face lattices) Let P be a polytope, and $L(P)$ its face lattice. Then we have the following:*

- *The face lattice $L(P)$ has a unique minimal element, which is the empty set, and a unique maximal element, which is P.*
- *The face lattice $L(P)$ is graded, which means that all maximal chains of $L(P)$ have the same length.*
- *Let F and G be two faces in $L(P)$. Then there is a unique maximal face $F \wedge G$ they both contain, and a unique minimal face $F \vee G$ containing them.*

Definition 2.1.20. Let P be a polytope, and F a face of P. The rank of F in the face lattice $L(P)$ is the length of the longest chain of $L(P)$ which has empty set and F as minimal and maximal elements respectively.

2.2 Notations

- A set $A \subset \mathbb{R}^n$ is a configuration, if it is contained in $\mathbb{Z}^n$.
- The configurations $A_1, \ldots, A_n$ are called essential, if the affine dimension of the lattice $\mathbb{Z}A_1 + \cdots + \mathbb{Z}A_k$ equals $k-1$ and for all $I \subsetneq \{1, \ldots, k\}$ the affine dimension of the lattice generated by $\{A_i : i \in I\}$ is greater or equal than $|I|$.
- Dense or full configurations are those, who consists of all the lattice points in their convex hull.

2.3 Partitions

Let us now describe throw an example how we arrive to multinomial coefficients through binomial.

- Think of the binomial $\binom{10}{4} = \frac{10!}{4!(10-4)!}$ as the number of ways to distribute 10 objects to two recipients such that one receives 4 objects and the other the remaining 6.
- Writing $\binom{10}{4,\ 6} = \frac{10!}{4!6!}$ instead of just $\binom{10}{4}$ makes explicit the number of objects each recipient receives.
- The multinomial coefficient $\binom{10}{3,\ 4,\ 3} = \frac{10!}{3!4!3!}$ counts the ways to distribute 10 objects to three recipients such that
  - the 1^{st} recipient receives 3 objects
  - the 2^{nd} recipient receives 4 objects
  - the 3^{rd} recipient receives 3 objects

In general, the multinomial coefficient is defined as

$$\binom{n}{\lambda_1,\ \lambda_2,\ \ldots,\ \lambda_k} = \frac{n!}{\lambda_1!\lambda_2!\ldots\lambda_k!}$$

and equals the number of distributions of n distinct objects to k distinct

the recipient i receives exactly λ_i objects.

Theorem 2.3.1. *Multinomial theorem*

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_k)^n = \sum_{\lambda_1+\cdots+\lambda_k=n} \binom{n}{\lambda_1,\ \ldots,\ \lambda_k} \prod_{1\leqslant j\leqslant k} \alpha_j^{\lambda_j}$$

What is a partition?

- λ is a partition of n , denoted as $\lambda \vdash n$,
  If $\lambda = (\lambda_1, \ldots, \lambda_k)$ is a weakly decreasing sequence of nonnegative integers,

  $$\lambda_1 \geqslant \cdots \geqslant \lambda_k \geqslant 0$$

  that sum up to n, i.e. $\lambda_1 + \cdots + \lambda_k = n$.
- The number of nonzero λ_i's is called the length of λ and is denoted as $l(\lambda)$.

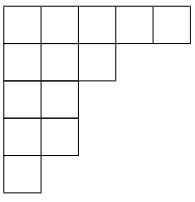
For example 4 has the following five partitions:

$$4$$
$$3+1$$
$$2+2$$
$$2+1+1$$
$$1+1+1+1$$

So $(2,1,1) \vdash 4$ and has length $l(2,1,1) = 3$.

Applying partitions on the variables $x_1, \ldots, x_n$ For any partition $\lambda = (\lambda_1, \ldots, \lambda_k) \vdash n$, where $k = l(\lambda)$,
we construct k blocks of size $\lambda_1, \ldots, \lambda_k$ in decreasing size order.

Example 2.3.2. The partition $(5,3,2,2,1) \vdash 13$ gives

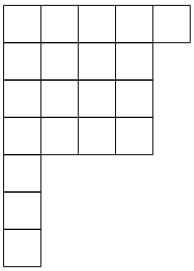


We fill in those blocks with the variables $x_1, \ldots, x_n$. The λ_i variables in the block i are identified by y_i and this gives us a ring homomorphism

$$\rho_\lambda : A[x_1, \ldots, x_n] \to A[y_1, \ldots, y_k]$$

Let us now Count partitions with certain specifications. The following is a fundamental example which leads to the definition of s_λ's How many partitions of 20 have

- one block of size 5
- three blocks of size 4
- three blocks of size 1 ?



Seems that

$$\binom{20}{1,\ 1,\ 1,\ 4,\ 4,\ 4,\ 5} = \frac{20!}{(1!)^3(4!)^3(5!)^1}$$

has something to do with the answer!

But it is too large to be the correct answer, since the recipients in $\binom{20}{1,\ 1,\ 1,\ 4,\ 4,\ 4,\ 5}$ are distinct instead of identical as we want! That is, the multinomial counts the following distributions as different:

$$\begin{aligned}
\{17\} &\to \textit{recipient } 1\\
\{3\} &\to \textit{recipient } 2\\
\{11\} &\to \textit{recipient } 3\\
\{2,5,6,10\} &\to \textit{recipient } 4\\
\{1,7,19,20\} &\to \textit{recipient } 5\\
\{9,15,16,18\} &\to \textit{recipient } 6\\
\{4,8,12,13,14\} &\to \textit{recipient } 7
\end{aligned}$$

$$\begin{aligned}
\{3\} &\to \textit{recipient } 1\\
\{17\} &\to \textit{recipient } 2\\
\{11\} &\to \textit{recipient } 3\\
\{2,5,6,10\} &\to \textit{recipient } 4\\
\{1,7,19,20\} &\to \textit{recipient } 5\\
\{9,15,16,18\} &\to \textit{recipient } 6\\
\{4,8,12,13,14\} &\to \textit{recipient } 7
\end{aligned}$$

The equivalence principle comes to the rescue:
We may arrange the assignment of

- the blocks of size 1 to the first three recipients in any of $3!$ ways
- the blocks of size 4 to the next three recipients in any of $3!$ ways
- the blocks of size 5 to the last recipient in any of $1!$ ways

and end up with an "equivalence partition".

So there are

$$\binom{20}{1,\ 1,\ 1,\ 4,\ 4,\ 4,\ 5}\Big/3!3!1!$$

partitions of 20 with blocks of the required description.

In a more formal way a *partition* is a sequence of weakly decreasing positive integers which is often written as $\lambda = (\lambda_1, \ldots, \lambda_k)$. The number k is called the *length* of λ and will be denoted by $l(\lambda)$. When $\sum_{i=1}^{k} \lambda_i = p$ we will say such a λ is a partition of p and write $\lambda \vdash p$.

Given a partition $\lambda \vdash n$, its associated *multinomial coefficient* is defined as the integer

$$\binom{n}{\lambda_1, \lambda_2, \ \ldots, \lambda_{l(\lambda)}} := \frac{n!}{\lambda_1!\lambda_2! \cdots \lambda_{l(\lambda)}!}. \tag{2.1}$$

It counts the number of distributions of n distinct objects to $l(\lambda)$ distinct recipients such that the recipient i receives exactly λ_i objects. In this counting, the objects are not ordered inside the boxes, but the boxes are ordered. To avoid the count of the permutations between the boxes having the same number of objects we have to divide (2.1) by the number of all these permutations. If s_j denotes the number of boxes having exactly j objects, $j \in [n]$, then this number of permutations is equal to $\prod_{j=1}^{n} s_j!$. Thus, for any partition $\lambda \vdash n$ we define the integer

$$m_\lambda := \frac{1}{\prod_{j=1}^{n} s_j!}\binom{n}{\lambda_1, \lambda_2, \ \ldots, \lambda_{l(\lambda)}}. \tag{2.2}$$

2.4 Symmetric polynomials

An n-variable polynomial $f(x_1, \cdots, x_n)$ is called *symmetric*, if it does not change by any permutation of its variables. The symmetric n-variable polynomials form a ring. A very common example of such polynomial is the Vandermonde determinant that we analyze below. Symmetric polynomials except for having their own interest, many times reduce a difficult polynomial problem to an easier one by studying it in a symmetric environment. This method is so often used in invariant theory, that is called *symmetrization*.

Definition 2.4.1. Symmetrization is therefore a process that converts any polynomial in n variables to a symmetric one in the same number of variables. Thus the symmetrization of a monomial $X_1^{a_1} \cdots X_n^{a_n}$ is defined as

$$S(X_1^{a_1} \cdots X_n^{a_n}) = \sum_{\sigma \in S_n} X_{\sigma(1)}^{a_1} \cdots X_{\sigma(n)}^{a_n},$$

where S_n stands for the symmetric group.

Example 2.4.2. The symmetrization of $X_1^3X_2$ in 3 variables X_1, X_2, X_3 is just

$$S(X_1^3X_2) = X_1^3X_2 + X_1^3X_3 + X_2^3X_3 + X_3^3X_1 + X_2^3X_1.$$

Symmetric polynomials are widely used in statistics through bootstrapping processes [69], in chemistry [4], in algebra [1], combinatorics [88], presentation theory of symmetric groups, general linear groups [57], and geometry [60].

For example, a distinguished family of symmetric polynomials called Schur polynomials, that are indexed by combinatorial objects called Young diagrams, describes the character theory of the symmetric group. The Schur polynomials and their generalizations such as Jack and Macdonald polynomials [68] are related to geometric objects such as symmetric spaces and flag varieties. They have also found connection with representation theory of super Lie algebras [83, 86]. Besides their connection with representation theory, symmetric functions also have an application to mathematical physics. They are applied in Boson-Femion correspondence which are applied in string theory [58] and integrable systems [76]. There is also an interesting connection to quantum physics: the Jack polynomials are the eigenstates of the Hamiltonian of the quantum n-body problem.

Monomial symmetric polynomials

The *monomial symmetric polynomial* m_a is determined by $\mathbf{X}^a = X_1^{a_1} \cdots X_n^{a_n}$ as the sum of all those obtained by symmetry from $\mathbf{X}^a$. Let us denote d its degree $a_1 + \cdots + a_n$.

Consider n-tuples $a = (a_1, a_2, \ldots, a_n)$ and define the relation " $\sim$ " between them, which expresses that one is a permutation of the other. Since $m_a = m_\beta$, when β is a permutation of a, one usually considers only those m_a for which $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n$ and add up to d; in other words the Young diagrams or partitions of d. Thus one can simply write

$$m_\alpha = \sum_{\beta \sim \alpha} \mathbf{X}^\beta$$

where b ranges over all distinct permutations of a.

Example 2.4.3. Given a partition $a = (2, 1, 1)$ we get the corresponding symmetric polynomial

$$m_{(2,1,1)}(X_1, X_2, X_3) = X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2.$$

The monomial symmetric polynomials form a basis of the infinite dimensional vector space of symmetric polynomials and as a consequence every symmetric polynomial F can be written as a linear combination of them. To this point, it suffices to separate the different types of monomials occurring in F. In particular, if F has integer coefficients, then so will the linear combination.

Power sum symmetric polynomials

For each integer $k \geqslant 0$, the monomial symmetric polynomial $m_{(k,0,\ldots,0)}(X_1,\ldots,X_n)$ is of special interest. It is called the *k-th power sum symmetric polynomial* and is denoted as $s_k(X_1,\ldots,X_n)$, so

$$s_k(X_1,\ldots,X_n) = X_1^k + X_2^k + \cdots + X_n^k$$

Any symmetric polynomial in $X_1,\ldots,X_n$ can be expressed as a polynomial expression with rational coefficients in the power sum symmetric polynomials $s_1(X_1,\ldots,X_n),\ldots,s_n(X_1,\ldots,X_n)$.

Remark 2.4.4. The ring of symmetric polynomials with coefficients in a field $\mathbb{K}$ of characteristic zero is equal to the polynomial ring $\mathbb{K}[s_1,\ldots,s_n]$.

Symmetric polynomials

Definition 2.4.5. Let $X_1,\ldots,X_n$ be indeterminates over $\mathbb{Z}$, where n is a positive integer. The monic polynomial $g \in \mathbb{Z}[X_1,\ldots,X_n][X]$ having roots $X_1,\ldots,X_n$ expands as

$$g(X) = \prod_{i=1}^{n}(X - X_i) = \sum_{j\in\mathbb{Z}}(-1)^j e_j X^{n-j}, \tag{2.3}$$

whose coefficients are, up to sign, the *elementary symmetric polynomials* of $X_1,\ldots,X_n$,

$$e_j = e_j(X_1,\ldots,X_n) = \sum_{1\leqslant i_1\leqslant\ldots\leqslant i_j\leqslant n}\prod_{k=1}^{j} X_{i_k},\ \ j \geqslant 0$$

and $e_j = 0$, for $j < 0$ and $j > n$, $e_0 = 1$.

An equivalent definition of elementary symmetric polynomials is the following: The *elementary symmetric polynomials* are particular cases of monomial symmetric polynomials. For $0 \leqslant k \leqslant n$, we define

$$e_k(X_1,\ldots,X_n) = m_\alpha(X_1,\ldots,X_n),$$

where $a = (\underbrace{1,\ldots,1}_{k},\underbrace{0,\ldots,0}_{n-k})$.

If now we give to the ring of polynomials in $X_1,\ldots,X_n$ over $\mathbb{Z}$ a name, $R = \mathbb{Z}[X_1,\ldots,X_n]$, then the symmetric group S_n of all permutations of $\{1,\ldots,n\}$ acts on R. That is a permutation $\sigma \in S_n$ gives rise to an automorphism $a_\sigma : S \to S$, defined as

$$a_\sigma(g(X_1,\ldots,X_n)) = g(X_{\sigma(1)},\ldots,X_{\sigma(n)}),\ \sigma \in S_n,\ f \in \mathbb{Z}[X_1,\ldots,X_n].$$

A polynomial $F \in R$ is called a *symmetric polynomial* if for all $\sigma \in S_n$

$$F(X_1,\ldots,X_n) = F(X_{\sigma(1)},\ldots,X_{\sigma(n)}).$$

The polynomials in R that are invariant under the action form a subring of R,

$$R_0 = \{S_n - \text{invariant polynomials in } R\}.$$

The product form (2.3) shows that the e_j are invariant under the action and hence $\mathbb{Z}[e_1, \ldots, e_n] \subset R_0$. In fact it is an equality.

Theorem 2.4.6. *(Fundamental Theorem of Symmetric Polynomials). The subring of polynomials in* $\mathbb{Z}[X_1, \ldots, X_n]$ *that are fixed under the action of* S_n *is* $\mathbb{Z}[e_1, \ldots, e_n]$.

This theorem is also true for any $\Re$ commutative ring. Then every symmetric polynomial in $\Re[X_1, \ldots, X_n]$ is a polynomial in the elementary symmetric polynomials in a unique way. In other words if $F(X_1, \ldots, X_n)$ is symmetric, then there exists a unique polynomial $q \in \Re[X_1, \ldots, X_n]$ such that

$$q(e_1, \ldots, e_n) = F(X_1, \ldots, X_n).$$

The discriminant of g in (2.3) is

$$\Delta(g) = \prod_{1 \leqslant i < j \leqslant n} (X_i - X_j)^2.$$

It is invariant under S_n and lies in the coefficient field of g. Expressing Δ in the terms of the e_j is not so easy, although the proof of the Fundamental Theorem of Symmetric Polynomials shows an algorithm which determines the expression for a given S_n-invariant polynomial in terms of the elementary ones. For example, in the case $n = 2$, the discriminant of g can be written in the terms of the elementary symmetric functions of the X_i as

$$\Delta(g) = (X_1 - X_2)^2 = X_1^2 - 2X_1X_2 + X_2^2 = (X_1 + X_2)^2 - 4X_1X_2 = e_1^2 - 4e_2.$$

The square root of the discriminant $\sqrt{\Delta} = \prod_{1 \leqslant i < j \leqslant n}(X_i - X_j)$ is not symmetric. In fact $\sqrt{\Delta}$ is fixed by A_n but not by S_n, where A_n stands for the subset of S_n that formed by even permutations and it is a group that called the alternating group. This polynomial, that we usually denote by $V(X_1, \ldots, X_n)$ is the value of the Vandermonde determinant of the matrix:

$$\begin{pmatrix} 1 & X_1 & X_1^2 & \cdots & X_1^{d-1} \\ 1 & X_2 & X_2^2 & \cdots & X_2^{d-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & X_n & X_n^2 & \cdots & X_n^{d-1} \end{pmatrix}.$$

Complete homogeneous symmetric polynomials

A symmetric polynomial is *homogeneous* in the variables $X_1, \ldots, X_n$ of degree d, if every monomial in it has total degree d. The *total degree* d of a monomial $cX_1^{a_1}, \ldots, X_n^{a_n}$ is the sum of the exponents, that is $d = a_1 + \cdots + a_n$.

For each nonnegative integer k, the *complete homogeneous symmetric polynomial* $h_k(X_1, \ldots, X_n)$ is the sum of all distinct monomials of degree k in the variables $X_1, \ldots, X_n$. For instance $h_3(X_1, X_2, X_3) =$

$$= X_1^3 + X_1^2X_2 + X_1^2X_3 + X_1X_2^2 + X_1X_2X_3 + X_1X_3^2 + X_2^3 + X_2^2X_3 + X_2X_3^2 + X_3^3.$$

The polynomial $h_k(X_1, \ldots, X_n)$ is also the sum of all distinct monomial symmetric polynomials of degree k in $X_1, \ldots, X_n$, for instance for the given example

$$h_3(X_1, X_2, X_3) = m_{(3)}(X_1, X_2, X_3) + m_{(2,1)}(X_1, X_2, X_3) + m_{(1,1,1)}(X_1, X_2, X_3).$$

All symmetric polynomials in variables $X_1, \ldots, X_n$ can be built up from complete homogeneous ones $h_1(X_1, \ldots, X_n), \ldots, h_n(X_1, \ldots, X_n)$ via multiplications and additions.

For example, for $n = 2$, the relevant complete homogeneous symmetric polynomials are $h_1(X_1, X_2) = X_1 + X_2$, and $h_2(X_1, X_2) = X_1^2 + X_1X_2 + X_2^2$. Thus the polynomial $X_1^3 + X_2^3 - 26$ takes the form

$$X_1^3 + X_2^3 - 7 = -2h_1(X_1, X_2)^3 + 3h_1(X_1, X_2)h_2(X_1, X_2) - 26.$$

An important aspect of complete homogeneous symmetric polynomials is their relation to elementary symmetric polynomials, which can be given as the identities

$$\sum_{i=0}^{k} (-1)^i e_i(X_1, \ldots, X_n)h_{k-i}(X_1, \ldots, X_n) = 0,$$

for all $k > 0$, and any number of variables n.

Since $e_0(X_1, \ldots, X_n)$ and $h_0(X_1, \ldots, X_n)$ are both equal to 1, one can isolate either the first or the last terms of these summations; the former gives a set of equations that allows to recursively express the successive complete homogeneous symmetric polynomials in terms of the elementary symmetric polynomials, and the latter gives a set of equations that allows doing the inverse. This implicitly shows that any symmetric polynomial can be expressed in terms of the $h_k(X_1, \ldots, X_n)$ with $1 \leqslant k \leqslant n$: one first expresses the symmetric polynomial in terms of the elementary symmetric polynomials and then expresses those in terms of the mentioned complete homogeneous ones.

In contrast to the situation for the elementary and complete homogeneous polynomials, a symmetric polynomial in n variables with integral coefficients need not be a polynomial function with integral coefficients of the power sum symmetric polynomials.

Example 2.4.7. For $n = 2$, the symmetric polynomial

$$m_{(2,1)}(X_1, X_2) = X_1^2X_2 + X_1X_2^2$$

has the expression

$$m_{(2,1)}(X_1, X_2) = \tfrac{1}{2}s_1(X_1, X_2)^3 - \tfrac{1}{2}s_2(X_1, X_2)s_1(X_1, X_2).$$

For $n = 3$ one gets a different expression

$$\begin{aligned} m_{(2,1)}(X_1, X_2, X_3) &= X_1^2X_2 + X_1X_2^2 + X_1^2X_3 + X_1X_3^2 + X_2^2X_3 + X_2X_3^2 \\ &= s_1(X_1, X_2, X_3)s_2(X_1, X_2, X_3) - s_3(X_1, X_2, X_3). \end{aligned}$$

2.5 Basics for Algorithms and their Running Time

Let two algorithms of input size n and their running times $f(n)$ and $g(n)$. That is $f(n)$ and $g(n)$ are functions from positive integers to positive reals. We define the Big-O notation and we say that $f = O(g)$ or f grows no faster than g, if there is a constant $c > 0$ such that $f(n) \leqslant c \cdot g(n)$. The analog of $\geqslant$ is defined as $f = \Omega(g)$ that means $g = O(f)$, and the analog of $=$ is defined as $f = \Theta(g)$ that means $f = O(g)$ and $f = \Theta(g)$. The rules that make $f(n)$ in $O(f(n))$ as simple as possible are:

1. Multiplicative constants can omitted.
2. n^a dominates n^b if $a > b$.
3. Any exponential dominates any polynomial.
4. Any polynomial dominates any logarithm.

Problem 1. Mergesort
The Algorithm for sorting a list of numbers is the Algorithm 1: We are given a list of numbers L and we split it into two halves. We then recursively sort each half and then merge the two sorted sublists.

This is a divide and conquer strategy.

Algorithm 1: mergesort

input : A list of numbers $L = [1, \cdots, n]$
output: a sorted list L

if $n > 1$*:* **then**
  return *merge (mergeshort (* $[1, \cdots, \lfloor \frac{n}{2} \rfloor]$ *) , mergeshort (* $[\lfloor \frac{n}{2} \rfloor, \cdots, n]$ *))*
else
  return *L*

In case we have as input two sorted lists L_1, L_2 and we want to merge them into a single sorted list, we use the Algorithm 2, where $\circ$ denotes concatenation.

The merge procedure does a constant amount of work per recursive call (provided the required array space is allocated in advance), for a total running time of $O(k + l)$. Thus merge's are linear and merge sort is $O(n \log n)$.

Problem 2. Set Cover

Greedy algorithms build up a solution step by step, by choosing the next step that offers the most obvious and immediate benefit.

The greedy algorithm of Set Cover is the following:

Algorithm 2: merge

input : A list of numbers $L_1 = [1, \cdots, k], L_2 = [1, \cdots, l]$
output: a sorted list L

if $k = 0$*:* **then**
  return $L_2 = [1, \cdots, l]$
if $l = 0$*:* **then**
  return $L_1 = [1, \cdots, k]$
if $L_1 \leqslant L_2$*:* **then**
  return $L_1 \circ$ *merge (* $L_1 = [2, \cdots, k]$ *,* $L_2 = [1, \cdots, l]$ *))*
else
  return $L_2 \circ$ *merge (* $L_1 = [1, \cdots, k]$ *,* $L_2 = [2, \cdots, l]$ *))*

Algorithm 3: Set Cover

input : A set of elements B; sets $S_1, \cdots, S_m \subset B$.
output: A selection of the S_i whose union is B.
cost : Number of sets picked.
repeat
  Pick the set S_i with the largest number of uncovered elements.
until *until all elements of* B *are covered:* ;

The greedy scheme is not optimal, but it is not far from optimal. In particular, if B contains n elements and the optimal cover consists of k sets, then greedy algorithm will use at most $k \ln n$ sets see [24]. The ratio between the greedy algorithm's solution an the optimal solution varies from input but it is less than $\ln n$. The maximum ratio is called approximation factor of the greedy algorithm.

2.5.1 NP-complete problems (or Hard problems)

Dynamic programming is a very powerful algorithmic paradigm in which a problem is solved by identifying a collection of subproblems and tackling them one by one, smallest first, using the answers to small problems to help figure out larger ones, until all of them are solved.

The defining characteristic of search problems is that there is an efficient checking algorithm C that takes as input the given instance I, the proposed solution S and outputs true if and only if S is a solution to instance I. The running time of $C(I, S)$ is counted by a polynomial in $|I|$, the length of the instance. We denote the class of all search problems by **NP**.

Nondeterministic polynomial time (**NP**) problem means that a solution to any search problem can be found and veryfied in polynomial time by a nondeterministic algorithm. **NP** was original defined not as a class of search problems but as a class of decision problems, i.e.

algorithmic questions that can be answered by yes or no.

The class of all search problems that can be solved in polynomial time is denoted by **P**.

Problem 3. Knapsack
We are given integer weights $w_1, \cdots, w_n$ and integer values $v_1, \cdots, v_n$ for n items. We are also given a weight capacity W and a target t (the former is present in the original optimization problem, the latter is added to make it search problem). We seek a set of items whose total weight is at most W and whose total value is at least t. If no such set exists, we should say so.

It is an **NP**-complete problem.

Problem 4. Subset Sum
Suppose that each item's value is equal to its weight (all given in binary) and the target t is the same as the capacity W. We seek a subset of a given set of integers that add up to exactly t. This problem is called Subset Sum and it is a special case of Knapsack.

3. CONTRIBUTIONS OF THIS THESIS

In [39] we describe discriminants in a general context, and relate them to an equally useful object, namely the resultant of an overconstrained polynomial system. We discuss several relevant applications in geometric modeling so as to motivate the use of such algebraic tools in further geometric problems. We focus on exploiting the sparseness of polynomials via the theory of Newton polytopes and sparse elimination. See Chapter 4. The main result of [14] (Theorem 4) is to prove a general decomposition formula of the resultant of a $\mathfrak{S}_n$-equivariant homogeneous polynomial system. This decomposition is given in terms of other resultants that are in principle easier to compute and that are expressed in terms of the divided differences of the input polynomial system. We emphasize that the multiplicity of each factor appearing in this decomposition is also given. The appearance of divided differences is not new in the context of $\mathfrak{S}_n$-equivariant polynomial system since it allows to produce some invariants in a natural way (e.g. [50, 81]). Another important point is that this formula is universal, that is to say that it remains valid (in particular it still has the correct geometric meaning) under any specialization of the coefficient ring of the input polynomial system. This kind of property is particularly important for applications in the fields of number theory and arithmetic geometry where the value of the resultant is as important as its vanishing.

The second main contribution of this paper is a decomposition of the discriminant of a homogeneous symmetric polynomial (Theorem 5). The work on this result was motivated by the unpublished note [81] by N. Perminov and S. Shakirov where a tentative formula is given without a complete proof. Another motivation was to improve the computations of discriminants for applications in convex geometry, following a paper by J. Nie where the boundary of the cone of non-negative polynomials on an algebraic variety is studied by means of discriminants [78]. We emphasize that the discriminant formula is obtained as a byproduct of our first formula on the resultant of a $\mathfrak{S}_n$-equivariant polynomial system. Therefore, it inherits the same features : it allows to split the discriminant into several resultants with multiplicities and it is universal. See Chapter 5 In [29] we mainly work in the case $n = 2$, where the results are more transparent and the basic ideas are already present, but all our results and methods can be generalized to any number of variables. This will be addressed in a subsequent paper [27]. Consider for instance a system of two polynomials in two variables and assume that, the first polynomial factors as $f_1 = f_1' \cdot f_1''$. Then, the discriminant also factors and we thus obtain a multiplicativity formula for it, which we make precise in Corollary 6.4.1. This significantly simplifies the discriminant's computation and generalizes the formula in [12] for the classical homogeneous case. This multiplicativity formula is a consequence of our main result (Theorem 6.3.3 in dimension 2, see also Theorem 6.3.4 in any dimension) relating the mixed discriminant and the resultant of the given polynomials and their *toric Jacobian* (see Section 6.3 for precise definitions and statements). As another consequence of Theorem 6.3.3, we reprove, in Corollary 6.3.6, the bidegree formula for planar mixed discriminants in [18]. See Chapter 6. In the classical problem of MinkDecomp, which is NP-complete, we are seeking a pair of polytopes whose Minkowski sum equals the input polytope. In this work, we compute instead all possible

Minkowski summands. In the first step, we compute the cone of combinatorially equivalent polytopes $U(A)_b$, a subcone of $U(A)$ whose rays and lines generate all the Minkowski summands of P_b. Then, we appropriately shift these rays so that they correspond to integer Minkowski summands. We give an algorithm and its implementation in sage [47] performing the computation of all Minkowski summands in any dimension d, extending ideas from [62]. See Chapter 7.

We introduce the kD-SS problem; it is clearly NP-complete. For its optimization version, we prove that it cannot be approximated efficiently within a constant factor, for general $k \geqslant 2$, hence it does not belong to APX, although the classic 1D-SS-opt has an FPTAS.

Next, we design algorithms with additive errors in the plane. We start with $2D$-SS-opt: given a multiset S, $|S| = n$, target t and $0 < \epsilon < 1$, the algorithm returns, in $O(n^3\epsilon^{-2})$ time, a subset of S whose vectors sum up to t', such that $dist(t, t') \leqslant OPT + \epsilon M_n$, where $M_n = \max P_n$. We also describe two more approximation algorithms which are expected to have better experimental behavior; we implement them and report on experimental results.

Applying one of these algorithms yields an approximation algorithm for MinkDecomp (Section 8.4): If Q is the input polygon the algorithm returns polygons A and B whose Minkowski sum defines polygon Q' such that $vol(Q) \leqslant vol(Q') \leqslant vol(Q) + \epsilon D^2$, $per(Q) \leqslant per(Q') \leqslant per(Q) + 2\epsilon D$, $i(Q) \leqslant i(Q') \leqslant i(Q) + \epsilon D^2$, where D is the diameter of Q. The Hausdorff distance of Q and Q' is bounded by $d_H(Q, Q') \leqslant \epsilon/2D$. See Chapter 8.

4. DISCRIMINANTS AND RESULTANTS

Polynomial algebra offers a standard, powerful, and robust approach to handle several important problems in geometric modeling and other areas. A key tool is the discriminant of a univariate polynomial, or of a well-constrained system of polynomial equations, which expresses the existence of multiple (or degenerate) roots. We describe discriminants in a general context, and relate them to an equally useful object, namely the resultant of an overconstrained polynomial system. We discuss several relevant applications in geometric modeling so as to motivate the use of such algebraic tools in further geometric problems. We focus on exploiting the sparseness of polynomials via the theory of Newton polytopes and sparse elimination.

4.1 Introduction

Polynomial algebra offers a standard approach to handle several problems in geometric modeling and other fields, which provides both powerful and robust methods. Polynomials arise in a variety of scientific and engineering applications, and can be manipulated either algebraically or numerically. Here we mostly focus on tools relevant for algebraic computation, but also useful in numerical calculations. In particular, the study and solution of systems of polynomial equations has been a major topic. Discriminants is a key tool when examining well-constrained systems, including the case of one univariate polynomial. Their theoretical study is a thriving and fruitful domain today, but they are also very useful in a variety of applications. Through the related software development, these algebraic tools can be applied in various practical questions.

The best studied discriminant is that of one polynomial in one variable, probably known since high school, where one studies the discriminant of a quadratic polynomial $f(x) = ax^2 + bx + c$, $a \neq 0$. Polynomial f has a double (real) root if and only if its discriminant

$$\Delta = b^2 - 4ac$$

is equal to zero. Equivalently, this can be defined as the condition for $f(x)$ and its derivative $f'(x)$ to have a common root:

$$\exists\, x \;:\; f(x) = ax^2 + bx + c = f'(x) = 2ax + b = 0 \;\Leftrightarrow \Delta = 0. \tag{4.1}$$

One can similarly consider the discriminant of a univariate polynomial of any degree. If we wish to calculate the discriminant of a polynomial f of degree five in one variable, we consider the condition that both polynomial and its derivative vanish:

$$\begin{aligned} f(x) &= ax^5 + bx^4 + cx^3 + dx^2 + ex + g = 0, \\ f'(x) &= 5ax^4 + 4bx^3 + 3cx^2 + 2dx + e = 0. \end{aligned}$$

In this case, elimination theory reduces the computation of discriminant Δ to the computation of a 9×9 Sylvester determinant, expressing the resultant of f, f'. If we develop

this determinant, we encounter an instance of the fact that the number of its monomials increases exponentially with the input degree:

$$\Delta = -2050a^2g^2bedc + 356abed^2c^2g - 80b^3ed^2cg + 18dc^3b^2g$$
$$e - 746agdcb^2e^2 + 144ab^2e^4c - 6ab^2e^3d^2 - 192a^2be^4d - 4d^2ac$$
$$^3e^2 + 144d^2a^2ce^3 - 4d^3b^3e^2 - 4c^3e^3b^2 - 80abe^3dc^2 + 18b^3e^3$$
$$dc + 18d^3acbe^2 + d^2c^2b^2e^2 - 27b^4e^4 - 128a^2e^4c^2 + 16ac^4e^3 - 27$$
$$a^2d^4e^2 + 256a^3e^5 + 3125a^4g^4 + 160a^2gbe^3c + 560a^2gdc^2e^2 + 1020$$
$$a^2gbd^2e^2 + 160ag^2b^3ed + 560ag^2d^2cb^2 + 1020ag^2b^2c^2e - 192$$
$$b^4ecg^2 + 24ab^2ed^3g + 24abe^2c^3g + 144b^4e^2dg - 6b^3e^2c^2g + 14$$
$$4dc^2b^3g^2 - 630dac^3bg^2 - 630d^3a^2ceg - 72d^4acbg - 72dac^4e$$
$$g - 4d^3c^2b^2g - 1600ag^3cb^3 - 2500a^3g^3be - 50a^2g^2b^2e^2 - 3750a^3$$
$$g^3dc + 2000a^2g^3db^2 + 2000a^3g^2ce^2 + 825a^2g^2d^2c^2 + 2250a^2g^3b$$
$$c^2 + 2250a^3g^2ed^2 - 900a^2g^2bd^3 - 900a^2g^2c^3e - 36agb^3e^3 - 1600$$
$$a^3ge^3d + 16d^3ac^3g - 128d^2b^4g^2 + 16d^4b^3g - 27c^4b^2g^2 + 108ac^5$$
$$g^2 + 108a^2d^5g + 256b^5g^3.$$

One univariate polynomial is the smallest well-constrained system. We can generalize the definition of discriminant to any well-constrained system of multivariate polynomials. In this chapter we are concerned with systems of polynomials and, in particular, sparse polynomials, in other words polynomials with fixed support, or set of nonzero terms.

