3 Computations

Gröbner basis computation is one of the main practical tools for solving systems of polynomial equations and computing the images of algebraic varieties under projections or rational maps.

3.0 Buchberger's Algorithm

How does one find or construct a Gröbner basis? We describe a method for transforming a generator set of a polynomial ideal into a Gröbner basis. This procedure is a common generalization of the Euclidean division algorithm and the row-reduction algorithm from linear algebra.

3.0.0 Algorithm (Buchberger)**.**

input: a monomial order on the ring $S := \mathbb{K}[x_1, x_2, \dots, x_n]$ and
    generators $g_1, g_2, \dots, g_m$ for an ideal in S
output: a Gröbner basis for the ideal $\langle g_1, g_2 \dots, g_m \rangle$

Set $\mathbf{G} := [g_1 \;\; g_2 \;\; \cdots \;\; g_m]$.
Set $\mathcal{P} := \{(g_j, g_k) \mid 1 \leqslant j < k \leqslant m\}$.
While $\mathcal{P} \neq \varnothing$ do
  Choose $(g_j, g_k) \in \mathcal{P}$.
  Set $\mathcal{P} := \mathcal{P} \setminus \{(g_j, g_k)\}$.
  Set $h := \operatorname{spoly}(g_j, g_k) \,\%\, \mathbf{G}$.
  If $h \neq 0$ then
    Set $\mathcal{P} := \mathcal{P} \cup \{(g, h) \mid g$ appears in a column of $\mathbf{G}\}$.
    Set $\mathbf{G} := [\mathbf{G} \;\; h]$.
Return the columns of $\mathbf{G}$.

How one chooses the pairs $(g_j, g_k) \in \mathcal{P}$ can have a dramatic effect on the speed of the algorithm.

Proof of correctness. The Buchberger Criterion 2.2.2 shows that the output is a Gröbner basis. The algorithm terminates because the ring S is noetherian and each step which adds an h creates a larger ideal:

$$\langle \operatorname{LT}(g_1), \operatorname{LT}(g_2), \dots, \operatorname{LT}(g_m) \rangle \subset \langle \operatorname{LT}(g_1), \operatorname{LT}(g_2), \dots, \operatorname{LT}(g_m), \operatorname{LT}(h) \rangle \,. \quad \square$$

Worst-case analysis shows that the computation of Gröbner bases can be very expensive. The degrees of all the polynomials occurring during the Buchberger algorithm are bounded by a function of the form $O\big((nd)^{(n+1)2^{n+1}}\big)$ where d is the maximum of the degrees of the input polynomials and n is the number of variables. Despite this, Gröbner bases are often computable in practice.

3.0.1 Problem. Compute a Gröbner basis of the ideal $\langle x^2 - y, x^3 - z \rangle$ in the polynomial ring $\mathbb{Q}[x, y, z]$ under the lexicographic order.

Solution. Set $g_1 := \underline{x^2} - y$, $g_2 := \underline{x^3} - z$, and $I := \langle g_1, g_2 \rangle$. We have

$$\operatorname{spoly}(g_1, g_2) = x\, g_1 - g_2 = -\underline{xy} + z \,.$$

Its leading term is not contained in the ideal $\langle \mathrm{LM}(g_1), \mathrm{LM}(g_2)\rangle = \langle x^2\rangle$, so we add $g_3 := \underline{xy} - z$ to our generating set $\mathbf{G} = [g_1 \;\; g_2 \;\; g_3]$. We also have $\mathrm{spoly}(g_1, g_3) = y\, g_1 - x g_3 = \underline{xz} - y^2$. Again, its leading term is not in $\langle \mathrm{LM}(g_1), \mathrm{LM}(g_2), \mathrm{LM}(g_3)\rangle = \langle x^2, xy\rangle$, so we add $g_4 := \underline{xz} - y^2$ to our generating set $\mathbf{G} = [g_1 \;\; g_2 \;\; g_3 \;\; g_4]$. Continuing, we obtain

