Zero-One Laws in Discrete Mathematics

Yuri Gurevich

Microsoft Research

Blass Fest, Fields Institute, November 2007

To Andreas, the true mathematician

To Andreas, the true mathematician

Story 1. Irritated math. celebrity

To Andreas, the true mathematician

Story 1. Irritated math. celebrity
Q (insists again and again): Why do you say that?

To Andreas, the true mathematician

Story 1. Irritated math. celebrity
Q (insists again and again): Why do you say that?
A (eventualy): To impress my friends and to get the girl.

To Andreas, the true mathematician

Story 1. Irritated math. celebrity
Q (insists again and again): Why do you say that?
A (eventualy): To impress my friends and to get the girl.

Story 2. Calm Blass

To Andreas, the true mathematician

Story 1. Irritated math. celebrity
Q (insists again and again): Why do you say that?
A (eventualy): To impress my friends and to get the girl.

Story 2. Calm Blass
Q: Why do you do set theory? Isn't it a closed world these days? Are there meaningful — to the mainstream math — results proved after 1960?

To Andreas, the true mathematician

Story 1. Irritated math. celebrity
Q (insists again and again): Why do you say that?
A (eventualy): To impress my friends and to get the girl.

Story 2. Calm Blass
Q: Why do you do set theory? Isn't it a closed world these days? Are there meaningful — to the mainstream math — results proved after 1960?
A: But it is fun!

Toronto blues

1978-79 academic year. My talk on the topology of real line,

Toronto blues

1978-79 academic year. My talk on the topology of real line, and Alan Meckler.

The most famous zero-one law

Consider independent random variables $X_1, X_2, \ldots$

The most famous zero-one law

Consider independent random variables $X_1, X_2, \ldots$

A *tail event* is independent of any finite subsequence of the variables.

The most famous zero-one law

Consider independent random variables $X_1, X_2, \ldots$

A *tail event* is independent of any finite subsequence of the variables.

Examples

- The sequence converges.
- $1/2$ occurs infinitely many times.

The most famous zero-one law

Consider independent random variables $X_1, X_2, \ldots$

A *tail event* is independent of any finite subsequence of the variables.

Examples

- The sequence converges.
- $1/2$ occurs infinitely many times.

Theorem (Kolmogorov)

Probability of any tail event is either 0 or 1.

A little math logic may be useful

Wikipedia: "In many situations, it can be easy to apply Kolmogorov's zero-one law to show that some event has probability 0 or 1, but surprisingly hard to determine which of these . . . values is the correct one."

A little math logic may be useful

Wikipedia: "In many situations, it can be easy to apply Kolmogorov's zero-one law to show that some event has probability 0 or 1, but surprisingly hard to determine which of these . . . values is the correct one."

Actually this is not that surprising.

A little math logic may be useful

Wikipedia: "In many situations, it can be easy to apply Kolmogorov's zero-one law to show that some event has probability 0 or 1, but surprisingly hard to determine which of these . . . values is the correct one."

Actually this is not that surprising.

Consider independent random variables X_i with only, two equally probable values, 0 and 1.

A little math logic may be useful

Wikipedia: "In many situations, it can be easy to apply Kolmogorov's zero-one law to show that some event has probability 0 or 1, but surprisingly hard to determine which of these . . . values is the correct one."

Actually this is not that surprising.

Consider independent random variables X_i with only, two equally probable values, 0 and 1.

For each polynomial $p(x_1, .., x_4)$, consider this event: the binary notations for an integer tuple $\langle k_1, \ldots, k_4 \rangle$ with $p(k_1, \ldots, , k_4) = 0$ appears infinitely often as a contiguous subsequence.

Finiteness

Proviso

By default, structures are finite.

The isomorphism problem

The isomorphism problem

Given two graphs, decide whether they are isomorphic.

The isomorphism problem

Given two graphs, decide whether they are isomorphic.

It is a known hard problem,

The isomorphism problem

Given two graphs, decide whether they are isomorphic.

It is a known hard problem,
not NP hard but neither is factoring —

The isomorphism problem

Given two graphs, decide whether they are isomorphic.

It is a known hard problem,
not NP hard but neither is factoring —
that is routinely solved in practice,

The isomorphism problem

Given two graphs, decide whether they are isomorphic.

It is a known hard problem,
not NP hard but neither is factoring —
that is routinely solved in practice,

e.g. in comparing the runtime heaps created by an object oriented program.

