## Logic and Probability

Probabilities on rich languages, random structures and 0-1 laws

Thomas Icard \& Krzysztof Mierzewski


August 10, 2022

## Measure theory vs. probabilities over a language

Probability spaces in the measure theoretic sense are structures $(\Omega, \mathcal{E}, \mu)$ with

- $(\Omega, \mathcal{E})$ a measurable space, i.e. we have
- $\Omega$ is an arbitrary set
- $\mathcal{E}$ is a $\sigma$-algebra over $\Omega$, i.e., a subset of $\wp(\Omega)$ closed under complement and countable unions.
- $\mu: \mathfrak{E} \rightarrow[0,1]$ a countably additive measure, i.e.
- $\mu(\Omega)=1$;
- $\mu\left(\bigcup_{i \in \mathbb{N}}\right)=\sum_{n=0}^{\infty} \mu\left(E_{i}\right)$, when $E_{i} \cap E_{j}=\varnothing$ for $i \neq j$.

How do these relate to probabilities defined directly on logical languages?

Everyone says "consider the probability that $X \geq 0$," where $X$ is a random variable, and only the pedant insists on replacing this phrase by "consider the measure of the set $\{\omega \in \Omega: X(\omega) \geq 0\}$." Indeed, when a process is specified, only the distribution is of interest, not a particular underlying sample space. In other words, practice shows that it is more natural in many situations to assign probabilities to statements rather than sets.
—Scott \& Krauss 1966

Suppose we have a countable propositional language $\mathcal{L}$ :

$$
\varphi \quad::=\quad A_{1}\left|A_{2}\right| \ldots|\varphi \wedge \varphi| \neg \varphi
$$

We can define a probability $\mathbb{P}: \mathcal{L} \rightarrow[0,1]$ directly on $\mathcal{L}$ :

- $\mathbb{P}(\varphi)=1$, for any tautology $\varphi$;
- $\mathbb{P}(\varphi \vee \psi)=\mathbb{P}(\varphi)+\mathbb{P}(\psi)$, whenever $\vDash \neg(\varphi \wedge \psi)$.

Equivalent set of requirements:

- $\mathbb{P}(\varphi)=1$, for any tautology ;
- $\mathbb{P}(\varphi) \leq \mathbb{P}(\psi)$ whenever $\vDash \varphi \rightarrow \psi$;
- $\mathbb{P}(\varphi)=\mathbb{P}(\varphi \wedge \psi)+\mathbb{P}(\varphi \wedge \neg \psi)$.


## Some measure-theoretic notions

A family of subsets $\mathcal{R} \subseteq \wp(\Omega)$ forms a ring if

- $\varnothing \in \mathcal{R}$
- If $A, B \in \mathcal{R}$ then $A \cup B \in \mathcal{R}$ and $A \backslash B \in \mathcal{R}$

A measure $\mu$ is finite if $\mu(\Omega)$ is finite.
Given a family of subsets $\mathcal{F} \subseteq \wp(\Omega)$, let $\sigma(\mathcal{F})$ the smallest $\sigma$-algebra containing $\mathcal{F}$.

Theorem (Carathéodory's Extension Theorem)
Let $\mu$ be a measure on a ring $(\Omega, \mathcal{R})$. If $\mu$ is a finite measure that is $\sigma$-additive on $\mathcal{R}$, then there is a unique $\sigma$-additive measure $\mu^{\prime}$ on $\sigma(\mathcal{R})$ that extends $\mu$.

## From Probabilities on Languages to Spaces

- Let $\mathcal{V}$ be the set of all valuations in language $\mathcal{L}$.
- Let $\mathcal{O} \triangleq\{\llbracket \varphi \rrbracket: \varphi \in \mathcal{L}\}$, where $\llbracket \varphi \rrbracket=\{v: v \vDash \varphi\}$. Then $\mathcal{O}$ forms a Boolean algebra, hence also a ring. Moreover, any probability measure $\mathbb{P}$ generates a measure that is $\sigma$-additive on $\mathcal{O}$. By the Carathéodory Extension Theorem, it uniquely extends to a $\sigma$-additive measure on the smallest $\sigma$-algebra extending $\mathcal{O}$ [this uses Compactness!].
- In fact, $\mathcal{O}$ forms a clopen basis of a topology on $\mathcal{V}$, which is homeomorphic to standard Cantor space (coin-tossing space: space of infinite binary sequences with clopen basis of cylinder sets). The $\sigma$-algebra generated by $\mathcal{O}$ is the standard Borel $\sigma$-algebra on Cantor space.
- In this way we can show that all functions $\mathbb{P}: \mathcal{L} \rightarrow[0,1]$ can define all the usual probability measures (Borel measures).