$$\begin{aligned}
\mathrm{spoly}(g_2, g_3) &= y\, g_2 - x^2\, g_3 = \underline{x^2 z} - yz = z\, g_1 \\
\mathrm{spoly}(g_1, g_4) &= z\, g_1 - x\, g_4 = \underline{xy^2} - yz = y\, g_3 \\
\mathrm{spoly}(g_2, g_4) &= z\, g_2 - x^2\, g_4 = \underline{x^2 y^2} - z^2 = y^2\, g_1 + (y^3 - z^2)\,;
\end{aligned}$$

for all three of these S-polynomials, the remainder on division by $\mathbf{G}$ is zero. Since $\mathrm{LT}(\underline{y^3} - z^2) = y^3$ is not contained in the ideal

$$\langle \mathrm{LM}(g_1), \mathrm{LM}(g_2), \mathrm{LM}(g_3), \mathrm{LM}(g_4)\rangle = \langle x^2, xy, xz\rangle \ ,$$

we add $g_5 := \underline{y^3} - z^2$ to our generating set. Lastly, we have

$$\begin{aligned}
\mathrm{spoly}(g_3, g_4) &= z\, g_3 - y\, g_4 = \underline{y^3} - z^2 = g_5 \\
\mathrm{spoly}(g_1, g_5) &= y^3\, g_1 - x^2\, g_5 = \underline{x^2 z^2} - y^3 = z^2\, g_1 - y\, g_5 \\
\mathrm{spoly}(g_2, g_5) &= y^3\, g_2 - x^3\, g_5 = \underline{x^3 z^2} - y^3 z = z^2\, g_2 + z\, g_5 \\
\mathrm{spoly}(g_3, g_5) &= y^2\, g_3 - x\, g_5 = \underline{xz^2} - y^2 z = z\, g_4 \\
\mathrm{spoly}(g_4, g_5) &= y^3\, g_4 - xz\, g_5 = \underline{xz^3} - y^5 = z^2\, g_4 - y^2\, g_5\,.
\end{aligned}$$

Thus, the polynomials $x^2 - y, x^3 - z, xy - z, xz - y^2, y^3 - z^2$ from a Gröbner basis for the ideal $\langle x^2 - y, x^3 - z\rangle$. ☐

Since $g_2 = x\, g_1 + g_3$, we can omit g_2 to obtain a smaller Gröbner basis.

3.0.2 Definition. A Gröbner basis $g_1, g_2, \dots, g_m$ is *minimal* if $g_k \neq 0$, for all $1 \leqslant k \leqslant m$, and the relation $j \neq k$ implies that $\mathrm{LM}(g_j)$ does not divide $\mathrm{LM}(g_k)$. Moreover, this Gröbner basis is *reduced* if it is minimal, $\mathrm{LC}(g_k) = 1$, and none of the monomials in $g_k - \mathrm{LT}(g_k)$ belong to the ideal $\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \dots, \mathrm{LT}(g_m)\rangle$, for all $1 \leqslant k \leqslant m$.

3.0.3 Proposition. *For any monomial order on the polynomial ring S, there exists a unique reduced Gröbner basis for every ideal in S.*

Sketch of proof. Let $g_1, g_2, \dots, g_m$ be a Gröbner basis of the ideal I.

(existence) Suppose that $\mathrm{LT}(g_j)$ is divisible by $\mathrm{LT}(g_k)$. It follows that $\mathrm{LT}(I) = \big\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \dots, \mathrm{LT}(g_{j-1}), \mathrm{LT}(g_{j+1}), \dots, \mathrm{LT}(g_m)\big\rangle$. Since the remainder of

$$\mathrm{spoly}(g_j, g_k) = \frac{1}{\mathrm{LC}(g_j)}\, g_j - \frac{\mathrm{LM}(g_j)}{\mathrm{LT}(g_k)}\, g_k$$

on division by $g_1, g_2, \cdots, g_{j-1}, g_{j+1}, \dots, g_m$ is zero, we deduce that $\big\langle g_1, g_2, \cdots, g_{j-1}, g_{j+1}, \dots, g_m\big\rangle = I$. We obtain a small Gröbner basis for I by omitting g_j. Therefore, we may assume without loss of generality that our Gröbner basis is minimal.

