Functional Polynomial Algorithms

Thomas Meek

May 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.")`

Linguistics

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?

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 $k[x_1, \ldots, x_n]$.

Polynomials

Definition

Let $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ be a polynomial in $k[x_1, \ldots, x_n]$.

Polynomials

Definition

Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $k[x_1, \ldots, x_n]$.

- We call a_α the **coefficient** of the monomial x^α.

Polynomials

Definition

Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $k[x_1, \ldots, x_n]$.

- We call a_α the **coefficient** of the monomial x^α.
- If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a **term** of f.

Polynomials

Definition

Let $f = \sum_\alpha a_\alpha x^\alpha$ be a polynomial in $k[x_1, \dots, x_n]$.

- We call a_α the **coefficient** of the monomial x^α.
- If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a **term** of f.
- The **total degree** of $f \neq 0$, denoted $\deg(f)$, is the maximum $|\alpha|$ such that the coefficient a_α is nonzero. The total degree of the zero polynomial is undefined.

Polynomials

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

- $>$ is a total ordering.

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 $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n)$ 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 $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n)$ 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 $I \subseteq k[x_1, \ldots, x_n]$ be an ideal other than $\{0\}$, and fix a monomial ordering on $k[x_1, \ldots, x_n]$. 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 $\mathrm{LT}(I)$ the set of leading terms of nonzero elements of I.
- We denote by $\langle \mathrm{LT}(I) \rangle$ the ideal generated by the elements of $\mathrm{LT}(I)$.

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 $x^2 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$.

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 $\mathrm{LM}(f)$ and $\mathrm{LM}(g)$, written $x^\gamma = \text{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$.

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 $x^\gamma = \text{lcm}(\mathrm{LM}(f), \mathrm{LM}(g))$.
- 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.
- $\text{Hom}(a, b) = \{(a, b)\}$ if $a \leq b$.
- $\text{Hom}(a, b) = \emptyset$ 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

End

Questions?