A related and equally useful tool is the *resultant*, or eliminant. The solvability of an overconstrained set of multivariate polynomials is equivalent to the vanishing of the resultant, which is again a polynomial in the input coefficients. The resultant generalizes the coefficient matrix of an overconstrained linear system and the Sylvester determinant of two polynomials in a single variable. We shall recall the (sparse) resultant, a fundamental object in sparse (or toric) elimination theory, and we shall connect it to the (sparse) discriminant. Here, sparsity means that only certain monomials in each of the $n+1$ polynomials have nonzero coefficients. Resultants are described in the sequel and their relation to discriminants is explained.

It shall become obvious that computing the (mixed) discriminant is an elimination problem, much akin to resultants. Discriminant computation is NP-hard when the system's dimension varies. There have been several approaches for computing discriminants, based on Gröbner bases or resultants. Recently, in [38], they focused on computing the discriminant of a multivariate polynomial via interpolation, based on [37], which essentially leads to an algorithm for predicting the discriminant's Newton polytope, hence its nonzero terms. This yields a new, efficient, and output-sensitive algorithm which, however, remains to be juxtaposed in practice to earlier approaches.

The rest of this chapter is organized as follows. The next section gives some applications of the discriminant, while Section 4.3 provides some general information about sparse elimination theory and resultants. Section 4.4 gives a general description of the discriminant and its properties.

4.2 Applications

In this section, we present some applications of discriminants, in order to motivate their study. Some applications are analyzed in depth, but others are only listed so as to show the breadth of possible applicability.

The main geometric application comes from the fact that discriminants express special geometric configurations, such as tangency between curves in the plane. Consider the following system of two polynomials in two variables:

$$f_1 = ax_1^2 + bx_1x_2 + cx_2^2 + dx_1 + ex_2 + g,$$
$$f_2 = hx_1^2 + ix_1x_2 + jx_2^2 + kx_1 + lx_2 + m.$$

The condition that the two quadrics f_1, f_2 are tangent is equivalent to the condition that the system's discriminant Δ vanishes, where Δ is of degree 12 and has 3210 monomials in coefficients $a, b, c, d, e, g, h, i, j, k, l, m$. An interesting remark, which we shall investigate in Section 4.4, is that the discriminant of a well-constrained system can be reduced to that of a single univariate polynomial, albeit of higher degree. In this case, the system's discriminant equals the discriminant of

$$\begin{aligned} f = \; & ax_1^2x_3 + bx_1x_2x_3 + cx_2^2x_3 + dx_1x_3 + ex_2x_3 + gx_3 + hx_1^2x_4 + ix_1x_2x_4 \\ & + jx_2^2x_4 + kx_1x_4 + lx_2x_4 + mx_4. \end{aligned}$$

Another geometric application of discriminants is in the computation of the Voronoi diagram of ellipses, or of general smooth convex closed sets, see Figure 4.1 (right). Expressing the *Voronoi circle* externally tangent to three given ellipses reduces to a discriminant computation. If the Voronoi circle of center (v_1, v_2) has radius $\sqrt{s}$, then for each of the three ellipses, we consider the resulting discriminant Δ_i expressing tangency between the i-th ellipse and the Voronoi circle, for $i = 1, 2, 3$. We thus get the following 3×3 polynomial system [45]:

$$\Delta_1(v_1, v_2, s) = \Delta_2(v_1, v_2, s) = \Delta_3(v_1, v_2, s) = 0,$$

see Figure 4.1 (left). The above system has one common root that specifies the unique Voronoi circle, but has several other roots that correspond to other (complex) tritangent circles to the three ellipses.

For a line to be tangent to two ellipses, the discriminant of the polynomials, expressing tangency between each ellipse and an (unknown) line, should vanish. All the real roots of the discriminant are the values of the parameter that correspond to the tangency points, which in turn allows us to compute the implicit equations of all bitangent lines. There are four bitangents to two disjoint ellipses unless the latter constitute a degenerate situation.

The discriminant is encountered in further geometric applications, for example in the description of the topology of plane curves [56]. In real algebraic geometry, the number of real roots of a real polynomial is constant, when the coefficients vary on each connected component of the zero set (or zero locus) of the (sparse) mixed discriminant, given that for the number of real roots to increase, two complex roots should merge.

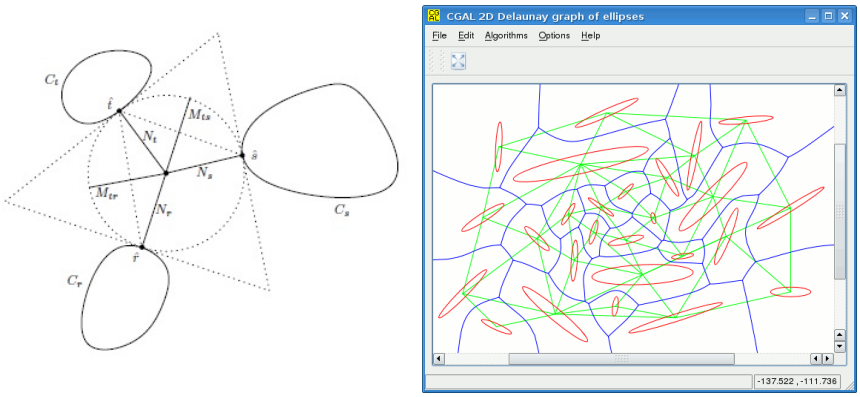


Figure 4.1: Left: Voronoi circle for 3 ellipses. Right: An example of a Voronoi diagram for non-intersecting ellipses, and the corresponding Delaunay graph. Both figures reproduced from [45]

Discriminants are thus used in solving systems of polynomial inequalities and in zero-dimensional system solving [48], in root classification and computation of real roots of square systems of sparse polynomials [31], in detecting real roots for n-variate $(n+2)$-monomial polynomials with integer exponents [9], in the description of the topology of real algebraic plane curves [56], and in the determination of cusp points of parallel manipulators [77].

In [43], based on precomputed discriminants, they classify, isolate with rational points, and compare the real roots of polynomials of degree up to 4. In [59] they present an algorithm for computing discriminants and prime ideal decomposition in number fields. The algorithm computes the p-valuation of the index of a generating equation $f(x)$ as well; in particular, it determines the discriminant of the number field, once one is able to factorize the discriminant of the defining equation. In [10], a key point is to show that the univariate polynomial below, with rational coefficients, namely:

$$x^{17} - 5x^{16} + 12x^{15} - 28x^{14} + 72x^{13} - 132x^{12} + 116x^{11} -$$
$$-74x^9 + 90x^8 - 28x^7 - 12x^6 + 24x^5 - 12x^4 - 4x^3 - 3x - 1$$

has Galois group $SL_2(\mathbb{F}_{16})$. This is achieved by the use of discriminants and their factorization. Furthermore, in [49] they break the Algebraic Surface Cryptosystem (ASC) proposed in 2009. The main idea is to decompose ideals deduced from the ciphertext in order to avoid to solve the section-finding problem. They achieve this by an algorithm that computes and factors resultants.

Another application is an algebraic problem, which arises from considering pairs of differential equations on the plane of the form

$$\dot{x} = P(x,y),\ \dot{y} = Q(x,y),$$

where P and Q are polynomials in x, y. To find the equilibrium points we have to find the intersections of the curves $P(x,y) = 0 = Q(x,y)$ and also to decide whether they touch at

these points, and whether the discriminant Δ vanishes there. Lastly, discriminants can be found in applied physics, e.g. in dark matter search [20]. Moreover, in [55] are established the algebraic conditions for a polynomial to have a pair of minima that have a common horizontal tangent, by computing, among others, a resultant and giving a factorization of the discriminant of a polynomial. This condition is exactly that required by the Maxwell convention of catastrophe theory. The extremal monomials and coefficients of the discriminant have interesting combinatorial descriptions. This has important applications in singularity theory and number theory.

Let us conclude with the following example, which is an application of (sparse) mixed discriminants that concerns the determination of real roots.

Example 4.2.1. [26] The Wilkinson polynomial

$$W_{20} = \prod_{i=1}^{20}(x+i) = \sum_{j=0}^{20} c_j x^j$$

is well known for its numerical instability [94]. It has 20 real roots, but the polynomial $W_{20}(x)+10^{-9}x^{19}$ has only 12 real roots and 4 pairs of complex roots, which do not seem to have small imaginary part, as one of these pairs is approximately equal to $-16.57173899 \pm 0.8833156071i$. On the other hand, if we subtract $10^{-9}x^{19}$ from W_{20} we get a polynomial with 14 real zeros. This unstable behavior could be explained by the fact that the vector of coefficients $(20!, \ldots, 210, 1)$ of W_{20} is very close not only to the variety (set) of ill-posed polynomials, but also very close to a singular point of this variety.

In [26], there are experiments with the following 2-dimensional family of polynomials of degree 20:

$$W(a,b,x) := W_{20}(x) + ax^{19} + bx^{18}.$$

The corresponding discriminant $\Delta(a,b)$ defines a singular curve traced inside the discriminant locus. The singularities of $\Delta(a,b) = 0$ are close to the point $a = b = 0$, i.e., to the vector of coefficients of the $Wilkinson$ polynomial. Figure 4.2 features sample points of $\Delta(a,b) = 0$ inside a small box around the origin, which is the point lying in the intersection of the two coordinate arrows.

Considering the distance, not just to the variety of ill-posed problems, but also to its singular locus would correspond, in the case of conditioning of square $m \times m$ matrices in linear algebra, to consider not only the smallest and greatest singular values, but also the behavior of the intermediate ones.

4.3 Sparse elimination theory

This section introduces sparse (or toric) elimination theory and its main tool, the sparse resultant.

Classical elimination theory and the classical multivariate resultant have a long and rich history that includes such luminaries as Euler, Bézout, Cayley and Macaulay; see [22,

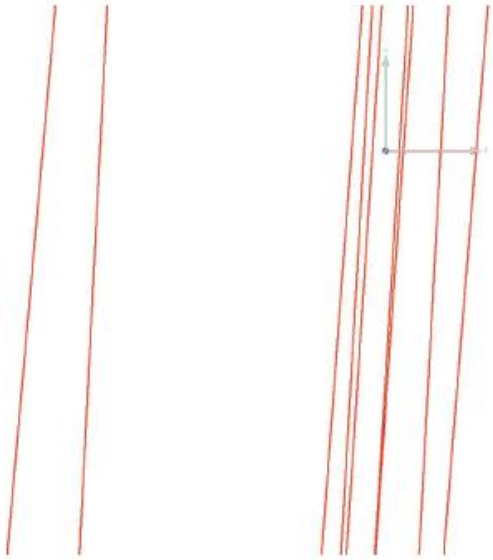


Figure 4.2: The figure is by B. Mourrain using software Mathemagix [92], see also [26]

28, 93]. Having been at the crossroads between pure and computational mathematics, it became the victim, in the second quarter of this century, of the polemic led by the promoters of abstract approaches. Characteristically, the third edition of van der Waerden's *Modern Algebra* has a chapter on elimination theory and resultants that has disappeared from later editions.

Moreover, when the number of variables exceeds four or five, elimination methods lead to matrices which are, of course, too large for hand calculations and quite demanding computationally. However, the advent of modern computers has revived this area. The last decade has seen efficient resultant-based solutions of certain algorithmic as well as applied problems. Some of these problems were impossible to tackle with other methods in real time. These areas include, among others, robotics [15],

and geometric modeling [73].

The classical (or projective) resultant of a system of n homogeneous polynomials in n variables vanishes exactly when there exists a common solution in projective space. The sparse (or toric) resultant of $n+1$ polynomials in n variables characterizes solvability over a smaller space which coincides with affine space under certain genericity conditions. Sparse elimination theory concerns the study of resultants and discriminants associated with toric varieties, in other words varieties defined for a given set of support points. This theory has its origin in the work of Gel'fand, Kapranov and Zelevinsky on multivariate hypergeometric functions. Singularities of such functions are discriminants, whereas

the denominator of rational hypergeometric functions is a product of resultants, that is, a product of special discriminants.

Let us start with some definitions: $conv(A)$ denotes the convex hull of set A. Volume, denoted by Vol$(\cdot)$, is always considered normalized with respect to the lattice $\mathbb{Z}^n$, so that

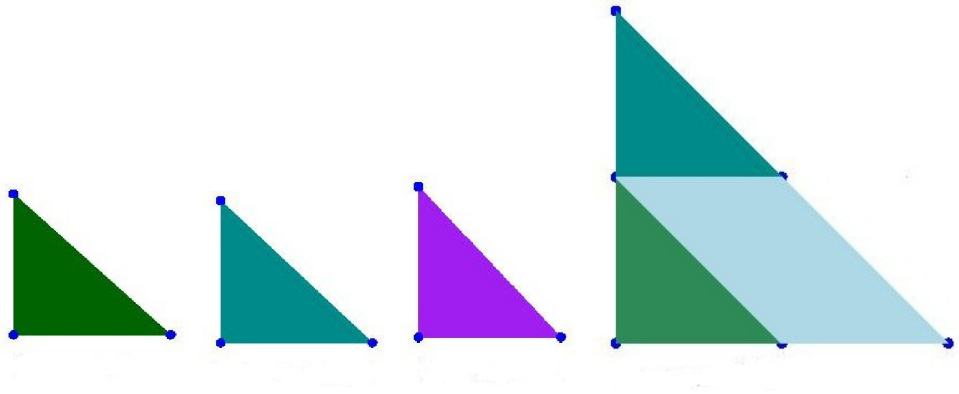


Figure 4.3: The Newton polygons $Q_1' = conv(A_1')$, $Q_1'' = conv(A_1'')$, $Q_2 = conv(A_2)$, and $Q_1 = conv(A_1)$

a primitive triangle or simplex has volume equal to 1. As usual $Q_1 + Q_2$ denotes the Minkowski sum of Q_1 and Q_2.

The *Newton polytope* $N(f)$ of a nonzero polynomial

$$f = \sum_{a \in A \subset \mathbb{Z}^n} c_a x^a, \quad c_a \neq 0,$$

is the polytope with integer vertices defined as the convex hull of A; the latter is the *support* of f and contains precisely the exponents occurring in f with non-zero coefficients.

Sparsity is measured in geometric terms by the Newton polytope of the polynomial, but what does sparsity mean? The number of nonzero monomials is not necessarily small, but they are modeled by the Newton polytope, thus leading to rich theory, which exploits combinatorial ideas and properties. The main notion, of course, is that a polynomial system is characterized by those monomials in each of the polynomials that have nonzero coefficients. Here is an example.

Example 4.3.1. Consider specific polynomials f_1', f_1'', f_2 and their supports, which are full dimensional in $\mathbb{Z}^2$ as follows:

$$A_1' = \{(0,0),(0,1),(1,0)\}, \quad A_1'' = \{(0,0),(0,1),(1,0)\}, \quad A_2 = \{(0,0),(0,1),(1,0)\}.$$

Let $f_1 = f_1' \cdot f_1'$, then its support is $A_1 = A_1' + A_1'' = \{(0,0),(0,1),(1,0),(2,0),(0,2),(1,1)\}$. All Newton polytopes (here, polygons) can be seen in Figure 4.3.

Example 4.3.2. Consider polynomials f_1', f_1'', f_2 and their supports, as follows:

$$A_1' = \{(0,0),(0,1),(0,2),(1,0)\}, \quad A_1'' = \{(0,0),(0,1),(1,0),(2,0)\},$$

and $A_2 = \{(0,0),(0,1),(0,2),(1,0),(2,0),(2,1),(2,2),(1,2)\}$. If $f_1 = f_1' \cdot f_1''$, then its support is

$$A_1 = A_1' + A_1'' = \{(0,0),(0,1),(1,0),(2,0),(0,2),(1,1),(2,1),(0,3),(1,2),(2,2),(3,0)\}.$$

All Newton polytopes (here, polygons) can be seen in Figure 4.4, and Figure 4.5.

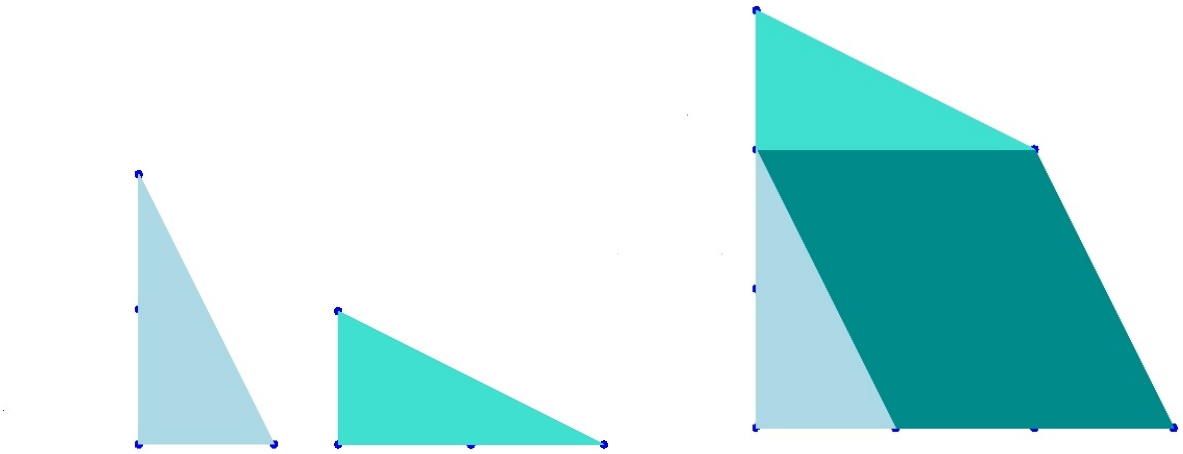


Figure 4.4: The Newton polygons $Q_1' = conv(A_1')$, $Q_1'' = conv(A_1'')$, and $Q_1 = conv(A_1)$

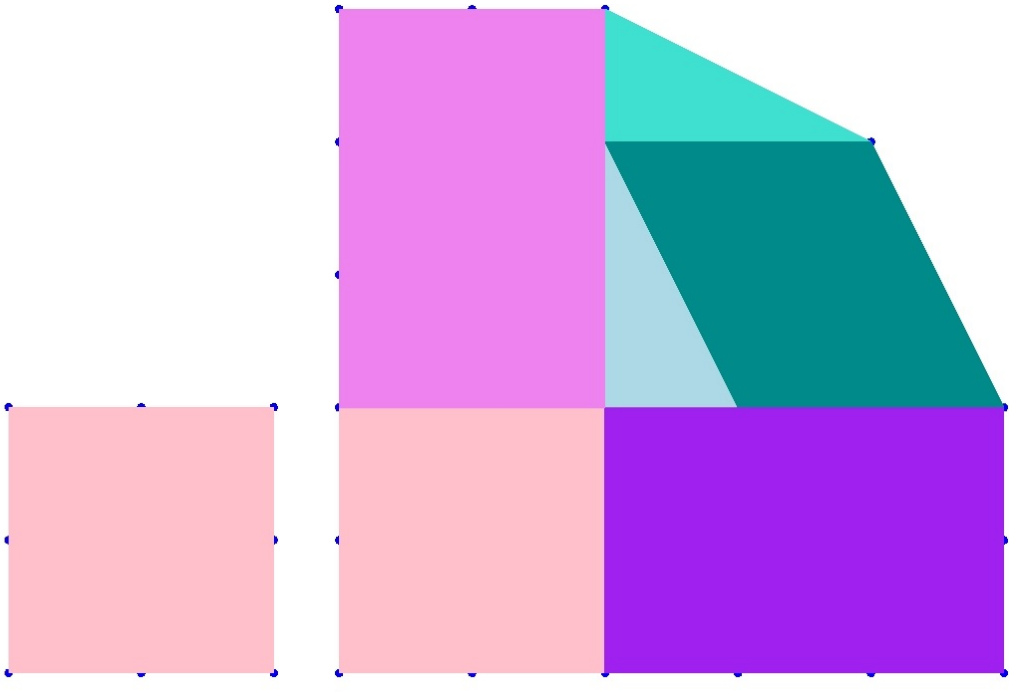


Figure 4.5: The Newton polygons $Q_2 = conv(A_2)$, and $Q_1 + Q_2 = conv(A_1 + A_2)$

The *mixed volume* $MV(Q_1,\ldots,Q_n)$ of n convex polytopes Q_i in $\mathbb{R}^n$ is a classic function in geometry, taking values in $\mathbb{N}$ and generalizing the notion of volume, in the sense that mixed volume equals $n!\mathsf{Vol}(Q_1)$, when $Q_1=\cdots=Q_n$. Mixed volume is multilinear with respect to scalar multiplication and Minkowski addition of the Q_i's.

The cornerstone of sparse elimination theory is the following theorem.

Theorem 1. [8] *The mixed volume of the Newton polytopes of polynomials $f_1(x),\ldots,f_n(x)$ in n variables bounds the number of common solutions of $f_1(x)=0,\ldots,f_n(x)=0$ in the algebraic torus $(K^*)^n$, where K is an algebraically closed field of the coefficients. If the coefficients of the polynomials are sufficiently generic, then the number of common solutions equals the mixed volume.*

This bound generalizes, to the sparse case, Bézout's classical bound, which is equal to the product of the n polynomials' total degrees, and bounds the number of solutions in n-dimensional complex projective space. For polynomials whose supports are simplices, as in Example 4.3.1, the mixed volume and Bézout's bound coincide.

Mixed volume can be computed in terms of Minkowski sum volumes:

$$MV_n(Q_1,\ldots,Q_n)=\sum_{k=1}^{n}(-1)^{n-k}\sum_{I\subset\{1,\ldots,n\},|I|=k}\mathsf{Vol}\Big(\sum_{i\in I}Q_i\Big).$$

This implies, for $n=2$:

$$MV(Q_1,Q_2)=\mathsf{Vol}(Q_1+Q_2)-\mathsf{Vol}(Q_1)-\mathsf{Vol}(Q_2). \tag{4.2}$$

In general, this formula does not lead to efficient computation. Instead, an efficient algorithm and implementation has been developed in [16].

4.3.1 Resultants

The strong interest in multivariate resultants is explained, because resultant-based methods have been found to be very efficient for solving certain classes of small and medium-size problems, say of dimension up to 10. For a system of $n+1$ arbitrary polynomial equations in n variables, it is a polynomial in the coefficients, hence it eliminates n variables. The resultant is defined when all polynomial coefficients are symbolic, but typically used when only some of them are symbolic.

One example is the determinant of the coefficient matrix of $n+1$ linear polynomials. Unless the coefficients are very particularly chosen, the resultant vanishes for a particular specialization of all coefficients if and only if the given system has a non-trivial solution.

Another example is the Sylvester resultant, namely for $n=1$. Then, the resultant equals the determinant of Sylvester's matrix. For generic polynomials $f_1(x), f_2(x)$ of degrees one and two, respectively, Sylvester's matrix S is as follows:

$$\left\{\begin{array}{ll} f_1(x)= & a_1x+a_0 \\ f_2(x)= & b_2x^2+b_1x+b_0 \end{array}\right\} \text{ and } S=\begin{bmatrix} a_1 & a_0 & 0 \\ 0 & a_1 & a_0 \\ b_2 & b_1 & b_0 \end{bmatrix}. \tag{4.3}$$

The resultant equals $\det S = a_1^2 b_0 + a_0^2 b_2 - a_0 a_1 b_1$. Thus S is an instance of a resultant matrix, in other words a matrix whose determinant yields the resultant. The principal merit of resultant matrices is that they reduce the solution of a non-linear system to a matrix problem, where we can use an arsenal of numeric linear algebra techniques and software, see e.g. [22, 28]. By construction, the existence of common solutions implies a decrease of matrix rank.

In most applications, we deal with *well-constrained* systems, namely systems of k polynomials in k unknowns. To obtain an overconstrained system, for which the resultant is defined, we should either add an extra polynomial or "hide" a variable in the coefficient field [22, 28, 93].

We now formally define the resultant polynomial of an overconstrained system.

Definition 4.3.3. The *resultant* $\mathrm{Res}(f_0, \ldots, f_n)$ of $n+1$ polynomials $f_0, \ldots, f_n$ in n variables is an irreducible polynomial in the coefficients of $f_0, \ldots, f_n$, which vanishes whenever $f_0, \ldots, f_n$ have a common root.

The *sparse resultant* has an analogous definition when the f_i are specified by their supports $A_i \subseteq \mathbb{Z}^n$. Formally, the *sparse resultant* of $f_0, \ldots, f_n)$, where each f_i has support A_i, is an irreducible polynomial with integer coefficients over the coefficients of the f_i such that it vanishes precisely when the system $f_0 = f_1 = \cdots = f_n = 0$ has a solution in $(\mathbb{C}^*)^n$.

The Newton polytope of the (sparse) resultant is called the resultant polytope, and it can be effectively computed by the algorithm in [37].

4.4 Discriminants

In this section we introduce discriminants of well constrained systems, provide some definitions and overview relevant properties in section 4.4.1.

Gel'fand, Kapranov and Zelevinsky [54] established the following definition, which we shall formally state later: The (sparse) *mixed discriminant* $\Delta(f_1, \ldots, f_n)$ of n polynomials in n variables is the irreducible polynomial in the coefficients of the f_i which vanishes whenever the system $f_1 = \cdots = f_n = 0$ has a multiple root or, equivalently, a root which is not simple. Consider a system of two polynomials in two variables:

$$f_1(x_1, x_2) = a_0 + a_1 x_1 + a_2 x_1^2 + a_3 x_2 + a_4 x_2^2 + a_5 x_1 x_2,$$
$$f_2(x_1, x_2) = b_0 + b_1 x_1 + b_2 x_2.$$

Their discriminant shows whether a common root is singular.

Let us formalize the definition of (sparse) discriminants. We consider n (finite) lattice configurations $A_1, \ldots, A_n$ in $\mathbb{Z}^n$ and we denote by $Q_1, \ldots, Q_n$ their respective convex hulls. Let $f_1, \ldots, f_n$ be Laurent polynomials with support $A_1, \ldots, A_n$ respectively:

$$f_i(x) = \sum_{\alpha \in A_i} c_{i,\alpha} x^\alpha, \quad i = 1 \ldots, n. \tag{4.4}$$

We define the *discriminantal variety* to be the closure of the locus of coefficients $c_{i,a}$ for which the associated system of n polynomial equations in n unknowns $x = (x_1, \ldots, x_n)$, over an algebraically closed field K, namely:

$$f_1(x) = \cdots = f_n(x) = 0, \tag{4.5}$$

has a non-degenerate multiple root.

Before the general definition we present the simplest case.

Example 4.4.1. Given a generic univariate polynomial of degree d,

$$P(z) = a_0 + a_1 z + \cdots + a_d z^d, \quad a_d \neq 0,$$

there exists an irreducible polynomial $\Delta(P) = \Delta(a_0, \ldots, a_d) \in \mathbb{Z}[a_0, \ldots, a_d]$, unique up to sign, called the *discriminant*, which verifies $\Delta(a_0, \ldots, a_n) \neq 0$ if and only if all roots of P are simple for any specialization of the coefficients in $\mathbb{C}$, with $a_d \neq 0$. Thus $\Delta(a_0, \ldots, a_n) = 0$ if and only if there exists $z \in \mathbb{C}$ with $P(z) = P'(z) = 0$. In fact, the corresponding Sylvester resultant $R(P, P')$ equals $a_d \Delta(P)$.

This discriminant is an instance of both A-discriminant and mixed discriminant and mixed discriminant, which are defined below.

Geometrically, the discriminant hypersurface

$$\{a = (a_0, \ldots, a_d) \in \mathbb{C}^{d+1} \, : \, \Delta(a) = 0\}$$

is the projection over the first $d+1$ coordinates of the intersection of the hypersurfaces $\{(a, z) \in \mathbb{C}^{d+2} \, : \, a_0 + a_1 z + \cdots + a_d z^d = 0\}$ and $\{(a, z) \in \mathbb{C}^{d+2} \, : \, a_1 + 2a_2 z + \cdots + d a_d z^{d-1} = 0\}$, in other words the variable z is eliminated.

An isolated solution $u \in (K^*)^n$ is a *nondegenerate multiple root* if the n gradient vectors

$$\left(\frac{\partial f_i}{\partial x_1}(u), \ldots, \frac{\partial f_i}{\partial x_n}(u) \right)$$

are linearly dependent, but any $n-1$ of them are linearly independent.

We now give the definition of (sparse) A-discriminant from [54]. It is related to some support set A, thus capturing the sparse structure of the data.

Definition 4.4.2. Consider the polynomial defined from system (4.4) for $n = 1$. We denote by Δ_A the *(sparse) A-discriminant*, which is the unique (up to sign) irreducible polynomial with integer coefficients, in the parameter coefficients $c_{i,a}$, where we follow the previous notation. Δ_A vanishes whenever the hypersurface is not smooth. Otherwise we refer to set A as a *defective* support, and set $\Delta_A = 1$.

Let $A_1, \ldots, A_n$ be pointsets in $\mathbb{Z}^n$, as specified for system (4.4). We define the (sparse) mixed discriminant from [18], which captures the structure in a given well-constrained polynomial system.

Definition 4.4.3. If the discriminantal variety is a hypersurface, we define the (sparse) *mixed discriminant* of system (4.5) to be the unique up to sign irreducible polynomial $\Delta_{A_1,\ldots,A_n}$ with integer coefficients in the unknown parameters $c_{i,a}$, which defines this hypersurface. Otherwise, we say that the system is defective and set $\Delta_{A_1,\ldots,A_n} = 1$.

We now relate the previous two notions with an important construction in algebraic combinatorics. Let $A_1, \ldots, A_n$ be supports in $\mathbb{Z}^n$, defining Laurent polynomials, then A shall be specified to be the corresponding Cayley matrix. This matrix is defined to ave $2n$ rows and $m = \sum_{i=1}^{n} |A_i|$ columns. We introduce n new variables $y_1, \ldots, y_n$ in order to encode the system $f_1 = \cdots = f_n = 0$ in a single polynomial with support in A. This is known as the *Cayley trick* and yields polynomial

$$\phi(x, y) = y_1 f_1(x) + \cdots + y_n f_n(x).$$

The Cayley matrix is:

$$A = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 \\ A_1 & A_2 & \ldots & A_n \end{pmatrix}.$$

By [18, Theorem 2.1], the mixed discriminant $\Delta_{A_1,\ldots,A_n}$ equals the A-discriminant of the associated Cayley matrix whenever $\Delta_A \neq 1$. Let us give an example of the relation between A-discriminant and mixed discriminant.

Example 4.4.4. Consider two planar configurations $A_1 = \{(6,0),(0,3),(0,1)\}$, and $A_2 = \{(0,6),(3,0),(1,0)\}$. These supports correspond to the following family of polynomials:

$$\begin{aligned} h_1(x, y) =& c_{11}x^6 + c_{12}y^3 + c_{13}y, \\ h_2(x, y) =& c_{21}y^6 + c_{22}x^3 + c_{23}x. \end{aligned}$$

We introduce two new variables a, b in order to encode the system $h_1 = h_2 = 0$ in a single polynomial, namely

$$\phi(x, y, a, b) = ah_1(x, y) + bh_2(x, y).$$

Then, A is the Cayley matrix associated to the supports A_1, A_2:

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 6 & 0 & 0 & 0 & 3 & 1 \\ 0 & 3 & 1 & 6 & 0 & 0 \end{pmatrix},$$

and the A-discriminant $\Delta_A(c) = \Delta_A(c_{11}, \ldots, c_{23})$ is the mixed discriminant of h_1, h_2. Now $\Delta_A(c) = 0$ whenever there exists a common zero $(x, y) \in K^2$, making both h_1, h_2 vanish, which is not simple.

It turns out that $\Delta_A(c)$ is a polynomial of degree 90 in c, with 58 monomials and huge integer coefficients.

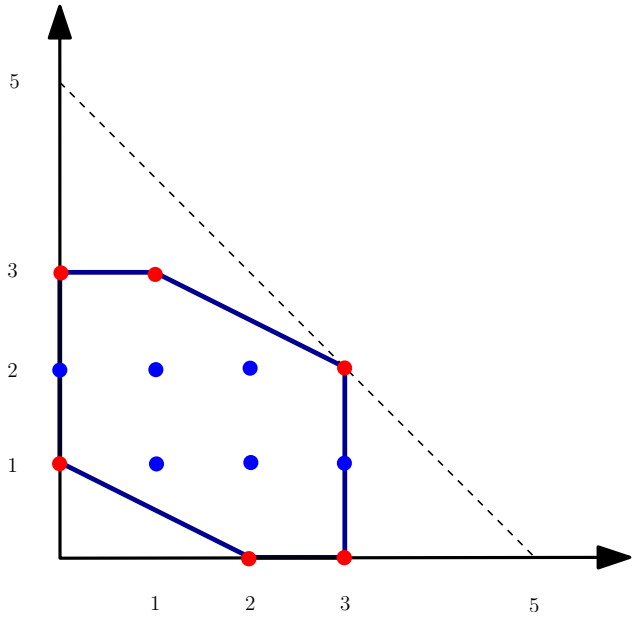


Figure 4.6: The discriminant polytope

4.4.1 Properties

4.4.1.1 Basic Properties and Examples

$$\Delta(f_1) = \frac{1}{a_n} Res_{d_1,d_1-1}(f_1, f_1')$$

For

$$f(x) = ax^2 + bx + c$$
$$f'(x) = 2ax + b$$

we find

$$\text{Res}(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = -a(b^2 - 4ac)$$

so that $D = b^2 - 4ac$.

