Session I: Monday, August 14

Track C: Random Finite Models

James F. Lynch

1 Fundamental Zero-One Laws

Let us begin by introducing the conventions we will use. $\mathcal{L}$ will denote a logic with a fixed vocabulary. $\mathcal{C}_0$, $\mathcal{C}_1$, $\mathcal{C}_2$, ... will stand for a sequence of $\mathcal{L}$-structures where all structures in $\mathcal{C}_n$ have $\{0, \ldots, n-1\}$ as universe. For every $n \in \omega$, pr_n is a probability measure on $\mathcal{C}_n$. For a sentence $\sigma \in \mathcal{L}$, we put $\mathrm{pr}(\sigma, n)$ for

$$\mathrm{pr}_n(\{\mathfrak{A} \in \mathcal{C}_n : \mathfrak{A} \models \sigma\}) .$$

In this series of lectures, we will examine the kinds of behavior $\mathrm{pr}(\sigma, n)$ shows for growing n (given $\mathcal{L}$, $(\mathcal{C}_n)_{n\in\omega}$, and $(\mathrm{pr}_n)_{n\in\omega}$). The following phenomena will be considered:

Zero-one Law: for every $\sigma \in \mathcal{L}$, $\lim_{n\to\infty} \mathrm{pr}(\sigma, n)$ exists and is either 0 or 1.

Convergence Law: for every $\sigma \in \mathcal{L}$, $\lim_{n\to\infty} \mathrm{pr}(\sigma, n)$ exists.

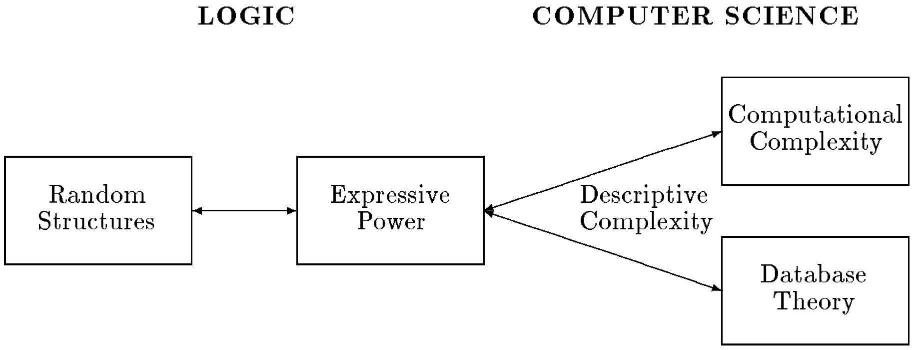
Nonconvergence: there is at least one $\sigma \in \mathcal{L}$ such that $\lim_{n\to\infty} \mathrm{pr}(\sigma, n)$ does not exist.

Subsequence Convergence: for every $\sigma \in \mathcal{L}$ there exists a finite partition of ω into infinite sets such that $\mathrm{pr}(\sigma, n)$ converges on every set of the partition.

Slow Variation: for every $\sigma \in \mathcal{L}$, $|\mathrm{pr}(\sigma, n) - \mathrm{pr}(\sigma, n+1)|$ is asymptotic to 0.

The term "slow variation" comes from the theory of generalized limits. The term "very weak 0-1 law" has been used in the theory of random finite structures for the same notion, but we prefer the former phrase, since it is already in use and is more accurate.

This diagram shows the relationship of our topic, Random Structures, to the other topics of the Finite Model Theory Tutorials and to Computer Science.



As will be shown in the other two tracks of these tutorials, Descriptive Complexity provides a bridge between Expressive Power of Logics and Database Theory and Computational Complexity. Problems in one area can be reformulated in the other area. The links between Random Structures and Computer Science are more indirect. Techniques of Expressive Power such as pebble games, play a vital role in Random Structures. Conversely, characterizations of various logics in terms of asymptotic probabilities of sentences can imply limitations on the expressive power of the logics. This, in turn, can establish limitations on the power of database languages and lower bounds in Computational Complexity. However, inexpressibility results in Finite Model Theory that have been obtained using random structure methods can usually be proven more directly.

In this lecture, we will give several proofs of the classic zero-one law for structures of a purely relational type, with a uniform probability distribution (i.e., all structures of a given size are equally likely). We will begin with a theorem by Gaifman, a zero-one law for countable structures. This result was proven before the zero-one laws for finite structures, but our interest in Gaifman's theorem is not strictly historical. The ideas used in the proof are central to the proofs we will present for the finite case, and can be extended to many more complex cases.

For simplicity, let us consider the case of a vocabulary with one r-ary relational symbol, R. Let U be a finite or countable set. In the cases examined in this lecture,

$$\begin{aligned} U &= \{0,1,\ldots,\} = \omega, \text{ or} \\ U &= \{0,1,\ldots,n-1\} = n \text{ for some } n \in \omega. \end{aligned}$$

U^r is the set of all r-tuples in U. Let μ be the standard product measure on 2^{U^r}, the power set of U^r. That is, for any $(a_1,\ldots,a_r) \in U^r$,

$$\mu(\{R \subseteq U^r : R(a_1,\ldots,a_r)\}) = \mu(\{R \subseteq U^r : \neg R(a_1,\ldots,a_r)\}) = 2^{-1}.$$

More generally, for any finite sets $A, B \subseteq U^r$ such that $A \cap B = \emptyset$,

$$\mu(\{R \subseteq U^r : A \subseteq R \wedge B \cap R = \emptyset\}) = 2^{-|A|-|B|}. \tag{1}$$

Sets of the form given in (1) are basic sets. The function μ can be extended to all measureable subsets of 2^{U^r}, and if S is a measurable set, then $\mu(S)$ is the probability that a random relation $R \subseteq U^r$ is in S.

When $|U| = \aleph_0$, there are non-measurable subsets of 2^{U^r}, but we will never see them since all our sets will be relations definable in first-order logic, and therefore Borel. When $|U| < \aleph_0$, all sets $S \subseteq 2^{U^r}$ are measurable, and

$$\mu(S) = \frac{|S|}{2^{|U|^r}}.$$

To take a common example, when $r = 2$ and $U = n \in \omega$, n^2 is the set of all ordered pairs on n, and 2^{n^2} is the set of all binary relations on n. Each $R \subseteq n^2$ can be identified with an $n \times n$ matrix of 0's and 1's where, for $i, j \in n$,

$$M_{i,j} = 1 \iff R(i,j).$$

Then $\mu(\{R\}) = 2^{-n^2}$ by (1), and, for any $S \subseteq 2^{n^2}$,

$$\mu(S) = \sum_{R \in S} \mu(\{R\}) = \frac{|S|}{2^{n^2}}.$$

This means that $\mu(S)$ is just the cardinality of S over the number of binary relations on U.

As above, given a logical language $\mathcal{L}$ over the vocabulary of an r-ary relation, we identify a sentence $\sigma \in \mathcal{L}$ with the set of relations it defines, and we put

$$\mu(\sigma) = \mu(\{R \subseteq U^r : \langle U, r\rangle \models \sigma\}).$$

Gaifman's theorem is the following.

Theorem 1.1 (Gaifman, 1964) *Let $\mathcal{L}$ be a relational first-order language and U a countable set. Then for every $\sigma \in \mathcal{L}$,*

$$\mu(\sigma) = 0 \text{ or } 1.$$

To prove this theorem, we will construct a consistent, complete theory T and show that every $\sigma \in T$ is true with probability 1. [As noted by Thomas Wilke, in the presence of a compactness theorem the existence of such a theory is an immediate consequence of the theorem itself.]

We will use the following definitions.

- A *basic formula* in the variables $x_1, \ldots, x_k$ is an atomic formula $R(y_1, \ldots, y_r)$ or its negation, where each $y_i \in \{x_1, \ldots, x_k\}$.

- A *k-type* (k a natural number) is a conjunction of the form

$$\bigwedge_{i=1}^{m} \alpha_i(x_1, \ldots, x_k)$$

  where $\{\alpha_i : 1 \leq i \leq m\}$ is consistent and complete, i.e., it is a maximal satisfiable set of basic formulas in $x_1, \ldots, x_k$; the logical constant TRUE is the only 0-type.

- A $(k+1)$-type $\gamma(x_1, \ldots, x_{k+1})$ *extends* a k-type $\beta(x_1, \ldots, x_k)$ if every conjunct of β is a conjunct of γ. In other words, β and γ agree on $x_1, \ldots, x_k$.

- For every $k \in \omega$, A_k is the set containing all sentences

$$\forall x_1 \ldots \forall x_k (\beta(x_1, \ldots, x_k) \rightarrow \exists x_{k+1}(\gamma(x_1, \ldots, x_{k+1}) \wedge \bigwedge_{i=1}^{k} x_{k+1} \neq x_i))$$

  where γ is a $(k+1)$-type extending a k-type β; note that $A_{k+1} \models A_k$.

- The set

$$A = \bigcup_{k \in \omega} A_k$$

  is the set of *extension axioms.*

Informally, a structure satisfies the extension axioms if every finite substructure can be finitely extended in every possible way. Again taking the example of the vocabulary of one binary relation, let $\beta(x_1, \ldots, x_k)$ be a k-type, $I, J, K, L \subseteq \{1, \ldots, k\}$ such that $I \cup J = K \cup L = \{1, \ldots, k\}$ and $I \cap J = K \cap L = \emptyset$. Let $\delta(x_{k+1})$ be $R(x_{k+1}, x_{k+1})$ or $\neg R(x_{k+1}, x_{k+1})$. Then

$$\begin{aligned}
&\beta(x_1, \ldots, x_k) \\
&\wedge(\bigwedge_{i \in I} R(x_i, x_{k+1})) \wedge (\bigwedge_{i \in J} \neg R(x_i, x_{k+1})) \\
&\wedge(\bigwedge_{i \in K} R(x_{k+1}, x_i)) \wedge (\bigwedge_{i \in L} \neg R(x_{k+1}, x_i)) \\
&\wedge \delta(x_{k+1})
\end{aligned}$$

is a $(k+1)$-type extending β, and all $(k+1)$-types extending β are obtained this way.

Theorem 1.2 *A is consistent, has no finite models, and is $\aleph_0$-categorical.*

[A set of sentences is $\aleph_0$-categorical if it has only one (up to isomorphism) countable model.]

Proof. By compactness, in order to show that A is consistent it is sufficient to show that A_k is consistent for every k. To construct a model of A_k start from the empty structure and add more and more elements to make sure that every substructure with at most k elements can be extended by one element in every possible way; the limit will do it. The details are left as an exercise. It is evident that A has no finite models.

To show that any two countable models of A are isomorphic, we use a back-and-forth argument very similar to the one that shows any two countable dense linear orders without endpoints are isomorphic. The crucial part goes as follows. Let $\mathfrak{A}$ and $\mathfrak{B}$ be two infinite countable models of A, say their universes are $\{a_i : i \in \omega\}$ and $\{b_i : i \in \omega\}$ respectively. We construct the isomorphism in stages. After each stage k, there will be subsets $C_k \subseteq \{a_i : i \in \omega\}$ and $D_k \subseteq \{b_i : i \in \omega\}$ such that $\mathfrak{A} \restriction C_k \cong \mathfrak{B} \restriction D_k$ and $|C_k| = 2k$. Initially, $A_0 = B_0 = \emptyset$.

Inductively, assume stage k has been completed, say

$$\begin{aligned} C_k &= \{c_1, \ldots, c_{2k}\} \text{ and} \\ D_k &= \{d_1, \ldots, d_{2k}\}, \end{aligned}$$

where $c_j \mapsto d_j$ for $1 \leq j \leq 2k$ is the partial isomorphism that has been constructed so far. Let c_{2k+1} be the least element of $\{a_i : i \in \omega\} - C_k$, β denote the $2k$-type of $c_1, \ldots, c_{2k}$ in $\mathfrak{A}$ and γ denote the $(2k+1)$-type of $c_1, \ldots, c_{2k+1}$. Then

$$\begin{aligned} (\mathfrak{A}, c_1, \ldots, c_{2k}) &\models \beta(x_1, \ldots, x_{2k}) \text{ and} \\ (\mathfrak{A}, c_1, \ldots, c_{2k+1}) &\models \gamma(x_1, \ldots, x_{2k+1}), \end{aligned}$$

and, since $c_j \mapsto d_j$ is a partial isomorphism,

$$(\mathfrak{B}, d_1, \ldots, d_{2k}) \models \beta(x_1, \ldots, x_{2k}).$$

By the assumption that $\mathfrak{B}$ is a model of A, we know that there exists $d_{2k+1} \in \{b_i : i \in \omega\}$ such that

$$(\mathfrak{B}, d_1, \ldots, d_{2k+1}) \models \gamma(x_1, \ldots, x_{2k+1}),$$

so the partial isomorphism can be extended to $c_{2k+1} \mapsto d_{2k+1}$. In a similar way, but starting with d_{2k+2} being the least element of $\{b_i : i \in \omega\} - (D_k \cup \{d_{2k+1}\})$, we extend it to $c_{2k+2} \mapsto d_{2k+2}$. Then $C_{k+1} = C_k \cup \{c_{2k+1}, c_{2k+2}\}$ and $D_{k+1} = D_k \cup \{d_{2k+1}, d_{2k+2}\}$.

By construction,

$$\begin{aligned} \{a_i : i \in \omega\} &= \bigcup_{k=1}^{\infty} C_k, \\ \{b_i : i \in \omega\} &= \bigcup_{k=1}^{\infty} D_k, \text{ and} \\ \mathfrak{A} &\cong \mathfrak{B}. \end{aligned}$$

□

In the following, we will put T for the theory of A. The Los-Vaught test (which, in particular, asserts that a set of sentences is a complete theory if it is consistent, has no finite models, and is $\aleph_0$-categorical) implies the following.

