LAKE FOREST COLLEGE

MATHEMATICAL ASSOCIATION OF AMERICA

Polynomials as Logic Gates

Solving Constraint Satisfaction Problems with Gröbner Bases

Sepehr Akbari

3/27/2026

Department of Math & CS, Lake Forest College

Solution Space of Linear Systems

Consider a simple system of linear equations:

$$x + y = 3 \quad \text{and} \quad x - y = 1$$

Represent this system as a matrix and perform Gaussian elimination, reducing it to row-echelon form:

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \end{bmatrix} \quad \xrightarrow{\text{RREF}} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

This eliminates variables, giving us

$$x = 2 \quad \text{and} \quad y = 1$$

Solution Space of Non-Linear Systems

What happens when we have a system of non-linear polynomials?

$$\begin{aligned} f_1 &: x^2 + y^2 - 2 = 0 \\ f_2 &: x^2 - y = 0 \end{aligned}$$

We can no longer use matrices or Gaussian elimination.

Our goal transitions from finding a single solution to finding the **solution space**, the set of all points where these equations simultaneously equal zero (vanish).

This solution space is called an **Affine Variety**, denoted $V(f_1, f_2)$.

The Ideal

To find the Variety, we study all polynomial linear combinations of our equations, known as the **Ideal** generated by f_1 and f_2, denoted $\langle f_1, f_2 \rangle$.

$$h = p(x, y) \cdot f_1 + q(x, y) \cdot f_2 \quad \text{for } h \in \langle f_1, f_2 \rangle$$

For $(x, y) \in V(f_1, f_2)$, we have $f_1(x, y) = 0$ and $f_2(x, y) = 0$. Therefore, for any $h \in \langle f_1, f_2 \rangle$, we also have $h(x, y) = 0$, regardless of p and q.

This means we can swap our original, messy equations for a *better generating set* that still describes the exact same Variety.

This better set of generators is called a **Gröbner basis**.

Gröbner Bases

A Gröbner basis is *better*, in this context, because it allows back-substitution.

Computing a Gröbner basis is done by Buchberger's algorithm. We usually use *Macaulay2* to compute the Gröbner basis.

```
-- a polynomial ring, with lexicographic ordering
R = QQ[x, y, MonomialOrder => Lex]
-- the ideal made from the system of equations
I = ideal(x^2 + y^2 - 2, x^2 - y)
-- computes the Gröbner basis
G = gb I
```

Gröbner Bases

For our example system, with lexicographic ordering $x > y$, we have

$$I = \langle x^2 + y^2 - 2,\ x^2 - y \rangle \in \mathbb{Q}[x, y]$$

and the Gröbner basis of I is:

$$G = \{y^2 + y - 2,\ x^2 - y\}$$

The variable x has been completely eliminated in the first generator.

Factor $y^2 + y - 2$ to find y, use back-substitution on $x^2 - y$ to find x.

If and only if $G = \{1\}$, we would say the Variety is empty, meaning there are no solutions to the system. This is a proof of non-existence.

What if we model discrete combinatorial problems
as a system of polynomials…

…and use Gröbner Bases
to explore their solution space?

Boolean Constraint

In combinatorics, a choice is either made or not made. We only want our variables to evaluate to True (1) or False (0).

We can force this by adding an **idempotency relation** as a generator to our ideal:

$$x^2 - x = 0$$

The only roots of this polynomial are $x = 0$ and $x = 1$.

Note: The affine variety is restricted to the vertices of a hypercube, where each vertex corresponds to a unique combination of True/False assignments.

Logic Gates

Since our variables are now boolean, we can represent logical operations as polynomial generators:

$$\begin{aligned}\text{NOT Gate:}\quad & \bar{x} && = 1 - x \\ \text{AND Gate:}\quad & x \wedge y && = xy \\ \text{OR Gate:}\quad & x \vee y && = x + y - xy \\ \text{XOR Gate:}\quad & x \oplus y && = x + y - 2xy\end{aligned}$$

Any logical constraint can be encoded as a polynomial.