Graph coloring algorithm

- $C_1(v)$ is the degree of v,

Graph coloring algorithm

- $C_1(v)$ is the degree of v,
- $C_{s+1}(v)$ is given by $C_s(v)$ and $\mathrm{Bag}(C_s(w) : vEw)$.

Graph coloring algorithm

- $C_1(v)$ is the degree of v,
- $C_{s+1}(v)$ is given by $C_s(v)$ and $\mathrm{Bag}(C_s(w) : vEw)$.
- Halt when the color-refinement process reaches a fixed point. Success = the final parts are all singletons.

Graph coloring algorithm

- $C_1(v)$ is the degree of v,
- $C_{s+1}(v)$ is given by $C_s(v)$ and $\mathrm{Bag}(C_s(w) : vEw)$.
- Halt when the color-refinement process reaches a fixed point. Success = the final parts are all singletons.

Graph coloring algorithm

- $C_1(v)$ is the degree of v,
- $C_{s+1}(v)$ is given by $C_s(v)$ and $\mathrm{Bag}(C_s(w) : vEw)$.
- Halt when the color-refinement process reaches a fixed point. Success = the final parts are all singletons.

Use the colors to establish *the* isomorphism.

Graph coloring algorithm

- $C_1(v)$ is the degree of v,
- $C_{s+1}(v)$ is given by $C_s(v)$ and $\mathrm{Bag}(C_s(w) : vEw)$.
- Halt when the color-refinement process reaches a fixed point. Success = the final parts are all singletons.

Use the colors to establish *the* isomorphism.

Generalize to relational structures of any fixed vocabulary.

Rigidity

A graph is *rigid* if it has only the trivial automorphism, the identity.

Rigidity

A graph is *rigid* if it has only the trivial automorphism, the identity.

The coloring algorithms gives a practical solution for the graph rigidity problem.

Uniform distribution

- Labeled version (the default).
  All graphs on $\{1, \ldots, n\}$ are equally probable; or toss a fair coin for every pair $\{i, j\}$ of distinct vertices.
- Unlabeled version.
  All isomorphism classes of n-vertex graphs are equally probable.

Almost sure properties

Definition

Let π be a graph property and p_n be the fraction of π graphs among all graphs on $\{1, \ldots, n\}$. If p_n approaches 1 when n grows to infinity, then π is almost sure.

Fact: The coloring algorithm almost surely succeeds. Hence graphs are a.s. rigid.

Almost sure properties

Definition

Let π be a graph property and p_n be the fraction of π graphs among all graphs on $\{1, \ldots, n\}$. If p_n approaches 1 when n grows to infinity, then π is almost sure.

Fact: The coloring algorithm almost surely succeeds. Hence graphs are a.s. rigid.

The fact survives in the unlabeled case.

Arbitrary structures

Consider arbitrary (but finite) purely relational structures of a fixed signature.

Arbitrary structures

Consider arbitrary (but finite) purely relational structures of a fixed signature.

Fact: Structures are a.s. rigid.

Arbitrary structures

Consider arbitrary (but finite) purely relational structures of a fixed signature.

Fact: Structures are a.s. rigid.

Curiosity: Graphs do not constitute a special case.

Thesauri

A *thesaurus* is a set of signa.

Thesauri

A *thesaurus* is a set of signa.

A signum R of arity j is a generalization of a relation symbol of arity j.
It also has:

- a value set V,
- a group G of permutations over $\{1, \ldots, j\}$,
- a homomorphism h from G to the permutation group of V.

Structures of a given thesaurus

The interpretation of a signum (R, j, V, G, h) assigns to each j-tuple $(a_1, \ldots, a_j)$ of distinct elements a value in V subject to a symmetry requirement

$$R(a_1, \ldots, a_j) = h(\pi)R(a_{\pi 1}, \ldots, a_{\pi j}) \quad \text{for every } \pi \in G.$$

Example: graphs

$V = \{\text{true}, \text{false}\}$.
G consists of all (two) permutations.
Every $h(\pi)$ is the identity.

Example: graphs

$V = \{\text{true}, \text{false}\}$.
G consists of all (two) permutations.
Every $h(\pi)$ is the identity.

If π is the swap, we have

$$E(a_1, a_2) = h(\pi)E(a_2, a_1) = E(a_2, a_1).$$

Example: tournaments

$V = \{\text{true}, \text{false}\}$.
G consists of all (two) permutations.
h of the swap is the negation.

