Functional Polynomial Algorithms

Thomas Meek

April 13, 2023

Linguistics

Linguistics

Declarative sentences

Linguistics

- Declarative sentences
- Imperative sentences

Linguistics

- Declarative sentences
- Imperative sentences
- Interrogative sentences

Declarative sentences

Declarative sentences

Steve has twelve eggs.

Declarative sentences

- Steve has twelve eggs.
- $f(x) = x^2$.

Imperative sentences

Imperative sentences

Make me an omelette.

Imperative sentences

- Make me an omelette.
- print("Hello world.")

Interrogative sentences

Interrogative sentences

• Where are my eggs?

Interrogative sentences

- Where are my eggs?
- Why is this guy talking about linguistics in a thesis defense for a mathematics degree?

Haskell

Procedural



- Procedural
- Object-oriented

- Procedural
- Object-oriented
- Functional

- Procedural ← Imperative
- ullet Object-oriented \leftarrow Imperative
- Functional

- Procedural ← Imperative
- ullet Object-oriented \leftarrow Imperative
- Functional ← Declarative

- Procedural ← Imperative (C)
- Object-oriented ← Imperative
- Functional ← Declarative

- ullet Procedural \leftarrow Imperative (C)
- Object-oriented ← Imperative (Java)
- Functional ← Declarative

- Procedural ← Imperative (C)
- Object-oriented ← Imperative (Java)
- Functional ← Declarative (Haskell)

- Procedural ← Imperative (C)
- Object-oriented ← Imperative (Java)
- Functional ← Declarative (Haskell)

Math

- Procedural ← Imperative (C)
- Object-oriented ← Imperative (Java)
- Functional ← Declarative (Haskell)
- \bullet Math \leftarrow Declarative

Polynomials

$$(x+a)^2$$

$$(x+a)^2 =_{\mathbb{F}_2} x^2 + a^2$$

Definition

A **monomial** in x_1, \ldots, x_n is a product of the form

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \cdot \cdot x_n^{\alpha_n},$$

where all of the exponents $\alpha_1, \ldots, \alpha_n$ are nonnegative integers.

Definition

Let $\alpha = (\alpha_1, \dots, \alpha_n)$ be an *n*-tuple of nonnegative integers. Then we set

$$x^{\alpha} = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}.$$

Definition

A **polynomial** f in the variables x_1, \ldots, x_n over a field k is a finite linear combination (with coefficients in k) of monomials in x_1, \ldots, x_n . We will write a polynomial f in the form

$$f=\sum_{lpha} \mathsf{a}_{lpha} \mathsf{x}^{lpha},\quad \mathsf{a}_{lpha}\in \mathsf{k},$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \dots, \alpha_n)$. The set of all polynomials in x_1, \dots, x_n with coefficients in k is denoted $k[x_1, \dots, x_n]$.

Leading term

Leading term

$$g = x^3 y z^2 + x^5 + x^2 y^3 z$$

Definition

A **monomial ordering** on $k[x_1, ..., x_n]$ is a relation > on the set of monomials x^{α} , $\alpha \in \mathbb{Z}_{>0}^n$ satisfying:

Definition

A monomial ordering on $k[x_1, ..., x_n]$ is a relation > on the set of monomials x^{α} , $\alpha \in \mathbb{Z}_{>0}^n$ satisfying:

> is a total ordering.

Definition

A **monomial ordering** on $k[x_1, ..., x_n]$ is a relation > on the set of monomials x^{α} , $\alpha \in \mathbb{Z}_{>0}^n$ satisfying:

- > is a total ordering.
- If $x^{\alpha} > x^{\beta}$ and $\gamma \in \mathbb{Z}^{n}_{\geq 0}$, then $x^{\alpha}x^{\gamma} > x^{\beta}x^{\gamma}$.