For some $1 \leqslant j \leqslant m$, set

$$r_j := g_j \,\%\, [g_1 \;\; g_2 \;\; \cdots \;\; g_{j-1} \;\; g_{j+1} \;\; \cdots \;\; g_m]^{\mathsf{T}} .$$

Since $\operatorname{LT}(g_j) \notin \langle \operatorname{LT}(g_1), \operatorname{LT}(g_2), \dots, \operatorname{LT}(g_{j-1}), \operatorname{LT}(g_{j+1}), \dots, \operatorname{LT}(g_m) \rangle$, we see that $\operatorname{LT}(g_j) = \operatorname{LT}(r_j)$. Thus, $g_1, g_2, \dots, g_{j-1}, r_j, g_{j+1}, \dots, g_m$ is a Gröbner basis for I. Because "being reduced" only depends on the leading monomials (which this process doesn't alter), we may repeat this process until we obtain a reduced Gröbner basis.

(uniqueness) Suppose that $g_1, g_2, \dots, g_m$ and $f_1, f_2, \dots, f_m$ are reduced Gröbner bases for I. For any $1 \leqslant j \leqslant m$, there exists an index k such that $\operatorname{LM}(g_j) = \operatorname{LM}(f_k)$. Since $g_j - f_k \in I$, we have

$$(g_j - f_k) \,\%\, [g_1 \;\; g_2 \;\; \cdots \;\; g_m]^{\mathsf{T}} = 0 .$$

The leading terms cancel and the remaining terms are divisible by none of the monomials in $\operatorname{LT}(I)$, so we must have $g_j - f_k = 0$. □

3.0.4 Examples. The polynomials $x^2 - y, xy - z, xz - y^2, y^3 - z^2$ form the reduced Gröbner basis with respect to $>_{\text{lex}}$. However, the polynomials $x^2 - y, xy - z, y^2 - xz$ form the reduced Gröbner basis for the same ideal with respect to $>_{\text{grevlex}}$. ◇

3.1 Macaulay2

Developed by Daniel Grayson and Michael Stillman, *Macaulay2* is a open-source software system devoted to supporting research in algebraic geometry and commutative algebra. Documentation can be found at `www.math.uiuc.edu/Macaulay2/`. A convenient online version can be found at `www.unimelb-macaulay2.cloud.edu.au/`.

Basic numerical operations are quite intuitive.

```
Macaulay2, version 1.21
with packages: ConwayPolynomials, Elimination, IntegralClosure, InverseSystems,
               Isomorphism, LLLBases, MinimalPrimes, OnlineLookup,
               PrimaryDecomposition, ReesAlgebra, Saturation, TangentCone

i1 : 2+2

o1 = 4

i2 : 1*2*3*4

o2 = 24

i3 : 2^199

o3 = 803469022129495137770981046170581301261101496891396417650688

i4 : 42!

o4 = 1405006117752879898543142606244511569936384000000000

i5 : 1;2;3*4

o7 = 12

i8 : 4*5

o8 = 20
```

```
i9 : 4 / 2
o9 = 2
o9 : QQ
i10 : 4 // 2
o10 = 2
i11 : 4 % 2
o11 = 0
i12 : 4 % 3
o12 = 1
i13 : 4 // 3
o13 = 1
i14 : oo
o14 = 1
i15 : o5+1
o15 = 2
```

We can also make functions in *Macaulay2*.

```
i16 : f = i -> i^3
o16 = f
o16 : FunctionClosure
i17 : f 5
o17 = 125
i18 : g = (x,y) -> x*y
o18 = g
o18 : FunctionClosure
i19 : g(6,9)
o19 = 54
```

