On the space of Minkowski summands of a convex polytope

Ioannis Z. Emiris *

Anna Karasoulou *

Eleni Tzanaki[†]

Zafeirakis Zafeirakopoulos[‡]

Abstract

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.

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

$$P_b = \{ x \in \mathbb{R}^d : Ax \le b \}$$

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

$$U(A) = \{ b \in \mathbb{R}^m : P_b \neq \emptyset \}.$$
(1)

Problem 1 Minkowski Summands. Given $A \in \mathbb{Z}^{m \times d}$ and $b \in \mathbb{R}^m$, such that $Ax \leq b$ is the *H*-representation of a convex integral polytope P_b , compute all integral MinkDecomp of P_b .

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 [9] performing the computation of all Minkowski summands in any dimension d, extending ideas from [5]. We 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 [5], polynomial factorization [4] or implicitization [3]. 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 [2, 3, 4]. The problem of computing a Minkowski summand in general dimension is reduced to the feasibility of a linear program [6], thus deciding if a polytope is decomposable in order to test polynomial irreducibility. In [1, 5] is explored the cone of combinatorially equivalent polytopes and its computational aspects. Some classical work on polytope decomposition is presented in [7].

2 Computing the Space of Minkowski Summands

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

Lemma 1 (Farkas 1894) The system of inequalities $Ax \leq b$ is feasible if and only if $y^{\top}b \geq 0$ for each $y \geq 0$ with $A^{\top}y = 0$.

The dual, $U^*(A) = \{ y \in \mathbb{R}^m : y^\top b \ge 0 \ \forall b \in U(A) \},$ in view of Lemma 1 becomes

$$U^*(A) = \{ y \in \mathbb{R}^m : A^\top y = 0 \text{ and } y \ge 0 \}.$$
 (2)

It is immediate from Equation (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 $b \in \mathbb{Z}^{10}$

| Г | 0 | 1 | 1 7 | | F 4 7 | |
|---|---------|---------|-----|--|-------|-----|
| | 1 | 0 | 1 | | 4 | |
| | 1 | 0 | 0 | $\left[\begin{array}{c} x\\ y\\ z\end{array}\right] \le$ | 3 | (3) |
| | 0 | 1 | 0 | | 3 | |
| | 0 | 0 | -1 | | 0 | |
| | 0 | 0 | 1 | | 2 | |
| | 0 | $^{-1}$ | 0 | | 0 | |
| | 0 | $^{-1}$ | 1 | | 1 | |
| | $^{-1}$ | 0 | 0 | | 0 | |
| L | -1 | 0 | 1 | | | |

^{*}Department of Informatics & Telecommunications, University of Athens, Athens, Greece. First two authors are partially supported from project "CGL", which acknowledges the financial support of the Future and Emerging Technologies program within the 7th Framework Program for research of the European Commission, under FET-Open grant number: 255827. The authors would like to thank the anonymous reviewers for valuable comments. emiris,akarasou@di.uoa.gr

 $^{^\}dagger Department$ of Applied Mathematics University of Crete, Crete, Greece, <code>etzanaki@tem.uoc.gr</code>

[‡]Institute of Information Technologies, Gebze Technical University, Kocaeli, Turkey, zafeirakopoulos@gtu.edu.tr

defining the polytope in Figure 1.



Figure 1: The polytope defined by System (3) and its 2 Minkowski summands.

The inequalities defining the cone U(A) are: $b_5 + b_6 \ge 0$ $b_4 + b_5 + b_8 \ge 0$ $b_2 + 2b_5 + b_{10} \ge 0$ $b_4 + b_7 \ge 0$ $b_4 + b_5 + b_{10} \ge 0$ $b_2 + b_5 + b_9 \ge 0$ $b_4 + b_5 + b_8 \ge 0$ $b_1 + b_5 + b_7 \ge 0$ $b_1 + 2b_5 + b_8 \ge 0$

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

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

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

$$\dim\{y \in P : v^{\top}y = h(P, v)\} = \\ = \dim\{y \in Q : v^{\top}y = h(Q, v)\}.$$

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 1 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 2** 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

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

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

$$U(A)_b := \{\eta_v : v \in U(A) \text{ such that } P_v \prec P_b\}.$$
(4)

In [5, 7, 8], 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 2 [7],[8] 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 $a^{\top}v \geq 0$ where $a, v \in \mathbb{R}^m$. These inequalities should be imposed from the feasibility of $Ax \leq v$ 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 $\{x \in \mathbb{R}^d : A_F x \leq b_F\}$ 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 $\{x \in \mathbb{R}^d : A_F x \leq y\}$ 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 $Ax \leq b$.

