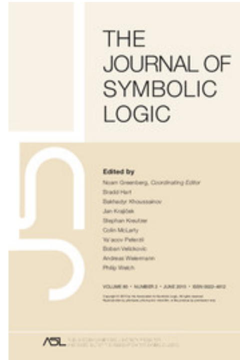


# Random models and the Gödel case of the decision problem

Yuri Gurevich and Saharon Shelah

The Journal of Symbolic Logic / Volume 48 / Issue 04 / December 1983, pp 1120 - 1124
DOI: 10.2307/2273674, Published online: 12 March 2014

THE JOURNAL OF SYMBOLIC LOGIC
Volume 48, Number 4, Dec. 1983

# RANDOM MODELS AND THE GÖDEL CASE OF THE DECISION PROBLEM

YURI GUREVICH AND SAHARON SHELAH[1]

**Abstract.** In a paper of 1933 Gödel proved that every satisfiable first-order $\forall^2\exists^*$ sentence has a finite model. Actually he constructed a finite model in an ingenious and sophisticated way. In this paper we use a simple and straightforward probabilistic argument to establish existence of a finite model of an arbitrary satisfiable $\forall^2\exists^*$ sentence.

**§0. Introduction.** We consider the usual first-order logic of textbooks. A first-order formula is called a sentence if it has no free individual variables. In this paper we restrict our attention to formulas without function symbols or individual constants. Unless we explicitly note otherwise, our formulas are without occurrences of equality.

THEOREM 1. *Let* $\phi = \forall v_1 \forall v_2 \exists v_3 \cdots \exists v_l \Phi(v_1, \ldots, v_l)$ *where* $\Phi$ *is quantifier free. If* $\phi$ *has a model it has a finite model.*

Theorem 1 was proved in Gödel [3]. It was proved independently in Schütte [9], [10]. Gödel's proof is much cleaner and easier than that of Schütte. Still it is very sophisticated. Its overall scheme is simple, however. Gödel formulates a syntactical criterion and proves that the criterion is necessary for satisfiability and sufficient for finite satisfiability. It is the proof of sufficiency that is difficult. In §1 we give the simple part of Gödel's proof. In §2 we define random finite structures and prove the sufficiency result in a straightforward way. Let us mention that the idea of random structures is not a perfect novelty: see Fagin [2].

COROLLARY. *There is an algorithm that decides satisfiability of* $\forall^2\exists^*$ *sentences.*

The Corollary was independently proved in Kalmar [6].

When our proof gives an easier proof of Theorem 1, Gödel's proof gives a better upper bound on the size of a minimal model of $\phi$. Additional information about models of $\forall^2\exists^*$ sentences can be found in Dreben and Goldfarb [1]. Lewis [8] gives lower and upper bounds on the computational complexity of algorithms that decide satisfiability of $\forall^2\exists^*$ sentences.

Both Theorem 1 and the Corollary are easily generalized to $\exists^*\forall^2\exists^*$ sentences, which form one of the maximal decidable for satisfiability classes of prenex sentences that is defined by type of prefix; see Lewis [7]. Even the $\forall^3\exists$ class with unary predicates and at most one binary predicate is undecidable for satisfiability. In

Received January 18, 1982.

[1]This paper was written essentially during the Logic Year 1980–81 in Jerusalem when both authors were fellows in the Institute for Advanced Studies of the Hebrew University.


0022-4812/83/4804-0018/$01.50

particular a satisfiable $\forall^3\exists$ sentence can have no finite models. Here is an example: $\forall x\forall y\forall z\exists u[(Rxy \,\&\, Ryz \to Rxz) \,\&\, \sim Rxx \,\&Rxu]$.

In §3 we generalize Theorem 1 for certain $\forall^*\exists^*$ sentences.

Gödel [3] mentioned that Theorem 1 remains true if we allow equality to appear in $\phi$. This claim of his remains unproved. Goldfarb [4] showed that there is no primitive recursive procedure that decides satisfiability of $\forall^2\exists$ sentences with equality and at most binary predicates. The reader may wonder where the proof of Theorem 1 breaks down in the case with equality. An answer can be found in §4.

More about the Gödel class with equality will appear in Goldfarb, Gurevich and Shelah [5].

We thank Warren Goldfarb for useful comments on a draft of this paper.

§1. **Gödel's criterion.** In this section we describe Gödel's scheme for proving Theorem 1, and we prove the easy part of the scheme.

LEMMA. *A first-order sentence $\forall v_1\forall v_2\exists v_3\cdots\exists v_l\Phi(v_1, \ldots, v_l)$ is equivalent to the sentence*

$$\forall v_1\forall v_2\exists v_3\cdots\exists v_l\exists v_3'\cdots\exists v_l'[v_1 \neq v_2 \to \Phi(v_1, v_2, v_3, \ldots, v_l) \\ \& \, \Phi(v_1, v_1, v_3', \ldots v_l')]$$

*in any structure for the language of $\phi$ containing at least* 2 *elements.*

PROOF is obvious.

