THE LOGIC IN COMPUTER SCIENCE COLUMN[1]

by

Yuri GUREVICH[2]

Electrical Engineering and Computer Science
University of Michigan, Ann Arbor, MI 48109-2122, USA
gurevich@eecs.umich.edu

Zero-One Laws

Quisani: I heard you talking on finite model theory the other day. It is interesting indeed that all those famous theorems about first-order logic fail in the case when only finite structures are allowed. I can understand that for those, like you, educated in the tradition of mathematical logic it seems very important to find out which of the classical theorems can be rescued. But finite structures are too important all by themselves. There's got to be deep finite model theory that has nothing to do with infinite structures.

Author: "Nothing to do" sounds a little extremist to me. Sometimes infinite objects are good approximations of finite objects.

Q: I do not understand this. Usually, finite objects approximate infinite ones.

A: It may happen that the infinite case is cleaner and easier to deal with. For example, a long finite sum may be replaced with a simpler integral. Returning to your question, there is indeed meaningful, inherently finite, model theory. One exciting issue is zero-one laws. Consider, say, undirected graphs and let π be a property of such graphs. For example, π may be connectivity. What fraction of n-vertex graphs have the property π? It turns out that, for many natural properties π, this fraction converges to 0 or 1 as n grows to infinity. If the fraction converges to 1, the property is called almost sure. In that sense, almost all graphs are connected, hamiltonian, not 3-colorable, rigid, etc. [BH, Co2, and references there].

[1] "Current Trends in Theoretical Computer Science", Eds. G. Rozenberg and A. Salomaa, World Scientific, Series in Computer Science, Volume 40, 1993

[2] Partially supported by NSF grant CCR 89-04728 and ONR grant N00014-91-J-11861.

Q: What is exactly the fraction of n-vertex graphs with property π? What does it mean that a graph is rigid?

A: A graph G is called rigid if the identity map is the only automorphism of G (i.e. the only isomorphism from G to G). Now, about that fraction. There are two different definitions in the literature:

Labeled Case: $l_n(\pi)$ is the number $L_n(\pi)$ of π graphs on $\{1,\ldots,n\}$ divided by $2^{n(n-1)/2}$, the total number of graphs on $\{1,\ldots,n\}$. In other words, $l_n(\pi) = L_n(\pi)/L_n(\tau)$ where τ is the trivial property that every graph has.

Unlabeled Case: $u_n(\pi)$ is the number $U_n(\pi)$ of isomorphism types of n-vertex π graphs divided by the total number $U_n(\tau)$ of isomorphism types of n-vertex graphs.

Of course, the property π in question is supposed to be preserved by isomorphisms. Somewhat loosely, people say that π obeys the labeled (resp. unlabeled) zero-one law if $l_n(\pi)$ (resp. $u_n(\pi)$) converges to 0 or 1. Let me say that two numerical sequences α_n and β_n are *asymptotically equivalent* if they converge to the same number or else they both diverge. I will use the sign $\sim$ to denote asymptotic equivalence. Notice that the asymptotic equivalence $\alpha_n \sim \beta_n$ is weaker than the asymptotic equality $\alpha_n \asymp \beta_n$; the latter means that the fraction α_n/β_n converges to 1. For example, $1/n$ is asymptotically equivalent but not asymptotically equal to $1/n^2$. It turns out that $l_n(\pi) \sim u_n(\pi)$. The reason for the asymptotic equivalence is that almost all graphs are rigid.

Q: In what sense are most graphs rigid?

A: Rigidity, which I will denote by ρ, obeys either of the two zero-one laws: $l_n(\rho) \sim u_n(\rho) \to 1$. Notice that each rigid n-vertex graph has exactly $n!$ distinct labelings, so that $L_n(\pi \wedge \rho) = U_n(\pi \wedge \rho) \cdot n!$. The desired asymptotic equivalence $l_n(\pi) \sim u_n(\pi)$ follows easily. Do you see how to derive it?

Q: I think I do. Since $l_n(\rho) \to 1$,

$$\frac{L_n(\pi)}{L_n(\tau)} = \frac{L_n(\pi \wedge \rho) + L_n(\pi \wedge \neg\rho)}{L_n(\tau)} \sim \frac{L_n(\pi \wedge \rho)}{L_n(\tau)} \sim \frac{L_n(\pi \wedge \rho)}{L_n(\rho)}.$$

Similarly, $\dfrac{U_n(\pi)}{U_n(\tau)} \sim \dfrac{U_n(\pi \wedge \rho)}{U_n(\rho)}$ because $u_n(\rho) \to 1$. But $\dfrac{U_n(\pi \wedge \rho)}{U_n(\rho)} = \dfrac{L_n(\pi \wedge \rho)}{L_n(\rho)}$.

A: Very good.

Q: Let me verify for myself that rigid graph has $n!$ distinct labelings.

There are $n!$ one-to-one functions f from the universe V of an n-vertex graph G onto $\{1,\ldots,n\}$. Each such f gives a graph G_f on $\{1,\ldots,n\}$, so that f is an isomorphism from G onto G_f. If $G_f = G_h$ then $h^{-1} \circ f$ is an automorphism of G. Thus, all $n!$ graphs G_f are distinct if G is rigid. Hence $L_n(\rho) = U_n(\rho)$.