- The Newton polytope of f, $N(f)$, is the convex hull of the set of exponents of its monomials with non-zero coefficient.
- The discriminant polytope is $N(\Delta)$. $f(x_1, x_2) = 8x_2 + x_1x_2 - 24x_2^2 - 16x_1^2 + 220x_1^2x_2 - 34x_1x_2^2 - 84x_1^3x_2 + 6x_1^2x_2^2 - 8x_1x_2^3 + 8x_1^3x_2^2 + 8x_1^3 + 18x_2^3$
- It holds $dim(N(\Delta)) = n - d + 1$.
- Knowing $N(\Delta)$, reduces the computation of Δ to a linear algebra problem

4.4.1.2 Multiplicativity formulae for Sparse Resultants and Discriminants

In this section we review existing work on the discriminant degree, and on multiplicativity formulae for sparse resultants and discriminants.

We start with the necessary notation for a theorem on the degree of the mixed discriminant of two polynomials with fixed supports. A subset $F \subseteq A$ is called *face* of A, if F is the intersection of A with a face of the polytope $conv(A)$. We shall write Res$(f_1, \ldots, f_n)$ and $\Delta(f_1, \ldots, f_n)$ without subscripts to imply Res$_{A_1,\ldots,A_n}(f_1, \ldots, f_n)$ and $\Delta_{A_1,\ldots,A_n}(f_1, \ldots, f_n)$. Let π denote the projection to $\mathbb{R}A/\mathbb{R}F$, where F is a face of A. We set

$$u(F, A) := \mathsf{Vol}\Big(conv(\pi(A)) - conv(\pi(A - F))\Big).$$

If e_1 and e_2 are parallel edges in Q_1 and Q_2 with same orientation, that is, same inward normal direction, then we call them *strongly parallel*. Let E_i denote the set of edges of A_i and set

$$P := \{(e_1, e_2) \in E_1 \times E_2 : e_1 \text{ is strongly parallel to } e_2\}.$$

We write $l(e)$ for the *normalized length* of an edge e with respect to the lattice $\mathbb{Z}^n$. If $v \in$ Vert(A_2), where Vert(A_2) are the vertices of A_2, we define its *mixed multiplicity* as follows:

$$mm(v) := MV(Q_1, Q_2) - MV(\mathsf{conv}(A_2 - \{v\}), Q_1).$$

Let us introduce polynomial

$$\tilde{\Delta}_{A_1,\ldots,A_n} = \Delta_{A_1,\ldots,A_n}^{i(A_1,\ldots,A_n)}$$

defined as the power of the mixed discriminant $\Delta_{A_1,\ldots,A_n}$ raised to the index

$$i(A_1, \ldots, A_n) = [\mathbb{Z}^n : \mathbb{Z}A_1 + \cdots + \mathbb{Z}A_n].$$

The latter stands for the index of lattice $\mathbb{Z}A_1 + \cdots + \mathbb{Z}A_{n+1}$ in $\mathbb{Z}^n$, as a subgroup. In general, this index equals 1. Let the discriminant degree in the coefficients of the i-th input polynomial be denoted by

$$\delta_i = deg_{A_i}(\tilde{\Delta}_{A_i,A_j}), \quad i = 1, 2.$$

Then, the following theorem holds.

Theorem 2. [18] *Let A_1 and A_2 be full-dimensional supports in $\mathbb{Z}^n$. Then δ_i equals*

$$2 \cdot \mathit{Vol}(Q_j) + 2 \cdot MV(Q_i, Q_j) - \sum_{(e_i,e_j)\in P} \min\{u(e_i, A_i), u(e_j, A_j)\} l(e_j) - \sum_{v \in \mathit{Vert}(A_i)} mm(v),$$

where $i = 1, 2$ and $j = 2, 1$, in other words $\{i, j\} = \{1, 2\}$.

An explicit degree formula for the special cases of plane curves is also presented in [18, Corollary 3.15]. We correct this formula. The degree of Δ_{A_1,A_2} can be computed as follows:

$$\delta_1 = area(Q_1 + Q_2) + area(Q_1) - perimeter(Q_2),$$

$$\delta_2 = area(Q_1 + Q_2) + area(Q_2) - perimeter(Q_1),$$

where $Q_i = conv(A_i)$, $i = 1, 2$, $Q_1 + Q_2$ is their Minkowski sum. The area (like volume above) is normalized, so that a primitive triangle has area 1 and the perimeter of Q_i is the cardinality of $\partial Q_i \cap \mathbb{Z}^2$.

Computing resultants and discriminants is usually a computationally hard task. However, if one polynomial factors as $f_1 = f_1' \cdot f_1''$, both resultant and discriminant factors, and we thus obtain a multiplicativity formula. This significantly simplifies the corresponding computation.

Let us recall the case when one polynomial factors as a product of two polynomials, in the case of resultants. The multiplicativity formula for sparse resultants can be found in [80, Proposition 7.1], see also [23, Corollary 2.20]. Consider polynomials $f_1, \ldots, f_{n+1}$ in variables $x_1, \ldots, x_n$ and let $f_1 = f_1' \cdot f_1''$ be a product of two polynomials, where all relevant supports are $A_1, A_1', A_1'', A_2, \ldots, A_{n+1} \subseteq \mathbb{Z}^n$ respectively. Then,

$$\mathsf{Res}(f_1' f_1'', f_2, \ldots, f_{n+1}) = \mathsf{Res}(f_1', f_2, \ldots, f_{n+1}) \cdot \mathsf{Res}(f_1'', f_2, \ldots, f_{n+1}). \tag{4.6}$$

We now pass to discriminants. The multiplicativity property of the discriminant in the case of (dense) homogeneous polynomials was already known to Sylvester [89], and has been generalized by Busé and Jouanolou [12]. They prove that for any n, when all A_i's correspond to (the lattice points in) a dilate of the standard simplex and $A_i = A_1' + A_1''$ is the sum of two dilates of the simplex then, given polynomials $f_1', f_1'', f_2, \ldots, f_n$ with corresponding supports $A_1', A_1'', A_2, \ldots, A_n$,

$$\Delta(f_1, \ldots, f_n) = \Delta(f_1', \ldots, f_n) \cdot \Delta(f_1'', \ldots, f_n) \cdot \mathsf{Res}(f_1', f_1'', \ldots, f_n)^2.$$

Recall that the discriminant of $n-1$ homogeneous polynomials of degree 1 equals 1 by convention.

Theorem 3. [12, 89] *Let $f_1', f_1'', f_2, \ldots, f_{n-1}$ be n homogeneous polynomials in $R[x_1, \ldots, x_n]$, of degrees $d_1', d_1'', d_2, \ldots, d_{n-1} \geqslant 1$, respectively. Then $\Delta(f_1' f_1'', f_2, \ldots, f_{n-1})$ factors as follows:*

$$(-1)^{d_1' d_1'' d_2 \ldots d_{n-1}} \cdot \Delta(f_1', f_2, \ldots, f_{n-1}) \cdot \Delta(f_1'', f_2, \ldots, f_{n-1}) \cdot \mathsf{Res}(f_1', f_1'', f_2, \ldots, f_{n-1})^2.$$

Our current work focuses on multiplicativity formulas for the mixed discriminant in the case $n = 2$, with fixed supports, always within the realm of sparse elimination theory [29], aiming at efficient algorithms. It turns out that a key issue is to understand the relation between the mixed discriminant of two bivariate Laurent polynomials, where one factors, and the sparse resultant of those three bivariate polynomials.

5. RESULTANT OF AN EQUIVARIANT POLYNOMIAL SYSTEM WITH RESPECT TO THE SYMMETRIC GROUP

Given a system of $n \geqslant 2$ homogeneous polynomials in n variables which is equivariant with respect to the symmetric group of n symbols, it is proved that its resultant can be decomposed into a product of several resultants that are given in terms of some divided differences. As an application, we obtain a decomposition formula for the discriminant of a multivariate homogeneous symmetric polynomial.

5.1 Introduction

The analysis and solving of polynomial systems are fundamental problems in computational algebra. In many applications, polynomial systems are structured and it is very useful to develop special methods in order to take into account structures. In this paper, we will focus on systems of n homogeneous polynomials $f_1, \ldots, f_n$ in n variables $x_1, \ldots, x_n$ that are globally invariant under the action of the symmetric group $\mathfrak{S}_n$ of n symbols. More precisely, we will assume that for any integer $i \in \{1, 2, \ldots, n\}$ and any permutation $\sigma \in \mathfrak{S}_n$

$$\sigma(f_i) := f_i(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f_{\sigma(i)}(x_1, x_2, \ldots, x_n).$$

In the language of invariant theory these systems are called equivariant with respect to the symmetric group $\mathfrak{S}_n$, or simply $\mathfrak{S}_n$-equivariant (see for instance [97, §4] or [33, Chapter 1]). Some recent interesting developments based on Gröbner basis techniques of this kind of systems, when the coordinates of the roots are all distinct, can be found in [50]. In this work, we will study the resultant of $\mathfrak{S}_n$-equivariant homogeneous polynomial systems in order to reveal their structure.

There are special cases for which a decomposition of the resultant of a $\mathfrak{S}_n$-equivariant homogeneous polynomial system is known. In the case $n = 2$, any $\mathfrak{S}_2$-equivariant homogeneous polynomial system is of the form

$$F^{\{1\}}(x_1, x_2) := a_0 x_1^d + a_1 x_1^{d-1} x_2 + \cdots + a_d x_2^d, \quad F^{\{2\}}(x_1, x_2) := F^{\{1\}}(x_2, x_1)$$

and one can show [2, Exercice 67] that there exists an irreducible polynomial $K_d \in \mathbb{Z}[a_0, \ldots, a_d]$ such that

$$\mathrm{Res}\left(F^{\{1\}}, F^{\{2\}}\right) = F^{\{1\}}(1,1)F^{\{1\}}(1,-1)K_d^2 = \left(\sum_{i=0}^{d} a_i\right)\left(\sum_{i=0}^{d} (-1)^i a_i\right) K_d^2.$$

As another example, suppose $n \geqslant 2$, $d = 1$ and set $F^{\{i\}}(x_1, \ldots, x_n) = ax_i + be_1(x_1, \ldots, x_n)$, $i = 1, \ldots, n$. Then, since the resultant of n linear forms in n variables is the determinant of the matrix of their associated linear system, it is a straightforward computation to show that

$$\mathrm{Res}\left(F^{\{1\}}, \ldots, F^{\{n\}}\right) = a^{n-1}(a + nb).$$

The main result of this paper (Theorem 4) is to prove a general decomposition formula of the resultant of a $\mathfrak{S}_n$-equivariant homogeneous polynomial system. This decomposition is given in terms of other resultants that are in principle easier to compute and that are expressed in terms of the divided differences of the input polynomial system. We emphasize that the multiplicity of each factor appearing in this decomposition is also given. The appearance of divided differences is not new in the context of -equivariant polynomial system since it allows to produce some invariants in a natural way (e.g. [50, 81]). Another important point is that this formula is universal, that is to say that it remains valid (in particular it still has the correct geometric meaning) under any specialization of the coefficient ring of the input polynomial system. This kind of property is particularly important for applications in the fields of number theory and arithmetic geometry where the value of the resultant is as important as its vanishing.

The discriminant of a homogeneous polynomial is also a fundamental tool in the field of computer algebra. Although the discriminant of the generic homogeneous polynomial of a given degree is irreducible, for some class of polynomials it can be decomposed and this decomposition is always deeply connected to the geometric properties of the class of polynomials. The second main contribution of this paper is a decomposition of the discriminant of a homogeneous symmetric polynomial (Theorem 5). The work on this result was motivated by the unpublished note [81] by N. Perminov and S. Shakirov where a tentative formula is given without a complete proof. We emphasize that the discriminant formula is obtained as a byproduct of our first formula on the resultant of a $\mathfrak{S}_n$-equivariant polynomial system. Therefore, it inherits the same features : it allows to split the discriminant into several resultants with multiplicities and it is universal.

The paper is organized as follows. In Section 5.2 we state the main result of this paper, namely a decomposition formula of a $\mathfrak{S}_n$-equivariant homogeneous polynomial system, and we also introduce the notions and notations that are needed (divided differences and partitions). The proof of this decomposition formula is provided in Section 5.4. The decomposition formula of the discriminant of a homogeneous symmetric polynomial is proved and discussed in Section 5.3.

5.2 The main result

In order to describe our main result, we first need to introduce some notations on divided differences and partitions. Hereafter, R denotes an arbitrary commutative ring. In addition, for any integer p the set $\{1, 2, \ldots, p\}$ will be denoted by $[p]$ and given a finite set I, $|I|$ will stand for its cardinality.

5.2.1 Notations

5.2.1.1 Divided differences

Let $P_1, ..., P_n$ be n homogeneous polynomials in $R[x_1, \ldots, x_n]$ of the same degree $d > 1$. Their divided differences are recursively defined by $P^{\{i\}} := P_i$ for all $i = 1, \ldots, n$ and

$$P^{\{i_1,\ldots,i_k\}} := \frac{P^{\{i_1,\ldots,i_{k-1}\}} - P^{\{i_1,\ldots,i_{k-2},i_k\}}}{x_{i_{k-1}} - x_{i_k}}$$

for any given set of (distinct) integers $I := \{i_1, \ldots, i_k\} \subset [n]$. It is well known that P^I depends on the set I and not on the order of the integers $i_1, \ldots, i_k$ for instance, as a consequence of the Newton's interpolation formula. Another important property is the following : if P^I are polynomials for all I such that $|I| = 2$, that is to say if

$$x_i - x_j \text{ divides } P^{\{i\}} - P^{\{j\}} \text{ for all } i, j \in [n], \tag{5.1}$$

then P^I are homogeneous polynomials for all $I \subset [n]$. Indeed, for any $J \subset [n]$ and any triple of distinct integers i, j, k such that $J \cap \{i, j, k\} = \emptyset$, a straightforward application of the definition of divided differences yields the equality

$$(x_i - x_j)P^{J\cup\{i,j\}} - (x_i - x_k)P^{J\cup\{i,k\}} + (x_j - x_k)P^{J\cup\{j,k\}} = 0$$

which can be rewritten as

$$(x_i - x_k)\left(P^{J\cup\{i,j\}} - P^{J\cup\{i,k\}}\right) = (x_j - x_k)\left(P^{J\cup\{i,j\}} - P^{J\cup\{j,k\}}\right).$$

From here the claimed property follows by induction on $|I|$. In addition, we observe that P^I is an homogeneous polynomial of degree $d - |I| + 1$. In particular, $P^I = 0$ if $d + 1 < |I| \leqslant n$ and $P^I = P^J$ for all subsets I and J of $[n]$ such that $|I| = |J| = d + 1 \leqslant n$.

Example 5.2.1. Any polynomial system of three linear homogeneous polynomials in 3 variables satisfying (5.1) is of the form

$$\begin{cases} P^{\{1\}} &= (a+d)x_1 + bx_2 + cx_3 \\ P^{\{2\}} &= ax_1 + (b+d)x_2 + cx_3 \\ P^{\{3\}} &= ax_1 + bx_2 + (c+d)x_3. \end{cases}$$

and straightforward computations show that $P^{\{1,2\}} = P^{\{1,3\}} = P^{\{2,3\}} = d$ and $P^{\{1,2,3\}} = 0$. □

5.2.1.2 $\mathfrak{S}_n$-equivariant polynomial systems

Consider a polynomial system of n homogeneous polynomials $F^{\{1\}}, \ldots, F^{\{n\}} \in R[x_1, \ldots, x_n]$ of the same degree $d \geqslant 1$ and assume that it is $\mathfrak{S}_n$-equivariant, that is to say that for any integer $i \in \{1, 2, \ldots, n\}$ and any permutation $\sigma \in \mathfrak{S}_n$

$$\sigma(F^{\{i\}}) := F^{\{i\}}(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = F^{\{\sigma(i)\}}(x_1, x_2, \ldots, x_n). \tag{5.2}$$

Equivalently, this means that for all $i = 1, \ldots, n$

$$F^{\{i\}}(x_1, \ldots, x_n) = \sum_{l=0}^{d} x_i^l S_l(x_1, \ldots, x_n)$$

where S_l is a symmetric homogeneous polynomials in $R[x_1, \ldots, x_n]$ of degree $d - l$ for all $l = 0, \ldots, d$. Suppose given in addition a partition $\lambda \vdash n$ and consider the morphism of polynomial algebras

$$\begin{array}{rcl} \rho_\lambda : R[x_1, \ldots, x_n] & \to & R[y_1, \ldots, y_{l(\lambda)}] \\ F(x_1, \ldots, x_n) & \mapsto & F(\underbrace{y_1, \ldots, y_1}_{\lambda_1}, \underbrace{y_2, \ldots, y_2}_{\lambda_2}, \ldots, \underbrace{y_{l(\lambda)}, \ldots, y_{l(\lambda)}}_{\lambda_{l(\lambda)}}) \end{array}$$

where $y_1, y_2, \ldots, y_{l(\lambda)}$ are new indeterminates. Since the polynomials $F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}$ satisfy (5.2), they also satisfy (5.1) (but this is not equivalent as shown in Example 5.2.1) and hence their divided differences F^I, $I \subset [n]$, are also polynomials. Moreover, it is easy to check that for any subset $\{i_1, \ldots, i_k\} \subset [n]$ and any permutation $\sigma \in \mathfrak{S}_n$

$$\sigma\left(F^{\{i_1, \ldots, i_k\}}\right) = F^{\{\sigma(i_1), \ldots, \sigma(i_k)\}}. \tag{5.3}$$

Now, observe that if $\rho_\lambda(x_i) = \rho_\lambda(x_j)$ then $\rho_\lambda(F^{\{i\}}) = \rho_\lambda(F^{\{j\}})$, so for any integer $i \in [l(\lambda)]$ we can define without ambiguity the homogeneous polynomial of degree d

$$F_\lambda^{\{i\}}(y_1, y_2, \ldots, y_{l(\lambda)}) := \rho_\lambda\left(F^{\{j\}}(x_1, \ldots, x_n)\right)$$

where $j \in [n]$ is such that $\rho_\lambda(x_j) = y_i$. Moreover, these polynomials also satisfy (5.1) and hence their divided differences are also polynomials; we will denote them by $F_\lambda^I(y_1, \ldots, y_{l(\lambda)})$, where $I \subset [l(\lambda)]$. Moreover, we have the following 'lifting" property : Given $I = \{i_1, \ldots, i_k\} \subset [n]$, define $J = \{j_1, \ldots, j_k\} \subset [l(\lambda)]$ by the equality $\rho_\lambda(x_{i_r}) = y_{j_r}$ for all $r \in [k]$. Then, if $|J| = |I|$ we have that

$$\rho_\lambda(F^I(x_1, \ldots, x_n)) = F_\lambda^J(y_1, \ldots, y_{l(\lambda)}).$$

5.2.2 The decomposition formula

We are now ready to state the main result of this paper, namely a decomposition of the multivariate resultant of a $\mathfrak{S}_n$-equivariant system of homogeneous polynomials of the same degree.

Theorem 4. *Assume $n \geqslant 2$ and suppose given a $\mathfrak{S}_n$-equivariant system of homogeneous polynomials $F^{\{1\}}, \ldots, F^{\{n\}} \in R[x_1, \ldots, x_n]$ of the same degree $d \geqslant 1$. Then, we have that*

$$\text{Res}\left(F^{\{1\}}, \ldots, F^{\{n\}}\right) = R_0 \times \prod_{\substack{\lambda \vdash n \\ l(\lambda) \leqslant d}} \text{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \ldots, F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}}\right)^{m_\lambda}$$

where $R_0 = 1$ *if* $d \geqslant n$ *and* $R_0 = \left(F^{\{1,\ldots,d+1\}}\right)^{m_0}$ *if* $d < n$. *In this latter case, the integer* m_0 *is defined by*

$$m_0 = nd^{n-1} - \sum_{k=1}^{d} A_{n,k} B_{d,k}$$

where

$$A_{n,k} := \sum_{\substack{\lambda \vdash n \\ l(\lambda)=k}} m_\lambda, \quad B_{d,k} := e_{k-1}(d, d-1, d-2, \ldots, d-k+1)$$

and where e_{k-1} *stands for the* $(k-1)$*-th elementary symmetric polynomial in* k *variables.*

Before giving the proof of this theorem which is postponed at the end of the chapter, in Section 5.4, we make observations on some computational aspects of this theorem. First, we emphasize that the above formula is *universal*, meaning that it holds in the ring of coefficients of the polynomials system $F^{\{1\}}, \ldots, F^{\{n\}}$ over $\mathbb{Z}$ and that it remains valid under any specialization of these coefficients. For that purpose, we use the formalism of the resultant as developed in [64] (see also [71, Chapter IX] and [22, Chapter 3]), in particular the resultant is normalized by setting $\mathrm{Res}(x_1, \ldots, x_n) = 1$. Besides that, we will also use many computation rules and properties of the resultant in the proof of Theorem 4.

The number of resultant factors appearing in the decomposition formula is in relation with the cardinality of the set of partitions of n. This quantity has been extensively studied and we refer the interested reader to the classical book [68]. These resultant factors can be computed separately, for instance by means of the Macaulay formula, but the situation is even better : all these factors can be deduced from a very small number of resultant computations since they are actually universal with respect to the integers $\lambda_1, \lambda_2, \ldots, \lambda_{l(\lambda)}$ defining a partition, providing $l(\lambda)$ is fixed. As a consequence, all the resultant factors appearing in the decomposition formula given in Theorem 4 can be obtained as specializations of only $\min\{n, d\}$ resultant computations. The following example illustrates this property.

Example 5.2.2. Consider the polynomials

$$F^{\{i\}}(x_1, \ldots, x_n) = ax_i^2 + bx_i e_1(x_1, \ldots, x_n) + ce_1(x_1, \ldots, x_n)^2 + de_2(x_1, \ldots, x_n), \quad i = 1, \ldots, n.$$

The partition $\lambda = (n)$ yields the factor

$$\mathrm{Res}\left(F_\lambda^{\{1\}}\right) = a + nb + n^2 c + \binom{n}{2} d$$

with multiplicity $m_\lambda = 1$. From Theorem 4 we know that the other factors come from the partitions of length 2. They are of the form $\lambda = (m, n-m)$ with $n-1 \geqslant m \geqslant n-m \geqslant 1$. The divided difference $F^{\{1,2\}}$ is equal to $a(x_1 + x_2) + be_1$ and we have

$$\rho_\lambda(e_1) = mx_1 + (n-m)x_2, \quad \rho_\lambda(e_2) = \binom{m}{2} x_1^2 + m(n-m)x_1 x_2 + \binom{n-m}{2} x_2,$$

$$F_\lambda^{\{1,2\}} = \rho_\lambda\left(F^{\{1,2\}}\right) = a(x_1+x_2) + b\rho_\lambda(e_1) = a(x_1+x_2) + b(mx_1 + (n-m)x_2).$$

Therefore, such a partition $\lambda = (m, n-m)$ yields the factor

$$\begin{aligned}\text{Res}\left(F^{\{1\}}_{(m,n-m)}, F^{\{1,2\}}_{(m,n-m)}\right) = {} & ab^2nm + 2\,dm^2ab - 1/2\,dmb^2n^2 + 1/2\,dm^2b^2n - 2\,dmna^2 - 4\,cmna^2 \\ & - 2\,dmabn + 1/2\,dn^2a^2 + 2\,dm^2a^2 + a^2bn - 1/2\,dna^2 + cn^2a^2 + 4\,cm^2a^2 - ab^2m^2 + a^3\end{aligned} \tag{5.4}$$

which is computed as the determinant of a 3×3 Sylvester matrix. To summarize, if $n = 2$ (and $d = 2$) we get

$$\text{Res}(F^{\{1\}}, F^{\{2\}}) = \text{Res}\left(F^{\{1\}}_{(2)}\right)\text{Res}\left(F^{\{1\}}_{(1,1)}, F^{\{1,2\}}_{(1,1)}\right) = (a+2b+4c+d)\,(a+b)^2\,(a-d)$$

where $\text{Res}\left(F^{\{1\}}_{(1,1)}, F^{\{1,2\}}_{(1,1)}\right)$ is obtained by specialization of (5.4). If $n > 2$ (and $d = 2$) then it is easy to check that $F^{\{1,2,3\}} = a$. Therefore, if $n = 2k+1$, k being a positive integer, then

$$\text{Res}(F^{\{1\}}, F^{\{2\}}) = (a)^{m_0}\left(a + nb + n^2c + \binom{n}{2}d\right)\prod_{m=k+1}^{n-1}\text{Res}\left(F^{\{1\}}_{(m,n-m)}, F^{\{1,2\}}_{(m,n-m)}\right)^{\frac{n!}{m!(n-m)!}}$$

where the resultants in this formula are again given by (5.4) and

$$m_0 = n2^{n-1} - 1 - 3\sum_{m=k+1}^{n-1}\frac{n!}{m!(n-m)!}$$

(for $B_{2,1} = 1$, $B_{2,2} = 3$, $A_{n,1} = 1$ and $A_{n,2} = \sum_{m=k+1}^{n-1}\frac{n!}{m!(n-m)!}$.) If $n = 2k$ with $k > 1$ then

$$\begin{aligned}\text{Res}(F^{\{1\}}, F^{\{2\}}) = (a)^{m_0}\left(a + nb + n^2c + \binom{n}{2}d\right)\text{Res}\left(F^{\{1\}}_{(k,k)}, F^{\{1,2\}}_{(k,k)}\right)^{\frac{1}{2}\frac{n!}{(k!)^2}} \times \\ \prod_{m=k+1}^{n-1}\text{Res}\left(F^{\{1\}}_{(m,n-m)}, F^{\{1,2\}}_{(m,n-m)}\right)^{\frac{n!}{m!(n-m)!}}\end{aligned}$$

where the resultants in this formula are always given by (5.4) and

$$m_0 = n2^{n-1} - 1 - \frac{3}{2}\frac{n!}{(k!)^2} - 3\sum_{m=k+1}^{n-1}\frac{n!}{m!(n-m)!}.$$

Before closing this example, we emphasize that the resultants appearing in Theorem 4 are not always irreducible polynomials. For instance, in the case where $n = 2k$ we have that

$$\text{Res}\left(F^{\{1\}}_{(k,k)}, F^{\{1,2\}}_{(k,k)}\right) = (a+bk)^2(a-dk). \tag{5.5}$$

However, we notice that $\text{Res}(F^{\{1\}}_\lambda)$ is obviously always irreducible. □

From a geometric point of view, Theorem 4 shows that the solutions of the algebraic polynomial system

$$\{F^{\{1\}} = 0, \ldots, F^{\{n\}} = 0\} \tag{5.6}$$

can be decomposed into several components that correspond to the algebraic systems

$$\{F_\lambda^{\{1\}} = 0, \ldots, F_\lambda^{\{1,\ldots,l(\lambda)\}} = 0\},\ \lambda \vdash n,\ l(\lambda) \leqslant d.$$

Each component has multiplicity m_λ and it corresponds to a particular configuration of the roots of the initial system, namely the roots whose coordinates can be grouped, up to permutations, into $l(\lambda)$ blocks of identical value and of size $\lambda_1, \ldots, \lambda_{l(\lambda)}$ respectively.

The component corresponding to the partition $\lambda = (1, \ldots, 1)$ is interesting for some applications as it corresponds to solutions of (5.6) whose coordinates are all distinct (e.g. [50]). A usual trick for dealing with this component is to sum up all the divided differences of the same order to get symmetric polynomials. More precisely, since the polynomials $F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}$ satisfy the property (5.3), for any integer $k \in [n]$ the polynomials

$$\sum_{I \subset [n],\, |I|=k} F^I = \sum_{I \subset [n],\, |I|=k} F^{\sigma(I)} = \sum_{I \subset [n],\, |I|=k} \sigma(F^I) = \sigma\left(\sum_{I \subset [n],\, |I|=k} F^I\right)$$

are symmetric (i.e. invariant under the action of $\mathfrak{S}_n$). As such, they can be rewritten by using the elementary symmetric polynomials and the number of roots of the component corresponding to $\lambda = (1, \ldots, 1)$ is hence reduced by a factor $n!$. In general, the above property is no longer true if we consider F_λ^I instead of F^I, $\lambda \neq (1, 1, \ldots, 1)$. Nevertheless, it is possible to reformulate Theorem 4 by means of these sums of divided differences of the same order.

Proposition 5.2.3. *Take again the notation of Theorem 4. Let λ be a partition of n such that $l(\lambda) \leqslant d$ and for all integer $k \in [l(\lambda)]$ define the polynomial*

$$\mathcal{F}_\lambda^{(k)} := \frac{1}{\binom{l(\lambda)}{k}} \sum_{I \subset [l(\lambda)],\, |I|=k} F_\lambda^I$$

(assuming that the coefficient ring contains the rational numbers). Then, we have that

$$\mathsf{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \ldots, F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}}\right) = \mathsf{Res}\left(\mathcal{F}_\lambda^{(1)}, \mathcal{F}_\lambda^{(2)}, \ldots, \mathcal{F}_\lambda^{(l(\lambda))}\right).$$

Proof. First, we claim that for any subset $I \subset [l(\lambda)]$ such that $|I| = l(\lambda) - 1$ then

$$F_\lambda^I = F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}} \mod \left(F_\lambda^{\{1,2,\ldots,l(\lambda\})}\right). \tag{5.7}$$

This is a consequence of the technical Lemma 5.2.4 which is given after the proof of this proposition. From (5.7) we deduce that

$$\sum_{I \subset [l(\lambda)],\, |I|=l(\lambda)-1} F_\lambda^I = l(\lambda)\, F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}} \mod \left(F_\lambda^{\{1,2,\ldots,l(\lambda\})}\right).$$

In the same way, for any subset $I \subset [l(\lambda)]$ such that $|I| = l(\lambda) - 2$, Lemma 5.2.4 shows that

$$F_\lambda^I = F_\lambda^{\{1,2,\ldots,l(\lambda)-2\}} \mod \left(\left\{ F_\lambda^I \right\}_{|I|=l(\lambda)-1}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}} \right).$$

Using (5.7), this equality can be simplified to give

$$F_\lambda^I = F_\lambda^{\{1,2,\ldots,l(\lambda)-2\}} \mod \left(F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}} \right).$$

We deduce that

$$\sum_{I \subset [l(\lambda)],\, |I|=l(\lambda)-2} F_\lambda^I = \binom{l(\lambda)}{2} F_\lambda^{\{1,2,\ldots,l(\lambda)-2\}} \mod \left(F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}} \right).$$

By applying iteratively this method, we obtain for all $k = 1, \ldots, l(\lambda) - 1$ the equality

$$\sum_{I \subset [l(\lambda)],\, |I|=l(\lambda)-k} F_\lambda^I = \binom{l(\lambda)}{k} F_\lambda^{\{1,2,\ldots,l(\lambda)-k\}} \mod \left(F_\lambda^{\{1,2,\ldots,l(\lambda)-k+1\}}, \ldots, F_\lambda^{\{1,2,\ldots,l(\lambda)\}} \right).$$

From these equalities, the invariance of the resultant under elementary transformations yields the claimed result (proceed from the right to the left). □

Lemma 5.2.4. *Using the notation of Section 5.2.1.1, let I and J be two subsets of $[n]$ of the same cardinality r with $1 \leqslant r \leqslant n-1$. Then, the polynomial $P^I - P^J$ belongs to the ideal of polynomials generated by the $(r+1)^{\text{th}}$ divided differences, i.e.*

$$P^I - P^J \in (\ldots, P^K, \ldots)_{K \subset [n], |K|=r+1}.$$

Proof. If $|I \cap J| = r-1$ then $P^I - P^J$ is a multiple of a divided difference P^K with $|K| = r+1$ by definition of divided differences (by choosing the appropriate order for the elements of I and J). Otherwise, $r \geqslant 2$, $|I \cap J| < r-1$ and hence there exist $j \in J \setminus I$ and $i \in I \setminus J$ (observe that $i \neq j$ necessarily). Now,

$$P^I - P^J = P^I - P^{(I \setminus \{i\}) \cup \{j\}} + P^{(I \setminus \{i\}) \cup \{j\}} - P^J$$

where the term $P^I - P^{(I \setminus \{i\}) \cup \{j\}}$ is a multiple of a divided difference P^K with $|K| = r+1$ since $|I \cap ((I \setminus \{i\}) \cup \{j\}))| = r-1$. So, to prove that $P^I - P^J$ belongs to the ideal generated by the $(r+1)^{\text{th}}$ divided differences amounts to prove that $P^{(I \setminus \{i\}) \cup \{j\}} - P^J$ belongs to this ideal. But notice that $|J \cap ((I \setminus \{i\}) \cup \{j\})| = |I \cap J| + 1$. Therefore, one can repeat this operation to reach a cardinality of $r-1$ and from there the conclusion follows. □

5.3 Discriminant of a homogeneous symmetric polynomial

The discriminant of a homogeneous polynomial is a rather complicated object which is known to be irreducible as a polynomial in the coefficients of the input polynomial (see for instance [13, §4] and [25, 54]). In this section, we will show that it decomposes if

the homogeneous polynomial is assumed to be symmetric. We will actually provide a decomposition formula (Theorem 5) that we will obtain as a particular case of our main result (Theorem 4).

