Polynomial irreducibility testing through Minkowski summand computation

Deepanjan Kesh and Shashank K Mehta*

Abstract

In this paper, we address the problem of deciding absolute irreducibility of multivariate polynomials. Our work has been motivated by a recent work due to Gao et. al. [1, 2, 3] where they have considered the problem for bivariate polynomials by studying the integral decomposability of polygons in the sense of Minkowski sum. We have generalized their result to polynomials containing arbitrary number of variables by reducing the problem of Minkowski decomposability of an integer (lattice) polytope to an integer linear program. We also present experimental results of computation of Minkowski decomposition using this integer program.

1 Introduction

Let $f = \sum_\alpha c_\alpha X^\alpha$ be a polynomial where $\alpha \in \mathbb{N}^n$ and the coefficients c_α are from a field, say K. The lattice polytope $New(f) = conv(\{\alpha | c_\alpha \neq 0\})$ is called the Newton polytope of f. A lattice polytope $\mathcal{P}$ is *integrally decomposable* if there exist non-trivial lattice polytopes $\mathcal{Q}$ and $\mathcal{R}$ such that $\mathcal{P}$ is their Minkowski sum, denoted as $\mathcal{Q} + \mathcal{R}$. Ostrowski [4] observed that if f, g, h are polynomials such that $f = g \cdot h$, then $New(f) = New(g) + New(h)$. This gives a simple irreducibility criterion for polynomials [2].

Lemma 1 *Let $f \in K[x_1, \ldots, x_n]$ and it is not divisible by any x_i for any i. If the Newton polytope of f is integrally indecomposable, then f is absolutely irreducible.*

Thus the integral indecomposability of the Newton polytope is a sufficient condition for testing the absolute irreducibility of a polynomial. Efficient decomposition algorithms are given by Silverman and Stein [9] and Emiris and Tsigaridas [8] for polygons and by Mount and Silverman [7] for 3-dimensional polytopes. Gao and Lauder [1] showed that the problem is NP-complete even in two-dimensions. They gave a pseudo-polynomial time algorithm to solve the integral decomposition of polygons, and a randomized heuristic algorithm for polytopes of higher dimensions [1, 3]. We present an exact criterion for integral decomposition of arbitrary dimensional lattice polytopes. We show that an integral decomposition of a polytope exists if and only if its edge-graph has a graph-minor satisfying certain conditions. The criterion is general and applies to non-lattice polytopes as well. In the rest of the discussion, polytopes or convex polytopes would refer to lattice convex polytopes unless stated otherwise.

*Department of Computer Science and Engineering, IIT Kanpur, Kanpur - 208016, {deepkesh, skmehta}@cse.iitk.ac.in

2 Oriented Walks and Oriented Weights

An *oriented walk* in an undirected graph $G = (V, E)$ is a non-empty sequence of vertices $w = v_0, \ldots, v_k$, not necessarily distinct, such that $e_i = v_i v_{i+1}$ is an edge of G for all $0 \leq i < k$. The orientation of e_i in w is in the direction $\overrightarrow{v_i v_{i+1}}$. We denote the walk in the reverse orientation, $v_k, v_{k-1}, \ldots, v_0$, by w^r. If $v_0 = v_k$, then the oriented walk is said to be *closed*. An oriented closed walk $v_0, \ldots, v_{k-1}, v_0$ with $k \geq 3$ is said to be a *simple* if $v_i \neq v_j$ for all $0 \leq i < j \leq k-1$. Simple closed walks are also called *cycles*. All closed walks of the form $v_0, v_1 \ldots, v_{k-1}, v_k, v_{k-1}, \ldots, v_1, v_0$ are called *zero-walks*.

We define the *oriented sum* of two oriented closed walks (or two sets of oriented closed walks) to be that collection of oriented closed walks which results after canceling each pair of occurrences of an edge which are in opposite orientations. The traditional concept of *cycle space* in algebraic graph theory is defined over the finite field $\mathbb{F}_2$ [5]. In this sense, the sum cancels each pair of occurrences of an edge without consideration of their orientations. For example, let *abcda* and *abdca* be two closed walks in a graph. Then the oriented sum of the two is $\{abca, abda\}$ while the algebraic sum is *acbda*. Observe that the oriented sum is a commutative and associative operation.

The *oriented weight* W for a graph G, is a mapping from the oriented edges of G to K^n for some fixed n such that $W(xy) = -W(yx)$ for each edge xy. We extend this mapping to oriented walks as follows. Let $w = v_0 v_1 \ldots v_k$ be an oriented walk, then $W(w) = \sum_{i=0}^{k-1} W(v_i v_{i+1})$. Thus $W(w^r) = -W(w)$ and the oriented weight of every zero-walk is zero. An oriented weight W for a graph is said to be *non-singular* if $W(w) = 0$ for each oriented closed walk w in the graph.

