On Simple Representation of Locally Closed Sets

Yosuke Sato [1] *Ryoya Fukasaku* [2] *Katsusuke Nabeshima* [3]

[1] ysato@rs.kagu.tus.ac.jp [2] fukasaku@rs.tus.ac.jp
[3] nabeshima@tokushima-u.ac.jp

[1,2] Department of Mathematical Information Science
Tokyo University of Science
1-3,Kagurazaka,Shinjukuku, Tokyo, Japan

[3] Graduate School of Science and Technology
Tokushima University
2-1, Minamijosanjima, Tokushima, Japan

Abstract

A locally closed set of an affine space is defined as a difference of two varieties. Simple representation of locally closed sets is of great importance in many areas of computational mathematics. We presents a practical simplification algorithm of locally closed sets. Our algorithm consists only of computations of Gröbner bases, it does not use any heavy computation of polynomial ideals such as a primary decomposition.

1 Introduction

A locally closed set of an affine space $\mathbb{C}^n$ is defined as a difference $V(I) \setminus V(J)$ of the varieties of two ideals I and J in a polynomial ring $\mathbb{Q}[X_1, \ldots, X_n]$. We need to handle it in many areas of computational mathematics. A simple representation of a locally closed set is especially important.

Consider the following example of quantifier elimination dealt with in our previous paper [9], which comes from the problem #4 of International Mathematical Olympiad 2013.

Example 1 $\forall x_1, x_2, y_1, y_2, m_1, m_2, h_2, w \in \mathbb{C}(w \neq 0 \wedge w \neq 1 \wedge F_1 = 0 \wedge F_2 = 0 \wedge F_3 = 0 \wedge F_4 = 0 \wedge F_5 = 0 \wedge F_6 = 0 \wedge F_7 = 0 \Rightarrow P = 0)$.

Where, $F_1 = m_1c_2 - m_2c_1, F_2 = (c_1-1)c_1 + h_2c_2, F_3 = (m_1-1)c_1 + m_2c_2, F_4 = ((1+w(c_1-1)) - x_1)^2 + (wc_2 - x_2)^2 - (((1+w(c_1-1)) + x_1 - 2c_1)^2 + (wc_2 + x_2)^2), F_5 = ((1+w(c_1-1)) - x_1)^2 + (wc_2 - x_2)^2 - (((1+w(c_1-1)) + x_1 - 2)^2 + (wc_2 + x_2)^2), F_6 = ((1+w(c_1-1)) - y_1)^2 + (wc_2 -$

$y_2)^2 - (((1+w(c_1-1))+y_1-2mc_1)^2+(wc_2+y_2-2mc_2)^2), F_7 = ((1+w(c_1-1))-y_1)^2+(wc_2-y_2)^2-(((1+w(c_1-1))+y_1-2c_1)^2+(wc_2+y_2-2c_2)^2), P = (y_1-c_1)(y_2-x_2)-(y_2-h_2)(y_1-x_1)$.

