Algebraic refutation systems

The Nullstellensatz system

Siert Wieringa

swiering@tcs.hut.fi

Introduction

- Algebraic Refutation/Proof Systems
- Transform propositional formulas to polynomials
- Proof or refute by solving linear equations
- This presentation will discuss the *Nullstellensatz System (NS)*

Hilbert's Nullstellensatz

Let F be a field, and

$$g(x_1,\ldots,x_n),\ f_1(x_1,\ldots,x_n),\ldots,\ f_m(x_1,\ldots,x_n)$$

be polynomials over F.

Hilbert's Nullstellensatz

Let F be a field, and

$$g(x_1,\ldots,x_n),\, f_1(x_1,\ldots,x_n),\ldots,\, f_m(x_1,\ldots,x_n)$$

be polynomials over F. Then the following are equivalent.

1 In all extension rings of F the following holds:

$$(\forall x_1,\ldots,x_n)\left[\bigwedge_{i=1}^{m} f_i(x_1,\ldots,x_n)=0 \rightarrow g(x_1,\ldots,x_n)=0\right]$$

2 $g \in I$, where $I = < f_1,\ldots, f_m >$ is the ideal generated by $f_1,\ldots, f_m$.

Hilbert's Nullstellensatz

Let F be a field, and

$$g(x_1,\ldots,x_n),\, f_1(x_1,\ldots,x_n),\ldots,\, f_m(x_1,\ldots,x_n)$$

be polynomials over F. Then the following are equivalent.

1 In all algebraically closed extension fields of F the following holds:

$$(\forall x_1,\ldots,x_n)\left[\bigwedge_{i=1}^{m} f_i(x_1,\ldots,x_n)=0 \rightarrow g(x_1,\ldots,x_n)=0\right]$$

2 $g^k \in I$, where $k \geq 1$ *and* $I = < f_1,\ldots, f_m >$ is the ideal generated by $f_1,\ldots, f_m$.

The canonical polynomial p_A

FALSE	0
TRUE	1
x_i	x_i
$\neg A$	$1 - A$
$A \wedge B$	$A \cdot B$
$A \vee B$	$A + B - A \cdot B$

The canonical polynomial p_A

FALSE	0
TRUE	1
x_i	x_i
$\neg A$	$1 - A$
$A \wedge B$	$A \cdot B$
$A \vee B$	$A + B - A \cdot B$

Example: PHP^2_1 (tautology)

$$\left(\neg x_{1,1} \vee \neg x_{2,1}\right) \vee \left(x_{1,1} \wedge x_{2,1}\right)$$

The canonical polynomial p_A

FALSE	0
TRUE	1
x_i	x_i
$\neg A$	$1 - A$
$A \wedge B$	$A \cdot B$
$A \vee B$	$A + B - A \cdot B$

Example: PHP_1^2 (tautology)

$$(\neg x_{1,1} \vee \neg x_{2,1}) \vee (x_{1,1} \wedge x_{2,1})$$

$$(1 - x_{1,1})$$

The canonical polynomial p_A

FALSE	0
TRUE	1
x_i	x_i
$\neg A$	$1 - A$
$A \wedge B$	$A \cdot B$
$A \vee B$	$A + B - A \cdot B$

Example: PHP^2_1 (tautology)

$$(\neg x_{1,1} \vee \neg x_{2,1}) \vee (x_{1,1} \wedge x_{2,1})$$

$$(1 - x_{1,1}) + (1 - x_{2,1}) - (1 - x_{1,1})(1 - x_{2,1})$$

The canonical polynomial p_A

FALSE	0
TRUE	1
x_i	x_i
$\neg A$	$1 - A$
$A \wedge B$	$A \cdot B$
$A \vee B$	$A + B - A \cdot B$

Example: PHP_1^2 (tautology)

$$(\neg x_{1,1} \vee \neg x_{2,1}) \vee (x_{1,1} \wedge x_{2,1})$$

$$1 - x_{1,1}x_{2,1} + x_{1,1}^2 x_{2,1}^2$$

The canonical polynomial p_A

FALSE	0
TRUE	1
x_i	x_i
$\neg A$	$1 - A$
$A \wedge B$	$A \cdot B$
$A \vee B$	$A + B - A \cdot B$

