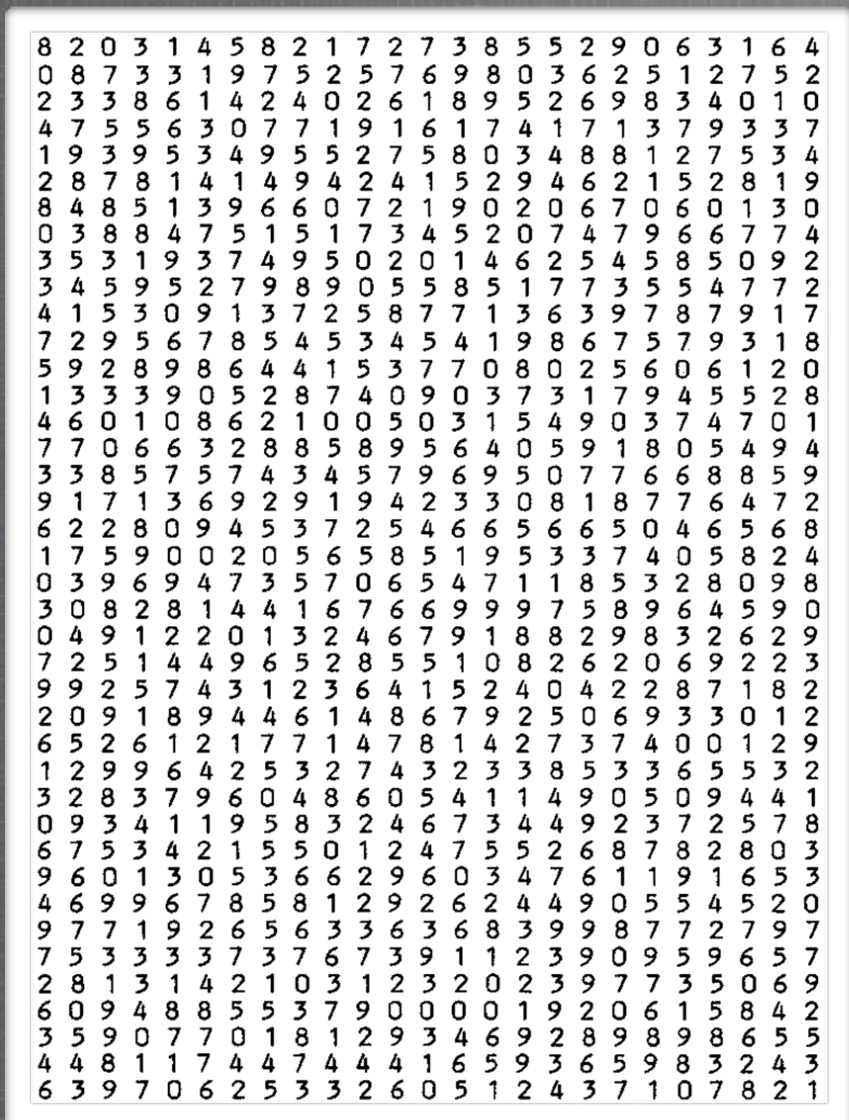


8	2	0	3	1	4	5	8	2	1	7	2	7	3	8	5	5	2	9	0	6	3	1	6	4
0	8	7	3	3	1	9	7	5	2	5	7	6	9	8	0	3	6	2	5	1	2	7	5	2
2	3	3	8	6	1	4	2	4	0	2	6	1	8	9	5	2	6	9	8	3	4	0	1	0
4	7	5	5	6	3	0	7	7	1	9	1	6	1	7	4	1	7	1	3	7	9	3	3	7
1	9	3	9	5	3	4	9	5	5	2	7	5	8	0	3	4	8	8	1	2	7	5	3	4
2	8	7	8	1	4	1	4	9	4	2	4	1	5	2	9	4	6	2	1	5	2	8	1	9
8	4	8	5	1	3	9	6	6	0	7	2	1	9	0	2	0	6	7	0	6	0	1	3	0
0	3	8	8	4	7	5	1	5	1	7	3	4	5	2	0	7	4	7	9	6	6	7	7	4
3	5	3	1	9	3	7	4	9	5	0	2	0	1	4	6	2	5	4	5	8	5	0	9	2
3	4	5	9	5	2	7	9	8	9	0	5	5	8	5	1	7	7	3	5	5	4	7	7	2
4	1	5	3	0	9	1	3	7	2	5	8	7	7	1	3	6	3	9	7	8	7	9	1	7
7	2	9	5	6	7	8	5	4	5	3	4	5	4	1	9	8	6	7	5	7	9	3	1	8
5	9	2	8	9	8	6	4	4	1	5	3	7	7	0	8	0	2	5	6	0	6	1	2	0
1	3	3	3	9	0	5	2	8	7	4	0	9	0	3	7	3	1	7	9	4	5	5	2	8
4	6	0	1	0	8	6	2	1	0	0	5	0	3	1	5	4	9	0	3	7	4	7	0	1
7	7	0	6	6	3	2	8	8	5	8	9	5	6	4	0	5	9	1	8	0	5	4	9	4
3	3	8	5	7	5	7	4	3	4	5	7	9	6	9	5	0	7	7	6	6	8	8	5	9
9	1	7	1	3	6	9	2	9	1	9	4	2	3	3	0	8	1	8	7	7	6	4	7	2
6	2	2	8	0	9	4	5	3	7	2	5	4	6	6	5	6	6	5	0	4	6	5	6	8
1	7	5	9	0	0	2	0	5	6	5	8	5	1	9	5	3	3	7	4	0	5	8	2	4
0	3	9	6	9	4	7	3	5	7	0	6	5	4	7	1	1	8	5	3	2	8	0	9	8
3	0	8	2	8	1	4	4	1	6	7	6	6	9	9	9	7	5	8	9	6	4	5	9	0
0	4	9	1	2	2	0	1	3	2	4	6	7	9	1	8	8	2	9	8	3	2	6	2	9
7	2	5	1	4	4	9	6	5	2	8	5	5	1	0	8	2	6	2	0	6	9	2	2	3
9	9	2	5	7	4	3	1	2	3	6	4	1	5	2	4	0	4	2	2	8	7	1	8	2
2	0	9	1	8	9	4	4	6	1	4	8	6	7	9	2	5	0	6	9	3	3	0	1	2
6	5	2	6	1	2	1	7	7	1	4	7	8	1	4	2	7	3	7	4	0	0	1	2	9
1	2	9	9	6	4	2	5	3	2	7	4	3	2	3	3	8	5	3	3	6	5	5	3	2
3	2	8	3	7	9	6	0	4	8	6	0	5	4	1	1	4	9	0	5	0	9	4	4	1
0	9	3	4	1	1	9	5	8	3	2	4	6	7	3	4	4	9	2	3	7	2	5	7	8
6	7	5	3	4	2	1	5	5	0	1	2	4	7	5	5	2	6	8	7	8	2	8	0	3
9	6	0	1	3	0	5	3	6	6	2	9	6	0	3	4	7	6	1	1	9	1	6	5	3
4	6	9	9	6	7	8	5	8	1	2	9	2	6	2	4	4	9	0	5	5	4	5	2	0
9	7	7	1	9	2	6	5	6	3	3	6	3	6	8	3	9	9	8	7	7	2	7	9	7
7	5	3	3	3	3	7	3	7	6	7	3	9	1	1	2	3	9	0	9	5	9	6	5	7
2	8	1	3	1	4	2	1	0	3	1	2	3	2	0	2	3	9	7	7	3	5	0	6	9
6	0	9	4	8	8	5	5	3	7	9	0	0	0	0	1	9	2	0	6	1	5	8	4	2
3	5	9	0	7	7	0	1	8	1	2	9	3	4	6	9	2	8	9	8	9	8	6	5	5
4	4	8	1	1	7	4	4	7	4	4	4	1	6	5	9	3	6	5	9	8	3	2	4	3
6	3	9	7	0	6	2	5	3	3	2	6	0	5	1	2	4	3	7	1	0	7	8	2	1

DEFINING RANDOMNESS

Christopher P. Porter
Université Paris 7

28 November 2013

A MOTIVATING QUESTION

What does it mean for a sequence of 0s and 1s to be random?

There are a number of ways to answer this question.

For instance, we might hold that a sequence is random if it is obtained by tossing an fair coin (where H = 0 and T = 1).

Alternatively, we might hold that a sequence is random if it *looks as if* it were obtained by tossing a fair coin.

AN EXTENDED EXAMPLE

For the moment, let's restrict our attention to sequences of length fifty.

Consider the following sequence S:

00000 00000 00000 00000 00000 00000 00000 00000 00000 00000

It is certainly *possible* to produce S by tossing a fair coin, and thus it would be counted as random in the first sense.

AN EXTENDED EXAMPLE, 2

However, S isn't the sort of sequence we'd expect to produce by tossing a fair coin fifty times.