Definition

A **monomial ordering** on $k[x_1, ..., x_n]$ is a relation > on the set of monomials x^{α} , $\alpha \in \mathbb{Z}_{>0}^n$ satisfying:

- > is a total ordering.
- If $x^{\alpha} > x^{\beta}$ and $\gamma \in \mathbb{Z}_{\geq 0}^n$, then $x^{\alpha}x^{\gamma} > x^{\beta}x^{\gamma}$.
- > is a well-ordering.

Theorem

Let X be a commutative free monoid and suppose the first two conditions in the definition above are satisfied. Then the following are equivalent:

Theorem

Let X be a commutative free monoid and suppose the first two conditions in the definition above are satisfied. Then the following are equivalent:

ullet > is a well-ordering on X.

Theorem

Let X be a commutative free monoid and suppose the first two conditions in the definition above are satisfied. Then the following are equivalent:

- \bullet > is a well-ordering on X.
- Every strictly decreasing sequence in X eventually terminates.

Theorem

Let X be a commutative free monoid and suppose the first two conditions in the definition above are satisfied. Then the following are equivalent:

- \bullet > is a well-ordering on X.
- Every strictly decreasing sequence in X eventually terminates.
- $x^{\alpha} \geq 1$ for all $\alpha \in \mathbb{Z}_{\geq 0}^{n}$.



Definition (Lexicographic Order)

Let $\alpha=(\alpha_1,\ldots,\alpha_n)$ and $\beta=(\beta_1,\ldots,\beta_n)$ be in $\mathbb{Z}_{\geq 0}^n$. We say $x^{\alpha}>_{Lex}x^{\beta}$ if the leftmost nonzero entry of the vector difference $\alpha-\beta\in\mathbb{Z}^n$ is positive.

Definition (Lexicographic Order)

Let $\alpha=(\alpha_1,\ldots,\alpha_n)$ and $\beta=(\beta_1,\ldots,\beta_n)$ be in $\mathbb{Z}_{\geq 0}^n$. We say $x^{\alpha}>_{Lex}x^{\beta}$ if the leftmost nonzero entry of the vector difference $\alpha-\beta\in\mathbb{Z}^n$ is positive.

$$g = x^3 y z^2 + x^5 + x^2 y^3 z$$

Definition (Graded Lex Order)

Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. We say $x^{\alpha} >_{GLex} x^{\beta}$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $x^{\alpha} >_{Lex} x^{\beta}$.

Definition (Graded Lex Order)

Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. We say $x^{\alpha} >_{GLex} x^{\beta}$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $x^{\alpha} >_{Lex} x^{\beta}$.

$$g = x^3 y z^2 + x^5 + x^2 y^3 z$$

Definition (Graded Reverse Lex Order)

Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. We say $x^{\alpha} >_{GRevLex} x^{\beta}$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and the rightmost nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is negative.

Definition (Graded Reverse Lex Order)

Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. We say $x^{\alpha} >_{GRevLex} x^{\beta}$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and the rightmost nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is negative.

$$g = x^3 y z^2 + x^5 + x^2 y^3 z$$

Ideals

Definition

A subset $I \subseteq k[x_1, ..., x_n]$ is an **ideal** if it satisfies:

Definition

A subset $I \subseteq k[x_1, ..., x_n]$ is an **ideal** if it satisfies:

0 ∈ I.

Definition

A subset $I \subseteq k[x_1, ..., x_n]$ is an **ideal** if it satisfies:

- 0 ∈ I.
- If $f, g \in I$, then $f + g \in I$.

Definition

A subset $I \subseteq k[x_1, ..., x_n]$ is an **ideal** if it satisfies:

- 0 ∈ I.
- If $f, g \in I$, then $f + g \in I$.
- If $f \in I$ and $h \in k[x_1, ..., x_n]$, then $hf \in I$.