Example: PHP_1^2 (tautology)

$$(\neg x_{1,1} \vee \neg x_{2,1}) \vee (x_{1,1} \wedge x_{2,1})$$

$$q = 1 - x_{1,1} x_{2,1} + x_{1,1}^2 x_{2,1}^2$$

The canonical polynomial p_A

FALSE	0
TRUE	1
x_i	x_i
$\neg A$	$1 - A$
$A \wedge B$	$A \cdot B$
$A \vee B$	$A + B - A \cdot B$

Example: PHP^2_1 (tautology)

$$(\neg x_{1,1} \vee \neg x_{2,1}) \vee (x_{1,1} \wedge x_{2,1})$$

$$q = 1 - x_{1,1}x_{2,1} + x^2_{1,1}x^2_{2,1}$$

So polynomial p_A for PHP^2_1 is: $q + x_{1,1}x_{2,1} - q \cdot x_{1,1}x_{2,1}$

The canonical polynomial p_A

FALSE	0
TRUE	1
x_i	x_i
$\neg A$	$1 - A$
$A \wedge B$	$A \cdot B$
$A \vee B$	$A + B - A \cdot B$

Example: PHP^2_1 (tautology)

$$(\neg x_{1,1} \vee \neg x_{2,1}) \vee (x_{1,1} \wedge x_{2,1})$$

$$q = 1 - x_{1,1} x_{2,1} + x^2_{1,1} x^2_{2,1}$$

So polynomial p_A for PHP^2_1 is: $1 - x_{1,1} x_{2,1} + x^2_{1,1} x^2_{2,1}$

Refutations and polynomial p_A

- A *Nullstellensatz refutation* of a propositional formula A with canonical translation p_A is given by

$$1 = (1 - p_A(x_1, \ldots, x_n)) \cdot g + \sum_{i=1}^{n} (x_i^2 - x_i) \cdot h_i$$

Refutations and polynomial p_A

- A *Nullstellensatz refutation* of a propositional formula A with canonical translation p_A is given by

$$1 = (1 - p_A(x_1, \ldots, x_n)) \cdot g + \sum_{i=1}^{n} (x_i^2 - x_i) \cdot h_i$$

- So a refutation for $\neg \mathrm{PHP}_1^2$ is formed by g, h_1 and h_2

$$1 = p_A \cdot g + (x_{1,1}^2 - x_{1,1}) \cdot h_1 + (x_{2,1}^2 - x_{2,1}) \cdot h_2$$

Refutations and polynomial p_A

- A *Nullstellensatz refutation* of a propositional formula A with canonical translation p_A is given by

$$1 = (1 - p_A(x_1, \ldots, x_n)) \cdot g + \sum_{i=1}^{n} (x_i^2 - x_i) \cdot h_i$$

- So a refutation for $\neg \mathrm{PHP}_1^2$ is formed by g, h_1 and h_2
$1 = p_A \cdot g + (x_{1,1}^2 - x_{1,1}) \cdot h_1 + (x_{2,1}^2 - x_{2,1}) \cdot h_2$
- Degree of a *NS* refutation is $deg(p_A \cdot g)$

Refutations and polynomial p_A

- A *Nullstellensatz refutation* of a propositional formula A with canonical translation p_A is given by

$$1 = (1 - p_A(x_1, \ldots, x_n)) \cdot g + \sum_{i=1}^{n} (x_i^2 - x_i) \cdot h_i$$

- So a refutation for $\neg\mathrm{PHP}_1^2$ is formed by g, h_1 and h_2
$1 = p_A \cdot g + (x_{1,1}^2 - x_{1,1}) \cdot h_1 + (x_{2,1}^2 - x_{2,1}) \cdot h_2$
- Degree of a *NS* refutation is $deg(p_A \cdot g)$
- Nullstellensatz refutations have constant degree if and only if their size is polynomial

A *NS* refutation for $\neg\mathrm{PHP}^2_1$

- Choose $g = 1$, $h_1 = -x^2_{2,1}$, $h_2 = -x_{1,1}$

$$1 = p_1 + (x^2_{1,1} - x_{1,1}) \cdot -x^2_{2,1} + (x^2_{2,1} - x_{2,1}) \cdot -x_{1,1}$$

A *NS* refutation for $\neg\mathrm{PHP}_1^2$

- Choose $g = 1$, $h_1 = -x_{2,1}^2$, $h_2 = -x_{1,1}$

$$1 = p_1 + (x_{1,1}^2 - x_{1,1}) \cdot -x_{2,1}^2 + (x_{2,1}^2 - x_{2,1}) \cdot -x_{1,1}$$