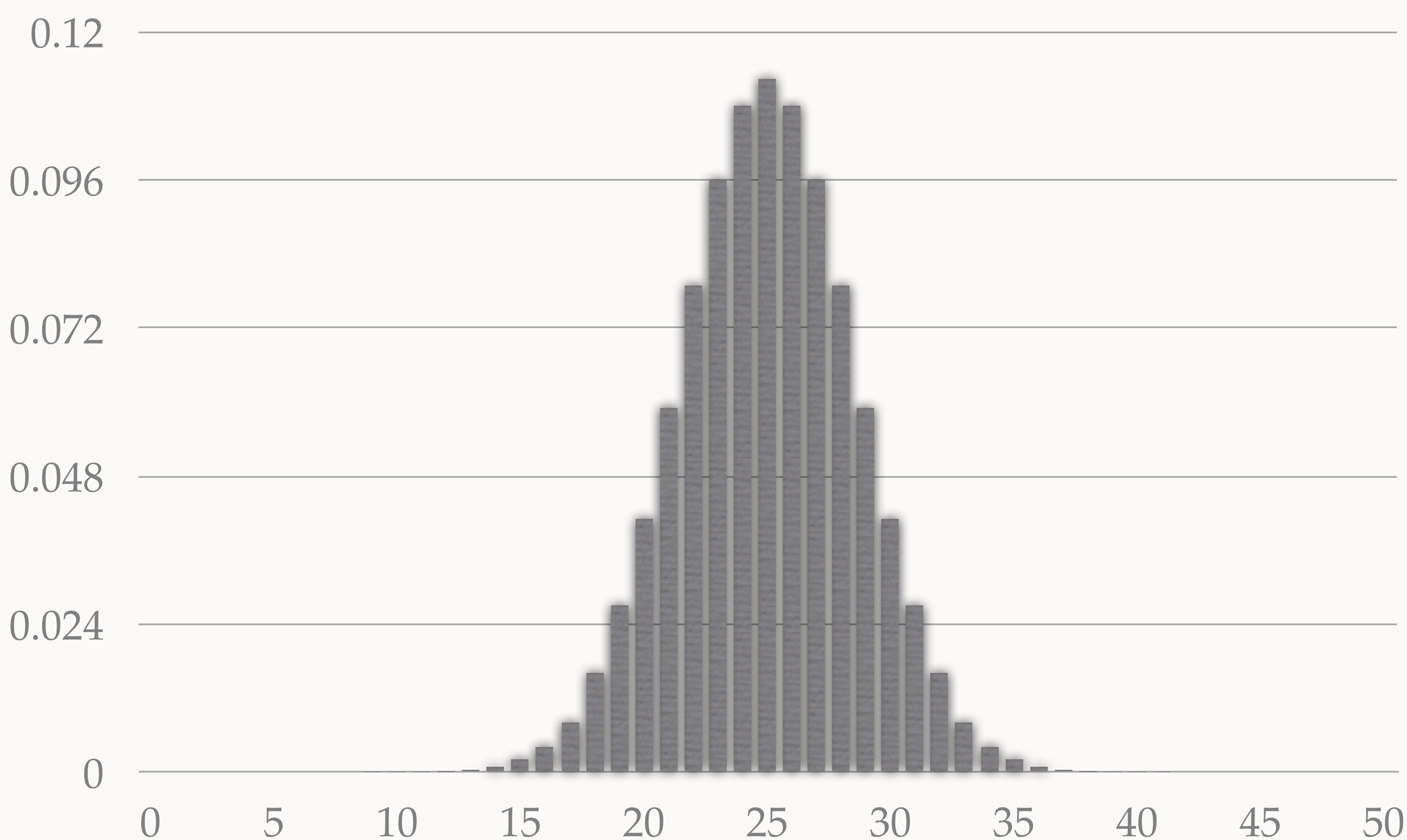
Since S doesn't look as it were produced by the tosses of a fair coin, we probably wouldn't count it as random in the second sense.

But what exactly is wrong with S?

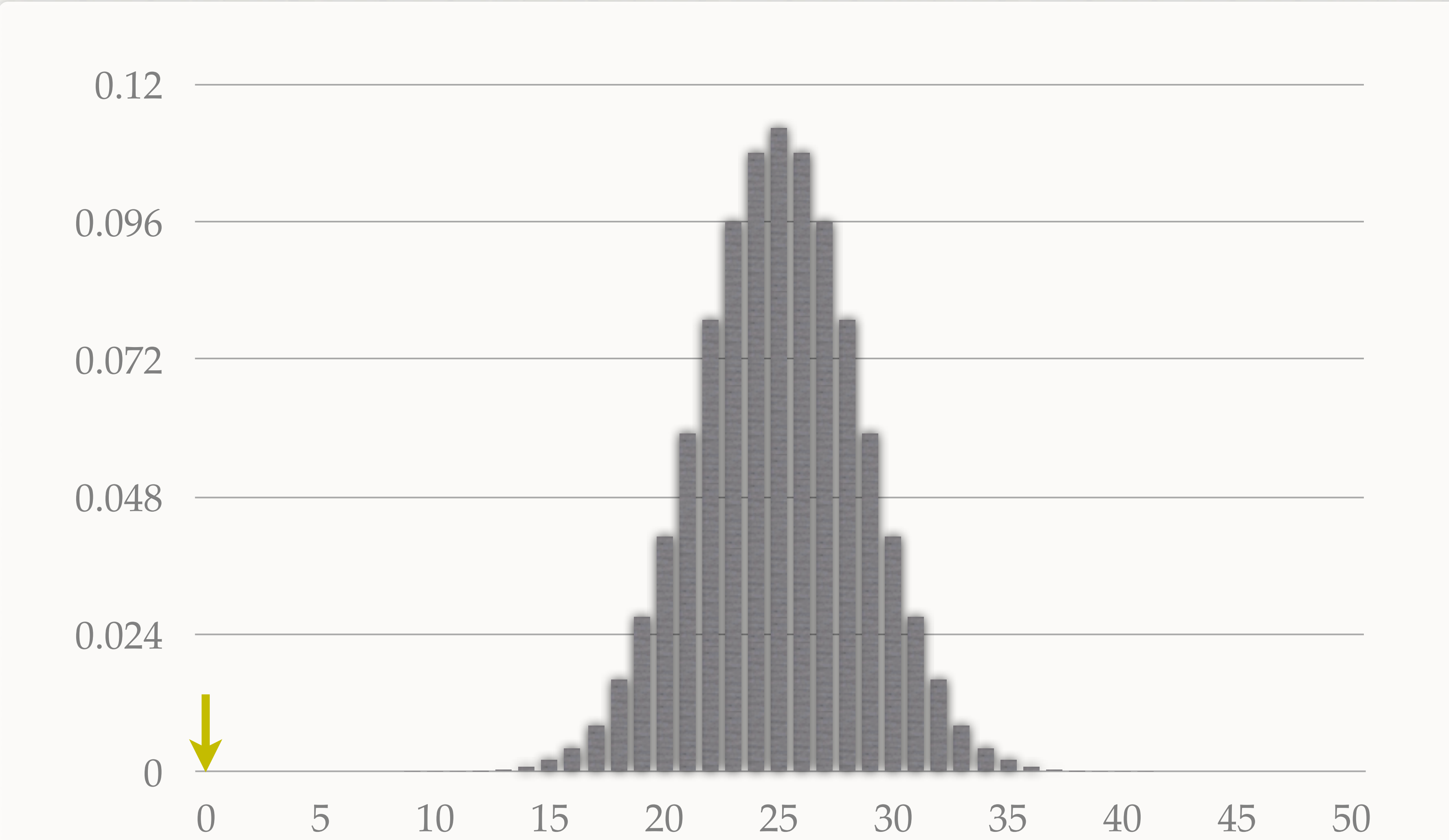
AN EXTENDED EXAMPLE, 3

In the first place, we expect that in tossing a fair coin fifty times, H comes up at least once.

AT LEAST ONE *H*



AT LEAST ONE *H*

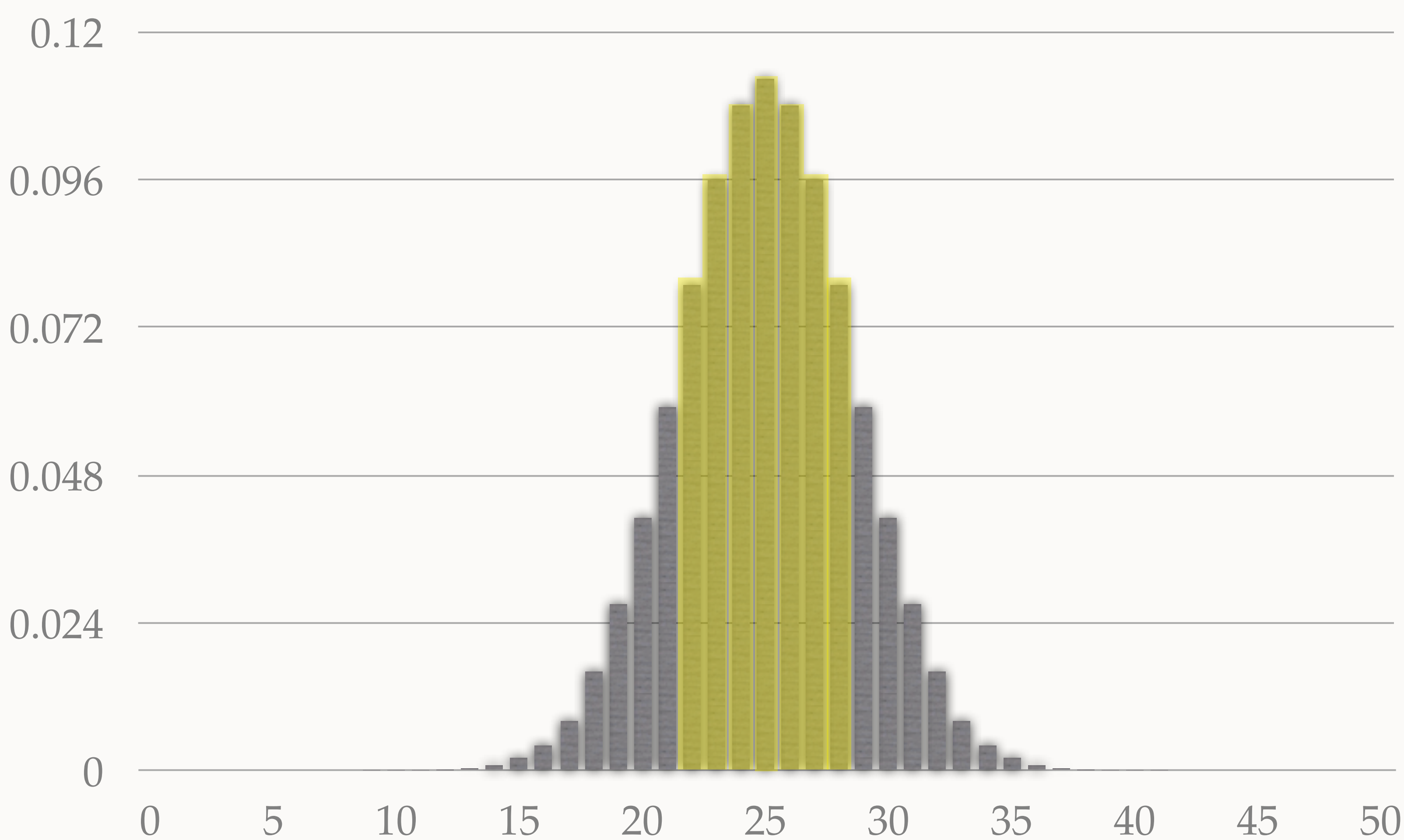


AN EXTENDED EXAMPLE, 3

In the first place, we expect that in tossing a fair coin fifty times, H comes up at least once.