Observation 1 *If w_1 and w_2 are oriented closed walks (or sets of walks) in a graph on which an oriented weight W is defined, then $W(w_1 + w_2) = W(w_1) + W(w_2)$.*

Proposition 2 *Let G be any graph with oriented weight W. Let w be any non-zero oriented closed walk in G, not necessarily simple, then there exists oriented cycles*

$w_1, \ldots, w_k$, *possibly with multiplicity, such that* $W(w) = W(w_1) + \cdots + W(w_k)$.

Proof. Assume the contrary. So there is at least one closed (non-zero) walk for which the claim is not true. The length of a walk is the number of edges in it, with multipmicity. Let $w = v_0, v_1, \ldots, v_{k-1}, v_0$ be a shortest non-zero closed walk in the graph for which the oriented weight cannot be expressed as the sum of those of some simple closed walks. Thus w is itself not a simple closed walk. Let i be the smallest index such that there exists an index $j(> i)$ with $v_i = v_j$. Let $l \geq 0$ be the maximum integer such that $v_{i+r} = v_{j-r}$ for all $0 \leq r \leq l$ and $i+l \leq j-l$. Then w can be split into three closed walks: $w_1 = v_j, v_{j+1}, \ldots, v_{k-1}, v_0, \ldots, v_i$; $w_2 = v_{i+l}, v_{i+l+1}, \ldots, v_{j-l}$; and $w_3 = v_i, \ldots, v_{i+l-1}, v_{i+l}, v_{j-l+1}, \ldots, v_j$. Since the edges of w are partitioned into those of w_1, w_2, and w_3, and the direction of the edges are preserved, the weight of w is equal to the sum of the weights of the three closed walks. Note that w_3 is a zero walk so its weight is zero and $W(w) = W(w_1) + W(w_2)$.

The lengths of w_1, w_2, w_3 are respectively $k-j+i, j-i-2l, 2l$, so w_1 and w_2 are both strictly smaller than w and at least one is a non-empty non-zero closed walk. Hence, by the choice of w, atleast one of the weights of w_1 and w_2 can be expressed as the sum of the weights of simple closed walks, while the other is either a zero-walk or can itself be expressed as the sum of the weights of closed walks. Thus the weight of w can also be expressed as the sum of weights of simple closed walks. This contradicts the assumption. Further, the argument is independent of the actual weights. □

A trivial consequence of this result is that the oriented weight of any oriented walk can be expressed as the linear sum of the oriented weight of some oriented cycles with integer coefficients.

A subset of oriented cycles, $\mathcal{B}$, is called an *oriented basis* if the weight of every closed non-zero walk can be expressed as the sum of the oriented weights of some of the oriented cycles in $\mathcal{B}$, with integer coefficients.

Through out this paper we will only deal with oriented walks, oriented sum, oriented weight, and oriented basis. Therefore for simplicity we may often drop the adjective *oriented*.

3 Oriented Bases

In this section we describe two oriented bases. The first is applicable only to the edge-graphs of polytopes and the second is for general graphs.

Theorem 3 *Let G be the edge graph of a polytope. Then 2-face cycles of the polytope, each oriented in any one direction, form a basis of G.*

Proof. From Proposition 2, it is sufficient to show that the oriented weight of every simple closed walk can be expressed as the sum of the oriented weights 2-face cycles. We will prove this by induction on the dimension of the polytope. The statement trivially holds for polygons. Assume that $\mathcal{P}$ is an n-dimensional polytope ($n > 2$) for which the claim is not true while it is true for all the smaller dimensional polytopes. Let ω be a direction such that all the vertices in $\mathcal{P}$ have unique projection along ω, i.e., for any pair of distinct vertices v_1 and v_2, $v_1.\omega \neq v_2.\omega$. Let w be a simple closed walk in $\mathcal{P}$ such that $W(w)$ is not expressible as the sum of the oriented weights of some 2-face cycles. Let v be the vertex on w having the highest projection along ω, i.e., $\omega.v > \omega.u$ for all u on w other than v. Without loss of generality assume that w is such a walk that $v.\omega$ is minimum.

Let the neighbors of v in w be x and y such that $w = xvy \ldots x$ where the subwalk $y \ldots x$ may be denoted by w'. Vertex v does not occur in w' since w is a simple closed walk. Pass a hyperplane through v cutting/touching $\mathcal{P}$, with normal ω. Consider the polytope $\mathcal{P}'$ lying on $-\omega$ side of the hyperplane. Let F be a face of $\mathcal{P}'$ due to the new plane, i.e., $F = face_\omega(\mathcal{P}')$. Thus w is contained in $\mathcal{P}'$ and no vertex of w, other than v, belongs to F.

If the plane cuts $\mathcal{P}$, then F will be a facet ($n-1$ dimensional face) but if it only touches it then F will be a vertex ($F = v$) because of distinct projections of the vertices on ω.

First, consider the case when F is a facet. Let F' and F'' be arbitrary facets of $\mathcal{P}'$, other than F, which contain edges vx and vy. Consider the dual polytope ${\mathcal{P}'}^D$, of $\mathcal{P}'$. The facet corresponding to v contains the vertices corresponding to F, F', F'' and is a $(n-1)$-dimensional polytope. Hence, it is $(n-1)$-connected from the connectivity result due to Balinski [10]. So removing the vertex corresponding to F still keeps the facet corresponding to v connected because $n > 2$. Then, there exists a path in the edge graph of ${\mathcal{P}'}^D$ from the vertex corresponding to F' to the vertex corresponding to F'', not containing F. Let the corresponding facets in $\mathcal{P}$ be $F', F_1, \ldots, F_{k-1}, F''$.