Definition

Let $I \subseteq k[x_1, ..., x_n]$ be an ideal other than $\{0\}$, and fix a monomial ordering on $k[x_1, ..., x_n]$. Then:

Definition

Let $I \subseteq k[x_1, ..., x_n]$ be an ideal other than $\{0\}$, and fix a monomial ordering on $k[x_1, ..., x_n]$. Then:

 We denote by LT(I) the set of leading terms of nonzero elements of I.

Definition

Let $I \subseteq k[x_1, ..., x_n]$ be an ideal other than $\{0\}$, and fix a monomial ordering on $k[x_1, ..., x_n]$. Then:

- We denote by LT(I) the set of leading terms of nonzero elements of I.
- We denote by $\langle LT(I) \rangle$ the ideal generated by the elements of LT(I).

Let
$$I = \langle f_1, \dots, f_t \rangle \subseteq k[x_1, \dots, x_n]$$
.

Let
$$I = \langle f_1, \dots, f_t \rangle \subseteq k[x_1, \dots, x_n].$$

$$\langle \text{LT}(f_1), \dots, \text{LT}(f_t) \rangle \subseteq \langle \text{LT}(I) \rangle.$$

•
$$f_1 = x^3 - 2xy$$
.

- $f_1 = x^3 2xy$.
- $f_2 = x^2y 2y^2 + x$.

- $f_1 = x^3 2xy$.
- $f_2 = x^2y 2y^2 + x$.
- $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Q}[x, y]$ with GRevLex.

- $f_1 = x^3 2xy$.
- $f_2 = x^2y 2y^2 + x$.
- $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Q}[x, y]$ with GRevLex.
- $x \cdot f_2 y \cdot f_1 = x^2$ so $x^2 \in I$.

- $f_1 = x^3 2xy$.
- $f_2 = x^2y 2y^2 + x$.
- $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Q}[x, y]$ with GRevLex.
- $x \cdot f_2 y \cdot f_1 = x^2 \text{ so } x^2 \in I$.
- $x^2 \in \langle LT(I) \rangle$.

- $f_1 = x^3 2xy$.
- $f_2 = x^2y 2y^2 + x$.
- $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Q}[x, y]$ with GRevLex.
- $x \cdot f_2 y \cdot f_1 = x^2 \text{ so } x^2 \in I$.
- $x^2 \in \langle LT(I) \rangle$.
- LT $(f_1) \nmid x^2$ and LT $(f_2) \nmid x^2$ so $x^2 \notin \langle LT(f_1), LT(f_2) \rangle$.

- $f_1 = x^3 2xy$.
- $f_2 = x^2y 2y^2 + x$.
- $I = \langle f_1, f_2 \rangle \subseteq \mathbb{Q}[x, y]$ with GRevLex.
- $x \cdot f_2 y \cdot f_1 = x^2 \text{ so } x^2 \in I$.
- $x^2 \in \langle LT(I) \rangle$.
- $LT(f_1) \nmid x^2$ and $LT(f_2) \nmid x^2$ so $x^2 \notin \langle LT(f_1), LT(f_2) \rangle$.
- $\langle LT(I) \rangle \not\subseteq \langle LT(f_1), LT(f_2) \rangle$.



Gröbner bases

Definition

Fix a monomial order on the polynomial ring $k[x_1, \ldots, x_n]$. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal $I \subseteq k[x_1, \ldots, x_n]$ different from $\{0\}$ is said to be a **Gröbner basis** if

$$\langle \operatorname{LT}(g_1), \ldots, \operatorname{LT}(g_t) \rangle = \langle \operatorname{LT}(I) \rangle.$$

Theorem

Let $G = \{g_1, \dots, g_t\}$ be a Gröbner basis for an ideal $I \subseteq k[x_1, \dots, x_n]$ and let $f \in k[x_1, \dots, x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.

Definition

We will write \overline{f}^F for the remainder on division of f by the ordered s-tuple $F = (f_1, \ldots, f_s)$. If F is a Gröbner basis for $\langle f_1, \ldots, f_s \rangle$, then we can regard F as a set (without any particular order).