In fact, about 66% of the time, H should appear between 22 and 28 times.

BETWEEN 22 AND 28 *H*'S



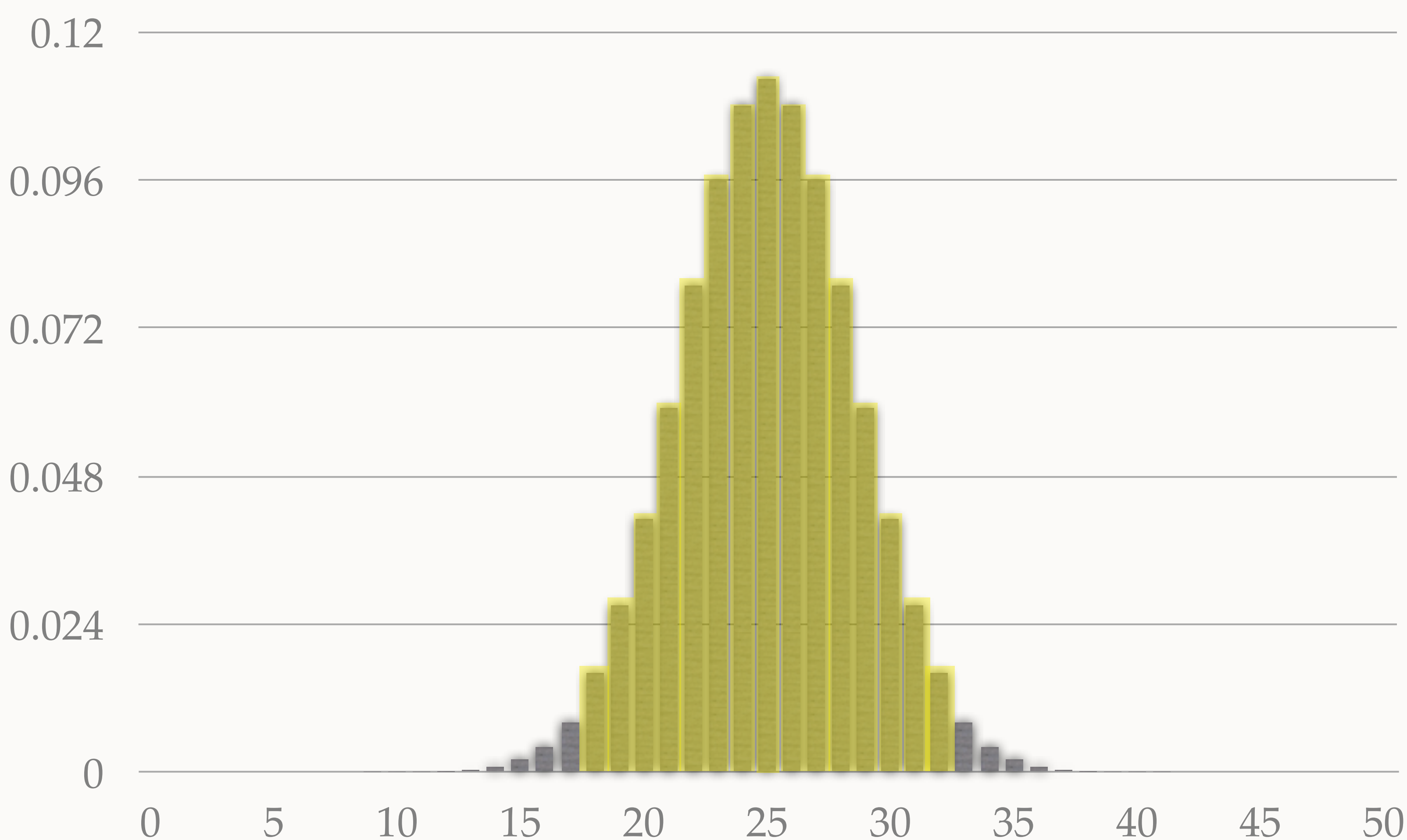
AN EXTENDED EXAMPLE, 3

In the first place, we expect that in tossing a fair coin fifty times, H comes up at least once.

In fact, about 66% of the time, H should appear between 22 and 28 times.

In fact, over 95% of the time, H should appear between 18 and 32 times.

BETWEEN 18 AND 32 *H*'S



AN EXTENDED EXAMPLE, 3

In the first place, we expect that in tossing a fair coin fifty times, H comes up at least once.

In fact, about 66% of the time, H should appear between 22 and 28 times.

In fact, over 95% of the time, H should appear between 18 and 32 times.

S should thus disqualified from being counted as random on statistical grounds.

“ROUGH” DEFINITION 1

The statistical definition of randomness

A sequence of 0s and 1s of length N is random if and only if it satisfies all statistical properties that “most” strings of length N satisfy.

A FEW WORRIES

1. This definition is hopelessly vague.

2. How can this definition be extended to define random infinite sequences?

- For every infinite sequence X, the property “not being equal to X” occurs with probability one, so most sequences satisfy this property.

- Unless we’re more careful, we will have an empty definition of randomness for infinite sequences.

AN ALTERNATIVE APPROACH

Alternatively, we might reason as follows:

- Most sequences produced by the tosses of a fair coin don't have any easily recognizable patterns.
- Moreover, due to this lack of patterns, most sequences are in a certain sense difficult to describe.
- But the sequence S is easy to describe: repeat 0 fifty times.
- Thus S should not be counted as random.

DESCRIPTIONS?

We need to be careful about what counts as an admissible description in this context:

- "the sequence of 50 0's" should count as admissible;
- "Walt's favorite string" should not.

Here I have a very specific kind of description in mind: I mean descriptions of a sequence that allows me to reconstruct the sequence from the description.

EASY TO DESCRIBE?

Once we've specified what counts as the admissible descriptions, we still need to define what is means for sequence to be "easy to describe."

Note that "the sequence of 50 0's" contains 22 symbols.

From a description of length 22, we can reconstruct a sequence of 50 symbols.

But here's another description of S:

"The first bit is a 0 and the second bit is a 0 and..."

This description has length much greater than 50, but it is a very redundant description.

“ROUGH” DEFINITION 2

The incompressibility definition of randomness

A sequence of 0s and 1s of length N is random if and only if its shortest admissible description has length at least N.

A FEW MORE WORRIES

1. Like the first definition of randomness, this definition as formulated is also quite unclear.

2. It is also not clear how this definition can be extended to define random infinite sequences.

- How does one describe an infinite sequence?
- There are uncountably many sequences of the form 00 11 11 00 00 11 00 11 11 00 ...
- These shouldn't be counted as random, but how do we describe each of these sequences?

THE PLAN

Step 1: Make precise the incompressibility definition of randomness.

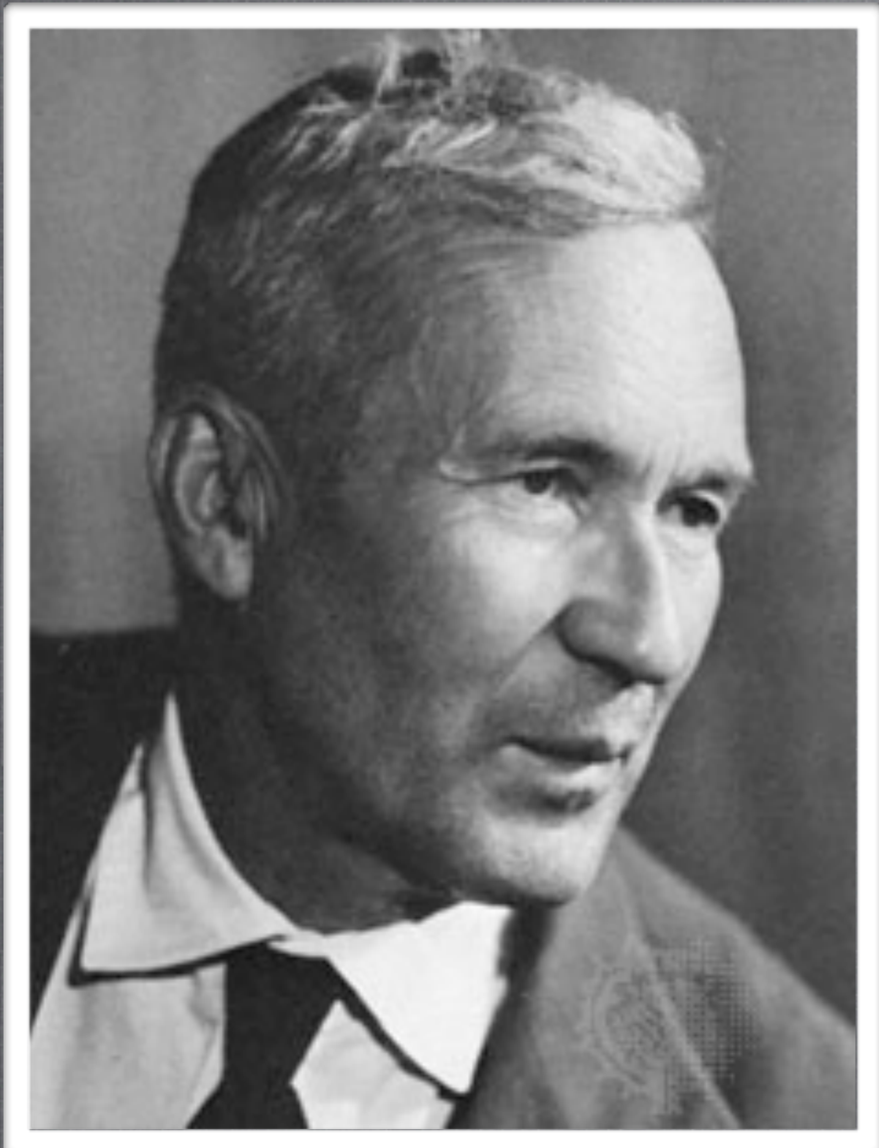
- Kolmogorov complexity

Step 2: Make precise the statistical definition of randomness.

