Communications to SIMAI Congress,
ISSN 1827-9015, Vol. 3 (2009) 317 (11pp)
DOI: 10.1685/CSC09317

Staircase polytopes and visualization of targets

ADELINA FABIANO
Department of Mathematics, Faculty of Engineering, University of Calabria
Campus di Arcavacata, Via P. Bucci - I 87036 RENDE (CS)
e-mail: fabiano@unical.it

GAETANA RESTUCCIA
Department of Mathematics, Faculty of Sciences, University of Messina
C.da Papardo, Sal. Sperone, 31 - I 98166 MESSINA
e-mail: grest@dipmat.unime.it

Abstract

Staircase diagrams of monomial ideals in two or three variables are employed for having geometric objects useful in some applications to security problems.

Keywords and phrases: Monomial ideals, graphs
AMS 2000 Classifications: 05E99, 68R10

Introduction

Monomial ideals are very interesting objects from the combinatorial point of view.
In the square-free case, their connection with graphs theory, simplicial complexes, makes them precious for the applications in different fields from the commutative algebra and algebraic geometry.

Our aim is a project of application in the field of security in the world to help to encrypt messages, to transmit reserved information.

The techniques that we have to utilize are complex and, as a consequence, accessible only a restricted and selected set of mathematicians, so they are a very sure instrument for reserved operations.

Source of inspiration is the staircase speak, in the 2- or 3-dimensional case, since we can build diagrams significant for our purposes.

More precisely, in section 1. we recall some definitions and introduce new classes of monomial ideals, obtained, through a selection process, by Veronese monomial ideals, the so-called ideals of Veronese type and the

Received 16/01/2009, in final form 24/06/2009
Published 31/07/2009

bounded ideals of Veronese type (see [1], [6]).

In section 2. we consider the bi-dimensional and three-dimensional cases and the staircase polytopes that are the diagrams of a monomial ideal. Then we consider the construction of selected staircase diagrams, useful in the security field.

In section 3. we give, as an application, the construction of a friend graph, located on the surface of the staircase polytope. From such a graph we can obtain new regions and new paths on the staircase surface, for reserved information.

1. Selection procedures for monomial ideals

In this section we will introduce some definitions and results that we will utilize later.

Let A be the polynomial ring $A = K[\, x_1, x_2, \ldots, x_n \,]$, K a field.

Definition 1.1. Let I be a monomial ideal of A generated in degree $q > 0$. We call I a *q-Veronese ideal* if I is generated by all monomials in A of degree q.

Let I be a monomial ideal of A and I_q denote the ideal generated by all monomials in I of degree q.

Definition 1.2. Let I be a monomial ideal of A.
We call I a *Veronese ideal* if I_q is a q-Veronese ideal, for each $q > 0$.

Definition 1.3. Let I be a monomial ideal of A generated in degree $q > 0$. We call I an *ideal of Veronese type* if I is generated by the set of monomials in A of degree q such that

$$\{x_1^{a_{i_1}} \cdots x_n^{a_{i_n}} | \sum_{j=1}^{n} a_{i_j} = q, \;\; 0 \leq a_{i_1} \leq s_1, \;\ldots,\; 0 \leq a_{i_n} \leq s_n\} \;\; .$$

We denote this ideal $I_{q;s_1,\ldots,s_n}$.
If $s_1 = \cdots = s_n = s$, we write $I_{q;s}$.
For $s = q$, it is $I_{q;s} = I_q$.

Definition 1.4. Let I be a monomial ideal of A.
We call I an *ideal of Veronese type* if I_q is Veronese type, for each $q > 0$.

Example 1.1. (Ideal of Veronese type generated in degree 3)
Let $A = K[x_1, x_2, x_3]$.

DOI: 10.1685/CSC09317

$I_{3;2} = (x_1^2x_2, x_1^2x_3, x_1x_2^2, x_2^2x_3, x_1x_3^2, x_2x_3^2, x_1x_2x_3)$
$I_{3;2,1,1} = (x_1^2x_2, x_1^2x_3, x_1x_2x_3)$

Example 1.2. (Ideal of Veronese type)
Let $A = K[x_1, x_2, x_3]$.
$I = (x_1^2, x_1x_2, x_2^2, x_1x_3^2, x_2x_3^2)$
$I_2 = I_{2;2} = (x_1^2, x_1x_2, x_2^2)$
$I_3 = I_{3;3,3,2} = (x_1^3, x_1^2x_2, x_1^2x_3, x_1x_2^2, x_1x_2x_3, x_1x_3^2, x_2^3, x_2^2x_3, x_2x_3^2)$
$I_4 = I_{4;4,4,3}$
$I_5 = I_{5;5,5,4}$
. . . . . .

