When Hilbert approximates: A Strong Nullstellensatz for Approximate Polynomial Satisfiability

Sanyam Agarwal
Saarland University

Sagnik Dutta
MPI for Informatics

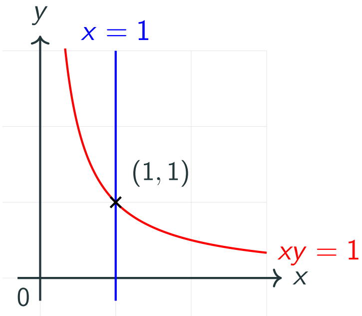
Anurag Pandey
Saarland University

Himanshu Shukla
University of Regensburg

Exact Polynomial Satisfiability

Let $f = x - 1$ and $g = xy - 1$.

Common root at $(1, 1)$.

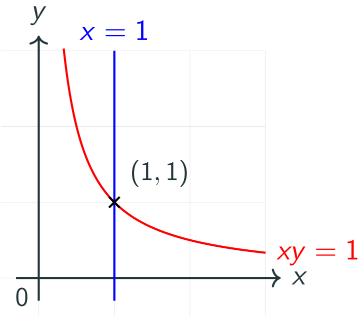


Exact Polynomial Satisfiability

Let $f = x - 1$ and $g = xy - 1$.

Common root at $(1, 1)$.

Alternative formulation:
$0 \in \mathrm{Im}(\phi)$ where $\phi = (f, g)$.



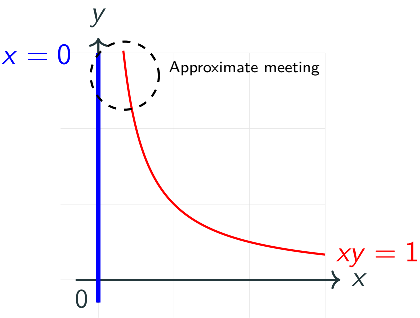
Approximate Polynomial Satisfiability (APS)

Let $f = x$ and $g = xy - 1$.

No common root.

But if we allow values in $\mathbb{C}(\epsilon)$:

$$x = \epsilon, y = \frac{1}{\epsilon}$$
$$\implies f, g = 0 \mod \epsilon.$$



Approximate Polynomial Satisfiability (APS)

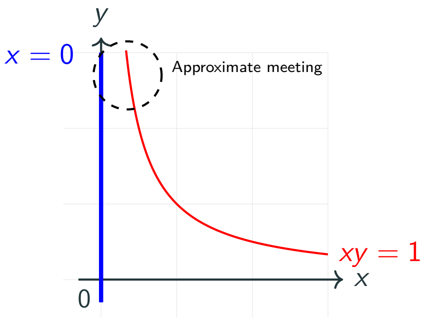
Let $f = x$ and $g = xy - 1$.

No common root.

But if we allow values in $\mathbb{C}(\epsilon)$:

$$x = \epsilon, y = \frac{1}{\epsilon}$$
$$\implies f, g = 0 \mod \epsilon.$$

Alternative formulation (GSS'18):
$0 \in \overline{\mathrm{Im}(\phi)}$ where $\phi = (f, g)$.



Vanishing Sets

For $\boldsymbol{f} = (f_1, \ldots, f_m) \in \mathbb{C}[x_1, \ldots, x_n]$, define

Exact vanishing set

$$V(\boldsymbol{f}) := \{a \in \mathbb{C}^n \mid f_i(a) = 0 \ \forall i\}.$$

Approximative vanishing set

$$\mathrm{AV}(\boldsymbol{f}) := \left\{\beta \in \mathbb{C}(\varepsilon)^n : f_i(\beta) = \varepsilon \frac{p_{i,\beta}(\varepsilon)}{q_{i,\beta}(\varepsilon)},\ q_{i,\beta}(0) \neq 0 \ \forall i\right\}.$$

$\longrightarrow \lim_{\varepsilon \to 0} f_i(\beta) = 0 \ \forall i$

Vanishing Sets

For $\boldsymbol{f} = (f_1, \ldots, f_m) \in \mathbb{C}[x_1, \ldots, x_n]$, define