- Martin-Löf randomness

Step 3: Explain how these two definitions relate to one another.

- The Levin-Schnorr Theorem



KOLMOGOROV COMPLEXITY

KOLMOGOROV'S 1965 PAPER

In his 1965 paper, "Three approaches to the definition of the notion of amount of information," Kolmogorov introduced a measure of complexity that is nowadays referred to as ***Kolmogorov complexity***.

As we'll see shortly, random sequences are those that have sufficiently high Kolmogorov complexity.

This definition of complexity is given in terms of computable functions, so we'll have to briefly discuss a few basic facts from computability theory.

THE NOTION OF A COMPUTABLE FUNCTION

Intuitively, a function $f : \mathbb{N} \to \mathbb{N}$ is computable if

(1) there is a finite set of instructions (each of which is finite) for determining the values of *f*,

(2) each value *f(n)* can be obtained in finitely many steps (in accordance with the instructions), and

(3) the instructions can be carried out, in principle, by a human working with pencil and paper (and not making use of any special insight or ingenuity).

FORMAL DEFINITIONS OF COMPUTABLE FUNCTION

For the purposes of today's talk, I won't give a formal definition of computable function.

However, it is important to emphasize that all reasonable definitions of computable number-theoretic function (such as those given in terms of Turing machines) have been shown to be equivalent.

The Church-Turing thesis: The formal definition of computable function captures the intuitive notion of computable function.

SOME USEFUL FACTS, 1

There are some important facts about computable functions that we'll need in what follows.

1. There is an effective enumeration of all partial computable functions $(\phi_i)_{i \in \mathbb{N}}$.

    - For each i, ϕ_i need not be defined on every natural number n.
    - If ϕ_i is defined on n, we write $\phi_i(n)\downarrow$.

2. There is a universal partial computable function:

$$\Phi(e, x) \simeq \phi_e(x)$$

SOME USEFUL FACTS, 2

3. A set of natural numbers A is computable if there is a total computable function ϕ that computes the characteristic function of A:

$$\phi(n) = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A \end{cases}$$

4. The halting set $K = \{e : \phi_e(e)\downarrow\}$ is not a computable set.

PLAIN KOLMOGOROV COMPLEXITY, 1

Hereafter, we will consider partial computable functions as maps from $2^{<\omega}$ to $2^{<\omega}$ (and I'll refer to these functions as ***machines***).

Let $M : 2^{<\omega} \to 2^{<\omega}$ be a machine and let $\tau \in 2^{<\omega}$.

Any $\sigma \in 2^{<\omega}$ such that $M(\sigma)\downarrow = \tau$ is called an M-description of τ.

Then we define $C_M(\tau) = \min\{|\sigma| : M(\sigma)\downarrow = \tau\}$ to be the ***plain Kolmogorov complexity of τ relative to M***.

PLAIN KOLMOGOROV COMPLEXITY, 2

Let $(M_i)_{i\in\mathbb{N}}$ be an effective enumeration of all machines.

We can define a universal machine $U : 2^{<\omega} \to 2^{<\omega}$ as follows:

$$U(1^i 0\sigma) \simeq M_i(\sigma)$$

Then $C_U(\tau) = \min\{|\sigma| : U(\sigma)\downarrow = \tau\}$ is the ***plain Kolmgorov complexity*** of τ. We set $C(\sigma) := C_U(\sigma)$.

Why are we justified defining $C(\cdot)$ in terms of one fixed universal machine?

OPTIMALITY AND INVARIANCE

The Optimality Theorem: Let U be a universal machine. Then for any machine M there is some c such that

$$C(\sigma) \leq C_M(\sigma) + c$$

for every $\sigma \in 2^{<\omega}$.

The Invariance Theorem: Let U_1 and U_2 be universal machines. Then there is some constant c_{U_1,U_2} such that

$$|C_{U_1}(\sigma) - C_{U_2}(\sigma)| \leq c_{U_1,U_2}$$

for every $\sigma \in 2^{<\omega}$.

A SIMPLE EXAMPLE

Let $M : 2^{<\omega} \to 2^{<\omega}$ be the machine such that $M(\sigma)\!\downarrow = \sigma$ for every $\sigma \in 2^{<\omega}$.

Then $C_M(\sigma) = |\sigma|$ for every $\sigma \in 2^{<\omega}$.

Thus there is some c such that

$$C(\sigma) \leq |\sigma| + c$$

for every $\sigma \in 2^{<\omega}$.

INCOMPRESSIBLE STRINGS, 1

For a fixed c, let us say that a string σ is ***c-compressible*** if $C(\sigma) < |\sigma| - c$.

Thus σ is ***c-incompressible*** if $C(\sigma) \geq |\sigma| - c$, which only makes sense if $|\sigma| > c$.

We can define σ to be random if $C(\sigma) \approx |\sigma|$, but to be precise, we should require that σ be c-incompressible for some $c \ll |\sigma|$.

INCOMPRESSIBLE STRINGS, 2

It's important to note that for a fixed c and $n > c$, there are many c-incompressible sequences of length n.

In fact, there are at least

$$2^n - (2^{n-c} - 1)$$

c-incompressible sequences of length n.

For example if $n = 10$ and $c = 4$, there are at least 961 c-incompressible sequences of length 10.

EXTENDING TO THE INFINITE?

How might we extend this definition to infinite sequences?

One reasonable suggestion is to define $X \in 2^\omega$ to be random if all of its initial segments are *c*-incompressible for some fixed *c*:

$$(\forall n) C(X \upharpoonright n) \geq n - c$$

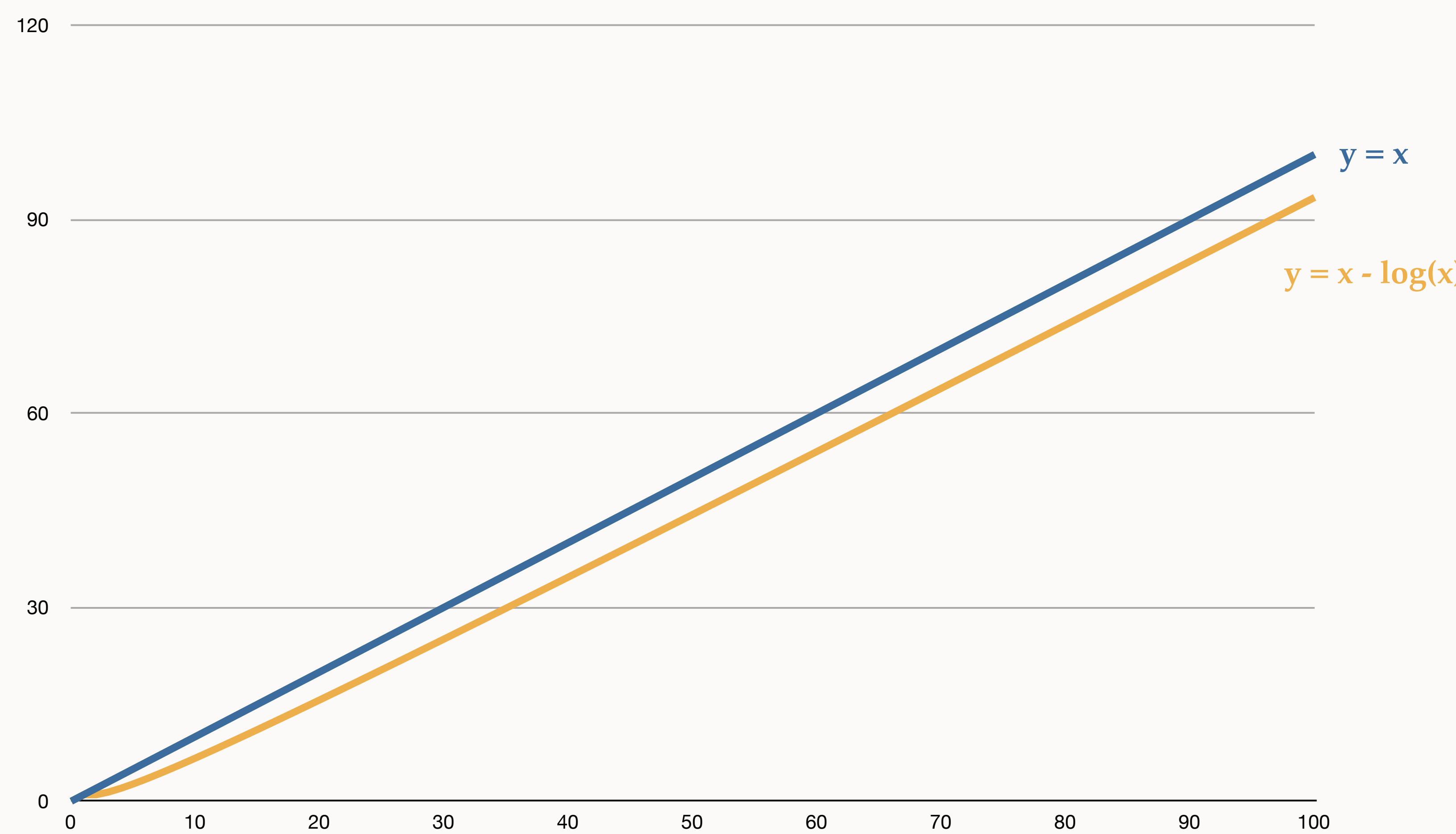
A VACUOUS DEFINITION

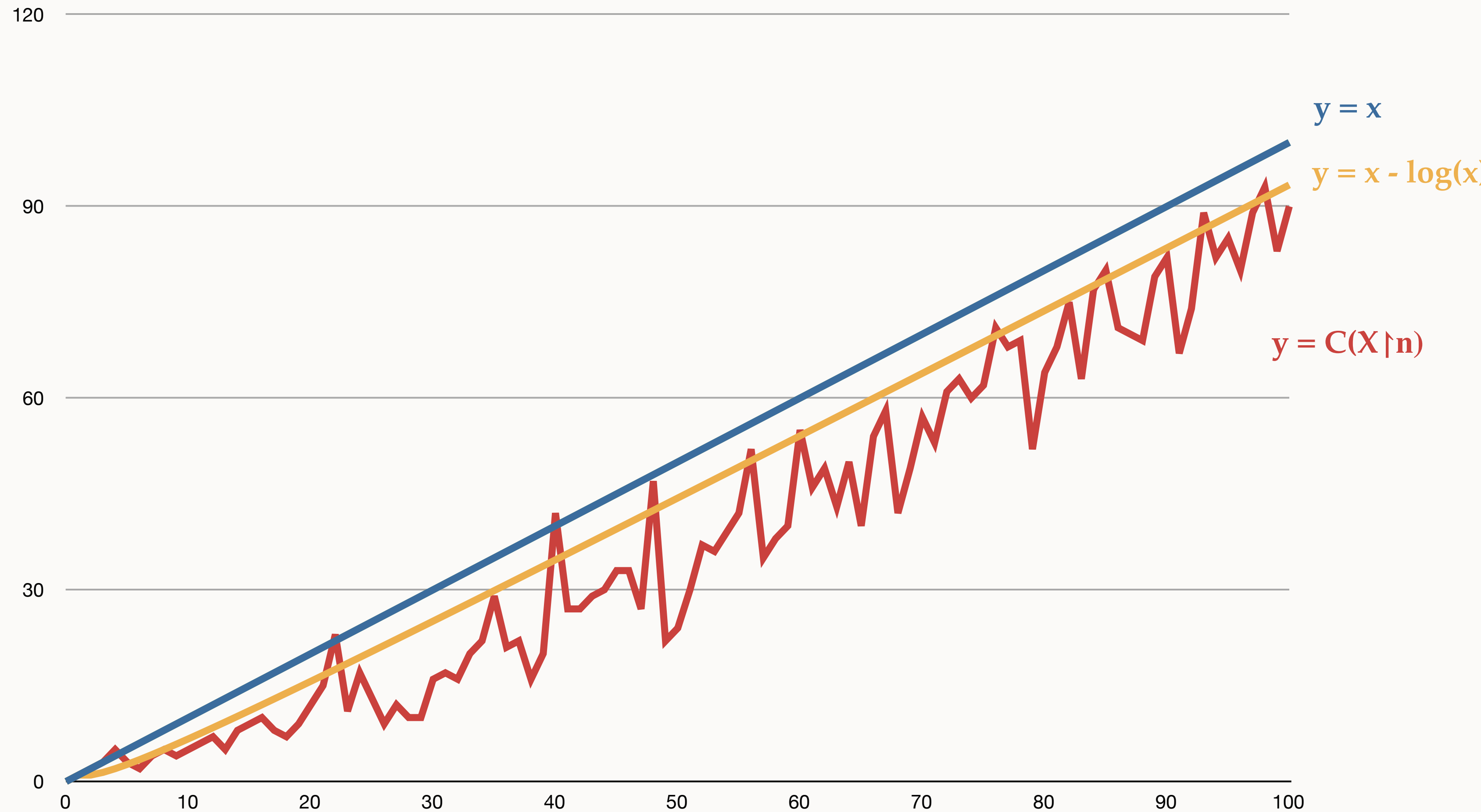
However, Martin-Löf proved the following:

Theorem: For every sequence X, there are infinitely many n such that

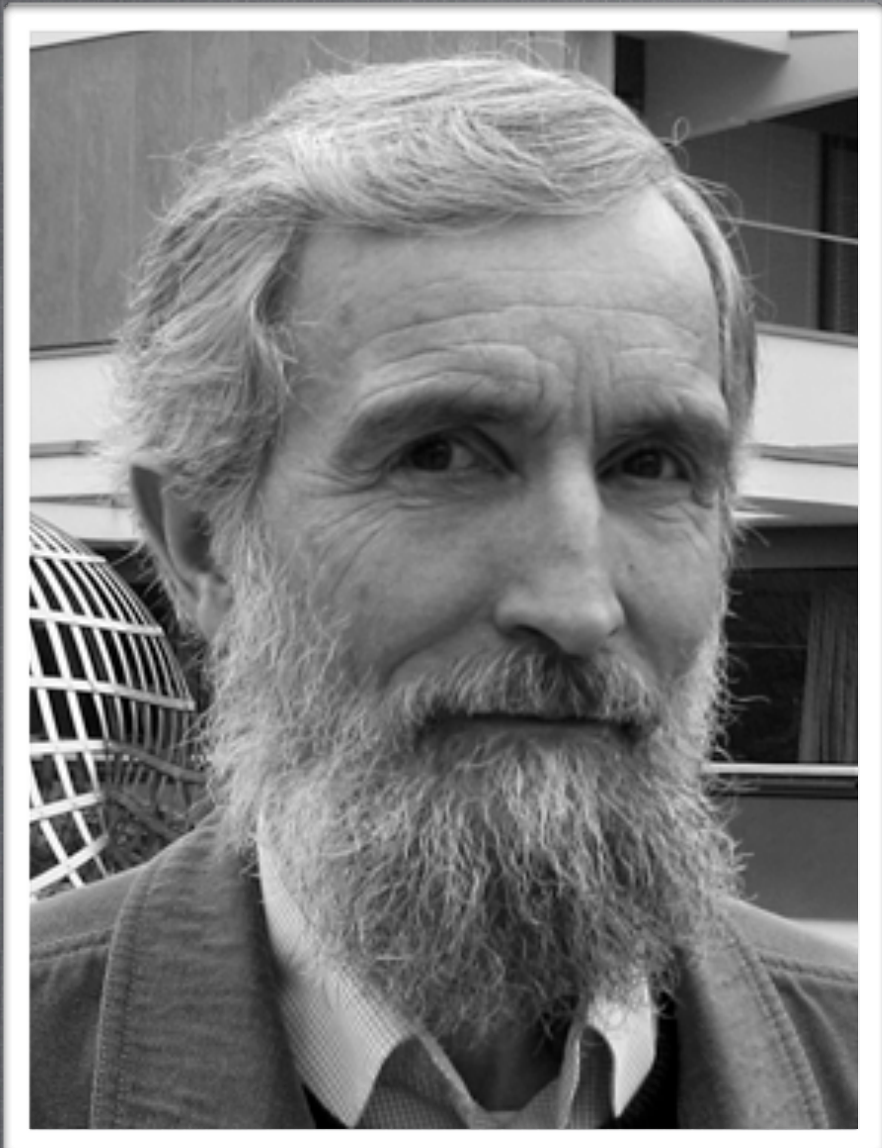
$$C(X{\upharpoonright}n) \leq n - log(n).$$

Thus, for each *c*, there is no sequence with only *c*-incompressible initial segments.


120
90
60
30
0
0
10
20
30
40
50
60
70
80
90
100
y = x
y = x - log(x)



$C(X\restriction n) \leq n - \log(n)$ for infinitely many n



MARTIN-LÖF RANDOMNESS

MARTIN-LÖF'S 1966 PAPER

Working under the supervision of Kolmogorov, Martin-Löf developed a statistical definition of randomness for finite and infinite sequences.

Both definitions are given in terms of certain effective statistical tests.

Nowadays these tests are referred to as *Martin-Löf tests*.

MARTIN-LÖF TESTS, 1

Suppose that we want to statistically test whether a given finite sequence σ was produced by the tosses of a fair coin.

Thus we subject σ to a battery of statistical tests, each of which picks out a critical region corresponding to some level of significance α.

If σ occurs in the critical region, we reject the hypothesis of randomness at significance level α.

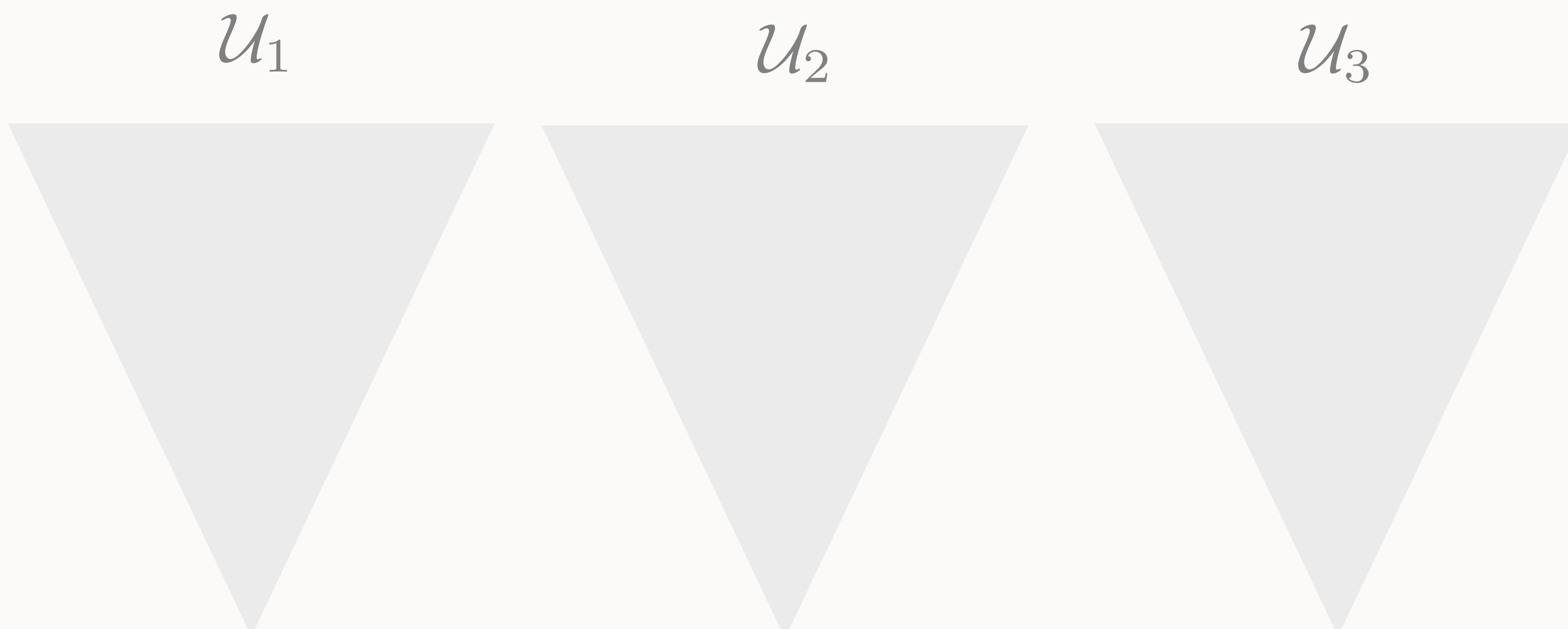
MARTIN-LÖF TESTS, 2

How should we statistically test the hypothesis that a given *infinite* sequence X was produced by the tosses of a fair coin?