Corollary 1.3 *T is a consistent and complete theory.*

Lemma 1.4 *For every $\alpha \in A$, $\mu(\alpha) = 1$.*

Proof. We show that $\mu(\neg\alpha) = 0$. For notational convenience, let $\bar{x}$ stand for $x_1, \ldots, x_k$, and $\alpha = \forall x_1 \ldots \forall x_k (\beta(\bar{x}) \rightarrow \exists x_{k+1}(\gamma(\bar{x}, x_{k+1}) \wedge \bigwedge_{i=1}^{k} x_{k+1} \neq x_i))$. For any $a_1, \ldots, a_{k+1} \in U$ such that $\bigwedge_{i=1}^{k} a_{k+1} \neq a_i$,

$$\mu(\beta(\bar{a}) \wedge \neg\gamma(\bar{a}, a_{k+1})) = \mu(\beta(\bar{a}))(1 - 2^{-c})$$

for some $c \geq 1$. [Recall the example when the vocabulary consists of one binary relation.] By independence,

$$\begin{aligned} \mu(\beta(\bar{a}) \wedge \forall x_{k+1}(\neg\gamma(\bar{a}, x_{k+1}) \vee \bigvee_{i=1}^{k} x_{k+1} = x_i)) &\leq \lim_{n\rightarrow\infty} (1 - 2^{-c})^n \\ &= 0, \end{aligned}$$

and by countable additivity,

$$\begin{aligned} \mu(\neg\alpha) &= \mu(\exists x_1 \ldots \exists x_k (\beta(\bar{x}) \wedge \forall x_{k+1}(\neg\gamma(\bar{x}, x_{k+1}) \vee \bigvee_{i=1}^{k} x_{k+1} = x_i))) \\ &= 0. \end{aligned}$$

□

Lemma 1.5 *For every $\sigma \in T$, $\mu(\sigma) = 1$.*

Proof. Since $A \models \sigma$, by compactness there is a finite set $\{\alpha_1, \ldots, \alpha_m\} \subseteq A$ such that

$$\models \bigwedge_{i=1}^{m} \alpha_i \rightarrow \sigma\,,$$

hence

$$\models \neg\sigma \rightarrow \bigvee_{i=1}^{m} \neg\alpha_i\,,$$

thus

$$\mu(\neg\sigma) \leq \mu(\bigvee_{i=1}^{m} \neg\alpha_i) \leq \sum_{i=1}^{m} \mu(\neg\alpha_i) = 0\,, \tag{2}$$

where the first inequality is obvious, the second is due to the subadditivity of the measure, and the equality follows from Lemma 1.4. From (2) we obtain $\mu(\sigma) = 1$. $\square$

Finally, we may complete the proof of Theorem 1.1.

Proof of Theorem 1.1. For any $\sigma \in \mathcal{L}$, since T is complete, either $\sigma \in T$ or $\neg\sigma \in T$. In the first case, $\mu(\sigma) = 1$ by Lemma 1.5. In the second case, $\mu(\neg\sigma) = 1$, which implies $\mu(\sigma) = 0$. $\square$

This proof is an example of the *transfer principle*: letting $\mathfrak{A}$ be the unique countable model of A,

$$\mathfrak{A} \models \sigma \Leftrightarrow \mu(\sigma) = 1.$$

That is, almost sure truth on random structures is transferred to absolute truth on $\mathfrak{A}$.

The rest of this lecture is dedicated to a finite version of Theorem 1.1, our first zero-one law. $\mathcal{L}$ is assumed to be as before, i.e., to be the first-order language of one r-ary relation; pr_n is the standard product measure μ on 2^{n^r}.

Theorem 1.6 (Fagin, 1976; Glebskiĭ et al. , 1969) *For every $\sigma \in \mathcal{L}$, $\lim_{n\to\infty} \mathrm{pr}(\sigma, n)$ exists and is equal to 0 or 1.*

We will give two proofs of this theorem, the first one based on Fagin's proof, which is another example of the transfer principle. It uses the fact that A is a consistent and complete theory (see Corollary 1.3 above) and the following two lemmas, which are finitistic versions of Lemmas 1.4 and 1.5.

Lemma 1.7 *For every $\alpha \in A$, $\lim_{n\to\infty} \mathrm{pr}(\alpha, n) = 1$.*

Proof. Let $\beta(\bar{x})$ and $\gamma(\bar{x}, x_{k+1})$ be as in the proof of Lemma 1.4. For any $a_1, \ldots, a_{k+1} \in n$ such that $\bigwedge_{i=1}^{k} a_{k+1} \neq a_i$,

$$\mathrm{pr}(\beta(\bar{a}) \wedge \neg\gamma(\bar{a}, a_{k+1}), n) = \mathrm{pr}(\beta(\bar{a}), n)(1 - 2^{-c})$$

for some $c \geq 1$. By independence,

$$\mathrm{pr}(\beta(\bar{a}) \wedge \forall x_{k+1}(\neg\gamma(\bar{a}, x_{k+1}) \vee \bigvee_{i=1}^{k} x_{k+1} = x_i), n) \leq (1 - 2^{-c})^{n-k}.$$

Therefore

$$\begin{aligned} \mathrm{pr}(\neg\alpha, n) &= \mathrm{pr}(\exists x_1 \ldots \exists x_k(\beta(\bar{x}) \wedge \forall x_{k+1}(\neg\gamma(\bar{x}, x_{k+1}) \vee \bigvee_{i=1}^{k} x_{k+1} = x_i)), n) \\ &\to 0 \text{ as } n \to \infty. \end{aligned}$$

$\square$

It should be noted that for this lemma (and Lemma 1.4), it is crucial that a product measure be used. This enables us to invoke the independence condition to bound joint probabilities from above.

Lemma 1.8 *For every $\sigma \in T$, $\lim_{n\to\infty} \mathrm{pr}(\sigma, n) = 1$.*

This lemma can be proved in the same way as Lemma 1.5, and it enables us to give the first proof of Theorem 1.6:

First proof of Theorem 1.6. As the proof of Theorem 1.1 but using Lemma 1.8 instead of Lemma 1.5. □

For the second – this time completely finitistic – proof of Theorem 1.6, we use the following lemma, whose full proof is left as an exercise.

Lemma 1.9 *Let $k \in \omega$ and $\mathfrak{A}$ and $\mathfrak{B}$ be models of A_k. Then $\mathfrak{A} \sim_{k+1} \mathfrak{B}$.*

Proof. The same argument explained in the proof sketch of Theorem 1.2 can be used to prove that the Duplicator has a winning strategy in the $(k+1)$-round EF game; recall that in general another way to describe that the Duplicator has a winning strategy for the EF game is to say that there exists a certain system of partial isomorphisms having the back-and-forth property. □

To finish the second proof of Theorem 1.6:

Second proof of Theorem 1.6. Let $\sigma \in \mathcal{L}$ have quantifier rank k. Let δ be the conjunction of all sentences in A_{k-1}. Then, by Lemma 1.9 and the theorem on EF games, δ defines a class of $\equiv_k$ structures. (In fact, it defines a $\equiv_k$-class.) So $\models \delta \to \sigma$ or $\models \delta \to \neg\sigma$. In the first case, we have $\lim_{n\to\infty} \mathrm{pr}(\sigma, n) \geq \lim_{n\to\infty} \mathrm{pr}(\delta, n) = 1$ by Lemma 1.8. In the second case, we have $\lim_{n\to\infty} \mathrm{pr}(\neg\sigma, n) = 1$, thus $\mathrm{pr}(\sigma, n) = 0$. □

We conclude with a summary of some related results.

Fagin also proved a zero-one law for unlabeled relational structures. For each $n \in \omega$, let $\mathcal{D}_n$ be the set of isomorphism types in $\mathcal{C}_n$. For $D \in \mathcal{D}_n$, say $D \models \sigma$ if $\mathfrak{A} \models \sigma$ for all $\mathfrak{A} \in D$. Let

$$\nu(\sigma, n) = \frac{|\{D \models \sigma : D \in \mathcal{D}_n\}|}{|\mathcal{D}_n|}.$$

Theorem 1.10 (Fagin) *For every $\sigma \in \mathcal{L}$, $\lim_{n\to\infty} \nu(\sigma, n)$ exists and is 0 or 1.*

The proof relies on the fact that almost all relational structures are rigid: $|\mathcal{D}_n| \sim |\mathcal{C}_n|/n!$.

The original proof of Theorem 1.6 by Glebskiĭ et. al. was by quantifier elimination, which also yields the following theorem.

Theorem 1.11 (Glebskiĭ et. al.) *Let $\mathcal{L}$ be a first-order language with relational symbols and constants. For each $n \in \omega$, let $\mathcal{C}$ be the class of all $\mathcal{L}$-structures on n and pr_n be the uniform probability distribution on $\mathcal{C}$. Then for every $\sigma \in \mathcal{L}$, $\lim_{n\to\infty} \mathrm{pr}(\sigma, n)$ exists and is equal to $u/2^v$ for some natural numbers u and v.*

The problem of deciding whether a given first-order sentence is true in all finite structures is undecidable (Trakhtenbrot, 1950) but co-r. e., of course. On the contrary, deciding whether $\lim_{n\to\infty} \mathrm{pr}(\sigma, n)$ is 0 or 1 is decidable. Details of the following decision procedure are left as an exercise. Given $\sigma \in \mathcal{L}$, construct δ as above, find a model $\mathfrak{A}$ of δ, and check whether $\mathfrak{A} \models \sigma$ or not; if $\mathfrak{A} \models \sigma$, then output "$\lim_{n\to\infty} \mathrm{pr}(\sigma, n) = 1$", else output "$\lim_{n\to\infty} \mathrm{pr}(\sigma, n) = 0$." A more efficient algorithm was found by Grandjean (1983), who showed that this problem is PSPACE-complete.

notes taken by Th. Wilke, wilke@dimacs.rutgers.edu

Session II: Tuesday, August 15

Track C: Random Finite Models

James F. Lynch

2 Convergence Laws from Extension Axioms

To recapitulate the first lecture, let $\mathcal{L}$ be a purely relational first-order logic. For $k \in \omega$, let A_k be the set of extension axioms for k elements. Then, under the uniform distribution, almost all finite $\mathcal{L}$-models satisfy A_k, and all models of A_k satisfy the same sentences of quantifier rank $k+1$. The 0-1 law follows immediately. It is natural to ask whether 0-1 or convergence laws hold for other classes of structures. This lecture will be on two such classes, one from mathematical logic and descriptive complexity, the other from random graph theory. Both classes violate the extension axioms, but a modified collection of extension axioms holds, and they describe a winning strategy for Duplicator in the k-round EF game.

2.1 Structures with a Successor Relation

Let the vocabulary of $\mathcal{L}$ consist of a relational symbol R of arity r plus the binary relational symbol S. R will be interpreted as a random relation on the universe. (We consider one symbol R for clarity only; all our results extend easily to any number of relational symbols $R_1, \ldots, R_m$.) S will be interpreted as a successor relation in two ways. For $n \in \omega$,

1. $\mathcal{C}_n = \{\langle n, R, S_n\rangle : R \subseteq n^r$ and $S_n = \{(i, i+1) : i < n-1\}\}$, and
2. $\mathcal{C}'_n = \{\langle n, R, S'_n\rangle : R \subseteq n^r$ and $S'_n = \{(i, i+1) :\ (\mathrm{mod}\ n) : i < n\}\}$. We will call S'_n a cyclic successor to distinguish it from the usual successor in Case 1.

For $\sigma \in \mathcal{L}$, S is interpreted as S_n in Case 1. and S'_n in Case 2. We write $y = x+1$ for $S(x,y)$. We put μ_n (resp. μ'_n) for the uniform distribution on $\mathcal{C}_n$ (resp. $\mathcal{C}'_n$). We define pr and pr$'$ similarly. For any structure $\langle A, R, \ldots\rangle$ and $B \subseteq A$, we abbreviate $\langle B, R \restriction B, \ldots\rangle$ by $\langle B, R, \ldots\rangle$.

It is easily seen that there is no 0-1 law for Case 1. Take the sentence

$$\sigma = \exists x \forall y (x \neq y+1 \wedge R(x, \ldots, x)).$$

Then $\mathrm{pr}(\sigma, n) = 1/2$ for $n > 0$. In fact, for every rational in $[0,1]$ of the form $u/2^v$ where $u, v \in \omega$, there is $\sigma \in \mathcal{L}$ such that $\mathrm{pr}(\sigma, n) = u/2^v$ for sufficiently large n. We will show that there is a convergence law for Case 1., and the asymptotic probability is always of that form. This will be an easy consequence of a 0-1 law for Case 2.

Theorem 2.1 (Lynch, 1980) *For every $\sigma \in \mathcal{L}$, $\lim_{n\to\infty} \mathrm{pr}'(\sigma, n) = 0$ or 1.*

Proof. Fix $k \in \omega$. We will show that there is some class $\mathcal{D}$ of $\mathcal{L}$ structures with a cyclic successor such that $\mathrm{pr}'(\mathfrak{A} \in \mathcal{D}, n) \to 1$ as $n \to \infty$, and all structures in $\mathcal{D}$ are $\sim_k$. The 0-1 law follows immediately.

As before, this class of structures is defined by a winning strategy for Duplicator in the k-round EF game. However, the simple strategy of the previous lecture won't work because the extension axioms fail. For example, when $n > 1$, no structure in $\mathcal{C}'_n$ satisfies $\forall x \forall y \exists z (z = x + 1 \wedge y = z + 1)$. The Duplicator must *plan ahead*, i.e., look at the "neighborhood" around each point chosen by the Spoiler, and try to match that rather than just match the chosen points. This is made precise by the following:

Definition 2.2
1. *For $a, b \in n \in \omega$, let $\delta_n(a, b) = \min\{|d| : a = b + d \pmod{n}\}$. It is easily seen that δ_n is a true metric.*
2. *For $n \in \omega$ and $d > 0$, $N_n(a, d) = \{b \in n : \delta_n(a, b) < d\}$. Thus $N_n(a, 1) = \{a\}$.*
3. *For $i, j, n \in \omega$, $\mathfrak{A} = \langle n, R, S_n \rangle$, and $a_1, \ldots, a_i \in n$, the j-closure of $a_1, \ldots, a_i$ in $\mathfrak{A}$ is*

$$\mathrm{Cl}^j(\mathfrak{A}; a_1, \ldots, a_i) = \langle \bigcup_{h=1}^{i} N_n(a_h, 3^j), R, S_n, a_1, \ldots, a_i \rangle.$$

When the context is clear, we will also use $\mathrm{Cl}^j(\mathfrak{A}; a_1, \ldots, a_i)$ to denote the universe of that structure.