In order to eliminate all quantifiers $\forall x_1, x_2, y_1, y_2, m_1, m_2, h_2, w$, we need to compute a comprehensive Gröbner system of the ideal $\langle w(w-1)v-1, Pu-1, F_1, F_2, F_3, F_4, F_5, F_6, F_7\rangle$ in the polynomial ring $\mathbb{Q}[c1, c2, u, v, x_1, x_2, y_1, y_2, m_1, m_2, h_2, w]$ with parameters c_1, c_2 and main variables $u, v, x_1, x_2, y_1, y_2, m_1, m_2, h_2, w$. (For more detailed descriptions, see [6] for example.)
The following is the output of the execution of our program written in Risa/Asir [4] which computes comprehensive Gröbner systems using the algorithm introduced in [8]. The output reads as follows. There are 5 segments of parameter space $\mathbb{C}^2$ each of which is given in a form of a locally closed set. After each segment, there is a corresponding list of a Gröbner basis. For example, the second segment `[[c1-1],[c2^3+c2,c1-1]]` is the locally closed set $V(\langle c_1-1\rangle)\setminus V(\langle c_2^3+c_2, c_1-1\rangle)$. For each value of c_1, c_2 lying in this segment, the Gröbner basis of the ideal $\langle w(w-1)v-1, Pu-1, F_1, F_2, F_3, F_4, F_5, F_6, F_7\rangle$ in $\mathbb{Q}[u, v, x_1, x_2, y_1, y_2, m_1, m_2, h_2, w]$ is $\{(w^2-w)v-1, c_2^2ux_1-c_2^2u-c_2, -c_2x_2, -c_2y_1-c_2^3w+c_2, c_2y_2-c_2^2, -m_1-m_2c_2+1, -m_2c_2^2+c_2-m_2, h_2c_2\}$. The term order is degree reverse lexicographic, which is assigned by `0` in
`cgs.cgs([w*(w-1)*v-1,P*u-1,F1,F2,F3,F4,F5,F6,F7],`
`[c1,c2],[u,v,x1,x2,y1,y2,m1,m2,h2,w],0)$`.

```
[1854] load("./cgs.rr")$
[2074] F1=m1*c2-m2*c1$
F2=(c1-1)*c1+h2*c2$
F3=(m1-1)*c1+m2*c2$
F4=((1+w*(c1-1))-x1)^2+(w*c2-x2)^2-(((1+w*(c1-1))+x1-2*c1)^2+(w*c2+x2)^2)$
F5=((1+w*(c1-1))-x1)^2+(w*c2-x2)^2-(((1+w*(c1-1))+x1-2)^2+(w*c2+x2)^2)$
F6=((1+w*(c1-1))-y1)^2+(w*c2-y2)^2-(((1+w*(c1-1))+y1-2*m1)^2+
                                                        (w*c2+y2-2*m2)^2)$
F7=((1+w*(c1-1))-y1)^2+(w*c2-y2)^2-(((1+w*(c1-1))+y1-2*c1)^2
                                                       +(w*c2+y2-2*c2)^2)$
P=(y1-c1)*(y2-x2)-(y2-h2)*(y1-x1)$
[2082] cgs.cgs([w*(w-1)*v-1,P*u-1,F1,F2,F3,F4,F5,F6,F7],
[c1,c2],[u,v,x1,x2,y1,y2,m1,m2,h2,w],0)$

CGS is the following:
[[c2^2+1,c1-1],[1]]
[1]

[[c1-1],[c2^3+c2,c1-1]]
[(w^2-w)*v-1,c2^2*u*x1-c2^2*u-c2,-c2*x2,-c2*y1-c2^3*w+c2,c2*y2-c2^2,
-m1-m2*c2+1,-m2*c2^2+c2-m2,h2*c2]

[[c1-1,c2],[1]]
[(-u*x1+u)*y2+(u*x2-h2*u)*y1-u*x2+h2*u*x1+1,(w^2-w)*v-1,-m1+1,m2]

[[c1^2-c1,c2],[c1-1,c2]]
[1]
```

```
[[c2^2+c1^2-c1],[c1^2-c1,c2]]
[(w^2-w)*v-1,c2*u*y2-c2^2*u-c2,(-c1+1)*u*y2+(c1-1)*c2*u+c1-1,
-c2*x1+(-c1+1)*c2*w+c1*c2,(-c1+1)*x1+(c2^2+c1-1)*w-c2^2,
-c2*x2+(-c2^2-c1+1)*w+c2^2+c1-1,-c1*c2*y2+c2^2*y1,c2*y2+(c1-1)*y1,
-m1+c1,-c2+m2,(c1-1)*c2-h2*c1+h2,-c2^2+h2*c2]

[[0],[(c1-1)*c2^2+c1^3-2*c1^2+c1]]
[(c1-1)*c2^2+c1^3-2*c1^2+c1]

No. of segment is
6
0.02668sec + gc : 0.00797sec(0.03525sec)
```

By Hilbert's Nullstellensatz, we have the following equivalent quantifier free formula:

$$(c_2^2+1=0 \wedge c_1=1) \vee ((c_1^2=c_1 \wedge c_2=0) \wedge (c_1 \neq 1 \vee c_2 \neq 0)) \vee (c_1-1)c_2^2+c_1^3-2c_1^2+c_1 \neq 0.$$

Note that the second formula $(c_1^2 = c_1 \wedge c_2 = 0) \wedge (c_1 \neq 1 \vee c_2 \neq 0)$ is equivalent to the much simpler formula $c_1 = 0 \wedge c_2 = 0$. In other words, the locally closed set $V(\langle c_1^2 - c_1, c_2\rangle) \setminus V(\langle c_1 - 1, c_2\rangle)$ is equal to the locally closed set $V(\langle c_1, c_2\rangle) \setminus V(\langle 1\rangle)$.

In [2], a simple representation of a locally closed set is introduced. Given ideals I and J of a polynomial ring $\mathbb{Q}[X_1, \ldots, X_n]$ such that $I \subset J$. (Since $V(I) \setminus V(J) = V(I) \setminus V(I+J)$, we can always assume that $I \subset J$ without loss of generality.) Let the prime decompositions of the radical ideals $\sqrt{I}$ and $\sqrt{J}$ be $\sqrt{I} = P_1 \cap \cdots \cap P_l \cap P_{l+1} \cap \cdots \cap P_m$ and $\sqrt{J} = P_{l+1} \cap \cdots \cap P_m$. They introduce a canonical representation of the locally closed set $V(I) \setminus V(J)$ as $V(P_1 \cap \cdots \cap P_l) \setminus V(P_{l+1} \cap \cdots \cap P_m + P_1 \cap \cdots \cap P_l)$. Since $V(P_1 \cap \cdots \cap P_l)$ is the Zariski closure $\overline{V(I) \setminus V(J)}$ of $V(I) \setminus V(J)$, i.e. the smallest variety which contains $V(I) \setminus V(J)$, the representation can be considered smallest. For the above example, $I = \langle c_1^2 - c_1, c_2\rangle$ and $J = \langle c_1 - 1, c_2\rangle$, we have $\sqrt{I} = P_1 \cap P_2$ and $\sqrt{J} = P_2$ with prime ideals $P_1 = \langle c_1, c_2\rangle$ and $P_2 = \langle c_1 - 1, c_2\rangle$. Since $P_1 + P_2 = \langle 1\rangle$, we have its canonical representation $V(\langle c_1, c_2\rangle) \setminus V(\langle 1\rangle)$ as is desired. In [2], they also give an algorithm to compute the canonical representation which is based on a primary decomposition algorithm of rational polynomial ideals. Their approach is simple and beautiful from a theoretical point of view. However, for some more advanced algorithm of computer algebra such as a recent real quantifier elimination algorithm introduced in [7], we often need to deal with a more complicated locally closed set. For such a case, their algorithm is not practical since a primary decomposition algorithm needs very heavy computations in general.