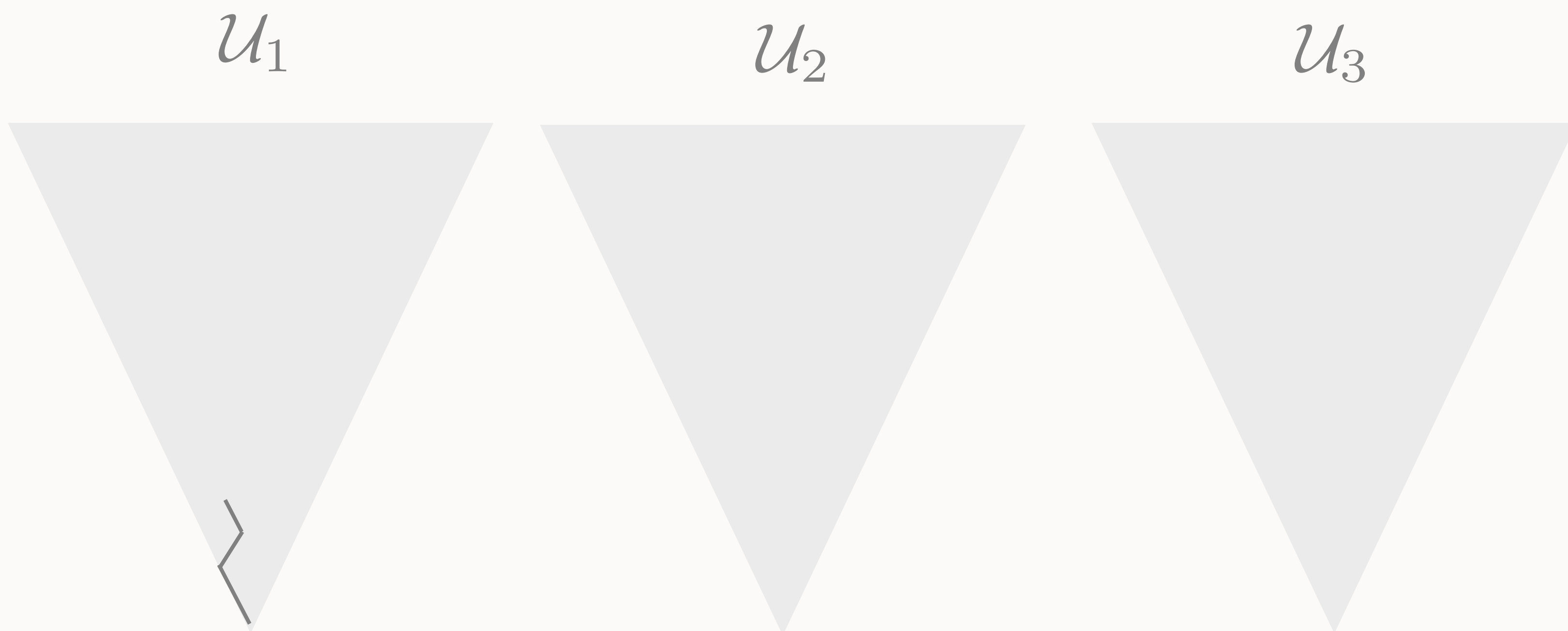
Martin-Löf's idea: We proceed as in the finite case, but we test at every level of significance of the form $\alpha = 2^{-n}$.

Further, Martin-Löf required that the tests we use be given by some *effective procedure.*