Let $\mathfrak{A}_0$ and $\mathfrak{A}_1$ be two structures with cyclic successor on which the k-round EF game is to be played. Duplicator's strategy is to ensure that, after each round $i = 0, \ldots, k$,

$$\mathrm{Cl}^{k-i}(\mathfrak{A}_0; a_1, \ldots, a_i) \cong \mathrm{Cl}^{k-i}(\mathfrak{A}_1; b_1, \ldots, b_i). \tag{3}$$

This condition is trivially true when $i = 0$, and when $i = k$, it implies that Duplicator has won. Thus it remains only to prove that Duplicator can follow this strategy with high probability. The next lemma is the key fact in proving this.

Lemma 2.3 *Let $\mathfrak{A} \in \mathcal{C}_n$. With probability asymptotic to 1 as $n \to \infty$, for any $i < k$, any structure $\mathcal{C}$ with cyclic successor, and any $c_1, \ldots, c_{i+1} \in \mathcal{C}$ such that $\mathrm{Cl}^{k-i-1}(\mathcal{C}; c_{i+1}) \cap \mathrm{Cl}^{k-i-1}(\mathcal{C}; c_1, \ldots, c_i) = \emptyset$,*

$$\begin{aligned} &\forall x_1 \ldots \forall x_i (\mathrm{Cl}^{k-i-1}(\mathfrak{A}; x_1, \ldots, x_i) \cong \mathrm{Cl}^{k-i-1}(\mathcal{C}; c_1, \ldots, c_i) \to \\ &\quad \exists x_{i+1} (\mathrm{Cl}^{k-i-1}(\mathfrak{A}; x_1, \ldots, x_{i+1}) \cong \mathrm{Cl}^{k-i-1}(\mathcal{C}; c_1, \ldots, c_{i+1}). \end{aligned}$$

Note the similarity to the extension axioms A_k. Indeed, the closure operators are definable in $\mathcal{L}$, and Lemma 2.3 can be phrased as a statement that a certain finite collection of first-order axioms holds almost surely.

Proof. There are only finitely many choices for i and the isomorphism type of $\mathrm{Cl}^{k-i-1}(\mathcal{C}; c_1, \ldots, c_{i+1})$, so we may as well fix them. Let

$$\begin{aligned} s &= |\mathrm{Cl}^{k-i-1}(\mathcal{C}; c_1, \ldots, c_{i+1})|^r - |\mathrm{Cl}^{k-i-1}(\mathcal{C}; c_1, \ldots, c_i)|^r \text{ and} \\ t &= 2 \cdot 3^{k-i-1} - 1 = |\mathrm{Cl}^{k-i-1}(\mathcal{C}; c)| \text{ for any } c \in \mathcal{C}. \end{aligned}$$

Using an argument similar to Lemma 1.7, and conditioning on $\mathrm{Cl}^{k-i-1}(\mathfrak{A}; x_1, \ldots, x_i) \cong \mathrm{Cl}^{k-i-1}(\mathcal{C}; c_1, \ldots, c_i)$, for any $x_{i+1} \in n$ such that $\mathrm{Cl}^{k-i-1}(\mathfrak{A}, x_{i+1}) \cap \mathrm{Cl}^{k-i-1}(\mathfrak{A}; x_1, \ldots, x_i) = \emptyset$,

$$\mathrm{pr}'(\mathrm{Cl}^{k-i-1}(\mathfrak{A}; x_1, \ldots, x_{i+1}) \ncong \mathrm{Cl}^{k-i-1}(\mathcal{C}; c_1, \ldots, c_{i+1}), n) = 1 - 2^{-s},$$

and by independence

$$\begin{aligned} &\mathrm{pr}'(\forall x_{i+1}(\mathrm{Cl}^{k-i-1}(\mathfrak{A}; x_1, \ldots, x_{i+1}) \ncong \mathrm{Cl}^{k-i-1}(\mathcal{C}; c_1, \ldots, c_{i+1}), n) \\ &\quad \leq \ (1 - 2^{-s})^{\lfloor (n-it)/t \rfloor}. \end{aligned}$$

Therefore

$$\begin{aligned} &\mathrm{pr}'(\exists x_1 \ldots \exists x_i(\mathrm{Cl}^{k-i-1}(\mathfrak{A}; x_1, \ldots, x_i) \cong \mathrm{Cl}^{k-i-1}(\mathcal{C}; c_1, \ldots, c_i) \\ &\wedge \forall x_{i+1}(\mathrm{Cl}^{k-i-1}(\mathfrak{A}; x_1, \ldots, x_{i+1}) \ncong \mathrm{Cl}^{k-i-1}(C; c_1, \ldots, c_{i+1}))), n) \\ &\quad \leq \ n^k(1 - 2^{-s})^{\lfloor (n-it)/t \rfloor} \\ &\quad \to \ 0 \text{ as } n \to \infty. \end{aligned}$$

□

To complete the proof, we need to show that $\mathfrak{A}_0 \sim_k \mathfrak{A}_1$ for any $\mathfrak{A}_0$ and $\mathfrak{A}_1$ satisfying the condition of Lemma 2.3. We do this by showing that if (3) holds for $i < k$, then Duplicator can choose so that it holds for $i + 1$. Let $|\mathfrak{A}_j| = n_j$ for $j = 0, 1$. Suppose Spoiler chooses $a_{i+1} \in n_0$ such that $\mathrm{Cl}^{k-i-1}(\mathfrak{A}_0; a_1, \ldots, a_{i+1}) \subseteq \mathrm{Cl}^{k-i}(\mathfrak{A}_0; a_1, \ldots, a_i)$. Let f be the isomorphism guaranteed by (3). Then Duplicator chooses $b_{i+1} = f(a_{i+i})$, and (3) holds for $i + 1$.

Suppose Spoiler chooses $a_{i+1} \in n_0$ such that there is $c \in \mathrm{Cl}^{k-i-1}(\mathfrak{A}_0; a_1, \ldots, a_{i+1}) - \mathrm{Cl}^{k-i}(\mathfrak{A}_0; a_1, \ldots, a_i)$. First, note that $\mathrm{Cl}^{k-i-1}(\mathfrak{A}_0; a_{i+1}) \cap \mathrm{Cl}^{k-i-1}(\mathfrak{A}_0; a_1, \ldots, a_i) = \emptyset$. Otherwise, there is $h \leq i$ and $d \in n_0$ such that

$$\begin{aligned} \delta_{n_0}(a_h, d) &< 3^{k-i-1} \text{ and} \\ \delta_{n_0}(a_{i+1}, d) &< 3^{k-i-1}. \end{aligned}$$

But also

$$\begin{aligned} \delta_{n_0}(a_{i+1}, c) &< 3^{k-i-1}, \text{ implying} \\ \delta_{n_0}(a_h, c) &< 3^{k-i}, \end{aligned}$$

and $c \in \mathrm{Cl}^{k-i}(\mathfrak{A}_0; a_1, \ldots, a_i)$, contradiction.

Thus, by Lemma 2.3, Duplicator can choose $b_{i+1} \in n_1$ and satisfy (3) for $i+1$. This completes the proof of Theorem 2.1 □

Theorem 2.4 (Lynch, 1980) *For every $\sigma \in \mathcal{L}$, $\lim_{n\to\infty} \mathrm{pr}(\sigma, n) = u/2^v$ for some $u, v \in \omega$.*

Proof. Add the constant 0 to $\mathcal{L}$ (with the obvious fixed interpretation in $\mathcal{C}'_n$). For every $\sigma \in \mathcal{L}$, form σ' by replacing all formulas of the form $y = x + 1$ by $y = x + 1 \wedge y \neq 0$. Then, for every $n \in \omega$ and $R \subseteq n^r$,

$$\langle n, R, S_n \rangle \models \sigma \Leftrightarrow \langle n, R, S'_n, 0 \rangle \models \sigma'.$$

We will show that the theorem holds for the expanded $\mathcal{L}$ and $\mathcal{C}'_n$.

Now, using the same arguments as in the proof of Theorem 2.1, if

$$\mathrm{Cl}^{k-i}(\mathfrak{A}_0; 0, a_1, \ldots, a_i) \cong \mathrm{Cl}^{k-i}(\mathfrak{A}_1; 0, b_1, \ldots, b_i)$$

then, with probability asymptotic to 1, Duplicator can ensure that it holds for $i+1$. That is, the $\sim_k$ classes are determined by $\mathrm{Cl}^k(\mathfrak{A}; 0)$. These classes have probability $u/2^v$ for some $u, v \in \omega$, for sufficiently large n. □

There are countable versions of Theorems 2.1 and 2.4. The language $\mathcal{L}$ is the same, and S is interpreted as the successor relation on the universe. As in the previous lecture, μ is the standard product measure on the power set of all r-tuples on the universe. $\mathbb{Z}$ is the set of integers.

Theorem 2.5 (Lynch, 1980) *For every $\sigma \in \mathcal{L}$,*

$$\begin{aligned} \mu(\{R \subseteq \mathbb{Z}^r : \langle \mathbb{Z}, R, S \rangle \models \sigma) &= 0 \text{ or } 1, \text{ and} \\ \mu(\{R \subseteq \omega^r : \langle \omega, R, S \rangle \models \sigma) &= u/2^v \text{ for some } u, v \in \omega. \end{aligned}$$

Closure operators and extension axioms have also been used to prove a kind of convergence law for structures with addition (mod n), and their countable analogue.

Theorem 2.6 (Lynch, 1980) *For $n \in \omega$, let $\mathcal{C}_n$ be the class of models*

$$\langle n, + \pmod{n}, S_n, R \rangle$$

where $R \subseteq n^r$, μ_n be the uniform distribution on $\mathcal{C}_n$, and $\mathcal{L}$ be the appropriate first-order language (with a symbol for + (mod n)). For every $\sigma \in \mathcal{L}$, there is a positive $a \in \omega$ (dependent on the quantifier rank of σ) such that for all $b = 0, \ldots, a-1$, $\lim_{n\to\infty} \mathrm{pr}(\sigma, an+b) = u_b/2^{v_b}$ for some $u_b, v_b \in \omega$.

Theorem 2.7 (Lynch, 1980) *Let μ be the standard product measure on the set of all r-tuples in $\mathbb{Z}$ and $\mathcal{L}$ be the first-order language of structures $\langle \mathbb{Z}, +, S, R \rangle$ where $R \subseteq \mathbb{Z}^r$, + is the usual addition operator, and S is the successor relation. For every $\sigma \in \mathcal{L}$, $\mu(\sigma) = u/2^v$ for some $u, v \in \omega$.*

2.2 Random Graphs

Random graph theory was introduced by Erdős and Rényi (1961), and has since grown into a very active branch of combinatorics. A good introductory text is Palmer (1985); for those with some familiarity with the subject, a standard reference is Bollobás (1985). We will consider only one model of random graph, but it is by far the most widely studied. This will be our first example of a class of random structures where the probability distribution is not uniform.

For each $n \in \omega$, $\mathcal{C}_n$ is the collection of undirected graphs whose vertex set is n. The probability distribution μ_n on $\mathcal{C}_n$ is defined in terms of the *edge probability*, a function $p(n)$ taking values in $[0, 1]$. For any $\langle n, E\rangle \in \mathcal{C}_n$,

$$\mu_n(\{\langle n, E\rangle\} = p(n)^{|E|}(1 - p(n))^{\binom{n}{2}-|E|}.$$

Another, perhaps more intuitive, way of regarding this probability is to construct the random graph $\langle n, E\rangle$ by choosing independently for each pair $\{i, j\} \subseteq n$, that $\{i, j\} \in E$ with probability $p(n)$. It is evident that when $p(n) = 1/2$ for all n, this is identical to the uniform distribution.

There are many possible edge probabilities, but we will restrict our attention to those of the form $p(n) = \beta n^{-\alpha}$, where $\alpha, \beta \geq 0$. This is a crude characterization of edge probabilities, but it is important because it is simple, involving only two parameters α and β, and yet by varying these parameters, a wide range of monotonically decreasing edge probabilities is covered. (Increasing edge probabilities are a symmetric case because we can replace $p(n)$ by $1 - p(n)$.) Constant edge probabilities occur when $\alpha = 0$. When $\alpha > 0$, the graph is said to be "sparse." As α increases, the random graph becomes sparser, i.e., its edge density decreases, until $\alpha > 2$, when almost all random graphs have no edges. Thus the interesting values of α are in the range $[0, 2)$. A slight generalization of the proofs of Fagin and Glebskiĭ et. al. extends their 0-1 law to all random graphs with constant edge probabilities. Thus we will consider $\alpha > 0$.

Random graph theorists are particularly interested in threshold functions. These are parameterized functions that characterize the random graph such that as the parameter passes through a certain value (the threshold), the qualitative behavior of the random graph changes. In the logics we will be considering, α is the important parameter for the edge probability. For example, the asymptotic probability that the graph has a 4-clique is 0 if $\alpha > 2/3$, 1 if $\alpha < 2/3$, and $1 - e^{-\beta^6/24}$ if $\alpha = 2/3$. In the logics we will be studying, as long as $\beta > 0$, its value does not affect the qualitative behavior of the random graph, so we will assume it is 1.

It can be shown (Shelah and Spencer, 1988) that every rational in $(0, 1)$ is a threshold, with respect to α, for some first-order property of random graphs. Conversely, no irrational is such a threshold. We will not prove these facts here, but we will prove another important result from the Shelah and Spencer paper.

