A Proof-Theoretic Approach to Nullstellensatz-type results

John Harrison

Intel Corporation

“Methods of Proof Theory in Mathematics”, MPI Bonn

Fri 8th June 2007

Inspirations

- Lombardi, “Effective real nullstellensatz and variants”, MEGA 1990
- Lifschitz, “Semantical Completeness Theorems in Logic and Algebra”, Proceedings of the AMS 1980
- Simmons, “The solution of a decision problem for several classes of rings”, Pacific Journal of Mathematics 1970

Objectives

- Don’t necessarily want completely constructive proofs. (We’ll be using other algorithms anyway to find certificates.)
- Want proofs that are conceptually simple (if you know some very basic logic)
- Want to emphasize links with word problems rather than algebraic geometry

The word problem for rings

We want to decide whether

$$\forall \overline{x}.\ s_1 = t_1 \wedge \cdots \wedge s_n = t_n \Rightarrow s = t$$

holds in all rings (uniform word problem). We can assume it's a standard polynomial form

$$\forall \overline{x}.\ p_1(\overline{x}) = 0 \wedge \cdots \wedge p_n(\overline{x}) = 0 \Rightarrow q(\overline{x}) = 0$$

Solution

$$\forall \overline{x}.\ p_1(\overline{x}) = 0 \wedge \cdots \wedge p_n(\overline{x}) = 0 \Rightarrow q(\overline{x}) = 0$$

holds in all rings iff

$$q \in \mathsf{Id}_{\mathbb{Z}} \langle p_1, \ldots, p_n \rangle$$

i.e. there exist ‘cofactor’ polynomials with integer coefficients such that

$$p_1 \cdot q_1 + \cdots + p_n \cdot q_n = q$$

Proof (model-theoretic)

If

$$p_1 \cdot q_1 + \cdots + p_n \cdot q_n = q$$

then whenever each $p_i(\overline{x}) = 0$, we must have $q(\overline{x}) = 0$.

Conversely if

$$q \notin \mathsf{Id}_{\mathbb{Z}} \langle p_1, \ldots, p_n \rangle$$

then the quotient ring $\mathbb{Z}[\overline{x}]/\mathsf{Id}_{\mathbb{Z}} \langle p_1, \ldots, p_n \rangle$ is a ring where each $p_i(\overline{x}) = 0$ but some $q(\overline{x}) \neq 0$.

Axioms for rings

$$x + y = y + x$$

$$x + (y + z) = (x + y) + z$$

$$x + 0 = x$$

$$x + (-x) = 0$$

$$x \cdot y = y \cdot x$$

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$x \cdot 1 = x$$

$$x \cdot (y + z) = x \cdot y + x \cdot z$$

Axioms for equality

We want to consider proofs in pure first order logic, without equality, so axiomatize it:

$$x = x$$

$$x = y \Rightarrow y = x$$

$$x = y \wedge y = z \Rightarrow x = z$$

$$x = x' \Rightarrow -x = -x'$$

$$x = x' \wedge y = y' \Rightarrow x + y = x' + y'$$

$$x = x' \wedge y = y' \Rightarrow x \cdot y = x' \cdot y'$$

Proofs in the theory of rings

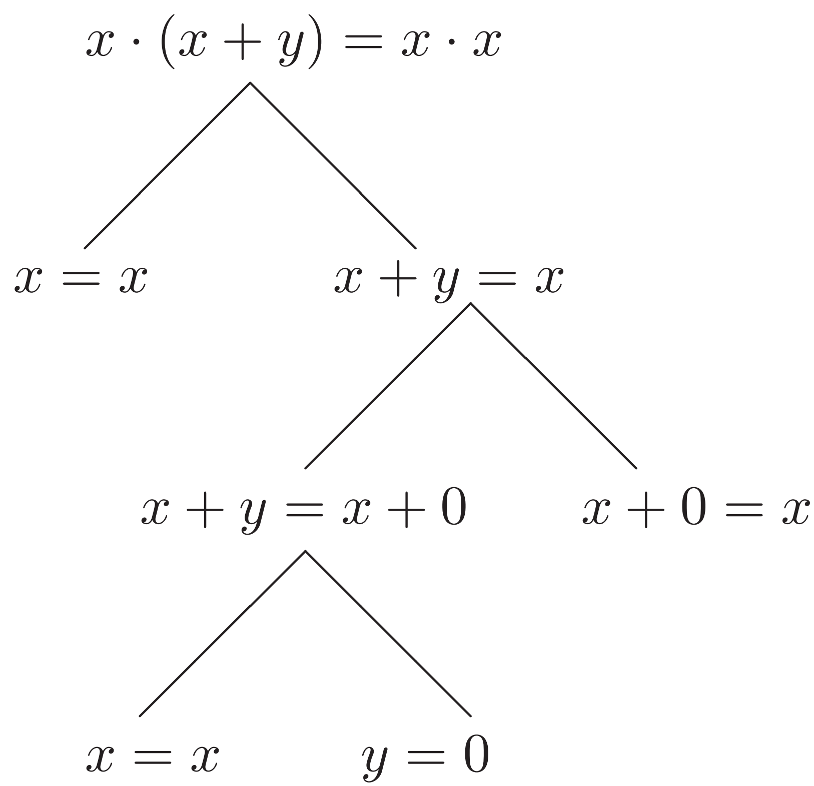
Let Ring be all the ring axioms and equality axioms.