To work with polynomials, we must first define the ambient ring.

```
i20 : S = ZZ/5[x,y,z]
o20 = S
o20 : PolynomialRing
i21 : (x+y)^5
       5    5
o21 = x  + y
o21 : S
i22 : 1_S
o22 = 1
o22 : S
i23 : 0_S
o23 = 0
o23 : S
i24 : numgens S
o24 = 3
i25 : gens S
o25 = {x, y, z}
o25 : List
i26 : vars S
o26 = | x y z |
               1        3
o26 : Matrix S  <--- S
```

```
i27 : coefficientRing S

      ZZ
o27 = --
       5

o27 : QuotientRing
i28 : random(3, S)

         3    2       2    3    2                  2      2     3
o28 = - x  - x y - x*y  + y  + x z - 2x*y*z + x*z  - 2y*z  + 2z
o28 : S
i29 : basis(2, S)
o29 = | x2 xy xz y2 yz z2 |

              1       6
o29 : Matrix S  <--- S
```

Every polynomial ring in *Macaulay2* is equipped with a monomial order.

```
i30 : S = ZZ/101[a,b,c]
o30 = S
o30 : PolynomialRing
i31 : (a+b+c+1)^3

       3     2         2    3     2                2         2       2    3     2
o31 = a  + 3a b + 3a*b  + b  + 3a c + 6a*b*c + 3b c + 3a*c  + 3b*c  + c  + 3a  +
      ------------------------------------------------------------------------------
                   2                     2
      6a*b + 3b  + 6a*c + 6b*c + 3c  + 3a + 3b + 3c + 1
o31 : S
```

Explicit comparison of monomials with respect to the chosen ordering is possible.

```
i32 : b^2 > a*c
o32 = true
```

The comparison operator ? returns a symbol indicating the result of the comparison: the convention is that the larger monomials are printed first (leftmost).

```
i33 : b^2 ? a*c
o33 = >
o33 : Keyword
```

The monomial ordering is also used when sorting lists with sort.

```
i34 : sort { 1_S, a, a^2, b, b^2, a*b, a^3, b^3}

                   2         2   3   3
o34 = {1, b, a, b , a*b, a , b , a }
o34 : List
```

Describe the default monomial ordering used in *Macaulay2*. The next ring uses optional argument `MonomialOrder` to specify lexicographic ordering.

```
i35 : S = ZZ/101[a,b,c, MonomialOrder => Lex];
i36 : (a+b+c+1)^3

       3     2       2       2        2                       2                  3
o36 = a  + 3a b + 3a c + 3a  + 3a*b  + 6a*b*c + 6a*b + 3a*c  + 6a*c + 3a + b  +
      ------------------------------------------------------------------------------
        2       2        2                  3     2
      3b c + 3b  + 3b*c  + 6b*c + 3b + c  + 3c  + 3c + 1
o36 : S
```

How would you describe the following monomial orders?

```
i37 : S = ZZ/101[a,b,c, MonomialOrder => Eliminate 2];
```

```
i38 : (a+b+c+1)^3

       3     2         2    3     2                2      2             2       2
o38 = a  + 3a b + 3a*b  + b  + 3a c + 6a*b*c + 3b c + 3a  + 6a*b + 3b  + 3a*c  +
      ------------------------------------------------------------------------
           2                              3     2
      3b*c  + 6a*c + 6b*c + 3a + 3b + c  + 3c  + 3c + 1
o38 : S
i39 : S = ZZ/101[a,b,c, MonomialOrder => ProductOrder{1,2}];
i40 : (a+b+c+1)^3

       3     2       2       2        2                 2                  3
o40 = a  + 3a b + 3a c + 3a  + 3a*b  + 6a*b*c + 3a*c  + 6a*b + 6a*c + 3a + b  +
      ------------------------------------------------------------------------
        2          2    3      2             2
      3b c + 3b*c  + c  + 3b  + 6b*c + 3c  + 3b + 3c + 1
o40 : S
i41 : S = ZZ/101[a,b,c, Degrees => {1,2,3}];
i42 : (a+b+c+1)^3

       3       2     2        2    3                2        2     2            2
o42 = c  + 3b*c  + 3b c + 3a*c  + b  + 6a*b*c + 3c  + 3a*b  + 3a c + 6b*c + 3a b
      ------------------------------------------------------------------------
          2           3                  2
      + 3b  + 6a*c + a  + 6a*b + 3c + 3a  + 3b + 3a + 1
o42 : S
```