- Let's fill in p_1

$$1 = 1 - x_{1,1}x_{2,1} + x_{1,1}^2 x_{2,1}^2 + (x_{1,1}^2 - x_{1,1}) \cdot -x_{2,1}^2 + (x_{2,1}^2 - x_{2,1}) \cdot -x_{1,1}$$

A *NS* refutation for $\neg\mathrm{PHP}^2_1$

- Choose $g = 1$, $h_1 = -x^2_{2,1}$, $h_2 = -x_{1,1}$

$$1 = p_1 + (x^2_{1,1} - x_{1,1}) \cdot -x^2_{2,1} + (x^2_{2,1} - x_{2,1}) \cdot -x_{1,1}$$

- Let's fill in p_1

$$1 = 1 - x_{1,1}x_{2,1} + x^2_{1,1}x^2_{2,1} + (x^2_{1,1} - x_{1,1}) \cdot -x^2_{2,1} + (x^2_{2,1} - x_{2,1}) \cdot -x_{1,1}$$

$$1 = 1 - x_{1,1}x_{2,1} + x^2_{1,1}x^2_{2,1} - x^2_{2,1}x^2_{1,1} + x^2_{2,1}x_{1,1} + (x^2_{2,1} - x_{2,1}) \cdot -x_{1,1}$$

A *NS* refutation for $\neg\mathrm{PHP}_1^2$

- Choose $g = 1$, $h_1 = -x_{2,1}^2$, $h_2 = -x_{1,1}$

$$1 = p_1 + (x_{1,1}^2 - x_{1,1}) \cdot -x_{2,1}^2 + (x_{2,1}^2 - x_{2,1}) \cdot -x_{1,1}$$

- Let's fill in p_1

$$1 = 1 - x_{1,1}x_{2,1} + x_{1,1}^2 x_{2,1}^2 + (x_{1,1}^2 - x_{1,1}) \cdot -x_{2,1}^2 + (x_{2,1}^2 - x_{2,1}) \cdot -x_{1,1}$$

$$1 = 1 - x_{1,1}x_{2,1} + x_{1,1}^2 x_{2,1}^2 - x_{2,1}^2 x_{1,1}^2 + x_{2,1}^2 x_{1,1} + (x_{2,1}^2 - x_{2,1}) \cdot -x_{1,1}$$

A *NS* refutation for $\neg\mathrm{PHP}^2_1$

- Choose $g = 1$, $h_1 = -x^2_{2,1}$, $h_2 = -x_{1,1}$

$$1 = p_1 + (x^2_{1,1} - x_{1,1}) \cdot -x^2_{2,1} + (x^2_{2,1} - x_{2,1}) \cdot -x_{1,1}$$

- Let's fill in p_1

$$1 = 1 - x_{1,1}x_{2,1} + x^2_{1,1}x^2_{2,1} + (x^2_{1,1} - x_{1,1}) \cdot -x^2_{2,1} + (x^2_{2,1} - x_{2,1}) \cdot -x_{1,1}$$

$$1 = 1 - x_{1,1}x_{2,1} + x^2_{2,1}x_{1,1} - x^2_{2,1}x_{1,1} + x_{2,1}x_{1,1}$$

A *NS* refutation for $\neg\mathrm{PHP}^2_1$

- Choose $g = 1$, $h_1 = -x^2_{2,1}$, $h_2 = -x_{1,1}$

$$1 = p_1 + (x^2_{1,1} - x_{1,1}) \cdot -x^2_{2,1} + (x^2_{2,1} - x_{2,1}) \cdot -x_{1,1}$$

- Let's fill in p_1

$$1 = 1 - x_{1,1}x_{2,1} + x^2_{1,1}x^2_{2,1} + (x^2_{1,1} - x_{1,1}) \cdot -x^2_{2,1} + (x^2_{2,1} - x_{2,1}) \cdot -x_{1,1}$$

$$1 = 1 - x_{1,1}x_{2,1} + x^2_{2,1}x_{1,1} - x^2_{2,1}x_{1,1} + x_{2,1}x_{1,1}$$

A *NS* refutation for $\neg\mathrm{PHP}_1^2$

- Choose $g = 1$, $h_1 = -x_{2,1}^2$, $h_2 = -x_{1,1}$

$$1 = p_1 + (x_{1,1}^2 - x_{1,1}) \cdot -x_{2,1}^2 + (x_{2,1}^2 - x_{2,1}) \cdot -x_{1,1}$$