Fix a positive integer $n \geqslant 2$. For any integer p we will denote by $e_p(x_1, \ldots, x_n)$ the p^{th} elementary symmetric polynomial in the variables $x_1, \ldots, x_n$. They satisfy the equality

$$\sum_{p \geqslant 0} e_p(x) t^p = \prod_{i=1}^{n} (1 + x_i t)$$

(observe that $e_0(x) = 1$ and that $e_p(x) = 0$ for all $p > n$). For any partition $\lambda = (\lambda_1 \geqslant \cdots \geqslant \lambda_k)$ we also define the polynomial

$$e_\lambda(x) := e_{\lambda_1}(x) e_{\lambda_2}(x) \cdots e_{\lambda_k}(x) \in \mathbb{Z}[x_1, \ldots, x_n].$$

Given a positive integer d, it is well known that the set

$$\{e_\lambda(x) \ : \ \lambda = (\lambda_1, \ldots, \lambda_k) \vdash d \text{ such that } n \geqslant \lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_k\} \tag{5.8}$$

is a basis (over $\mathbb{Z}$) of the homogeneous symmetric polynomials of degree d in n variables. In other words, any homogeneous symmetric polynomial of degree d with coefficients in a commutative ring is obtained as specialization of the generic homogeneous symmetric polynomial of degree d

$$F(x_1, \ldots, x_n) := \sum_{\lambda \vdash d} c_\lambda e_\lambda(x) \in \mathbb{Z}[c_\lambda : \lambda \vdash d][x_1, \ldots, x_n]. \tag{5.9}$$

We will denote by $\mathbb{U}$ its universal ring of coefficients $\mathbb{Z}[c_\lambda \ : \ \lambda \vdash d]$. In addition, for all $i \in \{1, \ldots, n\}$, we will denote the partial derivatives of F by

$$F^{\{i\}}(x_1, \ldots, x_n) := \frac{\partial F}{\partial x_i}(x_1, \ldots, x_n) \in \mathbb{U}[x_1, \ldots, x_n]_{d-1}.$$

Finally, we recall that the discriminant of F, denoted $\Delta(F)$, is defined by the equality

$$d^{a(n,d)} \Delta(F) = \text{Res}\left(F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}\right) \in \mathbb{U} \tag{5.10}$$

where

$$a(n, d) := \frac{(d-1)^n - (-1)^n}{d} \in \mathbb{Z}.$$

It is an homogeneous polynomial of degree $n(d-1)^{n-1}$ in $\mathbb{U}$. The integer factor $d^{a(n,d)}$ is important to ensure that the discriminant $\Delta(F)$ yields the expected smoothness criterion under any specialization (especially in coefficient rings having nonzero characteristic), namely : Let S be an algebraically closed field and g be a nonzero homogeneous polynomial in $S[x_1, \ldots, x_n]$, then $\Delta(g) = 0$ if and only if the hypersurface defined by the polynomial g in the projective space $\mathbb{P}_S^{n-1}$ is singular. For a detailed study of the discriminant and its numerous properties, mostly inherited from the ones of the resultant, we refer the reader to [13, 25, 54] and the references therein.

Lemma 5.3.1. *The partial derivatives $F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}$ of the symmetric polynomial F form a $\mathfrak{S}_n$-equivariant system of homogeneous polynomials of degree $d-1$.*

Proof. Since F is a polynomial in the elementary symmetric polynomials, the chain rule formula for the derivation of composed functions shows that there exist $\min\{d,n\}$ homogeneous symmetric polynomials $S_k(x_1,\ldots,x_n)$ such that for all $i=1,\ldots,n$

$$F^{\{i\}} = \frac{\partial F}{\partial x_i} = \sum_{k=1}^{\min\{d,n\}} \frac{\partial e_k}{\partial x_i} S_k(x_1,\ldots,x_n). \tag{5.11}$$

Moreover, for any pair of integers i,j we have

$$\frac{\partial e_j}{\partial x_i} = \sum_{r=0}^{j-1} (-1)^r x_i^r e_{j-1-r}. \tag{5.12}$$

Therefore, we deduce that $\sigma\left(F^{\{i\}}\right) = F^{\{\sigma(i)\}}$ for any $\sigma \in \mathfrak{S}_n$, as claimed. □

As a consequence of this lemma, Theorem 4 can be applied in order to decompose the resultant of the polynomials $F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}$ and hence, by (5.10), to decompose the discriminant of the symmetric polynomial F. We take again the notation of Theorem 4.

Theorem 5. *Assume that $n \geqslant 2$ and $d \geqslant 2$. With the above notation, we have that*

$$d^{a(n,d)}\Delta(F) = R_0 \times \prod_{\substack{\lambda \vdash n \\ l(\lambda)<d}} \mathrm{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \ldots, F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}}\right)^{m_\lambda}$$

where $R_0 = 1$ if $d > n$ and $R_0 = \left(F^{\{1,\ldots,d\}}\right)^{m_0}$ if $d \leqslant n$. In this latter case, m_0 is defined by

$$m_0 := n(d-1)^{n-1} - \sum_{k=1}^{d-1} A_{n,k} B_{d-1,k}$$

where

$$A_{n,k} := \sum_{\substack{\lambda \vdash n \\ l(\lambda)=k}} m_\lambda, \quad B_{d-1,k} := e_{k-1}(d-1, d-2, \ldots, d-k),$$

and if F is given explicitly by (5.9) *then $F^{\{1,\ldots,d\}} = (-1)^{d-1} c_{(d)}$.*

Proof. All these formulas are obtained by specialization of the formulas given in Theorem 4 with the difference that the polynomials $F^{\{i\}}$, $i=1,\ldots,n$ are of degree $d-1$ whereas they are of degree d as in Theorem 4. □

We emphasize that the formula given in this theorem is independent of the choice of basis that is used to represent F, although we have chosen the basis (5.8) for illustrations. We also mention that the formula given in Proposition 5.2.3 also applies here (this is actually

the point of view used in [81]). Below, we give two examples corresponding to low degree polynomials, namely the cases $d = 2$ and $d = 3$. In these two cases the number of variables n is large compared to d and the formulas given in Theorem 5 are hence computationally very interesting since a resultant computation in n variables is replaced by several resultant computations in at most d variables.

Case $\mathbf{n \geqslant d = 2}$ The generic homogeneous polynomial of degree 2 can be written as

$$F = c_{(2)}e_2 + c_{(1,1)}e_1^2.$$

Its derivatives are

$$F^{\{i\}} = c_{(2)}\frac{\partial e_2}{\partial x_1} + 2c_{(1,1)}e_1\frac{\partial e_1}{\partial x_1} = c_{(2)}(e_1 - x_1) + 2c_{(1,1)}e_1$$

and hence we deduce that

$$\mathsf{Res}\left(F_{(2)}^{\{1\}}\right) = (n-1)c_{(2)} + 2nc_{(1,1)}.$$

Observe that this polynomial is not irreducible over $\mathbb{Z}[c_{(2)}, c_{(1,1)}]$ if n is odd since it is divisible by 2. It is also not hard to check that $m_{(2)} = 1$ and $m_0 = n-1$ here. Finally, since $a(n,2) = 0$ if n is even and $a(n,2) = 1$ if n is odd, we get

$$\Delta(F) = \begin{cases} -c_{(2)}^{n-1}\left((n-1)c_{(2)} + 2nc_{(1,1)}\right) & \text{if } n \text{ is even,} \\ c_{(2)}^{n-1}\left(\frac{n-1}{2}c_{(2)} + nc_{(1,1)}\right) & \text{if } n \text{ is odd .} \end{cases}$$

Case $\mathbf{n \geqslant d = 3}$ Consider the generic homogeneous polynomial of degree 3

$$F = c_{(3)}e_3 + c_{(2,1)}e_2e_1 + c_{(1,1,1)}e_1^3.$$

The formula given in Theorem 5 shows that

$$3^{\frac{2^n-(-1)^n}{3}}\Delta(F) = c_{(3)}^{m_0}\mathsf{Res}\left(F_{(n)}^{\{1\}}\right)\prod_{k=1}^{\lfloor\frac{n}{2}\rfloor}\mathsf{Res}\left(F_{(n-k,k)}^{\{1\}}, F_{(n-k,k)}^{\{1,2\}}\right)^{m_{(n-k,k)}}$$

where all the factors can be described explicitly. To begin with, from (5.11) and (5.12) we get that for all $i = 1, \ldots, n$

$$F^{\{i\}} = c_{(3)}\left(e_2 - x_ie_1 + x_i^2\right) + c_{(2,1)}\left(e_2 + e_1(e_1 - x_i)\right) + 3c_{(1,1,1)}e_1^2.$$

It follows immediately that

$$\mathsf{Res}\left(F_{(n)}^{\{1\}}\right) = \binom{n-1}{2}c_{(3)} + 3\binom{n}{2}c_{(2,1)} + 3n^2c_{(1,1,1)}.$$

Now, let $(n-k,k)$ be a partition of length 2 of n. A straightforward computation shows that for any pair of distinct integers i,j we have

$$F^{\{i,j\}} = c_{(3)}\left(x_i + x_j - e_1\right) - c_{(2,1)}e_1$$

and we deduce, by means of a single (Sylvester) resultant computation that

$$\begin{aligned}\text{Res}\left(F^{\{1\}}_{(n-k,k)}, F^{\{1,2\}}_{(n-k,k)}\right) &= c_{(3)}^2\left(\binom{n-1}{2}c_{(3)} + 3\binom{n}{2}c_{(2,1)} + 3n^2c_{(1,1,1)}\right)\\ &- \frac{1}{2}k(n-k)\left((n-2)\,c_{(3)}^3 + \left(24c_{(1,1,1)} + 3nc_{(2,1)}\right)c_{(3)}^2 + (3n-6)\,c_{(2,1)}^2c_{(3)} + nc_{(2,1)}^3\right).\end{aligned}$$

The multiplicity $m_{(n-k,k)}$ are equal to the binomial $\binom{n}{k}$ for all $k = 1,\ldots,\lfloor\frac{n}{2}\rfloor$ except if n is even and $k = \frac{n}{2}$ in which case $m_{(\frac{n}{2},\frac{n}{2})} = \frac{1}{2}\binom{n}{\frac{n}{2}}$. Finally, it remains to determine the integer m_0. We have

$$m_0 = n2^{n-1} - m_{(n)} - 3\sum_{\substack{\lambda\vdash n\\ l(\lambda)=2}} m_\lambda = n2^{n-1} - 1 - 3\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor} m_{(n-k,k)}.$$

But since

$$2\sum_{k=1}^{\lfloor\frac{n}{2}\rfloor} m_{(n-k,k)} = \sum_{k=1}^{n-1}\binom{n}{k} = 2^n - 2 = 2(2^{n-1}-1),$$

we finally deduce that

$$m_0 = (n-3)2^{n-1} + 2.$$

To illustrate this general formula, we check the two particular cases $n=3$ and $n=4$. If $n=3$, we obtain

$$\Delta(F) = {c_{(3)}}^2\left(c_{(3)} + 9\,c_{(2,1)} + 27\,c_{(1,1,1)}\right)\left(-{c_{(2,1)}}^2c_{(3)} - {c_{(2,1)}}^3 + c_{(1,1,1)}{c_{(3)}}^2\right)^3$$

where

$$\text{Res}\left(F^{\{1\}}_{(3)}\right) = \left(c_{(3)} + 9\,c_{(2,1)} + 27\,c_{(1,1,1)}\right),\ m_{(3)} = 1$$

and

$$\text{Res}\left(F^{\{1\}}_{(2,1)}, F^{\{1,2\}}_{(2,1)}\right) = 3\left(-{c_{(2,1)}}^2c_{(3)} - {c_{(2,1)}}^3 + c_{(1,1,1)}{c_{(3)}}^2\right),\ m_{(2,1)} = 3.$$

If $n=4$ we get

$$\begin{aligned}\Delta(F) = -{c_{(3)}}^{10}\left(c_{(3)} + 2\,c_{(2,1)}\right)^9\left(6\,c_{(2,1)} + 16\,c_{(1,1,1)} + c_{(3)}\right)\times\\ \left(4\,c_{(1,1,1)}{c_{(3)}}^2 - 3\,{c_{(2,1)}}^2c_{(3)} - 2\,{c_{(2,1)}}^3\right)^4 \quad (5.13)\end{aligned}$$

where

$$\text{Res}\left(F^{\{1\}}_{(4)}\right) = 3\left(6\,c_{(2,1)} + 16\,c_{(1,1,1)} + c_{(3)}\right),\ m_{(4)} = 1,$$

$$\text{Res}\left(F^{\{1\}}_{(3,1)}, F^{\{1,2\}}_{(3,1)}\right) = 3\left(4\,c_{(1,1,1)}{c_{(3)}}^2 - 3\,{c_{(2,1)}}^2c_{(3)} - 2\,{c_{(2,1)}}^3\right),\ m_{(3,1)} = 4$$

and

$$\mathrm{Res}\left(F^{\{1\}}_{(2,2)}, F^{\{1,2\}}_{(2,2)}\right) = -\left(c_{(3)} + 2\,c_{(2,1)}\right)^3,\ m_{(2,2)} = 3. \tag{5.14}$$

For the Clebsch surface whose canonical equation is given by

$$h(x_1,x_2,x_3,x_4) = x_1^3 + x_2^3 + x_3^3 + x_4^3 - (x_1+x_2+x_3+x_4)^3 = 3e_3 - 3e_2e_1 = 0,$$

we recover that $h/3$ defines a smooth cubic in every characteristic except 5 (see [84, §5.4]). Indeed, (5.13) shows that

$$\Delta(h/3) = \Delta(e_3 - e_2e_1) = -(-1)^9(-6+1)(-3+2)^4 = -5.$$

Remark 5.3.2. Contrary to what was expected in [81], the resultant factors appearing in Theorem 5 are not always irreducible (see e.g. (5.14)). However, in all the experiments we noted that these resultant factors were always powers of irreducible polynomials (ground ring assumed to be a field), but we do not known if this is true in general. As an illustration, we notice that the resultant (5.5) appearing in Example 5.2.2 contains two irreducible and distinct factors, but it becomes a power of a single irreducible polynomial (over a field) when specialized to get the discriminant formula in the case $n \geqslant d = 3$. Indeed, comparing the notation in these two examples we get $d = -b = c_{(3)} + c_{(2,1)}$.

5.4 Proof of the Main Theorem

We take again the notation of Section 5.2. We begin by splitting the resultant of the $F^{\{i\}}$'s into several factors by means of their divided differences. This process can be divided into steps where we increase iteratively the order of the divided differences. Thus, in the first step we make use of the first order divided differences and write

$$\begin{aligned}\mathrm{Res}\left(F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}\right) = \\ \pm\,\mathrm{Res}\left(F^{\{1\}}, (x_1-x_2)F^{\{1,2\}}, (x_1-x_3)F^{\{1,3\}}, \ldots, (x_1-x_n)F^{\{1,n\}}\right).\end{aligned} \tag{5.15}$$

The divided differences $F^{\{1,j\}}$ are of degree $d-1$. If $d-1=0$ then they are all equal to the same constant (see Section 5.2.1.1) and it is straightforward to check that we get the claimed formula in this case, that is to say

$$\mathrm{Res}\left(F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}\right) = \left(F^{\{1,2\}}\right)^{n-1}\mathrm{Res}\left(F^{\{1\}}_{(n)}\right) = \left(F^{\{1,2\}}\right)^{n-1} F^{\{1\}}(1,1,\ldots,1).$$

If $d-1>0$, then (5.15) shows that the resultant of the $F^{\{i\}}$'s splits into 2^{n-1} factors by using the multiplicativity property of the resultant : for each polynomial $(x_1-x_j)F^{\{1,j\}}$, $j = 2,\ldots,n$, there is a choice between (x_1-x_j) and the divided difference $F^{\{1,j\}}$. Thus, these factors are in bijection with the subsets of $[n]$ which contain 1. If $I_1 = \{1, i_2, i_3, \ldots, i_{n-k+1}\} \subset [n]$ is such a subset, then the corresponding factor is simply

$$\pm\mathrm{Res}\left(F^{\{1\}}, F^{\{1,j_1\}}, F^{\{1,j_2\}}, \ldots, F^{\{1,j_{k-1}\}}, x_1 - x_{i_2}, x_1 - x_{i_3}, \ldots, x_1 - x_{i_{n-k+1}}\right)$$

where $\{j_1, \ldots, j_{k-1}\} = [n] \setminus I_1$. Moreover, by the specialization property of the resultant this factor is equal to

$$\pm\text{Res}\left(F_1^{\{1\}}, F_1^{\{1,2\}}, F_1^{\{1,3\}}, \ldots, F_1^{\{1,k\}}\right) \tag{5.16}$$

where we set $F_1^{\{1,r\}} := \rho_{I_1}(F^{\{1,j_r\}})$, ρ_{I_1} being a specialization map defined by

$$\begin{array}{rcl} \rho_{I_1} : k[x_1, \ldots, x_n] & \to & k[x_1, \ldots, x_k] \\ x_j,\, j \in I_1 & \mapsto & x_1 \\ x_{j_r},\, r = 1, \ldots, k-1 & \mapsto & x_{r+1}. \end{array}$$

Roughly speaking, this amounts to put all the variables x_j, $j \in I_1$, in the "same box" and to renumber the other variables from 2 to k.

Now, one can proceed to the second step by introducing the second order divided differences. For that purpose, we start from the factor (5.16) obtained at the end of the previous step. If $k \leqslant 2$ the procedure stops. Otherwise, if $k > 2$ then we can proceed exactly as in the first step, since

$$(x_2 - x_j)F_1^{\{1,2,j\}} = F_1^{\{1,2\}} - F_1^{\{1,j\}},\ j = 3, \ldots, k,$$

we get

$$\begin{aligned} &\text{Res}\left(F_1^{\{1\}}, F_1^{\{1,2\}}, F_1^{\{1,3\}}, \ldots, F_1^{\{1,k\}}\right) = \\ &\qquad \pm\,\text{Res}\left(F^{\{1\}}, F^{\{1,2\}}, (x_2 - x_3)F^{\{1,2,3\}}, (x_2 - x_4)F^{\{1,2,4\}}, \ldots, (x_2 - x_k)F^{\{1,2,k\}}\right). \end{aligned}$$

So, we are exactly in the same setting as in the previous step and hence we split this factor similarly. As a result, the factors we obtain are in bijection with subsets I_2 of $[n]$ that contain 2 but not 1. After this second step is completed, then one can continue to the third step, and so on. This splitting process stops for a given factor if either it involves divided differences of distinct orders or either the order of some divided differences is higher than the degree d.

In summary, the above process shows that the resultant $\text{Res}\left(F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}\right)$ splits into factors that are in bijection with ordered collections of subsets $(I_1, \ldots, I_k)$ that satisfy the following three conditions :

- $1 \leqslant k \leqslant \min\{d, n\}$ and $\emptyset \neq I_j \subset [n]$ for all $j \in [k]$,
- $I_1 \coprod I_2 \coprod \ldots \coprod I_k = [n]$ (disjoint union, so this is a partition of $[n]$),
- $1 = \min(I_1) < \min(I_2) < \cdots < \min(I_k)$.

Definition 5.4.1. A collection of subsets $(I_1, \ldots, I_k)$ satisfying to the three above conditions will be called an *admissible partition* (of $[n]$).

Given an admissible partition $(I_1, \ldots, I_k)$, we define the specialization map

$$\begin{array}{rcl} \rho_{(I_1,\ldots,I_k)} : k[x_1, \ldots, x_n] & \to & k[x_1, \ldots, x_k] \\ x_r, r \in I_s & \mapsto & x_s \end{array}$$

and the polynomials $F^{\{1,2,\ldots,r\}}_{(I_1,\ldots,I_k)} := \rho_{(I_1,\ldots,I_k)}(F^{\{1,i_2,\ldots,i_r\}})$, $r = 1, \ldots, k$, where we set

$$i_1 := 1 = \mathsf{min}(I_1) < i_2 := \mathsf{min}(I_2) < \cdots < i_k := \mathsf{min}(I_k).$$

Then, the factor of the resultant of the $F^{\{i\}}$'s corresponding to the admissible partition $(I_1, \ldots, I_k)$ is given by

$$R_{(I_1,\ldots,I_k)} := \mathsf{Res}\left(F^{\{1\}}_{(I_1,\ldots,I_k)}, F^{\{1,2\}}_{(I_1,\ldots,I_k)}, \ldots, F^{\{1,2,\ldots,k\}}_{(I_1,\ldots,I_k)}\right).$$

Therefore, we proved that

$$\mathsf{Res}\left(F^{\{1\}}, F^{\{2\}}, \ldots, F^{\{n\}}\right) = \pm \left(F^{\{1,\ldots,d+1\}}\right)^{\mu} \times \prod_{(I_1,\ldots,I_k)} R_{(I_1,\ldots,I_k)} \tag{5.17}$$

where the product runs over all admissible partitions of $[n]$ and μ is an integer. Moreover, $\mu > 0$ if and only if $n > d$.

Now, we define an equivalence relation $\sim$ on the set of admissible partitions of $[n]$. Given two admissible partitions $(I_1, \ldots, I_k)$ and $(J_1, \ldots, J_{k'})$, we set

$$(I_1, \ldots, I_k) \sim (J_1, \ldots, J_{k'}) \Leftrightarrow \begin{cases} k = k' \text{ and} \\ \exists\, \sigma \in \mathfrak{S}_k \text{ such that } |I_l| = |J_{\sigma(l)}| \text{ for all } l \in [k]. \end{cases}$$

It is straightforward to check that this binary relation is reflexive, symmetric and transitive so that it defines an equivalence relation. We denote by $[(I_1, \ldots, I_k)]$ its equivalence classes. Consider the admissible partitions $(L_1, \ldots, L_k)$ such that

$$l_1 := |L_1| \geqslant l_2 := |L_2| \geqslant \ldots l_k := |L_k| \text{ and} \tag{5.18}$$

$$L_j := \left\{1 + \sum_{i=1}^{j-1} l_i, 2 + \sum_{i=1}^{j-1} l_i, \ldots, \sum_{i=1}^{j} l_i\right\} \text{ for all } j \in [k].$$

Obviously, there is exactly one such admissible partition in each equivalent class of $\sim$. Moreover, these admissible partitions are in bijection with the partitions $\lambda \vdash n$ of length k by setting $\lambda := (l_1, l_2, \ldots, l_k) \vdash n$. As a consequence, we deduce that there is a bijection between the equivalence classes of $\sim$ and the partitions $\lambda \vdash n$ of length k and we write

$$[\lambda] := [(I_1, \ldots, I_k)] = [(L_1, \ldots, L_k)].$$

Lemma 5.4.2. *Let λ be a partition of n, then the cardinality of the equivalence class $[\lambda]$ is m_λ.*

Proof. Let λ be a partition of n and consider the equivalent class $[\lambda]$. The multinomial coefficient (2.1) counts the different ways of filling $k = (\lambda)$ boxes $J_1, \ldots, J_k$ with λ_j elements in the box J_j. These choices take into account the order between the boxes, but not inside the boxes. These boxes J_j can obviously be identified with subsets of $[n]$. Moreover, there exists a unique permutation $\sigma \in \mathfrak{S}_k$ such that

$$1 = \mathsf{min}(J_{\sigma(1)}) < \mathsf{min}(J_{\sigma(2)}) < \cdots \mathsf{min}(J_{\sigma(k)})$$

and hence such that the collection of subsets $(J_{\sigma(1)}, J_{\sigma(2)}, \ldots, J_{\sigma(k)})$ is an admissible partition. Therefore, any choice for filling the boxes $J_1, \ldots, J_k$ can be associated to a factor in the decomposition. Conversely, such a factor is associated to an admissible partition $(I_1, \ldots, I_k)$, but there are possibly several choices, i.e. permutations in $\mathfrak{S}_k$, that give a way of filling the boxes $J_1, \ldots, J_k$: it is possible to permute boxes that have the same cardinality. Therefore, we conclude that the cardinality of the equivalent class represented by a partition $\lambda \vdash n$ is exactly m_λ. □

The following result shows that admissible partitions that are equivalents give the same factor, up to sign, in the splitting process.

Proposition 5.4.3. *Let λ be a partition of n. Then, for any admissible partition $(I_1, \ldots, I_k)$ such that $[\lambda] = [(I_1, \ldots, I_k)]$,*

$$R_{(I_1,\ldots,I_k)} = \pm\mathsf{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \ldots, F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}}\right).$$

Proof. Let $(I_1, \ldots, I_k)$ be an admissible partition and set

$$i_1 := 1 = \mathsf{min}(I_1) < i_2 := \mathsf{min}(I_2) < \cdots < i_k := \mathsf{min}(I_k).$$

Its corresponding factor in the splitting process is nothing but the resultant, up to sign, of the following list of n polynomials in the n variables $x_1, \ldots, x_n$:

$$F^{\{1\}}, F^{\{1,i_2\}}, \ldots, F^{\{1,i_2,\ldots,i_k\}}, \{x_{i_1} - x_r\}_{r\in I_1\setminus\{1\}}, \ldots, \{x_{i_k} - x_r\}_{r\in I_k\setminus\{i_k\}}. \tag{5.19}$$

Now, let $(J_1, J_2, \ldots, J_k)$ be another admissible partition such that $[(I_1, \ldots, I_k)] = [(J_1, J_2, \ldots, J_k)]$ and set

$$j_1 := 1 = \mathsf{min}(J_1) < j_2 := \mathsf{min}(J_2) < \cdots < j_k := \mathsf{min}(J_k).$$

The corresponding factor of $(J_1, J_2, \ldots, J_k)$ can be described similarly as the resultant, up to sign, of the polynomials

$$F^{\{1\}}, F^{\{1,j_2\}}, \ldots, F^{\{1,j_2,\ldots,j_k\}}, \{x_{j_1} - x_r\}_{r\in J_1\setminus\{1\}}, \ldots, \{x_{j_k} - x_r\}_{r\in J_k\setminus\{j_k\}}. \tag{5.20}$$

First, observe that it is sufficient to prove that $R_{(I_1,\ldots,I_k)} = \pm R_{(J_1,\ldots,J_k)}$ by assuming that $|I_{\sigma(l)}| = |J_l|$ for all $l \in [k]$ where σ is an elementary transposition (a permutation which exchanges two successive elements and keeps all the others fixed) in $\mathfrak{S}_k$. This is because

$\mathfrak{S}_k$ is generated by the elementary transpositions and because of the transitivity of $\sim$. So, let $s \in [k-1]$ and assume that

$$|I_s| = |J_{s+1}|,\ |I_{s+1}| = |J_s| \text{ and } |I_l| = |J_l| \text{ for all } l \in [k] \setminus \{s, s+1\}.$$

Let us choose a permutation $\tau \in \mathfrak{S}_n$ such that

$$\begin{cases} \tau(I_l) = J_l \text{ and } \tau(i_l) = j_l \text{ for all } l \in [k], \\ \tau(I_s) = J_{s+1} \text{ and } \tau(i_s) = j_{s+1}, \\ \tau(I_{s+1}) = J_s \text{ and } \tau(i_{s+1}) = j_s. \end{cases}$$

By the property (5.3), the application of τ on the list of polynomials (5.19) returns the following list of polynomials

$$\begin{aligned} F^{\{1\}}, F^{\{1,j_2\}}, \ldots, F^{\{1,j_2,\ldots,j_{s-1},j_{s+1}\}}, F^{\{1,j_2,\ldots,j_{s-1},j_s,j_{s+1}\}}, \ldots, F^{\{1,j_2,\ldots,j_k\}}, \\ \left\{x_{j_1} - x_r\right\}_{r \in J_1 \setminus \{1\}}, \ldots, \left\{x_{j_{s-1}} - x_r\right\}_{r \in J_{s-1} \setminus \{j_{s-1}\}}, \left\{x_{j_{s+1}} - x_r\right\}_{r \in J_{s+1} \setminus \{j_{s+1}\}}, \\ \left\{x_{j_s} - x_r\right\}_{r \in J_s \setminus \{j_s\}}, \ldots, \left\{x_{j_k} - x_r\right\}_{r \in J_k \setminus \{j_k\}}. \end{aligned} \quad (5.21)$$

By the invariance, up to sign, of the resultant under permutations of polynomials and variables, we get that the resultant of the list of polynomials (5.19), i.e. $R_{(I_1,\ldots,I_k)}$, is equal to the resultant of the list of polynomials (5.21) up to sign. Now, by definition of divided differences we have that

$$F^{\{1,j_2,\ldots,j_{s-1},j_s\}} = F^{\{1,j_2,\ldots,j_{s-1},j_{s+1}\}} + (x_{j_s} - x_{j_{s+1}}) F^{\{1,j_2,\ldots,j_{s-1},j_s,j_{s+1}\}}$$

so that the resultant of the polynomials (5.21) is equal, up to sign, to the resultant of the polynomials (5.20), i.e. $R_{(J_1,\ldots,J_k)}$, by invariance of the resultant under the above elementary transformation and permutations of polynomials. Therefore, we have proved that $R_{(I_1,\ldots,I_k)} = \pm R_{(J_1,\ldots,J_k)}$.

Finally, to conclude the proof, let $(L_1, \ldots, L_k)$ be the particular representative of the class $[\lambda] = [(I_1, \ldots, I_k)]$ as defined in (5.18). Then, it is clear by the definitions that $\rho_{(L_1,\ldots,L_k)} = \rho_\lambda$ and that

$$R_{(L_1,\ldots,L_k)} = \text{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \ldots, F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}}\right).$$

□

The comparison of (5.17), Lemma 5.4.2 and Proposition 5.4.3 shows that if $d \geqslant n$ then

$$\text{Res}\left(F^{\{1\}}, \ldots, F^{\{n\}}\right) = \pm \prod_{\lambda \vdash n} \text{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \ldots, F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}}\right)^{m_\lambda} \quad (5.22)$$

and if $n > d$ then

$$\begin{aligned} &\text{Res}\left(F^{\{1\}}, \ldots, F^{\{n\}}\right) = \\ &\qquad \pm \left(F^{\{1,\ldots,d+1\}}\right)^\mu \prod_{\substack{\lambda \vdash n \\ l(\lambda) \leqslant d}} \text{Res}\left(F_\lambda^{\{1\}}, F_\lambda^{\{1,2\}}, \ldots, F_\lambda^{\{1,2,\ldots,l(\lambda)-1\}}, F_\lambda^{\{1,2,\ldots,l(\lambda)\}}\right)^{m_\lambda}. \end{aligned} \quad (5.23)$$

To determine the integer μ, we compare the degrees with respect to the coefficients of the $F^{\{i\}}$'s. The resultant on the left side is homogeneous of degree d^{n-1} with respect to the coefficients of each polynomial $F^{\{i\}}$, so it is homogeneous of degree nd^{n-1} with respect to the coefficients of all the polynomials $F^{\{i\}}$, $i = 1, \ldots, n$. Given a partition $\lambda \vdash n$, $l(\lambda) \leqslant d$, the polynomial $F_\lambda^{\{1,2,\ldots,j\}}$, $1 \leqslant j \leqslant l(\lambda)$ is of degree $d - j + 1$. Therefore, the resultant associated to this partition λ is homogeneous with respect to the coefficients of the $F^{\{i\}}$'s of degree

$$\sum_{j=1}^{l(\lambda)} \frac{d(d-1)\cdots(d-l(\lambda)+1)}{d-j+1} = e_{l(\lambda)-1}(d, d-1, \ldots, d-l(\lambda)+1).$$

Finally, since $F^{\{1,2,\ldots,d+1\}}$ is homogeneous of degree one in the coefficient of the $F^{\{i\}}$'s, we deduce that

$$\mu = nd^{n-1} - \sum_{\substack{\lambda \vdash n \\ l(\lambda) \leqslant d}} m_\lambda . e_{l(\lambda)-1}(d, d-1, \ldots, d-l(\lambda)+1),$$

that is to say

$$\mu = nd^{n-1} - \sum_{k=1}^{d} \sum_{\substack{\lambda \vdash n \\ l(\lambda)=k}} m_\lambda . e_{k-1}(d, d-1, \ldots, d-k+1).$$

From here we see immediately that μ is equal to the integer m_0 defined in the statement of Theorem 4.

To conclude the proof of Theorem 4, it remains to determine the signs that occur in the formulas (5.22) and (5.23). To this end, we examine the specialization of them, when $F^{\{i\}} = x_i^d$, $i = 1, \ldots, n$. First, the resultant of the $F^{\{i\}}$'s is equal to 1 (normalization of the resultant). Now, given any partition $\lambda \vdash n$, it is straightforward to check that $F_\lambda^{\{1\}} = x_1^d$. Then applying iteratively the defining property of the divided differences from $j = 1$ to $j = l(\lambda)$, we get that

$$F_\lambda^{\{1,2,\ldots,j\}} = x_j^d \mod (x_1, \ldots, x_{j-1}), \;\; j = 1, \ldots, l(\lambda).$$

Now, using the multiplicativity property of the resultant and its invariance under elementary transformations, we deduce that all the resultants associated to a partition λ specialize to 1. Similarly we observe that $F^{\{1,\ldots,d+1\}}$ also specializes to 1 when $n > d$, and this concludes the proof of Theorem 4.

6. MIXED DISCRIMINANTS

Polynomial algebra offers a standard approach to handle several problems in geometric modeling. A key tool is the discriminant of a univariate polynomial, or of a well-constrained system of polynomial equations, which expresses the existence of a multiple root. We describe discriminants in a general context, and focus on exploiting the sparseness of polynomials via the theory of Newton polytopes and sparse (or toric) elimination. We concentrate on bivariate polynomials and establish an original formula that relates the discriminant of two bivariate Laurent polynomials with fixed support, with the sparse resultant of these polynomials and their toric Jacobian. This allows us to obtain a new proof for the bidegree of the discriminant as well as to establish multipicativity formulas arising when one polynomial can be factored.

6.1 Introduction

Polynomial algebra offers a standard and powerful approach to handle several problems in geometric modeling. In particular, the study and solution of systems of polynomial equations has been a major topic. Discriminants provide a key tool when examining well-constrained systems, including the case of one univariate polynomial. Their theoretical study is a thriving and fruitful domain today, but they are also very useful in a variety of applications.