Let $\phi$ be a first-order sentence $\forall v_1\forall v_2\exists v_3\cdots\exists v_l(v_1 \neq v_2 \to \Phi(v_1, \ldots, v_l))$ where $\Phi$ is quantifier-free. In order to prove Theorem 1 it suffices to show that $\phi$ has a finite nonsingleton model if it has any nonsingleton model at all. (Nonsingleton means containing at least two different elements.) Without loss of generality $l \geq 3$.

DEFINITION. A *$k$-table* is a structure for the language of $\phi$ whose universe is the set $\{1, \ldots, k\}$.

DEFINITION. Let $M$ be a structure for the language of $\phi$ and $\bar{a} = (a_1, \ldots, a_k)$ a sequence of elements of $M$. The *table* $\mathrm{tb}_M(\bar{a})$ of $\bar{a}$ is the unique $k$-table $A$ such that the map$\{(i, a_i)\colon 1 \leq i \leq k\}$ is an isomorphism from $A$ onto a substructure of $M$.

If $\phi$ is satisfiable, and $M$ is a nonsingleton model of $\phi$, and

$$P = \{\mathrm{tb}_M(a)\colon a \in M\}, \qquad Q = \{\mathrm{tb}_M(a, b)\colon a, b \in M\},$$

then $P$, $Q$ are nonempty and satisfy the following conditions:

(G1) For all $A_1, A_2 \in P$ there is $B \in Q$ with $\mathrm{tb}_B(1) = A_1$, $\mathrm{tb}_B(2) = A_2$; and

(G2) For every $A \in Q$ there is an $l$-table $B$ such that $\mathrm{tb}_B(1, 2) = A$, and $\mathrm{tb}_B(i) \in P$ for $1 \leq i \leq l$, and $\mathrm{tb}_B(i,j) \in Q$ for $1 \leq i,j \leq l$, and $B \models \Phi(1, 2, \ldots, l)$.

THEOREM 2. *Suppose that a nonempty set $P$ of* 1*-tables and a set $Q$ of* 2*-tables satisfy conditions* (G1) *and* (G2). *Then $\phi$ has a finite nonsingleton model.*

It remains to prove Theorem 2.

§2. **Proof of Theorem 2.** Let $p$, $q$ be the cardinalities of $P$, $Q$, respectively. For $n \geq l$ we construct an $np$-table $M$. The truth values of $k$-place atomic formulas are defined as follows.

*Case* $k = 1$. If $a = ip + j$ for some $0 \leq i < n$, $1 \leq j \leq p$, define $\mathrm{tb}_M(a)$ to be equal to the $j$th table in an a priori fixed order on $P$.

*Case* $k = 2$. Suppose $1 \leq a < b \leq np$. By (G1) the set $\{A \in Q: \mathrm{tb}_A(1) = \mathrm{tb}_M(a), \mathrm{tb}_A(2) = \mathrm{tb}_M(b)\}$ is not empty. Choose at random a table $A$ in this set and define $\mathrm{tb}_M(a, b) = A$.

*Case* $3 \leq k \leq l$. If $R$ is a $j$-place predicate letter in $\phi$, and $(a_1, \ldots, a_j)$ is a $j$-tuple of elements of $M$ containing at least 3, and at most $l$, distinct members, define the truth-value of $R(a_1, \ldots, a_j)$ at random.

*Case* $k > l$. If $R$ is a $j$-place predicate letter in $\phi$, and $(a_1, \ldots, a_j)$ is a $j$-tuple of elements of $M$ containing more than $l$ distinct members, define $R(a_1, \ldots, a_j)$ to be false.

Let $S_n$ be the collection of possible values for $M$. We consider $S_n$ as a probability space with

$$\mathrm{Prob}[M = M_1] = \mathrm{Prob}[M = M_2] \quad \text{for } M_1, M_2 \text{ in } S_n.$$

Thus $M$ is a random member of $S_n$. Let $a_1, \ldots, a_l$ range over $\{1, \ldots, np\}$.

