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?

Linguistics

Interrogative sentences

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

Why?

Haskell

Why?

- Procedural

Why?

- Procedural
- Object-oriented

Why?

- Procedural
- Object-oriented
- Functional

Why?

- Procedural $\leftarrow$ Imperative
- Object-oriented $\leftarrow$ Imperative
- Functional

Why?

- Procedural $\leftarrow$ Imperative
- Object-oriented $\leftarrow$ Imperative
- Functional $\leftarrow$ Declarative

Why?

- Procedural $\leftarrow$ Imperative (C)
- Object-oriented $\leftarrow$ Imperative
- Functional $\leftarrow$ Declarative

Why?

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

Why?

- Procedural $\leftarrow$ Imperative (C)
- Object-oriented $\leftarrow$ Imperative (Java)
- Functional $\leftarrow$ Declarative (Haskell)

Why?

- Procedural $\leftarrow$ Imperative (C)
- Object-oriented $\leftarrow$ Imperative (Java)
- Functional $\leftarrow$ Declarative (Haskell)

- Math

Why?

- Procedural $\leftarrow$ Imperative (C)
- Object-oriented $\leftarrow$ Imperative (Java)
- Functional $\leftarrow$ Declarative (Haskell)

- Math $\leftarrow$ Declarative

Polynomials

Polynomials

$$(x + a)^2$$

Polynomials

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

Polynomials

Definition

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

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

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

Polynomials

Definition

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

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

Polynomials

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

$$f = \sum_{\alpha} a_\alpha x^\alpha, \quad a_\alpha \in k,$$

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

Leading term

Polynomials

Leading term

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

Polynomials

Definition

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

Polynomials

Definition

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

- $>$ is a total ordering.

Polynomials

Definition

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

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

Polynomials

Definition

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

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

Polynomials

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:

Polynomials

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:

- $>$ *is a well-ordering on* X.

Polynomials

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:

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

Polynomials

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:

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

Polynomials

Definition (Lexicographic Order)

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

Polynomials

Definition (Lexicographic Order)

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

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

Polynomials

Definition (Graded Lex Order)

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

Polynomials

Definition (Graded Lex Order)

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

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

Polynomials

Definition (Graded Reverse Lex Order)

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. 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.

Polynomials

Definition (Graded Reverse Lex Order)

Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. 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.

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

Ideals

Polynomials

Definition

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

Polynomials

Definition

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

- $0 \in I$.

Polynomials

Definition

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

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

Polynomials

Definition

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

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

Polynomials

Definition

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

Polynomials

Definition

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

- We denote by $\mathrm{LT}(I)$ the set of leading terms of nonzero elements of I.

Polynomials

Definition

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

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

Polynomials

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

Polynomials

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

$$\langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t) \rangle \subseteq \langle \mathrm{LT}(I) \rangle.$$

Polynomials

- $f_1 = x^3 - 2xy$.

Polynomials

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

Polynomials

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

Polynomials

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

Polynomials

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

Polynomials

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

Polynomials

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

Gröbner bases

Polynomials

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

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

Polynomials

Theorem

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

Polynomials

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).

Polynomials

Definition

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

Polynomials

Definition

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

- If $\text{multideg}(f) = \alpha$ and $\text{multideg}(g) = \beta$, 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 $\text{LM}(f)$ and $\text{LM}(g)$, written $x^\gamma = \text{lcm}(\text{LM}(f), \text{LM}(g))$.

Polynomials

Definition

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

- If $\text{multideg}(f) = \alpha$ and $\text{multideg}(g) = \beta$, 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 $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$, written $x^\gamma = \mathrm{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$.
- The **S-polynomial** of f and g is the combination

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

Polynomials

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.

Categories

Categories

- Objects and morphisms

Categories

- Objects and morphisms
- Identity morphisms

Categories

- Objects and morphisms
- Identity morphisms
- Associative composition law

Categories

- Let $(S, \leq)$ be a poset.

Categories

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

Categories

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

Categories

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

Categories

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

Categories

Definition

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

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

Categories

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 $\mathrm{Hom}(\mathcal{F}x, \mathcal{G}x)$.
- The following diagram commutes for all $a, b \in \mathsf{C}$.

$$\begin{tikzcd} \mathcal{F}a \arrow[r, "\tau_a"] \arrow[d, "\mathcal{F}f"'] & \mathcal{G}a \arrow[d, "\mathcal{G}f"] \\ \mathcal{F}b \arrow[r, "\tau_b"'] & \mathcal{G}b \end{tikzcd}$$

Definition

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

$$\begin{tikzcd} \mathsf{C} \arrow[r, "\mathcal{F}"] & \mathsf{D} \arrow[r, bend left, "\mathcal{H}"] \arrow[r, bend right, "\mathcal{K}"'] \arrow[r, phantom, "\Downarrow\beta"] & \mathsf{E} \arrow[r, "\mathcal{L}"] & \mathsf{F} \end{tikzcd}$$

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

Categories

Definition (Monad)

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

$$
\begin{tikzcd}
\mathcal{T}^3 \arrow[r, Rightarrow, "\mathcal{T}\mu"] \arrow[d, Rightarrow, "\mu\mathcal{T}"'] & \mathcal{T}^2 \arrow[d, Rightarrow, "\mu"] \\
\mathcal{T}^2 \arrow[r, Rightarrow, "\mu"'] & \mathcal{T}
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathcal{T} \arrow[r, Rightarrow, "\eta\mathcal{T}"] \arrow[dr, Rightarrow, "1_{\mathcal{T}}"'] & \mathcal{T}^2 \arrow[d, Rightarrow, "\mu"] & \mathcal{T} \arrow[l, Rightarrow, "\mathcal{T}\eta"'] \arrow[dl, Rightarrow, "1_{\mathcal{T}}"] \\
& \mathcal{T} &
\end{tikzcd}
$$

Functional Programming

Algorithms

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 ($i \leq s$ **and** division_occurred == **false**) **do**
    if ($\text{LT}(g_i)$ divides $\text{LT}(p)$) **then**
      $p := p - \frac{\text{LT}(p)}{\text{LT}(g_i)} g_i$
      division_occurred := **true**
    else
      $i := i + 1$
  if (division_occurred == **false**) **then**
    $r := r + \text{LT}(p)$
    $p := p - \text{LT}(p)$
return r

Algorithms

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.

Algorithms

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

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

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

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

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

Algorithms

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

Algorithms

Notation

Algorithms

Notation

- $X + t$

Algorithms

Notation

- $X + t$
- $X + Y$

Algorithms

Notation

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

Algorithms

Notation

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

Algorithms

Notation

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

Algorithms

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

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

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

$$\mathrm{gb}(F) = \varphi(F \times F, F)$$

Why should we care?

End

Questions?