Probabilities on propositional calculi are general, but not particularly expressive.

Let $\mathcal{L}$ be a first-order logical language, given by:

- a set $\mathcal{V}$ of individual variables;
- a set $\mathcal{C}$ of individual constants ;
- a set $\mathcal{P}$ of predicate variables .

Terms and formulas of $\mathcal{L}$ are defined as usual:

$$
\varphi \quad::=\quad R\left(t_{1}, \ldots, t_{n}\right)|\varphi \wedge \varphi| \neg \varphi|\exists x \varphi| \forall x \varphi
$$

Define $\mathcal{S}_{\mathcal{L}}$ to be the set of sentences of $\mathcal{L}$, i.e., formulas with no free variables, and $\mathcal{S}_{\mathcal{L}}^{0}$ to be the set of quantifier-free sentences of $\mathcal{L}$.

A probability on $\mathcal{L}^{\prime} \subseteq \mathcal{S}_{\mathcal{L}}$ is a function $\mathbb{P}: \mathcal{L}^{\prime} \rightarrow[0,1]$, with

- $\mathbb{P}(\varphi)=1$, for any first-order validity $\varphi$;
- $\mathbb{P}(\varphi \vee \psi)=\mathbb{P}(\varphi)+\mathbb{P}(\psi)$, whenever $\vDash \neg(\varphi \wedge \psi)$.

Question: Given a probability $\mathbb{P}: \mathcal{S}_{\mathcal{L}}^{0} \rightarrow[0,1]$, is there a natural extension of $\mathbb{P}$ to all of $\mathcal{S}_{\mathcal{L}}$ ?

Question: Given a probability $\mathbb{P}: \mathcal{S}_{\mathcal{L}}^{0} \rightarrow[0,1]$, is there a natural extension of $\mathbb{P}$ to all of $\mathcal{S}_{\mathcal{L}}$ ?

If there are only finitely many constants $c$ such that $\mathbb{P}(R(c))>0$, then:

$$
\mathbb{P}(\exists x R(x))=\mathbb{P}\left(\bigvee_{c \in \mathcal{C}} R(c)\right)
$$

What about in the case where the size of $\mathcal{C}$ is infinite?

## Example

Consider a simple first-order arithmetical language $\mathcal{L}$, with a constant $\mathbf{n}$ for each $n \in \mathbb{Z}^{+}=\{1,2,3 \ldots\}$. Let $R(x)$ be a one-place predicate. Define a probability function $\mathbb{P}: \mathcal{S}_{\mathcal{L}}^{0} \rightarrow[0,1]$ on the quantifier-free sentences so that:

- $\mathbb{P}(R(\mathbf{n}))=2^{-(n+1)}$, for all $n \in \mathbb{N}$;
- $\mathbb{P}\left(\bigwedge_{i \leq k} R\left(\mathbf{n}_{i}\right)\right)=\Pi_{i \leq k} \mathbb{P}\left(R\left(\mathbf{n}_{i}\right)\right)$.

In this case we should expect:

$$
\mathbb{P}(\exists x R(x))=\sum_{n=2}^{\infty} \frac{1}{2^{n}}=\frac{1}{2} .
$$

Let us assume in what follows that we have a countably infinite set of constant symbols.

## Definition (Gaifman's Condition)

A probability $\mathbb{P}: \mathcal{S}_{\mathcal{L}} \rightarrow[0,1]$ satisfies the Gaifman condition if for all formulas with one free variable $\varphi(x)$ :

$$
\mathbb{P}(\exists x \varphi(x))=\sup \left\{\mathbb{P}\left(\bigvee_{i=1}^{n} \varphi\left(c_{i}\right)\right) \mid c_{1}, \ldots, c_{n} \in \mathcal{C}\right\}
$$

or equivalently,

$$
\mathbb{P}(\forall x \varphi(x))=\inf \left\{\mathbb{P}\left(\bigwedge_{i=1}^{n} \varphi\left(c_{i}\right)\right) \mid c_{1}, \ldots, c_{n} \in \mathcal{C}\right\}
$$

## Theorem (Gaifman 1964)

Given $\mathbb{P}^{\prime}: \mathcal{S}_{\mathcal{L}}^{0} \rightarrow[0,1]$, there is exactly one extension $\mathbb{P}$ of $\mathbb{P}^{\prime}$ to all of $\mathcal{S}_{\mathcal{L}}$ that satisfies the Gaifman condition.