In the case when F is a vertex let F' and F'' be arbitrary facets of $\mathcal{P}$ containing the edges vx and vy respectively. Consider the dual polytope ${\mathcal{P}'}^D$. There will be vertices F' and F'' in the facet of F. Consider any path $F', F_1, \ldots, F_{k-1}, F''$ in the facet of F.

From here we consider both the cases simultaneously. If the sequence of the facets is written as $(F' = F_0)F_1 \ldots F_{k-1}(F_k = F'')$, then for all i, $F_i \neq F$ and $F_i \cap F_{i+1}$ is a $(n-2)$-dimensional face of $\mathcal{P}$. Moreover, v belongs to each of these $(n-2)$-dimensional faces.

Consider the faces F_0, F_1 and $F_0 \cap F_1 = F_{01}$. In ${\mathcal{P}'}^D$, F_0, F_1 are vertices and F_{01} is an edge between

them. As an edge is shared by two vertices only, no other facet of $\mathcal{P}$ contains F_{01}. Specifically, F_{01} is not contained in F. As $v \in F_0, F_1$, so $v \in F_{01}$. Moreover, there exists a neighbor, z_0 of v in F_{01}, such that $z_0 \notin F$. This is because the convex polyhedral cone at v with all the neighbours of v in F_{01} contains F_{01} and is contained in the hyperplane defining F. These two together would imply that $F_{01} \subset F$ which is a contradiction. One thing to note here is that ω projection of z_0 is less than that of v. We know that $face_\omega(\mathcal{P}') = F$ and $F_i \neq F$ so $face_{-\omega}(F_i) \cap F = \emptyset$. From Corollary 10, there exist paths from x and from z_0 to a common vertex in $face_{-\omega}(F_0)$. Both the paths are monotonic along $-\omega$, so none of the vertices of these paths belongs to F. Combine these paths to form a walk from z_0 to x, call it w'_0, which is contained in F_0 and none of its vertices are in F. Let the closed walk $[w'_0].[x, v, z_0]$ be denoted by w_0. Similarly for each i define closed walks $w_i = [w'_i].[z_{i-1}.v.z_i]$ which is in F_i and none of its vertices, other than v, is in F. Here z_k stands for y.

Consider the closed walks $w'' = [w'_0]^r.[w'_1]^r \dots [w'_k]^r.[w']$ which contains no vertex of F, and $w''' = [x, v, z_0, v, z_1, v, z_2, \dots, v, z_{k-1}, v, y].[w']$. Accounting for zero subwalks in w''' we have $W(w''') = W(w)$. Hence we have

$$\begin{aligned}
W(w) &= W(w''') \\
&= W([x, v, z_0, v, z_1, v, z_2, \dots, v, z_{k-1}, v, y] \cdot [w']) \\
&\quad + \sum_{i=0}^{k} W(w'_i) + \sum_{i=0}^{k} W([w'_i]^r) \\
&= W([x, v, z_0]) + W(w'_0) \\
&\quad + \sum_{i=1}^{k-1} (W([z_{i-1}, v, z_i]) + W(w'_i)) \\
&\quad + W([z_{k-1}, v, y]) + W(w'_k) \\
&\quad + W([w']) + \sum_{i=0}^{k} W([w'_i]^r) \\
&= \sum_{i=0}^{k} W(w_i) + W(w'')
\end{aligned}$$

Since all the vertices in w' have ω projection strictly less than that of v, due to the choice of w, $W(w'')$ can be expressed as the sum of the weights of 2-face cycles. Further, each w_i is a closed cycle in a facet of the polytope ($n-1$ dimensional) so from the induction hypothesis each $W(w_i)$ can also be expressed as the sum of the oriented weights of some 2-face cycles. Putting all together, we find that $W(w)$ is also expressible as the sum of the oriented weights of some 2-face cycles. This contradicts the assumption. □

Next we show that a set of fundamental cycles of a graph also forms a basis. Let $G = (V, E)$ be a graph and $T \subseteq G$ be one of its spanning trees. Let $\overleftrightarrow{c_e}$ denote the unoriented cycle in the graph $T \cup \{e\}$ for some non-tree edge e of G. Then the set of fundamental cycles (w.r.t. T) is the collection $\{c_e | e \in E(G) \setminus E(T)\}$, where c_e is $\overleftrightarrow{c_e}$ oriented in any one direction. We assign a unique integer between 1 and $|E(G)|$ to each edge in G such that the integer assigned to any edge in $E(G) \setminus E(T)$ is greater than all the integers assigned to edges in $E(T)$. Let c be a cycle or a set of cycles of G. Then $le(c)$ denotes that edge in c which has the largest integer assignment.