In this paper we introduce a more practical representation of a locally closed set. It is based on the fact that the Zariski closure $\overline{V(I) \setminus V(J)}$ is equal to the variety $V(I : J^\infty)$ of the saturation ideal $I : J^\infty$. Our representation of the locally closed set $V(I) \setminus V(J)$ is given by $V(I : J^\infty) \setminus V(J + (I : J^\infty))$. Since $\sqrt{I : J^\infty} = P_1 \cap \cdots \cap P_l$, our representation is same as the representation of [2] if $I : J^\infty$ and $J + I : J^\infty$ are radical. Even if they are not radical we have the same varieties $V(I : J^\infty) = V(P_1 \cap \cdots \cap P_l)$ and $V(J + (I : J^\infty)) = V(P_{l+1} \cap \cdots \cap P_m + P_1 \cap \cdots \cap P_l)$. Note that we can compute a saturation ideal by the computation of Gröbner bases. In general Gröbner bases computation is much lighter than the computation of primary decomposition of polynomial ideals.

The paper is organized as follows. In section 2, we describe basic properties of locally closed sets. The well-known fact $\overline{V(I) \setminus V(J)} = V(I : J^\infty)$ we are using in the paper may be already published in some paper. Nevertheless, in most standard texts of computer algebra such as [3], it is described only for very special cases such as I is a radical ideal or J is a principal ideal. We give a complete proof of it. Then we describe our algorithm which is naturally derived from it. In section 3, we give a typical computation example for seeing efficiency of our algorithm.

2 Basic Mathematics

Throughout this section K denotes the field of rational numbers $\mathbb{Q}$ and L denotes the field of complex numbers $\mathbb{C}$. Note that all results also hold for any computable field K and its algebraically closed extension L.

For an ideal I of a polynomial ring $K[X_1, \ldots, X_n]$, $V(I)$ denotes a variety of I in L that is $V(I) = \{\bar{c} \in L^n | \forall f \in I f(\bar{c}) = 0\}$. For a subset S of an affine space L^n, $\overline{S}$ denotes the Zariski closure of S, that is $\overline{S}$ is the smallest variety which contains S w.r.t. the order of set inclusion. $\bar{X}$ denotes variables $X_1, \ldots, X_n$.

2.1 Locally Closed Set

Definition 2 *A locally closed set of an affine space L^n is a subset of L^n which is equal to a difference $V(I) \setminus V(J)$ of the varieties of some ideals I and J in $K[\bar{X}]$.*
(Since $V(I) \setminus V(J) = V(I) \setminus V(J + I)$, we can assume $I \subset J$).

A locally closed set has the smallest representation. More precisely we have the following fact.

Theorem 3 *Let $\sqrt{I} = P_1 \cap \cdots \cap P_l \cap P_{l+1} \cap \cdots \cap P_m$ and $\sqrt{J} = P_{l+1} \cap \cdots \cap P_m$ be the prime decompositions of the radical ideals $\sqrt{I}$ and $\sqrt{J}$. Then $V(I) \setminus V(J) = V(P_1 \cap \cdots \cap P_l) \setminus V(P_{l+1} \cap \cdots \cap P_m + P_1 \cap \cdots \cap P_l)$. Moreover, if $V(I) \setminus V(J) = V_1 \setminus V_2$ for some varieties V_1 and V_2 then $V_1 \supset V(P_1 \cap \cdots \cap P_l)$ and $V_2 \supset V(P_{l+1} \cap \cdots \cap P_m + P_1 \cap \cdots \cap P_l)$.*

Proof. The proof is straightforward. See [2] for example. ■

As a corollary we have the following.

Corollary 4 *$\overline{V(I) \setminus V(J)} = V(P_1 \cap \cdots \cap P_l)$.*

For a given locally closed set $V(I) \setminus V(J)$ in terms of ideals I and J, [2] gives an algorithm to obtain its smallest representation using primary decomposition of I and J. As is described in the previous section, the computation of a primary decomposition is very heavy in general. We can avoid such heavy computations using saturation of ideal.

2.2 Saturation of Ideal

Definition 5 *Let I and J be ideals of a polynomial ring $K[\bar{X}]$. There exists a natural number N such that $I : J^N = I : J^{N+1} = I : J^{N+2} = \cdots$. The ideal $I : J^N$ is called the saturation ideal of I by J and denoted $I : J^\infty$.*

The following theorem enables us to compute the Zariski closure $\overline{V(I) \setminus V(J)}$ without the computation of primary decomposition. The result is well-known but in most standard texts of computer algebra such as [3], its proof is given only for special cases such as I is a radical ideal or J is a principal ideal.