## Theorem (Gaifman 1964)

Given $\mathbb{P}^{\prime}: \mathcal{S}_{\mathcal{L}}^{0} \rightarrow[0,1]$, there is exactly one extension $\mathbb{P}$ of $\mathbb{P}^{\prime}$ to all of $\mathcal{S}_{\mathcal{L}}$ that satisfies the Gaifman condition.

## Proof of Uniqueness.

Suppose we have $\mathbb{P}_{1}$ and $\mathbb{P}_{2}$ that agree on all of $\mathcal{S}_{\mathcal{L}}^{0}$. We show by induction on quantifier complexity that they agree on all $\varphi \in \mathcal{S}_{\mathcal{L}}$. Suppose the $\mathbb{P}_{i}$ 's agree all $\Pi_{n}$ sentences. Let $\varphi$ a $\Sigma_{n+1}$ sentence. We have $\varphi=\exists \vec{x} \psi(\vec{x})$ where $\psi(\vec{x})$ is $\Pi_{n}$. Now, since both satisfy the Gaifman condition, we have

$$
\mathbb{P}_{i}(\varphi)=\lim _{n \rightarrow \infty} \mathbb{P}_{i}\left(\bigvee_{k_{1}, \ldots, k_{m}<n} \psi\left(\mathbf{c}_{\mathbf{k}_{1}}, \ldots, \mathbf{c}_{\mathbf{k}_{\mathrm{m}}}\right)\right) .
$$

Each $\psi\left(\mathrm{c}_{\mathrm{k}_{1}}, \ldots, \mathrm{c}_{\mathrm{k}_{\mathrm{m}}}\right)$ is a $\Pi_{n}$ sentence. Since $\Pi_{n}$ sentences are closed under disjunctions, each such $V_{k_{1}, \ldots, k_{m}<n} \psi\left(\mathbf{c}_{k_{1}}, \ldots, \mathbf{c}_{k_{m}}\right)$ is also a $\Pi_{n}$ sentence, and by inductive hypothesis $\mathbb{P}_{1}$ and $\mathbb{P}_{2}$ must agree on it. This uniquely determines the limit above, and so the $\mathbb{P}_{i}$ 's must agree on $\varphi$. The same argument works for $\Pi_{n+1}$ sentences, using the closure of $\Sigma_{n}$ sentences under conjunctions.

## Theorem (Gaifman 1964)

Given $\mathbb{P}^{\prime}: \mathcal{S}_{\mathcal{L}}^{0} \rightarrow[0,1]$, there is exactly one extension $\mathbb{P}$ of $\mathbb{P}^{\prime}$ to all of $\mathcal{S}_{\mathcal{L}}$ that satisfies the Gaifman condition.

## Proof Sketch of Existence.

Consider the space $\operatorname{Mod}_{\omega}$ of all countable models with a fixed countable domain (take as domain set of constants $\mathcal{C}$ ). As in propositional case, let $\llbracket \varphi \rrbracket \triangleq\{\mathcal{M}=(\mathcal{C}, \mathcal{I}): \mathcal{M} \vDash \varphi\}$ for each $\varphi \in \mathcal{S}_{\mathcal{L}}^{0}$. This defines a Boolean algebra $\mathcal{B}_{0}$ (hence a ring) in the obvious way, and we can define a measure $\mu(\llbracket \varphi \rrbracket)=\mathbb{P}(\varphi)$, which can be canonically uniquely extended (by Carathéodory again) to a (countably additive) measure $\mu^{*}$ on the full $\sigma$-algebra $\sigma\left(\mathcal{B}_{0}\right)$ (NB. we use compactness!). Lastly, $\llbracket \exists x \varphi(x) \rrbracket=\bigcup_{c \in \mathcal{C}} \llbracket \varphi(c) \rrbracket$, so all sets of this form are in the $\sigma$-algebra. If we define $\mathbb{P}^{*}(\exists x \varphi(x)) \triangleq \mu^{*}(\llbracket \exists x \varphi(x) \rrbracket)$, then countable additivity guarantees the Gaifman condition.