Exact vanishing set

$$V(\boldsymbol{f}) := \{a \in \mathbb{C}^n \mid f_i(a) = 0 \ \forall i\}.$$

Approximative vanishing set

$$\mathrm{AV}(\boldsymbol{f}) := \left\{ \beta \in \mathbb{C}(\varepsilon)^n : f_i(\beta) = \varepsilon \frac{p_{i,\beta}(\varepsilon)}{q_{i,\beta}(\varepsilon)},\ q_{i,\beta}(0) \neq 0 \ \forall i \right\}.$$

$\longrightarrow \lim_{\varepsilon \to 0} f_i(\beta) = 0 \ \forall i$

- APS asks whether $\mathrm{AV}(\boldsymbol{f})$ is non-empty.
- This captures "border" phenomena: limits of polynomial maps and border complexity.

Known starting point: Weak Approximative Nullstellensatz

Definition

Let $A(y_1, \ldots, y_m)$ be an annihilator of $\boldsymbol{f}$ if

$$A(f_1, \ldots, f_m) = 0.$$

Known starting point: Weak Approximative Nullstellensatz

Definition

Let $A(y_1, \dots, y_m)$ be an annihilator of $\boldsymbol{f}$ if

$$A(f_1, \dots, f_m) = 0.$$

Theorem (GSS'18)

$$\mathrm{AV}(f_1, \dots, f_m) = \emptyset$$
$$\iff \exists \textit{ annihilator } A \textit{ of } f \textit{ with constant term } 1.$$

Known starting point: Weak Approximative Nullstellensatz

Definition

Let $A(y_1, \ldots, y_m)$ be an annihilator of $\boldsymbol{f}$ if

$$A(f_1, \ldots, f_m) = 0.$$

Theorem (GSS'18)

$$\mathrm{AV}(f_1, \ldots, f_m) = \emptyset$$

$\iff \exists$ *annihilator A of f with constant term* 1.

Classical WHN:

$$V(\boldsymbol{f}) = \emptyset$$

$$\iff 1 \in \langle f_1, \ldots, f_m \rangle.$$

Approximate analog (WAN):

$$\mathrm{AV}(\boldsymbol{f}) = \emptyset$$

$\iff \exists$ constant-1 annihilator.

Central Question

Classical Strong Hilbert's Nullstellensatz answers containment:

$$V(f_1, \dots, f_m) \subseteq V(g) \iff \exists r \in \mathbb{N},\ g^r = \sum_{i=1}^{m} f_i h_i$$

$$\text{for some } h_1, \dots, h_m \in \mathbb{C}[x_1, \dots, x_n]$$

$$\iff g \in \operatorname{rad}(\langle f_1, \dots, f_m \rangle).$$

Central Question

Classical Strong Hilbert's Nullstellensatz answers containment:

$$V(f_1,\dots,f_m)\subseteq V(g) \iff \exists r\in\mathbb{N},\ g^r=\sum_{i=1}^{m} f_i h_i$$

$$\text{for some } h_1,\dots,h_m\in\mathbb{C}[x_1,\dots,x_n]$$

$$\iff g\in \mathrm{rad}(\langle f_1,\dots,f_m\rangle).$$

Approximate containment problem

Given $f_1,\dots,f_m,g\in\mathbb{C}[x_1,\dots,x_n]$, decide whether

$$\mathrm{AV}(f_1,\dots,f_m)\subseteq\mathrm{AV}(g).$$

Equivalently: every infinitesimal solution of f also makes g vanish infinitesimally.