Theorem 6 *When $I \subset J$, $\overline{V(I) \setminus V(J)} = V(I : J^\infty)$.*

Proof. Let $I : J^\infty = I : J^N = I : J^{N+1} = \cdots$ and let $J = \langle g_1, \ldots, g_l \rangle$ for some $g_1, \ldots, g_l \in K[\bar{X}]$. For each $i = 1, \ldots, l$, there exists M_i such that $I : \langle g_i^{M_i} \rangle = I : \langle g_i \rangle^\infty$. Let M be $max(M_1, \ldots, M_l)$, then we have $I : \langle g_i^M \rangle = I : \langle g_i \rangle^\infty$ for every i. Note that there exists a natural number $m \geq N$ such that $J^m \subset \langle g_1^M, \ldots, g_l^M \rangle$. Then, $I : J^N = I : J^m \supset I : \langle g_1^M, \ldots, g_l^M \rangle = (I : \langle g_1^M \rangle) \cap \cdots \cap (I : \langle g_l^M \rangle) = (I : \langle g_1 \rangle^\infty) \cap \cdots \cap (I : \langle g_l \rangle^\infty)$. Note also that we have $\overline{V(I_1) \setminus V(I_2)} \subset V(I_1 : I_2)$ for any ideal I_1, I_2. (See section 4 of chapter 4 [3].) Hence, $\overline{V(I) \setminus V(J)} = \overline{V(I) \setminus V(J^N)} \subset V(I : J^N) \subset V(I : \langle g_1 \rangle^\infty) \cup \cdots \cup V(I : \langle g_l \rangle^\infty)$. Note also that $V(I : \langle f \rangle^\infty) = \overline{V(I) \setminus V(\langle f \rangle)}$ for any ideal I and polynomial f. (See section 4 of chapter 4 of [3].) Hence, $V(I : \langle g_1 \rangle^\infty) \cup \cdots \cup V(I : \langle g_l \rangle^\infty) = \overline{V(I) \setminus V(\langle g_1 \rangle)} \cup \cdots \cup \overline{V(I) \setminus V(\langle g_l \rangle)} = \overline{V(I) \setminus V(\langle g_1 \rangle) \cup \cdots \cup V(I) \setminus V(\langle g_l \rangle)} = \overline{V(I) \setminus V(\langle g_1, \ldots, g_l \rangle)} = \overline{V(I) \setminus V(J)}$. ■

By this theorem we have the following.

Corollary 7 *For a locally closed set $V(I) \setminus V(J)$ with ideals $I \subset J$, $V_1 = V(I : J^\infty)$ and $V_2 = V((I : J^\infty) + J)$ form the smallest varieties such that $V(I) \setminus V(J) = V_1 \setminus V_2$.*

2.3 Simplification Algorithm

The results presented in the previous subsection naturally lead us to the following simplification algorithm of a locally closed set.

Algorithm (Simplification of a locally closed set)
Input: $\{f_1, \ldots, f_l\}$ and $\{g_1, \ldots, g_m\} \subset K[\bar{X}]$;
Output: $\{p_1, \ldots, p_s\}$ and $\{q_1, \ldots, q_t\} \subset K[\bar{X}]$
such that $V_1 = V(\langle p_1, \ldots, p_s \rangle)$ and $V_2 = V(\langle q_1, \ldots, q_t \rangle)$ are the smallest varieties
such that $V_1 \setminus V_2 = V(\langle f_1, \ldots, f_l \rangle) \setminus V(\langle g_1, \ldots, g_m \rangle)$;
1: $Y \leftarrow$ a new variable;
For each $i = 1, \ldots, m$,
$H_i \leftarrow$ a reduced Gröbner basis of the ideal $\langle f_1, \ldots, f_l, Y g_i - 1 \rangle$ in $K[\bar{X}, Y]$ w.r.t. an elimination term order such that Y is lexicographically greater than $\bar{X}$;
$G_i \leftarrow H_i \cap K[\bar{X}]$;
2: $\bar{Z} = Z_1, \ldots, Z_{m-1} \leftarrow$ new variables;
$G \leftarrow$ a Gröbner basis of the ideal
$\langle \{Z_1 g | g \in G_1\} \cup \cdots \cup \{Z_{m-1} g | g \in G_{m-1}\} \cup \{(1 - Z_1 - \cdots - Z_{m-1}) g | g \in G_m\} \rangle$ in $K[\bar{X}, \bar{Z}]$
w.r.t. an elimination term order such that each Z_i is lexicographically greater than $\bar{X}$;
$\{p_1, \ldots, p_s\} \leftarrow G \cap K[\bar{X}]$;
3: $\{q_1, \ldots, q_t\} \leftarrow$ a Gröbner basis of $\langle p_1, \ldots, p_s, g_1, \ldots, g_m \rangle$ in $K[\bar{X}]$ w.r.t. some term order;

Proof of correctness. Each G_i is equal to the saturation ideal $\langle f_1, \ldots, f_l \rangle : \langle g_i \rangle^\infty$ by a well-known technique of Gröbner basis for the computation of a saturation ideal. $\{p_1, \ldots, p_s\}$ is a Gröbner basis of $\langle G_1 \rangle \cap \cdots \cap \langle G_m \rangle$ by also a well-known technique of Gröbner basis for the computation of an intersection of ideals. Since $\langle f_1, \ldots, f_l \rangle : \langle g_1 \rangle^\infty \cap \cdots \cap \langle f_1, \ldots, f_l \rangle : \langle g_m \rangle^\infty = \langle f_1, \ldots, f_l \rangle : \langle g_1, \ldots, g_m \rangle^\infty$, we have the desired properties by Corollary 7. ∎

3 Computation Example

We show two computation examples of our simplification algorithm using the Gröbner basis computation program `hgr` of Risa/Asir [4].