Theorem 2.8 (Shelah and Spencer, 1988) *Let $\mathcal{L}$ be the first-order logic of* *graphs. For $n \in \omega$, μ_n is the probability distribution on $\mathcal{C}_n$ characterized by edge probability $p(n) = n^{-\alpha}$, where α is irrational. For every $\sigma \in \mathcal{L}$, $\lim_{n\to\infty}(\sigma, n) = 0$ or 1.*

Proof. We will use the same general approach as in the proof of the 0-1 law for structures with a built-in cyclic successor (Theorem 2.1). Fixing $k \in \omega$, we will show that there is some class of graphs $\mathcal{D}$ such that $\mathrm{pr}(G \in \mathcal{D}, n) \to 1$ as $n \to \infty$, and all graphs in $\mathcal{D}$ are $\sim_k$.

Again, the difficulty is that Duplicator cannot simply match Spoiler's choices, but must match a neighborhood around Spoiler's choices. We will use another kind of closure operator to specify these neighborhoods.

We begin with a series of technical definitions and lemmas. As before, we will use the convention that if $\langle V, E\rangle$ is a graph, and $W \subseteq V$, then $\langle W, E\rangle$ is the graph $\langle W, E \restriction W\rangle$.

Definition 2.9

1. *$\langle V, E, c_1, \ldots, c_i\rangle$ is a rooted graph if $\langle V, E\rangle$ is a graph, and $c_1, \ldots, c_i \in V$. We also say $\langle V, E, R\rangle$ is a rooted graph when $R \subseteq V$, and the order of the vertices in R is immaterial.*
2. *The weight of $\langle V, E, R\rangle$, $\zeta(\langle V, E, R\rangle)$, is $|V - R| - \alpha|E - E \restriction R|$.*
3. *$\langle V, E, R\rangle$ is dense if $\zeta(\langle V, E, R\rangle) < 0$.*
4. *$\langle V, E, R\rangle$ is sparse if $\zeta(\langle V, E, R\rangle) > 0$.*
5. *$\langle V, E, R\rangle$ is rigid if $\langle V, E, S\rangle$ is dense for every set of vertices S such that $R \subseteq S \subset V$.*
6. *$\langle V, E, R\rangle$ is safe if $\langle S, E, R\rangle$ is sparse for every set of vertices S such that $R \subset S \subseteq V$.*

Note that, since α is irrational, the weight of a rooted graph cannot be 0 unless $V = R$. The proof of the next lemma is immediate from the above definition.

Lemma 2.10 *Let $R \subseteq S \subseteq V$. Then $\zeta(\langle V, E, R\rangle) = \zeta(\langle V, E, S\rangle) + \zeta(\langle S, E, R\rangle)$.*

Lemma 2.11 *Let $R \subseteq S \subseteq V$. If $\langle V, E, S\rangle$ and $\langle S, E, R\rangle$ are rigid, then so is $\langle V, E, R\rangle$.*

Proof. Take T such that $R \subseteq T \subset V$. Then $\zeta(\langle V, E, S \cup T\rangle) \leq 0$ since $\langle V, E, S\rangle$ is rigid. Also, $\zeta(\langle S, E, S \cap T\rangle) \leq 0$. Then $\zeta(\langle S \cup T, E, T\rangle) \leq 0$ since we have merely added extra roots to $\langle S, E, S \cap T\rangle$, and that can only decrease its weight. Therefore by Lemma 2.10, $\zeta(\langle V, E, T\rangle) \leq 0$. □

Lemma 2.12 *If $\langle V, E, R\rangle$ and $\langle W, E, R\rangle$ are rigid, then so is $\langle V \cup W, E, R\rangle$.*

Proof. $\langle W, E, V \cap W\rangle$ is rigid since $\langle W, E, R\rangle$ is rigid and $R \subseteq V \cap W$. Therefore $\langle V \cup W, E, V\rangle$ is rigid, and by Lemma 2.11, $\langle V \cup W, E, R\rangle$ is rigid. □

Definition 2.13 *For a rooted graph $\langle V, E, R\rangle$,* $\mathrm{Rig}(\langle V, E, R\rangle)$ *is the maximal set S such that $R \subseteq S \subseteq V$ and $\langle S, E, R\rangle$ is rigid. Note that by Lemma 2.12, S is unique.*

Lemma 2.14 *For any rooted graph $\langle V, E, R\rangle$, $\langle V, E, \mathrm{Rig}(\langle V, E, R\rangle)\rangle$ is safe.*

Proof. Let $S = \mathrm{Rig}(\langle V, E, R\rangle)$, and suppose $\langle V, E, S\rangle$ is not safe. Then there exists T such that $S \subset T \subseteq V$ and $\zeta(\langle T, E, S\rangle) < 0$. Assume T is minimal among such sets. We claim $\langle T, E, S\rangle$ is rigid. Take any U such that $S \subseteq U \subset T$. By minimality of T, $\zeta(\langle U, E, S\rangle) \geq 0$. By Lemma 2.10, $\zeta(\langle T, E, U\rangle) < 0$. But by Lemma 2.11, $\langle T, E, R\rangle$ is rigid, contradicting the maximality of S. $\square$

Definition 2.15 *Let $G = \langle V, E\rangle$. For $i, j \in \omega$ and $a_1, \ldots, a_i \in V$,* $\mathrm{Cl}^j(G; a_1, \ldots, a_i)$ *is defined by induction on j.*

$$\mathrm{Cl}^0(G; a_1, \ldots, a_i) = \langle \{a_1, \ldots, a_i\}, E, a_1, \ldots, a_i\rangle \text{for all } i \in \omega.$$

Assume Cl^j *has been defined for all $i \in \omega$. Fixing i and $a_1, \ldots, a_i \in V$, for all $a_{i+1} \in V$, let*

$$\begin{aligned} \mathrm{Cl}^j(G; a_1, \ldots, a_{i+1}) &= \langle V(a_{i+1}), E, a_1, \ldots, a_{i+1}\rangle, \text{ and} \\ S(a_{i+1}) &= \mathrm{Rig}(\langle V(a_{i+1}), E, a_1, \ldots, a_i\rangle). \end{aligned}$$

Then

$$Cl^{j+1}(G; a_1, \ldots, a_i) = \langle \bigcup_{a_{i+1} \in V} S(a_{i+1}), E, a_1, \ldots, a_i\rangle.$$

Note that, by Lemma 2.12, the closure is rigid. Unlike our previous closure operator, this one is not based on a true metric, and its size depends on the random relation itself. However, its size is bounded.

Lemma 2.16 *For every $i, j \in \omega$, there is m such that*

$$\mathrm{pr}(\forall a_1 \ldots \forall a_i \in G(|\mathrm{Cl}^j(G; a_1, \ldots, a_i)| \leq m), n) \to 1$$

as $n \to \infty$.

Proof. We use induction on j. When $j = 0$, we can take $m = i$.

Assume the lemma holds for $i + 1$, j, and m. We will show that there exists m' such that it holds for i, $j + 1$, and m'. Let $\gamma = \max(\{\zeta(\langle V, E, S\rangle) : |V| \leq m$, $S \subset V$, and $\langle V, E, S\rangle$ is dense $\})$. Then $\gamma < 0$ because there are only finitely many isomorphism classes among rooted graphs on at most m vertices. Since all closures are rigid, for all m',

$$\begin{aligned} \mathrm{pr}(\exists x_1 \ldots \exists x_i(|\mathrm{Cl}^{j+1}(G; x_1, \ldots, x_i)| \geq m'), n) &\leq n^i \times n^{\gamma \lfloor m'/m \rfloor} \\ &\to 0 \end{aligned}$$

if $m' > \lceil -i/\gamma \rceil m$. $\square$

Let G_0 and G_1 be two graphs on which the k-round EF game is to be played. Duplicator's strategy is to ensure that, after each round $i = 0, \dots, k$,

$$\mathrm{Cl}^{k-i}(G_0; a_1, \dots, a_i) \cong \mathrm{Cl}^{k-i}(G_1; b_1, \dots, b_i). \tag{4}$$

Again, it remains only to prove that Duplicator can follow this strategy with high probability.

Lemma 2.17 *Fix k and m. Let $G \in \mathcal{C}_n$. With probability asymptotic to 1 as $n \to \infty$, for any $i < k$, any rooted graph $H = \langle W, F, R \rangle$, and any $c_1, \dots, c_{i+1} \in W$ such that $|\mathrm{Cl}^{k-i-1}(H; c_1, \dots, c_{i+1})| \le m$, $R \subseteq \mathrm{Cl}^{k-i-1}(H; c_1, \dots, c_{i+1}) \cap \mathrm{Cl}^{k-i}(H; c_1, \dots, c_i)$, and $\langle \mathrm{Cl}^{k-i-1}(H; c_1, \dots, c_{i+1}), F, R \rangle$ is safe,*

$$\begin{aligned} &\forall x_1 \dots \forall x_i (\mathrm{Cl}^{k-i}(G; x_1, \dots, x_i) \cong \mathrm{Cl}^{k-i}(H; c_1, \dots, c_i) \to \\ &\quad \exists x_{i+1} (\mathrm{Cl}^{k-i-1}(G; x_1, \dots, x_{i+1}) \cong \mathrm{Cl}^{k-i-1}(H; c_1, \dots, c_{i+1}))). \end{aligned}$$

As before, Lemma 2.17 could be phrased as a statement that a certain finite collection of first-order axioms holds almost surely. It is also worth noting that it would not be sufficient to prove only that for all $x_1, \dots, x_i$ such that $\mathrm{Cl}^{k-i}(G; x_1, \dots, x_i) \cong \mathrm{Cl}^{k-i}(H; c_1, \dots, c_i)$, the probability that $\exists x_{i+1} (\mathrm{Cl}^{k-i-1}(G; x_1, \dots, x_{i+1}) \cong \mathrm{Cl}^{k-i-1}(H; c_1, \dots, c_{i+1}))$ approaches 1. Using sophisticated combinatorial techniques, Shelah and Spencer actually proved a result stronger than necessary: there is $\delta > 0$ such that with probability approaching 1, for all $x_1, ..., x_i$ such that $\mathrm{Cl}^{k-i}(G; x_1, \dots, x_i) \cong \mathrm{Cl}^{k-i}(H; c_1, \dots, c_i)$, the number of x_{i+1} such that $\mathrm{Cl}^{k-i-1}(G; x_1, \dots, x_{i+1}) \cong \mathrm{Cl}^{k-i-1}(H; c_1, \dots, c_{i+1})$ is $\Theta(n^\delta)$. We shall give a proof that uses only basic techniques from random graph theory.

Proof. There are only finitely many choices for i and the isomorphism type of $\langle \mathrm{Cl}^{k-i-1}(H; c_1, \dots, c_{i+1}), F, R \rangle$ so we may as well fix them, abbreviating the latter by $\langle V, F, R \rangle$. Let $v = |V - R|$ and $e = |F - F \restriction R|$. Fix $x_1, \dots, x_i \in n$ and condition on there being an isomorphism f from $\mathrm{Cl}^{k-i}(G; x_1, \dots, x_i)$ onto $\mathrm{Cl}^{k-i}(H; c_1, \dots, c_i)$. If $v = 0$, then $x_{i+1} = f^{-1}(c_{i+1})$ satisfies

$$\mathrm{Cl}^{k-i-1}(G; x_1, \dots, x_{i+1}) \cong \mathrm{Cl}^{k-i-1}(H; c_1, \dots, c_{i+1}).$$

If $v > 0$, then $v - \alpha e > 0$ because $\langle V, F, R \rangle$ is safe. Take any β such that $\alpha e'/v' < \beta < 1$ for all sparse rooted graphs $\langle V', F, R \rangle$ such that $R \subset V' \subseteq V$ and $v' = |V' - R|$ and $e' = |F \restriction V' - F \restriction R|$.

Partition $n - \mathrm{Cl}^{k-i}(G; x_1, \dots, x_i)$ into as many sets of size $\lceil n^\beta \rceil$ as possible. There will be more than $n^{1-\beta}/2$ of them. Take any one of these sets, say S. We will show that with positive probability, there is some $x_{i+1} \in S$ such that $\mathrm{Cl}^{k-i-1}(G; x_1, \dots, x_{i+1}) \cong \mathrm{Cl}^{k-i-1}(H; c_1, \dots, c_{i+1})$. This will be done through a routine application of the second moment method, one of the standard techniques of random graph theory.

For $T \subseteq S$ where $|T| = v$, let $\mathbf{X}_T$ be the indicator random variable that is 1 if and only if there exists x_{i+1} such that $T = \mathrm{Cl}^{k-i-1}(G; x_1, \ldots, x_{i+1}) - \mathrm{Cl}^{k-i}(G; x_1, \ldots, x_i)$ and there is an isomorphism g from $\mathrm{Cl}^{k-i-1}(G; x_1, \ldots, x_{i+1})$ to $\mathrm{Cl}^{k-i-1}(H; c_1, \ldots, c_{i+1})$ that extends f. Letting γ be the number of such g for a fixed T, and $\mathbf{X} = \sum_T \mathbf{X}_T$, the expectation of $\mathbf{X}$ is

$$\begin{aligned}
\mathbf{E}(\mathbf{X}) &= \sum_T \mathbf{E}(\mathbf{X}_T) \text{ by linearity of expectation} \\
&= \binom{\lceil n^\beta \rceil}{v} \gamma \times n^{-\alpha e}(1 - n^{-\alpha})^{\binom{v}{2}+|R|v-e} \\
&= \Theta(n^{\beta v - \alpha e}) \\
&\to \infty
\end{aligned}$$

as $n \to \infty$. That is, the average number of T for which $\mathbf{X}_T = 1$ is unbounded.