Main theorem: Strong Approximative Nullstellensatz

Theorem (SAN)

$$\mathrm{AV}(g) \supseteq \mathrm{AV}(f_1, \ldots, f_m) \iff \exists r \in \mathbb{N},\ g^r = \sum_{i=0}^{r-1} \frac{F_i(f_1,\ldots,f_m)}{1+G_i(f_1,\ldots,f_m)}\, g^i$$

where $F_i, G_i \in \mathbb{C}[y_1, \ldots, y_m]$ *are constant-free.*

Main theorem: Strong Approximative Nullstellensatz

Theorem (SAN)

$$\mathrm{AV}(g) \supseteq \mathrm{AV}(f_1, \ldots, f_m) \iff \exists r \in \mathbb{N},\ g^r = \sum_{i=0}^{r-1} \frac{F_i(f_1,\ldots,f_m)}{1+G_i(f_1,\ldots,f_m)}\, g^i$$

where $F_i, G_i \in \mathbb{C}[y_1, \ldots, y_m]$ are constant-free.

Let $R = \mathbb{C}[f_1, \ldots, f_m]$, $\mathfrak{m} = \langle f_1, \ldots, f_m \rangle \subset R$,
$S = R \setminus \mathfrak{m}$, $R_{\mathfrak{m}} = S^{-1}R$.

Theorem (Alternate formulation)

$\mathrm{AV}(f_1, \ldots, f_m) \subseteq \mathrm{AV}(g) \iff$ *g is integral over $\mathfrak{m}R_{\mathfrak{m}}$.*

Main theorem: Strong Approximative Nullstellensatz

Theorem (SAN)

$$\mathrm{AV}(g) \supseteq \mathrm{AV}(f_1, \ldots, f_m) \iff \exists r \in \mathbb{N},\ g^r = \sum_{i=0}^{r-1} \frac{F_i(f_1,\ldots,f_m)}{1+G_i(f_1,\ldots,f_m)}\, g^i$$

where $F_i, G_i \in \mathbb{C}[y_1, \ldots, y_m]$ are constant-free.

Let $R = \mathbb{C}[f_1, \ldots, f_m]$, $\mathfrak{m} = \langle f_1, \ldots, f_m \rangle \subset R$,
$S = R \setminus \mathfrak{m}$, $R_{\mathfrak{m}} = S^{-1}R$.

Theorem (Alternate formulation)

$\mathrm{AV}(f_1, \ldots, f_m) \subseteq \mathrm{AV}(g) \iff$ *g is integral over $\mathfrak{m}R_{\mathfrak{m}}$.*

Takeaway: From radicals, we shift to the new algebraic object of **integral closure** over a localized ideal.

Example

Let

$$f_1 = xy^2 - y + x^2 y, \qquad f_2 = xy - 1, \qquad g = x.$$

At first glance, $\mathrm{AV}(f_1, f_2) \subseteq \mathrm{AV}(g)$ is not obvious.

Example

Let

$$f_1 = xy^2 - y + x^2y, \qquad f_2 = xy - 1, \qquad g = x.$$

At first glance, $\mathrm{AV}(f_1, f_2) \subseteq \mathrm{AV}(g)$ is not obvious.

SAN gives a *short certificate*:

$$g^2 = \frac{f_1}{1 + f_2}\, g - f_2.$$

Equivalence of WHN and SHN

Rabinowitsch's Trick

Over algebraically closed field k,

$$V(g) \supseteq V(f_1, \ldots, f_m) \iff V(f_1, \ldots, f_m, 1 - gy) = \emptyset.$$

Intuitively: g vanishes with f if and only if $1 - yg$ doesn't vanish simultaneously.

Equivalence of WHN and SHN

Rabinowitsch's Trick

Over algebraically closed field k,

$$V(g) \supseteq V(f_1, \ldots, f_m) \iff V(f_1, \ldots, f_m, 1 - gy) = \emptyset.$$

Intuitively: g vanishes with f if and only if $1 - yg$ doesn't vanish simultaneously.

- $V(f_1, \ldots, f_m, 1 - gy) = \emptyset$
  $\iff 1 = \sum_{i=1}^{m} f_i(\mathbf{x}) h_i(\mathbf{x}, y) + (1 - gy) h_{m+1}(\mathbf{x}, y).$

Equivalence of WHN and SHN

Rabinowitsch's Trick

Over algebraically closed field k,

$$V(g) \supseteq V(f_1, \ldots, f_m) \iff V(f_1, \ldots, f_m, 1 - gy) = \emptyset.$$

Intuitively: g vanishes with f if and only if $1 - yg$ doesn't vanish simultaneously.