The first example is the simplification of the locally closed set $V(\langle c_1^2 - c_1, c_2 \rangle) \setminus V(\langle c_1 - 1, c_2 \rangle)$ discussed in the introduction. The inputs for our algorithm are $\{c_1^2 - c_1, c_2\}$ and $\{c_1 - 1, c_2\}$. The first two executions are the computations of the saturation ideals $\langle c_1^2 - c_1, c_2 \rangle : \langle c_1 - 1 \rangle$ and $\langle c_1^2 - c_1, c_2 \rangle : \langle c_2 \rangle$ (**1** of **Algorithm**). The third execution is the computation of $\{p_1, \ldots, p_s\}$, i.e. the intersection ideal of the obtained two saturation ideals (**2** of **Algorithm**). The last execution is the computation of $\{q_1, \ldots, q_t\}$ (**3** of **Algorithm**). We get a simple representation $V(\langle c_2, c_1 \rangle) \setminus V(\langle 1 \rangle)$.

```
[1855] hgr([c1^2-c1,c2,y*(c1-1)-1],[y,c1,c2],[[0,1],[0,2]]);

[c2,c1,-y-1]
0sec(0.0001938sec)

[1856] hgr([c1^2-c1,c2,y*c2-1],[y,c1,c2],[[0,1],[0,2]]);

[1]
0sec(6.795e-05sec)

[1857] hgr([z1*c2,z1*c1,(1-z1)*1],[z1,c1,c2],[[0,1],[0,2]]);

[c2,c1,-z1+1]
0sec(0.000273sec)

[1858] hgr([c2,c1,c1-1,c2],[c1,c2],0);

[1]
0.000133sec(0.0001321sec)
```

The second example is more complicated but such an example often rise up during the execution of the real quantifier elimination program introduced in [7].
Our locally closed set is $V(P_1 \cap P_2 \cap P_3) \setminus V(P_1 \cap P_2)$ with $P_1 = \langle 2x_1^2 + x_2^2 + 3x_3^2 - x_1, 3x_1^2 + x_2^2 + 2x_3^2 - x_2 \rangle$, $P_2 = \langle 2x_1^2 + 3x_2^2 + x_3^2 - x_1, 3x_1^2 + 2x_2^2 + x_3^2 - x_2 \rangle$, $P_3 = \langle 4x_1^2 + 2x_2^2 + 3x_3^2 - x_1, 4x_1^2 + 3x_2^2 + 2x_3^2 - x_3 \rangle$. $P_1 \cap P_2 \cap P_3$ and $P_1 \cap P_2$ have the following bases $\{f_1, f_2, f_3, f_4, f_5\}$ and $\{g_1, g_2\}$. Note that the locally closed set is given in terms of the polynomials $f_1, f_2, f_3, f_4, f_5, g_1, g_2$ and we do not know the polynomials P_1, P_2, P_3.
$f_1 = -4x_1^3 + (-4x_2^2 + 4x_3^2 + 4x_3 - 1)x_1^2 + (-2x_2^2 + 2x_2 + x_3)x_1 - x_2^4 + 2x_2^3 + x_3 x_2^2 + (-2x_3^2 -$