## The space of models

We have built a measure $\mu$ on the space of countable models.
$\operatorname{Mod}_{\omega}$ is the space of countable structures $\{\mathfrak{M}$ an $\mathcal{L}$-model $\mid \operatorname{dom}(\mathfrak{M})=\omega\}$ with the topology generated by opens

$$
\llbracket \pm R(\bar{a}) \rrbracket:=\left\{\mathcal{M} \in \operatorname{Mod}_{\omega} \mid \mathcal{M} \vDash \pm R(\bar{a})\right\} \text { with } \bar{a} \in \omega^{<\omega}
$$

This is a Polish space: it is homeomorphic to the Cantor space $\left(2^{\omega}, \mathcal{O}\right)$ with $\mathcal{O}$ generated by cylinder sets.

The same is true in the propositional case. if we take the space $(\mathcal{V}, \mathcal{O})$ with $\mathcal{O}$ the topology generated by $\llbracket \Lambda_{i \leq n} \pm p_{i} \rrbracket=\left\{v \in \mathcal{V} \mid v \vDash \bigwedge_{i \leq n} \pm p_{i}\right\}$.

In both cases, we can treat probability functions on our language $\mathcal{L}$ as probability measures on the standard Borel space $\operatorname{Mod}_{\omega}$.

In this sense we can get all the standard Borel measures: and we already have this with measures on propositional languages with countably many atomic propositions.

## From Probabilities on Languages to Spaces

Given a probability measure $\mathbb{P}$ on $\mathcal{L}$, we can see it as

- A measure on the Lindenbaum-Tarski algebra $\mathcal{L} / \equiv$ (the algebra of equivalence classes of formulas modulo logical equivalence), where we let

$$
\mathbb{P}^{*}([\varphi]):=\mathbb{P}(\varphi)
$$

- The induced countably additive measure $\mu$ on the space of models (/valuations), which satisfies:

$$
\mu(\{v \in \mathcal{V} \mid v \models \varphi\})=\mathbb{P}(\varphi)
$$

One should be careful about treating these as the same thing!

## From Probabilities on Languages to Spaces

One important difference:

- Consider a probability measure $\mathbb{P}$ on an infinite (countable) propositional language. The measure $\mu$ induced by $\mathbb{P}$ on $\operatorname{Mod}(\mathcal{L})$ is countably additive.
- ...but he measure $\mathbb{P}^{*}$ on the Lindenbaum-Tarski algebra always fails to be countably additive [Amer, 1985] and even badly so [Seidenfeld].

Takeway:
We can translate between the logical and measure-theoretic perspective without losing anything essential. (There are however some subtle points to take into consideration, such as the issue of $\sigma$-additivity.)

Now: when can logic and probability genuinely illuminate one another?
From logic to probability and back: the case of random structures.

## Asymptotic probability of graph properties

What is a typical property of a graph?

- Let $G_{n}$ the set of all (labelled) graphs on $n$ vertices.
- For a well-defined graph property $F$, define

$$
p_{n}(F):=\frac{\mid\left\{G \in \mathbb{G}_{n} \mid G \text { has } F\right\} \mid}{\left|G_{n}\right|}
$$

- When does $\mathrm{P}(F)=\lim _{n \rightarrow \infty} p_{n}(F)$ exist? What proportion of finite graphs has property $P$ (asymptotically)?


## Asymptotic probability

Consider various properties for $F$ :

- $G$ has a complete subgraph of size $m: \lim _{n \rightarrow \infty} p_{n}(F)=1$.
- $G$ is planar: $\lim _{n \rightarrow \infty} p_{n}(F)=0$.
- $G$ has an odd number of vertices: no asymptotic probability.

Which properties have a limiting probability? Which ones are typical, in the sense of occurring almost surely?

Let $\varphi$ a FOL sentence. Define

$$
p_{n}(\varphi):=\frac{\left|\left\{G \in \mathbb{G}_{n} \mid G \vDash \varphi\right\}\right|}{\left|\mathbb{G}_{n}\right|}
$$

0-1 law. Let $\varphi$ a FOL sentence. Then $\lim _{n \rightarrow \infty} p_{n}(\varphi)$ always exists, and takes a value in $\{0,1\}$.