Observation 2 *For every cycle c, $le(c) \in E(G) \setminus E(T)$.*

Theorem 4 *Fundamental cycles, each orieted in any one direction, form an oriented basis.*

Proof. In view of Proposition 2 it is sufficient to show that the weight of every set of cycles can be expressed as the sum of the weights of some fundamental cycles with integer coefficients. Assume that it is not true. So there is at least one set of oriented cycles whose weight cannot be expressed as the sum of weights of fundamental cycles. Let c be such a set such that label of $le(c)$ is smallest. Let $e = le(c)$. Then, by observation 2, $e \in E(G) \setminus E(T)$ where T is some fixed spanning tree. Let the fundamental cycle of e in G w.r.t. T be c_e, oriented in one of the two ways. Suppose e occurs in c for k_1 times in the same orientation as in c_e and for k_2 times in the opposite orientation. Define a new set of oriented cycles c' as $c + k_1.c_e^r + k_2.c_e$, where $k.x$ denotes the sum of k copies of x.

The new set c' of cycles has the property that the label of $le(c')$ is strictly less than the label assigned to e. From the assumption $W(c')$ can be expressed as the sum of the weights of fundamental cycles, say, $W(c') = W(c_1) + \dots + W(c_m)$ where each c_i is an oriented fundamental cycle. Then $W(c) = W(c_1) + \dots + W(c_m) + (k_1 - k_2).W(c_e)$. This contradicts the assumption that weight of c cannot be expressed as the sum of the weights of oriented fundamental cycles. □

4 Convex polytopes

In this section, we state a few basic facts about convex polytopes. The reader can find more details in [6].

A polytope is the convex-hull of a set of points in $\mathbb{R}^n$. In this paper a polytope refers only to the "shape" and the orientation of a polytope so its position in the space is ignored. Let $\mathcal{P}$ be a polytope in $\mathbb{R}^n$. Then $face_\omega(\mathcal{P})$ denotes the face of $\mathcal{P}$ with an outer normal ω, given by $\{x \in \mathcal{P} | \omega.x \geq \omega.y \ \forall y \in \mathcal{P}\}$. The set of all the outer normals of a face f of $\mathcal{P}$ is denoted by $N_\mathcal{P}(f)$ and is called the normal cone of the face f. The Minkowski sum of polytopes $\mathcal{Q}$ and $\mathcal{R}$ is the object given by $\mathcal{Q} + \mathcal{R} = \{x + y : x \in \mathcal{Q}, y \in \mathcal{R}\}$ which is also

a polytope. The locations of $\mathcal{Q}$ and $\mathcal{R}$ only affect the location of $\mathcal{Q}+\mathcal{R}$, not its shape or orientation. Polytope $\mathcal{Q}$ is said to be a Minkowski summand of a polytope $\mathcal{P}$ if there is a polytope $\mathcal{R}$ such that $\mathcal{P} = \mathcal{Q} + \mathcal{R}$. Let $\mathcal{P}$ be a polytope in $\mathbb{R}^n$. Then $G_{\mathcal{P}} = (V_{\mathcal{P}}, E_{\mathcal{P}})$ is called the edge-graph of $\mathcal{P}$ where $V_{\mathcal{P}}$ is the set of vertices (0-faces) of the polytope and $E_{\mathcal{P}}$ is the set of its edges (1-faces). We shall use the same symbol, to denote the position vector of a polytope vertex and the corresponding graph vertex.

Lemma 5 *For any direction ω, $face_\omega(\mathcal{Q} + \mathcal{R}) = face_\omega(\mathcal{Q}) + face_\omega(\mathcal{R})$.*

Lemma 6 *Let $\mathcal{P} = \mathcal{Q} + \mathcal{R}$. Let f_1 and f_2 be faces of $\mathcal{Q}$ and $\mathcal{R}$ respectively with $N_{\mathcal{Q}}(f_1) \cap N_{\mathcal{R}}(f_2) \neq \emptyset$, then $f_1 + f_2$ is a face of $\mathcal{P}$ with the normal cone being $N_{\mathcal{Q}}(f_1) \cap N_{\mathcal{R}}(f_2)$*

Lemma 7 *Let $\mathcal{P} = \mathcal{Q} + \mathcal{R}$ and $f \subset \mathcal{P}$ be a face. Then there exists unique faces $f_1 \subset \mathcal{Q}$ and $f_2 \subset \mathcal{R}$ such that $f = f_1 + f_2$.*

Lemma 8 *For every face f of a polytope in $\mathbb{R}^n$, $dim(f) + dim(N(f)) = n$, where $dim(\cdot)$ denotes the dimension.*

Lemma 9 *Let x be a vertex in a polytope $\mathcal{P}$ and ω be any direction. If x does not belong to $face_\omega(\mathcal{P})$, then there is at least one neighboring vertex y of x (i.e., xy is an edge) such that $y.\omega > x.\omega$.*

Proof. Let $y_1, \ldots, y_k$ be the neighbors of x. Let $z \in face_w(\mathcal{P})$. Then there exist non-negative λ_i such that $z - x = \sum_{i=1}^{k} \lambda_i.(y_i - x)$, because the polytope is in the positive hull of the vectors $y_i - x$. As $(z - x).\omega > 0$, there exists some j such that $y_j.\omega > x.\omega$. □