Next, we show that $\mathrm{Var}(\mathbf{X})$, the variance or second moment of $\mathbf{X}$, is small compared to $\mathbf{E}(\mathbf{X})^2$. From basic probability theory, $\mathrm{Var}(\mathbf{X}) = \mathbf{E}(\mathbf{X}^2) - \mathbf{E}(\mathbf{X})^2$. By linearity of expectation,

$$\mathbf{E}(\mathbf{X}^2) = \sum_{T \cap U = \emptyset} \mathbf{E}(\mathbf{X}_T \mathbf{X}_U) + \sum_{T \cap U \neq \emptyset} \mathbf{E}(\mathbf{X}_T \mathbf{X}_U).$$

We have $\sum_{T \cap U = \emptyset} \mathbf{E}(\mathbf{X}_T \mathbf{X}_U) \sim \mathbf{E}(\mathbf{X})^2$ by a calculation similar to the one for $\mathbf{E}(\mathbf{X})$. Now consider any T and U such that $T \cap U \neq \emptyset$ and $\mathbf{X}_T \mathbf{X}_U = 1$. Then there is V' such that $R \subseteq V' \subseteq V$ and an isomorphism h from $\langle T \cap U \cup f^{-1}(R), E, f^{-1}(R) \rangle$ to $\langle V', F, R \rangle$ that extends f. Let $v' = |V' - R|$ and $e' = |F \upharpoonright V' - F \upharpoonright R|$. Then $\beta v' - \alpha e' > 0$ because $\langle V, F, R \rangle$ is safe. Letting δ be the maximum number of such h,

$$\begin{aligned}
\mathbf{E}(\mathbf{X}_T \mathbf{X}_U) &\leq \delta n^{-\alpha(2e - e')}, \text{ and} \\
\sum_{T \cap U \neq \emptyset} \mathbf{E}(\mathbf{X}_T \mathbf{X}_U) &\leq \sum_{0 < v' \leq v} \binom{\lceil n^\beta \rceil}{v} \binom{\lceil n^\beta \rceil - v}{v - v'} \frac{\delta}{2} \times n^{-\alpha(2e - e')} \\
&= O(n^{2(\beta v - \alpha e) - \beta v' + \alpha e'}) \\
&= o(\mathbf{E}(\mathbf{X})^2).
\end{aligned}$$

Therefore $\mathbf{E}(\mathbf{X}^2) \sim \mathbf{E}(\mathbf{X})^2$ and $\mathrm{Var}(\mathbf{X}) = o(\mathbf{E}(\mathbf{X})^2)$. By Chebyshev's inequality,

$$\begin{aligned}
\mathrm{pr}(\mathbf{X} = 0, n) &\leq \frac{\mathrm{Var}(\mathbf{X})}{\mathbf{E}(\mathbf{X})^2} \\
&< \frac{1}{2}
\end{aligned}$$

for sufficiently large n.

By independence, the probability that there is no T in any S such that $\mathbf{X}_T = 1$ is bounded above by $2^{-n^{1-\beta}/2}$, and the probability that there exist $x_1, \ldots, x_i$ for which there is no T is bounded above by $n^i \times 2^{-n^{1-\beta}/2} \longrightarrow 0$ as $n \longrightarrow \infty$. □

To complete the proof, by Lemma 2.16, there is m such that with probability asymptotic to 1, $|\mathrm{Cl}^{k-i-1}(G; a_1, \ldots, a_{i+1})| \leq m$ for all $i < k$. We will show that $G_0 \sim_k G_1$ for any G_0 and G_1 satisfying this condition and the condition of Lemma 2.17. We do this by showing that if (4) holds for $i < k$, then Duplicator can choose so that it holds for $i + 1$. Let $G_j = \langle n_j, E_j \rangle$ for $j = 0, 1$. Suppose Spoiler chooses $a_{i+1} \in n_0$. Let

$$R = \mathrm{Rig}(\langle \mathrm{Cl}^{k-i-1}(G_0; a_1, \ldots, a_{i+1}), E_0, a_1, \ldots, a_i \rangle).$$

By Definition 2.15, $R \subseteq \mathrm{Cl}^{k-i}(G_0; a_1, \ldots, a_i)$. By Lemma 2.14, $\langle \mathrm{Cl}^{k-i-1}(G_0; a_1, \ldots, a_{i+1}),\ E_0, R \rangle$ is safe. Therefore by Lemma 2.17, there is $b_{i+1} \in n_1$ such that $\mathrm{Cl}^{k-i-1}(G_0; a_1, \ldots, a_{i+1}) \cong \mathrm{Cl}^{k-i-1}(G_1; b_1, \ldots, b_{i+1})$. □

notes taken by James Lynch, jlynch@sun.mcs.clarkson.edu

Session III: Wednesday, August 16

Track C: Random Finite Models

James F. Lynch

3 The Generating Function Approach

The material presented in the previous two lectures was, for the most part, based on areas of modern mathematics, i.e., logic and random graph theory. While some of the foundations of these subjects were laid several centuries ago, they are generally regarded as developments of twentieth century mathematics. In contrast, the methods of today's lecture are deeply rooted in classical mathematics. We will be using generating functions to solve combinatorial enumeration problems. This approach has been, and continues to be, one of the most fruitful methods for attacking problems in many areas of mathematics and computer science.

Let $\mathcal{C}$ be a class of structures of some fixed type. For $n \in \omega$ let $\mathcal{C}_n$ be the class of structures in $\mathcal{C}$ with universe $\{0, 1, \ldots, n-1\}$, and let $a_n = \mid \mathcal{C}_n \mid$. The *exponential generating function (egf)* of $\mathcal{C}$ is

$$a(x) = \Sigma_{n=0}^{\infty} \frac{a_n}{n!} x^n.$$

In this lecture, we will consider only labeled structures. That is, for structures in $\mathcal{C}_n$, all elements in n are distinguishable. There is a parallel theory of *ordinary generating functions* for unlabeled structures, where elements in n are not distinguishable, and two structures are identified if they are isomorphic. The interested reader may find analogous results for unlabeled structures in the literature (see e.g. Compton, 1989 or Wilf, 1990).

Let $\mathcal{L}$ be a logical language. For $\sigma \in L$, let

$$\begin{aligned} \mathcal{C}(\sigma) &= \{\mathfrak{A} \models \sigma : \mathfrak{A} \in \mathcal{C}\} \text{ and} \\ \mathcal{C}_n(\sigma) &= \{\mathfrak{A} \in \mathcal{C} : |\mathfrak{A}| = n\}. \end{aligned}$$

Given σ, we put

$$\begin{aligned} b_n &= \mid \mathcal{C}_n(\sigma) \mid, \\ b(x) &= \Sigma_{n=0}^{\infty} \frac{b_n}{n!} x^n, \text{ and} \\ \mu_n &= \frac{b_n}{a_n}. \end{aligned}$$

Here are some simple but important examples:

- $\mathcal{C}$ is any class of structures with a unique model on any finite set.

$$a(x) = \Sigma_{n=0}^{\infty} \frac{1}{n!} x^n \ = e^x.$$

- Permutations:

$$a(x) = \Sigma_{n=0}^{\infty} \frac{n!}{n!} x^n \ = \frac{1}{1-x}$$

- Unary relations:

$$a(x) = \Sigma_{n=0}^{\infty} \frac{2^n}{n!} x^n \ = e^{2x}$$

In these examples, we derived closed forms for the egf's from their coefficients. In actual practice, the problem is to recover the coefficients, given information about an egf (such as a closed form or a functional equation). Often, the best that can be done is to give an asymptotic estimate of the coefficients.

Although the manipulations of generating functions can be quite sophisticated and involved, there is a set of elementary rules of surprising power that is sufficient for many applications, and is the basis of the more advanced techniques.

Fundamental Relations. Let $\uplus$ denote the disjoint union of structures.

1. Let $\mathcal{C}, \mathcal{D}$ be disjoint classes of structures with egf's $a(x), c(x)$ respectively. The egf of $\{\mathfrak{A} \uplus \mathfrak{B} : \mathfrak{A} \in \mathcal{C}, \mathfrak{B} \in \mathcal{D}\}$ is given by $a(x)c(x)$.
   Proof. Given $k \in n$, the number of ways to choose $\mathfrak{A} \in \mathcal{C}_k$ and $\mathfrak{B} \in \mathcal{D}_{n-k}$ is given by
   $$\binom{n}{k} a_k c_{n-k}.$$
   Consequently, the egf in question is
   $$\begin{aligned} \sum_{n=0}^{\infty} \left(\frac{\sum_{k=0}^{n} \binom{n}{k} a_k c_{n-k}}{n!} \right) x^n &= \\ \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} \frac{a_k}{k!} \frac{c_{n-k}}{(n-k)!} \right) x^n &= \\ \left(\sum_{n=0}^{\infty} \frac{a_n}{n!} x^n \right) \left(\sum_{n=0}^{\infty} \frac{c_n}{n!} x^n \right) &= a(x)c(x). \end{aligned}$$
   $\square$.

2. Let $\mathcal{C}$ be a class of **connected** structures. The egf of
   $$\{\mathfrak{A}_1 \uplus \mathfrak{A}_2 : \mathfrak{A}_1, \mathfrak{A}_2 \in \mathcal{C}\}$$

is

$$\frac{(a(x))^2}{2}.$$

Proof. Similar.

More generally, for $k \in \omega$, the egf of

$$\{\mathfrak{A}_1 \uplus \mathfrak{A}_2 \uplus \ldots \uplus \mathfrak{A}_k : \mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k \in \mathcal{C}\}$$

is

$$\frac{(a(x))^k}{k!}.$$

3. If $\mathcal{C}$ is a class of connected structures, then the egf of the class of structures whose components are in $\mathcal{C}$ is

$$1 + a(x) + \frac{(a(x))^2}{2!} + \frac{(a(x))^3}{3!} + \ldots = e^{a(x)}.$$

We shall work with classes of structures that are closed under **disjoint unions** and **components**. Many important classes of finite structures in combinatorics are in this category. Some examples are :

- Permutations
- Equivalence relations
- Forests
- Graphs

to mention only a few. From this point on, we assume that $\mathcal{C}$ is a class of finite structures closed under disjoint unions and components.

Let us use the fundamental relations to derive egf's for two classes.

1. Equivalence Relations. A connected equivalence relation is a set with a binary relation that holds for every pair of elements in the set. Thus there is exactly one connected equivalence class of each cardinality, and the egf for connected equivalence classes is

$$\sum_{n=1}^{\infty} \frac{1}{n!} x^n = e^x - 1.$$

Hence the egf for arbitrary equivalence classes is (by fundamental relation 3.)

$$e^{e^x - 1}.$$

2. Derangements (permutations without fixed points). The egf for connected derangements (cycles of size greater than 1) is

$$\begin{aligned}\sum_{n=2}^{\infty} \frac{(n-1)!}{n!} x^n &= \sum_{n=2}^{\infty} \frac{x^n}{n} \\ &= \ln(1/(1-x)) - x.\end{aligned}$$

Hence the egf for derangements is

$$e^{\ln(1/(1-x))-x} = \frac{e^{-x}}{1-x}.$$

Now we shall discuss Compton's work on applying generating function techniques to the logic of random finite structures. For a connected structure $\mathfrak{A}$ let $\theta_{\mathfrak{A},j}$ be the sentence stating "There are exactly j components isomorphic to $\mathfrak{A}$." Let $\gamma(\mathfrak{A})$ be the number of automorphisms of $\mathfrak{A}$.

Lemma 3.1 *i. If $\mathfrak{A}_0, \mathfrak{A}_1, ..., \mathfrak{A}_{q-1}$ are nonisomorphic connected structures in $\mathcal{C}$ such that $\mid \mathfrak{A}_i \mid = m_i$ for each $i \in q$, and $j_0, j_1, ..., j_{q-1} \in \omega$, then the egf for $\{\mathfrak{A} \models \bigwedge_{i<q} \theta_{\mathfrak{A}_i, j_i} : \mathfrak{A} \in \mathcal{C}\}$ is*

$$a(x) \prod_{i<q} \frac{1}{j_i!} \left(\frac{x^{m_i}}{\gamma(\mathfrak{A}_i)} \right)^{j_i} e^{-x^{m_i}/\gamma(\mathfrak{A}_i)}.$$

ii. Let $\mathfrak{A}$ be a connected structure in $\mathcal{C}_m$. For $j, n < \omega$, let

$$c_{j,n} = \mid \{\mathfrak{B} \models \theta_{\mathfrak{A},j} : \mathfrak{B} \in \mathcal{C}_n\} \mid .$$

Then

$$\frac{c_{j,n-m}}{(n-m)!} = (j+1)\gamma(\mathfrak{A}) \frac{c_{j+1,n}}{n!}.$$

Proof. Follows from the fundamental relations discussed earlier.

The next lemma's proof is purely model theoretic, and is left as an exercise.

Lemma 3.2 *Assume $\mathcal{C}$ contains at least one finite model. Then*

$$T = \{\neg\theta_{\mathfrak{A},j} : \mathfrak{A} \text{ is connected and } j \in \omega\} \cup \bigcap_{\substack{\mathfrak{A}\in\mathcal{C} \\ \mathfrak{A}\text{finite}}} \mathrm{Th}(\mathfrak{A})$$

is a complete and consistent theory.

Compton's characterization of classes of finite structures that have a zero-one law is based on the growth rate of the coefficients of their generating functions. Letting $\mathcal{C}$ be a class of finite structures and $a(x)$ its generating function, we write $a(x) \to R$ for $R \in [0, \infty)$ if

$$\lim_{n\to\infty} \frac{a_{n-m}/(n-m)!}{a_n/n!} = R^m$$

for all m such that $\mathcal{C}$ has a connected structure of that size.