$2x_3)x_2 + x_3^4 + x_3^3$,
$f_2 = -16x_1^4 + 12x_1^3 + (8x_2 - 28x_3^2 - 12x_3 + 4)x_1^2 + (5x_2^2 - 8x_2 - 2x_3^2 - 3x_3)x_1 + x_2^4 - 2x_2^3 + (-5x_3^2 - 3x_3)x_2^2 + (12x_3^2 + 6x_3)x_2 - 6x_3^4 - 3x_3^3$,
$f_3 = (-192x_2 - 576x_3^2 - 224x_3 - 2)x_1^3 + ((192x_3^2 + 96x_3 + 60)x_2 + 288x_3^4 + 288x_3^3 - 122x_3^2 - 26x_3 + 13)x_1^2 + (-30x_2^4 - 192x_2^3 + (-408x_3^2 - 92x_3 + 10)x_2^2 + (72x_3^2 + 112x_3 - 26)x_2 - 210x_3^4 - 20x_3^3 - 22x_3^2 + 3x_3)x_1 + 20x_2^5 + (30x_3^2 + 10x_3 + 21)x_2^4 + (224x_3^2 + 48x_3 + 70)x_2^3 + (228x_3^4 + 124x_3^3 - 86x_3^2 - 37x_3)x_2^2 + (-4x_3^4 - 96x_3^3 + 70x_3^2 - 6x_3)x_2 + 102x_3^6 + 82x_3^5 - 35x_3^4 + 3x_3^3$,
$f_4 = (2688x_2 + 8064x_3^2 + 3136x_3 + 388)x_1^3 + ((-2688x_3^2 - 1344x_3 - 1080)x_2 - 4032x_3^4 - 4032x_3^3 + 988x_3^2 + 4x_3 - 137)x_1^2 + (160x_2^4 + 2688x_2^3 + (6232x_3^2 + 1648x_3 + 30)x_2^2 + (-528x_3^2 - 1328x_3 + 274)x_2 + 3400x_3^4 + 640x_3^3 + 308x_3^2 - 87x_3)x_1 + 100x_2^6 - 40x_2^5 + (-240x_3 - 169)x_2^4 + (-3136x_3^2 - 912x_3 - 1070)x_2^3 + (-3612x_3^4 - 2256x_3^3 + 1124x_3^2 + 393x_3)x_2^2 + (-184x_3^4 + 1104x_3^3 - 890x_3^2 + 174x_3)x_2 - 1528x_3^6 - 1248x_3^5 + 445x_3^4 - 87x_3^3$,
$f_5 = ((576x_3^3 + 576x_3^2 - 172x_3 - 84)x_2 + 384x_3^3 + 576x_3^2 + 72x_3 + 72)x_1^3 + ((720x_3^3 + 488x_3^2 + 12x_3 - 115)x_2 + 336x_3^3 + 192x_3^2 - 12x_3 - 18)x_1^2 + ((60x_3 + 20)x_2^5 + (184x_3 + 88)x_2^4 + (456x_3^3 + 248x_3^2 + 20x_3 + 46)x_2^3 + (160x_3^3 + 112x_3^2 + 100x_3 + 140)x_2^2 + (204x_3^5 + 164x_3^4 - 76x_3^3 - 172x_3^2 - 17x_3 + 20)x_2 + 136x_3^5 + 184x_3^4 + 24x_3^3 + 84x_3^2 - 12x_3)x_1 + (84x_3 + 33)x_2^5 + (56x_3 + 38)x_2^4 + (408x_3^3 + 200x_3^2 - 41x_3 - 112)x_2^3 + (-52x_3^3 - 128x_3^2 - 58x_3)x_2^2 + (228x_3^5 + 119x_3^4 - 113x_3^3 - 124x_3^2 + 24x_3)x_2 + 116x_3^5 + 38x_3^4 - 12x_3^3$.

$g_1 = 4x_1^2 + x_1 + x_2^2 - 2x_2 + x_3^2$,
$g_2 = (72x_2^2 + 48x_2 + 72x_3^2 + 9)x_1 - 20x_2^4 - 48x_2^3 + (-104x_3^2 - 7)x_2^2 + (-48x_3^2 - 18)x_2 - 20x_3^4 + 9x_3^2$.

So the inputs for our algorithm are $\{f_1, f_2, f_3, f_4, f_5\}$ and $\{g_1, g_2\}$.
The first two executions are the computations of the saturation ideals $\langle f_1, f_2, f_3, f_4, f_5\rangle : \langle g_1\rangle^\infty$ and $\langle f_1, f_2, f_3, f_4, f_5\rangle : \langle g_2\rangle^\infty$ (**1** of **Algorithm**). The third execution is the computation of ideal intersection of the obtained saturation ideals (**2** of **Algorithm**). The last execution is the computation of $\{q_1, \dots, q_t\}$ (**3** of **Algorithm**). Each computation terminates immediately and we get a simple representation $V(\langle -x_1 - x_2^2 + x_3^2 + x_3, -4x_1^2 + 3x_1 - 5x_3^2 - 2x_3\rangle) \setminus V(x_3, x_2, x_1)$.