Remark 1.1. If I is an ideal of Veronese type, for some $q > 0$, then I is Veronese type.

Let's now introduce a new class of ideals that, from our point of view, is more interesting than the previous class of ideals of Veronese type.

Definition 1.5. Let I be a monomial ideal of A generated in degree $q > 0$. We call I a *bounded ideal of Veronese type* if I is generated by the set of monomials in A of degree q such that

$$\{x_1^{a_{i_1}} \cdots x_n^{a_{i_n}} | \sum_{j=1}^{n} a_{i_j} = q, \;\; 0 \leq r_1 \leq a_{i_1} \leq s_1, \; \ldots, \; 0 \leq r_n \leq a_{i_n} \leq s_n\}.$$

We denote this ideal $I_{q;r_1,\ldots,r_n;s_1,\ldots,s_n}$.
If $r_1 = \cdots = r_n = 0$, the ideal I is an ideal of Veronese type in degree $q > 0$.

Definition 1.6. Let I be a monomial ideal of A.
We call I a *bounded ideal of Veronese type* if I_q is a bounded ideal of Veronese type, for each $q > 0$.

Definition 1.7. Let I be a monomial ideal of A.
A *selected ideal* I' from I is a monomial ideal generated by a subset of the set of minimal generators of I.

Prop 1.1. Let I be a Veronese ideal in degree q, I' be the ideal of Veronese type in degree q and I'' be the bounded ideal of Veronese type in degree q. Then I' and I'' are selected ideals from I, and I'' a selected ideal from I'.

Example 1.3. (selected ideals)
Let $A = K[x_1, x_2, x_3]$.
Let's consider the ideals in the Example 1.1 and select generators inside

them.
$I_{3;2,1,1;2,2,1} = (x_1^2x_2, x_1^2x_3, x_2^2x_3, x_2x_3^2)$.
In fact, we select 4 generators inside $I_{3;2}$.
$I_{3;2,1,1;2,1,1} = (x_1^2x_2, x_1^2x_3)$.
In fact, we select 2 generators inside $I_{3;2,1,1}$.

Definition 1.8. Let I be a monomial ideal in $K[x_1, x_2, x_3]$.
We call I a *strongly generic* ideal if every pair of minimal generators $x_1^i x_2^j x_3^k$ and $x_1^{i'} x_2^{j'} x_3^{k'}$ of I satisfies
$i \neq i'$ or $i = i' = 0$, $j \neq j'$ or $j = j' = 0$, and $k \neq k'$ or $k = k' = 0$.

Example 1.4. $I = (x_1^2, x_2^2, x_3^2, x_1x_2, x_2x_3) \subset K[x_1, x_2, x_3]$ is strongly generic.

Remark 1.2. In general, Veronese ideals or ideals of Veronese type are not strongly generic.
But $I = (x_1^2, x_1x_2, x_2^2)$ yes.

2. Staircase polytopes

The staircases speak uses the convex geometric techniques, and, contemporary, combinatorial and algebraic methods, to express data associated to arbitrary monomial ideals in two or three variables.

Our main purpose is that to describe the (planar) graphs arising from the monomial ideals in two or three variables. For this reason we will denote the variables x_1, x_2, x_3 by x, y, z, obtaining a visible effect.

Consider an arbitrary monomial ideal I in the bivariate polynomial ring $A = K[x, y]$, $I = (m_1, \ldots, m_r)$, where each m_i is a minimal monomial generator of I. We write

$$I = (m_1, \ldots, m_r) = (x^{a_1}y^{b_1}, x^{a_2}y^{b_2}, \ldots, x^{a_r}y^{b_r}),$$

where $a_1 > a_2 > \cdots > a_r \geq 0$ and $b_1 > b_2 > \cdots > b_r \geq 0$.