By (G2) there is a function Fun assigning an appropriate $l$-table $B = \mathrm{Fun}(A)$ to each $A \in Q$. Given an $l$-table $B$ we say that $a_3, \ldots, a_l$ *witness* $B$ for $a_1, a_2$ if the truth value of $R(a_{i_1}, \ldots, a_{i_k})$ in $M$ coincides with the truth value of $R(i_1, \ldots, i_k)$ in $B$ for every $1 \leq k \leq l$, every $k$-place predicate letter $R$ in $\phi$ and every $k$-tuple $i_1, \ldots, i_k$ of numbers such that $\{i_1, \ldots, i_k\}$ is included into $\{1, \ldots, l\}$ and meets $\{3, \ldots, l\}$. In the case when the predicate letters in $\phi$ are at most binary, elements $a_3, \ldots, a_l$ witness $B$ for $a_1, a_2$ iff $\mathrm{tb}_M(a_i, a_j) = \mathrm{tb}_B(i, j)$ for all distinct $i, j \in \{1, \ldots, l\}$ such that either $i \geq 3$ or $j \geq 3$.

Let $\varepsilon = (1/q)^r \cdot (1/2)^s$, where $r = \binom{l-2}{2} + 2(l-2)$ and $s$ is the number of atomic formulas $R(v_{i_1}, \ldots, v_{i_k})$ where $3 \leq k \leq l$, $R$ is a $k$-place predicate letter in $\phi$, and $(i_1, \ldots, i_k)$ is a $k$-tuple of numbers among $1, \ldots, l$ containing at least three distinct members. (If $l = 3$ then $r = 2$.)

LEMMA 1. *Suppose that* $A \in Q$, $B = \mathrm{Fun}(A)$ *and* $a_1, \ldots, a_l$ *are different elements of* $M$ *with* $\mathrm{tb}_M(a_i) = \mathrm{tb}_B(i)$ *for* $1 \leq i \leq l$. *Then*

$$\mathrm{Prob}[a_3, \ldots, a_l \textit{ witness } B \textit{ for } a_1, a_2] \geq \varepsilon.$$

PROOF is clear.

Let $m$ be the integer part of $(n-2)/(l-2)$.

LEMMA 2. *Let* $a_1, a_2$ *be different elements of* $M$. *Then*

$$\mathrm{Prob}[\exists v_3 \cdots \exists v_l \Phi(a_1, a_2, v_3, \ldots, v_l) \textit{ fails in } M] \leq (1 - \varepsilon)^m.$$

PROOF. Let $A$ be a possible value for $\mathrm{tb}_M(a_1, a_2)$ and $B = \mathrm{Fun}(A)$. It suffices to prove that

$$\mathrm{Prob}[\text{no } v_3, \ldots, v_l \text{ witness } B \text{ for } a_1, a_2] \leq (1 - \varepsilon)^m.$$

There are different elements $a_i^j \in M - \{a_1, a_2\}$ with $\mathrm{tb}(a_i^j) = \mathrm{tb}_B(i)$ for $3 \leq i \leq l$ and $1 \leq j \leq m$. The events "$a_3^j, \ldots, a_l^j$ witness $B$ for $a_1, a_2$" are independent and the intersection of their complements includes the event "no $v_3, \ldots, v_l$ witness $B$ for $a_1, a_2$". Now use Lemma 1. $\square$

Now,

$$[M \text{ does not satisfy } \phi] = \bigcup_{a_1 \neq a_2} [\exists v_3 \cdots \exists v_l \Phi(a_1, a_2, v_3, \ldots, v_l) \text{ fails in } M].$$

This and Lemma 2 give

$$\text{Prob}[M \text{ does not satisfy } \phi] < pn(pn - 1)(1 - \varepsilon)^m.$$

Suppose that $n$ is big enough so that $pn(pn - 1)(1 - \varepsilon)^m < 1$. Then the probability that $M$ satisfies $\phi$ is positive. Since the probability space $S_n$ is finite it means that some member of $S_n$ satisfies $\phi$. Theorem 2 is proved.

Our proof gives an upper bound $np$ on the size of a minimal nonsingleton model of $\phi$ where $n$ satisfies $2(l - 2)\log(np) \le \varepsilon(n - l) \log e$ and $e$ is the basis of natural logarithms.

For, suppose this inequality is satisfied. Since $m > (n - 2)/(l - 2) - 1 = (n - l)/(l - 2)$, we have $\log(np)^2 < \varepsilon m \log e$. Use the college calculus to check that $x \log e < -\log(1 - x)$ for $0 < x < 1$. Hence

$$\log(np)^2 < -m \log(1 - \varepsilon),$$
$$\therefore \log(np)^2 + m \log(1 - \varepsilon) < 0,$$
$$\therefore (np)^2(1 - \varepsilon)^m < 1,$$

which suffices in the proof of Theorem 2.

Gödel [3] gives a better upper bound on the size of a minimal nonsingleton model of $\phi$. It is $7L$ where $L$ satisfies the inequality $2(l - 2)q(\log_2(7L) + 1) \le L$.

In order to improve our bound we can be more cautious in defining a random structure $M$. In particular we can be more restrictive in defining $k$-place predicates for $k \ge 3$. A real sophistication is needed, however, to get Gödel's bound.