As is described in the previous sections, primary decomposition is a very heavy computation. The computer algebra system Singular [5] has a sophisticated fast implementation of primary decomposition. For the ideal `I=` $\langle f_1, f_2, f_3, f_4, f_5\rangle$, however, either of the following commands `primdecGTZ(I)` or `primdecSY(I)` does not terminate within one hour by our standard laptop computer which has a CPU Intel Core i5-4210U with 8GB memory running OS Ubuntu14.04. The computer algebra system Risa/Asir [4] also has a command `premadec` which is an excellent fast implementation of primary decomposition. It does not either terminate within one hour by the same computer.

```
[1855] hgr([-4*x1^3+(-4*x2^2+4*x3^2+4*x3-1)*x1^2+(-2*x2^2+2*x2+x3)*x1-x2^4+
2*x2^3+x3*x2^2+(-2*x3^2-2*x3)*x2+x3^4+x3^3,
-16*x1^4+12*x1^3+(8*x2-28*x3^2-12*x3+4)*x1^2+(5*x2^2-8*x2-2*x3^2-3*x3)*x1+
x2^4-2*x2^3+(-5*x3^2-3*x3)*x2^2+(12*x3^2+6*x3)*x2-6*x3^4-3*x3^3,
(-192*x2-576*x3^2-224*x3-2)*x1^3+((192*x3^2+96*x3+60)*x2+288*x3^4+288*x3^3-
122*x3^2-26*x3+13)*x1^2+(-30*x2^4-192*x2^3+(-408*x3^2-92*x3+10)*x2^2+
(72*x3^2+112*x3-26)*x2-210*x3^4-20*x3^3-22*x3^2+3*x3)*x1+20*x2^5+(30*x3^2+
10*x3+21)*x2^4+(224*x3^2+48*x3+70)*x2^3+(228*x3^4+124*x3^3-86*x3^2-37*x3)*
```

```
x2^2+(-4*x3^4-96*x3^3+70*x3^2-6*x3)*x2+102*x3^6+82*x3^5-35*x3^4+3*x3^3,
(2688*x2+8064*x3^2+3136*x3+388)*x1^3+((-2688*x3^2-1344*x3-1080)*x2-
4032*x3^4-4032*x3^3+988*x3^2+4*x3-137)*x1^2+(160*x2^4+2688*x2^3+(6232*x3^2+
1648*x3+30)*x2^2+(-528*x3^2-1328*x3+274)*x2+3400*x3^4+640*x3^3+308*x3^2-
87*x3)*x1+100*x2^6-40*x2^5+(-240*x3-169)*x2^4+(-3136*x3^2-912*x3-1070)*x2^3+
(-3612*x3^4-2256*x3^3+1124*x3^2+393*x3)*x2^2+(-184*x3^4+1104*x3^3-890*x3^2+
174*x3)*x2-1528*x3^6-1248*x3^5+445*x3^4-87*x3^3,
((576*x3^3+576*x3^2-172*x3-84)*x2+384*x3^3+576*x3^2+72*x3+72)*x1^3+((720*
x3^3+488*x3^2+12*x3-115)*x2+336*x3^3+192*x3^2-12*x3-18)*x1^2+((60*x3+20)*
x2^5+(184*x3+88)*x2^4+(456*x3^3+248*x3^2+20*x3+46)*x2^3+(160*x3^3+
112*x3^2+100*x3+140)*x2^2+(204*x3^5+164*x3^4-76*x3^3-172*x3^2-17*x3+20)*x2+
136*x3^5+184*x3^4+24*x3^3+84*x3^2-12*x3)*x1+(84*x3+33)*x2^5+(56*x3+38)*x2^4+
(408*x3^3+200*x3^2-41*x3-112)*x2^3+(-52*x3^3-128*x3^2-58*x3)*x2^2+(228*x3^5+
119*x3^4-113*x3^3-124*x3^2+24*x3)*x2+116*x3^5+38*x3^4-12*x3^3,
(4*x1^2+x1+x2^2-2*x2+x3^2)*y-1],[y,x1,x2,x3],[[0,1],[0,3]]);

[x1+x2^2-x3^2-x3,4*x1^2-3*x1+5*x3^2+2*x3,(3*x1-2*x2-3*x3^2-x3)*y-1]
0.001295sec(0.001433sec)

[1856] hgr([-4*x1^3+(-4*x2^2+4*x3^2+4*x3-1)*x1^2+(-2*x2^2+2*x2+x3)*x1-x2^4+
2*x2^3+x3*x2^2+(-2*x3^2-2*x3)*x2+x3^4+x3^3,
-16*x1^4+12*x1^3+(8*x2-28*x3^2-12*x3+4)*x1^2+(5*x2^2-8*x2-2*x3^2-3*x3)*x1+
x2^4-2*x2^3+(-5*x3^2-3*x3)*x2^2+(12*x3^2+6*x3)*x2-6*x3^4-3*x3^3,
(-192*x2-576*x3^2-224*x3-2)*x1^3+((192*x3^2+96*x3+60)*x2+288*x3^4+288*x3^3-
122*x3^2-26*x3+13)*x1^2+(-30*x2^4-192*x2^3+(-408*x3^2-92*x3+10)*x2^2+
(72*x3^2+112*x3-26)*x2-210*x3^4-20*x3^3-22*x3^2+3*x3)*x1+20*x2^5+(30*x3^2+
10*x3+21)*x2^4+(224*x3^2+48*x3+70)*x2^3+(228*x3^4+124*x3^3-86*x3^2-37*x3)*
x2^2+(-4*x3^4-96*x3^3+70*x3^2-6*x3)*x2+102*x3^6+82*x3^5-35*x3^4+3*x3^3,
(2688*x2+8064*x3^2+3136*x3+388)*x1^3+((-2688*x3^2-1344*x3-1080)*x2-
4032*x3^4-4032*x3^3+988*x3^2+4*x3-137)*x1^2+(160*x2^4+2688*x2^3+
(6232*x3^2+1648*x3+30)*x2^2+(-528*x3^2-1328*x3+274)*x2+3400*x3^4+640*x3^3+
308*x3^2-87*x3)*x1+100*x2^6-40*x2^5+(-240*x3-169)*x2^4+(-3136*x3^2-912*x3-
1070)*x2^3+(-3612*x3^4-2256*x3^3+1124*x3^2+393*x3)*x2^2+(-184*x3^4+
1104*x3^3-890*x3^2+174*x3)*x2-1528*x3^6-1248*x3^5+445*x3^4-87*x3^3,
((576*x3^3+576*x3^2-172*x3-84)*x2+384*x3^3+576*x3^2+72*x3+72)*x1^3+
((720*x3^3+488*x3^2+12*x3-115)*x2+336*x3^3+192*x3^2-12*x3-18)*x1^2+
((60*x3+20)*x2^5+(184*x3+88)*x2^4+(456*x3^3+248*x3^2+20*x3+46)*x2^3+
(160*x3^3+112*x3^2+100*x3+140)*x2^2+(204*x3^5+164*x3^4-76*x3^3-172*x3^2-
17*x3+20)*x2+136*x3^5+184*x3^4+24*x3^3+84*x3^2-12*x3)*x1+(84*x3+33)*x2^5+
(56*x3+38)*x2^4+(408*x3^3+200*x3^2-41*x3-112)*x2^3+(-52*x3^3-128*x3^2-
58*x3)*x2^2+(228*x3^5+119*x3^4-113*x3^3-124*x3^2+24*x3)*x2+116*x3^5+
38*x3^4-12*x3^3,
((72*x2^2+48*x2+72*x3^2+9)*x1-20*x2^4-48*x2^3+(-104*x3^2-7)*x2^2+
(-48*x3^2-18)*x2-20*x3^4+9*x3^2)*y-1],[y,x1,x2,x3],[[0,1],[0,3]]);
```

```
[x1+x2^2-x3^2-x3,4*x1^2-3*x1+5*x3^2+2*x3,
((96*x2+288*x3^2+112*x3-53)*x1+(-96*x3^2-48*x3-18)*x2-144*x3^4-144*x3^3+
97*x3^2+39*x3)*y-1]
0.003143sec(0.003063sec)

[1857] hgr([(x1+x2^2-x3^2-x3)*z1,(4*x1^2-3*x1+5*x3^2+2*x3)*z1,
(x1+x2^2-x3^2-x3)*(1-z1),(4*x1^2-3*x1+5*x3^2+2*x3)*(1-z1)],
[z1,x1,x2,x3],[[0,1],[0,3]]);

[-x1-x2^2+x3^2+x3,-4*x1^2+3*x1-5*x3^2-2*x3]
0.000563sec(0.0006039sec)

[1858] hgr(
[-x1-x2^2+x3^2+x3,-4*x1^2+3*x1-5*x3^2-2*x3,4*x1^2+x1+x2^2-2*x2+x3^2,
(72*x2^2+48*x2+72*x3^2+9)*x1-20*x2^4-48*x2^3+(-104*x3^2-7)*x2^2+
(-48*x3^2-18)*x2-20*x3^4+9*x3^2],[x1,x2,x3],0);

[x3,x2,x1]
0.000343sec(0.0005538sec)
```