The division algorithm discussed in class can be implemented in *Macaulay2* as follows:

```
i43 : division = (f, G) -> (
          S := ring f;
          p := f;
          r := 0_S;
          m := #G;
          Q := new MutableHashTable;
          for j from 0 to m-1 do Q#j = 0_S;
          while p != 0 do (
              i := 0;
              while i < m and leadTerm(p) % leadTerm(G#i) != 0 do i = i+1;
              if i < m then (
                  Q#i = Q#i + (leadTerm(p) // leadTerm(G#i));
                  p = p - (leadTerm(p) // leadTerm(G#i) * G#i)
                  )
              else (
                  r = r + leadTerm(p);
                  p = p - leadTerm(p)
                  )
              );
          L := apply(m, j -> Q#j);
          (r, L)
          )
o43 = division
o43 : FunctionClosure
```

What does the following input do?

```
i44 : f = x^2*y

       2
o44 = x y

      ZZ
o44 : --[x..z]
       5
i45 : G1 = {x*y-x, x^2-x}

                 2
o45 = {x*y - x, x  - x}
o45 : List
```

```
i46 : G2 = {x^2-y, x*y-x}
          2
o46 = {x  - y, x*y - x}
o46 : List
i47 : division(f, G1)
o47 = (x, {x, 1})
o47 : Sequence
i48 : f % matrix{G1}, f // matrix{G1}
o48 = (x, {2} | x |)
          {2} | 1 |
o48 : Sequence
i49 : gens gb ideal G1
o49 = | xy-x x2-x |
               ZZ        1       ZZ        2
o49 : Matrix (--[x..z])  <--- (--[x..z])
                5                5
i50 : division(f, G2)
          2
o50 = (y , {y, 0})
o50 : Sequence
i51 : f % matrix{G2}, f // matrix{G2}
o51 = (y, {2} | 1 |)
          {2} | x |
o51 : Sequence
i52 : gens gb ideal G2
o52 = | y2-y xy-x x2-y |
               ZZ        1       ZZ        3
o52 : Matrix (--[x..z])  <--- (--[x..z])
                5                5
```

The next example illustrates how the monomial order can affect the length and complexity of a Gröbner basis computation.

```
i53 : S = QQ[x,y,z];
i54 : I = ideal(x^7+y^6+z^5-1, x^4+y^3+z^2-1);
o54 : Ideal of S
i55 : time gens gb I;
     -- used 0.000455786 seconds
              1      4
o55 : Matrix S  <--- S
i56 : numColumns oo
o56 = 4
i57 : S’ = QQ[x,y,z, MonomialOrder => Lex];
i58 : I’ = ideal(x^7+y^6+z^5-1, x^4+y^3+z^2-1);
o58 : Ideal of S’
i59 : time gens gb I’;
     -- used 0.0333673 seconds
               1       9
o59 : Matrix S’  <--- S’
i60 : numColumns oo
o60 = 9
```

