Leture 1: Division Algorithm, Groebner basis, Monomial Ideals

James Carlson

CIMAT Lectures

February 7, 2008

Division algorithm

In one variable: given f, g, there exist a, r such that

$$f = ag + r$$

where $r = 0$ or $\deg r < \deg g$. How? Long division!

There is a division algorithm for more than one variable. But there are new requirements:

A monomial order is a total order on monomials compatible with multiplication. $M > N$ implies $AM > AN$ for all A.

Example: the lex order: $M > N$ if the first nonzero entry in $exponents(M) - exponents(N) > 0$. Thus $x^2y >_{lex} xy^9$.

Let $LT(f)$ be the leading term of f, e.g., $LT(7x^2y + 11xy^9) = 7x^2y$.

Division algorithm in several variables

Given f and $g_1, \ldots, g_s$ (the divisors), there are $a_1, \ldots, a_s$ (the quotients) and r (the remainder), such that

$$f = a_1 g_1 + \cdots a_s g_s + r$$

Moreover, no leading term of r is divisible by a leading term of the g_i.

Finally, $multideg(f) \geq multideg(a_i g_i)$, where $multideg(h)$ is the exponent of the leading term.

E.g. $multideg(7x^2y + 11xy^9) = (2, 1)$

How do we divide f by $g_1, g_2, \ldots$?

Long division!

Long division: $x^5 + y^5$ by $x^3 + y^2$ and $y^2 + 1$

```
a1:  x^2              a2:   -x^2 + y^3 - y
g1:  x^3 + y^2         |     x^5 + y^5
g2:  y^2 + 1           |     x^5 + x^2y^2
-----------------            -------------
r:   x^2                     -x^2y^2 + y^5
                             -x^2y^2 - x^2
                             -------------
                             x^2 + y^5
                             -------------
                             y^5
                             y^5 + y^3
                             -------------
                             -y^3
                             -y^3 - y
                             ------------
                             y
```

The result

$$x^5+y^5 = a_1g_1+a_2g_2+r = (x^2)(x^3+y^2)+(-x^2+y^3-y)(y^2+1)+(x^2+y)$$

Pseudocode

```
Input: g1, ..., gs, g;   Output: a1, ..., as, r
a1, ..., as = 0, ..., 0
r , p = 0, f
WHILE p <> 0:
    i = 1
    WHILE I <= s AND divisionoccured = false:
        IF LT(gi) divides LT(p):
            ai = ai + LT(p)/LT(gi)
            p = p - (LT(p)/LT(gi))gi
            divisionoccured = true
        ELSE:
            i = i + 1
    IF divisionoccured = false:
        r = r + LT(p)
        p = p - LT(p)
```

Sage

```
def div(f,g):
    n = len(g)
    p, r, a = f, 0,  [0 for x in range(0,n)]
    while p != 0:
        i, divisionoccured = 0, False
        while i < n and divisionoccured == False:
            if divides( LT(g[i]), LT(p) ):
                a[i] = a[i] + LT(p)//LT(g[i])
                p = p - (LT(p)//LT(g[i]))*g[i]
                divisionoccured = True
            else:
                i = i + 1
        if divisionoccured == False:
            r = r + LT(p)
            p = p - LT(p)
    return a, r
```

Pathologies

1. f can be in ideal generated by $G = g_1, \ldots, g_n$, but it is possible that $div(f, G) \neq 0$.
2. The remainder can depend on the order of the divisors.

```
sage: R.<x,y> = PolynomialRing(QQ)
sage: G = [x^2 + 1, x*y^2 + y]
sage: f = x*y - y^2
sage: f in ideal(G)
True
sage: div(f,G)
([0, 0], x*y - y^2)
```

Groebner bases

```
sage: R.<x,y> = PolynomialRing(QQ, order = 'lex')
sage: f = x*y - y^2
sage: I = ideal( x^2 + 1, x*y^2 + y )
sage: G = I.groebner_basis(); G
[y^3 + y, x*y - y^2, x^2 + 1]
sage: div(f,G)
([0, 1, 0], 0)
```

Theorem

A polynomial f is in $ideal(G)$ if and only if $div(f, G) = 0$, provided that G is a Groebner basis.

What is a Groebner basis? Do they exist? How do we construct them?

Note leading forms: $x^2 > xy^2 > y^3$

Definitions

Ideal of leading forms: $\langle LT(I) \rangle =$ ideal generated by all leading forms of elements of I.