Lemma 10 *Let v be a vertex of a face $face_\omega(\mathcal{P})$ and u_0 be any other vertex of a polytope $\mathcal{P}$. Then there is a* monotonic path *in the edge graph $u_0, u_1, \ldots, u_j, \ldots, u_k(= v)$ such that $(u_{i+1} - u_i).\omega > 0$ for all $0 \leq i \leq j$ and $(u_{i+1} - u_i).\omega = 0$ for all $j \leq i < k$.*

Proof. From the previous lemma, there is a path $u_0, u_1, \ldots, u_j$ such that $(u_{i+1} - u_i).\vec{w} > 0$ for $0 \leq i \leq j$ and $u_j \in face_\omega(\mathcal{P})$. Since the edge graph of $face_\omega(\mathcal{P})$ is connected, there is a path $u_j, \ldots, u_k(= v)$ in it. Thus $(u_{i+1} - u_i).\omega = 0$ for $j \leq i \leq k - 1$. □

4.1 Geometric Weight and Derived Weight

The oriented weight $W = \{w_{uv} = v - u\}_{uv \in E_{\mathcal{P}}}$ assigned to $G_{\mathcal{P}}$ is called the *geometric weight* of $G_{\mathcal{P}}$, where $v - u$ is the displacement vector from vertex u to vertex v in the space.

Observation 3 *The geometric weight of an edge graph of a polytope is non-singular.*

Consider a graph G with non-singular weight $W = \{w_{xy}\}_{xy \in E(G)}$. Then the weight $W_\alpha = \{\alpha_{xy}.w_{xy}\}_{e \in E(G)}$, where $0 \leq \alpha_{xy} = \alpha_{yx} \leq 1$ for all $xy \in E(G)$, is referred as *derived weight* of W if it is also non-singular. Further, the weight given by $\{(1 - \alpha_{xy}).w_{xy}\}_{xy \in E(G)}$ is denoted by $W_{1-\alpha}$. Since α's are independent of the orientation of the edge, we may express $\alpha_{xy} = \alpha_{yx}$ by α_e where e denotes the corresponding edge.

Observation 4 *Let W be a non-singular weight of some graph G. Then W_α is a derived weight iff $W_{1-\alpha}$ is also a derived weight.*

4.2 Polytope of embedding

Let G be a connected graph with a non-singular weight W where the vectors in the weight belong to $\mathbb{R}^n$. Let v_0 be a fixed vertex of G. We embed each vertex of G into $\mathbb{R}^n$ by a mapping $\phi_W : V(G) \to \mathbb{R}^n$ as follows. $\phi_W(v_0) = \vec{0}$; and for all $u \in V(G) - \{v_0\}$, $\phi_W(u) = W(P_u)$ where P_u is any arbitrary walk from v_0 to u in G. The mapping ϕ_W is well defined as W is non-singular. The convex-hull of the point set $\{\phi_W(u) : u \in V(G)\}$ defines a polytope denoted by $\phi_W(G)$. Vertices of this polytope are obviously from the set $\{\phi_W(u) : u \in V(G)\}$. We show that the converse is also true. It may be noted that the choice of v_0 is immaterial since it does not affect the shape or the orientation of the resulting polytope.

Let $G_{\mathcal{P}}$ be the edge graph of polytope $\mathcal{P}$ and W its geometric weight. Let W_α be a derived weight from W. Then the polytope $\phi_{W_\alpha}(G_{\mathcal{P}})$ is called a *derived polytope* of $\mathcal{P}$ and denoted by $\mathcal{P}_\alpha$. For simplicity we shall use ϕ_α in place of ϕ_{W_α}, where W should be clear from the context. We have the following important result.

Lemma 11 *For any $\mathcal{P}$, vertex v, direction vector ω, and a derived geometric weight W_α, if vertex $v \in face_\omega(\mathcal{P})$, then $\phi_\alpha(v) \in face_\omega(\mathcal{P}_\alpha)$.*

Proof. Consider any point $\phi_\alpha(u)$ in the embedding. Consider a monotonic sequence $u_0(= u), u_1, \ldots, u_k(= v)$ in ω direction in $\mathcal{P}$. So $(\phi_\alpha(v) - \phi_\alpha(u)).\omega = \sum_{i=0}^{k-1}(\phi_\alpha(u_{i+1}) - \phi_\alpha(u_i)).\omega = \sum_{i=0}^{k-1} \alpha_i.(u_{i+1} - u_i).\omega$, where α_i is the weight factor of the edge $u_i u_{i+1}$. Due to monotonicity $(u_{i+1} - u_i).\omega \geq 0$ and $0 \leq \alpha_i \leq 1$ for all i, so $(\phi_\alpha(v) - \phi_\alpha(u)).\omega \geq 0$. Since $\phi_\alpha(u)$ is an arbitrarily chosen point, $\phi_\alpha(v)$ must belong to $face_\omega(\mathcal{P}_\alpha)$. □

Corollary 12 *For each vertex v of $\mathcal{P}$, $\phi_\alpha(v)$ is a vertex of $\mathcal{P}_\alpha$.*

This result implies that every normal to a vertex of $\mathcal{P}$ is also a normal to the corresponding vertex of $\mathcal{P}_\alpha$. This leads to the following obvious corollary.

