0-1 Law For Graphs

We will only be considering *relational* structures; that is, our vocabulary σ will only contain relations, not functions or constants. A property $\mathcal{P}$ of finite σ-structures a set of finite σ-structures which is closed under isomorphism. Consider the probability of whether a randomly chosen structure is in $\mathcal{P}$. Denote by $Struct_n[\sigma]$ the class of all structures with signature σ on elements $\{0, ..., n-1\}$. Define

$$\mu_n(\mathcal{P}) := \frac{|(Struct_n[\sigma] \cap \mathcal{P})|}{|Struct_n[\sigma]|}$$

$\mu_n(\mathcal{P})$ is the probability of $\mathcal{P}$ holding for a structure of size n. Define

$$\mu(\mathcal{P}) := \lim_{n\to\infty} \mu_n(P)$$

so $\mu(\mathcal{P})$ is the asymptotic probability. Note that this definition can be relativized to some class $\mathcal{C}$, ie

$$\mu_n(\mathcal{P}|\mathcal{C}) := \frac{|(Struct_n[\sigma] \cap \mathcal{P} \cap \mathcal{C})|}{|(Struct_n[\sigma] \cap \mathcal{C})|}$$
$$\mu(\mathcal{P}|\mathcal{C}) := \lim_{n\to\infty} \mu_n(\mathcal{P}|\mathcal{C})$$

Often, $\mathcal{C}$ is taken to be the class $\mathcal{G}$ of simple graphs. For any pair of nodes n, n', exactly half of the graphs in $\mathcal{G}$ have an edge (n, n'). $\mu_n(\mathcal{P}|\mathcal{G})$ can then be thought of as the probability that a randomly selected simple graph of size n has property $\mathcal{P}$.

Theorem 1 (First-Order Zero-One Law For Graphs)**.** *If $\mathcal{P}$ is first-order defineable over graphs, then $\mu(\mathcal{P}|\mathcal{G}) \in \{0,1\}$.*

In general, say that *a logic $\mathcal{L}$ has the **zero-one law** over a class $\mathcal{C}$* iff for every property $\mathcal{P}$ defineable in $\mathcal{L}$ over $\mathcal{C}$, $\mu_n(\mathcal{P}|\mathcal{C}) \in \{0,1\}$.

If $\mu(\mathcal{P}) = 1$ we say "$\mathcal{P}$ holds almost always". If $\mu(\mathcal{P}) = 0$ we say "$\mathcal{P}$ holds almost never".

To prove 1, we use the following lemma

Lemma 2. *Let $\mathcal{L}$ be a logic. Suppose T is a $\mathcal{L}$-theory with the following properties*

1. *Every sentence in T holds almost always for structures in $\mathcal{C}$.*

2. *T is complete.*

Then $\mathcal{L}$ has a zero-one law over $\mathcal{C}$.

Proof. Consider a sentence ϕ. By completeness, either $T \models \phi$ or $T \models \neg\phi$. Suppose $T \models \phi$. Then by compactness ϕ follows from finitely many sentences $\psi_0, ..., \psi_m \in T$. But each ψ_i holds almost always among $\mathcal{C}$, so ϕ holds almost always among $\mathcal{C}$. Suppose $T \models \neg\phi$. Similarly then, $\neg\phi$ holds almost always, so ϕ holds almost never. $\square$

Extension Axioms

Define the *extension axiom* $EA_{k,l}$ as

$$EA_{k,l} := \forall x_1, ..., \forall x_{k+l}\left[\left(\bigwedge_{i\neq j} x_i \neq x_j\right) \implies \exists y\left(\bigwedge_i \begin{cases} E(x_i, y) \wedge x_i \neq y & i \leq k \\ \neg E(x_i, y) \wedge x_i \neq y & i > k \end{cases}\right)\right]$$

$EA_{k,l}$ says that given $k+l$ distinct vertices, a new vertex can be found that is adjacent to the first k and not adjacent to the last l. The theory EA is defined as $EA := \bigcup_{k,l\geq 0} EA_{k,l}$. EA will be the theory we use as our theory T from 2. To do so, we must first show that the elements of EA (that is, all $EA_{k,l}$) hold almost always. Next, we will show that EA is complete.