Definition

Let $f,g \in k[x_1,\ldots,x_n]$ be nonzero polynomials.

Definition

Let $f, g \in k[x_1, ..., x_n]$ be nonzero polynomials.

• If multideg $(f) = \alpha$ and multideg $(g) = \beta$, then let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We call x^{γ} the **least common multiple** of LM(f) and LM(g), written $x^{\gamma} = \text{lcm}(\text{LM}(f), \text{LM}(g))$.

Definition

Let $f, g \in k[x_1, ..., x_n]$ be nonzero polynomials.

- If $\operatorname{multideg}(f) = \alpha$ and $\operatorname{multideg}(g) = \beta$, then let $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We call x^{γ} the **least common multiple** of $\operatorname{LM}(f)$ and $\operatorname{LM}(g)$, written $x^{\gamma} = \operatorname{lcm}(\operatorname{LM}(f), \operatorname{LM}(g))$.
- The **S-polynomial** of f and g is the combination

$$S(f,g) = \frac{x^{\gamma}}{\operatorname{LT}(f)} \cdot f - \frac{x^{\gamma}}{\operatorname{LT}(g)} \cdot g.$$

Theorem (Buchberger's Criterion)

Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ of I is a Gröbner basis of I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero.

Objects and morphisms

- Objects and morphisms
- Identity morphisms

- Objects and morphisms
- Identity morphisms
- Associative composition law

• Let (S, \leq) be a poset.

- Let (S, \leq) be a poset.
- Define the category S whose objects are the elements of S.

- Let (S, \leq) be a poset.
- Define the category S whose objects are the elements of S.
- $Hom(a, b) = \{(a, b)\}\ if\ a \le b.$

- Let (S, \leq) be a poset.
- Define the category S whose objects are the elements of S.
- $Hom(a, b) = \{(a, b)\}\ if\ a \le b.$
- Hom $(a, b) = \emptyset$ if a > b.

- Let (S, \leq) be a poset.
- Define the category S whose objects are the elements of S.
- $Hom(a, b) = \{(a, b)\}\ if\ a \le b.$
- Hom $(a, b) = \emptyset$ if a > b.
- (a,b)(b,c) = (a,c).

Definition

A functor $\mathcal{F}: C \to D$ is:

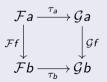
- An object $\mathcal{F}x \in D$ for each object $x \in C$.
- A morphism $\mathcal{F}f \in \mathsf{Hom}(\mathcal{F}a, \mathcal{F}b)$ for each morphism $f \in \mathsf{Hom}(a,b)$.
- For any composable pair of morphisms $f, g \in C$, $(\mathcal{F}f)(\mathcal{F}g) = \mathcal{F}(gf)$.
- For each object $x \in C$, $\mathcal{F}(1_x) = 1_{\mathcal{F}_X}$.



Definition

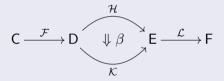
Given functors $\mathcal{F}, \mathcal{G}: \mathsf{C} \to \mathsf{D}$, a **natural transformation** $\tau: \mathcal{F} \Rightarrow \mathcal{G}$ maps objects in C to morphisms in D.

- If x is in C, then τ_x is in $\text{Hom}(\mathcal{F}x, \mathcal{G}x)$.
- The following diagram commutes for all $a, b \in C$.



Definition

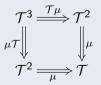
For a natural transformation β and functors $\mathcal F$ and $\mathcal L$,

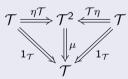


define a transformation $\mathcal{L}\beta\mathcal{F}: \mathcal{LHF} \Rightarrow \mathcal{LKF}$ by $(\mathcal{L}\beta\mathcal{F})_x = \mathcal{L}\beta_{\mathcal{F}_x}$. This is the **whiskered composite** of β with \mathcal{L} and \mathcal{F} .