The best studied discriminant is probably known since high school, where one studies the discriminant of a quadratic polynomial $f(x) = ax^2 + bx + c = 0$ ($a \neq 0$). The polynomial f has a double root if and only if its discriminant $\Delta_2 = b^2 - 4ac$ is equal to zero. Equivalently, this can be defined as the condition for $f(x)$ and its derivative $f'(x)$ to have a common root:

$$\exists\, x \;:\; f(x) = ax^2 + bx + c = f'(x) = 2ax + b = 0 \;\Leftrightarrow \Delta_2 = 0. \tag{6.1}$$

One can similarly consider the discriminant of a univariate polynomial of any degree. If we wish to calculate the discriminant $\Delta_5(f)$ of a polynomial f of degree five in one variable, we consider the condition that both f and its derivative vanish:

$$\begin{aligned} f(x) &= ax^5 + bx^4 + cx^3 + dx^2 + ex + g = 0, \\ f'(x) &= 5ax^4 + 4bx^3 + 3cx^2 + 2dx + e = 0. \end{aligned}$$

In this case, elimination theory reduces the computation of Δ_5 to the computation of a 9×9 Sylvester determinant, which equals $a\,\Delta_5(f)$. If we develop this determinant, we find out

that the number monomials in the discriminant increases rapidly with the input degree:

$$\Delta_5 = -2050a^2g^2bedc + 356abed^2c^2g - 80b^3ed^2cg + 18dc^3b^2g$$
$$e - 746agdcb^2e^2 + 144ab^2e^4c - 6ab^2e^3d^2 - 192a^2be^4d - 4d^2ac$$
$$^3e^2 + 144d^2a^2ce^3 - 4d^3b^3e^2 - 4c^3e^3b^2 - 80abe^3dc^2 + 18b^3e^3$$
$$dc + 18d^3acbe^2 + d^2c^2b^2e^2 - 27b^4e^4 - 128a^2e^4c^2 + 16ac^4e^3 - 27$$
$$a^2d^4e^2 + 256a^3e^5 + 3125a^4g^4 + 160a^2gbe^3c + 560a^2gdc^2e^2 + 1020$$
$$a^2gbd^2e^2 + 160ag^2b^3ed + 560ag^2d^2cb^2 + 1020ag^2b^2c^2e - 192$$
$$b^4ecg^2 + 24ab^2ed^3g + 24abe^2c^3g + 144b^4e^2dg - 6b^3e^2c^2g + 14$$
$$4dc^2b^3g^2 - 630dac^3bg^2 - 630d^3a^2ceg - 72d^4acbg - 72dac^4e$$
$$g - 4d^3c^2b^2g - 1600ag^3cb^3 - 2500a^3g^3be - 50a^2g^2b^2e^2 - 3750a^3$$
$$g^3dc + 2000a^2g^3db^2 + 2000a^3g^2ce^2 + 825a^2g^2d^2c^2 + 2250a^2g^3b$$
$$c^2 + 2250a^3g^2ed^2 - 900a^2g^2bd^3 - 900a^2g^2c^3e - 36agb^3e^3 - 1600$$
$$a^3ge^3d + 16d^3ac^3g - 128d^2b^4g^2 + 16d^4b^3g - 27c^4b^2g^2 + 108ac^5$$
$$g^2 + 108a^2d^5g + 256b^5g^3.$$

In fact, if we compute the resultant of f and xf' by means of the 10×10 Sylvester determinant, we find the more symmetric output: $a\, g\, \Delta_5(f)$. This formula is very well known for univariate discriminants [54], and we generalize it in Theorem 6.3.3.

One univariate polynomial is the smallest well-constrained system. We are concerned with multivariate systems of sparse polynomials, in other words, polynomials with fixed support, or set of nonzero terms. *Sparse (or toric)* elimination theory concerns the study of resultants and discriminants associated with toric varieties. This theory has its origin in the work of Gel'fand, Kapranov and Zelevinsky on multivariate hypergeometric functions. Discriminants arise as singularities of such functions [53].

Gel'fand, Kapranov and Zelevinsky [54] established a general definition of sparse discriminant, which gives as special case the following definition of (sparse) mixed discriminant (see Section 6.2 for the relation with the discriminant of the associated Cayley matrix and with the notion of mixed discriminant in [18]). In case $n = 2$, the mixed discriminant detects tangencies between families of curves with fixed supports. In general, the *mixed discriminant* $\Delta_{A_1,\ldots,A_n}(f_1, \ldots, f_n)$ of n polynomials in n variables with fixed supports $A_1, \ldots, A_n \subset \mathbb{Z}^n$ is the irreducible polynomial (with integer coprime coefficients, defined up to sign) in the coefficients of the f_i which vanishes whenever the system $f_1 = \cdots = f_n = 0$ has a multiple root (that is, a root which is not simple) with non-zero coordinates, in case this discriminantal variety is a hypersurface (and equal to the constant 1 otherwise). The zero locus of the mixed discriminant is the variety of ill-posed systems [87]. We shall work with the polynomial defining the *discriminant cycle* (see Section 6.2) which is defined as the power $\Delta_{A_1,\ldots,A_n}^{i(A_1,\ldots,A_n)}$ of the mixed discriminant raised to the index

$$i(A_1, \ldots, A_n) = [\mathbb{Z}^n : \mathbb{Z}A_1 + \cdots + \mathbb{Z}A_n], \tag{6.2}$$

which stands for the index of lattice $\mathbb{Z}A_1 + \cdots + \mathbb{Z}A_n$ in $\mathbb{Z}^n$. In general, this index equals 1 and so both concepts coincide.

Discriminants have many applications. Besides the classical application in the realm of differential equations to describe singularities, discriminants occur for instance in the de-

scription of the topology of real algebraic plane curves [56], in solving systems of polynomial inequalities and zero-dimensional systems [48], in determining the number of real roots of square systems of sparse polynomials [31], in studying the stability of numerical solving [26], in the computation of the Voronoi diagram of curved objects [44], or in the determination of cusp points of parallel manipulators [77].

Computing (mixed) discriminants is a (difficult) elimination problem. In principle, they can be computed with Gröbner bases, but this is very inefficient in general since these polynomials have a rich combinatorial structure [54]. Ad-hoc computations via complexes (i.e., via tailored homological algebra) are also possible, but they also turn out to be complicated. The tropical approach to compute discriminants was initiated in [30] and the tropicalization of mixed planar discriminants was described in [32]. Recently, in [38], the authors focus on computing the discriminant of a multivariate polynomial via interpolation, based on [37, 82]; the latter essentially offers an algorithm for predicting the discriminant's Newton polytope, hence its nonzero terms. This yields a new output-sensitive algorithm which, however, remains to be juxtaposed in practice to earlier approaches.

We mainly work in the case $n = 2$, where the results are more transparent and the basic ideas are already present, but all our results and methods can be generalized to any number of variables. This will be addressed in a subsequent paper [27]. Consider for instance a system of two polynomials in two variables and assume that, the first polynomial factors as $f_1 = f_1' \cdot f_1''$. Then, the discriminant also factors and we thus obtain a multiplicativity formula for it, which we make precise in Corollary 6.4.1. This significantly simplifies the discriminant's computation and generalizes the formula in [12] for the classical homogeneous case. This multiplicativity formula is a consequence of our main result (Theorem 6.3.3 in dimension 2, see also Theorem 6.3.4 in any dimension) relating the mixed discriminant and the resultant of the given polynomials and their *toric Jacobian* (see Section 6.3 for precise definitions and statements). As another consequence of Theorem 6.3.3, we reprove, in Corollary 6.3.6, the bidegree formula for planar mixed discriminants in [18].

The rest of this chapter is organized as follows. The next section overviews relevant existing work and definitions. In Section 6.3 we present our main results relating the mixed discriminant with the sparse resultant of the two polynomials and their toric Jacobian. In Section 6.4 we deduce the general multiplicativity formula for the mixed discriminant when one polynomial factors.

6.2 Previous work and notation

In this section we give a general description of discriminants and some definitions and notations that we are going to use in the following sections.

Given a set $A \subset \mathbb{R}^n$, let $Q = conv(A)$ denote the convex hull of A. We say that A is a lattice set or configuration if it is contained in $\mathbb{Z}^n$, whereas a polytope with integer vertices is called a lattice polytope. We denote by $\mathrm{Vol}(\cdot)$ the volume of a lattice polytope, normalized with respect to the lattice $\mathbb{Z}^n$, so that a primitive simplex has normalized volume equal to 1.

Normalized volume is obtained by multiplying Euclidean volume by $n!$.

Given a non-zero Laurent polynomial

$$f = \sum_a c_a x^a,$$

the finite subset A of $\mathbb{Z}^n$ of those exponents a for which $c_a \neq 0$ is called the *support* of f. The *Newton polytope* $N(f)$ of f is the lattice polytope defined as the convex hull of A.

A (finite) set A is said to be *full*, if it consists of all the lattice points in its convex hull. In [18], A is called *dense* in this case, but we prefer to reserve the word dense to refer to the classical homogeneous case. A subset $F \subseteq A$ is called a *face* of A, denoted $F \prec A$, if F is the intersection of A with a face of the polytope $conv(A)$.

As usual $Q_1 + Q_2$ denotes the Minkowski sum of sets Q_1 and Q_2 in $\mathbb{R}^n$. The *mixed volume* $MV(Q_1, \ldots, Q_n)$ of n convex polytopes Q_i in $\mathbb{R}^n$ is the multilinear function with respect to Minkowski sum that generalizes the notion of volume in the sense that $MV(Q, \ldots, Q) =$ Vol(Q), when all Q_i equal a fixed convex polytope Q.

The following key result is due to Bernstein and Kouchnirenko. The mixed volume of the Newton polytopes of n Laurent polynomials $f_1(x), \ldots, f_n(x)$ in n variables is an integer that bounds the number of isolated common solutions of $f_1(x) = 0, \ldots, f_n(x) = 0$ in the algebraic torus $(K^*)^n$, over an algebraically closed field K containing the coefficients. If the coefficients of the polynomials are generic, then the common solutions are isolated and their number equals the mixed volume. This bound generalized Bézout's classical bound to the sparse case: for homogeneous polynomials the mixed volume and Bézout's bound coincide.

Mixed volume can be defined in terms of Minkowski sum volumes as follows.

$$MV_n(Q_1, \ldots, Q_n) = \sum_{k=1}^{n} (-1)^{n-k} \sum_{I \subset \{1,\ldots,n\}, |I|=k} \frac{1}{n!} \text{Vol}\Big(\sum_{i \in I} Q_i \Big).$$

This implies, for $n = 2$:

$$2MV(Q_1, Q_2) = \text{Vol}(Q_1 + Q_2) - \text{Vol}(Q_1) - \text{Vol}(Q_2).$$

Definition 6.2.1. A family of finite lattice configurations $A_1, \ldots, A_k$ in $\mathbb{Z}^n$ is called essential if the affine dimension of the lattice $\mathbb{Z}A_1 + \cdots + \mathbb{Z}A_k$ equals $k-1$, and for all proper subsets $I \subset \{1, \ldots, k\}$ it holds that the affine dimension of the lattice generated by $\{A_i, i \in I\}$ is greater or equal than its cardinality $|I|$.

Definition/Theorem 1. [54, 89] Fix a family of $n+1$ finite lattice configurations $A_1, \ldots, A_{n+1}$ which contains a unique essential subfamily $\{A_i, i \in I\}$. Given Laurent polynomials $f_1, \ldots, f_{n+1}$ in n variables with respective supports $A_1, \ldots, A_{n+1}$, the *resultant* $\text{Res}_{A_1,\ldots,A_{n+1}}(f_1, \ldots, f_{n+1})$ is the irreducible polynomial with coprime integer coefficients (defined up to sign) in the coefficients of $f_1, \ldots, f_{n+1}$, which vanishes whenever $f_1, \ldots, f_{n+1}$ have a common root in the torus $(\mathbb{C}^*)^n$. In fact, in this case, the resultant only depends on the coefficients of f_i with $i \in I$.

If there exist more than one essential subfamilies, then the (closure of the) variety of solvable systems is not a hypersurface and in this case we set:

$$\mathsf{Res}_{A_1,\dots,A_{n+1}}(f_1,\dots,f_{n+1}) = 1.$$

In what follows, we consider n (finite) lattice configurations $A_1,\dots,A_n$ in $\mathbb{Z}^n$ and we denote by $Q_1,\dots,Q_n$ their respective convex hulls. Let $f_1,\dots,f_n$ be Laurent polynomials with support $A_1,\dots,A_n$ respectively:

$$f_i(x) = \sum_{\alpha\in A_i} c_{i,\alpha}x^\alpha, \quad i = 1\dots,n.$$

In [18] the *mixed discriminantal variety*, is defined as closure of the locus of coefficients $c_{i,\alpha}$ for which the associated system $f_1 = \cdots = f_n = 0$ has a non-degenerate multiple root $x \in (K^*)^n$. This means that x is an isolated root and the n gradient vectors

$$\left(\frac{\partial f_i}{\partial x_1}(x),\dots,\frac{\partial f_i}{\partial x_n}(x)\right)$$

are linearly dependent, but any $n-1$ of them are linearly independent.

Definition 6.2.2. If the mixed discriminantal variety is a hypersurface, the *mixed discriminant* of the previous system is the unique up to sign irreducible polynomial $\Delta_{A_1,\dots,A_n}$ with integer coefficients in the unknowns $c_{i,a}$ which defines this hypersurface. Otherwise, the family is said to be defective and we set $\Delta_{A_1,\dots,A_n} = 1$. The *mixed discriminant cycle* $\tilde{\Delta}_{A_1,\dots,A_n}$ is equal to $i(A_1,\dots,A_n)$ times the mixed discriminant variety, and thus its equation equals $\Delta_{A_1,\dots,A_n}$ raised to this integer (defined in (6.2)).

By [18, Theorem 2.1], when the family $A_1,\dots,A_n$ is non defective, the mixed discriminant $\Delta_{A_1,\dots,A_n}$ coincides with the A-discriminant defined in [54], where A is the Cayley matrix

$$A = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \\ A_1 & A_2 & \dots & A_n \end{pmatrix}.$$

This matrix has $2n$ rows and $m = \sum_{i=1}^n |A_i|$ columns, so $0 = (0,\dots,0)$ and $1 = (1,\dots,1)$ denote row vectors of appropriate lengths. We introduce n new variables $y_1,\dots,y_n$ in order to encode the system $f_1 = \cdots = f_n = 0$ in one polynomial with support in A, via the *Cayley trick*: $\phi(x,y) = y_1f_1(x) + \cdots + y_nf_n(x)$. Note that $i(A_1,\dots,A_n) = [\mathbb{Z}^{2n},\mathbb{Z}A]$.

In what follows when we refer to resultants or discriminants we will refer to the equations of the corresponding cycles, but we will omit the tildes in our notation. More explicitly, we will follow the convention in the article [23] by D'Andrea and Sombra. In general, both definitions coincide, but this convention allows us to present cleaner formulas. For instance, when the family $A_1,\dots,A_{n+1}$ is essential, our notion of resultant equals the resultant in [54, 89] raised to the index $i(A_1,\dots,A_{n+1})$. In most examples these two lattices coincide, and so our resultant cycle equals the resultant variety and the associated resultant polynomial is irreducible.

Remark 6.2.3. Assume A_1 consists of a single point α and that $\{1\}$ is the only essential subfamily of a given family $A_1, \ldots, A_{n+1}$. Let $f_1(x) = cx^\alpha$. Then, for any choice of Laurent polynomials $f_2, \ldots, f_{n+1}$ with supports $A_2, \ldots, A_{n+1}$, it holds that (cf. [23, Proposition 2.2])

$$\mathsf{Res}_{A_1,\ldots,A_{n+1}}(f_1, \ldots, f_n) \;=\; c^{MV(A_2,\ldots,A_{n+1})}. \tag{6.3}$$

With this convention, the following multiplicativity formula holds:

Theorem 6.2.4. [23, 80] *Let $A_1', A_1'', A_1, \ldots, A_{n+1}$ be finite subsets of $\mathbb{Z}^n$ with $A_1 = A_1' + A_1''$. Let $f_1, \ldots, f_{n+1}$ be polynomials with supports contained in $A_1, \ldots, A_{n+1}$ and assume that $f_1 = f_1' f_1''$ where f_1' has support A_1' and f_1'' has support A_1''. Then*

$$\mathsf{Res}_{A_1,\ldots,A_{n+1}}(f_1, \ldots, f_{n+1}) \;=\; \mathsf{Res}_{A_1',\ldots,A_{n+1}}(f_1', \ldots, f_{n+1}) \cdot \mathsf{Res}_{A_1'',\ldots,A_{n+1}}(f_1'', \ldots, f_{n+1}).$$

Cattani, Cueto, Dickenstein, Di Rocco and Sturmfels in [18] proved that the degree of the mixed discriminant Δ is a piecewise linear function in the Plücker coordinates of a mixed Grassmanian. An explicit degree formula for plane curves is also presented in [18, Corollary 3.15]. In case A_1, A_2 consist of all the lattice points in their convex hulls, they are two dimensional and with the same normal fan, then the bidegree of Δ_{A_1,A_2} satisfies the following: bidegree of Δ_{A_1,A_2} in the coefficients of f_i equals:

$$= \mathsf{Vol}(Q_1 + Q_2) - area(Q_i) - perimeter(Q_j),$$

where $i \in \{1, 2\}$, $i \neq j$. where $Q_i = conv(A_i)$, $i = 1, 2$, and $Q_1 + Q_2$ is their Minkowski sum. The area is normalized, so that a primitive triangle has area 1 and the perimeter of Q_i is the cardinality of $\partial Q_i \cap \mathbb{Z}^2$. We will recover the general formula for this degree and present it in Corollary 6.3.6.

Busé and Jouanolou consider in [12] the following equivalent definition of the mixed discriminant, in case where $f_1, \ldots, f_n$ are dense homogeneous polynomials in $(x_0, \ldots, x_n)$ of degrees $d_1, \ldots, d_n$ respectively, that is, their respective supports $A_i = d_i\sigma$ are all the lattice points in the d_i-th dilate of the unit simplex σ in $\mathbb{R}^n$. It is the non-zero polynomial in the coefficients of $f_1, \ldots, f_n$ which equals

$$\frac{\mathsf{Res}_{d_1\sigma,\ldots,d_n\sigma,\delta_i\sigma}(f_1, \ldots, f_n, J_i)}{\mathsf{Res}_{d_1\sigma,\ldots,d_n\sigma,\sigma}(f_1, \ldots, f_n, x_i)}, \tag{6.4}$$

for all $i \in \{1, \ldots, n\}$, where J_i is the maximal minor of the Jacobian matrix associated to $f_1, \ldots, f_n$ obtained by deleting the i-th. We give a more symmetric and general formula in Corollary 6.3.5 below.

The multiplicativity property of the discriminant in the case of dense homogeneous polynomials was already known to Sylvester [90] and generalized by Busé and Jouanolou in [12], where they proved that when in particular $A_1 = d_1\sigma = (d_1' + d_1'')\sigma$ and f_1 is equal to the product of two polynomials $f_1' \cdot f_1''$ with respective degrees d_1', d_1'', the following factorization holds:

$$\begin{aligned}\Delta_{d_1\sigma,\ldots,d_n\sigma}(f_1, \ldots, f_n) \;=& \Delta_{d_1'\sigma,\ldots,d_n\sigma}(f_1', \ldots, f_n) \cdot \Delta_{d_1''\sigma,\ldots,d_n\sigma}(f_1'', \ldots, f_n) \\ & \cdot \mathsf{Res}_{d_1'\sigma,d_1''\sigma,\ldots,d_n\sigma}(f_1', f_1'', \ldots, f_n)^2.\end{aligned} \tag{6.5}$$

It is straightforward to see in general from the definition, that in case where $\Delta_{A_1',\ldots,A_n}(f_1',\ldots,f_n) = 0$ or $\Delta_{A_1'',\ldots,A_n}(f_1'',\ldots,f_n) = 0$ or $\mathrm{Res}_{A_1',A_1'',\ldots,A_n}(f_1',f_1'',\ldots,f_n) = 0$ then,

$$\Delta_{A_1'+A_1'',\ldots,A_n}(f_1'f_1'',f_2,\ldots,f_n) = 0.$$

It follows from [46] that when each support configuration A_i is full, the Newton polytope of the discriminant $\Delta_{A_1'+A_1'',A_2,\ldots,A_n}(f_1'f_1'',f_2,\ldots,f_n)$ equals the Minkowski sum of the Newton polytopes of the discriminants $\Delta_{A_1',A_2,\ldots,A_n}(f_1',f_2,\ldots,f_n)$ and $\Delta_{A_1'',A_2,\ldots,A_n}(f_1'',f_2,\ldots,f_n)$ plus two times the Newton polytope of the resultant $\mathrm{Res}_{A_1',A_1'',A_2,\ldots,A_n}(f_1',f_1'',f_2,\ldots,f_n)$. So, a first guess would be that the factorization into the three factors in (6.5) above holds for general supports. We will see in Corollary 6.4.1 that indeed other factors may occur, which we describe explicitly.

This behavior already occurs in the univariate case:

Example 6.2.5. Let $A_1' = \{0, i_1, \ldots, i_m, d_1\}, A_1'' = \{0, j_1, \ldots, j_l, d_2\}$ be the support sets of $f_1' = a_0 + a_{i_1}x^{i_1} + \cdots + a_{i_m}x^{i_m} + a_{d_1}x^{d_1}$, $f_1'' = b_0 + b_{j_1}x^{j_1} + \cdots + b_{j_l}x^{j_l} + b_{d_2}x^{d_2}$ respectively. Then

$$\Delta(f_1'f_1'') = \Delta(f_1') \cdot \Delta(f_1'') \cdot R(f_1',f_1'')^2 \cdot E,$$

where $E = a_0^{i_1-m_0}\, b_0^{j_1-m_0}\, a_{d_1}^{d_1-i_m-m1}\, b_{d_2}^{d_2-j_l-m_1}$, with $m_0 := \min\{i_1, j_1\}$ and $m_1 := \min\{d_1 - i_m, d_2 - j_l\}$. On the other hand, in the full case $i_1 = j_1 = 1, i_m = d_1 - 1, j_l = d_2 - 1$, thus $E = 1$ because its exponents are equal to zero.

6.3 A general formula

The aim of this section is to present a formula which relates the mixed discriminant with the resultant of the given polynomials and their toric Jacobian, whose definition we recall.

Definition 6.3.1. Let $f_1(x_1,\ldots,x_n),\ldots,f_n(x_1,\ldots,x_n)$ be n Laurent polynomials in n variables. The associated toric Jacobian J_f^T equals $x_1\cdots x_n$ times the determinant of the *Jacobian matrix of f*, or equivalently, the determinant of the matrix:

$$\begin{bmatrix} x_1\dfrac{\partial f_1}{\partial x_1} & \cdots & x_n\dfrac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ x_1\dfrac{\partial f_n}{\partial x_1} & \cdots & x_n\dfrac{\partial f_n}{\partial x_n} \end{bmatrix}.$$

Note that the Newton polytope of J_f^T is contained in the sum of the Newton polytopes of $f_1,\ldots,f_n$.

As we remarked before, we will mainly deal in this chapter with the case $n = 2$. Also, to avoid excessive notations and make the main results cleaner, we assume below that A_1, A_2 are two finite lattice configurations whose convex hulls satisfy

$$\dim(Q_1) = \dim(Q_2) = 2.$$

Let f_1, f_2 be polynomials with respective supports A_1, A_2:

$$f_i(x) = \sum_{\alpha \in A_i} c_{i,\alpha} x^\alpha, \quad i = 1, 2,$$

where $x = (x_1, x_2)$. We denote by Σ the set of primitive inner normals $\eta \in (\mathbb{Z}^2)^*$ of the edges of $A_1 + A_2$. We call A_i^η the face of A_i where the inner product with η is minimized. We call this minumum value ν_i^η. We also denote by f_i^η the subsum of terms in f_i with exponents in this face

$$f_i^\eta(x) = \sum_{\alpha \in A_i^\eta} c_{i,\alpha} x^\alpha, \quad i = 1, 2,$$

which is η-homogeneous of degree ν_i^η. Up to multiplying f_i by a monomial (that is, after translation of A_i) we can assume without loss of generality that $\nu_i^\eta \neq 0$. Now, A_i^η is either a vertex of A_i (but not of both A_1, A_2 since two vertices do not give a Minkowski sum edge), or its convex hull is an edge of A_i (with inner normal η), which we denote by e_i^η. Note that if the face of $A_1 + A_2$ associated to η is a vertex, both polynomials f_i^η are monomials and their resultant locus has codimension two.

We denote by $\mu_i(\eta)$ $(i = 1, 2)$ the integer defined by the following difference:

$$\mu_i(\eta) = \min\{\langle \eta, m \rangle, m \in A_i - A_i^\eta\} \; - \; \nu_i^\eta. \tag{6.6}$$

and by

$$\mu(\eta) = \min\{\mu_1(\eta), \mu_2(\eta)\}, \tag{6.7}$$

the minimum of these two integers. Note that by our assumption that $\dim(Q_i) = 2$, we have that $\mu(\eta) \geq 1$.

Without loss of generality, we can translate the support sets A_1^η, A_2^η to the origin and consider the line L^η containing them. The residue (cycle) $\mathrm{Res}_{A_1^\eta, A_2^\eta}(f_1^\eta, f_2^\eta)$ is considered as before, with respect to the lattice $L^\eta \cap \mathbb{Z}^2$.

Remark 6.3.2. As in Remark 6.2.3, if f_1^η is a monomial, the resultant equals the coefficient of f_1^η raised to the normalized length $\ell(e_2^\eta)$ of the edge e_2^η of A_2 (that is, the number of integer points in the edge, minus 1). If η is an inner normal of edges A_1^η and A_2^η, then the resultant equals the irreducible resultant raised to the index of $\mathbb{Z}A_1^\eta + \mathbb{Z}A_2^\eta$ in $L^\eta \cap \mathbb{Z}^2$. In particular, the exponent $\mu(\eta) = 1$ if at least one of the configurations is full.

The following is our main result.

Theorem 6.3.3. *Let f_1, f_2 be generic Laurent polynomials with respective supports A_1, A_2. Then,*

$$\mathrm{Res}_{A_1, A_2, A_1 + A_2}(f_1, f_2, J_f^T) = \Delta_{A_1, A_2}(f_1, f_2) \cdot E,$$

where the factor E equals the finite product:

$$E = \prod_{\eta \in \Sigma} \mathrm{Res}_{A_1^\eta, A_2^\eta}(f_1^\eta, f_2^\eta)^{\mu(\eta)}.$$

Proof. Let X be the projective toric variety associated to $A_1 + A_2$. This compact variety consists of an open dense set T_X isomorphic to the torus $(\mathbb{C}^*)^2$ plus one toric divisor D_η for each $\eta \in \Sigma$. The Laurent polynomials f_1, f_2, J_f^T define sections L_1, L_2, L_J of globally generated line bundles on X. The resultant $\mathsf{Res}_{A_1,A_2,A_1+A_2}(f_1, f_2, J_f^T)$ vanishes if and only if L_1, L_2, L_J have a common zero on X, which could be at T_X or at any of the D_η.

There is an intersection point at T_X if and only if there is a common zero of f_1, f_2 and J_f^T in the torus $(\mathbb{C}^*)^2$. In this case, the discriminant $\Delta_{A_1,A_2}(f_1, f_2)$ would vanish. It follows that $\Delta_{A_1,A_2}(f_1, f_2)$ divides $\mathsf{Res}_{A_1,A_2,A_1+A_2}(f_1, f_2, J_f^T)$. (the indices $[\mathbb{Z}^2 : \mathbb{Z}A_1 + \mathbb{Z}A_2]$ and $[\mathbb{Z}^2 : \mathbb{Z}A_1 + \mathbb{Z}A_2 + \mathbb{Z}(A_1 + A_2)]$ are equal).

If instead there is a common zero at some D_η, this translates into the fact that f_1^η, f_2^η and $(J_f^T)^\eta = J_{f^\eta}^T$ (with obvious definition) have a common solution. But as f_i^η are η-homogeneous, they satisfy the weighted Euler equalities:

$$\eta_1 x_1 \frac{\partial f_i^\eta}{\partial x_1} + \eta_2 x_2 \frac{\partial f_i^\eta}{\partial x_2} = \nu_i^\eta f_i, \quad i = 1, 2, \tag{6.8}$$

from which we deduce that $J_{f^\eta}^T$ lies in the ideal $I(f_1^\eta, f_2^\eta)$ and so, the three polynomials will vanish exactly when there is a nontrivial common zero of f_1^η and f_2^η. This implies that all facet resultants $\mathsf{Res}_{A_1^\eta,A_2^\eta}(f_1^\eta, f_2^\eta)$ divide $\mathsf{Res}_{A_1,A_2,A_1+A_2}(f_1, f_2, J_f^T)$.

Now, we wish to see that the resultant $\mathsf{Res}_{A_1^\eta,A_2^\eta}(f_1^\eta, f_2^\eta)$ raised to the power $\mu(\eta)$ occurs as a factor. The following argument would be better written in terms of the multihomogeneous polynomials in the Cox coordinates of X which represent L_1, L_2, L_J [19]. Fix a primitive inner normal direction $\eta \in \Sigma$ of $A_1 + A_2$, let t be a new variable and define the following polynomials

$$F_i(t, x) = \sum_{\alpha \in A_i} c_{i,\alpha} t^{\langle \eta, \alpha \rangle - \nu_i^\eta} x^\alpha, \quad i = 1, 2, \tag{6.9}$$

so that

$$F_i(1, x) = f_i(x), \quad F_i(0, x) = f_i^\eta(x), \quad i = 1, 2,$$

and we can write

$$f_i^\eta(x) = F_i^\eta(t, x) - t^{\mu_i(\eta)} G_i(t, x), \quad i = 1, 2, \tag{6.10}$$

where the polynomials G_i are defined by these equalities. The polynomials F_1, F_2, J_F^T define the sections L_1, L_2, L_J. For each t, we deduce from the bilinearity of the determinant, that there exists a polynomial $H(t, x)$ such that the toric Jacobian can be written as $J_F^T = J_{f^\eta}^T + t^{\mu(\eta)} H(t, x)$. But, as we remarked, $J_{f^\eta}^T$ lies in the ideal $I(f_1^\eta, f_2^\eta)$, and using the equalities (6.10), we can write $J_F^T = H_1(t, x) + t^{\mu(\eta)} H_2(t, x)$, with $H_1 \in I(F_1, F_2)$. Note that if for instance $\eta_1 \neq 0$, then the power of x_1 in each monomial of F_i can be obtained from the power of t and the power of x_2, that is, we could use t and x_2 as "variables" instead. We will denote by Res^X the resultant defined over X [19]. Therefore,

$$\mathsf{Res}_{A_1,A_2,A_1+A_2}(f_1, f_2, J_f^T) = \mathsf{Res}^X_{A_1,A_2,A_1+A_2}(F_1, F_2, t^{\mu(\eta)} H_2).$$

Now, it follows from Theorem 6.2.4 that

$$\mathsf{Res}^X_{A_1,A_2,A_1+A_2}(F_1, F_2, t^{\mu(\eta)}) = \mathsf{Res}_{A_1^\eta,A_2^\eta}(f_1^\eta, f_2^\eta)^{\mu(\eta)}$$

is a factor of $\mathsf{Res}_{A_1,A_2,A_1+A_2}(f_1, f_2, J_f^T)$. Indeed, no positive power of t divides H_2 for generic coefficients. Considering all possible $\eta \in \Sigma$ we get the desired factorization. □

Theorem 6.3.3 and the proof will be extended to the general n-variate setting in a forthcoming paper [27]. We only state here the following general version without proof. Recall that a lattice polytope P of dimension n in $\mathbb{R}^n$ is said to be *smooth* if at each every vertex there are n concurrent facets and their primitive inner normal directions form a basis of $\mathbb{Z}^n$. In particular, integer dilates of the unit simplex or the unit (hyper)cube are smooth.

Theorem 6.3.4. *Let $P \subset \mathbb{R}^n$ be a smooth lattice polytope of dimension n. Let $A_i = (d_iP) \cap \mathbb{Z}^n$, $i = 1, \ldots, n$, $d_1, \ldots, d_n \in \mathbb{Z}_{>0}$, and $f_1, \ldots, f_n$ polynomials with these supports, respectively. Then, we have the following factorization*

$$\mathsf{Res}_{A_1,\ldots,A_n,A_1+\cdots+A_n}(f_1, \ldots, f_n, J_f^T) = \Delta_{A_1,\ldots,A_n}(f_1, \ldots, f_n) \cdot E,$$

where the factor E equals the finite product:

$$E = \prod_{\eta\in\Sigma} \mathsf{Res}_{A_1^\eta,\ldots,A_n^\eta}(f_1^\eta, \ldots, f_n^\eta).$$

Note that all the exponents in E equal 1 and all the lattice indices equal 1.

When the given lattice configurations A_i are the lattice points $d_i\sigma$ of the d_i-th dilate of the standard simplex σ in $\mathbb{R}^n$, (that is, in the homogeneous case studied in [12]), formula (6.4) gives for any n in our notation:

$$\begin{aligned}&\mathsf{Res}_{d_1\sigma,\ldots,d_n\sigma,\delta\sigma}(f_1, \ldots, f_n, J_i) = \\ &\Delta_{d_1\sigma,\ldots,d_n\sigma}(f_1, \ldots, f_n) \cdot \mathsf{Res}_{(d_1\sigma)^{e_i},\ldots,(d_n\sigma)^{e_i}}(f_1^{e_i}, \ldots, f_n^{e_i}),\end{aligned}$$

where $e_0, \ldots, e_n$ are the canonical basis vectors (or $e_0 = -e_1 - \cdots - e_n$, if we consider the corresponding dehomogenized polynomials, by setting $x_0 = 1$). Note that Theorem 6.3.4 gives the following more symmetric formula:

Corollary 6.3.5. *With the previous notation, it holds:*

$$\begin{aligned}&\mathsf{Res}_{d_1\sigma,\ldots,d_n\sigma,(d_1+\cdots+d_n)\sigma}(f_1, \ldots, f_n, J_f^T) = \\ &\Delta_{d_1\sigma,\ldots,d_n\sigma}(f_1, \ldots, f_n) \cdot \prod_{i=0}^{n} \mathsf{Res}_{(d_1\sigma)^{e_i},\ldots,(d_n\sigma)^{e_i}}(f_1^{e_i}, \ldots, f_n^{e_i}).\end{aligned}$$

It is straightforward to deduce from this expression the degree of the homogeneous mixed discriminant, obtained independently in [6, 12, 78]. Similar formulas can be obtained, for instance, in the multihomogeneous case.