Lemma 3. $\mu(EA_{k,l}|\mathcal{G}) = 1$

Proof. Let n be the size of our graph. We prove that $\mu(\neg EA_{k,l}|\mathcal{G}) = 0$. That is, the probability that there are $k+l$ distinct vertices and no $(k+l+1)^{st}$ vertex which connects to the first k and not the last l goes to zero as $n \to \infty$.

Fix $x_1, ..., x_{k+l}$. For each y which is not one of the x_i's, the chance that it is connected correctly (ie, to the first k, not the last l) is $\frac{1}{2^{k+l}}$. So the likelihood that none of the $n-k-l$ nodes have the right connections is $(1-1/2^{k+l})^{n-k-l}$. There are $\frac{n!}{(n-k-l)!}$ ways to pick the $x_1, ..., x_{k+l}$. So the worst-case probability of there being at least one such subset witnessing $\neg EA_{k,l}$ is $\frac{n!}{(n-k-l)!}(1-1/2^{k+l})^{n-k-l} = O(n^{k+l}(1-1/2^{k+l})^n)$. The O-bound goes to 0 as $n \to \infty$, so $\mu(\neg EA_{k,l}|\mathcal{G}) = 0$, so $\mu(EA_{k,l}|\mathcal{G}) = 1$. □

Random Graphs

We construct a countable model for EA, called the *random graph*. Let $[i]_j$ denote the j^{th} bit of the binary expansion of (the natural number) i. Define the *random graph* $\mathfrak{RG}$ as having vertices $V = \{v_i | i \in \mathbb{N}\}$ and an edge (v_i, v_j) iff $[i]_j = 1$ or $[j]_i = 1$. This is equivalent to the graph obtained by building up a countable graph by adding new vertices one at a time, adding edges connecting to each old vertex with even probability.

Lemma 4. $\mathfrak{RG} \models EA$

Proof. We verify $\mathfrak{RG} \models EA_{k,l}$ for arbitrary k, l. Fix k, l and suppose we are given $K, L \subseteq V$ such that $, V \cap L = \emptyset, |K| = k, |L| = l$. We want to find a y adjacent to all of K and not adjacent to anything in L. Consider

$$s = \sum_{v_i \in K} 2^i$$

and let $y = v_s$. Then y is connected to all elements of K because $[s]_i = 1$ for all $\{i | v_i \in K\}$. Moreover, we never have $[s]_i = 1$ for $v_i \in L$. However, we could have $[i]_s = 1$ for some $v_i \in L$ if s is too small. We fix this by picking some $l > max(K \cup L)$ and letting

$$s' = s + 2^l$$

which has the same lower bits as before, meaning $[s']_i$ is 1 or 0 if $v_i \in K, L$ respectively. Moreover, there is no chance that $[i]_{s'} = 1$ when $v_i \in L$, because $s' \geq 2^l > l > max(K \cup L) \geq \lg max(L) + 1$ (which is the max number of binary digits in an element of L). $\square$

On the other hand, every countable model of EA is isomorphic to $\mathfrak{RG}$.

Lemma 5. *EA is ω-categorical.*

Proof. We inductively build an isomorphism between countable models $\mathfrak{A}, \mathfrak{B} \models EA$. Suppose wlog that $\mathfrak{A}, \mathfrak{B}$ have universe $\{0, 1, 2, ...\}$

BASE: the trivial isomorphism i_0 from $\mathfrak{A}_0 = \emptyset$ to $\mathfrak{B}_0 = \emptyset$.

INDUCT: On the k^{th} step, $k > 0$, do one "$\mathfrak{A}\mathfrak{B}$-step" and one "$\mathfrak{B}\mathfrak{A}$-step".

- $\mathfrak{A}\mathfrak{B}$-step: Find the least $a \in \mathfrak{A}_k - \mathfrak{A}_{k-1}$ (ie, the least unmatched element in $\mathfrak{A}$). Let K be the vertices of $\mathfrak{A}_{k-1}$ adjacent to a, and L the ones not adjacent. $EA_{|K|,|L|}$ applied to $i_{k-1}(K), i_{k-1}(L) \in \mathfrak{B}_{k-1} = i_{k-1}(\mathfrak{A}_{k-1})$ guarantees there is a vertex $b \in \mathfrak{B}$ such that when we extend i_{k-1} by sending a to b, we get an isomorphism i'_{k-1} from $\mathfrak{A}'_{k-1} = \mathfrak{A}_{k-1} \cup \{a\}$ to $\mathfrak{B}'_{k-1} = \mathfrak{B}_{k-1} \cup \{b\}$.
- $\mathfrak{B}\mathfrak{A}$-step: same as above, but reverse the roles of $\mathfrak{A}, \mathfrak{B}$ to muve from $i'_{k-1} : \mathfrak{A}'_{k-1} \to \mathfrak{B}'_{k-1}$ to $i_k : \mathfrak{A}_k \to \mathfrak{B}_k$.