The ideal generated by these polynomials will have a variety that represents all valid configurations of the combinatorial problem.

Case Study:
The Constrained Secret Santa

An Algebraic Christmas

Consider a gift exchange between n people, by defining n^2 variables $\{x_{i,j}\}$, where

$$\begin{aligned} x_{i,j} &= 1 \quad \text{if person } i \text{ gives to person } j \\ x_{i,j} &= 0 \quad \text{otherwise} \end{aligned}$$

What are the constraints of a valid Secret Santa assignment?

Boolean constraint: $x_{i,j}^2 - x_{i,j} = 0 \qquad \forall i, j$

Nobody gifts themselves: $x_{i,i} = 0 \qquad \forall i$

Everyone gives exactly one gift: $\sum_{j=1}^{n} x_{i,j} - 1 = 0 \qquad \forall i \in \{1, \ldots, n\}$

Everyone receives exactly one gift: $\sum_{i=1}^{n} x_{i,j} - 1 = 0 \qquad \forall j \in \{1, \ldots, n\}$

An Algebraic Christmas

We have modeled the standard derangement problem, but the real world is messy!

Consider a 4-person exchange between Alice (A), Bob (B), Dave (D), and Frank (F).

From a purely combinatorial perspective, there are

$$!4 = 4!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!}\right) = 9$$

valid derangements.

But what if we add new constraints that might exist in this group of people?

An Algebraic Christmas

What if Alice and Bob are partners and cannot gift each other?

$$x_{A,B} = 0 \quad \text{and} \quad x_{B,A} = 0$$

What if Frank had Dave last year and they want to avoid a repeat?

$$x_{F,D} = 0$$

Finally, let's forbid two people from just swapping gifts.

$$x_{i,j} \cdot x_{j,i} = 0 \quad \forall i, j$$

We can add all these generators to an ideal, J.

An Algebraic Christmas

The Gröbner basis G of J, computed with lexicographic order, gives us a simplified system of polynomials that describes all valid gift assignments.

$$G = \begin{cases} x_{A,D} + x_{F,B} - 1 & = 0 \\ x_{D,B} + x_{A,F} - 1 & = 0 \\ x_{F,A} + x_{F,B} - 1 & = 0 \\ x_{A,F} - x_{F,B} & = 0 \\ \vdots \end{cases}$$

$$x_{A,D} + x_{F,B} = 1 \text{ and } x_{A,F} = x_{F,B} \implies x_{A,D} + x_{A,F} = 1$$

(Alice must gift either Dave or Frank)

$$\text{If } x_{A,D} = 1 \implies x_{A,F} = 0 \implies x_{D,B} = 1$$
$$\text{If } x_{A,F} = 1 \implies x_{F,B} = 1 \implies x_{D,B} = 0$$

$$A \to D \to B \to F \to A$$
$$A \to F \to B \to D \to A$$

An Algebraic Christmas

Consider that Dave and Bob have a fight and refuse to gift each other.

We can easily add the generators $x_{D,B} = 0$ and $x_{B,D} = 0$ to our ideal J.

This time the Gröbner basis of the new ideal is:

$$G = \{1\}$$

So by the Weak Nullstellensatz, the variety is empty. The constraints make the problem mathematically impossible.

Why use Algebra for Combinatorics?

- Combinatorial search algorithms often require custom coding to handle conditional rules. The algebraic approach is **constraint-agnostic**.
- A Gröbner basis is **unique**, so it provides a deterministic decision tree for all valid solutions.
- The algebraic method offers a mathematical **proof of impossibility**, rather than just a failure to find a solution.
- Buchberger's algorithm is computationally intensive, but there are many **optimizations and heuristics** available, instead of exhaustively searching through all combinatorial possibilities.

Thank You!

Questions?

Sepehr Akbari
akbaris79@lakeforest.edu
Department of Math & CS, Lake Forest College