- $V(f_1, \ldots, f_m, 1 - gy) = \emptyset$
  $\iff 1 = \sum_{i=1}^{m} f_i(\mathbf{x}) h_i(\mathbf{x}, y) + (1 - gy) h_{m+1}(\mathbf{x}, y)$.
- Set $y = 1/g$ in $k(\mathbf{x})[y]$ and cancel denominators to get $g^r \in \langle f_1, \ldots, f_m \rangle$.

Equivalence of WHN and SHN

Rabinowitsch's Trick

Over algebraically closed field k,

$$V(g) \supseteq V(f_1, \ldots, f_m) \iff V(f_1, \ldots, f_m, 1 - gy) = \emptyset.$$

Intuitively: g vanishes with f if and only if $1 - yg$ doesn't vanish simultaneously.

- $V(f_1, \ldots, f_m, 1 - gy) = \emptyset$
  $\iff 1 = \sum_{i=1}^{m} f_i(\mathbf{x}) h_i(\mathbf{x}, y) + (1 - gy) h_{m+1}(\mathbf{x}, y).$
- Set $y = 1/g$ in $k(\mathbf{x})[y]$ and cancel denominators to get $g^r \in \langle f_1, \ldots, f_m \rangle$.

WHN and SHN are also computationally equivalent.

Why classical Rabinowitsch does not transfer

g and $1 - yg$ can vanish simulataneously:

$$\text{If} \quad g(\beta) = \varepsilon \frac{p(\varepsilon)}{q(\varepsilon)}, \qquad p(\varepsilon) \neq 0$$

then choosing

$$y = \frac{q(\varepsilon)}{\varepsilon p(\varepsilon)}$$

makes $1 - yg$ vanish exactly.

Proof idea: approximate Rabinowitsch tricks

$\mathrm{AV}(\boldsymbol{f}) \subseteq \mathrm{AV}(g)$ is equivalent to two APS-infeasibility statements: whenever $\boldsymbol{f}$ goes to 0,

- g doesn't diverge, and
- g doesn't converge to a non-zero constant.

Proof idea: approximate Rabinowitsch tricks

$\mathrm{AV}(\boldsymbol{f}) \subseteq \mathrm{AV}(g)$ is equivalent to two APS-infeasibility statements: whenever $\boldsymbol{f}$ goes to 0,

- g doesn't diverge, and
- g doesn't converge to a non-zero constant.

No divergence

$f_1, \ldots, f_m, y, 1 - yg$
have no common APS.

No nonzero constant limit

$\forall c \in \mathbb{C}^\times : \quad f_1, \ldots, f_m, g - c$
have no common APS.

