Hilbert's Nullstellensatz and proving Infeasibility

Peter Malkin*, UC Davis

Math and Computers 165

Nov 19th, 2008

Hilbert's Nullstellensatz

- **Theorem:** Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ its algebraic closure field. Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. The system of equations $f_1 = f_2 = \cdots = f_s = 0$ has **no** solution over $\overline{\mathbb{K}}$ iff there exist $\alpha_1, \ldots, \alpha_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$1 = \sum_{i=1}^{s} \alpha_i f_i$$

This polynomial identity is a *Nullstellensatz certificate*.

Hilbert's Nullstellensatz

- **Theorem:** Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ its algebraic closure field. Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. The system of equations $f_1 = f_2 = \cdots = f_s = 0$ has **no** solution over $\overline{\mathbb{K}}$ iff there exist $\alpha_1, \ldots, \alpha_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that

$$1 = \sum_{i=1}^{s} \alpha_i f_i$$

  This polynomial identity is a *Nullstellensatz certificate*.
- If $x \in \overline{\mathbb{K}}^n$ was a solution, then $\sum_{i=1}^{s} \alpha_i(x) f_i(x) = 0 \neq 1$.
- Nullstellensatz certificates are certificates of *infeasibility*.
- Let $d = \max\{\deg(\alpha_1), \deg(\alpha_2), \ldots, \deg(\alpha_s)\}$. Then, we say that d is the degree of the Nullstellensatz certificate.

Hilbert's Nullstellensatz

- Hilbert's Nullstellensatz is equivalent to the statement that the system $f_1 = f_2 = \cdots = f_s = 0$ has **no** solution over $\overline{\mathbb{K}}$ iff $1 \in \langle f_1, ..., f_s \rangle$ or equivalently every Gröbner basis is trivial (i.e. $\{1\}$) or equivalently $\langle f_1, ..., f_s \rangle = \mathbb{K}[x_1, ..., x_n]$.

Hilbert's Nullstellensatz

- Hilbert's Nullstellensatz is equivalent to the statement that the system $f_1 = f_2 = \cdots = f_s = 0$ has **no** solution over $\overline{\mathbb{K}}$ iff $1 \in \langle f_1, \ldots, f_s \rangle$ or equivalently every Gröbner basis is trivial (i.e. $\{1\}$) or equivalently $\langle f_1, \ldots, f_s \rangle = \mathbb{K}[x_1, \ldots, x_n]$.
- So, to show that a system is infeasible we could compute a Gröbner basis, but this often takes too long!

How do we find a Nullstellensatz certificate

Key point:

For fixed degree, this is a linear algebra problem over $\mathbb{K}$!!

How do we find a Nullstellensatz certificate

Key point:

For fixed degree, this is a linear algebra problem over $\mathbb{K}$!!

E.g. Consider the system of polynomial equations

$$f_1 = x_1^2 - 1 = 0,\ f_2 = x_1 + x_2 = 0,\ f_3 = x_1 + x_3 = 0,\ f_4 = x_2 + x_3 = 0$$

- This system has no solution over $\mathbb{C}$.

How do we find a Nullstellensatz certificate

Key point:

For fixed degree, this is a linear algebra problem over $\mathbb{K}$!!

E.g. Consider the system of polynomial equations

$$f_1 = x_1^2 - 1 = 0,\ f_2 = x_1 + x_2 = 0,\ f_3 = x_1 + x_3 = 0,\ f_4 = x_2 + x_3 = 0$$

- This system has no solution over $\mathbb{C}$.
- Does this system have a Nullstellensatz certificate of degree 1?