Which affine subvarieties do the following ideals define?

```
i61 : S = QQ[x,y,z];
i62 : I = ideal(x*y, x*z)
o62 = ideal (x*y, x*z)
o62 : Ideal of S
i63 : decompose(I)
o63 = {ideal x, ideal (z, y)}
o63 : List
i64 : I == intersect(oo)
o64 = true
i65 : clearAll
i66 : n = 4
o66 = 4
i67 : S = QQ[x_1..x_n];
i68 : M = matrix table(n, n, (j,k) -> S_j^k)
o68 = | 1 x_1 x_1^2 x_1^3 |
      | 1 x_2 x_2^2 x_2^3 |
      | 1 x_3 x_3^2 x_3^3 |
      | 1 x_4 x_4^2 x_4^3 |
                4       4
o68 : Matrix S  <--- S
i69 : factor det M
o69 = (x  - x )(x  - x )(x  - x )(x  - x )(x  - x )(x  - x )
        3    4   2    4   2    3   1    4   1    3   1    2
o69 : Expression of class Product
i70 : S = QQ[a..i];
i71 : M = genericMatrix(S,a,3,3)
o71 = | a d g |
      | b e h |
      | c f i |
                3       3
o71 : Matrix S  <--- S
i72 : I = ideal det M
o72 = ideal(- c*e*g + b*f*g + c*d*h - a*f*h - b*d*i + a*e*i)
o72 : Ideal of S
i73 : J = minors(2, M);
o73 : Ideal of S
i74 : mingens J
o74 = | fh-ei ch-bi fg-di eg-dh cg-ai bg-ah ce-bf cd-af bd-ae |
                1       9
o74 : Matrix S  <--- S
i75 : S = QQ[t,a..i];
i76 : M = genericMatrix(S,a,3,3)
o76 = | a d g |
      | b e h |
      | c f i |
                3       3
o76 : Matrix S  <--- S
i77 : Mt = t*id_(S^3) - M
o77 = | t-a -d  -g  |
      | -b  t-e -h  |
      | -c  -f  t-i |
                3       3
o77 : Matrix S  <--- S
```

```
i78 : I = ideal substitute(
          contract(matrix{{t^2, t,1}}, det(Mt)),
          {t => 0_S});
o78 : Ideal of S
i79 : transpose gens I
O79 = {-1} | -a-e-i                    |
      {-2} | -bd+ae-cg-fh+ai+ei        |
      {-3} | ceg-bfg-cdh+afh+bdi-aei |
                3      1
o79 : Matrix S  <--- S
```

3.2 Solving Systems

How do Gröbner bases help with finding solutions to a system of polynomial equations?

3.2.0 Problem. Determine all complex solutions to the following system of equations: $x^2 + y + z = 1$, $x + y^2 + z = 1$, $x + y + z^2 = 1$.

Solution. Set $I := \langle x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 \rangle$. The reduced Gröbner basis of I with respect to $>_{\text{lex}}$ is

$$z^6 - 4z^4 + 4z^3 - z^2, yz^2 + 0.5z^4 - 0.5z^2, y^2 - y - z^2 + z, x + y^2 + z - 1\,.$$

Since $z^6 - 4z^4 + 4z^3 - z^2 = z^2(z-1)^2(z^2 + 2z - 1)$, the possible z's are 0, 1 and $-1 \pm \sqrt{2}$. Substituting these values into $y^2 - y - z^2 + z = 0$ and $yz^2 + 0.5z^4 - 0.5z^2 = 0$, we can determine the possible y's. Similarly, the equation $x + y^2 + z = 1$ gives the corresponding x's. In this way, one checks that the equations have exactly five solutions:

$$\begin{array}{lll} \big(-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}\big)\,, & (1,0,0)\,, & (0,0,1)\,. \\ \big(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}\big)\,, & (0,1,0)\,, & \end{array} \qquad \square$$

Why could we find these solutions? There are two key features.

(elimination) We could find a consequence of the given polynomial equations that involved only one variable.

(extension) Having solved the equation in one variable, we could extend these solutions to the given polynomial equations.

We first focus on elimination theory.

