Gröbner bases and Integer Programming

RANT

Alex Dunbar

March 23 2021

Emory University

Table of contents

Integer Programs

IPs

An integer progam is an optimization problem

$$\begin{aligned} \max \quad & c^\top x \\ \text{s.t.} \quad & Ax = b \\ & x \in \mathbb{Z}^n_+ \end{aligned} \tag{IP}$$

Traditional Solution of IPs

Theorem (Fundamental Theorem of Applied Math)

If $\mathcal{P}$ is a hard problem, then turning $\mathcal{P}$ into a linear algebra problem and throwing it into MATLAB provides a solution.

Proof.

Attend a scientific computing talk. $\square$

Traditional Solution of IPs (Serious)

Theorem (Fundamental Theorem of Integer Programming[1])

Let $\mathcal{X} = \{x \in \mathbb{Z}^n_+ | Ax = b\}$ *the feasible region to* (IP)*. Then,*

$$\max\{c^\top x | x \in \mathcal{X}\} = \max\{c^\top x | x \in conv(\mathcal{X})\}$$

[1] See e.g. Nemhauser-Wolsey *Integer and Combinatorial Optimization*

Traditional Solution of IPs (Serious)

Theorem (Fundamental Theorem of Integer Programming[1])

Let $\mathcal{X} = \{x \in \mathbb{Z}_+^n | Ax = b\}$ *the feasible region to* (IP). *Then,*

$$\max\{c^\top x | x \in \mathcal{X}\} = \max\{c^\top x | x \in conv(\mathcal{X})\}$$

Key idea: Can solve a sequence of linear programs over polyhedra which contain conv($\mathcal{X}$).

[1] See e.g. Nemhauser-Wolsey *Integer and Combinatorial Optimization*

Traditional Solution of IPs (Serious)

Theorem (Fundamental Theorem of Integer Programming[1])

Let $\mathcal{X} = \{x \in \mathbb{Z}^n_+ | Ax = b\}$ *the feasible region to* (IP). *Then,*

$$\max\{c^\top x | x \in \mathcal{X}\} = \max\{c^\top x | x \in conv(\mathcal{X})\}$$

Key idea: Can solve a sequence of linear programs over polyhedra which contain conv($\mathcal{X}$).

Leads to Branch & Bound and Cutting Plane algorithms.

[1] See e.g. Nemhauser-Wolsey *Integer and Combinatorial Optimization*

Example

$$
\begin{aligned}
\max \quad & \sum_{i,j,k=1}^{9} x_{i,j,k} & \\
\text{s.t.} \quad & \sum_{i=1}^{9} x_{i,j,k} = 1 & \forall j, k, \\
& \sum_{j=1}^{9} x_{i,j,k} = 1 & \forall i, k, \\
& \sum_{(i,j)\in S_\ell} x_{i,j,k} = 1 & \forall k, S_\ell, \\
& \sum_{k=1}^{9} x_{i,j,k} = 1 & \forall i, j, \\
& x_{i,j,k} = 1 & (i,j,k) \in \mathcal{C} \\
& x \in \{0,1\}^{729} &
\end{aligned}
$$

					3	6		
				8		4		
7				5				
		4				1		
	6		4					
								8
			6				2	7
8							5	
			1					

Example

$$
\begin{aligned}
\max \quad & \sum_{i,j,k=1}^{9} x_{i,j,k} \\
\text{s.t.} \quad & \sum_{i=1}^{9} x_{i,j,k} = 1 && \forall j, k, \\
& \sum_{j=1}^{9} x_{i,j,k} = 1 && \forall i, k, \\
& \sum_{(i,j) \in S_\ell} x_{i,j,k} = 1 && \forall k, S_\ell, \\
& \sum_{k=1}^{9} x_{i,j,k} = 1 && \forall i, j, \\
& x_{i,j,k} = 1 && (i,j,k) \in \mathcal{C} \\
& x \in \{0,1\}^{729}
\end{aligned}
$$

2	8	9	7	4	3	6	1	5
6	5	3	2	8	1	4	7	9
7	4	1	9	5	6	2	8	3
5	7	4	8	3	2	1	9	6
9	6	8	4	1	7	5	3	2
1	3	2	5	6	9	7	4	8
4	1	5	6	9	8	3	2	7
8	2	6	3	7	4	9	5	1
3	9	7	1	2	5	8	6	4

Gröbner Bases

Motivation

Consider a linear system of equations $Ax = b$, $A \in GL_n(\mathbb{C})$.