$$1 = \underbrace{(c_0x_1 + c_1x_2 + c_2x_3 + c_3)}_{\alpha_1}\underbrace{(x_1^2 - 1)}_{f_1} + \underbrace{(c_4x_1 + c_5x_2 + c_6x_3 + c_7)}_{\alpha_2}\underbrace{(x_1 + x_2)}_{f_2}$$
$$+ \underbrace{(c_8x_1 + c_9x_2 + c_{10}x_3 + c_{11})}_{\alpha_3}\underbrace{(x_1 + x_3)}_{f_3} + \underbrace{(c_{12}x_1 + c_{13}x_2 + c_{14}x_3 + c_{15})}_{\alpha_4}\underbrace{(x_2 + x_3)}_{f_4}$$

- Expand the Nullstellensatz certificate grouping by monomials.

$$1 = c_0x_1^3 + c_1x_1^2x_2 + c_2x_1^2x_3 + (c_3 + c_4 + c_8)x_1^2 + (c_5 + c_{13})x_2^2 + (c_{10} + c_{14})x_3^2$$
$$+(c_4 + c_5 + c_9 + c_{12})x_1x_2 + (c_6 + c_8 + c_{10} + c_{12})x_1x_3 + (c_6 + c_9 + c_{13} + c_{14})x_2x_3$$
$$+(c_7 + c_{11} - c_0)x_1 + (c_7 + c_{15} - c_1)x_2 + (c_{11} + c_{15} - c_2)x_3 - c_3$$

- Extract a *linear* system of equations from expanded certificate.

$$c_0 = 0,\ \ldots,\ c_3 + c_4 + c_8 = 0,\ c_{11} + c_{15} - c_2 = 0,\ -c_3 = 1$$

- Expand the Nullstellensatz certificate grouping by monomials.

$$1 = c_0x_1^3 + c_1x_1^2x_2 + c_2x_1^2x_3 + (c_3 + c_4 + c_8)x_1^2 + (c_5 + c_{13})x_2^2 + (c_{10} + c_{14})x_3^2$$
$$+(c_4 + c_5 + c_9 + c_{12})x_1x_2 + (c_6 + c_8 + c_{10} + c_{12})x_1x_3 + (c_6 + c_9 + c_{13} + c_{14})x_2x_3$$
$$+(c_7 + c_{11} - c_0)x_1 + (c_7 + c_{15} - c_1)x_2 + (c_{11} + c_{15} - c_2)x_3 - c_3$$

- Extract a *linear* system of equations from expanded certificate.

$$c_0 = 0,\ \ldots,\ c_3 + c_4 + c_8 = 0,\ c_{11} + c_{15} - c_2 = 0,\ -c_3 = 1$$

- Solve the linear system. This linear system is feasible, so we have found a certificate and proven the polynomial system is infeasible. **Note:** the linear system is over $\mathbb{R}$ and not $\mathbb{C}$.

- Expand the Nullstellensatz certificate grouping by monomials.

$$1 = c_0x_1^3 + c_1x_1^2x_2 + c_2x_1^2x_3 + (c_3 + c_4 + c_8)x_1^2 + (c_5 + c_{13})x_2^2 + (c_{10} + c_{14})x_3^2$$
$$+(c_4 + c_5 + c_9 + c_{12})x_1x_2 + (c_6 + c_8 + c_{10} + c_{12})x_1x_3 + (c_6 + c_9 + c_{13} + c_{14})x_2x_3$$
$$+(c_7 + c_{11} - c_0)x_1 + (c_7 + c_{15} - c_1)x_2 + (c_{11} + c_{15} - c_2)x_3 - c_3$$

- Extract a *linear* system of equations from expanded certificate.

$$c_0 = 0,\ \ldots,\ c_3 + c_4 + c_8 = 0,\ c_{11} + c_{15} - c_2 = 0,\ -c_3 = 1$$

- Solve the linear system. This linear system is feasible, so we have found a certificate and proven the polynomial system is infeasible. **Note:** the linear system is over $\mathbb{R}$ and not $\mathbb{C}$.
- Reconstruct the Nullstellensatz certificate from a solution of the linear system.