Remark 2.1. The diagram for I shows the interface between two regions of the plane xy:
1st region: contains monomials in I (as exponent vectors of the monomials),
2nd region: contains monomials not belonging to I.

The staircase diagram for the ideal I is the following:

DOI: 10.1685/CSC09317

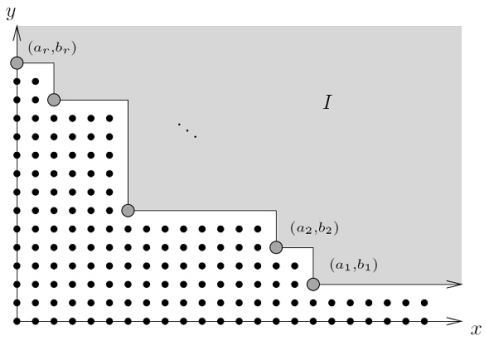
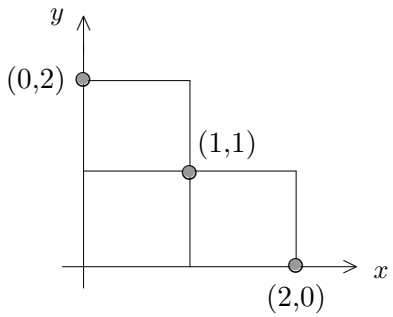


Fig. 1.

Let I be a Veronese ideal in degree q, I' be the ideal of Veronese type in degree q and I'' be the bounded ideal of Veronese type in degree q.
Let's D denote the staircase diagram of I and D', D'' denote the staircase diagrams of I', I'' respectively.

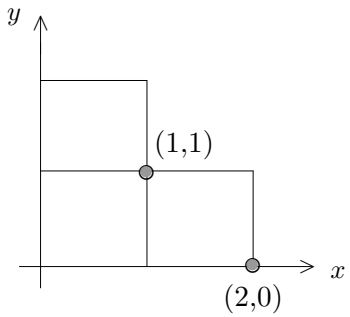
Remark 2.2. The diagrams D' and D'' can be obtained from D by skipping some corners.

Example 2.1. $I = (x^2, xy, y^2)$

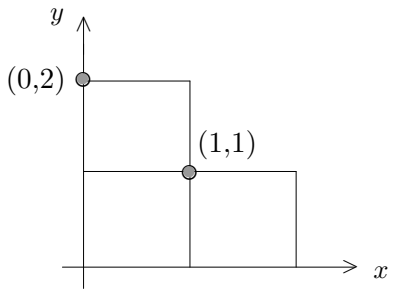


$x \notin I \Longrightarrow (1,0) \in 2^{\text{nd}}$ region
$x^3y \in I \Longrightarrow (3,1) \in 1^{\text{st}}$ region

Example 2.2. $I = (x^2, xy)$



Example 2.3. $I = (xy, y^2)$



Remark 2.3. In the Examples 2.2, 2.3, we delete (or select) a lattice joint. Moreover:

in the Example 2.1, I is the 2-Veronese ideal of $K[x, y]$;
in the Example 2.2, I is the ideal of Veronese type of $K[x, y]$ in degree 2, with $i_1 \leq 2$, $i_2 \leq 1$;
in the Example 2.3, I is the ideal of Veronese type of $K[x, y]$ in degree 2, with $i_1 \leq 1$, $i_2 \leq 2$.

In the following we will look at these examples in two variables for some ideas about security.

Each ideal of Veronese type in degree q selects monomials inside the minimal generators of the q-Veronese ideal.

Example 2.4. Let $q = 4$, $I = (x^4, x^3y, x^2y^2, xy^3, y^4)$ be the 4-Veronese ideal. We can consider the correspondences:

$$4 \longrightarrow \{(4,0), (3,1), (2,2), (1,3), (0,4)\}$$

$$(4; 3, 2) \longrightarrow \{(3,1), (2,2)\},$$

where $(4; 3, 2)$ means the Veronese ideal generated in degree 4 and type $(3, 2)$, in the sense that $I = (x^{i_1}x^{i_2} \mid i_1 + i_2 = 4\,,\ i_1 \leqslant 3\,,\ i_2 \leqslant 2)\,.$

DOI: 10.1685/CSC09317

Other examples:

$(4;3,1) \longrightarrow \{(3,1)\}$
$(4;2,2) \longrightarrow \{(2,2)\}$
$(4;1,3) \longrightarrow \{(1,3)\}$
$(4;3,3) \longrightarrow \{(3,1),(2,2),(1,3)\}$

Remark 2.4. In the staircase diagram of a Veronese ideal, no step is skipped.
In the staircase diagram of an ideal of Veronese type, some steps are skipped.