Motivation

Consider a linear system of equations $Ax = b$, $A \in GL_n(\mathbb{C})$.

If $A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ & a_{2,2} & \cdots & a_{2,n} \\ & & \ddots & \vdots \\ & & & a_{nn} \end{bmatrix}$ is upper triangular, we can solve $Ax = b$ with n equations of a single variable via backsubstitution.

Motivation

Consider a linear system of equations $Ax = b$, $A \in GL_n(\mathbb{C})$.

If $A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ & a_{2,2} & \cdots & a_{2,n} \\ & & \ddots & \vdots \\ & & & a_{nn} \end{bmatrix}$ is upper triangular, we can solve $Ax = b$ with n equations of a single variable via <u>backsubstitution</u>.

Moreover, we can decompose general $A \in GL_n(\mathbb{C})$ into $A = LU$ and solve $Ax = b$ “easily”.

Gröbner Bases [2]

Fix the lexicographic monomial ordering on $\mathbb{C}[x_1, x_2, \ldots, x_n]$. If $I \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$ is an ideal, set $LT(I) = \langle LT(f) | f \in I \rangle$.

[2]See e.g Dummit& Foote Section 9.6 or Cox, Little, O'Shea *Ideals, Varieties, and Algorithms* Ch. 2& 3

Gröbner Bases [2]

Fix the lexicographic monomial ordering on $\mathbb{C}[x_1, x_2, \ldots, x_n]$. If $I \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$ is an ideal, set $LT(I) = \langle LT(f) | f \in I \rangle$.

A subset $G \subseteq I$ is a <u>Gröbner Basis</u> of I if $I = \langle G \rangle$ and $LT(I) = \langle LT(g) | g \in G \rangle$.

[2] See e.g Dummit& Foote Section 9.6 or Cox, Little, O'Shea *Ideals, Varieties, and Algorithms* Ch. 2& 3

Gröbner Bases [2]

Fix the lexicographic monomial ordering on $\mathbb{C}[x_1, x_2, \ldots, x_n]$. If $I \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$ is an ideal, set $LT(I) = \langle LT(f) | f \in I \rangle$.

A subset $G \subseteq I$ is a <u>Gröbner Basis</u> of I if $I = \langle G \rangle$ and $LT(I) = \langle LT(g) | g \in G \rangle$.

G is <u>reduced</u> if each $g_i \in G$ is monic and if $LT(g_i)$ does not divide any term of g_j for $i \neq j$.

[2] See e.g Dummit& Foote Section 9.6 or Cox, Little, O'Shea *Ideals, Varieties, and Algorithms* Ch. 2& 3

Gröbner Bases

Theorem

1. *Every ideal* $I \subset \mathbb{C}[x_1, x_2, \ldots, x_n]$ *has a unique reduced Gröbner basis* $G = \{g_1, g_2, \ldots, g_m\}$
2. *Every* $f \in \mathbb{C}[x_1, x_2, \ldots, x_n]$ *can be written uniquely in the form* $f = f_I + r$*, where* $f_I \in I$ *and no monomial in* r *is divisible by* $LT(g_i)$*.*

Denote $r = f \mod G$.

Buchberger's Algorithm

Given $I = \langle f_1, f_2, \ldots, f_m \rangle \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$, we can find a Gröbner Basis:

1. $G = \{f_1, f_2, \ldots, f_m\}$

Buchberger's Algorithm

Given $I = \langle f_1, f_2, \ldots, f_m \rangle \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$, we can find a Gröbner Basis:

1. $G = \{f_1, f_2, \ldots, f_m\}$
2. For each $f_i, f_j \in G$,
    2.1 Set $S(f_i, f_j) = \frac{LCM(LT(f_i), LT(f_j))}{LT(f_i)} f_i - \frac{LCM(LT(f_i), LT(f_j))}{LT(f_j)} f_j$

Buchberger's Algorithm

Given $I = \langle f_1, f_2, \dots, f_m \rangle \subseteq \mathbb{C}[x_1, x_2, \dots, x_n]$, we can find a Gröbner Basis:

1. $G = \{f_1, f_2, \dots, f_m\}$
2. For each $f_i, f_j \in G$,
   2.1 Set $S(f_i, f_j) = \frac{LCM(LT(f_i), LT(f_j))}{LT(f_i)} f_i - \frac{LCM(LT(f_i), LT(f_j))}{LT(f_j)} f_j$
   2.2 If $S(f_i, f_j) = 0 \mod G$, continue iterating

Buchberger's Algorithm

Given $I = \langle f_1, f_2, \ldots, f_m \rangle \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$, we can find a Gröbner Basis:

1. $G = \{f_1, f_2, \ldots, f_m\}$
2. For each $f_i, f_j \in G$,
   - 2.1 Set $S(f_i, f_j) = \frac{LCM(LT(f_i), LT(f_j))}{LT(f_i)} f_i - \frac{LCM(LT(f_i), LT(f_j))}{LT(f_j)} f_j$
   - 2.2 If $S(f_i, f_j) = 0 \mod G$, continue iterating
   - 2.3 If $S(f_i, f_j) \neq 0 \mod G$, append $G = G \cup \{S(f_i, f_j) \mod G\}$ and go back to 2.

Example

Consider $I = \langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3 \rangle$.

Example

Consider $I = \langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3 \rangle$.

A Gröbner Basis for I is

$$G = \Big\{ x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3, \\ x_2x_3 - x_2 - 2x_3 + 2, x_3 - 1 \Big\}$$

Example

Consider $I = \langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3 \rangle$.

A Gröbner Basis for I is

$$G = \Big\{ x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3, \\ x_2x_3 - x_2 - 2x_3 + 2, x_3 - 1 \Big\}$$

The reduced Gröbner basis for I is

$$G_{\mathrm{red}} = \Big\{ x_1 + x_2 - 1, x_2^2 - x_2, x_3 - 1 \Big\}$$

Elimination

For each $1 \leq \ell \leq n$, let $I_\ell = I \cap \mathbb{C}[x_{\ell+1}, x_{\ell+2}, \ldots, x_n]$ be the ℓ^{th} elimination ideal.

Elimination

For each $1 \leq \ell \leq n$, let $I_\ell = I \cap \mathbb{C}[x_{\ell+1}, x_{\ell+2}, \ldots, x_n]$ be the ℓ^{th} elimination ideal.

Theorem

If G is a Gröbner basis of I, then $G \cap \mathbb{C}[x_{\ell+1}, x_{\ell+2}, \ldots, x_n]$ is a Gröbner basis of I_ℓ.

Extension

Why is elimination useful?

Extension

Why is elimination useful?

Theorem

Let $I = \langle f_1, f_2, \ldots, f_s \rangle \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$*. Then,* $LT(f_i) = g_i(x_2, x_3, \ldots, x_n)x_1^{N_i}$ *for some* $g_i \in \mathbb{C}[x_2, x_3, \ldots, x_n]$*. Moreover, if* $(a_2, a_3, \ldots, a_n) \in V(I_1)$*, and* $(a_2, a_3, \ldots, a_n) \notin V(\langle g_i \rangle)$*, then* $\exists\, a_1 \in \mathbb{C}$ *such that* $(a_1, a_2, \ldots, a_n) \in V(I)$*.*

Extension

Why is elimination useful?

Theorem

Let $I = \langle f_1, f_2, \dots, f_s \rangle \subseteq \mathbb{C}[x_1, x_2, \dots, x_n]$. *Then,* $LT(f_i) = g_i(x_2, x_3, \dots, x_n)x_1^{N_i}$ *for some* $g_i \in \mathbb{C}[x_2, x_3, \dots, x_n]$. *Moreover, if* $(a_2, a_3, \dots, a_n) \in V(I_1)$, *and* $(a_2, a_3, \dots, a_n) \notin V(\langle g_i \rangle)$, *then* $\exists\, a_1 \in \mathbb{C}$ *such that* $(a_1, a_2, \dots, a_n) \in V(I)$.

Key takeaway: Can use partial solutions to get full solutions.