Corollary 13 *Let $\mathcal{P}$ be a polytope and $\mathcal{Q} = \mathcal{P}_\alpha$ be a derived polytope. Then for every vertex v of $\mathcal{P}$, $N_\mathcal{P}(v) \subset N_\mathcal{Q}(\phi_\alpha(v))$.*

Lemma 14 *Let $\mathcal{P}$ be a polytope. If $\mathcal{P}_\alpha$ is a derived polytope, then $\mathcal{P}_\alpha + \mathcal{P}_{1-\alpha} = \mathcal{P}$.*

Proof. Denote $\mathcal{P}_\alpha$ by $\mathcal{Q}$, $\mathcal{P}_{1-\alpha}$ by $\mathcal{R}$ and $\mathcal{P}_\alpha + \mathcal{P}_{1-\alpha}$ by $\mathcal{P}'$.

Consider an arbitrary vertex v in $\mathcal{P}$. Let $v' = \phi_\alpha(v)$ and $v'' = \phi_{1-\alpha}(v)$. Then from the previous corollary $N_\mathcal{P}(v) \subseteq N_\mathcal{Q}(v') \cap N_\mathcal{R}(v'')$. From Lemma 6 $v''' = v' + v''$ is a vertex of $\mathcal{P}'$ with $N_{\mathcal{P}'}(v''') = N_\mathcal{Q}(v') \cap N_\mathcal{R}(v'')$. So $N_\mathcal{P}(v) \subseteq N_{\mathcal{P}'}(v''')$. Since $\cup_{v \in V_\mathcal{P}} N_\mathcal{P}(v) = \mathbb{R}^n$, $\cup_{v''' \in V_\mathcal{P}} N_\mathcal{P}(v) = \mathbb{R}^n$. This shows that the vertex set of $\mathcal{P}'$ is exactly $\{v''' : v \in V_\mathcal{P}\}$.

To show that $\mathcal{P} = \mathcal{P}'$ we also have to show that $v''' - u''' = v - u$ for each pair of vertices u, v of $\mathcal{P}$. Let $(w_e, d_e)_{e \in E(\mathcal{P})}$ be the geometric weight of $\mathcal{P}$. Consider any walk $u_0(= u), u_1, \ldots, u_k(= v)$. Then $v' - u' = \phi_\alpha(u_k) - \phi_\alpha(u_0) = \sum_{i=0}^{k-1} \alpha_i.(u_{i+1} - u_i)$. Similarly $v'' - u'' = \sum_{i=0}^{k-1}(1 - \alpha_i).(u_{i+1} - u_i)$. This gives $v''' - u''' = \sum_{i=0}^{k-1}(u_{i+1} - u_i) = u_k - u_0 = v - u$. □

Corollary 15 *Every derived polytope is a Minkowski summand of the original polytope.*

Next we will show the converse, namely, every Minkowski summand is a derived polytope.

Lemma 16 *Let polytope $\mathcal{Q}$ be a Minkowski summand of polytope $\mathcal{P}$. Then for each face f in $\mathcal{P}$, there is a face f' of $\mathcal{Q}$ such that f' is a Minkowski summand of f and $N_\mathcal{P}(f) \subseteq N_\mathcal{Q}(f')$.*

Proof. Let $\mathcal{R}$ be a polytope such that $\mathcal{P} = \mathcal{Q} + \mathcal{R}$. Let ω be a direction in $N_\mathcal{P}(f)$. So $f = face_\omega(\mathcal{P}) = face_\omega(\mathcal{Q}) + face_\omega(\mathcal{R})$ from Lemma 5. Let $f' = face_\omega(\mathcal{Q})$. From Lemma 6 $N_\mathcal{P}(f) \subseteq N_\mathcal{Q}(f')$. □

Let polytope $\mathcal{Q}$ be a Minkowski summand of polytope $\mathcal{P}$. Then define a map ψ from the faces of $\mathcal{P}$ to those of $\mathcal{Q}$ as stated in the above lemma - if f is a face of $\mathcal{P}$, and if f' is a face of $\mathcal{Q}$ such that a face $\exists f''$ of $\mathcal{R}$ such that $f = f' + f''$, then $\psi(f) = f'$. Lemma 7 shows that the map ψ is well-defined. For the 0- and 1-faces of $\mathcal{P}$, we will abuse the notation ψ. If $\vec{v}$ is the position vector of a vertex of $\mathcal{P}$, then $\psi(\vec{v})$ will denote the position vector of the corresponding vertex in $\mathcal{Q}$. Similarly if $\vec{e}$ denotes the edge vector of e then $\psi(\vec{e})$ will denote the edge vector for $\psi(e)$.