- Let's fill in p_1

$$1 = 1 - x_{1,1}x_{2,1} + x_{1,1}^2 x_{2,1}^2 + (x_{1,1}^2 - x_{1,1}) \cdot -x_{2,1}^2 + (x_{2,1}^2 - x_{2,1}) \cdot -x_{1,1}$$

$$1 = 1$$

A *NS* refutation for $\neg\mathrm{PHP}^2_1$

- Choose $g = 1$, $h_1 = -x^2_{2,1}$, $h_2 = -x_{1,1}$

$$1 = p_1 + (x^2_{1,1} - x_{1,1}) \cdot -x^2_{2,1} + (x^2_{2,1} - x_{2,1}) \cdot -x_{1,1}$$

- Let's fill in p_1

$$1 = 1 - x_{1,1}x_{2,1} + x^2_{1,1}x^2_{2,1} + (x^2_{1,1} - x_{1,1}) \cdot -x^2_{2,1} + (x^2_{2,1} - x_{2,1}) \cdot -x_{1,1}$$

- So g, h_1 and h_2 form a valid Nullstellensatz refutation for $\neg\mathrm{PHP}^2_1$

The canonical polynomial q_A

- A different representation, q_A is the preferred representation for CNF formulas
- Let F be a fixed field. Let $A \equiv \bigwedge_{i=1}^{r} C_i$ be an unsatisfiable CNF formula. A Nullstellensatz refutation of A, using canonical representation q_a, is given by

$$1 = \sum_{i=1}^{m} q_{C_i} \cdot g_i + \sum_{i=1}^{n} (x_i^2 - x_i) \cdot h_i$$

- The degree of the refutation is $max\{deg(q_{C_i} \cdot g_i) : 1 \leq i \leq m\}$.

The canonical polynomial q_A

FALSE	1
TRUE	0
x_i	$1 - x_i$
$\neg A$	$1 - A$
$A \wedge B$	$A + B - A \cdot B$
$A \vee B$	$A \cdot B$

The canonical polynomial q_A

FALSE	1
TRUE	0
x_i	$1-x_i$
$\neg A$	$1-A$
$A \wedge B$	$A+B-A\cdot B$
$A \vee B$	$A \cdot B$

Example: $\neg\mathrm{PHP}_1^2$ in CNF

$p_{1,1} \wedge p_{2,1} \wedge (\neg p_{1,1} \vee \neg p_{2,1})$

$$q_1 = 1 - x_{1,1}$$
$$q_2 = 1 - x_{2,1}$$
$$q_3 = x_{1,1}x_{2,1}$$

The canonical polynomial q_A

FALSE	1
TRUE	0
x_i	$1 - x_i$
$\neg A$	$1 - A$
$A \wedge B$	$A + B - A \cdot B$
$A \vee B$	$A \cdot B$

Example: $\neg\mathrm{PHP}^2_1$ in CNF

$$p_{1,1} \wedge p_{2,1} \wedge (\neg p_{1,1} \vee \neg p_{2,1})$$

$$q_1 = 1 - x_{1,1}$$
$$q_2 = 1 - x_{2,1}$$
$$q_3 = x_{1,1} x_{2,1}$$

The canonical polynomial q_A

FALSE	1
TRUE	0
x_i	$1 - x_i$
$\neg A$	$1 - A$
$A \wedge B$	$A + B - A \cdot B$
$A \vee B$	$A \cdot B$

Example: $\neg\mathrm{PHP}^2_1$ in CNF

$$p_{1,1} \wedge p_{2,1} \wedge (\neg p_{1,1} \vee \neg p_{2,1})$$

$$q_1 = 1 - x_{1,1}$$
$$q_2 = 1 - x_{2,1}$$
$$q_3 = x_{1,1} x_{2,1}$$

The canonical polynomial q_A

FALSE	1
TRUE	0
x_i	$1 - x_i$
$\neg A$	$1 - A$
$A \wedge B$	$A + B - A \cdot B$
$A \vee B$	$A \cdot B$

Example: $\neg \mathrm{PHP}^2_1$ in CNF

$$p_{1,1} \wedge p_{2,1} \wedge (\neg p_{1,1} \vee \neg p_{2,1})$$

$$q_1 = 1 - x_{1,1}$$
$$q_2 = 1 - x_{2,1}$$
$$q_3 = x_{1,1} x_{2,1}$$

The canonical polynomial q_A

FALSE	1
TRUE	0
x_i	$1 - x_i$
$\neg A$	$1 - A$
$A \wedge B$	$A + B - A \cdot B$
$A \vee B$	$A \cdot B$