I think we are getting somewhere. If G is not rigid and ι is a nontrivial automorphism of G, then each graph G_f equals $G_{h\circ\iota}$. Thus, a nonrigid n-vertex graph has at most $n!/2$ distinct labelings, so that $L_n(\neg\rho) \le U_n(\neg\rho)\cdot n!/2 < U_n(\neg\rho)\cdot n!$. We have

$$u_n(\rho) = \frac{U_n(\rho)}{U_n(\rho)+U_n(\neg\rho)} = \frac{U_n(\rho)\cdot n!}{U_n(\rho)\cdot n! + U_n(\neg\rho)\cdot n!} < \frac{L_n(\rho)}{L_n(\rho)+L_n(\neg\rho)} = l_n(\rho)$$

and therefore $l_n(\rho) \to 1$ if $u_n(\rho) \to 1$. However, I do not see why the latter is true.

A: There is a good reason for the difficulty. Until now, we worked in great generality. We could speak as well about directed graphs or groups, etc. But now we need information specific to graphs. The following simple formula of Pólya [HP, Section 9.1] is worth remembering:

$$U_n(\tau) \asymp \frac{L_n(\tau)}{n!}.$$

By Pólya's formula,

$$\frac{U_n(\rho)+U_n(\neg\rho)/2}{U_n(\tau)} = \frac{U_n(\rho)n! + U_n(\neg\rho)n!/2}{U_n(\tau)n!} \ge \frac{L_n(\rho)+L_n(\neg\rho)}{U_n(\tau)n!} = \frac{L_n(\tau)}{U_n(\tau)n!} \to 1.$$

Thus, $1 - u_n(\neg\rho)/2 = \dfrac{U_n(\rho)+U_n(\neg\rho)}{U_n(\tau)} - \dfrac{U_n(\neg\rho)/2}{U_n(\tau)} = \dfrac{U_n(\rho)+U_n(\neg\rho)/2}{U_n(\tau)} \to 1$ and therefore $u_n(\neg\rho) \to 0$.

It is often easier to deal with labeled graphs. The fraction $l_n(\pi)$ can be seen as the probability of π in the sample space of graphs with universe $\{1,\dots,n\}$ and the uniform probability distribution.

Q: Similarly, the fraction $u_n(\pi)$ can be interpreted as the probability of π in an appropriate sample space.

A: True, but the sample space of labeled graphs is easier to deal with. In the case of labeled graphs, for example, the probability of an event "$\{i,j\}$ is an edge" is $1/2$ whenever $i \ne j$. Further, any two such events are pairwise independent. The sample space can be viewed as the set of outcomes of the following experiment: for each pair $\{i,j\}$ of distinct elements of $\{1,\dots,n\}$, toss a fair coin to decide whether the pair is an edge.

Q: How does logic come in?

A: It turns out that every first-order property π satisfies the zero-one law [GKLT, and independently Fa1].

Q: Wow!

A: We may say that first-order logic obeys the zero-one law.

Q: Do you mean the labeled or unlabeled law? Maybe you are talking about properties of graphs only. We know that $l_n(\pi) \sim u_n(\pi)$ for any graph property π preserved by isomorphisms.

A: I am talking about first-order logic with equality and unary, binary, ternary, etc. predicate symbols, but without function symbols or individual constants.

Q: Sure. If c is an individual constant then the probability of a sentence $P(c)$ is $1/2$ in the case of labeled structures.

A: Right. It turns out that $l_n(\pi) \sim u_n(\pi)$ for every property π of structures of a given signature σ. Let me say this more carefully. First of all, I consider only finite signatures. Given a finite collection σ of predicate symbols of specified arities, consider a class K of finite structures of signature σ. A property π of K structures can be viewed as a function on K that assigns *true* or *false* to each structure A in K. We will consider only those properties which are preserved under isomorphisms.

Q: You got me worried. Do you mean that K is a class and not necessarily a set?

A: No, no. I do not intend to involve us in set theory. We are only interested in isomorphism types of structures and their labelings. Generalize the definitions of l_n and u_n from graphs to structures in K and consider the case when K is the class of all σ structures. For every property π of σ structures, $l_n(\pi) \sim u_n(\pi)$.

Q: It is clear that $l_n(\pi) \sim u_n(\pi)$ if unlabeled σ-structures are almost surely rigid. Are they?

A: Not if σ comprises only unary predicates. But the case of unary predicates is easily analyzable directly and we may ignore it. If σ contains at least one predicate of arity > 1 then the unlabeled zero-one law for the rigidity of σ structures follows from the unlabeled zero-one law for graph rigidity.

Q: How does it follow?

A: For simplicity, I suppose that σ contains a binary predicate P. Given a σ structure A, construct a graph G on the universe of A such that any pair $\{a, b\}$ of distinct elements of A is an edge if and only if either both $P(a, b)$ and $P(b, a)$ are true in A or else both $P(a, b)$ and $P(b, a)$ are false in A. Every automorphism of A is also an automorphism of G. Hence all pre-images A of a rigid graph G are rigid. Further, a rigid n-vertex graph has more pre-images than a nonrigid one. It follows that the fraction of rigid n-element σ-structures is larger than the fraction of rigid n-vertex graphs.

Q: What if σ contains only predicates of arity ≥ 3?

A: May I leave this as an exercise? By the way, historical references related to rigidity may be found in [Co2].

Q: Fair enough. I would love to see a proof of a zero-one law for first-order logic.

A: We may forget about the unlabeled law and concentrate on the labeled one. The original proof of Glebsky *et al.* is somewhat involved. A nice sketch of the proof is in [Co2].

Q: Did you know the four coauthors?

A: Yes. Kogan, Liogonky and Talanov were students of Glebsky at Gorky (now Nijny Novgorod) University in Russia. I visited Gorky to participate, as an official "opponent", in the ceremony of the public "defense" by Liogonky of his Ph.D. thesis [Li] where he proved the unlabeled law for first-order logic.