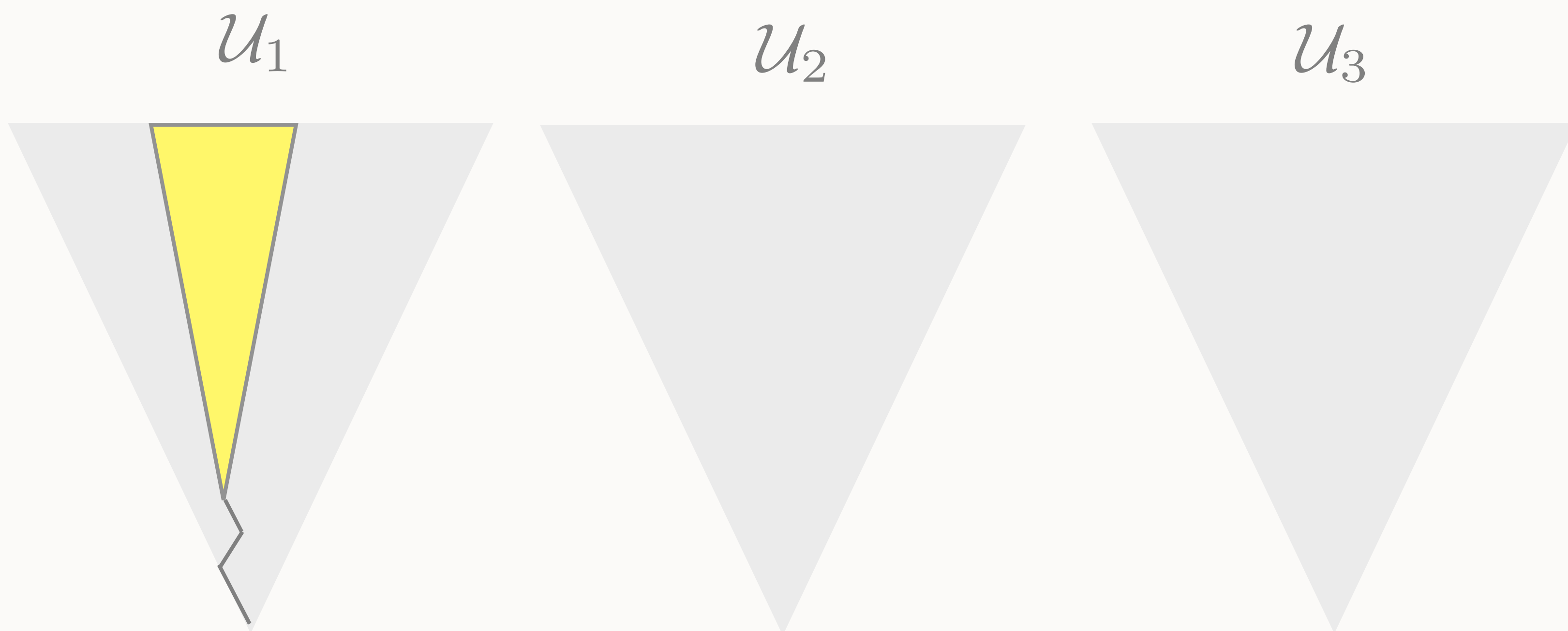
AN ABSTRACT EXAMPLE



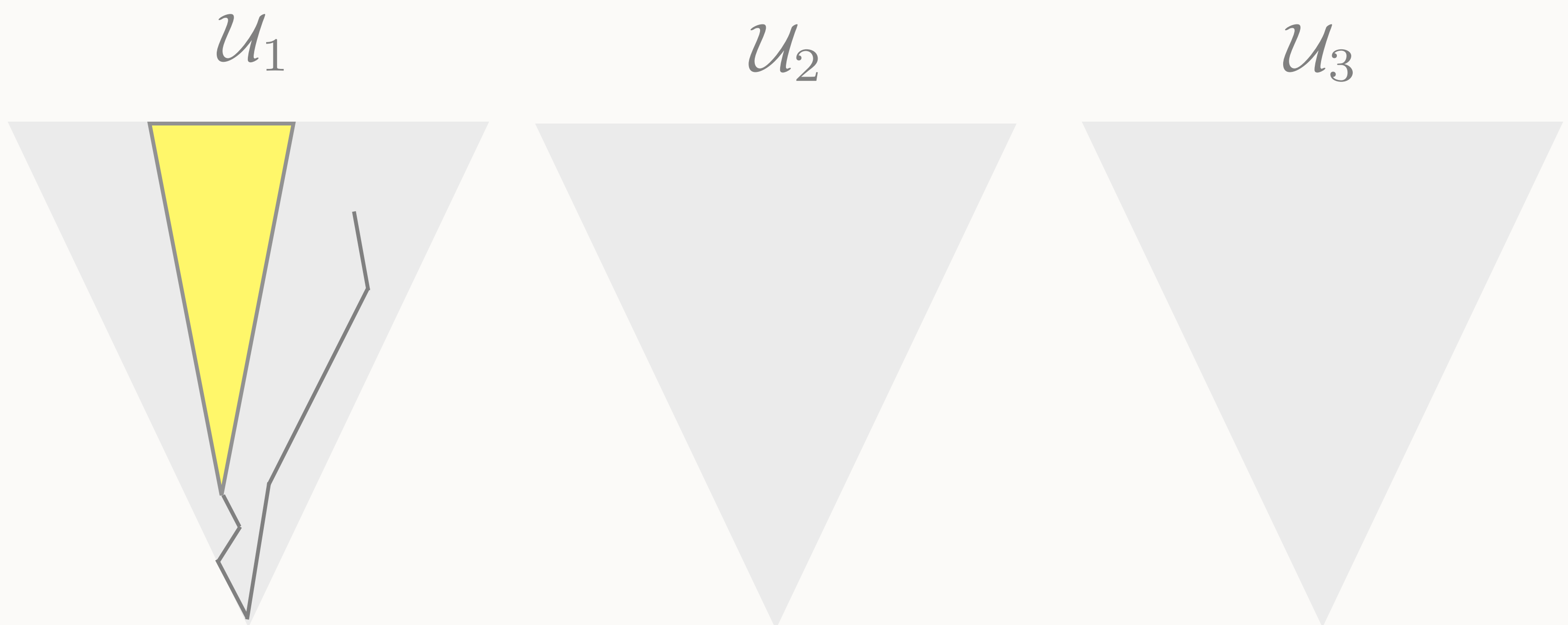
AN ABSTRACT EXAMPLE



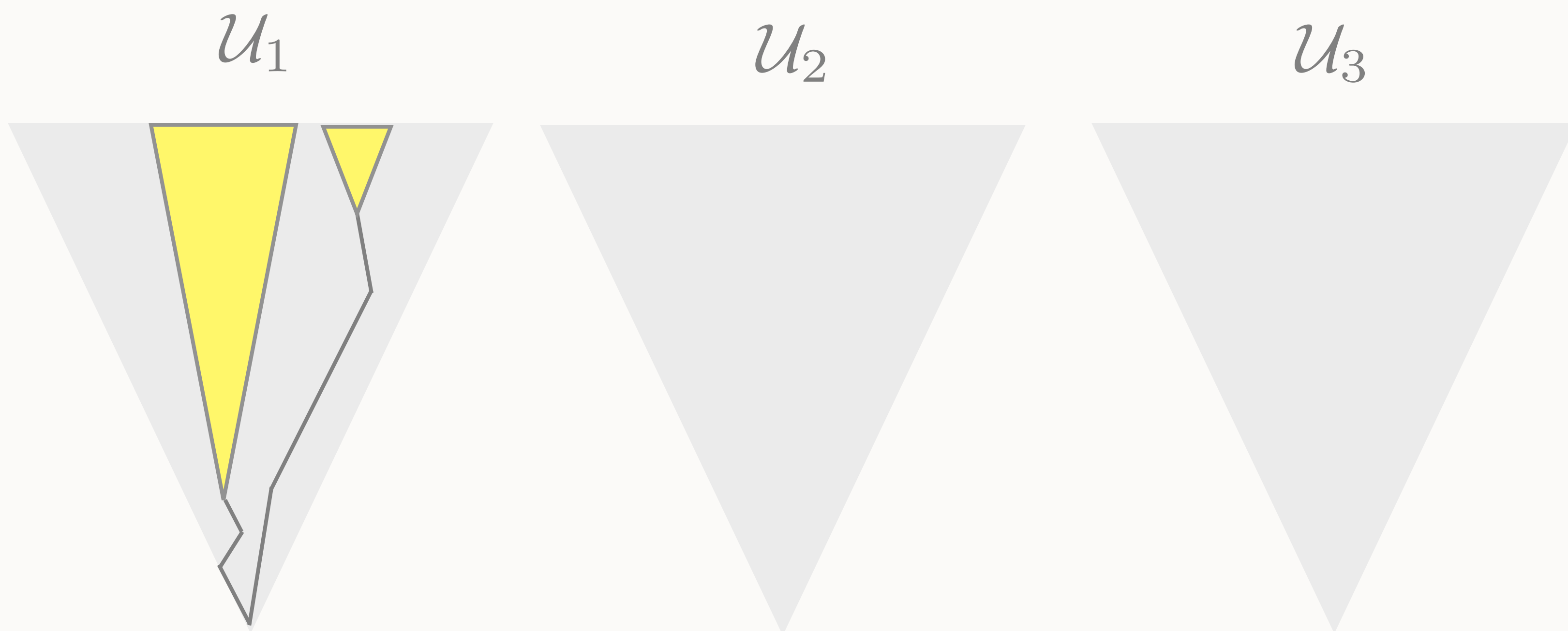
AN ABSTRACT EXAMPLE



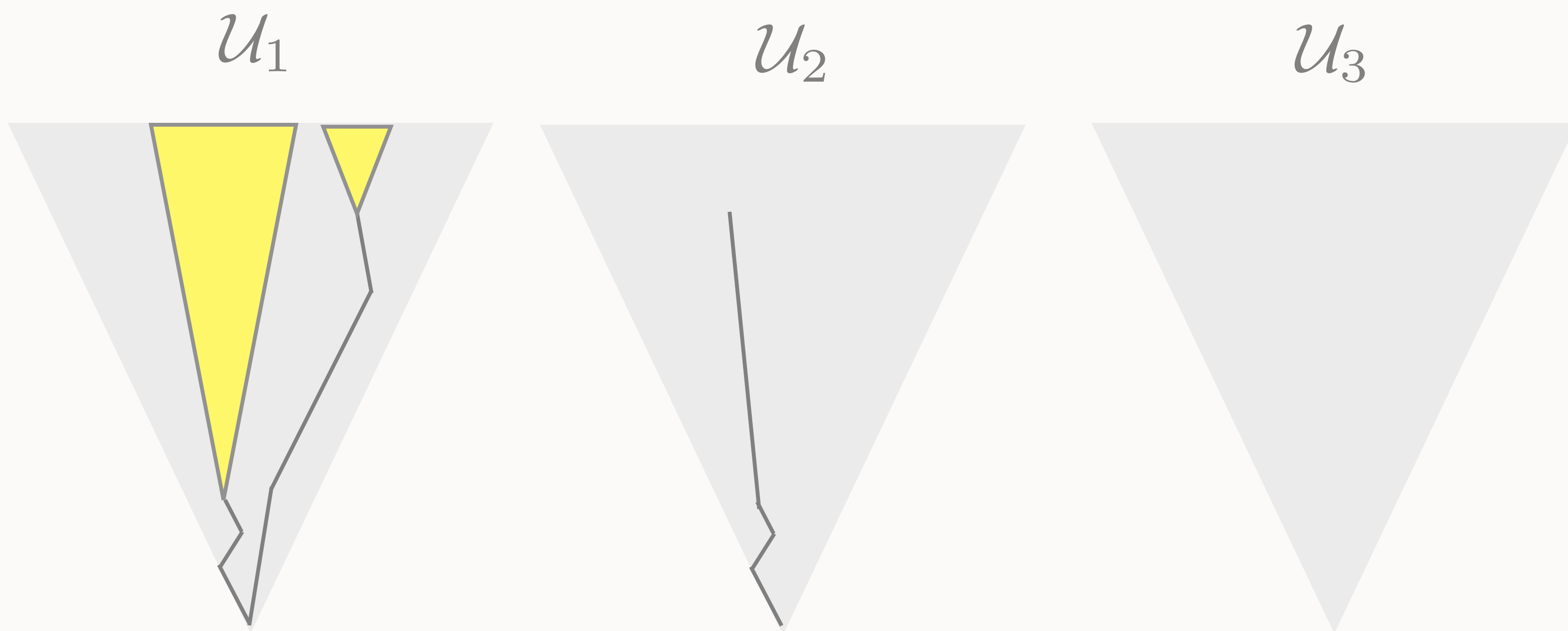
AN ABSTRACT EXAMPLE