We recall the following definition from [18]. If v is a vertex of A_i, we define its *mixed multiplicity* as

$$mm_{A_1,A_2}(v) := MV(Q_1, Q_2) - MV(C_i, Q_j), \quad \{i, j\} = \{1, 2\}, \tag{6.11}$$

where $C_i = conv(A_i - \{v\})$.

Let $\Sigma' \subset \Sigma$ be the set of inner normals of $A_1 + A_2$ that cut out, or define, edges e_i^η in both Q_1, Q_2. The factorization formula in Theorem 6.3.3 can be written as follows, and allows us to recover the bidegree formulas for planar mixed discriminants in [18].

Corollary 6.3.6. *Let A_1, A_2 be two lattice configurations of dimension 2 in the plane, and let f_1, f_2 be polynomials with these respective supports. Then, the resultant of f_1, f_2 and their toric Jacobian, namely* $\mathrm{Res}_{A_1,A_2,A_1+A_2}(f_1, f_2, J_f^T)$*, factors as follows:*

$$\Delta_{A_1,A_2}(f_1,f_2) \cdot \prod_{v \text{ vertex of } A_1 \text{ or } A_2} c_v^{\mathsf{mm}_{\mathsf{A_1},\mathsf{A_2}}(\mathsf{v})} \cdot \prod_{\eta\in\Sigma'} \mathrm{Res}_{A_1^\eta,A_2^\eta}(f_1^\eta, f_2^\eta)^{\mu(\eta)}. \tag{6.12}$$

The bidegree (δ_1, δ_2) of the mixed discriminant $\Delta_{A_1,A_2}(f_1, f_2)$ in the coefficients of f_1 and f_2, respectively, is then given by the following:

$$\mathit{Vol}(Q_j) + 2 \cdot MV(Q_1, Q_2) - \sum_{\eta\in\Sigma'} \ell(e_j^\eta) \cdot \mu(\eta) - \sum_{v \text{ vertex of } (A_i)} mm_{A_1,A_2}(v), \tag{6.13}$$

where $i \in \{1, 2\}$, $i \neq j$.

Proof. To prove equality (6.12), we need to show by Theorem 6.3.3 that the factor

$$E = \prod_{\eta\in\Sigma} \mathrm{Res}_{A_1^\eta,A_2^\eta}(f_1^\eta, f_2^\eta)^{\mu(\eta)}$$

equals the product

$$\prod_{v \text{ vertex of } A_1 \text{ or } A_2} c_v^{\mathsf{mm}_{\mathsf{A_1},\mathsf{A_2}}(\mathsf{v})} \cdot \prod_{\eta\in\Sigma'} \mathrm{Res}_{A_1^\eta,A_2^\eta}(f_1^\eta, f_2^\eta)^{\mu(\eta)}.$$

When $\eta \in \Sigma'$, i.e. η is a common inner normal to edges of both Q_i, we get the same factor on both terms, since that our quantity $\mu(\eta)$ coincides with the index $\min\{u(e_1(\eta), A_1), u(e_2(\eta), A_2)\}$, in the notation of [18].

Assume then that η is only an inner normal to Q_2. So, A_1^η is a vertex v, $f_1^\eta = cx^v$ is a monomial (with coefficient c) and f_2^η is a polynomial whose support equals the edge e_2^η of A_2 orthogonal to η. In this case, $\mathrm{Res}_{A_1^\eta,A_2^\eta}(f_1^\eta, f_2^\eta) = c^{\ell(f_\eta)}$ by Remark 6.2.3.

For such a vertex v, denote by $\mathcal{E}(v)$ the set of those $\eta' \notin \Sigma'$ for which $v + e_2^{\eta'}$ is an edge of $Q_1 + Q_2$. Note that it follows from the proof of [18, Prop.3.13] (cf in particular Figure 1 there), that there exist non negative integers $\mu'(\eta')$ such that

$$\mathsf{mm}(v) = \sum_{\eta' \in\, \mathcal{E}(v)} \ell(e_2^{\eta'}) \cdot \mu'(\eta').$$

Indeed, $\mu(\eta') = \mu'(\eta')$.

To compute the bidegree, we use the multilinearity of the mixed volume with respect to Minkowski sum. Observe that the toric Jacobian has bidegree $(1, 1)$ in the coefficients

of f_1, f_2, from which we get that the bidegree of the resultant $\mathsf{Res}_{A_1,A_2,A_1+A_2}(f_1, f_2, J_f^T)$ is equal to

$$(2MV(A_1, A_2) + \mathsf{Vol}(Q_2),\ 2MV(A_1, A_2) + \mathsf{Vol}(Q_1)). \tag{6.14}$$

Substracting the degree of the other factors and taking into account that the bidegree of the resultant $\mathsf{Res}_{A_1^\eta,A_2^\eta}(f_1^\eta, f_2^\eta)$ equals $(\ell(e_2^\eta), \ell(e_1^\eta))$, we deduce the formula (6.13), as desired. □

6.4 The multiplicativity of the mixed discriminant

This section studies the factorization of the discriminant when one of the polynomials factors. We make the hypothesis that f_1', f_1'', f_2 have fixed support sets, and $A_1', A_1'', A_2 \subseteq \mathbb{Z}^2$. So $f_1 = f_1' \cdot f_1''$ has support in the Minkowski sum $A_1 := A_1' + A_1''$; in fact, its support is generically equal to A_1. We will denote by $\mu'(\eta)$ (resp. $\mu''(\eta)$) the integer defined in (6.7), with A_1 replaced by A_1' (resp. A_1'').

Corollary 6.4.1. *Assume A_1', A_1'' and A_2 are full planar configurations of dimension 2. Let f_1', f_1'', f_2 be generic polynomials with these supports and let $f_1 = f_1' \cdot f_1''$. Then,*

$$\Delta_{A_1,A_2}(f_1, f_2) = \Delta_{A_1',A_2}(f_1', f_2) \cdot \Delta_{A_1'',A_2}(f_1'', f_2) \cdot \mathsf{Res}_{A_1',A_1'',A_2}(f_1', f_1'', f_2)^2 \cdot E,$$

where E equals the following product:

$$\prod_{\eta\in\Sigma} \mathsf{Res}_{(A_1')^\eta,A_2^\eta}((f_1')^\eta, f_2^\eta)^{\mu'(\eta)-\mu(\eta)} \cdot \mathsf{Res}_{(A_1'')^\eta,A_2^\eta}((f_1'')^\eta, f_2^\eta)^{\mu''(\eta)-\mu(\eta)}. \tag{6.15}$$

Proof. By Theorem 6.3.3, we get that

$$\Delta_{A_1,A_2}(f_1, f_2) = \frac{R_{A_1,A_2,A_1+A_2}(f_1, f_2, J_f^T)}{\prod_{\eta\in\Sigma} R_{A_1^\eta,A_2^\eta}(f_1^\eta, f_2^\eta)^{\mu(\eta)}}, \tag{6.16}$$

and similarly for $\Delta_{A_1',A_2}(f_1', f_2)$ and $\Delta_{A_1'',A_2}(f_1'', f_2)$. Let us write the numerator of (6.16) as follows:

$$R_{A_1'+A_1'',A_2,A_1'+A_1''+A_2}(f_1'f_1'', f_2, J^T_{f_1'f_1'',f_2}),$$

where $J^T_{f_1'f_1'',f_2} = f_1' J^T_{f_1''f_2} + f_1'' J^T_{f_1',f_2}$. Let us apply Theorem 6.2.4 to re-write it as follows:

$$R_{A_1',A_2,A_1'+A_1''+A_2}(f_1', f_2, J^T_{f_1'f_1'',f_2})\, R_{A_1'',A_2,A_1'+A_1''+A_2}(f_1'', f_2, J^T_{f_1'f_1'',f_2}) =$$

$$= R_{A_1',A_2,A_1'+A_1''+A_2}(f_1', f_2, f_1'' J^T_{f_1',f_2})\, R_{A_1'',A_2,A_1'+A_1''+A_2}(f_1'', f_2, f_1' J^T_{f_1'',f_2}),$$

because the resultant of $\{h_1, h_2 + gh_1, \dots\}$ equals the resultant of $\{h_1, h_2, \dots\}$, for any choice of polynomials h_1, h_2, g (with suitable supports). We employ again Theorem 6.2.4 to finalize the numerator as follows:

$$R_{A_1',A_2,A_1'+A_2}(f_1', f_2, J^T_{f_1',f_2}) \cdot R_{A_1'',A_2,A_1''+A_2}(f_1'', f_2, J^T_{f_1'',f_2}) \cdot R_{A_1',A_1'',A_2}(f_1', f_1'', f_2)^2.$$

For the denominator of (6.16), we use again Theorem 6.2.4 to write:

$$\prod_{\eta\in\Sigma'} R_{A_1'^{\eta},A_2^{\eta}}(f_1'^{\eta}, f_2^{\eta})^{\mu'(\eta)} \cdot \prod_{\eta\in\Sigma''} R_{A_1''^{\eta},A_2^{\eta}}(f_1''^{\eta}, f_2^{\eta})^{\mu''(\eta)} =$$
$$\prod_{\eta\in\Sigma} R_{A_1'^{\eta}+A_1''^{\eta},A_2^{\eta}}(f'^{\eta}_1 f''^{\eta}_1, f_2^{\eta})^{\mu(\eta)} \cdot E,$$

because the products

$$\prod_{\eta\in\Sigma\setminus\Sigma'} R_{A_1'^{\eta},A_2^{\eta}}(f_1'^{\eta}, f_2^{\eta})^{\mu'(\eta)} = \prod_{\eta\in\Sigma\setminus\Sigma''} R_{A_1''^{\eta},A_2^{\eta}}(f_1''^{\eta}, f_2^{\eta})^{\mu''(\eta)} = 1,$$

since $f_1'^{\eta}, f_2^{\eta}$ (resp. $f_1''^{\eta}, f_2^{\eta}$) are both monomials. To conclude the proof, simply assemble the above equations. □

As a consequence, we have $\mathsf{deg}_{A_1,A_2}\,\Delta(f_1,f_2) =$

$$= \mathsf{deg}_{A_1',A_2}\,\Delta(f_1',f_2) + \mathsf{deg}_{A_1'',A_2}\,\Delta(f_1'',f_2) + 2\cdot \mathsf{deg}_{A_1',A_1'',A_2}\,R(f_1',f_1'',f_2) - \mathsf{deg}(E).$$

When all the configurations are full and with the same normal fan, all the exponents $\mu(\eta) = \mu'(\eta) = \mu''(\eta) = 1$. Therefore, $E = 1$ and no extra factor occurs.

We define $\mu_1'(\eta), \mu_1''(\eta)$ as in (6.6). Indeed, we now fix η and will simply write $\mu_1', \mu_1'', \mu_1, \mu_2$. It happens that only one of the factors associated to η can occur in E with non zero coefficient. More explicitly, we have the following corollary, whose proof is straightforward.

Corollary 6.4.2. *With the notations of Corollary 6.4.1, for any $\eta \in \Sigma$ it holds that:*

- *If $\mu_1' = \mu_1''$, then $\mu' = \mu'' = \mu$ and there is no factor in E "coming from η".*
- *If $\mu_1' \neq \mu_1''$, assume wlog that $\mu_1 = \mu_1' < \mu_1''$. There are three subcases:*
  - *If $\mu_2 \leq \mu_1$, again there is no factor in E "coming from η".*
  - *If $\mu_1 = \mu_1' < \mu_2 < \mu_1''$, then the resultant $\mathsf{Res}_{(A_1')^{\eta},A_2^{\eta}}((f_1')^{\eta}, f_2^{\eta})$ does not occur, but $\mathsf{Res}_{(A_1'')^{\eta},A_2^{\eta}}((f_1'')^{\eta}, f_2^{\eta})$ has nonzero exponent (this resultant could just be the coefficient of a vertex raised to the mixed multiplicity).*
  - *If $\mu_1 = \mu_1' < \mu_1'' \leq \mu_2$, the situation is just the opposite than in the previous case.*

6.5 Conclusion and future work

The intent of this book chapter was to present our main results relating the mixed discriminant with the sparse resultant of two bivariate Laurent polynomials with fixed support and their toric Jacobian. On our way, we deduced a general multiplicativity formula for the mixed discriminant when one polynomial factors as $f = f' \cdot f''$. This formula occurred as a consequence of our main result, Theorem 6.3.3, and generalized known formulas in the

homogeneous case to the sparse setting. Furthermore, we obtained a new proof of the bidegree formula for planar mixed discriminants, which appeared in [18].

The generalization of our formulas to any number of variables will allow us to extend our applications and to develop effective computational techniques for sparse discriminants based on well tuned software for the computation of resultants.

7. ON THE SPACE OF MINKOWSKI SUMMANDS OF A CONVEX POLYTOPE

We present an algorithm for computing all Minkowski Decompositions (MinkDecomp) of a given convex, integral d-dimensional polytope, using the cone of combinatorially equivalent polytopes. An implementation is given in sage.

7.1 Introduction

Let $A \in \mathbb{Z}^{m\times d}$ be a matrix whose row vectors $a_i \in \mathbb{Z}^d$ positively span $\mathbb{R}^d$. For $b \in \mathbb{R}^m$ the set

$$P_b = \{x \in \mathbb{R}^d \mid Ax \leqslant b\}$$

is a polytope. The set of all *non-empty polytopes* P_b arising this way can be parameterized by their right-hand side vectors b. Let us denote the set of such right hand side vectors b by

$$U(A) = \{b \in \mathbb{R}^m \mid P_b \neq \emptyset\}. \tag{7.1}$$

In this work, we present an algorithm solving the following problem:

Problem 5. Minkowski Summands. Given $A \in \mathbb{Z}^{m\times d}$ and $b \in \mathbb{R}^m$, such that $Ax \leqslant b$ is the H-representation of a convex integral polytope P_b, compute all integral MinkDecomp of P_b.

In this work, we particularly focus on the integral decomposition of polytopes. The integral decomposition of polytopes has applications in various areas of mathematics such as integer and mixed integer programming [62], polynomial factorization [52] or implicitization [42]. Since it may happen that an integral polytope has a rational but not an integral decomposition, such a distinction does make sense. Although, qualitatively, a dilation resolves this problem, in many applications, e.g., factorization of polynomials, such a step is not allowed.

Previous work on MinkDecomp algorithms mainly focuses in low dimension [43, 42, 52]. The problem of computing a Minkowski summand in general dimension is reduced to the feasibility of a linear program [66], thus deciding if a polytope is decomposable in order to test polynomial irreducibility. In [35, 62] is explored the cone of combinatorially equivalent polytopes and its computational aspects. Some classical work on polytope decomposition is presented in [74].

7.2 Computing the Space of Minkowski Summands

A system of inequalities $Ax \leqslant b$ is *feasible* if it has a solution. Feasibility is characterized by Farkas' lemma.

Lemma 7.2.1 (Farkas 1894)**.** *The system of inequalities $Ax \leqslant b$ is feasible if and only if $y^\top b \geqslant 0$ for each $y \geqslant 0$ with $A^\top y = 0$.*

The dual, $U^*(A) = \{y \in \mathbb{R}^m : y^\top b \geqslant 0 \; \forall b \in U(A)\}$, in view of Lemma 7.2.1 becomes

$$U^*(A) = \{y \in \mathbb{R}^m : A^\top y = 0 \text{ and } y \geqslant 0\}. \tag{7.2}$$

It is immediate from Equation (7.2) that $U^*(A)$ is the intersection of $\ker(A^\top)$ with the positive orthant $\mathbb{R}^m_+$ of $\mathbb{R}^m$. Therefore, $U^*(A)$ is a cone and its primal set $U(A)$ is a cone as well and both contain the origin.

Throughout we will use the following example.

Example Consider the matrix $A \in \mathbb{Z}^{10\times 3}$ and the vector $b \in \mathbb{Z}^{10}$

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \\ 0 & -1 & 1 \\ -1 & 0 & 0 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \leqslant \begin{bmatrix} 4 \\ 4 \\ 3 \\ 3 \\ 0 \\ 2 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \tag{7.3}$$

defining the polytope in Figure 7.1.

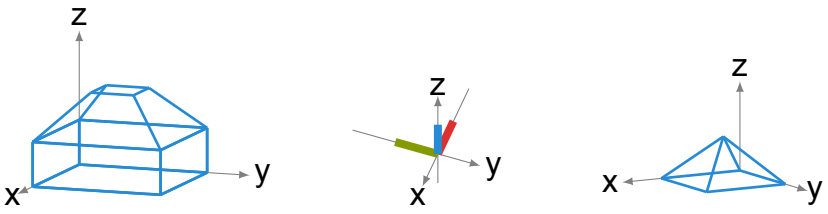


Figure 7.1: The polytope defined by System (7.3) and its 2 Minkowski summands.

The inequalities defining the cone $U(A)$ are:

$$\begin{array}{lll} b_5 + b_6 \geqslant 0 & b_4 + b_5 + b_8 \geqslant 0 & b_2 + 2b_5 + b_{10} \geqslant 0 \\ b_4 + b_7 \geqslant 0 & b_4 + b_5 + b_{10} \geqslant 0 & b_2 + b_5 + b_9 \geqslant 0 \\ b_4 + b_5 + b_8 \geqslant 0 & b_1 + b_5 + b_7 \geqslant 0 & b_1 + 2b_5 + b_8 \geqslant 0 \end{array}$$

Switching from the H-representation to its V-representation, the cone $U(A)$ is generated by 9 rays and 3 lines in $\mathbb{Z}^{10}$.

The *normal cone* of a face F of a polytope P in $\mathbb{R}^d$ is the set

$$\mathcal{N}(F;P) = \{v \in \mathbb{R}^d \mid v^\top x = h(P,v) \text{ for all } x \in F\}.$$

The dimension of the normal cone of a k-dimensional face is $(d-k)$. The *normal fan* $\mathcal{N}(P)$ *of P*, which is the collection of the normal cones of all faces of P, is a complete fan in $\mathbb{R}^d$.

The *support function* of a polytope P in $\mathbb{R}^d$, $h(P,;)$, is defined over all $u \in \mathbb{R}^d$ as $h(P,u) = \max\{u^\top x : x \in P\}$. In geometric terms, the evaluation of the support function at $u \in \mathbb{R}^d$ implies that the hyperplane $H_u : x^\top u = h(P,u)$ contains P in one of its closed halfspaces and $H_u \cap P \neq \emptyset$. We call every such H_u an *active* or *supporting hyperplane* of P.

Definition 7.2.2. Two polytopes P, Q in $\mathbb{R}^d$ are *strongly combinatorially equivalent* if, for all $v \in \mathbb{R}^d$

$$\begin{aligned}&\dim\{y \in P \mid v^\top y = h(P,v)\} = \\ &= \dim\{y \in Q \mid v^\top y = h(Q,v)\}.\end{aligned}$$

If polytopes P, Q have the same defining hyperplanes, as in our setup, their normal fans are related by inclusion, i.e., one fan is a subfan of the other. If, in addition, P, Q are strongly combinatorially equivalent, Definition 7.2.2 implies $\mathcal{N}(P) = \mathcal{N}(Q)$. We can therefore say that two polytopes are strongly combinatorially equivalent if and only if they have the same normal fan.

Let us give some definitions related to MinkDecomp. Polytopes P_1, P_2 in $\mathbb{R}^d$ are *homothetic* if $P_1 = \rho P_2 + v$ for some $v \in \mathbb{R}^d$ and $\rho > 0$.

Definition 7.2.3. A polytope P in $\mathbb{R}^d$ is called *(homothetically) decomposable* if two polytopes P_1 and P_2 exist with $P = P_1 + P_2$, where P_i in not homothetic to P for $i \in \{1,2\}$. Otherwise P is *(homothetically) indecomposable*.

A polytope P_1 is a *summand* of a polytope P (denoted as $P_1 \prec P$) if there exists a scalar $\rho > 0$ and a polytope P_2 such that $P = \rho P_1 + P_2$.

In view of the definition above, trivial polytopes, i.e., points, are indecomposable.

For $b \in U(A)$, we define the *support vector* η_b of the polytope P_b as

$$\eta_b = (h(P_b, a_1), h(P_b, a_2), \ldots, h(P_b, a_d))\,.$$

We note that $\eta_b \in \mathbb{Z}^m$ is the componentwise-least right hand side for which $P_b = P_{\eta_b}$. Let us now define the set

$$U(A)_b := \{\eta_v \mid v \in U(A) \text{ such that } P_v \prec P_b\}. \tag{7.4}$$

In [62, 74, 75], the authors show that $U(A)_b$ is a rational polyhedral subcone of $U(A)$ whose structure and extreme rays convey important information on decomposability.

Theorem 7.2.4. [74],[75] The set $U(A)_b := \{\eta_v : v \in U(A) \text{ such that } P_v \prec P_b\}$ is a rational polyhedral subcone of $U(A)$ whose extreme rays correspond to indecomposable polytopes and its interior consists of all b' for which $P_{b'}$ is strongly combinatorially equivalent to P_b.

Since $U(A)_b$ is a subcone of the homogeneous (i.e., defined by linear halfspaces) cone $U(A)$, we wish to express $U(A)_b$ as a set of linear inequalities of type $a^\top v \geqslant 0$ where $a, v \in \mathbb{R}^m$. These inequalities should be imposed from the feasibility of $Ax \leqslant v$ but, more importantly, they should incorporate the fact that strong combinatorial equivalence is preserved over all faces as well.

Since each face F of P_b can be viewed as a polytope, we can express it as a set $\{x \in \mathbb{R}^d : A_F\, x \leqslant b_F\}$ where $A_F \in \mathbb{Z}^{\lambda \times d}$, $b_F \in \mathbb{Z}^\lambda$ and $\lambda \in \mathbb{N}$. In this context, we can define $U(A_F)$ and find its subcone $U(A)_{b_F}$ containing all those $y \in \mathbb{Z}^\lambda$ for which the polytope $\{x \in \mathbb{R}^d : A_F\, x \leqslant y\}$ is combinatorially equivalent to F. However, without reference to the original polytope P_b, the computation of $U(A_F)_{b_F}$ does not keep track of the restrictions imposed on the elements of $U(A)_b$. This indicates that F should be expressed using equalities and inequalities from the original system $Ax \leqslant b$.

Example (Cont'd) We will apply the procedure described above on a face of our example. Let us pick the facet F defined by $[1, 0, 1]^\top [x, y, z] = b_1$. Then the system $A_F x \leqslant b$ for the facet F is

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \\ 0 & -1 & 1 \\ -1 & 0 & 0 \\ -1 & 0 & 1 \\ -1 & 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \leqslant \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \\ b_9 \\ -b_1 \end{bmatrix} \tag{7.5}$$

For the polyhedron defined by System (7.5), we obtain the following H-representation of $U(A_F)$:

$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \tilde{b} \geqslant \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, and by mapping the $\tilde{b}_i$'s back to the corresponding b_i's of the input system (note that $\tilde{b} = (b_0, \ldots, b_9, -b_1)$) we obtain the following two constraints: $b_2 + b_8 \geqslant 0$ and $b_1 + b_4 + b_8 \geqslant 0$.

The idea in Algorithm 4 is to repeat the above procedure for every face of the input polytope so that none of them "loses support". Note that visiting each face of P_b is essential. If, for example, in the polytope of Figure 7.1 the algorithm does not visit the top facet, then some b' in the interior of $U(A)_b$ corresponds to the square pyramid. This happens because no restriction prevents the four top vertices to behave as one. This, however,

is not acceptable since the square pyramid is not strongly combinatorially equivalent to P_b. Also, starting with $U(A)$ is necessary, since it determines the orientation of the outer normals of P_b. If in our example we started the algorithm with $U(A) = \emptyset$, then we would get the reverse square pyramid as a summand of the polytope, which is not true.

Using the knowledge of the structure of the cone of combinatorially equivalent polytopes, we can compute all indecomposable Minkowski summands of a given polytope. It is however essential, once we have computed the rays of $U(A)_b$, to read out those which produce non-trivial indecomposable polytopes. This is the content of Proposition 7.2.5.

We say that $Ax \leqslant b$, $A \in \mathbb{Z}^{m\times d}$ is an *irredundant description* of $P_b = \{x : Ax \leqslant b\}$, if the removal of any of the inequalities of the linear system, results in a different polytope (or polyhedron). Notice that this is stronger than requiring b to be the support vector η_b of P_b. The irredundant description of a full dimensional polytope P_b is unique and each of its inequalities supports P_b along a facet. Thus, if $Ax \leqslant b$ is an irredundant description of a d-polytope with m facets then $A \in \mathbb{Z}^{m\times d}$.

Below we show that, if the input is an irredundant description of P_b, then it is only the rays of $U(A)_b$ that account for the (in)decomposability of P_b.

Proposition 7.2.5. *Assume $P_b = \{x : Ax \leqslant b\}$, $A \in \mathbb{R}^{m\times d}$ is a d-polytope with m facets. Then, the generating rays $b_1, \ldots, b_k$ of $U(A)_b$ correspond to nontrivial indecomposable polytopes, while the generating lines $\pm c_1, \ldots, \pm c_d$ of $U(A)_b$ correspond to points.*

Combining Proposition 7.2.5 and Theorem 7.2.4, we deduce that each MinkDecomp of P_b into non-trivial indecomposable polytopes is a sum:

$$P_b = \lambda_1 P_{b_1} + \cdots + \lambda_k P_{b_k} + T \tag{7.6}$$

where $\lambda_1, \ldots, \lambda_k \geqslant 0$ and $T = \mu_1 P_{c_1} + \cdots + \mu_d P_{c_d}$, $\mu_1, \ldots, \mu_d \in \mathbb{R}$, is a translation.

Lemma 7.2.6. *For each polytope $P_c = \{x \in \mathbb{R}^d : Ax \leqslant c\}$, $A \in \mathbb{R}^{m\times d}$, $0 \neq c \in \mathbb{R}^d$, such that $Ax \leqslant c$ is feasible,*

1. *if $Ax \leqslant -c$ is feasible then P_c is a point*
2. *if $Ax \leqslant -c$ is not feasible then P_c is a non-trivial polytope or P_c is a point whose description $Ax \leqslant c$ contains a non-active inequality ($c \neq \eta_c$).*

Proof. Since $Ax \leqslant c$ is a polytope, feasibility of $Ax \leqslant -c$ implies the existence of a point beyond all faces of P_c. This cannot happen unless P_c is a point. Arguing as above, we see that point 2 is true when P_c is nontrivial. If, however, P_c is a point, the feasibility of both $Ax \leqslant \pm c$ fails only if the description $Ax \leqslant c$ contains a hyperplane that does not support P_c. □

Proof of Proposition 7.2.5. If a polytope P_{b_i} corresponds to an extreme ray of $U(A)_b$, then $Ax \leqslant b_i$ is feasible whereas $Ax \leqslant -b_i$ is not. Since, by definition, the cone $U(A)_b$ contains polytopes all whose inequalities are active, Lemma 7.2.6.2 rules out the case where

$\dim(P_{b_i}) = 0$. Thus, P_{b_i} is a non-trivial indecomposable summand of P_b. If, on the other hand, a polytope P_{c_i} corresponds to an extreme line of $U(A)_b$, then both $Ax \leqslant c_i$ and $Ax \leqslant -c_i$ are feasible. In this case, Lemma 7.2.6.1 implies that P_{c_i} is a point. □

If we only want to decide whether P_b is indecomposable, Proposition 7.2.5 is simplified as follows.

Corollary 7.2.7. *Let $P_b = \{x : Ax \leqslant b\}$, $A \in \mathbb{Z}^{m\times d}$ be a d-polytope with m facets. Then, P_b is indecomposable if and only if cone $U(A)_b$ has a single generating ray.*

Example (Cont'd) We consider the intersection $I = U(A) \cap_i F_i$ of all cones corresponging to faces F_i of the polytope. We compute the V-representation of $U(A)_b$ and get its rays; I is a 7-dimensional cone, with rays:

b_i	$Ax \leqslant b_i$	vertex set:
$\pm(1,1,0,0,-1,1,0,1,0,1)$	0-dim	$\{(0,0,\pm1)\}$
$\pm(1,1,0,0,-1,1,0,1,0,1)$	0-dim	$\{(\pm1,0,0)\}$
$\pm(1,0,0,1,0,0,-1,-1,0,0)$	0-dim	$\{(0,\pm1,0)\}$
$(0,0,0,0,0,0,1,1,0,0)$	1-dim	$\{(0,0,0),(0,-1,0)\}$
$(0,0,0,0,0,0,0,0,1,1)$	1-dim	$\{(0,0,0),(-1,0,0)\}$
$(1,1,0,0,0,1,0,1,0,1)$	1-dim	$\{(0,0,0),(0,0,1)\}$
$(0,0,0,0,0,1,2,2,2,2)$	2-dim	$\{(0,0,0),(-2,0,0),$
		$(0,-2,0),(-2,-2,0),\}$
		$(-1,-1,1)\}$

The rays $\pm b_1, \pm b_2, \pm b_3$ correspond to points. The next three rays correspond to line segments and the last ray corresponds to a square pyramid, which are exactly the Minkowski summands of the polytope defined by System (7.3).

In order to find integer indecomposable summands, the rays of $U(A)_b$ may not suffice since they only convey information about the combinatorial type of a polytope.

To resolve this issue, we find an appropriate integer polytope corresponding to each P_{b_i} in Equation (7.6). More precisely, we find an integer polytope $P_{b_i'}$, combinatorially equivalent to P_{b_i}, such that for all $0 < \lambda < 1$ and all $v \in \mathbb{R}^d$ the polytope $\lambda P_{b_i'} + v$ is not integer.

The first step is to dilate/shrink P_{b_i} enough, so that we get the "smallest possible" integer polytope corresponding to b_i. This can be achieved in the following way: First ensure that one of the vertices of P_{b_i} is the origin, by translating the polytope if needed. Now consider the vertices $v_j = (\frac{a_{j1}}{b_{j1}}, \ldots, \frac{a_{jd}}{b_{jd}}) \in \mathbb{Q}^d$, $1 \leqslant j \leqslant s$, of P_{b_i}, where each $\frac{a_{jk}}{b_{jk}}$ is in reduced form. Then, define:

$$\begin{aligned}\mathsf{gcd}(v_1,\ldots,v_s) &:= \mathsf{gcd}\{a_{jk} : 1 \leqslant j \leqslant s, 1 \leqslant k \leqslant d\},\\ \mathsf{lcm}(v_1,\ldots,v_s) &:= \mathsf{lcm}\{b_{jk} : 1 \leqslant j \leqslant s, 1 \leqslant k \leqslant d\}.\end{aligned}$$

It is not hard to see that $P'_{b_i} := \{x : Ax \leqslant \lambda' b_i\}$ where $\lambda' = \lambda'(P_{b_i}) := \frac{\mathsf{lcm}(v_1,\ldots,v_s)}{\mathsf{gcd}(v_1,\ldots,v_s)}$ is an integer polytope with the additional property that for any $0 < \lambda < 1$ the polytope $\lambda P'_{b_i}$ is not.

The second and final step is to find a generating set of integer translations. Rather than repeating the above procedure for the trivial polytopes P_{c_i} in Equation (7.6), we show that the columns $\tilde{c}_1, \ldots, \tilde{c}_d$ of A form a set of integer translation generators in $U(A)_b$.

Lemma 7.2.8. *Let $P_b = \{x : Ax \leqslant b\}$, $A \in \mathbb{Z}^{m\times d}$ be a d-polytope with m facets. For each $1 \leqslant i \leqslant d$ set $\tilde{c}_i := Ae_i$ where $e_1, \ldots, e_d$ is the standard basis of $\mathbb{R}^d$. The polytope $\{x : Ax \leqslant \tilde{c}_i\}$ is the unique point e_i.*

Proof. Since the rows of A positively span $\mathbb{R}^d$, the system $Ax \leqslant 0$ has a unique solution. Thus, the same holds for $Ax \leqslant Ae_i$, with unique solution e_i. □

We therefore use the vectors $\tilde{c}_1, \ldots, \tilde{c}_d \in U(A)_b$ as generators of the integer translations in $\mathbb{R}^d$.