Fagin rediscovered the zero-one law for first-order logic in [Fa1]. His proof is very instructive. Imagine the following infinite experiment: For each pair $\{i, j\}$ of distinct positive positive integers, toss a fair coin to decide if $\{i, j\}$ is an edge. Outcomes of the experiment are graphs on positive integers. What do you think is the probability that two outcomes are isomorphic?

Q: I would say zero, but I feel a trap. Would you give me a hint?

A: Try to build an isomorphism piecemeal. Suppose that f is a partial isomorphism from one outcome graph to another such that the domain of f is finite. Let i be an integer outside the domain of f. Can f be extended to i?

Q: For every j outside the range of f, the probability p that the extension of f by $f(i) = j$ is a partial isomorphism equals 2^{-k} where k is the cardinality of the domain of f. The probability that at least one of m such j's is appropriate is $(1 - (1 - p)^m)$, which tends to 1 as m grows. Thus, the probability that f can be extended to include i into its domain is 1. I see it now. Start with the empty partial isomorphism and keep extending it to include the smallest integer outside the domain, the smallest integer outside the range, the smallest integer outside the domain, etc. I presume that the union of countably many events of probability zero has probability zero in our sample space.

A: Yes, it is easy to check that the probability measure is countably additive.

Q: Then the intersection of countably many events of probability 1 has probability 1. Hence, with probability 1, the back-and-forth construction results in an isomorphism between two random outcomes. This is amazing.

A: I think so too. The prevalent outcome (if we identify isomorphic graphs) is called the *infinite random graph*. Can you define an *infinite random directed graph* ?

Q: Yes. Modify the experiment to toss a coin for every ordered pair (i, j) of positive integers which are not necessarily distinct. The same back-and-forth argument shows that, with probability 1, two outcomes are isomorphic.

A: Right. We can define the *infinite random structure* of an arbitrary (finite) signature σ in a similar way. For every predicate symbol P in σ and for every tuple $(i_1, \ldots, i_r)$ of (not necessarily distinct) positive integers, toss a fair coin to decide whether $P(i_1, \ldots, i_r)$ is true. Here r is of course the arity of P. With probability 1, two outcomes of the infinite experiment are isomorphic.

Q: How is this related to the zero-one law for first-order logic?

A: For each positive integer k, consider an extension axiom

$$\left(\exists u_1 \ldots \exists u_k \bigwedge_{1 \le i < j \le k} u_i \neq u_j\right) \wedge$$

$$\bigwedge_{X \subseteq A_k} \forall u_1 \ldots \forall u_k \exists v \left[\left(\bigwedge_{1 \le i < j \le k} u_i \neq u_j\right) \rightarrow \left(\left(\bigwedge_{i=1}^{k} u_i \neq v\right) \wedge \left(\bigwedge_{\alpha \in X} \alpha\right) \wedge \left(\bigwedge_{\alpha \in A_k - X} \neg\alpha\right)\right)\right]$$

which I will denote ε_k. Here A_k comprises all atomic formulas $\alpha = P(w_1, \ldots, w_r)$ such that $P \in \sigma$ and $v \in \{w_1, \ldots, w_r\} \subseteq \{u_1, \ldots, u_k, v\}$. For example, if σ comprises one binary predicate P then

$$A_k = \{P(v,v), P(u_1,v), \ldots, P(u_k,v), P(v,u_1), \ldots, P(v,u_k)\}.$$

The axiom ε_k says that there exist at least k distinct elements and every k-element substructure can be extended by one additional element in every possible way. Notice that each ε_{k+1} implies ε_k. It is easy to see that the infinite random σ-structure satisfies all extension axioms and that every two countably infinite σ-structures satisfying all extension axioms are isomorphic.

Further, using a couple of classical theorems about first-order logic, one can infer that, for every first-order sentence ϕ, either ϕ or $\neg\phi$ follows from some extension axiom. Indeed, suppose by contradiction that neither of the two formulas is implied by any extension axiom and therefore by any finite set of extension axioms. By the Compactness Theorem, there is a graph G_1 satisfying ϕ and all extension axioms and there is a graph G_2 satisfying $\neg\phi$ and all extension axioms. Obviously, the two graphs are infinite. By the Löwenheim-Skolem Theorem, every infinite structure has a countable substructure with the same first-order properties. Thus, we may assume without loss of generality that the two graphs are countable. But then G_1 and G_2 are isomorphic which is impossible.

All these facts were known before Fagin's paper. To make this long story shorter, let me refer again to Compton's comprehensive survey [Co2] for the history of the subject. But Fagin connected all this with finite structures. Every extension axiom is almost sure. Hence either ϕ or $\neg\phi$ is almost sure.

Q: And the almost sure theory of finite structures is exactly the theory of the infinite random structure. A nice illustration of the thesis that an infinite object may approximate finite ones. But was it necessary to use infinite graphs?

A: No. One can prove directly that every first-order sentence is decided by some extension axiom. One way is to use Ehrenfeucht games. You can check easily that if two graphs G_1 and G_2 satisfy ε_k, then Player II has a winning strategy in the k-step Ehrenfeucht game $\Gamma_k(G_1, G_2)$ and thus, by Ehrenfeucht's Theorem [Eh], no

prenex (with quantifiers up front) first-order sentence with k quantifiers distinguishes between G_1 and G_2.

Q: So what?

A: Oh, consider an arbitrary first-order sentence ϕ. A standard algorithm transforms ϕ into a logically equivalent prenex first-order sentence ϕ'. Let k be the number of quantifiers in ϕ'. By the argument above, ϕ' does not distinguish between any two models of ε_k. Hence ϕ does not distinguish between any two models of ε_k. Either all models of ε_k satisfy ϕ, or else all models of ε_k satisfy $\neg\phi$. In the first case, ϕ is almost surely true, and in the second case, ϕ is almost surely false.