All first-order properties (1) have a limiting probability and (2) are either typical or atypical!

## Alice's Restaurant Property

You can get anything you want at Alice's Restaurant.

$$
\begin{aligned}
& \forall x_{1}, \ldots x_{k}, y_{1}, \ldots, y_{m} \\
& \left(\bigwedge_{i \leq k, j \leq m} x_{i} \neq y_{j} \rightarrow \exists z\left(\bigwedge_{i \leq k} z \neq x_{i} \wedge R\left(z, x_{i}\right) \wedge \bigwedge_{i \leq m} z \neq y_{i} \wedge \neg R\left(z, y_{i}\right)\right)\right)
\end{aligned}
$$

Given $X=\left\{x_{1}, \ldots x_{k}\right\}$ and $Y=\left\{y_{1}, \ldots, y_{m}\right\}$ we say $z$ as above is a witness for $X$ and $Y$ : we write $\mathrm{W}(z, X, Y)$.

There is a unique (up to isomorphism) countably infinite graph with the ARP.

Uniqueness: the AFP gives a winning strategy for Duplicator in $\mathrm{EF}_{\omega}$. Existence?

## Probabilistic construction

Take $\mathbb{N}$ as vertex set, and for each $(n, m) \in \mathbb{N}^{2}$ with $n \neq m$, toss a fair coin to decide if $R(n, m)$. This random process generates a countable random structure $(\mathbb{N}, R)$. Now:

The Random graph. The procedure above almost surely generates a graph satisfying the Alice's Restaurant Property.

So by drawing edges independently at random with probability $1 / 2$, we almost-surely generate the unique countable graph satisfying ARP. This is the Random/Rado graph $\mathfrak{R}$.

## Probabilistic construction

## Proof.

Fix $A=\left\{a_{1}, \ldots, a_{k}\right\}$ and $B=\left\{b_{1}, \ldots, b_{m}\right\}$ two disjoint sets of vertices. List all vertices $\left\langle v_{n}\right\rangle_{n \in \omega}$ not belonging to either set. For any such $v_{n}$, $\mathrm{P}(\mathrm{W}(A, B, v))=1 / 2^{k+m}$. The probability that no other vertex is a witness is

$$
\begin{aligned}
\mathrm{P}\left(\bigcap_{n} \neg \mathrm{~W}\left(v_{n}, A, B\right)\right) & =\lim _{n \rightarrow \infty} \mathrm{P}\left(\bigcap_{i \leq n} \neg \mathrm{~W}\left(v_{n}, A, B\right)\right) \\
& =\lim _{n \rightarrow \infty}\left(1-1 / 2^{k+m}\right)^{n}=0
\end{aligned}
$$

(edges are drawn independently). Now $\mathrm{P}(\neg A R P)$ is at most

$$
\mathrm{P}\left(\bigcup_{A, B \in S}\left(\bigcap_{n} \neg \mathrm{~W}\left(v_{n}, A, B\right)\right)\right)
$$

where $S$ ranges over disjoints pairs of finite sets of vertices. This is a countable union of probability 0 events, so it has probability 0 .

## Asymptotic probabilities and random structures

Now for the 0-1 law. Let $\alpha_{k, m}$ denote the sentence

$$
\forall x_{1}, \ldots x_{k}, y_{1}, \ldots, y_{m}\left(\bigwedge_{i \leq k, j \leq m} x_{i} \neq y_{j} \rightarrow \exists z \mathrm{~W}\left(z, x_{1}, \ldots x_{k}, y_{1}, \ldots, y_{m}\right)\right)
$$

Let $T_{R}:=\left\{\alpha_{n, m} \mid n, m<\omega\right\}$.
Thm (Glebskii et al. [1969], Fagin [1976]). Let $\varphi$ a first-order sentence.
The following are equivalent:

$$
\lim _{n \rightarrow \infty} p_{n}(\varphi)=1
$$

$\varphi$ holds on the random graph;

$$
T_{R} \vdash \varphi .
$$

A sentence $\varphi$ holds almost surely-in almost all finite graphs-if and only if it holds on the random graph.