Definition (Monad)

- ullet an endofunctor $\mathcal{T}:\mathsf{C}\to\mathsf{C}$,
- ullet a natural transformation $\eta:1_{\mathsf{C}}\Rightarrow\mathcal{T}$, and
- ullet a natural transformation $\mu:\mathcal{T}^2\Rightarrow\mathcal{T}$,





Functional Programming

Functional Programming

Algorithms

```
Algorithm 1 The Division Algorithm in k[x_1, \ldots, x_n]
```

```
p := f
r := 0
while (p \neq 0) do
    i := 1
    division occurred := false
    while (i \le s \text{ and division\_occurred} == \text{false}) do
         if (LT(g_i) divides LT(p)) then
             p := p - \frac{\operatorname{LT}(p)}{\operatorname{LT}(q_i)} g_i
             division\_occurred := true
         else
             i := i + 1
    if (division_occurred == false) then
         r := r + \operatorname{LT}(p)
         p := p - LT(p)
return r
```

Given a set T, denote the set of finite ordered lists of elements of T as [T]. Let $\emptyset \in [T]$ denote the empty list.

$$\varphi : [k[\mathbf{x}]] \times (k[\mathbf{x}] \times k[\mathbf{x}]) \to k[\mathbf{x}] \times k[\mathbf{x}]$$

$$\varphi(G,(p,r)) = \begin{cases} (p - \text{LT}(p), r + \text{LT}(p)) & \text{if } G = \emptyset, \\ (p - \frac{\text{LT}(p)}{\text{LT}(g_1)} g_1, r) & \text{if } G \neq \emptyset \text{ and } \text{LT}(g_1) | \text{LT}(p), \\ \varphi(G \setminus g_1, (p, r)) & \text{if } G \neq \emptyset \text{ and } \text{LT}(g_1) | \text{LT}(p). \end{cases}$$

$$\psi : [k[\mathbf{x}]] \times (k[\mathbf{x}] \times k[\mathbf{x}]) \to k[\mathbf{x}]$$

$$\psi(G,(p,r)) = \begin{cases} r & \text{if } p = 0, \\ \psi(G,\varphi(G,(p,r))) & \text{if } p \neq 0. \end{cases}$$

$$\overline{f}^G = \psi(G,(f,0)).$$

Algorithm 2 Buchberger's Algorithm

```
G := F
repeat
    G' := G
    for each pair \{p,q\} \in G' do
       r := \overline{S(p,q)}^{G'}
       if (r \neq 0) then
           G := G \cup \{r\}
until (G == G')
return G
```

Notation

 \bullet X + t

- X + t X + Y

- \bullet X + t
- \bullet X + Y
- y × X

- $\bullet X + t$
- \bullet X + Y
- y × X
- $\bullet X \times Y$

- \bullet X + t
- \bullet X + Y
- y × X
- \bullet $X \times Y$
- For $x = (f, g) \in k[\mathbf{x}] \times k[\mathbf{x}]$, Sx = S(f, g).

$$\varphi:[k[\mathbf{x}] \times k[\mathbf{x}]] \times [k[\mathbf{x}]] \to [k[\mathbf{x}]]$$

$$\varphi(X,G) = \begin{cases} G & \text{if } X = \emptyset, \\ \varphi(X \setminus x_1, G) & \text{if } X \neq \emptyset \text{ and } \overline{Sx_1}^G = 0, \\ \varphi\left(X \setminus x_1 + (\overline{Sx_1}^G \times G), G + \overline{Sx_1}^G\right) & \text{if } X \neq \emptyset \text{ and } \overline{Sx_1}^G \neq 0. \end{cases}$$

$$gb:[k[\mathbf{x}]] \to [k[\mathbf{x}]]$$

$$gb(F) = \varphi(F \times F, F)$$

Why?

Why should we care?



End

Questions?