Observation 5 *The ψ-image of every vertex of $\mathcal{P}$ is a vertex and that of every edge of $\mathcal{P}$ is either a vertex or an edge. The image of a walk P from u to v is a walk from $\psi(u)$ to $\psi(v)$.*

Lemma 17 *Let $\mathcal{Q}$ be a Minkowski summand of a polytope $\mathcal{P}$ then it is a derived polytope of $\mathcal{P}$.*

Proof. From the previous lemma we know that for each edge $\vec{e}$ of $\mathcal{P}$, $\psi(\vec{e})$ is an edge/vertex of $\mathcal{Q}$ which is a summand of $\vec{e}$. Thus $\psi(\vec{e})$ is parallel to $\vec{e}$. Let α_e denote $|\psi(\vec{e})|/|\vec{e}|$ for each edge $\vec{e}$ of $\mathcal{P}$, which is less than or equal to 1. Consider the derived weight W_α defined by $\{\alpha_e\}_{e \in E}$.

Consider an arbitrary walk $w = u_0, u_1 \ldots, u_m$ in $\mathcal{P}$. Then $\phi_\alpha(\vec{u_m}) - \phi_\alpha(\vec{u_0}) = \sum_{i=0}^{m-1}(\phi_\alpha(\vec{u_{i+1}}) - \phi_\alpha(\vec{u_i})) = \sum_{i=0}^{m-1} \alpha_i.(\vec{u_{i+1}} - \vec{u_i}) = \sum_{i=0}^{m-1} \psi(e_i) = \sum_{i=0}^{m-1}(\psi(\vec{u_{i+1}}) - \psi(\vec{u_i})) = \psi(\vec{u_m}) - \psi(\vec{u_0})$. This establishes that $\mathcal{Q} = \mathcal{P}_\alpha$. □

Combining lemma 15 and 17 we have the main result.

Theorem 18 *For any polytope $\mathcal{P}$, a polytope $\mathcal{Q}$ is a Minkowski summand iff $\mathcal{Q}$ is some derived polytope of $\mathcal{P}$.*

The theorem can be equivalently stated as following.

Corollary 19 *A polytope has a proper Minkowski summand iff its edge graph has a proper derived weight (neither all α_e are 0 nor are all 1).*

Corollary 20 *For any lattice polytope $\mathcal{P}$, a lattice polytope $\mathcal{Q}$ is a Minkowski summand iff $\mathcal{Q}$ is a derived polytope $\mathcal{P}_\alpha$ such that all components of $\alpha_e.(\vec{v} - \vec{u})$ are integers for all edges $e = uv \in E_\mathcal{P}$.*

5 Computation of Minkowski summand

The Corollary 19 suggests that to discover a Minkowski summand of a polytope we only need to find if its edge graph has a derived weight. In this section we formulate a linear program (LP) which is feasible if and only if a derived weight exists.

Let $\mathcal{P}$ be a polytope. Each edge of the polytope $e = uv$, has the geometric weight $w_{uv} = \vec{v} - \vec{u}$ (equivalently $w_{vu} = \vec{u} - \vec{v}$). To compute a derived weight, we define a variable x_e for each edge e. The weight $\{w'_{uv} = x_e.(\vec{v} - \vec{u})$ would be a derived weight if and only if the weight of each basis cycle is zero (Theorem 3). The problem can be stated as a linear feasibility program.

Let $\mathcal{B}$ be a basis of $G_\mathcal{P}$. Let $c \in \mathcal{B}$ be denoted as $u_0, u_1, \ldots, u_m, u_{m+1}(= u_0)$, where u_j are the vertices on the cycle and let the edge $u_j u_{j+1}$ be denoted by e_j. Then the linear feasibility program (LP) is

$\sum_j x_{e_j}.(\vec{u_{j+1}} - \vec{u_j}) = \vec{0}, \quad \forall c \in \mathcal{B},$ **[P1]**
subject to
$0 \leq x_e \leq 1, \ \forall e \in E_\mathcal{P}; \sum_{e \in E_\mathcal{P}} x_e > 0;$
and $\sum_{uv \in E_\mathcal{P}}(1 - x_{uv}) > 0.$

The solution of the LP gives a derived weight of $G_\mathcal{P}$. The corresponding polytope, which is a summand of $\mathcal{P}$,

can be computed using the embedding described in the previous section. A trivial solution of this LP is $x_e = c$ where c is a constant in the interval $(0, 1)$. This gives Minkowski summands, both of which are *similar* to the original polytope.

If $\mathcal{P}$ is a lattice polytope and the summand should also be a lattice polytope, then we need to satisfy an additional condition that $x_e(\vec{v}-\vec{u})$ has all integral components, i.e., $x_e.gcd(\vec{v}-\vec{u})$ must be an integer (recall that $gcd(\vec{a})$ is the gcd of all the components of $\vec{a}$). This additional condition transforms the LP into the following linear integer feasibility program (IP) by defining integral variables y_e for $x_e.gcd(\vec{v}-\vec{u})$.