Summarizing, we have the following algorithm:

Algorithm 4: MinkowskiSummands(A, b)

$H_i^- \leftarrow \{x \in \mathbb{R} \mid a_i x \leqslant b_i\}$
$H_i \leftarrow \{x \in \mathbb{R} \mid a_i x = b_i\}$
$R \leftarrow$ rays of ker $\left(A^\top\right) \cap \mathbb{R}^m_+$
$U(A) \leftarrow \left\{x \in \mathbb{R}^m \mid r^\top x \geqslant 0 \text{ for } r \in R\right\}$
$U(A)_b \leftarrow U(A)$
for $k \leftarrow 0 \ldots \dim(P) - 1$ **do**
  for F *face with* $\dim(F) = k$ **do**
    $I \leftarrow \{i_1, \ldots, i_\ell\} \subseteq [m]$ such that $F \subseteq H_{i_s}$
    $A_F \leftarrow \begin{bmatrix} a_i \\ -a_i \\ a_j \end{bmatrix}$ for $i \in I$ and $j \in [m] \setminus I$
    $R \leftarrow$ rays of ker $\left(A_F^\top\right) \cap \mathbb{R}^{m+\ell}_+$
    $U(A_F) \leftarrow \left\{\tilde{b} \in \mathbb{R}^{m+\ell} \mid r^\top \tilde{b} \geqslant 0 \text{ for } r \in R\right\}$
    Substitute using $\{\tilde{b}_1, \tilde{b}_2, \ldots, \tilde{b}_{d+\ell}\} = \{b_{i_1}, -b_{i_1}, \ldots, b_{i_\ell}, -b_{i_\ell}, b_{i_{\ell+1}}, \ldots, b_{i_d}\}$
    Compute H-rep of $U(A_F)$ wrt $(b_1, \ldots, b_m)$
    $U(A)_b \longleftarrow U(A)_b \cap U(A_F)$
R $\leftarrow$ rays of $U(A)_b$
Summands=$\emptyset$
for r_i *in* R **do**
  Ensure the origin is a vertex of P_{r_i}
  Compute the vertices $(\frac{a_{j1}}{b_{j1}}, \ldots, \frac{a_{jd}}{b_{jd}})$ of P_{r_i}
  $\lambda' \leftarrow \frac{\mathsf{lcm}(v_1,\ldots,v_s)}{\mathsf{gcd}(v_1,\ldots,v_s)}$
  Summands $\leftarrow \lambda' r_i$
return *Summands*

The above algorithm returns a finite set $b_1, \ldots, b_k \in \mathbb{R}^m$ which, together with $\tilde{c}_1, \ldots, \tilde{c}_d$, produces all MinkDecomp of the input polytope P_b. Thus, each way to write $b = \sum_i \lambda_i b_i +$

$\sum_j \mu_j \tilde{c}_j$ yields a decomposition of P_b as in Equation (7.6). If we want to find integral decompositions of P_b, then the choices for the above λ_i, μ_j should be integers. This allows only a finite number of decompositions.

8. APPROXIMATING MULTIDIMENSIONAL SUBSET SUM AND THE MINKOWSKI DECOMPOSITION OF POLYGONS

We consider the approximation of two NP-hard problems: Minkowski Decomposition (MinkDecomp) of lattice polygons in the plane and the closely related problem of Multidimensional Subset Sum (kD-SS) in arbitrary dimension. In kD-SS, a multiset S of k-dimensional vectors is given, along with a target vector t, and one must decide whether there exists a subset of S that sums up to t. We prove, through a gap-preserving reduction from Set Cover that, for general dimension k, the corresponding optimization problem kD-SS-opt is not in APX, although the classic $1D$-SS-opt has a PTAS. Our approach relates kD-SS with the well studied Closest Vector Problem. On the positive side, we present a $O(n^3/\epsilon^2)$ approximation algorithm for $2D$-SS-opt, where n is the cardinality of the multiset and $\epsilon > 0$ bounds the additive error in terms of some property of the input. We state two variations of this algorithm, which are more suitable for implementation. Employing a reduction of the optimization version of MinkDecomp to $2D$-SS-opt we approximate the former: For an input polygon Q and parameter $\epsilon > 0$, we compute summand polygons A and B, where $Q' = A + B$ is such that some geometric function differs on Q and Q' by $O(\epsilon\, D)$, where D is the diameter of Q, or the Hausdorff distance between Q and Q' is also in $O(\epsilon\, D)$. We conclude with experimental results based on our implementations.

8.1 Introduction

This paper considers the fundamental combinatorial problem of Subset Sum, in the context of two and higher dimensions. We relate this problem to the decomposition of convex polygons and polytopes to Minkowski summands. This is motivated by a key concept in the study of multivariate polynomial systems, namely the Newton polytope of a polynomial.

Every polynomial is related to its Newton polytope, and a theorem by Ostrowski [79] states that, if the Newton polytope of a polynomial does not have a Minkowski decomposition, then the polynomial is irreducible. Based on that, Gao [51] devised an irreducibility test for a polynomial, by checking whether its Newton polytope is decomposable. In this paper, we consider the problem of decomposition of integral polygons in the plane, by reducing this problem to a two-dimensional version of the Subset Sum. An approximate solution to the latter also provides a solution to the first. The Subset Sum problem is well studied from a theoretical perspective, but also for applications, e.g. in cryptosystems. The approximation approach on Subset Sum is mostly interested in the theoretical aspects of the problem or at least we are unaware of any practical use. The 2D-Subset Sum (generally, kD-Subset Sum) problem is defined below, and our motivation comes mainly from (approximate) factoring and irreducibility testing.

Let us start with some definitions. A polygon Q is called an (integral) *lattice polygon*, when all its vertices are points with integer coordinates.

Definition 8.1.1. The Minkowski sum of two sets of vectors A and B in Euclidean space

is defined by adding each vector in A to each vector in B, namely: $A + B = \{a + b \,|\, a \in A, b \in B\}$.

Problem 6. Minkowski Decomposition (MinkDecomp). Given a lattice convex polygon Q, decide if it is decomposable, that is, if there are nontrivial lattice polygons A and B such that $A + B = Q$, where $+$ denotes Minkowski addition. Polygons A and B are called *summands*.

Problem 6 is proven NP-complete by Gao and Lauder [52] and can be reduced to a two dimensional Subset Sum problem as defined in Problem 8. For the reduction see Section 8.4. The approximation version of MinkDecomp can be defined as follows.

Problem 7. MinkDecomp-μ-approx.
Input: A lattice polygon Q, a parameter $0 < \epsilon < 1$ and a function μ.
Output: Lattice polygons A, B such that $0 \leq \mu(A+B) - \mu(Q) < \epsilon \cdot \phi(D)$, where μ expresses a geometric property of a polygon, D is the diameter of Q, and ϕ a polynomial. We call such an output an $\epsilon \cdot \phi(D)$-solution.

Function $\mu(\cdot)$ is specialized as follows: Euclidean volume $vol(\cdot)$, polygon perimeter $per(\cdot)$, number of interior lattice points $i(\cdot)$ or, by abuse of notation, we may consider the Hausdorff distance d_H between Q and $A + B$ denoted by $d_H(Q, A + B)$ instead of $\mu(A + B) - \mu(Q)$. The problem is straightforward for $\epsilon > 1/2$ by using an enclosing rectangle.

Problem 8. kD-Subset Sum (kD-SS).
Input: A multiset of vectors $S = \{v_i \mid 1 \leqslant i \leqslant n\} \subset \mathbb{Z}^k$, for $k \geqslant 1$, and a target vector $t \in \mathbb{Z}^k$.
Output: YES, if there exists a subset $S' \subseteq S$ such that $\sum_{v_i \in S'} v_i = t$, and NO otherwise.

We use a multiset to allow for multiple occurrence of the same vector. This is a generalization of the classic $1D$-SS problem, and as such, it is also NP-complete. Here is the approximation version:

Problem 9. kD-SS-opt.
Input: A multiset $S = \{v_i \mid 1 \leqslant i \leqslant n\} \subset \mathbb{Z}^k$, for $k \geqslant 1$, and a target $t \in \mathbb{Z}^k$.
Output: Subset $S' \subseteq S$ whose corresponding vector sum $t' = \sum v_i,\ v_i \in S'$, minimizes $dist(t, t')$.

We consider the Euclidean distance l_2 throughout the paper, except where noted otherwise. Our algorithms could be generalized to any distance norm l_p, $1 \leqslant p < \infty$, due to the equivalence of any two norms on a finite-dimensional vector space. For more details see [17, Thm 8.22].

Definition 8.1.2. A PTAS (Polynomial Time Approximation Scheme) is an algorithm, which receives as input an instance of an optimization problem and a parameter $\epsilon > 0$ and, in polynomial time in input size n (but with arbitrary dependence on ϵ), produces a solution which is within a factor $1+\epsilon$ of being optimal for minimization problems or within $1-\epsilon$ of the

optimal for maximization problems. A PTAS can be specialized in two ways. An EPTAS (Efficient PTAS) has time complexity polynomial in n but independent of ϵ, and an FPTAS (Fully PTAS) has time complexity polynomial in both n and ϵ.

APX is the set of NP optimization problems that allow polynomial-time approximation algorithms with approximation ratio bounded by a constant. This class contains every problem with a PTAS.

$1D$-SS is not strongly NP-complete and can be solved exactly in pseudopolynomial time: given a multiset S of n positive integers and a target integer $t > 0$, this problem asks whether there exists a subset S' of S summing up to exactly t. This is solved in $O(nt)$ by standard methods, see [21]; in fact these methods shall inspire our algorithms below. The current record bound has been recently improved to $\tilde{O}(\sqrt{n}t)$ [67], where the soft big-Oh notation $\tilde{O}$ shows that we have ignored polylogarithmic factors. In [11], they present a simple randomized algorithm running in $\tilde{O}(n + t)$, which is likely to be near-optimal. This yields improvements upon the best known polynomial-space algorithms from time $\tilde{O}(n^3t)$ and space $\tilde{O}(n^2)$ to time $\tilde{O}(nt)$ and space $\tilde{O}(n \log t)$, assuming the Extended Riemann Hypothesis. Unconditionally, they obtain time $\tilde{O}(nt^{1+\rho})$ and space $\tilde{O}(nt^{\rho})$ for any constant $\rho > 0$ All of these results concern randomized algorithms.

Let P_i be the set of all possible vector sums that can be produced by summing up i vectors among the vectors of S. Then, $P_n \subset \mathbb{Z}^k$ is the set of all possible vector sums. Generalizing the idea of $1D$-SS, kD-SS is solved in $O(n|M_n|^k)$, where $M_n = \max P_n$ is the farthest reachable point as a sum of input vectors. Moreover, $1D$-SS-opt has an FPTAS, see [63]. A related problem is the Multidimensional Knapsack. Firstly, it was proved in [72], that this problem does not have an FPTAS. Later, in [70], it was shown that it does not have an EPTAS, while Knapsack has an FPTAS, see [95, 96]. The optimization version of $1D$-SS is a special case of Knapsack and both are defined as maximization problems. In two or higher dimensions, it makes more sense to define kD-SS as a minimization problem, since a vector sum with maximum length may be far from the target vector. In fact, in dimension two or higher, the problem is not related to Multidimensional Knapsack but rather to CVP.

In the Closest Vector Problem (CVP), we are given a set of basis vectors $B = \{b_1, \ldots, b_n\}$, where $b_i \in \mathbb{Z}^k$, and a target vector $t \in \mathbb{Z}^k$, and we have to compute the closest vector to t in the lattice $\mathcal{L}(B)$ generated by B, where

$$\mathcal{L}(B) = \{\sum_{i=1}^{n} a_i b_i \mid a_i \in \mathbb{Z}\}.$$

CVP is known to be in APX, and it is known that it cannot be approximated within a factor of $2^{\log^{1-\epsilon} n}$ with $\epsilon = (\log(\log n))^c$, for $c < 1/2$ [3, 34].

MinkDecomp has received a fair share of attention. One application is in the factorization of bivariate polynomials through their Newton polygons: Consider a bivariate polynomial $f \in K[x, y]$. To each monomial $x^i y^j$ appearing in f with a nonzero coefficient, we associate point (i, j) in the Euclidean plane. The Newton polygon of f is the convex hull of all these points. As noticed by Ostrowski in 1921, if a polynomial factors, then its Newton

polygon has a Minkowski decomposition. An algorithm for polynomial irreducibility testing using MinkDecomp is presented in [66], motivated by previous similar work in [51]. They present a criterion for MinkDecomp that reduces the decision problem to a linear programming question. In [36] they compute all possible Minkowski summands and not those in a particular Minkowski decomposition. The integer decomposition of polytopes has applications in various areas of mathematics such as integer and mixed integer programming [61].

Extending some results of [43, sec.4,5], we propose a polynomial-time algorithm that solves MinkDecomp approximately using a solver for $2D$-SS-opt. A preliminary version of most of these results can be found in [40] and in [41].

8.2 kD-SS-opt is not in APX

This section establishes that kD-SS-opt is not in APX, for general dimension k. For this, we shall adapt the approach used to prove that CVP is not in APX, see [3].

Proposition 8.2.1. *[5, Lem.4.1] For every $c > 1$ there is a polynomial time reduction that, given an instance ϕ of SAT, produces an instance of Set Cover $\{\mathcal{U}, (S_1, \ldots, S_m)\}$ where $\mathcal{U}$ is the input set of integers and $S_1, \ldots, S_m$ are subsets of $\mathcal{U}$, and integer K with the following property: If ϕ is satisfiable, there is an exact cover of size K, otherwise all set covers have size more than cK.*

Given a CNF formula ϕ we invoke Proposition 8.2.1 and get an instance of the Set Cover problem. This is a gap introducing reduction; because if ϕ is satisfiable then the instance of Set Cover has a solution of size exactly K and if ϕ is not satisfiable every solution has size at least cK for a constant c. From this instance of Set Cover we create an instance for kD-SS-opt that preserves the gap. Now, if ϕ is satisfiable, the closest vector to a given target t has distance exactly K. If ϕ is not satisfiable, the closest vector in target t has distance at least cK.

We reduce kD-SS-opt to Set Cover for norm l_1, but this can easily be generalized to any l_p, where p is a positive integer. We say that a cover is *exact* if the sets in the cover are pairwise disjoint.

Theorem 8.2.2. *Given an instance $\mathcal{U}, (S_1, \ldots, S_m), K$ of the Set Cover problem where $\mathcal{U}$ is the set of elements, $S_i \subset \mathcal{U}$ and $K \in \mathbb{Z}$, we create an instance $\{v_1, \ldots, v_m; t\}$ of kD-SS-opt. If the instance of the Set Cover has an exact cover of size K, then the minimum distance of a possible vector sum from t is smaller than K, otherwise it is larger than cK.*

Proof. Let $v_i \in \mathbb{Z}^{n+m}$, where $|\mathcal{U}| = n$. We will create such a vector v_i for every set S_i, $1 \leqslant i \leqslant m$. Let $L = cK$. Then the first n coordinates of each vector v_i have their j-th coordinate ($j \leqslant n$) equal to L if the corresponding j-th element belongs to set S_i, or 0 otherwise. The remaining m coordinates have 1 in the $(n+i)$-th coordinate and zeros everywhere else:

$$v_i = (L \cdot \chi_{S_i}, 0, \ldots, 1, \ldots 0) = (L \cdot \chi_{S_i}, e_i),$$

where χ_{S_i} is the characteristic function of the set S_i. The target vector t has in the first n coordinates L and the last m coordinates are zeros, $t = (L, \ldots, L, 0, \ldots, 0)$.

Now, let the instance of Set-Cover have an exact cover of size K. We will prove that the minimum distance of every $v \in P_n$ from target t is less than K. Without loss of generality, let the solution be $\{S_1, \ldots, S_K\}$. For each S_i, $1 \leqslant i \leqslant K$, sum the corresponding vectors v_i and let this sum be $\zeta \in \mathbb{Z}^{n+m}$:

$$\zeta = \sum_{i=1}^{K} v_i = (\underbrace{L, \ldots, L}_{n}, \underbrace{1, \ldots, 1}_{K} \underbrace{0, \ldots, 0}_{m-K}).$$

The first n coordinates must sum up to $(L, L \ldots, L)$, because if one of the coordinates was 0, the solution would not be a cover and if one of them was greater than L, then some element is covered more than once and the solution would not be exact. Note that each of the first n coordinates is either 0 or greater than L. The key point is that in the last m coordinates we will have exactly K units and everything else 0. The distance of this vector ζ from t is

$$\| - t + \zeta\|_1 = \|(\underbrace{0, \ldots, 0}_{n}, \underbrace{1, \ldots, 1}_{K} \underbrace{0, \ldots, 0}_{m-K})\|_1 = K$$

Thus, there is a point in P_n that its distance from t is at most K.

Let us consider the other direction, where the Set Cover instance has a solution set which contains a vector whose distance from t is larger than $cK = L$. We will show that the closest vector to t has distance at least L from t. This solution must have at least $cK = L$ sets. As before, $\| - t + \zeta\|_1 \geqslant L$ (this time the cover need not be exact).

Towards a contradiction, suppose there exists a vector ξ such that $\| - t + \xi\|_1 < L$. If the corresponding sets do not form a cover of S, then one of the first n coordinates of ξ is 0 and this alone is enough for $\| - t + \xi\|_1 > L$. If the sets form a cover that is not exact, then in at least one of the first n coordinates of ξ will be greater than L (for the element that is covered more than once) and will force $\| - t + \xi\|_1$ to be greater than L. Finally, if the sets form an exact cover, the first n coordinates of $\| - t + \xi\|_1$ will be 0. For the distance to be less than L, in the last m coordinates there must be less than L units implying that the sets in the cover are less than L contradicting our hypothesis.

In all cases, there cannot exist a vector whose distance from t is less than cK. □

Theorem 8.2.3. *kD-SS-opt is not in APX unless* P=NP.

Proof. Let ϕ be a given formula as an instance of SAT. Use Proposition 8.2.1 to get an instance of Set Cover and then the reduction from Theorem 8.2.2 to get an instance of kD-SS-opt. Suppose there exists an algorithm $\mathcal{A}$ for kD-SS-opt that is in APX. $\mathcal{A}$ returns a vector t' such that $\|t - t'\|_1 \leqslant (1+\epsilon)OPT$, where $OPT = \|t - t^*\|_1$ and t^* is the closest vector in P_n. From Theorem 8.2.2, if ϕ is satisfiable then $OPT \leqslant K$, and if ϕ is not satisfiable, then $OPT > cK$.

We must run algorithm $\mathcal{A}$ with a suitable parameter ϵ so we can distinguish if the optimum solution t^* is within distance K or not. When ϕ is satisfiable we would want $(1 + \epsilon)K <$

$cK \implies \epsilon < c-1$. Set $c' < c-1$, call $\mathcal{A}$ with parameter $\epsilon = c'$ and let t' be the returned vector. In the case where ϕ is satisfiable and $OPT \leqslant K$ we have

$$\|t - t'\|_1 \leqslant (1+\epsilon)OPT < cK$$

Of course if ϕ is not satisfiable for any t' we have that $\|t-t'\|_1 > cK$. Thus, $\|t-t'\|_1 < cK$ if and only if ϕ is satisfiable. Since ϵ is a constant and $\mathcal{A}$ is in APX, we can decide SAT in polynomial time. □

Although there can be no algorithm that returns a constant factor approximation with multiplicative error for general dimension k, we will present algorithms that approximate the solution with additive error, in the plane. Specifically, the returned vector t' is an $(OPT+\epsilon M_n)$ solution, where $M_n = \max P_n$ is the largest possible vector sum.

8.3 Approximation algorithms for $2D$-SS-opt

This section presents and analyzes three algorithms for $2D$-SS-opt with additive error. The first is meant to introduce our algorithmic tools. The next two are implemented since they are more efficient in practice. The last one, the hybrid algorithm, combines ideas from the first two, namely $\mathrm{annulus\text{-}slice}$ and the grid-based algorithm. Whenever we refer to distance, it is the Euclidean distance.

8.3.1 The $\mathrm{annulus\text{-}slice}$ algorithm

The idea of this algorithm is to create all possible vector sums, step by step. At each step, if two vector sums are close to each other, one is deleted. The algorithm is given in Algorithm 5, Algorithm 6. Let us start with some notation.

- Input: the multiset $S = \{v_i \mid 1 \leqslant i \leqslant n\}$ for $v_i \in \mathbb{Z}^2$ and a parameter $0 < \epsilon < 1$ that bounds the Euclidean distance between the optimal and the returned solution.
- P_i is the set of all possible vectors that can be produced by adding the first i vectors from S. P_n is the set of all possible vector sums.
- $E_i = L_{i-1} \cup [w + v_i \mid w \in L_{i-1}]$ is the list created at the beginning of every step and that is about to get trimmed.
- $L_i = \mathrm{trim}(E_i, \delta)$ is the trimmed list and $\delta = \epsilon/2n,\ 0 \leqslant \delta \leqslant 1$. Notice that $L_i, E_i \subset \mathbb{Z}^2$.

At the beginning of the i-th step we create the list $E_i = L_{i-1} \cup [w + v_i \mid w \in L_{i-1}]$. Notice that addition is over $\mathbb{Z}^2$. After a point is found we calculate its length, sort E_i based on the lengths and call $\mathrm{trim}\ (E_i, \epsilon/2n)$. For each vector $u \in E_i$ with length $|u|$ and angle $\theta(u)$ from the x-axis, check all the vectors $u' \in E_i$ that have length that satisfy the condition:

$$|u| \leqslant |u'| \leqslant (1+\delta)|u|. \tag{8.1}$$

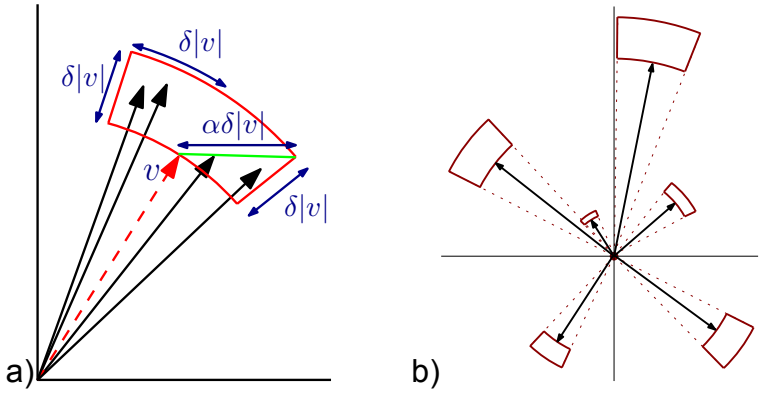


Figure 8.1: a) A single cell for the dashed vector v. All vectors in the cell will be deleted. The distances are shown and the furthest point is in distance $\alpha\delta|v|$. b) After the trim a few cells remain. Every vector in the cells will be deleted and "represented" by one of the black vectors shown. Notice that the size of each cell depends on the vector that creates it: the shorter the vector the smaller the cell.

If they also satisfy the condition:

$$\theta(u) - \delta \leqslant \theta(u') \leqslant \theta(u) + \delta, \tag{8.2}$$

remove u' from E_i. The remaining trimmed list is the list L_i. The two conditions ensure that $dist(u', u) \leqslant \alpha\delta|u|$, where $1 \leqslant \alpha \leqslant 2$ is a constant. Indeed as seen in Figure 8.1 a), we use the cosine rule for the angle $\theta(u) - \theta(u')$ which is at most δ to get the desired.

Every vector that is deleted from E_i is not very far away from a vector in L_i:

$$\forall u \in E_i, \exists w \in L_i : u = w + r_w,\ |r_w| \leqslant \alpha\delta|w| \tag{8.3}$$

hence, $|w| \leqslant |u| \leqslant (1+\delta)|w|$. See Figure 8.1.

Since all vectors have integer coordinates, any vector $u \in E_i$ such that $|u| < 1/\alpha\delta < \sqrt{2}n/\epsilon$ implies that $\alpha\delta|u| < 1$. Thus, the area around u does not contain any other other lattice points except u.

Lemma 8.3.1. *Using the above notation, call function* $L_i = \mathrm{trim}(E_i, \delta)$*, with parameter* $\delta = \epsilon/2n$ *and let* $M_i = max\{|u| : u \in E_i\}$*, the vector in* E_i *with the largest length. It holds that* $|L_i| = O(n^3\epsilon^{-2})$ *for* $1 \leqslant i \leqslant n$.

Proof. Every vector in E_i has length between $(1+\delta)^r$ and $(1+\delta)^{r+1}$. These are circles with center $(0,0)$ and radius $(1+\delta), (1+\delta)^2, \ldots, (1+\delta)^r$ for some r. We call every two successive circles from an annulus a zone. We must cover all $u \in P_n$, and r is the minimum such that $(1+\delta)^r > M_n$, where M_n is the vector in E_n with the largest length. Solving $(1+\delta)^r \geqslant M_n$ for r, we get $r \geqslant \log_{1+\delta} M_n$. We know that $\log(1+\delta) \leqslant \delta$ for $\delta > -1$. Therefore

$$r \geqslant \frac{\log M_n}{\log(1+\delta)} \geqslant \frac{\log M_n}{\delta}.$$

Thus $r = O(n \ln M_n/\epsilon)$. Therefore, there are $O(n \log M_n/\epsilon) = O(n^2/\epsilon)$ many zones that can be created. Every zone is divided into cells. Each cell is taken in such a way that it covers $2\delta R$ of the inner circle of the zone, where R is the radius of this circle (Figure 8.1a). Thus, every zone between the circles with radius R and $(1+\delta)R$ has at most $2\pi R/\delta R = 4\pi n/\epsilon$ cells.

Since a list L_i has at most an entry for every cell created in every zone, its size can be at most $(n^2/\epsilon) \cdot (4\pi n/\epsilon) = O(n^3\epsilon^{-2})$. □

Function trim uses time $|E_i|$ to consider all vectors and, in the worst case, we have to check each vector in E_i against all others, thus leading to time $O(|E_i|^2) = O(|L_i|^2)$. Algorithm 6 takes time $n \cdot T(\mathrm{trim}) = O(n|L_n|^2)$ and overall, from Theorem 8.3.1, requires time $O(n^5\epsilon^{-4} \log^2 M_n)$. The algorithm stores at each step list L_i, so space consumption is $O(n^2\epsilon^{-2} \log M_n)$.

Theorem 8.3.2. *For $\delta = \epsilon/2n$, the running time of Algorithm 6 is in $O(n^5\epsilon^{-4} \log^2 M_n)$, and the space required is in $O(n^2\epsilon^{-2} \log M_n)$.*

Algorithm 5: trim

input : $E \subset \mathbb{Z}^2$, $0 \leqslant \delta \leqslant 1$
output: a trimmed list $L \subset \mathbb{Z}^2$

sort(E)
for $v_k \in E$ **do**
  $i = 1$
  while $|v_{k+i}| \leqslant (1+\delta)|v_k|$ **do**
    if $\theta(v_{k+i}) - \delta \leqslant \theta(v_k) \leqslant \theta(v_{k+i}) + \delta$ **then**
      remove v_{k+i} from E
    $i = i + 1$
return *E*

Algorithm 6: annulus-slice

input : $S \subset \mathbb{Z}^2$, $0 \leqslant \epsilon \leqslant 1$
output: all approximation points $L_n \subset \mathbb{Z}^2$

L_0=∅
for $v_i \in S$ **do**
  $E_i = L_{i-1} \cup [L_{i-1} + [v_i]]$
  $L_i = \mathrm{trim}\ (E_i, \epsilon/2n)$
return L_n

Let us now establish correctness of the algorithm.

Lemma 8.3.3. *For a multiset $S = \{v_i \mid 0 \leqslant i \leqslant n\}$ where $v_i \in \mathbb{Z}^2$, every possible vector sum $v \in P_n$ can be approximated by a vector w such that*

$$\forall v \in P_n, \exists w \in L_n, \exists r_w \in \mathbb{Z}^2 : v = w + r_w,\ |r_w| \leqslant n\delta M_n,$$

Proof. The proof is by induction. The base step, it is easy to see that if we only have one element the theorem holds. The induction hypothesis

$$\forall v \in P_{n-1}, \exists w \in L_{n-1}, \exists r_w : v = w + r_w,\ |r_w| \leqslant (n-1)\delta M_{n-1}.$$

Now suppose $v \in P_n \setminus P_{n-1}$ because, if $v \in P_{n-1}$, the theorem holds straight from the induction hypothesis. We write v as $v = z + v_n,\ z \in P_{n-1}$, and the induction hypothesis holds for z, thus

$$\exists p \in L_{n-1}, \exists r_p : z = p + r_p,\ |r_p| \leqslant (n-1)\delta M_{n-1}. \tag{8.4}$$

Since $p \in L_{n-1}$ this means that $p + v_n \in E_n$ and $L_n = \mathrm{trim}\ (E_n)$. From the guarantee of function trim we know that

$$\exists q \in L_n : p + v_n = q + r_q,\ |r_q| \leqslant \delta|q|. \tag{8.5}$$

From (8.4), (8.5) we obtain $v = z + v_n = p + v_n + r_p = q + r_q + r_p$. This proves that for $v \in P_n$, there exists a vector $q \in L_n$ that approximates it; but how close are they? We will bound the length $|r_q + r_p|$. From (8.4) we get

$$|r_p| \leqslant (n-1)\delta\, \mathsf{max}\{L_{n-1}\} \leqslant (n-1)\delta M_n,$$

and from (8.5) we get

$$|r_q| \leqslant \delta|q|,\ q \in L_n \implies |r_q| \leqslant \delta M_n.$$

Thus,

$$|r_q + r_p| \leqslant |r_q| + |r_p| \leqslant (n-1)\delta M_n + \delta M_n \leqslant n\delta M_n.$$

□

Setting $\delta = \epsilon/2n$, we ensure that every possible vector sum will be approximated by a vector in L_n at most ϵM_n far (Figure 8.2). Implementing and testing the algorithm, much better bounds are obtained, see Section 8.5.

8.3.2 Grid-based algorithm

In this subsection we describe a $O(n^3/\epsilon^2)$ approximation grid-based algorithm for $2D$-SS. The input is a multiset $S = \{v_i \mid 1 \leqslant i \leqslant n\}$, $v_i \in \mathbb{Z}^2$. We define the list $E_i = L_{i-1} \cup [w + v_i \mid w \in L_{i-1}]$ and, at step i, we trim it via Algorithm 5, using parameter δ to obtain trimmed list $L_i = \mathrm{trim}\ (E_i, \delta) \subset \mathbb{Z}^2$. Let P_i be now the set of all possible vector sums defined by any subset of the first i vectors of S.

It turns out that the same approximation ratio ϵM_n can be achieved by a faster algorithm that subdivides the plane into a grid, where vector $M_n \in E_i$ has maximum length. Instead of creating different annulus-slice cells, we define a regular orthogonal grid $[-M_n, M_n] \times [-M_n, M_n]$, where each square cell has edge of length $d = \epsilon M_n/2n$.

For each $v(x, y) \in E_i$, the trimmed list L_i stores the vector with its coordinates rounded to an integer multiple of d:

$$\forall v(x, y) \in E_i \, \exists w(x', y') \in L_i : x' = \left\lfloor \frac{x}{d} \right\rfloor, \, y' = \left\lfloor \frac{y}{d} \right\rfloor$$

and

$$dist(v, w) \leq \sqrt{2}d = \frac{\epsilon M_n}{\sqrt{2}n} \leqslant \frac{\epsilon M_n}{n}$$

and the maximum value reaches when v and w are in the diagonal of the cell.

The whole grid has size $2M_n$ and since $d = \epsilon M_n/2n$ the grid has $O((M_n/d)^2) = O((n/\epsilon)^2)$ cells. In the worst case we will have a vector in every cell and this means that the time to traverse the lists E_i at each step is $O(n^2\epsilon^{-2})$. Since we have n lists the total running time of the new algorithm is $O(n^3\epsilon^{-2})$ and the space requirements are $O(n^2\epsilon^{-2})$.

Also, every $u \in P_n$ is the sum of at most n vectors from S. In the worst case, every time we call trim, we represent a vector $u \in E_i$ by another one that has distance form u at most d. In that case we lost at most $nd = \epsilon M_n/2$:

$$\forall v \in P_n \exists w \in L_n : dist(v, w) \leqslant \epsilon M_n.$$

Thus, for every given target vector t the algorithm will return an approximation solution that is $nd = \epsilon M_n$ far from being optimum. See Figure 8.2.

Theorem 8.3.4. *The grid-based algorithm runs in time $O(n^3\epsilon^{-2})$, requires space $O(n^2\epsilon^{-2})$ and returns a solution t' such that $dist(t, t') \leqslant OPT + \epsilon M_n$.*

In the 2D case there is a factor of $\sqrt{2}$ that we omit from our approximation. This happens because the maximum distance inside a cell is not d but $\sqrt{2}d$. In general dimension k, the minimum distance is $\sqrt{k}d$ and this affects the algorithm in higher dimensions. However, using a general principle to turn pseudopolynomial dynamic programming algorithms into approximation algorithms, see [95, 96], the algorithm generalizes to higher dimensions.

8.3.3 Hybrid algorithm

In this subsection we describe an algorithm that is a combination of $\mathrm{annulus\text{-}slice}$ and the grid-based algorithm, and is expected to perform better in practice.

The grid-based algorithm reduces the length of a vector by at most d. This reduction does not depend on the length of the vectors. On the other hand, it is fast, because it does not have to check any other vectors; for every vector it sees it rounds it on the spot, thus having linear time in the size of the lists. We can make a version of a circular grid, where each cell does not have a constant side length. For small vectors we create smaller cells and, as the length increases, so does the cell side. This way we can provide a better experimental approximation ratio. At step i, we have the list E_i and we trim it with a factor δ. We will consider the polar coordinates of the vectors. For a vector $v(\phi, r)$ let $\phi = \theta(v)$

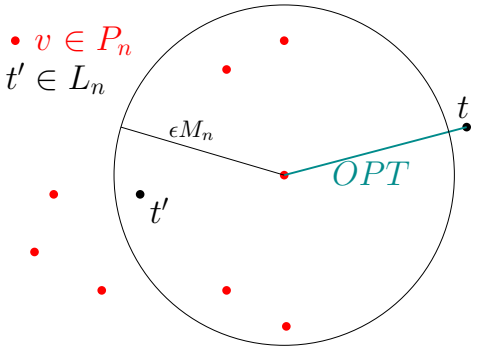


Figure 8.2: For every t the returned vector t' is in distance at most $\epsilon M_n + OPT$, where OPT is the optimum distance.

be the angle with the x axis and $r = |v|$ its Euclidean length. Let v be a vector in E_i and, to get the list L_i, we will replace v by $v' = (\phi', r')$. First round its angle to a multiple of $\delta : \phi' = \lfloor \phi/\delta \rfloor$. Next, we round its length. The idea is to round in such a way that shorter vectors are approximated better than the longer ones. We construct an array A with all the acceptable rounded lengths. The entries of A are the lengths $[1, (1+\delta), \ldots, (1+\delta)^i]$ for the minimum i, such that $(1+\delta)^i > M_n$. Solving this inequality we get that $i = O(n \log M_n/\epsilon)$, and this is the size of A.