For monomial ideals in three variables, the staircase diagram is more interesting from our point of view. Consider the monomial ideal

$$I = (x^4, y^4, z^4, x^3y^2z, xy^3z^2, xy^2, x^2yz^3)$$

(not generated in the same degree).
Its staircase diagram in three variables is the following ([3], Fig. 3.1):

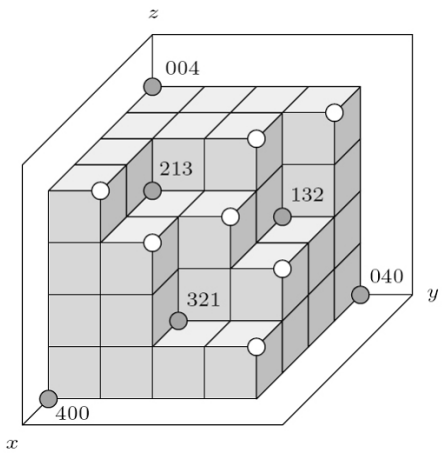


Fig. 2.

The surface of the staircase diagram is the interface between being in I or not being in I. The lattice points strictly behind the interface are those outside of I. Any lattice point that is visible in the staircase diagram is the exponent vector of a monomial in I. Dark dots correspond to the minimal generators of I (sit at the inner corner).

In the same way, as in the 2-dimensional case, we can select lattice points in the staircase diagram in 3-dimensional case.
In particular, if we consider ideals of Veronese type or bounded ideals of Veronese type instead of Veronese ideals, we have a combinatorial rule to select points (loci) in possible displacements of targets.

3. Buchberger graphs

Definition 3.1. ([3], Def. 3.4)
Let $A = K[x_1, x_2, \ldots, x_n]$ be the multivariate polynomial ring over a field K. Let $I = (m_1, \ldots, m_r)$ be a monomial ideal of A.
The *Buchberger graph* of I, Buch(I), is a graph such that:
1) its number of vertices equals the number of minimal generators of I;
2) the couple (i, j) is an edge if, denoted $m = \mathrm{lmc}\,(m_i, m_j)$, each generator m_k, $k \neq i, j$, having degree different from that of m in every variable that occurs in m, satisfies $m_k \nmid m$.

Example 3.1. If $I = (m_1, \ldots, m_r)$ is a monomial ideal in $K[x, y]$, then Buch(I) has r vertices and $r - 1$ consecutive edges.

In the 3-dimensional case, there exist monomial ideals such that Buch(I) can be embedded nicely into staircase diagrams, in the sense that one requires that Buch(I) is planar or Buch(I) is connected, and other its nice properties.

Example 3.2. Let $I = (x^4, y^4, z^4, x^3y^2z, xy^3z^2, xy^2, x^2yz^3)$.
We have the following picture for Buch(I) ([3], page 48),

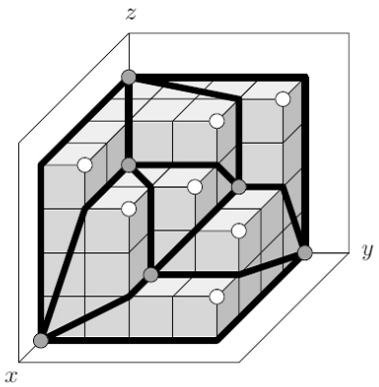


Fig. 3.

DOI: 10.1685/CSC09317

This is a planar and connected graph.

Proposition 3.1. *If $I \subset K[x,y,z]$ is a strongly generic ideal, then the Buchberger graph is planar and connected.*

Proof. See [3], Prop. 3.9 .