Because we pick the smallest unmatched vertex each time, each verex will eventually be paired up. $\bigcup_k i_k$ gives an isomorphism $i : \mathfrak{A} \to \mathfrak{B}$. $\square$

Lemma 6. *EA is complete.*

Proof. Suppose ad reductio that there were some ϕ s.t. neither $EA \models \phi$ nor $EA \models \neg\phi$. Then $\{EA \cup \phi\}$ and $\{EA \cup \neg\phi\}$ are both consistent and so have models (which must be infinite by the definition of EA). By the downward Lowenheim-Skolem theorem, $EA \cup \{\phi\}$ and $EA \cup \{\neg\phi\}$ have countable models $\mathfrak{M}_0, \mathfrak{M}_1$ respectively. As EA is ω-categorical, $\mathfrak{M}_0 \cong \mathfrak{M}_1 \cong \mathfrak{RG}$. But then $\mathfrak{RG} \models \phi$ and $\mathfrak{RG} \models \neg\phi$, a contradiction. So EA is complete. $\square$

Proof of Theorem 1. By Lemma 3, every sentence of EA holds almost always among $\mathcal{G}$. By Lemma 6, EA is complete. Lemma 2 applies and the result follows. $\square$

Corollary 7. *For FO sentences ϕ, $\mathfrak{RG} \models \phi \iff \mu(\phi) = 1$*

Proof. Let $EA_i := EA_{i,i}$. Suppose $\mathfrak{RG} \models \phi$. By completeness, $EA \models \phi$ and by compactness, for some $k > 0$, $\{EA_i | i \leq k\} \models \phi$. So $EA_k \models \phi$, so $\mu(\phi) \geq \mu(EA_k) = 1$.

Suppose $\mathfrak{RG} \not\models \phi$. Then $\mathfrak{RG} \models \neg\phi$. Then $\mu(\neg\phi) = 1$ so $\mu(\phi) = 0$. $\square$

Lemma 8. *EA is decidable.*

Proof. EA is recursively axiomatizeable so it is decidable. $\square$

Corollary 9. *For a FO sentence ϕ, whether $\mu(\phi) = 1$ is decidable.*

Trakhtenbrot's theorem (see Prof. Tannen's Friendly Logic Notes) shows that it is undecidable whether a sentence is true in all finite models. By Corrolary 9, however, it is decidable whether a sentence is true in almost all finite models.

Theorem 10 (Grandjean)**.** *The problem of checking whether $\mu(\mathcal{P})$ is* 0 *or* 1 *is PSPACE-complete.*

Proof. See here for the original proof. □

Because of this, we have a fairly tight epistemological bound on what we can know about the properties of finite structures using only first-order methods. We cannot decide using first-order methods whether a property holds of all finite structures, but we can decide whether it holds of almost all finite structures in PSPACE. Unless $P = PSPACE$ (which is an open problem, but seems unlikely), the PSPACE-completeness of deciding $\mu(\mathcal{P})$ entails that it is unlikely that it will ever be decided by a sufficiently efficient algorithm.

References

[1] Joshua Horowitz. *Zero-One Laws, Random Graphs, and Fraisse Limits.* April 24, 2008.

[2] Etienne Grandjean. *Complexity of the first-order theory of almost all finite structures, Information and Control, Volume 57, Issue 2, 1983*, Pages 180-204, ISSN 0019-9958 http://www.sciencedirect.com/science/article/pii/S0019995883800436

[3] Val Tannen. *Friendly Logics, Fall 2015, Lecture Notes 1.* https://www.cis.upenn.edu/~val/CIS682/ln1.pdf

[4] Leonid Libkin. *Elements of Finite Model Theory*, Springer, 2012.