

Theorem 1. *For any Horn existential second-order expression $\exists P\phi$, the problem $\exists P\phi$ -GRAPHS is in P.*

Proof

Let $\exists P\phi = \exists P\forall x_1 \dots \forall x_k \eta$

where η is the conjunction of Horn clauses and the arity of P is r .

Is there a relation $P \subseteq V^r$ such that ϕ is satisfied?

Let $V = \{1, 2, \dots, n\}$.

We can substitute all possible values of x_i in ϕ to get:

$$\bigwedge_{v_1, \dots, v_k=1}^n \eta[x_1 \leftarrow v_1, \dots, x_k \leftarrow v_k]$$

The above expression contains exactly hn^k clauses, where h is the number of clauses in η .

The atomic expression in each clause of above can be of only 3 kinds: $G(v_i, v_j)$, $v_i = v_j$, or $P(v_{i_1}, \dots, v_{i_r})$.

The above boils down to determining the satisfaction of a conjunction of at most hn^k clauses, each of which is the disjunction of atomic expressions of the form $P(v_{i_1}, \dots, v_{i_r})$ and their negations.

Each of these atomic expressions can be true or false.

Hence treat each of them as a boolean variable.

We can solve for the satisfiability of the above formula in polynomial time.

Axiomatizing Number Theory

Can we come up with a set of axioms for number theory that is sound and complete?

Consider the following set of axioms NT :

$$NT1 : \forall x(\sigma(x) \neq 0)$$

$$NT2 : \forall x \forall y(\sigma(x) = \sigma(y) \Rightarrow x = y)$$

$$NT3 : \forall x(x = 0 \vee \exists y \sigma(y) = x)$$

$$NT4 : \forall x(x + 0 = x)$$

$$NT5 : \forall x \forall y(x + \sigma(y) = \sigma(x + y))$$

$$NT6 : \forall x(x \times 0 = 0)$$

$$NT7 : \forall x \forall y(x \times \sigma(y) = (x \times y) + x)$$

$$NT8 : \forall x(x \uparrow 0 = \sigma(0))$$

$$NT9 : \forall x \forall y(x \uparrow \sigma(y) = (x \uparrow y) \times x)$$

$$NT10 : \forall x(x < \sigma(x))$$

$$NT11 : \forall x\forall y(x < y \Rightarrow \sigma(x) \leq y)$$

$$NT12 : \forall x\forall y(\neg(x < y) \Rightarrow y \leq x)$$

$$NT13 : \forall x\forall y\forall z(((x < y) \wedge (y < z)) \Rightarrow x < z)$$

$$NT14 : \forall x\forall y\forall z\forall z'(mod(x, y, z) \wedge mod(x, y, z') \Rightarrow z = z')$$

$(mod(x, y, z)$ stands for $\exists w(x = y \times w + z \wedge z < y)$).

Power of NT

Definition 1. A **variable-free** sentence is one that has no variable occurrences (free or bound).

We can prove from NT any true variable-free sentence and disprove any false one.

Theorem 2. Suppose that ϕ is a variable-free sentence. Then $N \models \phi$ iff $NT \vdash \phi$.

We can also prove from NT expressions involving quantifiers.

Examples:

1. $\forall x(\sigma(x) = x + 1)$.

2. Let $\phi = (x \uparrow x) + (x \uparrow 2) = 4 \times x$.

$$NT \vdash \exists x \phi.$$

$$N \models \phi[x \leftarrow 2].$$

Power of NT

Definition 2. We use the notation $(\forall x < t)\phi$ where t is a term as a shorthand for $\forall x((x < t) \Rightarrow \phi)$; similarly for $(\exists x < t)\phi$. These are called **bounded quantifiers**. When both bounded and unbounded quantifiers precede the rest of the expression, we say that the expression is in **bounded prenex form**. A sentence is **bounded** if all its universal quantifiers are bounded and the sentence is in bounded prenex form.

Example: $(\forall x < 9)\exists y(\forall z < 2 \times y)(x + z + 10 < 4 \times y)$.