A formula ϕ holds in all rings iff Ring $\vdash \phi$.

NB: all the axioms in Ring are Horn clauses.

So if there's a proof of Ring $\vdash \phi$ there's a Prolog-style proof tree.

Prolog-style proof tree



Alternative proof

By induction on such a proof, for each equation $s = t$ deduced, $(s - t) \in \mathrm{Id}_{\mathbb{Z}} \langle s_1 - t_1, \ldots, s_n - t_n \rangle$ where the $s_i = t_i$ are the hypotheses.

Alternative proof

By induction on such a proof, for each equation $s = t$ deduced, $(s - t) \in \mathsf{Id}_{\mathbb{Z}}\langle s_1 - t_1, \ldots, s_n - t_n\rangle$ where the $s_i = t_i$ are the hypotheses.

Also, based on general convexity properties of Horn clause theories, we can decide the whole universal theory of rings since

$$\mathsf{Ring} \vdash p_1 = 0 \wedge \cdots \wedge p_n = 0 \Rightarrow q_1 = 0 \vee \cdots \vee q_m = 0$$

iff for some $1 \leq i \leq m$ we have

$$\mathsf{Ring} \vdash p_1 = 0 \wedge \cdots \wedge p_n = 0 \Rightarrow q_i = 0$$

Generalizes to torsion-free rings

Torsion-free ring axioms are

$$\text{TFRing} = \text{Ring} \cup \{\overbrace{x + \cdots + x}^{n \text{ times}} = 0 \Rightarrow x = 0 \mid n \in \mathbb{N}^+\}$$

Generalizes to torsion-free rings

Torsion-free ring axioms are

$$\text{TFRing} = \text{Ring} \cup \{\overbrace{x + \cdots + x}^{n \text{ times}} = 0 \Rightarrow x = 0 \mid n \in \mathbb{N}^{+}\}$$

By an almost identical induction on proofs

$$\text{TFRing} \vdash p_1 = 0 \land \cdots \land p_n = 0 \Rightarrow q = 0$$

iff

$$q \in \text{Id}_{\mathbb{Q}} \langle p_1, \ldots, p_n \rangle$$

Generalizes to linear existential theorems

$$\text{Ring} \vdash \forall \overline{x}. \bigwedge_{i=1}^{m} e_i(\overline{x}) = 0 \Rightarrow \exists y_1 \ \cdots \ y_n. \ p_1(\overline{x})y_1 + \cdots + p_n(\overline{x})y_n = a(\overline{x})$$

iff (Horn-Herbrand) there are terms in the language of rings s.t.

$$\text{Ring} \vdash \forall \overline{x}. \bigwedge_{i=1}^{m} e_i(\overline{x}) = 0 \Rightarrow \ p_1(\overline{x})t_1(\overline{x}) + \cdots + p_n(\overline{x})t_n(\overline{x}) = a(\overline{x})$$

iff (previous theorem)

$$a \in \text{Id}_{\mathbb{Z}} \langle e_1, \ldots, e_m, p_1, \ldots, p_n \rangle$$

. . . and simultaneous linear existentials

$$\text{Ring} \vdash \forall \overline{x}.\ \bigwedge_{i=1}^{m} e_i(\overline{x}) = 0 \Rightarrow \exists y_1 \ \cdots \ y_n.\ \begin{array}{l} p_{11}(\overline{x})y_1 + \cdots + p_{1n}(\overline{x})y_n = a_1(\overline{x}) \wedge \\ \cdots \wedge \\ p_{k1}(\overline{x})y_1 + \cdots + p_{kn}(\overline{x})y_n = a_k(\overline{x}) \end{array}$$

iff

$$(a_1 u_1 + \cdots + a_k u_k)$$
$$\in \text{Id}_{\mathbb{Z}} \langle e_1, \ldots, e_m, (p_{11}u_1 + \cdots + p_{k1}u_k), (p_{1n}u_1 + \cdots + p_{kn}u_k) \rangle$$

where the u_i are fresh variables.