Lemma 3.3 *Assume that $\mathcal{C}$ contains at least one finite model. If $a(x)$ has radius of convergence $R \in (0, \infty)$, then $a(x) \to R$ if and only if*

$$\lim_{n\to\infty} \frac{a_{n-1}/(n-1)!}{a_n/n!} = R.$$

Now suppose $\sigma \in \mathcal{L}$ and b_n is defined as before. We would like to compute $\lim_{n\to\infty} b_n/a_n$ from $a(x)$ and $b(x)$. Suppose we knew that $b(x)/a(x) \to P$ as $x \to R$. Could we conclude $b_n/a_n \to P$? In general, no. However, by imposing some additional conditions, the answer is yes. Such conditions are called *side conditions*, and the resulting theorem is called a *Tauberian* theorem. The following is an example. It is a generalization by Compton of a well-known Tauberian theorem.

Theorem 3.4 *Let*

$$\begin{aligned} a(x) &= \sum_{n=0}^{\infty} a_n\, x^n, \\ b(x) &= \sum_{n=0}^{\infty} b_n\, x^n, \text{ and} \\ c(x) &= \sum_{n=0}^{\infty} c_n\, x^n. \end{aligned}$$

Further, assume

$$\begin{aligned} \lim_{n\to\infty} \frac{a_{n-k}}{a_n} &= R^k \text{ for some } k > 0 \text{ and } R \geq 0. \\ \frac{b(x)}{a(x)} &= c(x^k) \text{ where } c(x^k) \text{ has radius of convergence } S > R. \\ \lim_{x\to R} c(x^k) &= P. \end{aligned}$$

Then

$$\lim_{n\to\infty} \frac{b_n}{a_n} = P.$$

Example. Let a_n be the number of permutations on n and b_n be the number of derangements on n. Recall that $a(x) = 1/(1-x)$ and $b(x) = e^{-x}/(1-x)$. Then the hypotheses of Theorem 3.4 are satisfied:

$$\begin{aligned} \lim_{n\to\infty} \frac{a_{n-1}}{a_n} &= 1. \\ c(x) = \frac{b(x)}{a(x)} &= e^{-x}, \text{ which has radius of convergence } \infty. \\ \lim_{x\to 1} c(x) = e^{-1}. & \end{aligned}$$

Therefore

$$\frac{a_n}{b_n} \to \frac{1}{e}.$$

This example illustrates the technique Compton used to derive formulas for $\mathrm{pr}(\sigma, n)$ when

$$\sigma = \bigwedge_{i<q} \theta_{\mathfrak{A}_i, j_i}.$$

Theorem 3.5 *Let $\sigma = \bigwedge_{i<q} \theta_{\mathfrak{A}_i, j_i}$. If $a(x) \to R$ then*

$$\lim_{n\to\infty} pr(\sigma, n) = \prod_{i<q} \frac{\lambda_i^{j_i}}{j_i!} e^{-\lambda_i}$$

where $\lambda_i = R^{m_i}/\gamma(\mathfrak{A}_i)$. [When $R = \infty$, this means $pr(\sigma, n) \to 0$.]

Proof. First, assume $R < \infty$. From Lemma 3.1.i,

$$b(x) = a(x) \prod_{i<q} \frac{1}{j_i!} \left(\frac{x^{m_i}}{\gamma(\mathfrak{A}_i)} \right)^{j_i} e^{-x^{m_i}/\gamma(\mathfrak{A}_i)}. \tag{5}$$

If $R > 0$, then by Lemma 3.3,

$$\lim_{n\to\infty} \frac{a_{n-1}/(n-1)!}{a_n/n!} = R.$$

The radius of convergence of $b(x)/a(x)$ is ∞. Therefore, by Theorem 3.4,

$$\begin{aligned} \lim_{n\to\infty} \frac{b_n}{a_n} &= \lim_{x\to R} \frac{b(x)}{a(x)} \\ &= \prod_{i<q} \frac{\lambda_i^{j_i}}{j_i!} e^{-\lambda_i}. \end{aligned}$$

If $R = 0$, let us compute $\mathrm{pr}(\theta_{\mathfrak{A},j}, n)$, i.e., the probability of a single conjunct of σ. Taking $q = 1$ in Equation (5) and dropping subscripts,

$$\frac{b(x)}{a(x)} = \frac{1}{j!} \left(\frac{x^m}{\gamma(\mathfrak{A})} \right)^j e^{-x^m/\gamma(\mathfrak{A})}$$

is a power series in x^m. Since $|\mathfrak{A}| = m$ and $a(x) \to 0$, we know

$$\lim_{n\to\infty} \frac{a_{n-m}/(n-m)!}{a_n/n!} = 0.$$

Applying Theorem 3.4,

$$\mathrm{pr}(\theta_{\mathfrak{A},j}, n) = \begin{cases} 1 & \text{if} \quad j = 0 \\ 0 & \text{if} \quad j > 0. \end{cases}$$

Therefore $\mathrm{pr}(\sigma, n) \to 0$ or 1.

If $R = \infty$, again we look at a single conjunct. Let $c_{j,n} = |\{\mathfrak{B} \models \theta_{\mathfrak{A},j} : \mathfrak{B} \in \mathcal{C}_n\}|$. By Lemma 3.1.ii,

$$\frac{c_{j,n-m}}{(n-m)!} = (j+1)\gamma(\mathfrak{A}) \frac{c_{j+1,n}}{n!},$$

so

$$\begin{aligned} \frac{c_{j,n-m}}{a_{n-m}} &= (j+1)\gamma(\mathfrak{A}) \frac{c_{j+1,n}/n!}{a_{n-m}/(n-m)!} \\ &\leq (j+1)\gamma(\mathfrak{A}) \left(\frac{a_{n-m}/(n-m)!}{a_n/n!} \right)^{-1} \\ &\to 0 \end{aligned}$$

since $a(x) \to \infty$. Therefore $\mathrm{pr}(\sigma, n) \to 0$. $\Box$.

A converse of some sort to the above theorem also holds.

Theorem 3.6 *Let $\mathcal{C}$ be a class of finite structures such that $\lim_{n\to\infty} \mathrm{pr}(\sigma, n)$ exists for every σ of the form $\theta_{\mathfrak{A},j}$. Then $a(x) \to R$ for some $R \in [0, \infty]$.*

We may now state Compton's condition for 0-1 Laws.

Theorem 3.7 *Let $\mathcal{C}$ be a class of finite structures such that the radius of convergence of $a(x)$ is positive. Then $\mathcal{C}$ has a 0-1 law if and only if $a(x) \to \infty$.*

Proof. Assume $\mathcal{C}$ has a 0-1 law. By Theorem 3.6, $a(x) \to R$ for some $R \in [0, \infty]$. By Theorem 3.5, $R = \infty$ because otherwise some sentences have probability asymptotic neither to 0 or 1.

Now assume $a(x) \to \infty$. We show there is a complete theory T such that every $\sigma \in T$ has probability asymptotic to 1. T is provided by Lemma 3.2. To show that any $\sigma \in T$ has probability asymptotic to 1, by Theorem 3.5, $\lim_{n\to\infty} \mathrm{pr}(\neg\theta_{\mathfrak{A},j}, n) = 1$. Also, any sentence true in all finite models has probability equal to 1. $\Box$.

Examples.

- **Permutations**

$$a(x) = \sum_{n=0}^{\infty} x^n.$$

Hence $a(x) \to 1$. So there is no 0-1 law.

- **Unary functions**
$$a(x) = \sum_{n=0}^{\infty} \frac{n^n}{n!} x^n.$$
Hence
$$\frac{a_{n-1}/(n-1)!}{a_n/n!} = \frac{(n-1)^{n-1}}{n^{n-1}} \to \frac{1}{e}.$$
Again, there is no 0-1 law.

  Fagin had previously shown that the probability that a random unary function has no fixed point is asymptotic to $\frac{1}{e}$. However, Lynch (1985) proved a convergence law for random unary functions.

- **Equivalence relations**
$$a(x) = e^{e^x - 1}.$$
With some work one can show $a(x) \to \infty$, so the 0-1 law holds.

notes taken by Sandeep K. Shukla, sandeep@cs.albany.edu

Session IV: Thursday, August 17

Track C: Random Finite Models

James F. Lynch

4 Convergence Laws for Higher-Order Logics

Although higher-order logics usually are too expressive to have a convergence law, there are exceptional cases. We shall investigate three of them in this lecture.

4.1 Monadic Second-Order Logic

Compton's characterization of classes with first-order zero-one laws (Theorem 3.7 of the Wednesday lecture) extends to monadic second-order logic.

Theorem 4.1 (Compton, 1989) *Let $\mathcal{C}$ be a class of labeled structures over a fixed vocabulary closed under disjoint union and components.*[1] *Let $a(x)$ be the exponential generating function (egf) of $\mathcal{C}$. Then the following are equivalent:*

i. $a(x) \to \infty$

ii. $\mathcal{C}$ *has a first-order 0-1 law*

iii. $\mathcal{C}$ *has a monadic second-order 0-1 law*

The proof employs a lot of machinery developed for proving that i. implies ii. Analogous results can be shown for unlabeled structures.

Proof Sketch. Theorem 3.7 from Wednesday tells us that i. and ii. are equivalent, and clearly iii. implies ii. Thus we need only show that i. implies iii. For $\mathfrak{A}, \mathfrak{B} \in \mathcal{C}$ and $k \in \omega$, put $\mathfrak{A} \equiv'_k \mathfrak{B}$ if $\mathfrak{A}$ and $\mathfrak{B}$ agree on all monadic second-order sentences of quantifier rank $\leq k$, and $\mathfrak{A} \sim'_k \mathfrak{B}$ if Duplicator wins the k-round monadic second-order EF game on $\mathfrak{A}$ and $\mathfrak{B}$. The following lemma is a straightforward extension of the fundamental theorem about the first-order EF game.

Lemma 4.2 *For all structures $\mathfrak{A}$ and $\mathfrak{B}$ of the same type and all $k \in \omega$, $\mathfrak{A} \equiv'_k \mathfrak{B}$ if and only if $\mathfrak{A} \sim'_k \mathfrak{B}$.*

Let $\mathfrak{A}_i$, $i \in q$, be representatives from each $\sim'_k$ class of connected structures in $\mathcal{C}$ (there are only finitely many such classes). For $K \in \omega$, put $\mathfrak{A} \approx_K \mathfrak{B}$ if and only if, for every $i \in q$, $\mathfrak{A}$ and $\mathfrak{B}$ have the same number of components in the $\sim'_k$ class of $\mathfrak{A}_i$ or $\mathfrak{A}$ and $\mathfrak{B}$ both have at least K components in the $\sim'_k$ class of $\mathfrak{A}_i$. Thus $\approx_K$ is an equivalence relation with only finitely many equivalence classes.

[1] Compare the Wednesday lecture.

Lemma 4.3 *For every $k \in \omega$, there is $K \in \omega$ such that for all $\mathfrak{A}, \mathfrak{B} \in \mathcal{C}$, $\mathfrak{A} \approx_K \mathfrak{B}$ implies $\mathfrak{A} \equiv'_k \mathfrak{B}$.*

The proof of this lemma is an application of Lemma 4.2.

To complete the proof that i. implies iii., we need only show that if $a(x) \to \infty$, then there is one $\approx_K$ class whose probability approaches 1. For any $i < q$ and $j \in \omega$, let $\theta_{\mathfrak{A}_i,j}$ be the sentence that says "There are exactly j components isomorphic to $\mathfrak{A}_i$." By Theorem 3.5 of Wednesday, $\lim_{n\to\infty} \mathrm{pr}(\theta_{\mathfrak{A}_i,j}, n) = 0$. Therefore the $\approx_K$ class consisting of structures with at least K components $\sim'_k \mathfrak{A}_i$ for each $i < q$ has probability asymptotic to 1.

4.2 Fragments of SO∃

SO∃ is the class of second order existential formulas

$$\exists S_1 \cdots \exists S_k \theta$$

where θ is first order. Unless stated otherwise, we assume that the first-order language contains equality. In general, SO∃ has neither a 0-1 law nor a convergence law.

Example: SO∃ can express that the size of the model is even. Therefore, SO∃ in general has no 0-1 law.

QUESTION: Can we classify the SO∃ sentences which have a 0-1 law?

Before answering this question, let us turn to Trakhtenbrot's classical result:

Theorem 4.4 (Trakhtenbrot, 1950) *The class of first-order sentences which are satisfied by some finite model is not recursive, but only recursively enumerable.*

However, if we classify first-order formulas by their quantifier prefix it turns out that for the following two prefix classes the finite satisfiability problem is solvable:

- Bernays-Schönfinkel (B-S) class:[2] $\exists^*\forall^*$
- Ackermann class: $\exists^*\forall\exists^*$

For *all* other prefix classes, the full strength of Trakhtenbrot's theorem applies, even when restricted to sentences without equality. B-S and Ackermann are also the only prefix classes for which the satisfiability problem is solvable.

We say that a class of sentences has a solvable 0-1 law if it has a 0-1 law and the problem of determining the asymptotic probability of a sentence is recursive. Let us consider fragments of SO∃ obtained by restricting the prefix

[2] Here, $\exists^*$ (or $\forall^*$) denotes a sequence of $\exists$ ($\forall$ resp.) quantifiers of arbitrary length.

of the first-order part. One can show that a solvable 0-1 law for a subclass of SO$\exists$ implies a solvable finite satisfiability problem for the corresponding first-order class (without equality). Therefore, SO$\exists$ with its first-order part in Bernays-Schönfinkel or Ackermann remain as the only candidates for a solvable 0-1 law. In fact, both formula classes have a 0-1 law, while the other prefix classes don't even have convergence. Thus we have the surprising fact that the SO$\exists$ sentences can be partitioned into fragments, and in each fragment the three notions of solvability agree.

We shall give a proof for the 0-1 law of B-S. 3SAT and $k-$colorability are expressible in this fragment of SO$\exists$. This implies that either almost all graphs are $3-$colorable, or almost all graphs are not $3-$colorable.

Theorem 4.5 (Kolaitis and Vardi, 1987) *For every SO$\exists$ sentence σ whose first-order part is in the Bernays-Schönfinkel class,*

$$\lim_{n\to\infty} \mathrm{pr}(\sigma, n) = 0 \text{ or } 1$$

under uniform distribution on relational structures.