Q: Would you remind me what exactly Ehrenfeucht games are?

A: That is not necessary. Let me explain to you how to prove the zero-one law for first-order logic by quantifier elimination. This even more direct method is due to Etienne Grandjean [Gr]. By induction on (the logical depth of the) first-order formula $\phi(\bar{u})$, we will prove that there exists k such that $\phi(\bar{u})$ is equivalent to some quantifier-free formula $\Phi(\bar{u})$ on structures satisfying ε_k. Here $\bar{u}$ is a tuple of free variables. If ϕ has no free variables, then Φ is *true* or *false*. Thus every sentence ϕ is almost surely true or almost surely false.

The atomic case is trivial and the case when ϕ is a boolean combination of proper subformulas is obvious. It remains to consider the case $\phi(u_1, \ldots, u_r) = (\exists v)\psi(u_1, \ldots, u_r, v)$. By induction hypothesis, there exists j such that ψ is equivalent to a quantifier-free formula on structures satisfying ε_j. Let $k = \max(j, r)$. We check that ϕ is equivalent to a quantifier-free formula on structures satisfying ε_k. Since $k \geq j$, we may assume without loss of generality that ψ itself is quantifier-free. Since $(\exists v)(\alpha \vee \beta)$ is logically equivalent to $[(\exists v)\alpha] \vee [(\exists v)\beta]$, we may suppose that ψ is a conjunction of atomic formulas and negated atomic formulas. Moreover, we may suppose that, for every pair (u_p, u_q) with $1 \leq p < q \leq r$, ϕ contains the conjunct $u_p = u_q$ or the conjunct $u_p \neq u_q$, and that ψ contains conjuncts $u_1 \neq v, \ldots, u_r \neq v$. If ψ is not satisfiable at all, choose Φ to be logically false. Otherwise, the desired $\Phi(\bar{u})$ is obtained from $\psi(\bar{u}, v)$ by deleting all (negated or non-negated) atomic formulas that mention v. Obviously $\phi(\bar{u})$ logically implies $\Phi(\bar{u})$. It is easy to see that the implication $\Phi(\bar{u}) \rightarrow \phi(\bar{u})$ follows from ε_r and therefore from ε_k.

Q: It looks like the desired k is less than largest number of free variables in subformulas of ϕ. One can actually compute the desired Φ and, in the case ϕ has no free variables, decide whether it is almost surely true or almost surely false. Did somebody look into the complexity of this decision problem?

A: Grandjean did. The decision problem is PSPACE complete [Gr].

Q: So it may be hard to tell whether a given first-order sentence is almost sure.

A: To put things into proper perspective, let me quote two facts. The problem whether a given sentence in the first-order language of equality (without any other

predicate symbols) is true in every finite structure (and therefore logically true) is PSPACE complete [St]. The problem whether a given first-order sentence is true in every finite structure is undecidable [Tr].

Q: It popped up in my mind that the zero-one law for first-order graph properties does not follow from the zero-one law for first-order logic because the properties of symmetry and irreflexivity, which characterize undirected graphs, are almost surely false.

A: That is true, but the same proofs establish the zero-one law for graph properties.

Q: It is interesting that that the zero-one law survives the restriction to graphs. I wonder if this is a special case of a general phenomenon. Maybe, the restricting axioms should be universal like the axioms of reflexivity and symmetry.

A: Here is a trivial counterexample. Consider the class of structures with two unary predicates P and Q satisfying the axiom $\forall u \forall v[(P(u) \wedge P(v)) \rightarrow u = v]$. The sentence $\phi = (\exists u)(P(u) \wedge Q(u))$ is neither almost surely true nor almost surely false.

However, sometimes the zero-one law survives. Andreas Blass and Frank Harary proved the zero-one law for simplicial complexes proved by [BH]. Kevin Compton proved the zero-one law for partial orders [Co1]. He used a theorem of Kleitman and Rothschild according to which a typical random partial order of size n has, somewhat surprisingly, no chains of length more than 3. Such partial orders can be seen as graphs with three layers of vertices where each edge connects a vertex of the middle layer with a vertex of the lower or the upper level. The appropriate infinite random partial order also has this form, and Compton's proof proceeds along the lines of Fagin's proof. Kolaitis, Prömel and Rothschild proved that, for each $l \geq 2$, the class of K_{l+1}-free graphs obeys the zero-one law [KPR]. Here K_{l+1} is the complete graph on $l+1$ vertices; a graph is called K_{l+1}-free if it does not have any subgraph isomorphic to K_{l+1}.

Q: Your counterexample is not very satisfactory because $l_n(\phi)$ converges to $1/2$. The formula ϕ satisfies the "convergence law", which is weaker than the zero-one law but still very meaningful.

A: You may want to look at some papers of Jim Lynch. He proves, for example, the convergence law for the first-order logic of unary functions [Ly2]. But here is another counterexample for your hypothesis [Bl]. Use universal axioms to say that P is a linear order, and if $Q(u,v,w)$ holds then v is the successor of u with respect to P and $R(u) \leftrightarrow \neg R(v)$. Let K be the class of (finite) structures satisfying the universal axioms. The relation $Q'(u,v) = \exists w Q(u,v,w)$ is a partial successor relation appropriate to linear order P on K structures.

Q: Why do you need w?

A: How do you assert, using only universal axioms, that every element, except for the last one, has a successor? The additional argument allow us to assert a statistical

version of this statement. Almost surely, Q' is the complete successor relation. Hence, almost surely, R marks either all even or all odd elements in the linear order. Write a sentence ϕ saying that the first (with respect to P) element satisfies R if and only if the last (with respect to P) element does. It is easy to see that $l_{2n}(\phi) \to 0$ and $l_{2n+1}(\phi) \to 1$. Thus ϕ violates the convergence law.