Application to automated reasoning

Eliminate divisibility notions in terms of existentials:

- $s \mid t$ to $\exists d.\ t = sd$
- $s \equiv t \pmod{u}$ to $\exists d.\ t - s = ud$
- $\mathrm{coprime}(s, t)$ to $\exists x\ y.\ sx + ty = 1$.

Many basic facts about divisibility can be automatically reduced to ideal membership problems.

Examples

$$d|a \wedge d|b \Rightarrow d|(a-b)$$

$$\text{coprime}(d,a) \wedge \text{coprime}(d,b) \Rightarrow \text{coprime}(d,ab)$$

$$\text{coprime}(d,ab) \Rightarrow \text{coprime}(d,a)$$

$$\text{coprime}(a,b) \wedge x \equiv y \pmod{a} \wedge x \equiv y \pmod{b} \Rightarrow x \equiv y \pmod{(ab)}$$

$$m|r \wedge n|r \wedge \text{coprime}(m,n) \Rightarrow (mn)|r$$

$$\text{coprime}(xy, x^2+y^2) \Leftrightarrow \text{coprime}(x,y)$$

$$\text{coprime}(a,b) \Rightarrow \exists x.\ x \equiv u \pmod{a} \wedge x \equiv v \pmod{b}$$

$$ax \equiv ay \pmod{n} \wedge \text{coprime}(a,n) \Rightarrow x \equiv y \pmod{n}$$

$$\gcd(a,n) \mid b \Rightarrow \exists x.\ ax \equiv b \pmod{n}$$

Integral domains

$$\text{ID} = \text{Ring} \cup \{x \cdot y = 0 \Rightarrow x = 0 \vee y = 0\} \cup \{\neg(1 = 0)\}$$

The nontriviality axiom isn't that important, since word problems are always true in the trivial ring.

Integral domains

$$\text{ID} = \text{Ring} \cup \{x \cdot y = 0 \Rightarrow x = 0 \lor y = 0\} \cup \{\neg(1 = 0)\}$$

The nontriviality axiom isn't that important, since word problems are always true in the trivial ring.

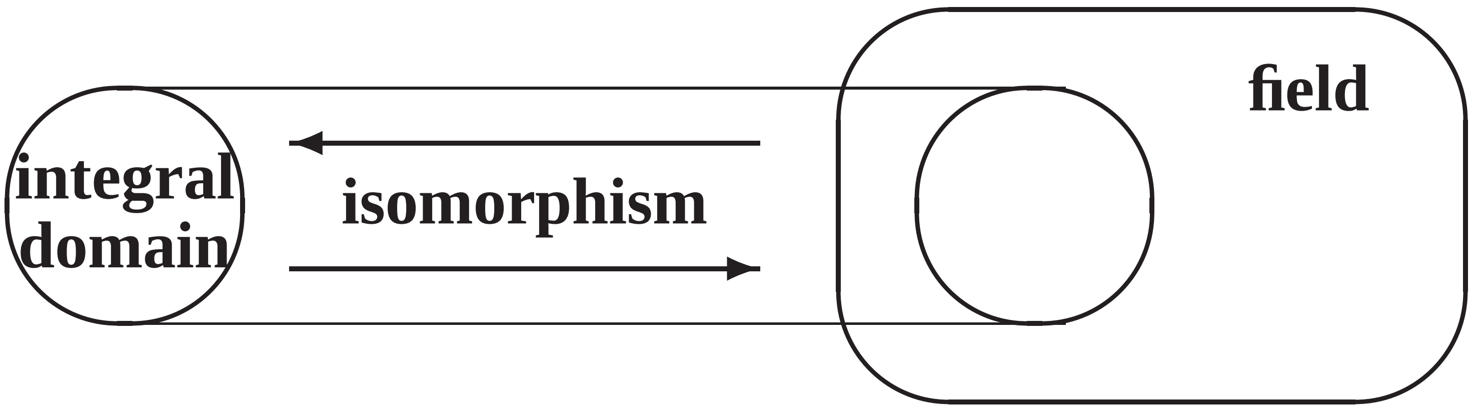
Solving the word problem is again equivalent to solving the entire universal theory of integral domains, though for a different reason:

$$\text{ID} \vdash p_1 = 0 \land \cdots \land p_n = 0 \Rightarrow q_1 = 0 \lor \cdots \lor q_m = 0$$

iff

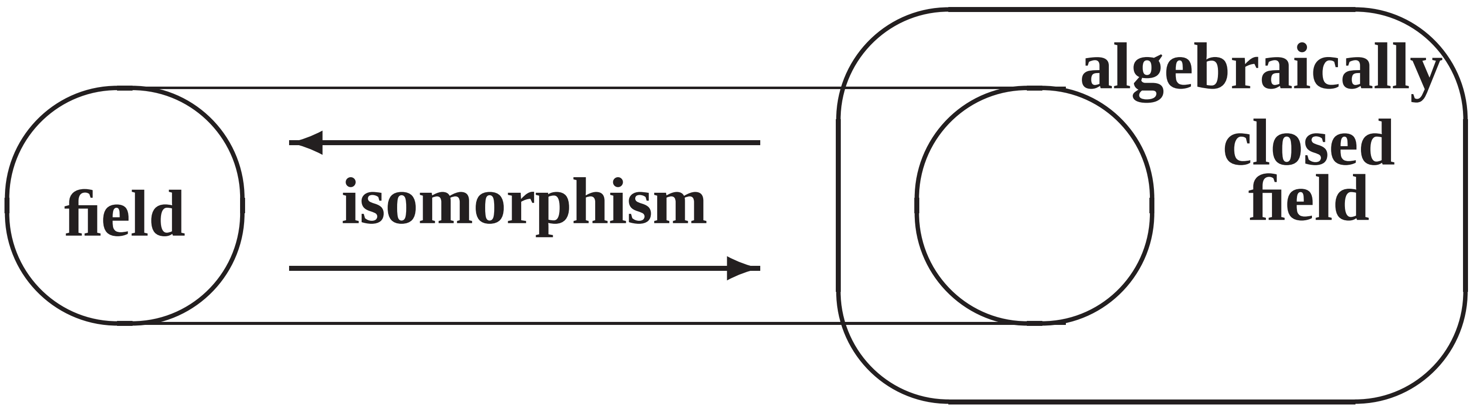
$$\text{ID} \vdash p_1 = 0 \land \cdots \land p_n = 0 \Rightarrow q_1 \cdots q_m = 0$$

Embedding in field of fractions



Universal formula in the language of rings holds in all integral domains [of characteristic p] iff it holds in all fields [of characteristic p].

Embedding in algebraic closure



Universal formula in the language of rings holds in all fields [of characteristic p] iff it holds in all algebraically closed fields [of characteristic p]

Connection to the Nullstellensatz

Also, algebraically closed fields of the same characteristic are elementarily equivalent.

For a universal formula in the language of rings, all these are equivalent:

- It holds in all integral domains of characteristic 0
- It holds in all fields of characteristic 0
- It holds in all algebraically closed fields of characteristic 0
- It holds in any given algebraically closed field of characteristic 0
- It holds in $\mathbb{C}$

Penultimate case is basically the Hilbert Nullstellensatz.

Choice of proof system

The key integral domain axiom is non-Horn, so we can no longer use Prolog-style proofs.

Lifschitz uses hyperresolution proofs in a sharp canonical form, and gets a similar argument.

We consider refutation proofs using simple binary resolution.

Assume that all axioms are instantiated first (Herbrand) so we just need to consider propositional resolution

Resolution

Propositional resolution is the rule:

$$\frac{p \lor A \quad \neg p \lor B}{A \lor B}$$

Resolution

Propositional resolution is the rule:

$$\frac{p \vee A \quad \neg p \vee B}{A \vee B}$$

We consider the disjunctions as multisets, not sets, so we need a "factoring" rule:

$$\frac{p \vee p \vee A}{p \vee A}$$

For example, an instance of the integral domain axiom is $\neg(x^2 = 0) \vee x = 0 \vee x = 0$ and a factoring step gives $\neg(x^2 = 0) \vee x = 0$

Refutation completeness

Resolution is not complete: can't deduce $p \lor q$ from p

However, it's refutation complete, so if a set of clauses is inconsistent, one can derive the empty disjunction $\bot$

Proof is an easy induction on the number of variables occurring both positively and negatively.