Flow of the proof

$f_1, \ldots, f_m, y, 1 - yg$
have no common APS

$\forall c \in \mathbb{C}^\times,$
$f_1, \ldots, f_m, g - c$
have no common APS

Goal: $g^r = \sum_{i=0}^{r} g^i F_i(\boldsymbol{f})$
for all F_i constant-free

Flow of the proof

$f_1, \ldots, f_m, y, 1 - yg$
have no common APS

$\xrightarrow{\text{WAN}}$

$A(f_1, \ldots, f_m, y, 1 - yg) = 1$

$\forall c \in \mathbb{C}^\times$,
$f_1, \ldots, f_m, g - c$
have no common APS

Goal: $g^r = \sum_{i=0}^{r} g^i F_i(\boldsymbol{f})$
for all F_i constant-free

Flow of the proof

$f_1, \ldots, f_m, y, 1 - yg$
have no common APS

$\big\downarrow$ WAN

$A(f_1, \ldots, f_m, y, 1 - yg) = 1$

$\big\downarrow$ $y = 1/g$

$g^s = \sum_{i=0}^{s} g^i Q_i(\boldsymbol{f})$
Q_s constant-free

$\forall c \in \mathbb{C}^\times$,
$f_1, \ldots, f_m, g - c$
have no common APS

Goal: $g^r = \sum_{i=0}^{r} g^i F_i(\boldsymbol{f})$
for all F_i constant-free

Flow of the proof

$f_1, \ldots, f_m, y, 1 - yg$
have no common APS

WAN

$A(f_1, \ldots, f_m, y, 1 - yg) = 1$

$y = 1/g$

$g^s = \sum_{i=0}^{s} g^i Q_i(\boldsymbol{f})$
Q_s constant-free

$\forall c \in \mathbb{C}^\times$,
$f_1, \ldots, f_m, g - c$
have no common APS

Take an annihilator
$A'(\boldsymbol{f}, g) = 0$
and rewrite it as
$B(\boldsymbol{f}, g) + Q(g) = 0.$

Goal: $g^r = \sum_{i=0}^{r} g^i F_i(\boldsymbol{f})$
for all F_i constant-free

Flow of the proof

$f_1, \ldots, f_m, y, 1 - yg$
have no common APS

$\downarrow$ WAN

$A(f_1, \ldots, f_m, y, 1 - yg) = 1$

$\downarrow$ $y = 1/g$

$g^s = \sum_{i=0}^{s} g^i Q_i(\boldsymbol{f})$
Q_s constant-free

$\forall c \in \mathbb{C}^\times$,
$f_1, \ldots, f_m, g - c$
have no common APS

Take an annihilator
$A'(\boldsymbol{f}, g) = 0$
and rewrite it as
$B(\boldsymbol{f}, g) + Q(g) = 0.$

$\downarrow$

$\forall c \in \text{Roots}(Q)$,
$f_1, \ldots, f_m, g - c$
have no common APS

Goal: $g^r = \sum_{i=0}^{r} g^i F_i(\boldsymbol{f})$
for all F_i constant-free

Flow of the proof

$f_1, \ldots, f_m, y, 1 - yg$
have no common APS

$\downarrow$ WAN

$A(f_1, \ldots, f_m, y, 1 - yg) = 1$

$\downarrow$ $y = 1/g$

$g^s = \sum_{i=0}^{s} g^i Q_i(\boldsymbol{f})$
Q_s constant-free

$\forall c \in \mathbb{C}^{\times}$,
$f_1, \ldots, f_m, g - c$
have no common APS

Take an annihilator
$A'(\boldsymbol{f}, g) = 0$
and rewrite it as
$B(\boldsymbol{f}, g) + Q(g) = 0.$

$\downarrow$

$\forall c \in \mathrm{Roots}(Q)$,
$f_1, \ldots, f_m, g - c$
have no common APS

$\downarrow$ Use WAN and combine over c

$g^k = \sum_{i=0}^{\ell} g^i F_i(\boldsymbol{f})$
all F_i constant-free

Goal: $g^r = \sum_{i=0}^{r} g^i F_i(\boldsymbol{f})$
for all F_i constant-free

Flow of the proof

$f_1, \ldots, f_m, y, 1 - yg$
have no common APS

WAN

$A(f_1, \ldots, f_m, y, 1 - yg) = 1$

$y = 1/g$

$g^s = \sum_{i=0}^{s} g^i Q_i(\boldsymbol{f})$
Q_s constant-free

$\forall c \in \mathbb{C}^\times$,
$f_1, \ldots, f_m, g - c$
have no common APS

Take an annihilator
$A'(\boldsymbol{f}, g) = 0$
and rewrite it as
$B(\boldsymbol{f}, g) + Q(g) = 0.$

$\forall c \in \mathrm{Roots}(Q)$,
$f_1, \ldots, f_m, g - c$
have no common APS

Use WAN and combine over c

$g^k = \sum_{i=0}^{\ell} g^i F_i(\boldsymbol{f})$
all F_i constant-free

algebraic manipulation

Goal: $g^r = \sum_{i=0}^{r} g^i F_i(\boldsymbol{f})$
for all F_i constant-free

Complexity of SAN

Theorem (GSS18)

WAN is in PSPACE.