By the way, some weaker but nontrivial forms of the convergence law may survive even if the parity of the universe is expressible. For example, enrich each universe $\{1, \ldots, n\}$ with the successor relation $S(x, y) \longleftrightarrow y = x + 1$ and modular addition $P(x, y, z) \longleftrightarrow x + y = z \bmod n$. It easy to see that the sentence $\forall u \exists v P(v, v, u)$ holds if and only if n is odd. Nevertheless, for every first-order sentence ϕ in this language, there exists a positive integer m such that, for each $i < m$, the fraction of enriched structures of cardinality $i + km$ that satisfy ϕ converges when k grows to infinity [Ly1]. However, our second counterexample can be modified to violate the weak form of the convergence law.

Q: I suspect that the zero-one law for first-order logic inspired attempts to generalize it.

A: Yes, a whole new area of research has been created. You may want to read a nicely written comprehensive survey of the area by Kevin Compton [Co2]. One generalization of the (labeled) zero-one law for first-order logic is related to the probability distribution on the set of graphs with universe $\{1, \ldots, n\}$. Above, we tossed a fair coin to determine whether a pair $\{i, j\}$ of distinct vertices is an edge. Alter the experiment by using a biased coin, so that the probability that a pair $\{i, j\}$ of distinct vertices is an edge is some positive number $p < 1$. It is easy to see that all the results survive. The situation changes drastically if p is allowed to vary as n grows [SS, Sp, Ly3].

Q: I wonder if attempts were made to find logics with a zero-one law which are more expressive than first-order logic and which express properties like connectivity and hamiltonicity.

A: Yes, you bet. It is easy to see that second-order logic violates the zero-one law and the convergence law. You can write a formula saying that the cardinality of the universe is even. Matt Kaufmann and Saharon Shelah proved that the convergence law fails miserably in the case of monadic second-order logic [KS]. Kaufmann went on to show that even existential monadic second-order logic violates the convergence law [Ka].

Apparently, the first positive result in this direction has been proved by Talanov, who established the zero-one law for first-order logic extended with a transitive closure operator [Ta]. His logic is able to express graph connectivity. Unfortunately, his paper was published in an obscure place and went unnoticed. Blass, Gurevich and Kozen proved the zero-one law for fixed-point logic [BGK], which is more expressive (*cf.* [TK]). Recently Kolaitis and Vardi proved the zero-one law for the infinitary logic $L^{\omega}_{\infty,\omega}$ which is even more expressive.

Q: In what sense is that last logic infinitary?

A: Formulas can be infinitely long. Actually, the syntax of $L^{\omega}_{\infty,\omega}$ is very easy to describe. Formulas are built from atomic formulas by means of connectives $\neg, \wedge, \vee$ and quantifiers $\forall$ and $\exists$. The novelty, in comparison to first-order logic, is that you are allowed to form the conjunction and disjunction of an arbitrary set of formulas provided that the total number of predicate symbols and the total number of individual variables in these formulas is finite. The semantics is obvious.

Q: It's a joke. Formulas are supposed to be writable on a sheet of paper.

A: Be broader-minded. Fragments of $L^{\omega}_{\infty,\omega}$ allow succinct presentations, and certainly there is nothing wrong in proving a zero-one law for infinite formulas.

Q: I do not see what do infinite conjunctions and disjunctions buy you if you keep the number of individual variables bounded.

A: The trick is to reuse variables. Here is an example in the language of graphs with edge relation E. Consider the first-order formulas

$$\pi_1(u,v) = E(u,v), \quad \pi_{n+1}(u,v) = (\exists w)[E(u,w) \wedge (\exists u)(u = w \wedge \pi_n(u,v))].$$

Each of them has (the same) two free variables, and only three variables altogether. Of course, the meaning of π_n is that there exists a path of length n from u to v. Thus, the infinite formula

$$\forall u \forall v \bigvee_{n=1}^{\infty} \pi_n$$

expresses connectivity.

The quantifier elimination proof of the zero-one law for first-order logic can be modified to establish the zero-one law for $L^{\omega}_{\infty,\omega}$ [KV4]. Would you like to try? It should be instructive.

Q: Sure. By induction on a formula ϕ, we prove that that there is k such that ϕ is equivalent to some quantifier-free formula Φ (with the same predicate symbols) on models of ε_k. I can require that Φ is finite, but this does not matter. An infinitary quantifier-free formula with finite many predicate symbols and individual variables is logically equivalent to a finite quantifier-free formula.

Since $\bigvee_{i \in I} \phi_i \longleftrightarrow \neg \bigwedge_{i \in I} \neg \phi_i$, we need only to consider one new case $\phi = \bigwedge_{i \in I} \phi_i$ in the induction step. Without loss of generality, all formulas ϕ_i have the same free variables. By induction hypothesis, for each i, there exists k_i such that ϕ_i is equivalent to a quantifier-free formula Φ_i on models of ε_{k_i}. Now I am in trouble. If there is a finite bound k for all k_i then ϕ is equivalent to the conjunction of formulas Φ_i on models of ε_k. How do I ensure the existence of such a bound?

A: You did not take full advantage of the restriction on the number of variables. Strengthen the induction claim by requiring that the desired k does not exceed the number of variables (all variables, bound and free) in ϕ.

Q: OK, let me give another try. The basis of induction is trivial, the case of negation is obvious, and the treatment of the existential quantifier above seems to be fine. In the case of infinite conjunction, I can continue the argument above. By the induction hypothesis, each k_i is bounded by the number of variables in ϕ_i and therefore by the number of variables in ϕ. This gives the desired bound and finishes the argument. Nice.