Main induction hypothesis

Consider resolution refutations with axioms

$$\mathsf{ID} \cup \{p_1 = 0, \ldots, p_n = 0\} \cup \{q_1 \neq 0, \ldots, q_m \neq 0\}$$

For every clause deduced of the form

$$\bigvee_{i=1}^{r} e_i \neq 0 \vee \bigvee_{j=1}^{s} f_j = 0$$

there is some integer $k \geq 0$ such that

$$((\prod_{i=1}^{m} q_i)(\prod_{j=1}^{s} f_j))^k \in \mathsf{Id}_{\mathbb{Z}} \langle e_1, \ldots, e_r, p_1, \ldots, p_n \rangle$$

Proof for the axioms

Easy to establish for the axioms, e.g. the congruence for equality:

$$x = x' \wedge y = y' \Rightarrow x \cdot y = x' \cdot y'$$

where it suffices to show

$$(x \cdot y - x' \cdot y') \in \mathsf{Id}_{\mathbb{Z}} \langle x - x', y - y', p_1, \ldots, p_n \rangle$$

which is true since

$$x \cdot y - x' \cdot y' = y \cdot (x - x') + x' \cdot (y - y')$$

Proof for factoring

Factoring two instances of a of a negated equation

$$\frac{\neg(e = 0) \vee \neg(e = 0) \vee \Gamma}{\neg(e = 0) \vee \Gamma}$$

is trivial since $\text{Id}_{\mathbb{Z}} \langle e, e, \ldots \rangle$ is the same as $\text{Id}_{\mathbb{Z}} \langle e, \ldots \rangle$.

Proof for factoring

Factoring two instances of a of a negated equation

$$\frac{\neg(e = 0) \vee \neg(e = 0) \vee \Gamma}{\neg(e = 0) \vee \Gamma}$$

is trivial since $\mathsf{Id}_{\mathbb{Z}} \langle e, e, \ldots \rangle$ is the same as $\mathsf{Id}_{\mathbb{Z}} \langle e, \ldots \rangle$.

Consider now factoring a positive equation

$$\frac{f = 0 \vee f = 0 \vee \Gamma}{f = 0 \vee \Gamma}$$

By the inductive hypothesis we have $(p \cdot f \cdot f)^k \in I$, so $(p \cdot f)^{2k} \in I$

Proof for resolution (1)

$$\frac{e \neq 0 \vee \bigvee_{i=1}^{r} e_i \neq 0 \vee \bigvee_{j=1}^{s} f_j = 0 \qquad e = 0 \vee \bigvee_{i=1}^{t} g_i \neq 0 \vee \bigvee_{j=1}^{u} h_j = 0}{\bigvee_{i=1}^{r} e_i \neq 0 \vee \bigvee_{i=1}^{t} g_i \neq 0 \vee \bigvee_{j=1}^{s} f_j = 0 \vee \bigvee_{j=1}^{u} h_j = 0}$$

By the inductive hypothesis, for some $k \geq 0$, $l \geq 0$

$$(QF)^k \in \mathsf{Id}_{\mathbb{Z}} \langle e, e_1, \ldots, e_r, p_1, \ldots, p_n \rangle$$
$$(QeH)^l \in \mathsf{Id}_{\mathbb{Z}} \langle g_1, \ldots, g_t, p_1, \ldots, p_n \rangle$$

where $Q = \prod_{i=1}^{m} q_i$, $F = \prod_{j=1}^{s} f_j$ and $H = \prod_{j=1}^{u} h_j$.

Proof for resolution (1)

$$\frac{e \neq 0 \vee \bigvee_{i=1}^{r} e_i \neq 0 \vee \bigvee_{j=1}^{s} f_j = 0 \quad e = 0 \vee \bigvee_{i=1}^{t} g_i \neq 0 \vee \bigvee_{j=1}^{u} h_j = 0}{\bigvee_{i=1}^{r} e_i \neq 0 \vee \bigvee_{i=1}^{t} g_i \neq 0 \vee \bigvee_{j=1}^{s} f_j = 0 \vee \bigvee_{j=1}^{u} h_j = 0}$$