$$1 = -(x_1^2 - 1) + \frac{1}{2}x_1(x_1 + x_2) - \frac{1}{2}x_1(x_2 + x_3) + \frac{1}{2}x_1(x_1 + x_3)$$

- Expand the Nullstellensatz certificate grouping by monomials.

$$1 = c_0x_1^3 + c_1x_1^2x_2 + c_2x_1^2x_3 + (c_3 + c_4 + c_8)x_1^2 + (c_5 + c_{13})x_2^2 + (c_{10} + c_{14})x_3^2$$
$$+(c_4 + c_5 + c_9 + c_{12})x_1x_2 + (c_6 + c_8 + c_{10} + c_{12})x_1x_3 + (c_6 + c_9 + c_{13} + c_{14})x_2x_3$$
$$+(c_7 + c_{11} - c_0)x_1 + (c_7 + c_{15} - c_1)x_2 + (c_{11} + c_{15} - c_2)x_3 - c_3$$

- Extract a *linear* system of equations from expanded certificate.

$$c_0 = 0,\ \ldots,\ c_3 + c_4 + c_8 = 0,\ c_{11} + c_{15} - c_2 = 0,\ -c_3 = 1$$

- Solve the linear system. This linear system is feasible, so we have found a certificate and proven the polynomial system is infeasible. **Note:** the linear system is over $\mathbb{R}$ and not $\mathbb{C}$.
- Reconstruct the Nullstellensatz certificate from a solution of the linear system.

$$1 = -(x_1^2 - 1) + \frac{1}{2}x_1(x_1 + x_2) - \frac{1}{2}x_1(x_2 + x_3) + \frac{1}{2}x_1(x_1 + x_3)$$

- If the linear system was not feasible, we would have had to try a higher degree.

Bounds for the Nullstellensatz degree

Question:

How big can the degree of a Nullstellensatz certificate be?

Bounds for the Nullstellensatz degree

Question:

How big can the degree of a Nullstellensatz certificate be?

The most general bound...

Theorem: (Kollár)

The degree is bounded by $\max\{3, D\}^n$, where n is the number of variables and $D = \max\{\deg(f_1), \deg(f_2), \ldots, \deg(f_s)\}$.

Bounds for the Nullstellensatz degree

Question:

How big can the degree of a Nullstellensatz certificate be?

The most general bound...

Theorem: (Kollár)

The degree is bounded by $\max\{3, D\}^n$, where n is the number of variables and $D = \max\{\deg(f_1), \deg(f_2), \ldots, \deg(f_s)\}$.

But for some types of systems have a better bound:

Theorem: (Lazard)

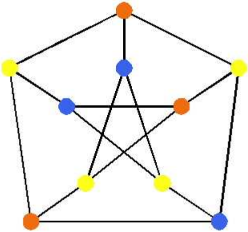
The degree is bounded by $n(D-1)$.

NulLA: Nullstellensatz linear algebra algorithm

- **Input:** A system of polynomial equations $F = \{f_1 = 0, f_2 = 0, \ldots, f_s = 0\}$.
- Set $d = 0$.
- **While** $d \leq$ HNBound and no solution found for L_d:
  - Construct a tentative Nullstellensatz certificate of degree d.
  - Extract a linear system of equations L_d.
  - Solve the linear system L_d.
  - **If** there is a solution, **then** reconstruct the certificate and **Output**: F is INFEASIBLE.
  - **Else** Set $d = d + 1$.
- **If** $d =$ HNBound and no solution found for L_d, **then** **Output**: F is FEASIBLE.

Graph Coloring

- **Graph vertex coloring:** Given a graph G and an integer k, can the vertices be colored with k colors in such a way that no two adjacent vertices are the same color?
- E.g. the **Petersen Graph** is 3-colorable.