Now, for a vector v we just make a binary search in A for $|v|$ that returns the zone such that $(1+\delta)^k \leqslant |v| \leqslant (1+\delta)^{k+1}$ and $r' = bin\_search(A, |v|) = (1+\delta)^k$. The plane is divided in $O(\delta) = O(n/\epsilon)$ angles and $O(n \log M_n/\epsilon)$ different lengths. Each E_i has size $O(n^2\epsilon^{-2} \log M_n)$. We have saved a quadratic factor, but incurred $\log |E_i|$ for binary search. The whole algorithm runs in

$$O(n|E_i| \log |E_i|) = O(n^3\epsilon^{-2} \log M_n \log \frac{n^2 \log M_n}{\epsilon^2})$$

and guarantees the same approximation error, since $\forall v \in E_i, \exists w \in Li : dist(v, w) \leqslant \epsilon|w|$ as before. Lastly, the binary search may be avoided by using a method to round the lengths in $O(1)$ time, thus avoiding the $\log |E_i|$ factor. Therefore we arrive at the following lemma:

Lemma 8.3.5. *With the above notation, the hybrid approximation algorithm runs in time* $O(n^3\epsilon^{-2} \log M_n)$.

We expect the algorithm to offer better approximations in practice.

8.4 Approximating Minkowski Decomposition using $2D$-SS-opt

In this section, we describe an algorithm for approximating MinkDecomp. We also state the connection between the Problem 7 and the proposed algorithm in Theorem 8.4.3, where we describe the solution that the algorithm provides for the MinkDecomp-μ-approx.

The algorithm takes an input polygon Q, transforms it to an instance $\{S, t\}$ of $2D$-SS-opt and calls the algorithm for the latter. Then the output is converted to an approximate solution to MinkDecomp. We remark that the algorithms for $2D$-SS-opt return an array of several possible solutions. So the trivial ones can be ruled out.

Let Q be the input to MinkDecomp: $Q = \{v_i \mid 0 \leqslant i \leqslant n\}$ for $v_i \in \mathbb{Z}^2$, such that $\sum_0^n v_i = (0,0)$. First, we create the multiset $s(Q)$ of vectors by subtracting successive vertices of Q (in clockwise order): $s(Q) = \{v_0 - v_1, v_1 - v_2, \ldots, v_n - v_0\}$. Each vector in $s(Q)$ is called an *edge vector* and $s(Q)$ is called the *edge sequence* of Q:

Algorithm 7: approx-MinkDecomp

input : polygon Q, $0 \leq \epsilon \leq 1$
output: polygon Q'

S = primitive_edge_sequence(Q)
//get the edge sequence for the two summands
s(A) = approx-2D-SS (S,(0,0))
s(B) = S\A
A=get-points(s(A))
B=get-points(s(B))
return *Q'= A + B*

Definition 8.4.1. Let $v = (a, b) \in \mathbb{Z}^2$ be a vector and $d = \mathsf{gcd}(a, b) \in \mathbb{N}$. The *primitive vector of* v *is* $e = (a/d, b/d)$.

For every edge vector $(x, y) \in s(Q)$ we calculate its primitive vector $e = (x/d, y/d)$. For each vector in $s(Q)$, we compute the scalars $d_0, \ldots, d_{\lfloor \log_2 d/2 \rfloor + 1}$ as follows:

$$d_i = 2^i,\ i = 0, \ldots, \lfloor \log_2 d/2 \rfloor \text{ and } d_{\lfloor \log_2 d/2 \rfloor + 1} = d - \sum_{i=0}^{\lfloor \log_2 d/2 \rfloor} d_i.$$

Thus, $\sum_{i=0}^{\lfloor \log_2 d/2 \rfloor + 1} d_i = d$. We include in S the vectors $d_i e$ and repeat the procedure for all vectors $v \in s(Q)$,

$$S = \{(x/d, y/d)2^i \mid i = 0, \ldots, \lfloor \log_2 d/2 \rfloor, \lfloor \log_2 d/2 \rfloor + 1,\ d = \mathsf{gcd}(x, y) : (x, y) \in s(Q)\}.$$

The sum of all vectors in S is also $(0, 0)$. Using this construction, the number of the primitive vectors included are about $\log d$ for every $v \in s(Q)$ keeping the size of S polynomial with respect to the number of edges of Q.

As an example take an edge with endpoints $(0, 0)$ and $(100, 0)$ and the associated vector is $v = (100, 0)$. Then $d = 100$ and $e = (1, 0)$. Instead of including the vector $(1, 0)$ 100 times we include in $s(Q)$ the vectors: $(1, 0), (2, 0), (4, 0), (8, 0), (16, 0), (32, 0)$ and $(37, 0)$. Multiset S corresponds to a unique polygon up to translation determined by v_0. This is a standard procedure, as in [43, 52].

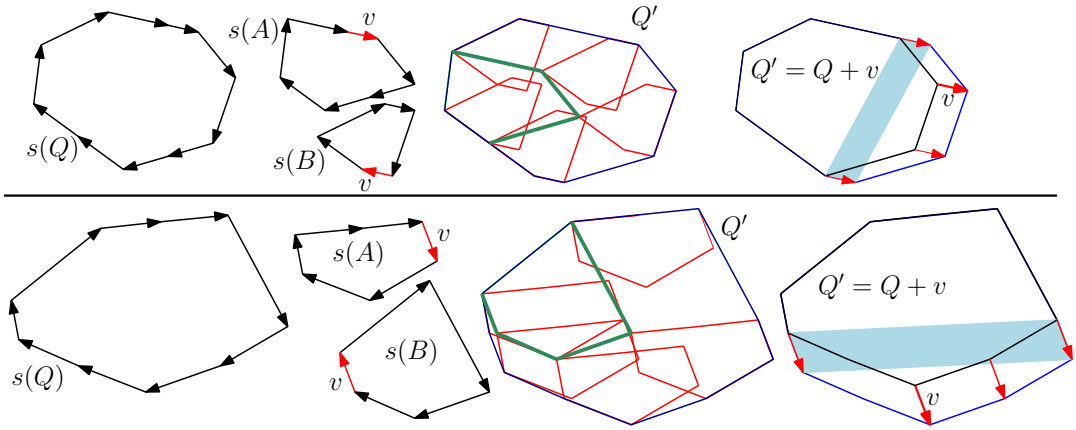


Figure 8.3: Two examples for two polygons Q. Their summands are shown and the red vector v is the new vector added to fill the gap. At the end, the new polygon Q' is Minkowski Sum of the two summands.

Summarizing, the size of S is in $O(n \log d)$. If we employ the grid algorithm for $2D$-SS-opt, Algorithm 7 has time complexity $O(n^3 \log^3 D\epsilon^{-2})$, where $D = \max_{v \in s(Q)} d$, and it returns the multiset of vectors s_a and $s_b = S \setminus s_a$.

The weakness in this approach is that the algorithm returns a sequence of vectors that sums up to a vector close to $(0,0)$ but possibly not $(0,0)$. Hence the corresponding edge sequence does not form a closed polygon. To overcome this, we include in s_a the vector v, defined so that when added to the last point it yields the first one. If the vectors in s_a sum up to point (x,y), by including vector $v = (-x,-y)$ the edge sequence $s_a \cup \{v\}$ sums up to $(0,0)$. If we order the vectors by their angles, they form a closed, convex polygon denoted by A'. We do the same for the sequence s_b. The vector used is $-v = (x,y)$ and this sequence (ordered) also forms a closed, convex polygon, denoted by B'. Let $s(A') = s_a \cup \{v\}$, $s(B') = s_b \cup \{v\}$ be the edge sequences, and consider Minkowski Sum $Q' = A' + B'$. We now measure the difference between Q' and Q. Let D denote the diameter of Q, which is the maximum distance between two vertices of Q.

Lemma 8.4.2. *Let Q be the input polygon of diameter D, and Q' be the polygon computed above. Let $vol(\cdot)$ stand for Euclidean volume, $per(\cdot)$ for polygon perimeter, $i()$ for the number of interior lattice points, and let $d_H(\cdot,\cdot)$ denote the Hausdorff distance between two polygons. We deduce that:*

1. $vol(Q) \leqslant vol(Q') \leqslant vol(Q) + \epsilon D^2$,
2. $per(Q) \leqslant per(Q') \leqslant per(Q) + 2\epsilon D$,
3. $i(Q) \leqslant i(Q') \leqslant i(Q) + \epsilon D^2$,
4. $d_H(Q,Q') \leqslant \epsilon/2D$.

Proof. We observe that

$$s(Q') = s(A') \cup s(B') = s_a \cup s_b \cup \{v\} \cup \{-v\} \implies$$
$$s(Q') = s(Q) \cup \{v\} \cup \{-v\}.$$

This equals adding to Q a single segment s of length $|s| = |v|$ and $Q' = Q + s$. The length of vector v we add to close the gap, is the key factor to bound polygon Q'. From the guarantees of the $2D$-SS-opt solution, we know that s_a (respectively, s_b) sum up to a vector with length at most $\epsilon \max\{L_n\}$. This is vector v and thus $|v| \leqslant \epsilon \max\{L_n\}$. Since $\max\{L_n\} \leqslant D$, we get $|s| = |v| \leqslant \epsilon D$.

It follows that:

1. $per(Q) = \sum_{v \in s(Q)} |v|$, it follows $per(Q') = per(Q) + 2|v| \leqslant per(Q) + 2\epsilon D$.
2. $vol(Q') \leqslant vol(Q) + sD \leqslant vol(Q) + \epsilon D^2$.
3. By Pick's theorem, $vol(Q) = i(Q) + b(Q)/2 - 1 \implies i(Q) = vol(Q) - b(Q)/2 + 1$. Note that $b(Q) = \sum_{\forall v \in s(Q)} d_v$, where $v = (x, y) \in s(Q)$ and $d_v = \gcd(x, y)$, as is Definition 8.4.1. Now, $i(Q') = i(Q) + i(sD)$, since sD is the maximum volume added, and $i(sD) \leqslant sD - b(sD)/2 + 1 \leqslant sD - 1 \leqslant \epsilon D^2$. Thus, $i(Q') \leqslant i(Q) + \epsilon D^2$
4. If we translate Q by $s/2$ units in the direction of v, then $d_H(Q, Q') = s/2 \implies d_H(Q, Q') \leqslant \epsilon D/2$.

□

Therefore Theorem 8.4.2 solves Problem 7. A hard case is illustrated in Figure 8.4, where the added vector is (almost) perpendicular to D maximizing the extra volume and number of interior lattice points. Theorem 8.4.2 leads to the following conclusion:

Theorem 8.4.3. *The proposed algorithm provides a $2\epsilon D$-solution for MinkDecomp-per-approx, an ϵD^2-solution for MinkDecomp-vol-approx and MinkDecomp-$latt\_p$-approx, and an $\epsilon/2D$-solution for MinkDecomp-d_H-approx.*

8.5 Implementation and experimental results

This section discusses the implementation of Algorithm 6 and Algorithm 7, both developed in Python3. The code can be accessed on Github [1] and is roughly 750 lines long.

To test Algorithm 6 we created vectors v_i at random with $|v_i| \leqslant 5000$. For Algorithm 7 we create random points and take their convex hull to form input polygon Q. All tests were executed on an Intel Core i5-2320 @ 3.00 GHz with 8Gb RAM, 64-bit Ubuntu GNU/Linux.

[1] https://github.com/tzovas/Approximation-Subset-Sum-and-Minkowski-Decomposition

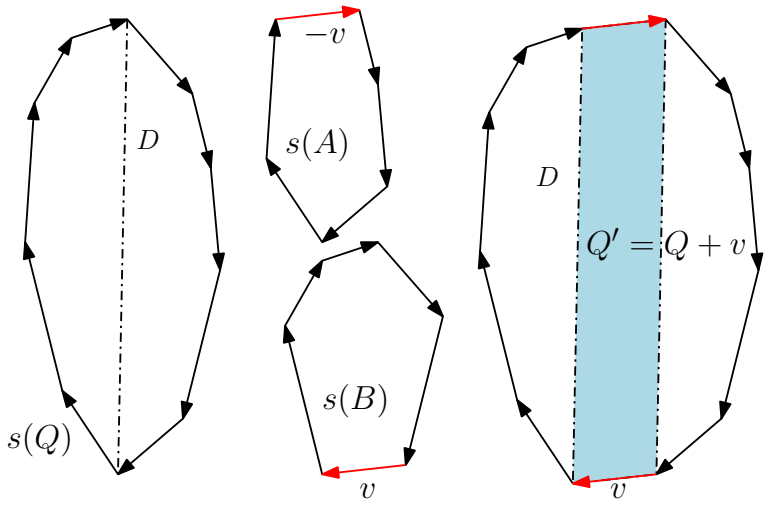


Figure 8.4: A worst case example where the vector v is (almost) perpendicular to the diameter D maximizing the extra volume added. Moreover, D and v have no lattice points thus the interior points added are also maximum (D is not vertical).

#vertices	#examples	vol(Q)/vol(Q')	per(Q)-per(Q')	Hausdorff	ϵ	time(sec)
3-10	51	0.93	18.55	3.32	0.18	4.1
11-16	45	0.977	3.43	1.81	0.33	126.4
17-25	54	0.994	1.12	1.25	0.38	377.5

Table 8.1: Results for MinkDecomp-μ-approx: input polygon Q, output Q' ($per(Q) > 1000$). We measure volume, perimeter and Hausdorff distance and present their mean values.

Results for Algorithm 6 are shown in Figure 8.5 and for Algorithm 7 in Table 8.1. It is clear in Figure 8.5 that our results stay below the expected time and behave analogously. In Table 8.1 the results obtained are much better than the proven bounds and in most cases volume and perimeter are almost the same and the polygons differ slightly.

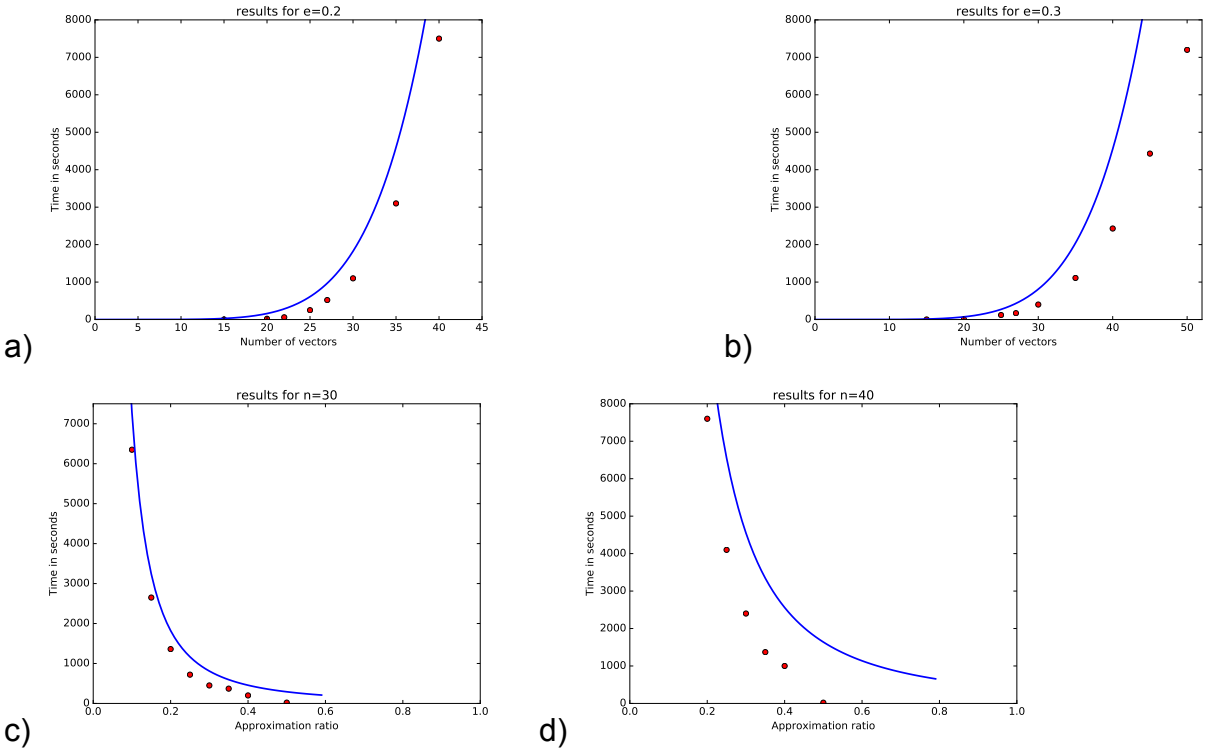


Figure 8.5: Experimental results for $2D$-SS-opt : a) $\epsilon = 0.2$, b) $\epsilon = 0.30$, c) $n = 30$, and d) $n = 40$. The blue line represents the expected time, the red dots correspond to our experiments.

9. EXTENSIONS AND OPEN PROBLEMS

Several intriguing open questions emerge by the study of this thesis.

From the computational algebra and combinatorics point of view one direction is to generalize the result of Chapter 5 to multi-symmetric polynomials or other types of symmetry. The case of non-homogeneous polynomials can also be studied. The other direction is the generalization of our formulas in Chapter 6 to any number of variables. This will allow us to extend our applications and to develop effective computational techniques for sparse discriminants based on well tuned software for the computation of resultants.

From the Computational Geometry, Optimization and Algebraic Algorithms point of view there are some related problem to Chapters 7 and 8. The first one is given $A \in \mathbb{Z}^{m\times d}$ and $b \in \mathbb{Z}^m$, such that $Ax \leqslant b$ is the H-representation of a convex (integral) polytope P_b, define and compute approximate (integral) summands. The second one would be to employ these methods in algebraic problems like approximate polynomial factoring or irreducibility testing. Given a polynomial f_Q defined on its Newton polygon Q, we use MimkDecomp to find an approximation decomposition $Q' = A' + B'$. Using the irreducibility test in [85], we either find a bivariate factorization or that $f_{Q'}$ is irreducible. In the latter case, we use approximate polynomial factorization [65]. All monomials of f_Q lie in the support of $f_{Q'}$, therefore the corresponding coefficients are constrained by those of f_Q. So, we need to determine whether there exist valid coefficients for the monomials that correspond to lattice points in $Q' \setminus Q$.

REFERENCES

[1] M. Aguiar, C. André, C. Benedetti, N. Bergeron, Z. Chen, P. Diaconis, A. Hendrickson, S. Hsiao, I. M. Isaacs, A. Jedwab, and et al. Supercharacters, symmetric functions in noncommuting variables, and related hopf algebras. *Advances in Mathematics*, 229(4):2310–2337, 2012.

[2] F. Apery and J.-P. Jouanolou. Elimination: le cas d'une variable. *Collection Methodes*, 2006.

[3] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. *Journal of Computer and System Sciences*, 54(2):317 – 331, 1997.

[4] R. Barakat. Characteristic polynomials of chemical graphs via symmetric function theory. *Theoret. Chim. Acta*, 69:35–39, 1986.

[5] M. Bellare, S. Goldwasser, C. Lund, and A. Russell. Efficient probabilistically checkable proofs and applications to approximations. In *Proceedings of the Twenty-fifth Annual ACM*, STOC '93, pages 294–304, New York, NY, USA, 1993. ACM.

[6] O. Benoist. Degré d'homogénéité de l'ensemble des interactions complexes singulieres. *Annales de l'Institut Fourier*, 62(3):1189–1214, 2012.

[7] M. Berger. *Geometry I*. Springer, 1987.

[8] D. N. Bernstein. The number of roots of a system of equations. *Funct. Anal. and Appl.*, 9(2):183–185, 1975.

[9] F. Bihan, J. M. Rojas, and C. E. Stella. Faster real feasibility via circuit discriminants. In *Proc. ACM ISSAC*, pages 39–46, 2009.

[10] J. Bosman. A polynomial with galois group $sl_2(\mathbb{F}_{16})$. 2007.

[11] K. Bringmann. A near-linear pseudopolynomial time algorithm for subset sum. In *Proc. ACM-SIAM Symposium on Discrete Algorithms*, pages 1073–1084, Philadelphia, USA, 2017. SIAM.

[12] L. Busé and J.-P. Jouanolou. A computational approach to the discriminant of homogeneous polynomials. *Preprint*, 2012.

[13] L. Busé and J.-P. Jouanolou. On the discriminant scheme of homogeneous polynomials. *Math. Comput. Sci.*, 8(2):175–234, 2014.

[14] L. Busé and A. Karasoulou. Resultant of an equivariant polynomial system with respect to the symmetric group. *Journal of Symbolic Computation (Elsevier)*, 76:142–157, 2016.

[15] J. F. Canny. The complexity of robot motion planning. *M.I.T. Press*, 1988.

[16] J. F. Canny and I. Z. Emiris. Efficient incremental algorithms for the sparse resultant and the mixed volume. *J. Symb. Comput.*, 20(2):117–149, 1995.

[17] N. L. Carothers. *Real Analysis*. Cambridge University Press, 2000. Cambridge Books Online.

[18] E. Cattani, M. A. Cueto, A. Dickenstein, S. Di Rocco, and B. Sturmfels. Mixed discriminants. *Math. Z.*, 2013.

[19] E. Cattani, A. Dickenstein, and B. Sturmfels. Residues and resultants. *Journal of Math. Sciences*, 5:119–148, 1998.

[20] H. Cheng and Z. Han. Minimal kinematic constraints and mt2. *JHEP 0812:063*, 2008.

[21] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms, Third Edition*. The MIT Press, 3rd edition, 2009.

[22] D. A. Cox, J. B. Little, and D. O'Shea. *Using Algebraic Geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer-Verlag, NY, 1998.

[23] C. D'Andrea and M. Sombra. A poisson formula for the sparse resultant. *Proceedings of the London Mathematical Society*, 110(4):932, 2015.

[24] S. Dasgupta, C. H. Papadimitriou, and U. Vazirani. *Algorithms*. McGraw-Hill, Inc., New York, NY, USA, 1 edition, 2008.

[25] M. Demazure. Resultant, discriminant. *Enseign. Math.*, 58(2):333–373, 2012.

[26] A. Dickenstein. A world of binomials. *London Mathematical Society Lecture Note Series*, 363:42–66, 2009.

[27] A. Dickenstein. Mixed discriminants and toric jacobians. Manuscript, 2013.

[28] A. Dickenstein and I. Z. Emiris, editors. *Solving Polynomial Equations: Foundations, Algorithms, and Applications (Algorithms and Computation in Mathematics)*. Springer, June 2005.

[29] A. Dickenstein, I. Z. Emiris, and A. Karasoulou. *Plane mixed discriminants and toric Jacobians*, volume 10 of *Series in Geometry and Computing*. Springer, 2014.

[30] A. Dickenstein, E. M. Feichtner, and B. Sturmfels. Tropical discriminants. *J. Amer. Math. Soc.*, 20:1111–1133, 2007.

[31] A. Dickenstein, J. M. Rojas, K. Rusek, and J. Shih. Extremal real algebraic geometry and a-discriminants. *Moscow Mathematical J.*, 7(3):425–452, 2007.

[32] A. Dickenstein and L. F. Tabera. Singular tropical hypersurfaces. *Discrete & Computational Geometry*, 47(2):430–453, 2012.

[33] J. A. Dieudonne and J. B. Carrell. Invariant theory, old and new. *Academic Press*, 1971.

[34] I. Dinur, G. Kindler, R. Raz, and S. Safra. Approximating CVP to within almost-polynomial factors is NP-hard. *Combinatorica*, 23(2):205–243, 2003.

[35] E. Eisenschmidt, R. Hemmecke, and M. Köppe. Computation of atomic fibers of z-linear maps. *Contributions to Discrete Mathematics*, 6(2), 2011.

[36] I. Emiris, A. Karasoulou, E. Tzanaki, and Z. Zafeirakopoulos. On the space of minkowski summands of a convex polytope. *European Workshop on Computational Geometry*, 2016.

[37] I. Z. Emiris, V. Fisikopoulos, C. Konaxis, and L. Penaranda. An output-sensitive algorithm for computing projections of resultant polytopes. In *Proc. ACM Symp. on Computational Geometry*, pages 179–188, 2012.

[38] I. Z. Emiris, T. Kalinka, C. Konaxis, and T. Luu Ba. Sparse implicitization by interpolation: Characterizing non-exactness and an application to computing discriminants. *J. Computer Aided Design*, 45:252–261, 2013.

[39] I. Z. Emiris and A. Karasoulou. *Sparse Discriminants and Applications*, volume 84 of *Proc. Math. and Stat.* Springer, 2014.

[40] I. Z. Emiris, A. Karasoulou, and C. Tzovas. Approximate subset sum and minkowski decomposition of polytopes. *European Workshop on Computational Geometry*, 2016.

[41] I. Z. Emiris, A. Karasoulou, and C. Tzovas. Approximate subset sum and minkowski decomposition of polytopes. *Mathematics in Computer Science*, 11(1), 2017.

[42] I. Z. Emiris, C. Konaxis, and Z. Zafeirakopoulos. Minkowski decomposition and geometric predicates in sparse implicitization. In *Proc ACM ISSAC*, pages 157–164, NY, USA, 2015.

[43] I. Z. Emiris and E. Tsigaridas. Minkowski decomposition of convex lattice polygons. In Mohamed Elkadi, Bernard Mourrain, and Ragni Piene, editors, *Algebraic Geometry and Geometric Modeling*, Mathematics and Visualization, pages 217–236. Springer Berlin Heidelberg, 2006.

[44] I. Z. Emiris, E. Tsigaridas, and G. Tzoumas. The predicates for the exact voronoi diagram of ellipses under the euclidean metric. *Int. J. Comput. Geometry Appl.*, 18(6):567–597, 2008.

[45] I. Z. Emiris, E. Tsigaridas, and G. Tzoumas. Exact delaunay graph of smooth convex pseudo-circles: General predicates, and implementation for ellipses. *SIAM/ACM Joint Conference on Geometric & Physical Modeling*, pages 211–222, 2009.

[46] A. Esterov. Newton polyhedra of discriminants of projections. *Discrete & Computational Geometry*, 44(1):96–148, 2010.

[47] W. Stein et al. Sage Mathematics Software. *The Sage Development Team*.

[48] J. C. Faugére, G. Moroz, F. Rouillier, and M. Safey El Din. Classification of the perspective-three-point problem: Discriminant variety and real solving polynomial systems of inequalities. In *Proc. ACM ISSAC*, pages 79–86, 2008.

[49] J. C. Faugére and P. J. Spaenlehauer. Algebraic cryptanalysis of the pkc 2009 algebraic surface cryptosystem. *Public Key Cryptography*, pages 35–52, 2010.

[50] J. C. Faugére and J. Svartz. Solving polynomial systems globally invariant under an action of symmetric group and application to the equillibria of n vortices in the plane. In *Proc ACM ISSAC*, pages 170–178, 2012.

[51] S. Gao. Absolute irreducibility of polynomials via newton polytopes. *Journal of Algebra*, 237(2):501 – 520, 2001.

[52] S. Gao and A. G B Lauder. Decomposition of polytopes and polynomials. *Discrete and Computanional Geometry*, 26(1):89–104, 7 2001.

[53] I. M. Gel'fand, M. M. Kapranov, and A. V. Zelevinsky. Hyper-geo-metric functions and toric varieties. *Funktsional. Anal. i Prilozhen*, 23(2), 1989.

[54] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants & multidimensional determinants*. Birkhauser, 1994.

[55] A. N. Godwin. The precise determination of maxwell sets for cuspoid catastrophes. *International Journal Mathematical Education Science and Technology*, 15(2):167–182, 2006.

[56] L. González-Vega and I. Nacula. Efficient topology determination of implicitly defined algebraic plane curves. *Computer Aided Geometric Design*, 19(9), 2002.

[57] J. A. Green. The characters of the finite general linear groups. *Transactions of the American Mathematical Society*, 80(2):402–447, 1955.

[58] M. B. Green, J. H. Schwarz, and E. Witten. Superstring theory: volume 2, loop amplitudes, anomalies and phenomenology. *Cambridge university press*, 2012.

[59] J. Guárdia, J. Montes, and E. Nart. Higher newton polygons in the computation of discriminants and prime ideal decomposition in number fields. *Journal de Théorie des Nombres de Bordeaux*, 23:667–696, 2011.

[60] S. Helgason. Differential geometry and symmetric spaces. *American Mathematical Soc.*, 341, 2001.

[61] M. Henk, M. Köppe, and R. Weismantel. Integral decomposition of polyhedra and some applications in mixed integer programming. *Mathematical Programming*, 94(2):193–206, 2003.

[62] M. Henk, M. Köppe, and R. Weismantel. Integral decompositions of polyhedra and some applications in mixed integer programming. *Math. Program., Ser. B*, 94:93–206, 2003.

[63] O. H. Ibarra and C. E. Kim. Fast approximation algorithms for the knapsack and sum of subset problems. *J. ACM*, 22(4):463–468, October 1975.

[64] J.-P. Jouanolou. Le formalism du resultant. *Adv. Math.*, 90(2):117–263, 1991.

[65] E. Kaltofen, J. P. May, Z. Yang, and L. Zhi. Approximate factorization of multivariate polynomials using singular value decomposition. *Journal of Symbolic Computation*, 43(5):359 – 376, 2008.

[66] D. Kesh and S. Mehta. Polynomial irreducibility testing through Minkowski summand computation. In *Proc. Canad. Conf. Comp. Geom.*, pages 43–46, 2008.

[67] K. Koiliaris and C. Xu. A faster pseudopolynomial time algorithm for subset sum. In *Proc. ACM-SIAM Symposium on Discrete Algorithms*, SODA '17, pages 1062–1072, Philadelphia, USA, 2017. SIAM. Also available as: arxiv.org/abs/1507.02318.

[68] I. G kon. *Symmetric Functions and Hall Polynomials*. Oxford University Press, 1995.

[69] V. S. Korolyuk and Y. V. Borovskich. *Theory of U-Statistics*. Mathematics and Its Applications. Springer Netherlands, 2013.

[70] A. Kulik and H. Shachnai. There is no EPTAS for two-dimensional knapsack. *Inf. Process. Lett.*, 110(16):707–710, July 2010.

[71] S. Lang. *Algebra*, volume 211. Springer-Verlag, 2002.

[72] M. J. Magazine and M.-S. Chern. A note on approximation schemes for multidimensional knapsack problems. *Math. Oper. Res.*, 9(2):244–247, May 1984.

[73] D. Manocha and J. Demmel. Algorithms for intersecting parametric and algebraic curves II: Multiple intersections. *Graphical Models and Image Proc.*, 57(2):81–100, 1995.

[74] P. McMullen. Representations of polytopes and polyhedral sets. *Geometriae Dedicata*, 2:83–99, 1973.

[75] W. Meyer. Indecomposable polytopes. *Trans. Amer. Math. Soc.*, 190:77–86, 1974.

[76] T. Miwa, M. Jimbo, and E. Date. Solitons: Differential equations, symmetries and infinite dimensional algebras. *Cambridge University Press*, 135, 2000.

[77] G. Moroz, F. Rouiller, D. Chablat, and P. Wenger. On the determination of cusp points of 3-rpr parallel manipulators. *Mechanism and Machine Theory*, 45(11):1555–1567, 2010.

[78] J. Nie. Discriminants and non-negative polynomials. *J. Symbolic Comput.*, 47:167–191, 2012.

[79] A.M. Ostrowski. On multiplication and factorization of polynomials, II. irreducibility discussion. *Aequationes Mathematicae*, 14:1–31, 1976.

[80] P. Pedersen and B. Sturmfels. Product formulas for resultants and chow forms. *Math. Z.*, 214:377–396, 1993.

[81] N. Perminov and S. Shakirov. Discriminants of symmetric polynomials. *Preprint*, 2009.

[82] E. F. Rincón. Computing tropical linear spaces. *J. Symbolic Comput.*, 51:86–93, 2013.

[83] S. Sahi and H. Salmasian. The capelli problem for gl(m|n) and the spectrum of invariant differential operators. *Advances in Mathematics*, 303:1–38, 2016.

[84] T. Saito. The discriminant and the determinant of a hypersurface of even dimension. *Math. Res. Lett.*, 19(4):855–871, 2012.

[85] F. A. Salem, S. Gao, and A. G. B. Lauder. Factoring polynomials via polytopes. In *Proc ACM ISSAC*, pages 4–11, 2004.

[86] A. Sergeev and A. Veselov. Calogero–moser operator and super jacobi polynomials. *Advances in Mathematics*, 222(5):1687–1726, 2009.

[87] M. Shub and S. Smale. Complexity of bézout's theorem i. geometric aspects. *J. Amer. Math. Soc.*, 6(2):459–501, 1993.

[88] R. Stanley. Some combinatorial properties of jack symmetric functions. *Adv. Math*, 77:76–115, 1989.

[89] B. Sturmfels. The newton polytope of the resultant. *J. Algebraic Combin.*, 3:207–236, 1994.

[90] J. J. Sylvester. Sur l'extension de la théorie des résultants algébriques. *Comptes Rendus de l'Académie des Sciences*, LVIII:1074–1079, 1864.

[91] H. Tuy. *Convex Analysis and Global Optimization*, volume 110 of *Springer Optimization and its Applications*. Springer, 2016.

[92] J. van der Hoeven, G. Lecerf, and B. Mourain. *Mathemagix*, 2002.

[93] B. L. van der Waerden. F. Ungar Publishing Co., 1950.

[94] J. H. Wilkinson. Dover, 1994.

[95] G.J. Woeginger. When does a dynamic programming formulation guarantee the existence of an FPTAS? In *Proc. ACM-SIAM Symposium on Discrete Algorithms*, SODA '99, pages 820–829, Philadelphia, USA, 1999. SIAM.

[96] G.J. Woeginger. When does a dynamic programming formulation guarantee the existence of a fully polynomial time approximation scheme (FPTAS)? *INFORMS J. Computing*, 12(1):57–74, 2000.

[97] P. A. Worfolk. Zeros of equivariant vector elds: algorithms for an invariant approach. *J. Symbolic Comput.*, 17(6):487–511, 1994.