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 $A_F x \leq b$ for the facet F is

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \\ 0 & -1 & 1 \\ -1 & 0 & 0 \\ -1 & 0 & 1 \\ -1 & 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \leq \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \\ b_8 \\ b_9 \\ -b_1 \end{bmatrix}$$
(5)

For the polyhedron defined by System (5), we obtain the following H-representation of $U(A_F)$:

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: $b_2 + b_8 \ge 0$ and $b_1 + b_4 + b_8 \ge 0$.

The idea in Algorithm 1 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 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 3.

We say that $Ax \leq b$, $A \in \mathbb{Z}^{m \times d}$ is an *irredundant* description of $P_b = \{x : Ax \leq b\}$, 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 $Ax \leq b$ 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 3 Assume $P_b = \{x : Ax \leq b\}, A \in \mathbb{R}^{m \times d}$ is a *d*-polytope with *m* facets. Then, the generating rays b_1, \ldots, b_k of $U(A)_b$ correspond to nontrivial

 $\pm c_1, \ldots, \pm c_d$ of $U(A)_b$ correspond to points.

Combining Proposition 3 and Theorem 2, we deduce that each MinkDecomp of P_b into non-trivial indecomposable polytopes is a sum:

$$P_b = \lambda_1 P_{b_1} + \dots + \lambda_k P_{b_k} + T \tag{6}$$

where $\lambda_1, \ldots, \lambda_k \ge 0$ 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 4 For each polytope $P_c = \{x \in \mathbb{R}^d : Ax \leq c\}, A \in \mathbb{R}^{m \times d}, 0 \neq c \in \mathbb{R}^d$, such that $Ax \leq c$ is feasible,

- 1. if $Ax \leq -c$ is feasible then P_c is a point
- 2. if $Ax \leq -c$ is not feasible then P_c is a non-trivial polytope or P_c is a point whose description $Ax \leq c$ contains a non-active inequality $(c \neq \eta_c)$.

Proof. Since $Ax \leq c$ is a polytope, feasibility of $Ax \leq -c$ 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 $Ax \leq \pm c$ fails only if the description $Ax \leq c$ contains a hyperplane that does not support P_c . \Box

Proof. [Proof of Proposition 3] If a polytope P_{b_i} corresponds to an extreme ray of $U(A)_b$, then $Ax \leq b_i$ is feasible whereas $Ax \leq -b_i$ is not. Since, by definition, the cone $U(A)_b$ contains polytopes all whose inequalities are active, Lemma 4.2 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 $Ax \leq c_i$ and $Ax \leq -c_i$ are feasible. In this case, Lemma 4.1 implies that P_{c_i} is a point.

If we only want to decide whether P_b is indecomposable, Proposition 3 is simplified as follows.

Corollary 5 Let $P_b = \{x : Ax \leq b\}, A \in \mathbb{Z}^{m \times d}$ 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 corresponding 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 | $Ax \leq b_i$ | vertex set: |
|---|---------------|-------------------------|
| $\pm(1, 1, 0, 0, -1, 1, 0, 1, 0, 1)$ |) 0-dim | $\{(0, 0, \pm 1)\}$ |
| $\pm(1,1,0,0,-1,1,0,1,0,1)$ |) 0-dim | $\{(\pm 1, 0, 0)\}$ |
| $\pm(1,0,0,1,0,0,-1,-1,0,0)$ |) 0-dim | $\{(0,\pm 1,0)\}$ |
| (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, 0, 1, 1) |) 1-dim | $\{(0,0,0),(-1,0,0)\}$ |
| (1, 1, 0, 0, 0, 1, 0, |) 1-dim | $\{(0,0,0),(0,0,1)\}$ |
| (0, 0, 0, 0, 0, 1, 2, 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 (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 (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 $v_j = \left(\frac{a_{j1}}{b_{j1}}, \ldots, \frac{a_{jd}}{b_{jd}}\right) \in \mathbb{Q}^d$, $1 \leq j \leq s$, of P_{b_i} , where each $\frac{a_{jk}}{b_{jk}}$ is in reduced form. Then, define:

$$gcd(v_1, \dots, v_s) := gcd\{a_{jk} : 1 \le j \le s, 1 \le k \le d\},\$$
$$lcm(v_1, \dots, v_s) := lcm\{b_{jk} : 1 \le j \le s, 1 \le k \le d\}.$$

It is not hard to see that $P'_{b_i} := \{x : Ax \leq \lambda' b_i\}$ where $\lambda' = \lambda'(P_{b_i}) := \frac{\operatorname{lcm}(v_1, \dots, v_s)}{\operatorname{gcd}(v_1, \dots, v_s)}$ 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 (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 6 Let $P_b = \{x : Ax \leq b\}, A \in \mathbb{Z}^{m \times d}$ be a *d*-polytope with *m* facets. For each $1 \leq i \leq d$ set $\tilde{c}_i := Ae_i$ where e_1, \ldots, e_d is the standard basis of \mathbb{R}^d . The polytope $\{x : Ax \leq \tilde{c}_i\}$ is the unique point e_i .