Return to Example

We had $G = \left\{x_1 + x_2 - 1, x_2^2 - x_2, x_3 - 1\right\}$ was a reduced Gröbner basis of $I = \langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3\rangle$.

Return to Example

We had $G = \left\{x_1 + x_2 - 1, x_2^2 - x_2, x_3 - 1\right\}$ was a reduced Gröbner basis of $I = \langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3\rangle$.

$$G_2 = G \cap \mathbb{C}[x_3] = \langle x_3 - 1\rangle \implies \left[x \in V(I_2) \implies x_3 = 1\right]$$

Return to Example

We had $G = \left\{x_1 + x_2 - 1, x_2^2 - x_2, x_3 - 1\right\}$ was a reduced Gröbner basis of $I = \langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3 \rangle$.

$$G_2 = G \cap \mathbb{C}[x_3] = \langle x_3 - 1 \rangle \implies \left[x \in V(I_2) \implies x_3 = 1\right]$$

$$I_1 = \langle x_2^2 - x_2, x_3 - 1 \rangle \implies \left[x \in V(I_1) \implies x_2 \in \{0, 1\} \text{ and } x_3 = 1\right]$$

Return to Example

We had $G = \left\{x_1 + x_2 - 1, x_2^2 - x_2, x_3 - 1\right\}$ was a reduced Gröbner basis of $I = \langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3 \rangle$.

$$G_2 = G \cap \mathbb{C}[x_3] = \langle x_3 - 1 \rangle \implies \left[x \in V(I_2) \implies x_3 = 1\right]$$

$$I_1 = \langle x_2^2 - x_2, x_3 - 1 \rangle \implies \left[x \in V(I_1) \implies x_2 \in \{0,1\} \text{ and } x_3 = 1\right]$$

$$I = \langle x_1 + x_2 - 1, x_2^2 - x_2, x_3 - 1 \rangle \implies V(I) = \{(1,0,1),(0,1,1)\}$$

Using Gröbner Bases for Integer Programming

Return to Integer Programming[3]

Restrict our attention to binary integer programs:

$$\mathcal{X} = \{x \in \{0,1\}^n | Ax = b\}$$

[3] Bertsimas et. al *A New Algebraic Geometry Algorithm for Integer Programming*

Return to Integer Programming[3]

Restrict our attention to binary integer programs:

$$\mathcal{X} = \{x \in \{0,1\}^n | Ax = b\}$$

Then,

$$x \in \mathcal{X} \iff x \in V(\langle x_i^2 - x_i, \sum_{j=1}^{n} a_{i,j}x_j - b_i \rangle)$$

[3] Bertsimas et. al *A New Algebraic Geometry Algorithm for Integer Programming*

Solving IPs

Using

$$x \in \mathcal{X} \iff x \in V(\langle x_i^2 - x_i, \sum_{j=1}^{n} a_{i,j} x_j - b_i \rangle)$$

and the Elimination and Extension theorems, we can either determine that a problem is infeasible or enumerate its solutions

Example Part 3

Consider the BIP feasible region

$$\mathcal{X} = \{x \in \{0,1\}^3 | x_1 + x_2 + 3x_3 = 4\}$$

Example Part 3

Consider the BIP feasible region

$$\mathcal{X} = \{x \in \{0,1\}^3 | \, x_1 + x_2 + 3x_3 = 4\}$$

In our “new” language,

$$\mathcal{X} = V(\langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3 \rangle)$$

Example Part 3

Consider the BIP feasible region

$$\mathcal{X} = \{x \in \{0,1\}^3 | \, x_1 + x_2 + 3x_3 = 4\}$$

In our “new” language,

$$\begin{aligned} \mathcal{X} &= V(\langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3 \rangle) \\ &= V(\langle x_1 + x_2 - 1, x_2^2 - x_2, x_3 - 1 \rangle) \end{aligned}$$

Example Part 3

Consider the BIP feasible region

$$\mathcal{X} = \{x \in \{0,1\}^3 | \, x_1 + x_2 + 3x_3 = 4\}$$

In our "new" language,

$$\begin{aligned} \mathcal{X} &= V(\langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3 \rangle) \\ &= V(\langle x_1 + x_2 - 1, x_2^2 - x_2, x_3 - 1 \rangle) \\ &= \{(1,0,1), (0,1,1)\} \end{aligned}$$

Structure of Feasible Set

The terms of the reduced Göbner basis capture the logical dependency of the optimization variables:

$$\langle x_1 + x_2 - 1, x_2^2 - x_2, x_3 - 1 \rangle$$

Structure of Feasible Set

The terms of the reduced Göbner basis capture the logical dependency of the optimization variables:

$$\langle x_1 + x_2 - 1, x_2^2 - x_2, x_3 - 1 \rangle$$

Exactly one of x_1 or x_2 is 1, x_3 must be 1.