By the inductive hypothesis, for some $k \geq 0$, $l \geq 0$

$$(QF)^k \in \mathsf{Id}_{\mathbb{Z}} \langle e, e_1, \ldots, e_r, p_1, \ldots, p_n \rangle$$

$$(QeH)^l \in \mathsf{Id}_{\mathbb{Z}} \langle g_1, \ldots, g_t, p_1, \ldots, p_n \rangle$$

where $Q = \prod_{i=1}^{m} q_i$, $F = \prod_{j=1}^{s} f_j$ and $H = \prod_{j=1}^{u} h_j$. Write first as:

$$(QF)^k - re \in \mathsf{Id}_{\mathbb{Z}} \langle e_1, \ldots, e_r, p_1, \ldots, p_n \rangle$$

Proof for resolution (2)

Since $x^l - y^l$ is always divisible by $x - y$:

$$(QF)^{kl} - r^l e^l \in \mathsf{Id}_{\mathbb{Z}} \langle e_1, \ldots, e_r, p_1, \ldots, p_n \rangle$$

Use closure under multiplication:

$$(QF)^{kl}(QH)^l - r^l (QeH)^l \in \mathsf{Id}_{\mathbb{Z}} \langle e_1, \ldots, e_r, p_1, \ldots, p_n \rangle$$

Use second part of inductive hypothesis:

$$(QF)^{kl}(QH)^l \in \mathsf{Id}_{\mathbb{Z}} \langle e_1, \ldots, e_r, g_1, \ldots, g_t, p_1, \ldots, p_n \rangle$$

Use closure under multiplication:

$$(QFH)^{kl+l} \in \mathsf{Id}_{\mathbb{Z}} \langle e_1, \ldots, e_r, g_1, \ldots, g_t, p_1, \ldots, p_n \rangle$$

The Nullstellensatz

In the case of the empty clause we deduce:

$$\mathsf{ID} \vdash \forall \overline{x}.\, p_1(\overline{x}) = 0 \wedge \cdots \wedge p_n(\overline{x}) = 0 \Rightarrow q_1(\overline{x}) = 0 \vee \cdots \vee q_m(\overline{x}) = 0$$

iff there is a nonnegative integer k with

$$(\prod_{i=1}^{m} q_i)^k \in \mathsf{Id}_{\mathbb{Z}} \langle p_1, \ldots, p_n \rangle$$

In the special case of the word problem:

$$p_1 = 0 \wedge \cdots \wedge p_n = 0 \Rightarrow q = 0$$

iff there is a nonnegative integer k with

$$q^k \in \mathsf{Id}_{\mathbb{Z}} \langle p_1, \ldots, p_n \rangle$$

Other variants

$$p_1 = 0 \wedge \cdots \wedge p_n = 0 \Rightarrow q = 0$$

holds in

- All integral domains / fields / algebraically closed fields iff some $q^k \in \mathsf{Id}_{\mathbb{Z}} \langle p_1, \ldots, p_n \rangle$
- All integral domains / fields / algebraically closed fields of characteristic p iff some $cq^k \in \mathsf{Id}_{\mathbb{Z}} \langle p, p_1, \ldots, p_n \rangle$ for $p \not| c$
- All integral domains / fields / algebraically closed fields of characteristic 0 iff some $cq^k \in \mathsf{Id}_{\mathbb{Z}} \langle p_1, \ldots, p_n \rangle$ for $c \neq 0$ i.e. iff $q^k \in \mathsf{Id}_{\mathbb{Q}} \langle p_1, \ldots, p_n \rangle$

The Real Nullstellensatz / Positivstellensatz

Same basic approach is workable for real-closed fields.

Every ordered integral domain can be embedded in a real-closed field.

So focus on resolution refutations in the theory of ordered rings. (Can eliminate equality in terms of ordering for simplicity.)

Details are a bit more technical but we can recover the usual Stengle Positivstellensatz.

Positivstellensatz for discrete ordered integral domains?

We can also consider *discrete* ordered integral domains, with axiom

$$x \leq y \vee y + 1 \leq x$$

Details remain to be worked out.

Maybe we can get an analog of the Stengle Positivstellensatz but with terms of the form $x^2 - x$ in place of the usual x^2.

Conclusions

- Close connection between Nullstellensatz-type results and word problems
- Easy model-theoretic embedding argument saves us from arguing about more complicated axioms
- Get one possible insight into where certain hypotheses get used and where the complexity comes from
- Some merit to the simple free-variable calculi from automated deduction
- Not clear we can get more refined forms like Schmüdgen PSatz from this kind of analysis.