Proof. Recall the methodology developed in the Monday lecture for the first order 0-1 law: A denotes the set of extension axioms, and $\mathfrak{A}$ is the unique countable model of A. As argued there, it suffices to show the *transfer principle*:

$$\underbrace{\mathfrak{A} \models \sigma}_{\text{truth}} \quad \Leftrightarrow \quad \underbrace{\mathrm{pr}(\sigma, n) \to 1}_{\text{probabilistic truth}}$$

$\Rightarrow$: First we show that there is a first-order sentence ψ, such that $\lim_{n\to\infty} \mathrm{pr}(\psi, n) = 1$ and $\models_{\text{fin}} \psi \Rightarrow \sigma$. Let $\sigma = (\exists\overline{S})(\exists\overline{x})(\forall\overline{y})\theta(\overline{S}, \overline{x}, \overline{y})$. By assumption $\mathfrak{A} \models \sigma$, hence there exist witnesses $\overline{S}, \overline{a}$, such that

$$< \mathfrak{A}, \overline{S} > \models (\forall\overline{y})\theta(\overline{S}, \overline{a}, \overline{y})$$

Let $\mathfrak{A}_0$ be the restriction $\mathfrak{A} \restriction \overline{a}$, i.e. the *finite* substructure of $\mathfrak{A}$ whose universe consists just of the elements of $\overline{a}$. Then there is a first-order sentence $\psi = \alpha_1 \wedge \cdots \wedge \alpha_k$ which is a finite conjunction of extension axioms, such that each model of ψ has a substructure which is isomorphic to $\mathfrak{A}_0$.

Let $\mathfrak{B}$ be a finite model of ψ. Since $\mathfrak{A} \models A$, we can use the extension axioms to find a substructure $\mathfrak{B}^*$ of $\mathfrak{A}$, such that $\mathfrak{B}^*$ contains $\mathfrak{A}_0$ and is isomorphic to $\mathfrak{B}$.

Since $< \mathfrak{A}, \overline{S} > \models (\forall\overline{y})\theta(\overline{S}, \overline{a}, \overline{y})$ and universal statements are preserved under substructures, we conclude that $< \mathfrak{B}^*, S > \models (\forall\overline{y})\theta(\overline{S}, \overline{a}, \overline{y})$. $\mathfrak{B}$ and $\mathfrak{B}^*$ are isomorphic, hence it follows that $\mathfrak{B} \models (\exists\overline{S})(\exists\overline{x})(\forall\overline{y})\theta(\overline{S}, \overline{x}, \overline{y})$, and $\models_{\text{fin}} \psi \Rightarrow \sigma$.

Since σ is the consequence of a finite number of axioms, it has probability 1, i.e. $\mathrm{pr}(\sigma, n) \to 1$.

$\Leftarrow$: By contraposition, we assume that $\mathfrak{A} \models \neg\sigma$, and show that there exists a first-order sentence ψ, such that $\mathrm{pr}(\psi, n) \to 1$ and $\models_{\text{fin}} \psi \Rightarrow \neg\sigma$. Let $\sigma = (\exists\overline{S})\theta(\overline{S})$ be a SO$\exists$ formula. (For this direction of the proof, it is not necessary that θ be B-S.)

Claim: There exists a finite conjunction $\psi = \alpha_1 \wedge \cdots \wedge \alpha_k$ of extension axioms, such that $\models \psi \Rightarrow \neg\sigma$.

Since ψ has asymptotic probability 1, $\neg\sigma$ has asymptotic probability 1, hence σ has asymptotic probability 0, and we are done.

Proof of Claim. Suppose not. Then for any finite collection of axioms $A' \subset A$, the set $A' \cup \{\theta(\overline{S})\}$ is satisfiable (over the vocabulary of A, expanded by $\overline{S}$). By the Compactness and downward Löwenhein-Skolem theorems $A' \cup \{\theta(\overline{S})\}$ has a countable model $\mathfrak{B}$. The reduct of $\mathfrak{B}$ to the vocabulary of A is a model of A, and therefore must be isomorphic to $\mathfrak{A}$ via an isomorphism f, because A is categorical. But then $\mathfrak{A} \models (\exists\overline{S})\theta(\overline{S})$ with the witness for $\overline{S}$ being $f(S^{\mathfrak{B}})$. Contradiction. $\square$

Related results:

1. For SO$\exists$ B-S formulas, the problem of deciding whether a sentence has limiting probability 1 is NEXPTIME-complete, and thus solvable. The proof uses Ramsey theory.

2. The SO$\exists$ Ackermann class has a 0-1 law and, like B-S, the problem of deciding if a sentence has limiting probability 1 is NEXPTIME-complete.

3. If the language does not contain equality, then the Gödel class $\exists^*\forall^2\exists^*$ has a 0-1 law, and therefore a solvable finite satisfiability problem.

4.3 Random Graphs

A random graph, as introduced in Tuesday's lecture, is a graph on n vertices such that for each pair of vertices i and j, $\{i, j\}$ is an edge of the graph with probability $p(n) = \beta n^{-\alpha}$, for some constants $\alpha, \beta \geq 0$. As before, when $\alpha = 0$, $0 \leq \beta \leq 1$, and when $\alpha > 0$, we take $\beta = 1$.

The asymptotic behaviour of first-order logic over random graphs is now fairly well understood:

First-Order Logic over Random Graphs

1. $0 < \alpha < 1$, α rational: nonconvergence.

2. $\alpha = 1$ or $\alpha = \frac{m+1}{m}$ for $m = 1, 2, 3, \ldots$: convergence.

3. For all other cases: 0-1 law.

For $L^{\omega}_{\infty\omega}$, when $1 \geq \alpha > 0$, nonconvergence holds; everything else is the same. Let us now turn to some of the more specific results, giving exacter account of the convergence rate.

The first results for higher-order logics pertained to constant edge probability, and culminated with the following theorem:

Theorem 4.6 (Kolaitis and Vardi, 1992) *For p =constant, every sentence $\sigma \in L^{\omega}_{\infty\omega}$ has $\lim_{n\to\infty} \mathrm{pr}(\sigma, n) = 0$ or 1.*

Proof Idea. For structures $\mathfrak{A}$ and $\mathfrak{B}$ and $k \in \omega$, let $\mathfrak{A} \sim^{\infty}_{k} \mathfrak{B}$ mean Duplicator has a winning strategy for the infinitary k-pebble game on $\mathfrak{A}$ and $\mathfrak{B}$, and let $\mathfrak{A} \equiv^{\infty}_{k} \mathfrak{B}$ mean $\mathfrak{A}$ and $\mathfrak{B}$ agree on all sentences in $L^{k}_{\infty\omega}$. As in the case of first-order logic, these two notions are equivalent. We can find a large $\sim^{\infty}_{k}$ class of graphs. As with first-order logic, this is the class of graphs satisfying the axioms in A_k, which has asymptotic probability 1. □

By looking at the rate estimates in the proof, it can be seen that the probability converges exponentially fast to the limit of 0 or 1. In addition, for every formula $\sigma(x_1, \ldots, x_k) \in L^{\omega}_{\infty\omega}$, there is a first-order formula $\sigma'(x_1, \ldots, x_k)$ and $d > 0$, such that asymptotically

$$\mathrm{pr}(\forall x_1, \ldots, \forall x_k(\sigma \leftrightarrow \sigma')) > 1 - 2^{-n^d}.$$

The cases where a 0-1 or convergence law holds for variable edge probability are covered in the next theorem.

Theorem 4.7 (Lynch, 1993) *Let $p(n) = n^{-\alpha}$ where $\alpha > 1$. Then for every $\sigma \in L^{\omega}_{\infty\omega}$, either*

1. $\mathrm{pr}(\sigma, n) < 2^{-n^d}$ *for some* $d > 0$, *or*
2. $\mathrm{pr}(\sigma, n) \sim cn^{-d}$ *for some* $c > 0, d \geq 0$.

Further, for every formula $\sigma(x_1, \ldots, x_k) \in L^{\omega}_{\infty\omega}$, there is a first-order formula $\sigma'(x_1, \ldots, x_k)$ and $d > 0$, such that asymptotically

$$\mathrm{pr}(\forall x_1, \ldots, \forall x_k(\sigma \leftrightarrow \sigma')) > 1 - 2^{-n^d}$$

Thus, for the cases where a 0-1 or convergence law holds, first-order logic and $L^{\omega}_{\infty\omega}$ are asymptotically very close. The proof of Theorem 4.7 uses sieve methods and Chernoff bounds, but a weaker version of this theorem can be proven using only basic methods of random graph theory.

Theorem 4.8 *Let $p(n) = n^{-\alpha}$, where $\frac{m}{m-1} > \alpha > \frac{m+1}{m}$, $m \in \{1, 2, 3, \ldots\}$. Then for every $\sigma \in L^{\omega}_{\infty\omega}$, $\lim_{n\to\infty} \mathrm{pr}(\sigma, n) = 0$ or 1.*

Proof Idea. The proof uses the following theorem, which is similar to Lemma 4.3:

Theorem 4.9 (Kolaitis, 1991) *Let $H \sqsubseteq G$ mean that H is a component of G. Let G_0, G_1 be two graphs such that for every connected graph H, either*

$$|\{H_0 \sqsubseteq G_0 : H_0 \equiv_k^\infty H\}|, |\{H_1 \sqsubseteq G_1 : H_1 \equiv_k^\infty H\}| \geq k$$

or

$$|\{H_0 \sqsubseteq G_0 : H_0 \equiv_k^\infty H\}| = |\{H_1 \sqsubseteq G_1 : H_1 \equiv_k^\infty H\}|$$

Then G_0 and G_1 agree on all sentences in $L^k_{\infty\omega}$.

Proof. Infinitary $k-$pebble game. □

Corollary 4.10 *Same as above, with $H_i \equiv_k^\infty H$ replaced by $H_i \cong H$, $i = 0, 1$.*

Some basic results of random graph theory are that with asymptotic probability 1 the following hold:

1. All components of the graph will be trees.
2. There won't be tree components with $\geq m + 1$ vertices.
3. For any number K and tree T with $\leq m$ vertices, there will be at least K components isomorphic to T.

Combined with the above corollary, the theorem follows. □

4.4 Optimizing Database Queries

We conclude with a potential application of the previous results on rapid convergence to database query optimization. Relational databases can be seen as finite structures where a suitable logic serves as database query language.

Let $\mathfrak{A}$ be a finite structure of size n. Then $\mathfrak{A}$ can be encoded by a string of size n^r for some constant r dependent on the vocabulary. Let $\sigma(x_1, \ldots, x_k) \in L^k_{\infty\omega}$ be a query, and let $C_1, \ldots, C_d$ be a collection of $\equiv_k^\infty$ classes of $k-$tuples on inputs $\mathfrak{A}$, such that for almost all $\mathfrak{A}$, every $k-$tuple is in $\bigcup_{i=1}^d C_i$. If $d \ll n^r$, there is the potential for optimizing σ.

Abiteboul, Compton, and Vianu (1992) investigated the case where the vocabulary is relational, and pr_n is the uniform distribution. They proved the following result:

Theorem 4.11 *For every $k \in \omega$, there is a finite set of $\equiv_k^\infty$ classes $C_1, \ldots, C_d$ and first-order formulas $\phi_1(x_1, \ldots, x_k), \ldots, \phi_d(x_1, \ldots, x_k)$, such that*

1. $\forall \mathfrak{A}\ \forall a_1, \ldots, a_k \in |\mathfrak{A}|\ \forall i = 1, \ldots, d$, it holds that

$$\langle \mathfrak{A}, a_1, \ldots, a_k \rangle \in C_i \ \Leftrightarrow\ \mathfrak{A} \models \phi_i(a_1, \ldots, a_k)$$

.

2. There is $c < 1$ such that

$$\mathrm{pr}\left(\exists x_1 \ldots \exists x_k \left((x_1, \ldots, x_k) \notin \bigcup_{i=1}^{d} C_i\right), n\right) < c^n.$$

On a parallel processor, a first-order query has constant time complexity, but a fixed point query has time complexity n^t for some t. Therefore, the average time complexity of a query $\sigma(x_1, \ldots, x_k)$ is bounded above by

$$\begin{aligned}
& \mathrm{pr}(\forall x_1 \ldots \forall x_k ((x_1, \ldots, x_k) \in \bigcup_{i=1}^{d} C_i), n) \\
& \times \max_{i=1,\ldots,d} (\mathrm{complexity}(\langle \mathfrak{A}, x_1, \ldots, x_k \rangle \in C_i)) \\
& + \mathrm{pr}(\exists x_1 \ldots \exists x_k ((x_1, \ldots, x_k) \notin \bigcup_{i=1}^{d} C_i, n)) \times \mathrm{complexity}(\sigma) \\
\leq \; & \max_{i=1,\ldots,d} (\mathrm{complexity}(\phi_i)) + c^n \times n^t \\
\leq \; & K
\end{aligned}$$

for some constant K.

notes taken by H.Veith, veith@dbai.tuwien.ac.at

Session V: Friday, August 18

Track C: Random Finite Models

James F. Lynch

5 Nonconvergence

Up to now, we have concentrated on examples of convergent behavior. There is an equally well-developed theory of nonconvergence in random finite structures. We will cover some aspects of it today. First, however, left's summarize the asymptotic behavior of classes of first-order properties, where a lot is known.