Example: tournaments

$V = \{\text{true}, \text{false}\}$.
G consists of all (two) permutations.
h of the swap is the negation.

If π is the swap, we have

$$E(a_1, a_2) = h(\pi)E(a_2, a_1) = \neg E(a_2, a_1).$$

Example: tournaments

$V = \{\text{true}, \text{false}\}$.
G consists of all (two) permutations.
h of the swap is the negation.

If π is the swap, we have

$$E(a_1, a_2) = h(\pi)E(a_2, a_1) = \neg E(a_2, a_1).$$

Consider the generalization to tournaments with ties.

Two special cases

1. Structures of a fixed purely relational vocabulary.
2. Graphs.

To simplify the exposition, we speak about graphs.

Random infinite graphs

Toss a fair coin for every pair $i < j$ of natural numbers; if it turns up heads then put an edge between i and j.
What is the probability that two outcomes are isomorphic?

Random infinite graphs

Toss a fair coin for every pair $i < j$ of natural numbers; if it turns up heads then put an edge between i and j.
What is the probability that two outcomes are isomorphic?

The answer is 1,

Random infinite graphs

Toss a fair coin for every pair $i < j$ of natural numbers; if it turns up heads then put an edge between i and j.
What is the probability that two outcomes are isomorphic?

The answer is 1,
by the back and forth argument.

Random infinite graphs

Toss a fair coin for every pair $i < j$ of natural numbers; if it turns up heads then put an edge between i and j.
What is the probability that two outcomes are isomorphic?

The answer is 1,
by the back and forth argument.

By the same argument, the infinite random graph has continuum many automorphisms.

Extension axioms

E_k for all disjoint k-element sets X, Y,
there is an element z
adjacent to all vertices in X and no vertex in Y.

Extension axioms

E_k for all disjoint k-element sets X, Y,
there is an element z
adjacent to all vertices in X and no vertex in Y.

Every E_k is almost surely true.

Almost sure theory

Let T be the theory given by all extension axioms E_k.

Almost sure theory

Let T be the theory given by all extension axioms E_k.

T has no finite models.

Almost sure theory

Let T be the theory given by all extension axioms E_k.

T has no finite models.

Any two countable models of T are isomorphic.

Almost sure theory

Let T be the theory given by all extension axioms E_k.

T has no finite models.

Any two countable models of T are isomorphic.

T is complete and decdiable.

Zero-one law: graphs

Theorem (Transfer)

φ is a.s. true iff it holds at the random graph.

Theorem

Every first-order sentence φ in the language of graphs is a.s. true or a.s. false. The almost sure theory is decidable.

Zero-one law: graphs

Theorem (Transfer)

φ is a.s. true iff it holds at the random graph.

Theorem

Every first-order sentence φ in the language of graphs is a.s. true or a.s. false. The almost sure theory is decidable.

Proof. Use the completeness and the fact that the axioms are almost sure.

Zero-one law for relational structures

Theorem (Glebsky et al. 1969; Fagin 1976)

Every first-order sentence φ is a.s. true or a.s. false. The almost sure theory is decidable.

Lemma (Transfer lemma)

A first-order sentence φ is a.s. true if and only if it holds at the random structure.

Theorem (Grandjean 1983)

The almost sure theory is pspace complete.

Zero-one law for thesaurus structures

Oberschelp, *Generalizations to graphs and other "parametric conditions"*, 1982.
Blass and Gurevich, *Zero-one laws: thesauri and parametric conditions*, 2007

Richer logics

Zero-one laws "unexplained"
Blass and Harrary

Richer logics

Zero-one laws "unexplained"
Blass and Harrary

First-order logic with fixed-points
Blass, Gurevich, Kozen; Talanov

Richer logics

Zero-one laws "unexplained"
Blass and Harrary

First-order logic with fixed-points
Blass, Gurevich, Kozen; Talanov

The infinitary logic
Kolaitis and Vardi

Some other generalizations

Special theories
e.g. partial orders (Kolaitis)

Some other generalizations

Special theories
e.g. partial orders (Kolaitis)

Model theory (Compton)

Some other generalizations

Special theories
e.g. partial orders (Kolaitis)

Model theory (Compton)

Playing with probabilities
Notably, Shelah and Spencer

Geometric zero-one law

This is a joint work with Bob Gilman of Stevens and with Alexei Miasnikov of McGill.

Geometric zero-one law

This is a joint work with Bob Gilman of Stevens and with Alexei Miasnikov of McGill.