4 Conclusion and Remarks

Our algorithm is given in a very naive form. There exist some more efficient techniques for the computation of saturation ideals or intersection ideals. Nevertheless, it is certainly more practical than the one using primary ideal decomposition. A computation of a saturation ideal corresponds to a polynomial division of a univariate polynomial ring, whereas a computation of primary ideal decomposition corresponds to a polynomial factorization. It is a natural consequence that our approach is more practical than the one using primary ideal decomposition.

Any algebraically constructible set is represented as a finite union of basic constructible sets, i.e. a special locally closed set $V(I)\setminus V(J)$ with a principal ideal J. (See Chapter 1 of [1] for example.) Therefore general locally closed sets do not draw much attention of most researchers of computer algebra. However, locally closed sets play an important role for achieving a canonical form of a comprehensive Gröbner system as is reported in [10]. Furthermore, the recent quantifier elimination algorithm introduced in [6] handles locally closed sets. The algorithm achieves the fastest ever real quantifier elimination program for first order formulas with many equalities. We can expect that our simplification algorithm will further improve this real quantifier elimination algorithm.

References

[1] Basu,S., Pollack,R. and Roy,M. Algorithms in Real Algebraic Geometry. Algorithms and Computation in Mathematics Volume 10, 2nd edn. Springer, 2006.

[2] Brunat, JM. and Montes, A. Computing the Canonical Representation of Constructible Sets. Mathematics in Computer Science, vol. 10-1, pp. 165-178, 2016.

[3] Cox, D., Little, J., O ' Shea, D.: Ideals, varieties and algorithms, 3rd edn. Springer, 2007.

[4] Noro, M. et al.: Risa/Asir — A computer algebra system for polynomial computations. http://www.math.kobe-u.ac.jp/Asir/asir.html (2016).

[5] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR 4-0-2 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2016).

[6] Fukasaku, R.,Inoue, S. and Sato, Y. On QE Algorithms over an Algebraically Closed Field based on Comprehensive Gröbner Systems. Mathematics in Computer Science, vol. 9-3, pp. 267-281, 2015.

[7] Fukasaku, R., Iwane, H. and Sato, Y. Real Quantifier Elimination by Computation of Comprehensive Gröbner Systems. Proceedings of International Symposium on Symbolic and Algebraic Computation, pp. 173-180, ACM, 2015.

[8] Nabeshima, K. Stability Conditions of Monomial Bases and Comprehensive Gröbner systems. Lecture Notes in Computer Science, Vol. 7442, pp. 248-259, Springer, 2012.

[9] Sato, Y. and Fukasaku, R. Detecting unnecessary assumptions of elementary geometry problems by CAS. Proceedings of the 20th Asian Technology Conference in Mathematics, pp. 316-325, 2015.

[10] Suzuki, A. and Sato, Y. An Alternative Approach to Comprehensive Gröbner Bases. JOURNAL OF SYMBOLIC COMPUTATION, Vol. 34 3-4, pp. 649-667, 2003.