Example: $\neg\mathrm{PHP}^2_1$ in CNF

$$p_{1,1} \wedge p_{2,1} \wedge (\neg p_{1,1} \vee \neg p_{2,1})$$

$$q_1 = 1 - x_{1,1}$$
$$q_2 = 1 - x_{2,1}$$
$$q_3 = x_{1,1} x_{2,1}$$

- A valid refutation is given by:

$$1 = q_1 \cdot x_{2,1} + q_2 \cdot 1 + q_3 \cdot 1$$

Automatizablity

- Let F be a finite field. The degree d bounded Nullstellensatz system over F is automatizable.

Automatizablity

- Let F be a finite field. The degree d bounded Nullstellensatz system over F is automatizable.

- There is a polynomial time algorithm, which given polynomial $p_1,\dots,p_k \in F[x_1,\dots,x_n]$, outputs polynomials $g_i,\dots,g_m,h_i,\dots,h_n \in F[x_1,\dots,x_n]$, such that

$$1 = \sum_{i=1}^{m} p_i \cdot g_i + \sum_{i=1}^{n} (x_i^2 - x_i) \cdot h_i$$

and

$$max\{deg(p_i \cdot g_i), deg((x_j^2 - x_j) \cdot h_i) : 1 \leq i \leq m, 1 \leq j \leq n\} \leq d$$

Proof of automatizablity (1)

- For each subset r of $\{1, \ldots, n\}$, let x_r denote the multilinear power product $\prod_{i \in r} x_i$ where if $r = \emptyset$, then $x_r = 1$.

Proof of automatizablity (1)

- For each subset r of $\{1, ..., n\}$, let x_r denote the multilinear power product $\prod_{i \in r} x_i$ where if $r = \emptyset$, then $x_r = 1$.
- Let $P_{\leq d}(\{1, ..., n\})$ denote the collection of subsets of $\{1, ..., n\}$ of size at most d.

Proof of automatizablity (1)

- For each subset r of $\{1,\ldots,n\}$, let x_r denote the multilinear power product $\prod_{i\in r} x_i$ where if $r=\emptyset$, then $x_r = 1$.
- Let $P_{\leq d}(\{1,\ldots,n\})$ denote the collection of subsets of $\{1,\ldots,n\}$ of size at most d.
- Assume that there exists a degree d Nullstellensatz refutation of $p_1,\ldots,p_k$ over field F.

Proof of automatizablity (2)

- It follows that there exists $a_{i,r} \in F$, for $1 \leq i \leq m$, and $b_{j,r} \in F$, for $1 \leq j \leq n$, such that

$$1 = \sum_{i=1}^{m} \left(p_i \cdot \sum_r a_{i,r} x_r \right) + \sum_{i=1}^{n} \left((x_i^2 - x_i) \cdot \sum_r b_{j,r} x_r \right)$$

Where r varies over $P_{\leq d}(\{1, \ldots, n\})$.

Proof of automatizablity (2)

- It follows that there exists $a_{i,r} \in F$, for $1 \leq i \leq m$, and $b_{j,r} \in F$, for $1 \leq j \leq n$, such that

$$1 = \sum_{i=1}^{m} \left(p_i \cdot \sum_r a_{i,r} x_r \right) + \sum_{i=1}^{n} \left((x_i^2 - x_i) \cdot \sum_r b_{j,r} x_r \right)$$

  Where r varies over $P_{\leq d}(\{1, \ldots, n\})$.

- Results in a set of linear equations, one for each $r \in P_{\leq d}(\{1, \ldots, n\})$.

Proof of automatizablity (3)

- By polynomial time Gaussian elimination over F we can solve $a_{i,r}$ and $b_{j,r}$ to determine:

$$g_i = \sum_r a_{i,r} x_r$$

$$h_j = \sum_r b_{j,r} x_r$$

Conclusion

- If $P \neq NP$ the degree of Nullstellensatz refutations is not bounded by a constant.

Conclusion

- If $P \neq NP$ the degree of Nullstellensatz refutations is not bounded by a constant.
- The book does not proof the actual lowerbound as it continous to discuss *polynomial calculus (PC)* which polynomially simulates the Nullstellensatz System *(NS)* and is strictly stronger.

Questions?