Maximization

Add in an objective function $z = c^\top x$:

$$\begin{aligned} \max \;\; & z = c^\top x \\ \text{s.t.} \;\; & Ax = b \\ & x \in \{0,1\}^n \end{aligned}$$

Maximization

Add in an objective function $z = c^\top x$:

$$\begin{aligned} \max\ & z = c^\top x \\ \text{s.t. } & Ax = b \\ & x \in \{0,1\}^n \end{aligned}$$

Look at

$$I = \langle x_i^2 - x_i, \sum_{j=1}^{n} a_{i,j}x_j - b_i, \sum_{j=1}^{n} c_j x_j - z \rangle \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n, z]$$

Example Part 4

Look at the Binary IP

$$\begin{aligned} \max \quad & z = x_1 + 3x_2 + 5x_3 \\ \text{s.t.} \quad & x_1 + x_2 + 3x_3 = 4 \\ & x \in \{0,1\}^3 \end{aligned}$$

Example Part 4

Look at the Binary IP

$$\begin{aligned} \max \;\; & z = x_1 + 3x_2 + 5x_3 \\ \text{s.t.} \;\; & x_1 + x_2 + 3x_3 = 4 \\ & x \in \{0,1\}^3 \end{aligned}$$

Ideal is

$$I = \langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3, x_1 + 3x_2 + 5x_3 - z \rangle$$

Example Part 4

Look at the Binary IP

$$\begin{aligned} \max\ \ & z = x_1 + 3x_2 + 5x_3 \\ \text{s.t.}\ \ & x_1 + x_2 + 3x_3 = 4 \\ & x \in \{0,1\}^3 \end{aligned}$$

Ideal is

$$\begin{aligned} I &= \langle x_1 + x_2 + 3x_3 - 4, x_1^2 - x_1, x_2^2 - x_2, x_3^2 - x_3, x_1 + 3x_2 + 5x_3 - z\rangle \\ &= \langle x_1 + \frac{1}{2}z - 4, x_2 - \frac{1}{2}z + 3, x_3 - 1, z^2 - 14z + 48\rangle \end{aligned}$$

Example Part 4 (cont.)

$$I = \langle x_1 + \frac{1}{2}z - 4, x_2 - \frac{1}{2}z + 3, x_3 - 1, z^2 - 14z + 48\rangle$$

So, $I_3 = I \cap \mathbb{C}[z] = \langle z^2 - 14z + 48\rangle$.

Example Part 4 (cont.)

$$I = \langle x_1 + \frac{1}{2}z - 4, x_2 - \frac{1}{2}z + 3, x_3 - 1, z^2 - 14z + 48 \rangle$$

So, $I_3 = I \cap \mathbb{C}[z] = \langle z^2 - 14z + 48 \rangle$.

Feasible Objective Values are:

$$V(I_3) = \{6, 8\}$$

Example Part 4 (cont.)

$$I = \langle x_1 + \frac{1}{2}z - 4, x_2 - \frac{1}{2}z + 3, x_3 - 1, z^2 - 14z + 48\rangle$$

So, $I_3 = I \cap \mathbb{C}[z] = \langle z^2 - 14z + 48\rangle$.

Feasible Objective Values are:

$$V(I_3) = \{6, 8\}$$

Take $z = 8$ and apply extension theorem:

$$(x_1, x_2, x_3; z) = (0, 1, 1; 8)$$

is optimal solution & objective value.

Conclusions

- Integer Programs are an interesting class of optimization problems
- Gröbner Bases assist in computation in polynomial rings
- Integer Programs can be translated into questions about ideals in $\mathbb{C}[x_1, x_2, \ldots, x_n, z]$.
- Don't try to implement this in MATLAB