3.2.1 Definition. An *elimination order* for the variables $x_1, x_2, \dots, x_n$ on the ring $R := \mathbb{K}[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$ is a monomial order such that any polynomial in R, whose leading term belongs to the subring $\mathbb{K}[y_1, y_2, \dots, y_m]$, is itself contained in $\mathbb{K}[y_1, y_2, \dots, y_m]$.

3.2.2 Example. Lexicographic order on R satisfying $x_i > y_j$, for all i and j, is an elimination order for the variables $x_1, x_2, \dots, x_n$. ◇

3.2.3 Example. Fix monomials orders $>_x$ and $>_y$ on $\mathbb{K}[x_1, x_2, \dots, x_n]$ and $\mathbb{K}[y_1, y_2, \dots, y_m]$ respectively. The *product order* on the larger polynomial ring $\mathbb{K}[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$, defined by declaring that $x^a y^b > x^u y^v$ whenever $x^a >_x x^u$ or $x^a = x^u$ and $y^b >_y y^v$, is an elimination order. ◇

3.2.4 Theorem (Elimination). *Fix an elimination order $>$ on the ring $R := \mathbb{K}[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m]$ for the variables $x_1, x_2, \dots, x_n$. For any Gröbner basis of an ideal I in R with respect to $>$, the subset lying in $\mathbb{K}[y_1, y_2, \dots, y_m]$ forms a Gröbner basis for the ideal $I \cap \mathbb{K}[y_1, y_2, \dots, y_m]$ in the subring $\mathbb{K}[y_1, y_2, \dots, y_m]$.*

The monomial order on the subring $\mathbb{K}[y_1, y_2, \dots, y_m]$ is inherited from the elimination order on $\mathbb{K}[y_1, y_2, \dots, y_m]$.

Proof. Let $g_1, g_2, \dots, g_\ell \in R$ be a Gröbner basis of the ideal I relative to given elimination order $>$. Set $J := I \cap \mathbb{K}[y_1, y_2, \dots, y_m]$ and, for some $1 \leqslant k \leqslant \ell$, let $g_k, g_{k+1}, \dots, g_\ell$ be the elements in the Gröbner basis lying in the subring $\mathbb{K}[y_1, y_2, \dots, y_m]$. Since $g_k, g_{k+1}, \dots, g_\ell \in J$, it is enough to show that $\operatorname{LT}(J) \subseteq \langle \operatorname{LT}(g_k), \operatorname{LT}(g_{k+1}), \dots, \operatorname{LT}(g_\ell) \rangle$.

We need only prove that the leading term $\operatorname{LT}(f)$, for any $f \in J$, is divisible by $\operatorname{LT}(g_j)$ for some $k \leqslant j \leqslant \ell$. A polynomial $f \in J$ lies in I, so its leading term $\operatorname{LT}(f)$ is divisible by $\operatorname{LT}(g_j)$ for some $1 \leqslant j \leqslant \ell$. As $f \in J$, the leading term $\operatorname{LT}(g_j)$ lies in the subring $\mathbb{K}[y_1, y_2, \dots, y_m]$. From the defining property of an elimination order, we see that $g_j \in \mathbb{K}[y_1, y_2, \dots, y_m]$, so we have $k \leqslant j \leqslant \ell$. □

The ideal $I \cap \mathbb{K}[y_1, y_2, \dots, y_m]$ has a geometric interpretation.

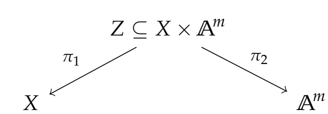
3.2.5 Theorem (Closure). *Let $\mathbb{K}$ be an algebraically closed field and let $X \subseteq \mathbb{A}^{n+m}$ be an affine subvariety with $I := \operatorname{I}(X)$. For the projection map $\pi \colon \mathbb{A}^{n+m} \to \mathbb{A}^m$ defined by*

$$(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m) \mapsto (y_1, y_2, \dots, y_m)\,,$$

we have $\overline{\pi(X)} = \operatorname{V}(I \cap \mathbb{K}[y_1, y_2, \dots, y_m])$. ■

To utilize the algebraically closed hypothesis, we need another result, so we postpone presenting the proof.