Graph coloring modeled by a polynomial system

- One **variable** x_i per **vertex** $i \in \{1, ..., n\}$.
- **Vertex polynomials:** For every vertex $i = 1, \ldots, n$,

$$x_i^k - 1 = 0.$$

- **Edge polynomials:** For every edge $(i, j) \in E$,

$$x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} = 0.$$

NB: $x_i^k - x_j^k = (x_i - x_j)(x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1}) = 0.$

Graph coloring modeled by a polynomial system

- One **variable** x_i per **vertex** $i \in \{1, ..., n\}$.
- **Vertex polynomials:** For every vertex $i = 1, \dots, n$,

$$x_i^k - 1 = 0.$$

- **Edge polynomials:** For every edge $(i, j) \in E$,

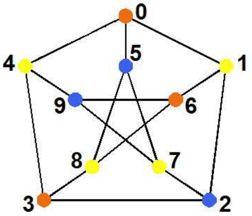
$$x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1} = 0.$$

NB: $x_i^k - x_j^k = (x_i - x_j)(x_i^{k-1} + x_i^{k-2}x_j + \cdots + x_i x_j^{k-2} + x_j^{k-1}) = 0.$

- **Theorem:** (D. Bayer) Let k be an integer and let G be a graph encoded as vertex and edge polynomials as above. This system has a solution iff G is k-colorable.
- **Theorem:** For a graph G, the following system of polynomial equations in $\mathbb{F}_2[x]$ has a solution over $\overline{\mathbb{F}}_2$ iff G is 3-colorable.

$$x_i^3 + 1 = 0 \; \forall i \in V, \quad x_i^2 + x_i x_j + x_j^2 = 0 \; \forall (i, j) \in E.$$

E.g. Petersen graph polynomial system of equations



This system has a solution iff the Petersen graph is 3-colorable.

$$\begin{array}{ll}
x_0^3 - 1 = 0,\ x_1^3 - 1 = 0, & x_0^2 + x_0x_1 + x_1^2 = 0,\ x_0^2 + x_0x_4 + x_4^2 = 0, \\
x_2^3 - 1 = 0,\ x_3^3 - 1 = 0, & x_0^2 + x_0x_5 + x_5^2 = 0,\ x_1^2 + x_1x_2 + x_2^2 = 0, \\
x_4^3 - 1 = 0,\ x_5^3 - 1 = 0, & x_1^2 + x_1x_6 + x_6^2 = 0,\ x_2^2 + x_2x_7 + x_7^2 = 0, \\
x_6^3 - 1 = 0,\ x_7^3 - 1 = 0, & \cdots\cdots \qquad\qquad \cdots\cdots \\
x_8^3 - 1 = 0,\ x_9^3 - 1 = 0, & x_6^2 + x_6x_8 + x_8^2 = 0,\ x_7^2 + x_7x_9 + x_9^2 = 0.
\end{array}$$

Experimental results for NulLA 3-colorability

Graph	$\lvert V \rvert$	$\lvert E \rvert$	#*rows*	#*cols*	*d*	*sec*
Mycielski 7	95	755	64,281	71,726	1	1
Mycielski 9	383	7,271	2,477,931	2,784,794	1	269
Mycielski 10	767	22,196	15,270,943	17,024,333	1	14835
$(8, 3)$-Kneser	56	280	15,737	15,681	1	0
$(10, 4)$-Kneser	210	1,575	349,651	330,751	1	4
$(12, 5)$-Kneser	792	8,316	7,030,585	6,586,273	1	467
$(13, 5)$-Kneser	1,287	36,036	45,980,650	46,378,333	1	216105
1-Insertions_5	202	1,227	268,049	247,855	1	2
2-Insertions_5	597	3,936	2,628,805	2,349,793	1	18
3-Insertions_5	1,406	9,695	15,392,209	13,631,171	1	83
ash331GPIA	662	4,185	3,147,007	2,770,471	1	14
ash608GPIA	1,216	7,844	10,904,642	9,538,305	1	35
ash958GPIA	1,916	12,506	27,450,965	23,961,497	1	90

Table: DIMACS graphs without 4-cliques.