Decision Problem of SAN

When the input polynomials are given by algebraic circuits, deciding whether $\mathrm{AV}(f_1, \ldots, f_m) \subseteq \mathrm{AV}(g)$.

Complexity of SAN

Theorem (GSS18)

WAN is in PSPACE.

Decision Problem of SAN

When the input polynomials are given by algebraic circuits, deciding whether $\mathrm{AV}(f_1, \ldots, f_m) \subseteq \mathrm{AV}(g)$.

Recall that WHN and SHN were computationally equivalent.

But the reduction from SAN to WAN involves roots of a univariate polynomial, which may not be computable.

Algorithmic result: SAN is in PSPACE

Theorem

SAN is in PSPACE.

Algorithmic result: SAN is in PSPACE

Theorem

SAN is in PSPACE.

We essentially prove "effective" versions of our approximate Rabinowitsch tricks using:

- annihilator degree bounds;
- GSS random reductions;

Algorithmic result: SAN is in PSPACE

Theorem

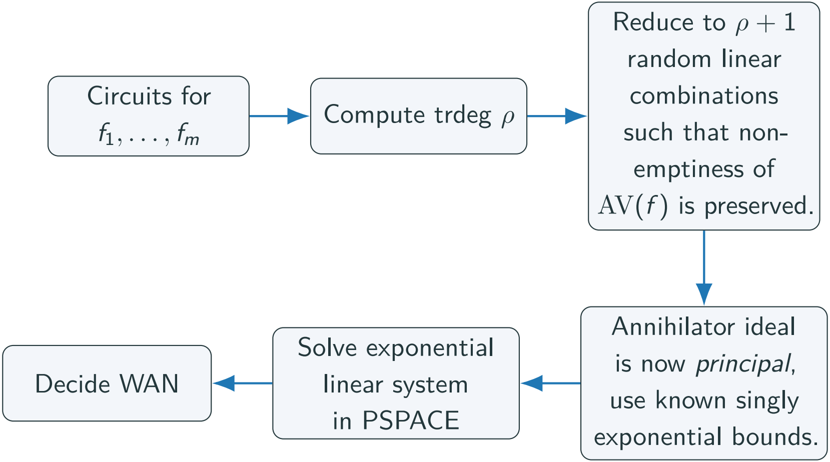
SAN is in PSPACE.

We essentially prove "effective" versions of our approximate Rabinowitsch tricks using:

- annihilator degree bounds;
- GSS random reductions;

to obtain an exponential-sized linear algebra system, which can be solved in PSPACE.

Use of GSS random reductions



We use this framework on our system of WAN-infeasibilities to get a singly exponential bound on the degree of the SAN certificate.

Conclusion and open directions

1. WAN is the weak Nullstellensatz for APS; SAN is the strong version.
2. Approximate containment is governed by integral closure over a localized ideal.
3. Despite apparent EXPSPACE barriers, SAN has a PSPACE decision algorithm.

Conclusion and open directions

1. WAN is the weak Nullstellensatz for APS; SAN is the strong version.
2. Approximate containment is governed by integral closure over a localized ideal.
3. Despite apparent EXPSPACE barriers, SAN has a PSPACE decision algorithm.

Open questions

- Define a useful notion of dimension for approximative vanishing sets.

Conclusion and open directions

1. WAN is the weak Nullstellensatz for APS; SAN is the strong version.
2. Approximate containment is governed by integral closure over a localized ideal.
3. Despite apparent EXPSPACE barriers, SAN has a PSPACE decision algorithm.

Open questions

- Define a useful notion of dimension for approximative vanishing sets.
- Can we improve complexity of WAN? Put it in CH or even PH?

Conclusion and open directions

1. WAN is the weak Nullstellensatz for APS; SAN is the strong version.
2. Approximate containment is governed by integral closure over a localized ideal.
3. Despite apparent EXPSPACE barriers, SAN has a PSPACE decision algorithm.

Open questions

- Define a useful notion of dimension for approximative vanishing sets.
- Can we improve complexity of WAN? Put it in CH or even PH?
- What about generators of the integral closure in SAN? Can we algorithmically obtain them?

Thank You!

Questions?