3.2.6 Definition. Let X be an affine subvariety in $\mathbb{A}^n$. The *graph* Z of a polynomial map $\rho \colon X \to \mathbb{A}^m$ is the locus $\{(a, \rho(a)) \mid a \in \mathbb{A}^n\}$ in $X \times \mathbb{A}^m$. The graph Z comes with two maps $\pi_1 \colon Z \to X$ and $\pi_2 \colon Z \to \mathbb{A}^m$ given by $(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m) \mapsto (x_1, x_2, \dots, x_n)$ and $(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m) \mapsto (y_1, y_2, \dots, y_m)$ respectively. The map π_1 is invertible and $\pi_2(Z) = \rho(X)$.



3.2.7 Proposition (Graphs as subvarieties). *For any polynomial map $\rho \colon X \subseteq \mathbb{A}^n \to \mathbb{A}^m$ with graph $Z \subseteq \mathbb{A}^{n+m}$, we have $Z = \operatorname{V}(\operatorname{I}(Z))$ and*

$$\operatorname{I}(Z) = \pi_1^*(\operatorname{I}(X)) + \langle y_1 - \rho_1, y_2 - \rho_2, \dots, y_m - \rho_m \rangle\;.$$

For any $f \in \mathbb{K}[x_1, x_2, \dots, x_n]$, let $\pi_1^*(f)$ denote the same polynomial regarded as an element in the larger ring $\mathbb{K}[x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n]$.

Proof. The inclusions $Z \subseteq X \times \mathbb{A}^m \subseteq \mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$ imply that $\pi_1^*(\operatorname{I}(X)) \subseteq \operatorname{I}(Z)$. For any point $a := (a_1, a_2, \dots, a_n) \in X$, we have

$$\rho(a) = \big(\rho_1(a_1, a_2, \dots, a_n), \rho_2(a_1, a_2, \dots, a_n), , \dots, \rho_m(a_1, a_2, \dots, a_n)\big)\,,$$

so the polynomial $y_j - \rho_j$ vanishes at $\big(a, \rho(a)\big)$ for all $1 \leqslant j \leqslant m$. Hence, we have $\mathrm{I}(Z) \supseteq \pi_1^*\big(\mathrm{I}(X)\big) + \langle y_1 - \rho_1, y_2 - \rho_2, \ldots, y_m - \rho_m \rangle$.

The Buchberger criteria establish that the polynomial generators $y_1 - \rho_1, y_2 - \rho_2, \ldots, y_m - \rho_m$ form a Gröbner basis with respect to the lexicographic order where

$$y_1 > y_2 > \cdots > y_m > x_1 > x_2 > \cdots > x_n \,.$$

The remainders modulo this ideal lie in the subring $\mathbb{K}[x_1, x_2, \ldots, x_n]$. For any polynomial f in the subring $\mathbb{K}[x_1, x_2, \ldots, x_n]$ that vanishes on Z, we deduce that $f \in \mathrm{I}(X)$. Therefore, we have the opposite inclusion $\mathrm{I}(Z) \subseteq \pi_1^*\big(\mathrm{I}(X)\big) + \langle y_1 - \rho_1, y_2 - \rho_2, \ldots, y_m - \rho_m \rangle$.

Finally, suppose that $(a, b) \in \mathrm{V}\big(\mathrm{I}(Z)\big)$. Since $\pi_1^*\big(\mathrm{I}(X)\big) \subseteq \mathrm{I}(Z)$, it follows that $\mathrm{V}\big(\mathrm{I}(Z)\big) \subseteq \pi_1^{-1}(X)$ and $a \in X$. Moreover, the equations $y_j = \rho_j$, for all $1 \leqslant j \leqslant m$, imply that $b = \rho(a)$ and $(a, b) \in Z$. □