$$
\operatorname{Cn}\left(T_{R}\right)=\operatorname{Th}(\mathfrak{R})=\left\{\varphi \in \operatorname{Sent} \mid \lim _{n \rightarrow \infty} p_{n}(\varphi)=1\right\}
$$

## The 0-1 law

Proof.
By our back-and-forth argument, $T_{R}$ is $\omega$-categorical, and has no finite models:
so it is complete. It has $\mathfrak{R}$ as a model, and so $T_{R} \vdash \varphi$ is equivalent to $\varphi$ holding on the random graph. Next, we show that $T_{R} \vdash \varphi$ entails $\lim _{n \rightarrow \infty} p_{n}(\varphi)=1 . T_{R} \vdash \varphi$ means that there is a finite set $\Gamma$ of extension axioms $\alpha_{k, m}$ such that $\Gamma \vdash \varphi$. It is enough to show that each $\alpha_{k, m}$ holds (asymptotically) almost surely.
As before, for a finite graph $G$ of size $n$ and two disjoint subsets $A, B \subseteq G$ of respective sizes $k$ and $m$, the probability that no $v \in G \backslash(A \cup B)$ is a witness is $\left(1-1 / 2^{k+m}\right)^{n-k-m}$.

## The 0-1 law

## Proof.

For sufficiently large $n, \alpha_{k, m}$ fails with probability at most

$$
\binom{n}{k}\binom{n-k}{m}\left(1-1 / 2^{k+m}\right)^{n-k-m}
$$

and indeed an cruder upper bound for $\lim _{n \rightarrow \infty} p_{n}\left(\neg \alpha_{k, m}\right)$ is

$$
\lim _{n \rightarrow \infty} n^{k+m}\left(1-1 / 2^{k+m}\right)^{n-k-m}=0
$$

Now the expression is of the form $n^{\alpha} \times \beta^{n-\alpha}$ with $\alpha, \beta$ constants and $0<\beta<1$ : the term $\beta^{n-\alpha}$ going to 0 exponentially, while $n^{\alpha}$ has only polynomial growth. So it goes to 0 , and so we conclude $\lim _{n \rightarrow \infty} p_{n}\left(\neg \alpha_{k, m}\right)=0$.

## The 0-1 law

## Proof.

Lastly, we show that $\lim _{n \rightarrow \infty} p_{n}(\varphi)=1$ entails $T_{R} \vdash \varphi$. Suppose $T_{R} \nvdash \varphi$. By completeness of $T$, we have $T_{R} \vdash \neg \varphi$. By the previous argument, this means that $\lim _{n \rightarrow \infty} p_{n}(\neg \varphi)=1$, and so $\varphi$ cannot hold in almost all finite graphs.

## Consequences

Thm Let $\varphi$ a first-order sentence. The following are equivalent

$$
\lim _{n \rightarrow \infty} p_{n}(\varphi)=1
$$

$\varphi$ holds on the random graph;

$$
T_{R} \vdash \varphi .
$$

Trakhtenbrot:
sure properties over finite structures are undecidable
The theory $T_{R}:=\left\{\alpha_{n, m} \mid n, m<\omega\right\}$ is $\omega$-categorical and so it is complete.
The axiomatisation is also recursive. Consequence:
almost sure properties over finite graphs are decidable! (in fact, PSPACE)

## Bonus: constructing the Rado graph

We built the random graph by randomly (i.i.d) deciding on each potential edge $(a, b) \in \mathbb{N}^{2}$. But the infinite random graph is easy to get.
The brute-force construction: starting from the empty graph, build an infinite increasing sequence of graphs $G_{0} \subseteq \ldots G_{n} \subseteq G_{n+1} \subseteq \ldots$ as follows:

$$
\text { Given } G_{n}=\left(V_{n}, E_{n}\right), \text { let } G_{n+1}=\left(V_{n+1}, E_{n+1}\right) \text { where }
$$

- $V_{n+1}:=V_{n} \cup\left\{v_{A} \mid A \subseteq V_{n}\right\}$,
- $E_{n+1} \cap V_{n}^{2}=E_{n}$,
- for all $A \subseteq V_{n}$, we let $E_{n+1}\left(v_{A}, x\right) \Leftrightarrow x \in A$

At each stage, for each subset of vertices, we add a vertex that has precisely this subset as neighbours.
By design, $G_{\omega}:=\bigcup_{n \in \mathbb{N}} G_{n}$ is an infinite countable graph satisfying ARP.