By the way, I remember seeing another Kolaitis-Vardi paper on zero-one laws. It was somehow related to that classification of prefix classes that you were talking about a year ago [Gu2].

A: Oh, yes. This is also an interesting story. You may want to read the survey [KV2] of Kolaitis and Vardi. They notice that every universal second-order sentence $(\forall P)\phi(P)$ satisfied by the infinite random structure (of the appropriate signature) follows from some extension axiom and thus is almost sure. Here ϕ is first-order.

Q: That seems quite mysterious.

A: The proof is simple. The crucial observation is that an extension axiom is consistent with $(\exists P)\neg\phi(P)$ if and only if it is consistent with the first-order formula $\neg\phi$. This observation allows us to use the usual theorems about first-order logic. Suppose that every extension axiom is consistent with $\neg\phi$. By the compactness theorem, $\neg\phi$ is consistent with the whole collection of extension axioms; let A be a model of all these sentences. By the Löwenheim-Skolem Theorem, A has a countable substructure B satisfying all these sentences. Since B satisfies all extension axioms, it is the infinite random structure with an additional relation P. Since B satisfies $\neg\phi$, the infinite random structure fails to satisfy $(\forall P)\phi(P)$. That's it. Instead of $(\forall P)\phi(P)$, we could speak about $(\forall \bar{P})\phi(\bar{P})$ where $\bar{P}$ is a tuple of predicate symbols.

Q: This does not prove the zero-one law for universal second-order sentences, does it? It leaves the possibility that some existential second-order sentence holds on the infinite random structure but is not almost sure. Does this really happen?

A: What do you think? This question is not difficult.

Q: Then there has to be a counterexample, I feel. Right. I got it. There exists an order without a last element on the infinite graph, but of course there is no such thing on any finite graph.

A: Good. Kolaitis and Vardi investigated fragments $E(\Pi)$ of existential second-order logic. Here Π is a prefix type and $E(\Pi)$ is the collection of existential second-order sentences $(\exists \bar{P})\phi(\bar{P})$ where ϕ is a prenex first-order sentence with prefix of type Π. They proved for example that $E(\exists^*\forall^*)$ obeys the zero-one law. That particular proof is easy and I can explain it.

Q: I am listening.

A: Let $\phi(\bar{P}) = (\exists u_1 \ldots \exists u_m)(\forall \bar{v})\Phi(\bar{P}, u_1, \ldots, u_m, \bar{v})$ where Φ is quantifier-free, and suppose that the existential second-order formula $\phi^* = (\exists \bar{P})\phi(\bar{P})$ holds on the infinite random structure S of the appropriate signature, namely the signature σ that

comprises free predicate symbols of ϕ^*. We will show that, on finite (and countable) structures, ϕ^* follows from the extension axiom ε_m (in signature σ). For simplicity, I suppose that $\bar{P}$ is just one predicate variable P.

Fix a particular value P_0 of P and particular elements $a_1, \ldots, a_m$ of S such that $S \models (\forall \bar{v})\Phi(P_0, a_1, \ldots, a_m, \bar{v})$. Let A be the substructure with elements $a_0, \ldots, a_m$. Notice that every substructure A' of S containing A satisfies ϕ^* (with P equal to the restriction of P_0 to A' and with $u_1 = a_1, \ldots, u_m = a_m$). Now let B be an arbitrary finite model of ε_m. Obviously, B has a substructure isomorphic to A. In other words, there exists a partial isomorphism f from B to S whose range is A. Since S satisfies all extension axioms, f can be extended to an isomorphism from B onto a substructure A' of S that contains A. Since ϕ^* holds on A', it holds on B as well.

Q: You told me that prefix types, ordered by inclusion, form a well partially ordered set [Gu2]. I would like to see how this applies to the situation at hand. Let F^+ (resp. F^-) be the collection of fragments $E(\Pi)$ that obey (resp. violate) the zero-one law. Because of the well partial ordering, the collection of minimal members of F^- is finite and every member of F^- includes some minimal member.

A: We can say more about F^+ and F^-. Notice that the union of fragments satisfying the zero-one law satisfies the zero-one law. It follows that every minimal member of F^- has the form $E(\{s\})$ where s is a particular prefix. Further, do you remember special prefix types?

Q: Yes. A type is special if it contains all prefixes or is represented by a string in the 4-letter alphabet $\{\forall, \exists, \forall^*, \exists^*\}$. I remember also that the union of any ascending chain of special types is special.

A: Right. In particular, let Π be the collection of prefixes s such that $E(\{s\})$ obeys the zero-one law. Obviously, $E(\Pi)$ is the greatest element of F^+. It is easy to see that Π is the union a finite collection of special types Π_i, namely the maximal special subtypes of Π. Let me say that a fragment $E(\Pi')$ is special if the prefix type Π' is special. Then the fragments $E(\Pi_i)$ are the maximal special members of F^+.

Q: Are the maximal special members of F^+ known? Are the minimal members of F^- known?

A: The maximal special members of F^+ are $E(\exists^*\forall^*)$ and $E(\exists^*\forall\exists^*)$, and the minimal members of F^- are $E(\forall\exists\forall)$ and $E(\forall^2\exists)$. The two zero-one laws and the failure of the zero-one law for $E(\forall\exists\forall)$ were proved by Kolaitis and Vardi; the proofs are found in their survey [KV2]. Pacholski and Szwast proved that $E(\forall^2\exists)$ violates the zero-one law [PS1, PS2]; they used a technique developed by Goldfarb in order to prove the undecidability of the satisfiability problem for $\forall^2\exists$ sentences with equality [Go].