**§3. A generalization for the $\forall^*\exists^*$ case.** It may seem that the proof of Theorem 1 is straightforwardly generalizable for the $\forall^*\exists^*$ case. The sentence

$$\forall x \forall y \forall z \exists u[(Rxy \mathbin{\&} Ryz \to Rxz) \mathbin{\&} \sim Rxx \mathbin{\&} Rxu]$$

has, however, only infinite models. Where does the would-be generalization of Theorem 1 break down when $\phi$ is this sentence? To answer this question note that the definition of a random structure fails to ensure "$R$ is transitive". Technically speaking we lose independence of events that were used to prove Lemmas 1 and 2 in §2.

THEOREM 3. *Let $\phi$ be a sentence $\forall v_1 \cdots \forall v_k \exists v_{k+1} \cdots \exists v_l \Phi(v_l, \ldots, v_l)$ where $\Phi$ is quantifier free. Suppose that $M$ is a model of $\phi$ such that for every $1 < j < k$, the table* $\text{tb}_M(a_1, \ldots, a_j)$ *of arbitrary $j$-tuple $a_1, \ldots, a_j$ of elements of $M$ is uniquely defined by* $\text{tb}_M(a_1), \ldots, \text{tb}_M(a_j)$. *Then $\phi$ has a finite model.*

The proof of Theorem 3 is a straightforward generalization of the proof of Theorem 1.

**§4. A note on equality.** As we mentioned in §0, it is still unknown whether every satisfiable dyadic $\forall^2\exists$ sentence with equality has a finite model. Why is equality so important? Where did we use the fact that equality does not appear in $\phi$?

The situation appears to be even more intriguing if one notices that we do ensure in the proof of Theorem 2 that the desired witnesses $a_3, \ldots, a_l$ are different between themselves and different from $a_1, a_2$. Moreover, the proof of Theorem 2 does not use absence of equality at all. However, absence of equality was used in §1 to prove necessity of (G1).

DEFINITION. Let $M$ be a structure. An element $a$ of $M$ is a *king* if there is no other element $b$ of $M$ with $\mathrm{tb}_M(b) = \mathrm{tb}_M(a)$.

Any satisfiable first-order sentence $\phi$ without equality has a model without kings. We demonstrate that statement in an example. Suppose that a dyadic predicate symbol $R$ is the only nonlogical constant in $\phi$. If $M$ is a model of $\phi$ and $a \in M$ throw into $M$ a new element $a'$ (a duplicate of $a$) and define $Ra'b \leftrightarrow Rab$, $Rba' \leftrightarrow Rba$ for all $b \in M$. Evidently the new model satisfies $\phi$ and neither $a$ nor $a'$ is a king in the new model.

If we allow equality in $\phi$ but suppose that $\phi$ has a model without kings then Theorem 1 remains valid.

See also Goldfarb, Gurevich and Shelah [5].

## REFERENCES

[1] BURTON S. DREBEN and WARREN D. GOLDFARB, ***The decision problem: Solvable classes of quantificational formulas,*** Addison-Wesley, Reading, Mass., 1979.

[2] RONALD FAGIN, *Probabilities on finite models*, this JOURNAL, vol. 41 (1976), pp. 50–57.

[3] KURT GÖDEL, *Zum Entscheidungsproblem des logischen Funktionenkalküls*, ***Monatshefte für Mathematik und Physik,*** vol. 40 (1933), pp. 433–443.

[4] WARREN D. GOLDFARB, *On the Gödel class with identity,* this JOURNAL, vol. 46 (1981), pp. 354–364.

[5] WARREN D. GOLDFARB, YURI GUREVICH and SAHARON SHELAH, *On the Gödel class with identity* (in preparation).

[6] LASZLO KALMAR, *Über die Erfüllbarkeit derjenigen Zahlausdrucke, welche in der Normalform zwei benachbarte Allzeichen enthalten,* ***Mathematische Annalen,*** vol. 108 (1933), pp. 466–484.

[7] HARRY R. LEWIS, ***Unsolvable classes of quantificational formulas,*** Addison-Wesley, Reading, Mass., 1979.

[8] ———, *Complexity results for classes of quantificational formulas*, ***Journal of Computer and System Sciences,*** vol. 21 (1980), pp. 317–353.

[9] KURT SCHÜTTE, *Untersuchungen zum Entscheidungsproblem der mathematischen Logik*, ***Mathematische Annalen,*** vol. 109 (1934), pp. 572–603.

[10] ———, *Über die Erfüllbarkeit einer Klasse von logischen Formeln*, ***Mathematische Annalen,*** vol. 110 (1934), pp. 161–194.

UNIVERSITY OF MICHIGAN
ANN ARBOR, MICHIGAN 48109

HEBREW UNIVERSITY
JERUSALEM, ISRAEL