Proof. Since the rows of A positively span \mathbb{R}^d , the system $Ax \leq 0$ has a unique solution. Thus, the same holds for $Ax \leq Ae_i$, 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:

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 (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.

Algorithm 1 MINKOWSKISUMMANDS(A, b)

1: $H_i^- \leftarrow \{x \in \mathbb{R} : a_i x \le b_i\}$ 2: $H_i \leftarrow \{x \in \mathbb{R} : a_i x = b_i\}$ 3: $R \leftarrow \text{rays of } \ker (A^{\top}) \cap \mathbb{R}^m_+$ 4: $U(A) \leftarrow \{x \in \mathbb{R}^{m} : r^{\top}x \ge 0 \text{ for } r \in R\}$ 5: $U(A)_b \leftarrow U(A)$ 6: for $k \leftarrow 0 \dots \dim(P) - 1$ do for F face with $\dim(F) = k$ do 7: $I \leftarrow \{i_1, \dots, i_\ell\} \subseteq [m] \text{ such that } F \subseteq H_{i_s}$ $A_F \leftarrow \begin{bmatrix} a_i \\ -a_i \\ a_j \end{bmatrix} \text{ for } i \in I \text{ and } j \in [m] \setminus I$ 8: 9 $R \leftarrow \text{rays of } \ker \left(A_F^{\top} \right) \cap \mathbb{R}_+^{m+\ell} \\ U\left(A_F \right) \leftarrow \left\{ \tilde{b} \in \mathbb{R}^{m+\ell} : r^{\top} \tilde{b} \ge 0 \text{ for } r \in R \right\}$ 10: 11: Substitute using $\{\tilde{b}_1, \tilde{b}_2, \ldots, \tilde{b}_{d+\ell}\} =$ 12: $\{b_{i_1}, -b_{i_1}, \ldots, b_{i_{\ell}}, -b_{i_{\ell}}, b_{i_{\ell+1}}, \ldots, b_{i_d}\}$ Compute *H*-rep of $U(A_F)$ wrt (b_1, \ldots, b_m) 13: $U(A)_b \longleftarrow U(A)_b \cap U(A_F)$ 14: 15: $R \leftarrow \text{rays of } U(A)_b$ 16: Summands= \emptyset 17: for r_i in R do Ensure the origin is a vertex of P_{r_i} Compute the vertices $\left(\frac{a_{j1}}{b_{j1}}, \ldots, \frac{a_{jd}}{b_{jd}}\right)$ of P_{r_i} 18:19: $\begin{array}{l} \lambda' \leftarrow \frac{\operatorname{lcm}(v_1, \ldots, v_s)}{\operatorname{gcd}(v_1, \ldots, v_s)} \\ \operatorname{Summands} \leftarrow \lambda' r_i \end{array}$ 20: 21:22: return Summands

References

- E. Eisenschmidt, R. Hemmecke, and M. Köppe. Computation of atomic fibers of z-linear maps. *Contributions to Discrete Mathematics*, 6(2), 2011.
- [2] I.Z. Emiris and E. Tsigaridas. Minkowski decomposition of convex lattice polygons. In M. Elkadi, B. Mourrain, and R. Piene, eds, *Algebraic Geometry and Geometric Modeling*, pages 217–236. Springer, 2006.
- [3] I.Z. Emiris, C. Konaxis, and Z. Zafeirakopoulos. Minkowski decomposition and geometric predicates in sparse implicitization. In *Proc. ACM Intern. Symp. Symb. Alg. Comp.*, pages 157–164, 2015.
- [4] S. Gao and A. Lauder. Decomposition of polytopes and polynomials. Discr. & Comp. Geometry, 26:89– 104, 2001.
- [5] 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.
- [6] D. Kesh and S. Mehta. Polynomial irreducibility testing through Minkowski summand computation. In *Proc. Canad. Conf. Comp. Geom.*, pages 43–46, 2008.
- [7] P. McMullen. Representations of polytopes and polyhedral sets. *Geometriae Dedicata*, 2:83–99, 1973.
- [8] W. Meyer. Indecomposable polytopes. Trans. Amer. Math. Soc., 190:77–86, 1974.
- [9] W. Stein et al. Sage Mathematics Software. The Sage Development Team.