Forget thesauri; we are going back to relational structures even though the generalization to thesauri may be straightforward.

The Gaifman graph

For every relational structure X, we define the *graph* of X.

The Gaifman graph

For every relational structure X, we define the *graph* of X.

Vertices are the elements of X.

The Gaifman graph

For every relational structure X, we define the *graph* of X.

Vertices are the elements of X.

A pair $\{x, y\}$ is an edge if $x \neq y$ and there is a true atomic relationship $R(a_1, \ldots, a_j)$ whose arguments contain both x and y.

The Gaifman graph

For every relational structure X, we define the *graph* of X.

Vertices are the elements of X.

A pair $\{x, y\}$ is an edge if $x \neq y$ and there is a true atomic relationship $R(a_1, \ldots, a_j)$ whose arguments contain both x and y.

The graph allows us to speak about distances, balls, etc.

A structure of interest

Fix an infinite relational structure X such that every the degree (in the sense of Graph(X)) of X is finite. Then every ball $B_n(x)$ is finite.

A good example for our purposes is the Cayley graph of a finitely generated infinite group.

We are interested in finite substructures of X.
What does or should mean that a property π is a.s. true for finite substructures of X?

Almost sure

A property π is a.s. true on finite substructures of X if, for every $x \in X$, the fraction of π-substructures of the ball $B_n(x)$ approaches 1 as n grows to infinity.

Geometric zero-one law: version 1

Theorem G1. Suppose that the infinite structure X is

- connected,
- of bounded degree,
- with the duplicate substructure property.

Then any first-order sentence φ in the language of X is either a.s. true or a.s. false on finite substructures of X

Pseudo-connectivity

A class C of finite structures is *pseudo-connected* if every $Y \in C$ can be embedded into a connected member of C.

Geometric zero-one law: version 2

Theorem G2. Let C be a pseudo-connected class of finite structures of bounded degree that closed under substructures and disjoint unions.

Geometric zero-one law: version 2

Theorem G2. Let C be a pseudo-connected class of finite structures of bounded degree that closed under substructures and disjoint unions.

Ambient structure. There is an infinite structure X, an *ambient structure* for C such that X satisfies the conditions of Theorem G1 and C is the collection of (isomorphic copies) of substructures of X.

Geometric zero-one law: version 2

Theorem G2. Let C be a pseudo-connected class of finite structures of bounded degree that closed under substructures and disjoint unions.

Ambient structure. There is an infinite structure X, an *ambient structure* for C such that X satisfies the conditions of Theorem G1 and C is the collection of (isomorphic copies) of substructures of X.

Transfer. Let S be the disjoint union of the members of C. A first-order sentence φ is a.s. true for C if and only if it holds in S.

Examples

The Cayley diagram of a finitely generated infinite group.

Examples

The Cayley diagram of a finitely generated infinite group.

An infinite connected vertex-transitive graph of finite degree. For example the graph obtained from a Cayley diagram of the type just mentioned by removing all loops and combining all edges between any two distinct vertices joined by an edge into a single undirected edge.

Examples

The Cayley diagram of a finitely generated infinite group.

An infinite connected vertex-transitive graph of finite degree. For example the graph obtained from a Cayley diagram of the type just mentioned by removing all loops and combining all edges between any two distinct vertices joined by an edge into a single undirected edge.

The Cayley diagram of a free finitely generated monoid.

Examples

The Cayley diagram of a finitely generated infinite group.

An infinite connected vertex-transitive graph of finite degree. For example the graph obtained from a Cayley diagram of the type just mentioned by removing all loops and combining all edges between any two distinct vertices joined by an edge into a single undirected edge.

The Cayley diagram of a free finitely generated monoid.

The full binary tree; i.e., the tree with one vertex of degree two and all others of degree three. More generally the full k-ary tree for $k \geq 1$.

Axioms

Call a finite graph G *positive* if it isomorphic to a member of C; otherwise call it *negative*.

Axioms

Call a finite graph G *positive* if it isomorphic to a member of C; otherwise call it *negative*.

Here is an axiom system for the a.s. theory of C. There is one axiom for every (up to isomorphism) finite graph G.

Positive G There is a component isomorphic to G.

Negative G There are is no subgraph isomorphic to G.

Is the geometric law different?

Theorem G3. There is a class C of finite structures that obeys the geometric 0-1 law but does not obey the classical labeled or unlabeled law.