$\sum_j y_{e_j}.(\vec{u_{j+1}} - \vec{u_j})/gcd(\vec{u_{j+1}} - \vec{u_j}) = \vec{0}, \quad \forall c \in \mathcal{B}, \quad$ **[P2]**
subject to
$0 \leq y_{uv} \leq gcd(\vec{v}-\vec{u}), \ \forall e \in E_{\mathcal{P}}$;
$\sum_{e \in E_{\mathcal{P}}} y_e > 0$; and $\sum_{e \in E_{\mathcal{P}}} (gcd(\vec{v}-\vec{u}) - y_e) > 0$, where y_e are integer variables.

The number of variables in the IP is equal to the number of the edges in the polytope, $|E_{\mathcal{P}}|$. The number of equations is n times the number of cycles in the basis, which is $|E_{\mathcal{P}}| - |V_{\mathcal{P}}| + 1$ in case $\mathcal{B}$ is the set of fundamental cycles.

6 Experimental Results

We have discussed earlier that Gao and Lauder [1] have shown that the Minkowski decomposition of convex lattice polytope is an NP-complete problem even in 2 dimensions. Therefore no exact method is expected to be polynomial in complexity. In this section we show that the proposed solution based on solving an integer linear program is a reasonably practical approach.

Given positive integers d and an n, we randomly generate n lattice points in $\mathbb{R}^d$. In the first step we compute the edge-graph of the convexhull of these points. In the second step we solve the integer program P2. The edges of the polytope are computed by solving a linear program for each pair of vertices, checking whether the line segment connecting them is a face or not. We use GLPK (GNU linear programming kit) to solve the LP's and the IP. The experiments were carried out on a 32-bit machine running on Intel Pentium 4 processor with 2 GB RAM and the code was written in the `C` programming language.

We ran ten instances of each case and reported the average time in the Tables 1 and 2. As the method is exact the success rate is always 100%. The times consumed in the two steps are reported separately to highlight the fact that the first step used up most of the time. This is because we could not find an efficient algorithm to compute the edges of a polytope. From Gao and Lauder's experiments [3] we see that their method is more reliable for higher dimensions (d) and smaller point-sets (n). In lower dimensions our method is competative with their method in terms of the time. Since our method is exact, we believe its complements their algorithm.

Table 1: Time(secs) to find the edges

Dimension, d	**Points,** n			
	10	50	100	200
2	0.13	0.38	0.49	0.54
5	0.46	9.24	30.39	106.76
10	0.49	16.93	89.17	590.94
20	0.50	18.88	113.93	851.37

Table 2: Time(secs) to decide indecomposability, i.e., time to solve IP

Dimension, d	**Points,** n			
	10	50	100	200
2	0.00	0.01	0.01	0.01
5	0.01	0.08	0.17	0.35
10	0.01	0.42	1.72	6.48
20	0.02	0.81	3.74	18.70

Table 3: Time comparison in seconds between the algorithms for polytopes in 3 dimensions

n	**Gao's time [3]**		**Our time**	
	Success %	**Time**	**Graph**	**Ip soln.**
25	63	0.03	1.20	0.01
50	37	0.05	2.67	0.01
100	40	0.19	5.16	0.01
200	43	0.94	10.77	0.02
400	45	5.8	27.62	0.02
800	54	35.9	112.15	0.02

7 Conclusion

We have presented a criterion for Minkowski decomposition, general as well as integral. This reduces the problem of computing Minkowski summand into a linear (integer) program. We have reported experimental results. The performance of this approach can be improved significantly by using an efficient algorithm to compute the edges of the polytope. We believe this would give a performance comparable with the heuristic method proposed in [1].

References

[1] S. Gao and A. G. B. Lauder Decomposition of Polytopes and Polynomials. *Discrete and Computational Geometry* , 26:89–104, 2001.

[2] S. Gao Absolute irreducibility of polynomials via Newton polytopes. *J. of Algebra* , 231:501–520, 2001.

[3] S. Gao and A. G. B. Lauder Fast absolute irreducibility testing via Newton Polytopes. *preprint*

http://www.math.clemson.edu/faculty/Gao/papers/fastabs.pdf, 14 pages, 2004.

[4] A. M. Ostrowski Uber die Bedeutung der Theorie der konvexen Polyeder fur die formale Algebra. *Jahresberichte Deutsche Math. Verein* , 30:98–99, 1921.

[5] Reinhard Diestel Graph Theory. *Graduate text in Mathematics, Springer*, 173, July 2005

[6] Bernd Sturmfels Gröbner Bases and Convex Polytopes. *University Lecture Series, American Mathematical Society*, 8, December 1995

[7] D. Mount and R. Silverman Combinatorial and computational aspects of Minkowski decomposition. *Contemporary Mathematics* , 199:107-124, 1991.

[8] I. Emiris and E. Tsigaridas Minkowski decomposition of convex lattice polygons. *Algebraic geometry and geometric modelling. Mathematics and Visualization, Springer* , 207–224, 2005.

[9] R. Silverman and A. Stein Algorithms for the decomposition of convex polygons. *Comtemporary Mathematics* , 119:159–168, 1991.

[10] M. L. Balinski On the graph structure of convex polyhedra in n-space. *Pacific Journal Of Mathematics* , 11:431–434, 1961.