Summary of Asymptotic Behavior, First-Order Logic

1. Labeled structures, uniform distribution
   (a) purely relational: 0-1 law (Fagin, 1976; Glebskiĭ et al., 1969)
   (b) relations, constants: convergence (Glebskiĭ et al.)
   (c) unary functions: convergence (Lynch, 1985; extends to unary functions + unary relations + constants)
   (d) 1 binary function: nonconvergence (Compton, Henson, and Shelah, 1987)
   (e) 1 unary function + 1 binary relation: nonconvergence (Tyszkiewicz, 1996)
2. Unlabeled structures, uniform distribution
   (a) purely relational: 0-1 law (Liogon'kiĭ, 1970; Fagin, 1976)
   (b) relations + constants: convergence (Liogon'kiĭ)
   (c) 2 unary functions + unary relations + constants: convergence (Foy and Woods, 1990)
   (d) 1 unary function + unary relations: convergence, even for monadic SOL (Woods, 1996)
   (e) 1 unary function + unary relations + constants: open problem (?)
   (f) 1 binary function: nonconvergence (Freese, 1990)
   (g) 1 unary function + 1 binary relation: nonconvergence (Tyszkiewicz, 1996)
3. Structures with built-in relations, uniform distribution
   (a) unary relations + constants:+ built-in $\leq$: convergence (subsequence convergence for monadic SOL) (Lynch, 1993)

(b) relations + constants + built-in successor: convergence (Lynch, 1980)

(c) binary relation + built-in $\leq$: nonconvergence (Compton, Henson, and Shelah, 1987)

4. Random graphs, edge probability $p(n) = n^{-\alpha}$

   (a) $\alpha = 0$: 0-1 law (Fagin; Glebskiĭ et al.)

   (b) $0 < \alpha < 1$, irrational: 0-1 law (Shelah and Spencer, 1988)

   (c) $0 < \alpha < 1$, rational: nonconvergence (Shelah and Spencer)

   (d) $\alpha = 1$: convergence (Lynch, 1992)

   (e) $\alpha > 1$, $\alpha \neq (k+1)/k$: 0-1 law (Shelah and Spencer)

   (f) $\alpha = (k+1)/k$: convergence (Lynch)

Today we will examine three cases where convergence fails. In these, and indeed in most of the proofs of nonconvergence, the key idea is to find in the random structure of size n, some set of r-tuples which is definable in $\mathcal{L}$ and whose size is an unbounded function f of n. Let P and Q be disjoint, infinite subsets of the range of f. If there exists $\sigma \in \mathcal{L}$ such that with probability asymptotic to 1,

$$\begin{aligned} f(n) \in P \quad &\Rightarrow \quad \mathfrak{A} \models \sigma \text{ and} \\ f(n) \in Q \quad &\Rightarrow \quad \mathfrak{A} \models \neg\sigma, \end{aligned}$$

then the probability of σ does not converge. The definition of the set of r-tuples can be quite involved. Sometimes it is done by encoding either an initial segment of arithmetic or a sequence of instantaneous descriptions of a Turing machine. A built-in linear ordering helps, of course. This is demonstrated by our first theorem, which is an extension of 3. (c) above. It shows that when the vertices of a random graph are linearly ordered, convergence fails not only for all edge probabilities of the form $n^{-\alpha}$, but for all reasonable edge probabilities. (Compare with the various cases in 4. above.)

Theorem 5.1 (Dolan and Lynch, 1993) *Let $\mathcal{L}$ be the first-order language of ordered graphs, i.e. structures of the form $\langle\{0,\ldots,n-1\}, E, \leq\rangle$, where $\langle\{0,\ldots,n-1\}, E\rangle$ is a graph and $\leq$ is the usual linear ordering on $\{0,\ldots,n-1\}$. Let $p(n) \geq g(n)/n^2$ for some unbounded recursive function g. Then there exists $\sigma \in \mathcal{L}$ such that* $\mathrm{pr}(\sigma, n)$ *does not converge.*

The proof, which is quite technical, involves the encoding of the moves of a Turing machine by a binary relation defined on the random graph.

The same key idea often works for proving nonconvergence in higher-order logics. Although the $L^{\omega}_{\infty,\omega}$ logic of random graphs obeys a convergence law when $p(n) = n^{-\alpha}$ and $\alpha > 1$, convergence fails when $\alpha \leq 1$. [3] In fact, the following stronger result holds when $\alpha = 1$.

Theorem 5.2 (Lynch and Tyszkiewicz, 1995) *Let $\mathcal{L}$ be the deterministic transitive closure logic of random graphs with edge probability n^{-1}. Then there exists $\sigma \in \mathcal{L}$ such that $\mathrm{pr}(\sigma, n)$ does not converge.*

Proof Sketch Let $\mathrm{lc}(G)$ be the size of the largest chain component in G. With probability asymptotic to 1,

$$\frac{\ln n}{2} < \mathrm{lc}(G) \leq 4 \ln n.$$

Thus if $n = \lfloor e^{2 \cdot 8^{2k}} \rfloor$, then

$$8^{2k} \leq \mathrm{lc}(G) < 8^{2k+1} \text{ and}$$
$$\lfloor \log_8(\mathrm{lc}(G)) \rfloor = 2k.$$

But if $n = \lfloor e^{2 \cdot 8^{2k+1}} \rfloor$, then

$$\lfloor \log_8(\mathrm{lc}(G)) \rfloor = 2k + 1.$$

We will be done when we show that "$\log_8$ of the size of the largest chain component is even," is expressible in deterministic transitive closure (DTC).

A *chain component* of a graph is a component that is a simple path. In order to "determinize" chain components, we will use pairs of vertices $\mathbf{x} = (x_1, x_2)$ such that $\{x_1, x_2\} \in E$ and the dual relation $D(\mathbf{x}, \mathbf{y})$ which holds for $\mathbf{x} = (x_1, x_2)$, $\mathbf{y} = (y_1, y_2)$ when $x_2 = y_1$ and $x_1 \neq y_2$. We can express in DTC:

1. "$\mathbf{x}$ is in a component with no vertices of degree > 2 and no cycles." That is, $\mathbf{x}$ is in a chain component.

2. "$\mathbf{x}$ is in a maximal size chain component."

3. "$\mathbf{x}$ and $\mathbf{y}$ are in the same chain component."

4. For $\mathbf{x}$ and $\mathbf{y}$ satisfying 1.–3. and $\mathbf{x}'$ and $\mathbf{y}'$ satisfying 1.–3., "the distance from $\mathbf{x}'$ to $\mathbf{y}'$ is twice the distance from $\mathbf{x}$ to $\mathbf{y}$".

It is fairly straightforward to express these properties in DTC. For example, 4. is the deterministic transitive closure of

$$D(\mathbf{x}, \mathbf{y}) \wedge \exists \mathbf{z}(D(\mathbf{x}', \mathbf{z}) \wedge D(\mathbf{z}, \mathbf{y}')).$$

[3] It was erroneously reported in Lynch and Tyszkiewicz (1995) that convergence holds for $L^{\omega}_{\infty,\omega}$ when $\alpha < 1$ and is irrational. This was shown to be false by McArthur. However, convergence does hold for the transitive closure logic of random graphs in this case.

For $\mathbf{u}$ and $\mathbf{v}$ satisfying 1.–3., by using 4. we can express $\mathbf{u} = 2\mathbf{v}$, meaning "$\mathbf{u}$ is twice as far from one endpoint of its chain component as $\mathbf{v}$ is." Similarly, we can express $\mathbf{u} = 64\mathbf{v}$. Then $\mathbf{u} = 8^{2k}\mathbf{v}$ for some $k \in \omega$ is expressible as the deterministic transitive closure of $\mathbf{u} = 64\mathbf{v}$. From this, we can express "$\lfloor \log_8(\mathrm{lc}(G)) \rfloor$ is even." □

Our third example is one of the first important nonconvergence theorems. It was originally proven by Kaufmann and Shelah (1985) for monadic second-order logic. Here we give a stronger result and a newer proof due to Kaufmann (1988).

Theorem 5.3 (Kaufmann, 1988) *Let $\mathcal{L}$ be the monadic SO∃ logic of four binary relation symbols with a uniform distribution. Then*

1. *There exists $\sigma \in \mathcal{L}$ such that $\mathrm{pr}(\sigma, n)$ does not converge.*
2. *For every rational $r \in [0,1]$, there exists $\sigma \in \mathcal{L}$ such that $\lim_{n\to\infty} \mathrm{pr}(\sigma, n) = r$.*

Proof. The theorem is a consequence of the following lemma, whose proof is deferred.

Lemma 5.4 *There is a first-order formula $\phi(x,y)$ in the vocabulary of $\mathcal{L}$ expanded with additional unary relation symbols $\overline{P}$ such that the following sentence has probability asymptotic to 1.*

$$\exists \overline{P}(\phi(x,y) \text{ defines a linear order on the universe.})$$

Assuming this lemma, let Q be a unary relation symbol. Form the monadic SO∃ sentence

$$\begin{aligned}\exists \overline{P} \exists Q(\ & \phi(x,y) \text{ defines a linear order on the universe,} \\ & \text{and } Q \text{ contains every other element, including the first and the last.})\end{aligned}$$

This sentence is true if and only if the size of the universe is odd, and part 1. of the theorem follows.

To prove 2., let R be one of the binary relation symbols in the vocabulary of $\mathcal{L}$. Take any $r = p/q$, where $p, q \in \omega$, $p \le q$. For each $i = 0, \ldots, p-1$, construct a monadic SO∃ sentence which means $|\{x : R(x,x)\}| \equiv i \pmod q$. For example,

$$\begin{aligned}\exists \overline{P} \exists Q(\ & \phi(x,y) \text{ defines a linear order on the universe,} \\ & \text{and } Q \text{ contains every } q\text{th element of } \{x : R(x,x)\}, \\ & \text{including the first and the last.})\end{aligned}$$

means $|\{x : R(x,x)\}| \equiv 1 \pmod q$. Each of these sentences has probability asymptotic to $1/q$. Therefore

$$\bigvee_{i=0}^{p-1} |\{x : R(x,x)\}| \equiv i \pmod q$$

has probability asymptotic to p/q.

We now begin the proof of the main lemma 5.4.

Definition 5.5 *Let $\mathfrak{A} = \langle A, R\rangle$ where R is a binary relation on A, and let $S, T \subseteq A$.*

1. *For $t \in T$, we say t R-codes $\{s \in S : (s,t) \in R\}$.*
2. *T R-codes distinct subsets of S if no two members of T R-code the same subset of S.*
3. *T R-codes the power set of S if T R-codes distinct subsets of S and every subset of S is R-coded by some member of T.*

Lemma 5.6 *Let $\mathfrak{A} = \langle A, R\rangle$ where R is a random binary relation on A. If $S, T \subseteq A$ and $|T| \geq |S|2^{|S|}$, then with probability asymptotic to 1 as $|S| \to \infty$, some subset of T R-codes the power set of S.*

Proof. We need only show every subset of S is R-coded by some element of T. The probability that this fails is

$$\begin{aligned}
&\leq \sum_{S' \subseteq S} \mathrm{pr}(S' \text{ not } R\text{-coded by some } t \in T, n) \\
&= \sum_{S' \subseteq S} \prod_{t \in T} \mathrm{pr}(S' \text{ not } R\text{-coded by } t, n) \\
&\leq 2^{|S|}(1 - 2^{-|S|})^{|S|2^{|S|}} \\
&\leq 2^{|S|}e^{-|S|} \\
&\to 0.
\end{aligned}$$

□

Lemma 5.7 *Let $\mathfrak{A} = \langle A, R, S, T\rangle$ where R is a binary relation on A and $S, T \subseteq A$. If T R-codes distinct subsets of S and there is a first-order definable $<_S$ on S, then there is a first-order definable $<_T$ on T.*

Proof. Since T R-codes distinct subsets of S, the elements of T can be lexicographically ordered as follows. Let $x, y \in T$ R-code $U, V \subseteq S$, and let w be the $<_S$-smallest member of $(U - V) \cup (V - U)$. Then $x <_T y$ if and only if $x \neq y$ and $w \notin U$. □

Lemma 5.8 *Let $R \subseteq \{0, 1, \ldots, k-1\}^2$ and $n > k^2 4^k$. Let $p(k)$ be the probability that a random model $\langle \{0, 1, \ldots, n-1\}, R'\rangle$ contains an isomorphic copy of $\langle \{0, 1, \ldots, k-1\}, R\rangle$. Then*

$$\lim_{k \to \infty} p(k) \to 1$$

(uniformly in n).

Proof. Let $a = k4^k$, and $\bigcup_{i=0}^{k-1} S_i \subseteq n$ where $|S_i| = a$ and $S_i \cap S_j = \emptyset$ when $i \neq j$. Inductively, for $j = 0, \ldots, k-1$, try to extend an embedding of $\langle\{0, 1, \ldots, j-1\}, R\rangle$ into $\bigcup_{i=0}^{j-1} S_i$ to an embedding of $\langle\{0, \ldots, j\}, R\rangle$ into $\bigcup_{i=0}^{j} S_i$, where j is mapped to some $j' \in S_j$. The probability that this fails is

$$\begin{aligned} &\leq \sum_{j=0}^{k-1}(1 - \frac{1}{2 \cdot 4^j})^a \\ &\leq k(1 - \frac{1}{4^k})^a \\ &\to 0 \end{aligned}$$

since $a = k4^k$. □

We can now finish the proof of the main lemma 5.4. Take a random model $\langle\{0, 1, \ldots, n-1\}, R, R_0, R_1, R_2\rangle$. Let k be the largest integer such that $n \geq 2^k 2^{2^k}$. Since $2^{2^k} > k^2 4^k$ (k sufficiently large), by Lemma 5.8, with probability asymptotic to 1, there is a $P_0 \subseteq n$ such that $|P_0| = k$ and $R \restriction P_0$ is a linear order.

By Lemma 5.6, with probability asymptotic to 1, there is a $P_1 \subseteq n$ such that P_1 R_0-codes the power set of P_0 and $P_2 \subseteq n$ such that P_2 R_1-codes the power set of P_1. The probability that n does *not* R_2-code distinct subsets of P_2 is

$$\begin{aligned} &\leq n^2 \times 2^{-2^{2^k}} \\ &\leq (2^{k+1}2^{2^{k+1}})^2 \times 2^{-2^{2^k}} \\ &\to 0. \end{aligned}$$

Using Lemma 5.7 three times, there is a definable $<$ on n. □

notes taken by Ida Pu, ida@dcs.warwick.ac.uk