Theorem 3. Let ϕ be a bounded sentence. Then $N \models \phi$ iff $NT \vdash \phi$.

Proof

We will show that $N \models \phi$ implies $NT \vdash \phi$ by induction on the number k of quantifiers.

1. $k = 0$: Variable-free sentence, already proved.

2. $\phi = \exists x\psi$: Since $N \models \phi$, there is an integer n such that $N \models \psi[x \leftarrow n]$.

Hence $NT \vdash \phi$.

3. $\phi = (\forall x < t)\psi$. W.l.o.g assume that $t = n$, for some integer n .

By repeated applications of $NT10$ and $NT11$, we can prove

$$\psi_1 = \forall x(x < n \Rightarrow (x = 0 \vee x = 1 \vee x = 2 \vee \dots \vee x = n - 1)).$$

By induction, $NT \vdash \psi[x \leftarrow j]$ for each j , $0 \leq j < n$.

Thus, $NT \vdash \psi_2 = \forall x(x = 0 \vee x = 1 \vee \dots \vee x = n - 1) \Rightarrow \psi$.

Having proved ψ_1 and ψ_2 from NT , we deduce $\phi = \forall x((x < n) \Rightarrow \psi)$.

Using Number Theory and Logic to Capture Computation

Consider a ordinary single string TM $M = (K, \Sigma, \delta, s)$.

Assume w.l.o.g., M halts at either “yes” or “no” (or it may never halt), it never writes \triangleright (starting symbol) on the string, and halts by moving all the way to the right (e.g., never writes \sqcup in the middle of the string).

We encode symbols and states as integers.

$\Sigma = \{0, 1, \dots, |\Sigma| - 1\}$ and $K = \{|\Sigma|, |\Sigma| + 1, \dots, |\Sigma| + |K| - 1\}$.

Starting state s is Σ and \triangleright is 0. “yes” is $|\Sigma| + 1$ and “no” is $|\Sigma| + 2$, and \sqcup is 1.

We need totally $b = |\Sigma| + |K|$ integers.

Encoding Configurations

We encode configurations as sequences of integers in $\{0, 1, \dots, b - 1\}$, i.e., as a integer in b -ary with the most significant bit first.

E.g., configuration $C = (q, w, u)$ is encoded by

$C = (w_1, w_2, \dots, w_m, q, u_1, u_2, \dots, u_n)$ where $|w| = m$ and $|u| = n$.

i.e., by the unique integer whose b -ary representation is this sequence:

$$\sum_{i=1}^m w_i b^{m+n+1-i} + qb^n + \sum_{i=1}^n u_i b^{n-i}.$$

Example: The configuration $(q, \triangleright aa, \sqcup, \sqcup)$ is encoded by $(0, 2, 2, 7, 1, 1)$ or by the integer $022711_8 = 9673_{10}$ (assuming $b = 8$).

Encoding Yields Relation

"Yields in one step" relation over configurations of M defines a relation $Y_M \subset \mathcal{N}^2$ over the integers.

For example,

$$(q, \triangleright aa, \sqcup \sqcup) \rightarrow^M (q, \triangleright a, \sqcup \sqcup \sqcup).$$

i.e., $m = 022711_8 \rightarrow^M n = 027111_8$. Hence $Y_M(m, n)$.

We can express this relation as an expression in Number Theory:

there is an expression $yields_M(x, y)$ with two free variables x and y such that $N_{x=m, y=n} \models yields_M(x, y)$ iff $Y_M(m, n)$.

We can tell whether $Y_M(m, n)$ holds by just looking at m and n : the change is caused by a *local replacement of digits* corresponding to a transition step.

E.g., here it was because of the rule $\delta(q, a) = (q, \sqcup, \leftarrow)$.

In general, a move can cause a local replacement of *triples of digits*.

We can exhaustively list all the triples and their replacements for any given machine M in a table. This in turn can be represented as an expression in FOL (in CNF form).