Q: At the beginning of this conversation, you told me that the zero-one phenomenon is common in combinatorics. Do you see zero-one laws for various logics as sort of an "explanation" of the combinatorial phenomenon? If yes, how successful was the explanation?

A: I do not think that either of the discoveries [GKLT, Fa1] was driven by the enthusiasm to "explain" the combinatorial phenomenon, but the paper [BH] of Blass and Harary projects this contagious enthusiasm. This enthusiasm drove us to generalize the zero-one law to fixed-point logic and, I believe, it was an important motivation for Kolaitis and Vardi.

The success of the explanation is partial. Blass and Harary list numerous natural properties of graphs expressible in first-order logic and thus obeying the zero-one law. For example, almost surely, the diameter of a graph is 2. However, it is easier to check directly that all those properties obey the zero-one law. More interesting graph properties, like connectivity, 3-colorability, hamiltonicity or rigidity, are not expressible in first-order logic.

Q: But almost sure connectivity follows from the almost sure property that the diameter equals 2, which is first-order.

A: That is true. Also, the negation of 3-colorability follows from the almost sure first-order property that there exists a complete 4-vertex subgraph. Still, neither connectivity nor 3-colorability is expressible in first-order logic. Connectivity is expressible in Talanov's logic though, and 3-colorability (as well as any k-colorability with $k \geq 2$) is expressible by a sentence in $E(\forall^2) \subseteq E(\exists^*\forall^*)$ [KV2]. But none of the zero-one laws above "explains" hamiltonicity or rigidity: Blass and Harary prove that neither hamiltonicity nor rigidity follow from any extension axiom [BH].

Q: How can you prove that?

A: Here is a sketch of the proof that graph rigidity does not follow from ε_k. Pick a graph G with vertices $-l, -l+1, \ldots, l-1, l$ randomly subject to the constraint that the function $f(i) = -i$ be an automorphism of G. It is not too difficult to check that with high probability G satisfies ε_k provided l is sufficiently large. Thus there exists a nonrigid graph that satisfies ε_k.

Blass and Harary pose a problem to find "a natural class of properties, broader than the class of first-order properties", that includes "properties like hamiltonicity and rigidity" and obeys the zero-one law. This problem is still wide open.

Q: On the other hand, there are probably many interesting properties expressible in fixed-point logic or $L^{\omega}_{\infty,\omega}$ that combinatorialists did not consider.

A: That is true. Many problems complete for polynomial time are expressible in fixed-point logic. Many problems complete for polynomial space are expressible in partial fixed-point logic, which is sandwiched between fixed-point logic and $L^{\omega}_{\infty,\omega}$ from the point of view of expressive power [KV2].

Q: What is the relevance of zero-one laws to computer science? Let me play devil's advocate. Was there any direct application of zero-one laws to computer science?

A: In a similar vein you can claim that modern group theory or graph theory is irrelevant to physics. It is conceivable that even if all pure mathematical research were

stopped, physics would develop without impediments for a while. But eventually physics would suffer greatly. In addition to being used directly in physics, mathematical education creates an atmosphere of rigor necessary to raise good physicists.

Q: This may justify theoretical computer science at large, but maybe zero-one laws do not belong there.

A: Actually, I was thinking about an analogy for logic vs. computer science rather than for theoretical computer science vs. applied computer science.

Q: I do not doubt the relevance of zero-one laws to logic. But why is this kind of logic relevant to computer science? Do you think it is relevant?

A: Yes, I do. By the way, relevance is not by itself a zero-one notion. It can be quantified. I do not know any direct applications of zero-one laws to, say, complexity theory, but such applications are certainly possible especially in the context of probabilistic algorithms that usually run fast or the average case analysis of deterministic algorithms [Va]. The case of decreasing edge probability [SS, Sp, Ly3] may be especially relevant because that probabilistic model is very popular in complexity theory. Even the uniform distribution is not irrelevant. If you have to deal with a database about which you do not know anything, you may as well suppose that it is drawn randomly.

Q: No, this does not sound convincing. Natural databases satisfy all kind of dependencies.

A: Maybe, it is worth checking whether the zero-one law (I am assuming that database queries are first-order and I am talking about the zero-one law for first-order logic) survives the imposition of dependencies.

It is important, however, to see zero-one laws in the context of finite model theory. Logic changed many mathematical fields; set theory is a good example. Its influence in computer science is even greater. The development of finite model theory reflects the desire to take the new applications seriously.

Q: You mean, it would be expensive to maintain an infinite database?

A: Exactly. Well, I spoke enough of the importance of finite model theory [Gu1]. Zero-one laws are integral part of inherently-finite model theory and are very important in this context. Am I succeeding in my propaganda?

Q: Let me think about it.

Acknowledgment. Many thanks to Andreas Blass for very beneficial and enjoyable discussions and to Ron Fagin, Warren Goldfarb, Jim Lynch, Leszek Pacholski and Moshe Vardi for very helpful comments.

References:

Bl Andreas Blass, private communication.

BGK Andreas Blass, Yuri Gurevich and Dexter Kozen, "A Zero-One Law for Logic with a Fixed-Point Operator", Information and Control 67 (1985), 70–90.

BH Andreas Blass and Frank Harary, "Properties of Almost All Graphs and Complexes", J. Graph Theory 3 (1979), 225–240.

Co1 Kevin J. Compton, "The Computational Complexity of Asymptotic Problems I: Partial Orders", Information and Computation 78:2 (1988), 108–123.

Co2 Kevin J. Compton, "0–1 Laws in Logic and Combinatorics", Proc. NATO Advanced Study Institute on Algorithms and Order (I. Rival, ed.), Reidel, Dordrecht, 1988, 353–383.