BB is a Groebner basis for $I = ideal(B)$ if the leading forms of the BB_i generate the ideal of leading forms of I.

Caution: In general, $\langle LT(ideal(B)) \rangle$ is not be the same as $ideal(LT(B_1), \ldots, LT(B_n))$.

E.g. $[xy - y^2, x^2 + 1] \neq [y^3 + y, xy - y^2, x^2 + 1]$

S polynomials

Let $f = x^2 + 1$, $g = xy^2 + y$. Let's try to cook up an expression $S = Af + Bg$ in which the terms coming from $LT(f) = x^2$ and $LT(g) = xy^2$ cancel:

$$S = y^2 f - xg = (x^2y^2 + y^2) - (x^2y^2 + xy) = -xy + y^2$$

Note: (1) $LT(S) = -xy$ is in $\langle LT(I) \rangle$. (2) $LT(S) \neq x^2, xy^2$ (3) We have discovered a new element of the ideal of leading forms: $x^2 > xy^2 > xy$.

In general we must take $S(f, g)$ % B.

Definition: Let $LCM = LCM(LM(f), LM(g))$

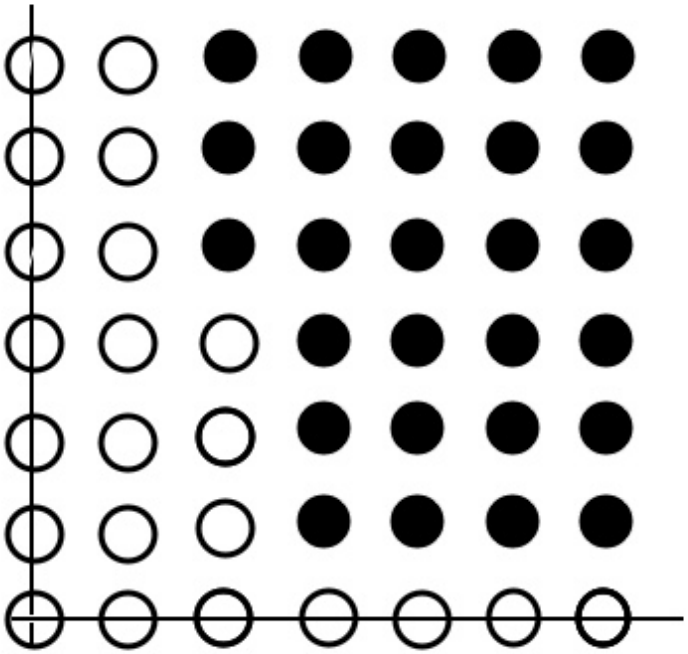
$$S(f, g) = \frac{LCM}{LT(f)} f - \frac{LCM}{LT(g)} g$$

Algorithm

```
def gb(F):
    G = [p for p in F]
    nn, n = -1, -2
    while nn != n:
        n = len(G)
        for i in range(0,n):
            for j in range(i+1,n):
                spoly = S(G[i], G[j])
                spoly = div(spoly,G)[1]
                if spoly != 0:
                    G += [spoly]
        nn = len(G)
    return G
```

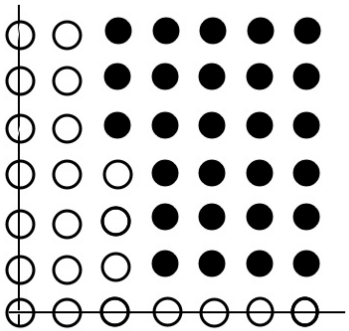
Monomial ideals

These are ideals generated by monomials. $I = \langle x^3y, x^2y^4 \rangle$



Lemma

(Dickson) Every monomial ideal is finitely generated.



In the example, the generators are the vertices of the "black cone." Proof in general is by induction on number of variables. Case of one variable is trivial.

Buchberger's algorithm terminates because of Dickson's lemma: $\langle LT(I) \rangle$ a monomial ideal and so is finitely generated. After a while $S(G_i, G_j) \ \% \ G$ discovers no new leading terms.

Philosophy

(1) It is often easy to "see" what is true for monomial ideals.

(2) What is true for monomial ideals is often true for general ideals.

(3) There is frequently an easy reduction of the general to the monomial case.

Examples:

(1) Hilbert basis theorem

(2) Hilbert functions

(3) Dimension theory