Definition 3.2. Let $I \subset A$ be a Veronese ideal in degree q, I' be an ideal of Veronese type in degree q and I'' be a bounded ideal of Veronese type in degree q.
Let G be the Buchberger graph of I.
The Buchberger graphs G', G'' of I', I'' respectively, are called *selected graphs* from G.

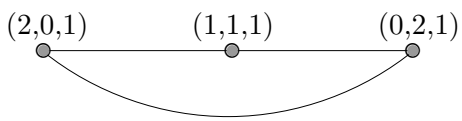
Remark 3.1. G' and G'' are obtained from G by deleting vertices and joining the remaining vertices.

The following definition characterizes classes of graphs in the 3-dimensional case with nice properties.

Definition 3.3. Let $I = (m_1, \ldots, m_r)$ be a monomial ideal of $K[x_1, x_2, \ldots, x_n]$.
We call Buch(I) a *friend graph* if the following conditions are satisfied:
1) $\mathrm{lmc}\,(m_i, m_j)$ lies on the staircase surface of the staircase diagram of I;
2) $\mathrm{lmc}\,(m_i, m_j)$ has not other edge passing through it;
3) each edge (i,j) in Buch(I) is drawn in the staircase surface as the union of two line segments (from m_i to $\mathrm{lmc}\,(m_i, m_j)$ and from m_j to $\mathrm{lmc}\,(m_i, m_j)$).

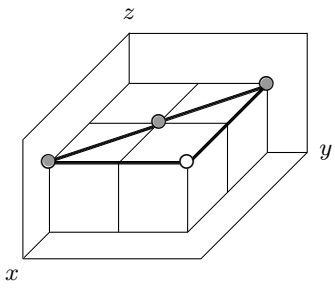
Example 3.3. If $I \subset K[x,y,z]$ is strongly generic, then Buch(I) is a friend graph and, in addition, Buch(I) lies on its staircase surface.

Example 3.4. $I = (x^2z, xyz, y^2z) \subset K[x,y,z]$ is a friend graph.
In fact, *Buch*(I) is the graph:



and $\mathrm{lmc}\,(x^2z, xyz) = x^2yz$, $\mathrm{lmc}\,(x^2z, y^2z) = x^2y^2z$, $\mathrm{lmc}\,(xyz, y^2z) = xy^2z$.

The staircase diagram is the following:



and we can see the planar graph on the plane $z = 1$.
The lattice point (2,2,1) on the surface of the staircase polytope is not a vertex of the graph, but it satisfies conditions 1), 2), 3) of Definition 3.3 .

Proposition 3.2. *Let I be a monomial ideal of $A = K[x, y, z]$ generated by r monomials $m_{ijk} = x^i y^j z^k$, $i, j, k \leqslant 0$ such that $i = const$, or $j = const$, or $k = const$. Then Buch (I) is planar and it has r vertices and $r-1$ edges.*

Proof. In $i = \text{const}$, all lattice points that correspond to the generators of I lie on the plane $x = \text{const}$ of the staircase diagram. Then Buch (I) is planar. Similarly for the remaining cases. □

Remark 3.2. In particular, if $i = j$, all lattice points lie on the line having equation $i = \text{const}$, $j = \text{const}$, and Buch (I) is a path with r vertices and $r - 1$ edges. Analogue result if $i = k$ or $j = k$.

We encourage to utilize the previous results for developing topics and their applications in security fields. The same direction has been followed in the papers [2], [4].

REFERENCES

1. Bruns W., Herzog J. - *Cohen-Macaulay rings*, Revised Edition, Cambridge University Press (1997).
2. Crupi M., Rinaldo G. - *A defense strategy by edge ideals*, *Communications to SIMAI Congress* (on line), Vol. **3** (2009) - ISSN: 1827-9015.
3. Miller E., Sturmfels B. - *Combinatorial Commutative Algebra*, Springer GTM **227** (2004).
4. Staglianò P.L. - *Integral closure of monomial ideals*, *Communications to SIMAI Congress* (on line), Vol. **3** (2009) - ISSN: 1827-9015.

DOI: 10.1685/CSC09317

5. Sturmfels B. - *Gröbner Bases and Convex Polytopes*, AMS Univ. Lect. Ser. **8** (1996).

6. Villarreal R.H. - *Monomial algebras*, Dekker, New York (2001).