## Set-theoretic construction

Take $(M, \in)$, a countable model of ZFC.
For $a, b \in M$, define $R(a, b)$ if and only if $a \in b$ or $b \in a$.
Then $(M, R)$ is isomorphic to the Rado graph.
Why? Foundation! Let $a_{1}, \ldots a_{n}, b_{1}, \ldots, b_{m} \in M$ with the $a$ 's and $b$ 's pairwise distinct. Consider the set

$$
z:=\left\{a_{1}, \ldots, a_{n},\left\{b_{1}, \ldots, b_{m}\right\}\right\}
$$

Note that $R\left(z, b_{i}\right)$ would mean that there are $\in$-cycles in $M$. $(M, R)$ is thus a countable graph satisfying ARP, and so $(M, \in) \cong \mathfrak{R}$. (what if we take non well-founded set theory, e.g. ZFA?)

## Number-theoretic construction (Payley)

Let $V:=\{p \in \mathbb{P} \mid p \equiv 1(\bmod 4)\}$, and let $R(p, q)$ if and only if $\exists x \in$ $\{0, \ldots, q\}, p \equiv x^{2}(\bmod p)$. Then $(V, R) \cong \mathfrak{R}$.

Let $\left\{u_{1}, \ldots, u_{k}\right\}$ and $\left\{v_{1}, \ldots, v_{m}\right\}$ disjoint sets in $V$. Pick some $b_{i}$ 's st.
$\neg \exists x, x^{2} \equiv b_{i}\left(\bmod v_{i}\right)$.
By the Chinese Remainder Theorem, there is an $x \in \mathbb{N}$ such that

$$
\begin{aligned}
& x \equiv 1(\bmod 4) \\
& x \equiv 1\left(\bmod u_{i}\right) \text { for } i \leq k \\
& x \equiv b_{i}\left(\bmod v_{i}\right) \text { for } i \leq m
\end{aligned}
$$

and any number in the progression $\langle x+n d\rangle_{n}\left(d=4 u_{1} \ldots u_{k} v_{1} \ldots v_{n}\right)$ is also a solution to the above congruences. By Dirichlet's Theorem on arithmetic progressions, there exists a prime $p^{\prime}$ of this form, so that $p^{\prime}=x$ satisfies the above. Then $p^{\prime}$ is a witness for $\left\{u_{1}, \ldots, u_{k}\right\}$ and $\left\{v_{1}, \ldots, v_{m}\right\}$, as desired.

## Properties of the random graph

What is special about the random graph?

- Uniqueness (back-and-forth)
- Almost-sure theory
- Universality
- Symmetry (ultra-homogeneous)
- Its relation to the class of finite graphs: a kind of limit, encoding probabilistic information.

This construction (and the 0-1 law) generalises to finite relational signatures: we can carry over the same general model-theoretic construction for the class of all finite models (via Fraïssé limits)

## Perspectives on typicality

Random structures offer fertile ground for exploring different notions of typicality:

- Asymptotic over finite structures
- Measure theoretic
- Probability space $\left(\operatorname{Mod}_{\omega}, \mathcal{F}, \mu\right)$ with $\mathcal{F}$ the Borel algebra of the underlying topology. The Lebesgue measure concentrates on the isomorphism class of the random graph (assigns it measure one). [Symmetric probabilistic constructions: $\mu$ a $S_{\infty}$-invariant measure, i.e for every Borel set $A$ and permutation $g \in S_{\infty}, \mu(A)=\mu(g A)$ ].
- Topological:
- Seeing $\operatorname{Mod}_{\omega}$ as a topological space, the isomorphism class of the random graph forms a co-meagre set (topologically large).

But these notions of typicality need not always agree with one another. How to they relate? By virtue of which property of a theory or class of structures?

## Conclusion

Random structures lie at the cusp of probability and logic, bridging together model theory and combinatorics. They can be put to use to:

- establish asymptotic 0-1 laws for logics over classes of finite structures
- display infinitary structures 'approximating' finite ones
- investigate the connection between symmetries of a structure and probabilistic models
- explore the relationship between topological and measure-theoretic notions of typicality.


## Tomorrow:

Probabilistic grammars and probabilistic programs