Eh Andrzej Ehrenfeucht, "An Application of Games to the Completeness Problem for Formalized Theories", Fund. Math. 49 (1961), 129–141.

Fa1 Ronald Fagin, "Probabilities on Finite Models", J. Symbolic Logic 41:1 (1976), 50–58. (Notices of AMS, Oct. 1972.)

Fa2 Ronald Fagin, "Finite-Model Theory: A Personal Perspective", Springer Lecture Notes in Computer Science 470 (1990), 3–24. To appear in Theoretical Computer Science.

GKLT Y. V. Glebsky, D. I. Kogan, M. I. Liogonky and V. A. Talanov, "Range and Degree of Realizability of Formulas in the Restricted Predicate Calculus", Kibernetika (Kiev) 2 (1969), 17–28. English translation in Cybernetics 5 (1969), 142–154.

Go Warren D. Goldfarb, "The Unsolvability of the Gödel Class", J. Symb. Logic 49 (1984), 1237–1252.

Gr Etienne Grandjean, "Complexity of the First-Order Theory of Almost All Structures", Information and Control 52 (1983), 180–204.

Gu1 Yuri Gurevich, "Logic and the Challenge of Computer Science", In "Current Trends in Theoretical Computer Science" (ed. E. Börger), Computer Science Press, 1988, 1–57.

Gu2 Yuri Gurevich, "On the Classical Decision Problem", Bulletin of European Assoc. for Theor. Computer Science, Oct. 1990, 140–150.

HP Frank Harary and Edgar M. Palmer, "Graphical Enumeration", Academic Press, New York and London, 1973.

Ka Matt Kaufmann, "A Counterexample to the 0–1 Law for Existential Monadic Second Order Logic", Internal Note 32, Computational Logic, Inc., December 1987.

KS Matt Kaufmann and Saharon Shelah, "On Random Models of Finite Power and Monadic Logic", Discrete Mathematics 54 (1983), 285–293.

KR D. J. Kleitman and B. L. Rothschild, "Asymptotic enumeration of partial orders on a finite set", Trans. Amer. Math. Soc. 205 (1975), 205–220.

Kn V. V. Knyazev, "Iterative Extensions of First-Order Logic", Math. Problems in Cybernetics, Moscow, 1989, 123–130 (Russian). Math. Reviews 91a:03062.

KPR P. G. Kolaitis, H. J. Prömel and B. L. Rothschild, "K_{l+1}-Free Graphs: Asymptotic Structure and a 0–1 Law", Trans. Amer. Math. Soc. 303, no.2 (Oct. 1987), 637–671.

KV1 Phokion G. Kolaitis and Moshe Y. Vardi, "The Decision Problem for the Probabilities of Higher-Order Properties", Symp. on Theory of Computing, ACM, 1987, 425–435.

KV2 Phokion G. Kolaitis and Moshe Y. Vardi, "0–1 Laws for Fragments of Second-Order Logic: An Overview", MSRI Workshop on Logic from Computer Science (ed. Yiannis N. Moschovakis), Berkeley 1989, to appear.

KV3 Phokion G. Kolaitis and Moshe Y. Vardi, "0–1 Laws and Decision Problems for Fragments of Second-Order Logic", Information and Computation 87 (1990), 302–338.

KV4 Phokion G. Kolaitis and Moshe Y. Vardi, "Infinitary Logics and 0–1 Laws", Research Report 8195 (75154), IBM, June 1991, to appear in Information and Computation (a special issue on LICS'90).

Li M. I. Liogonky, "On the Question of Quantitative Characteristics of Logical Formulae", Kibernetika (Kiev) 3 (1970), 16–22. English translation in Cybernetics 6 (1970), 205–211.

Ly1 James F. Lynch, "Almost Sure Theories", Annals of Mathematical Logic 18 (1980), 91–135.

Ly2 James F. Lynch, "Probabilities of First-Order Sentences about Unary Functions", Transactions of American Mathematical Society 287 (1985), 543–568.

Ly3 James F. Lynch, "Probabilities of Sentences about Very Sparse Random Graphs", Random Structures and Algorithms 3 (1992), 33-53.

PS1 Leszek Pacholski and Wieslaw Szwast, "Asymptotic Probabilities of Existential Second Order Gödel Sentences", Journal of Symbolic Logic 56 (1991), 427–438.

PS2 Leszek Pacholski and Wieslaw Szwast, "On the 0–1 Law for the Class of Existential Second Order Minimal Gödel Sentences with Equality", Proc. 6th Annual Symposium on Logic and Computer Science, IEEE, 1991, 280–285.

Sp Joel Spencer, "Threshold Spectra via the Ehrenfeucht Game", Discrete Appl. Math. 30 (1991), 235–252.

SS Saharon Shelah and Joel Spencer, "Zero-One Laws for Sparse Random Graphs", J. Amer. Math. Soc. 1 (1988), 97–115.

St Larry Stockmeyer, "The Polynomial-Time Hierarchy", Theoretical Computer Science 3 (1977), 1–22.

Ta V. A. Talanov, "Asymptotic Solvability of Logical Formulas", in "Combinatorial-Algebraic Methods in Applied Mathematics", Gorky University, USSR, 1981, 118–126 (Russian). Math. Reviews 85i:03081.

TK V. A. Talanov and V. V. Knyazev, "The Asymptotic Truth Value of Infinite Formulas", Proc. of the All-Union Seminar on Discrete Math. and its Applications, Moscow, 1986, 56–61 (Russian). Math Reviews 89g:03054.

Tr Boris A. Trachtenbrot, "The Impossibility of an Algorithm for the Decision Problem for Finite Models", Dokl. Akad. Nauk SSSR 70 (1950), 569–572.

Va Moshe Y. Vardi, private communication.