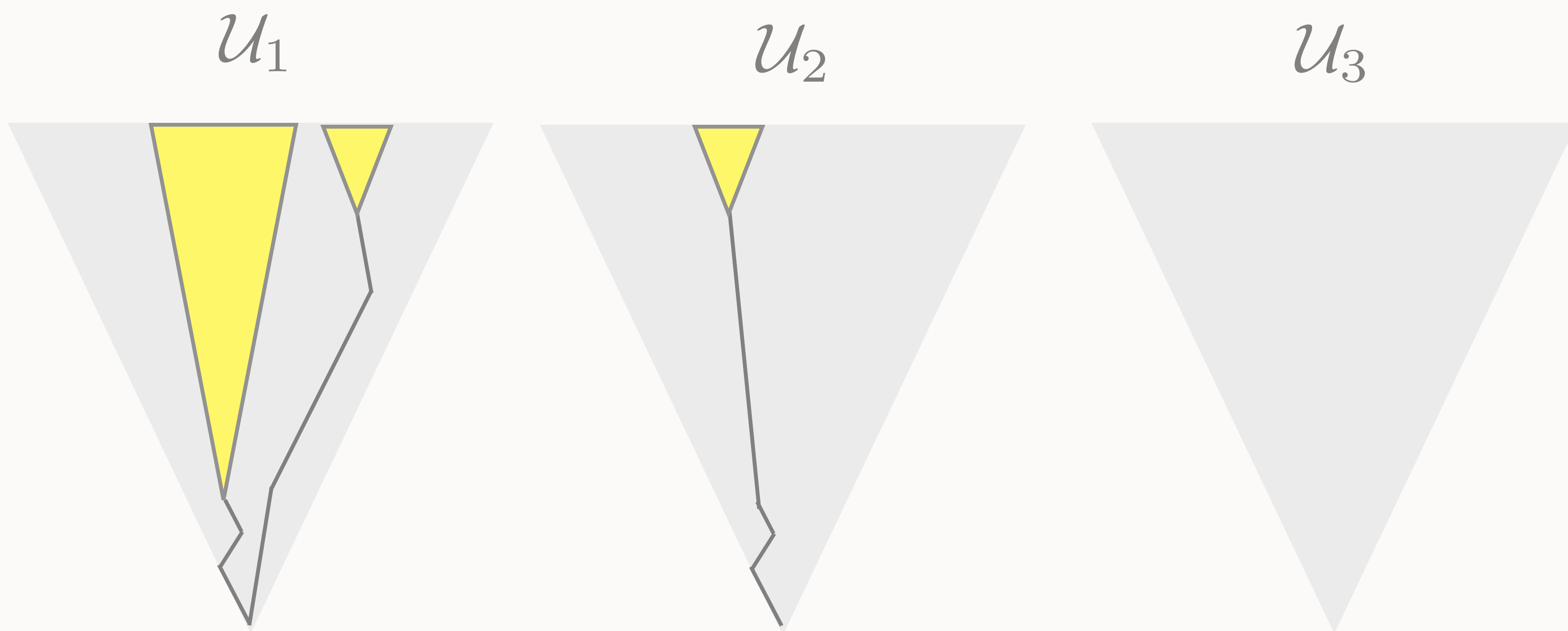
AN ABSTRACT EXAMPLE



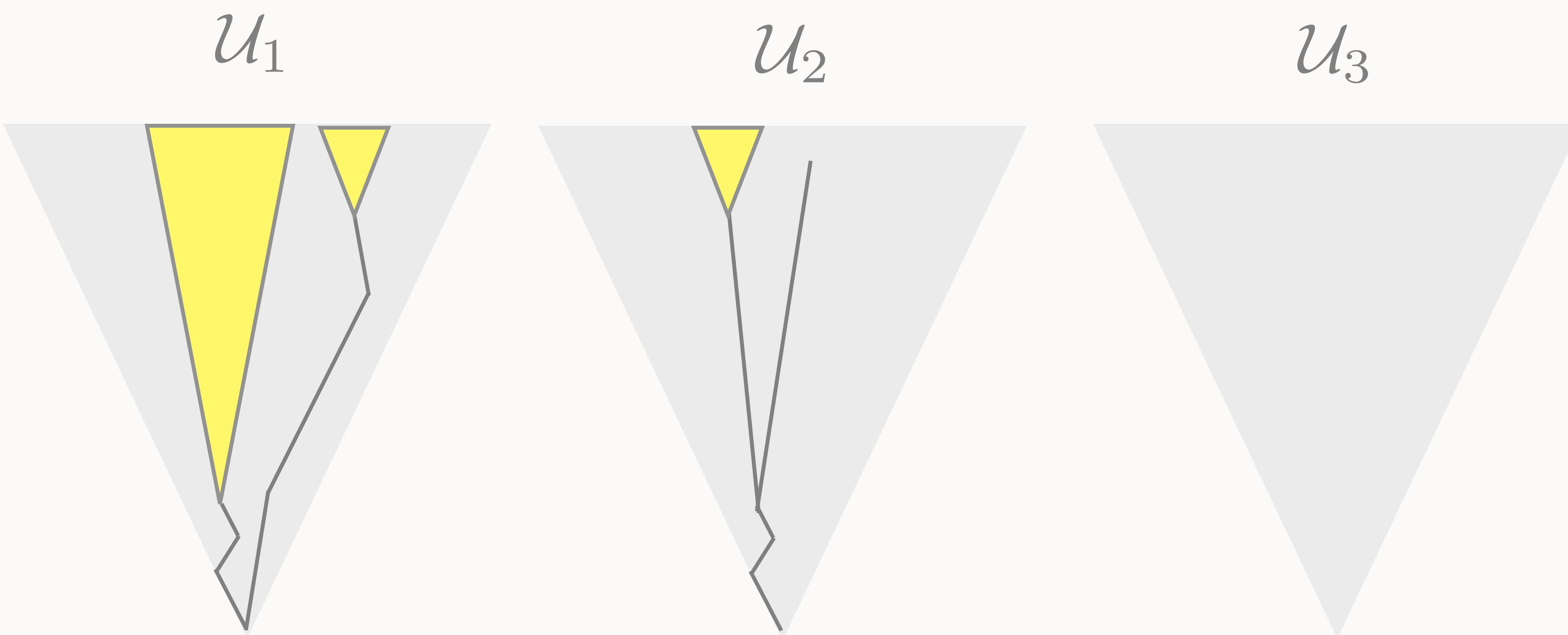
AN ABSTRACT EXAMPLE



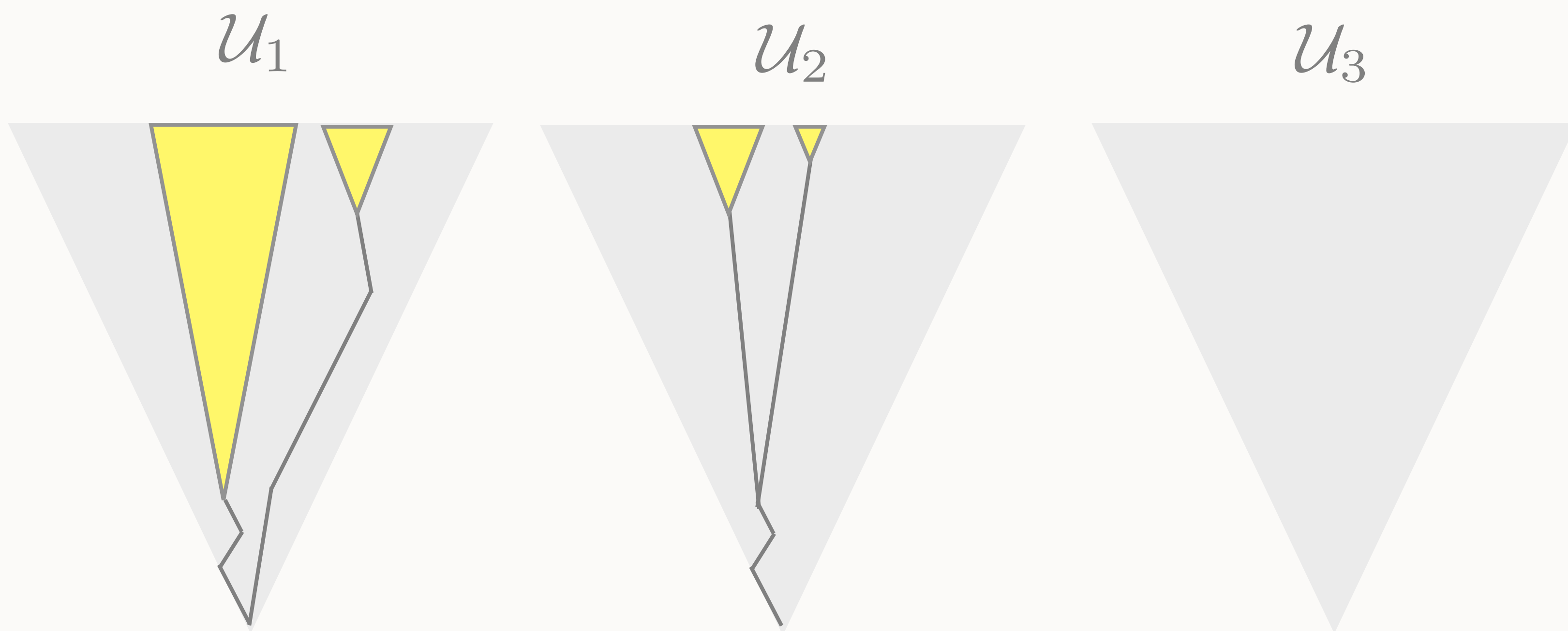
AN ABSTRACT EXAMPLE



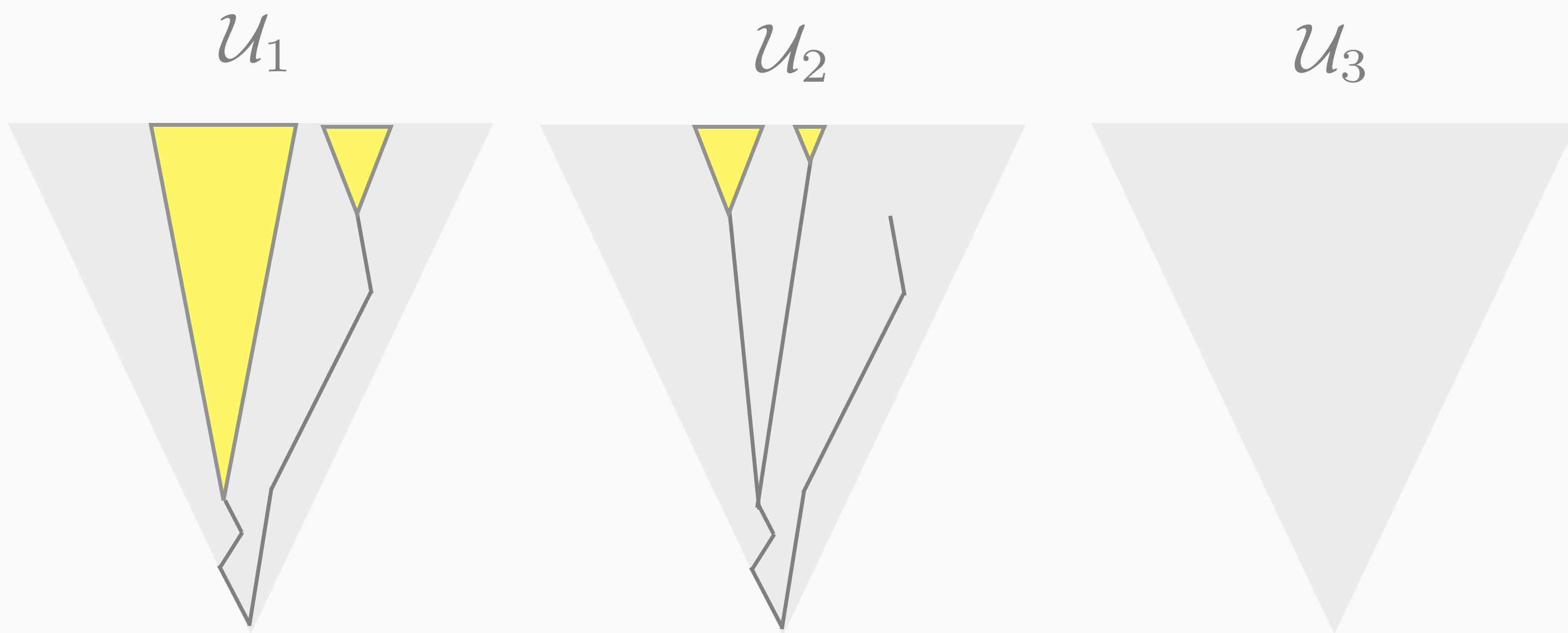
AN ABSTRACT EXAMPLE



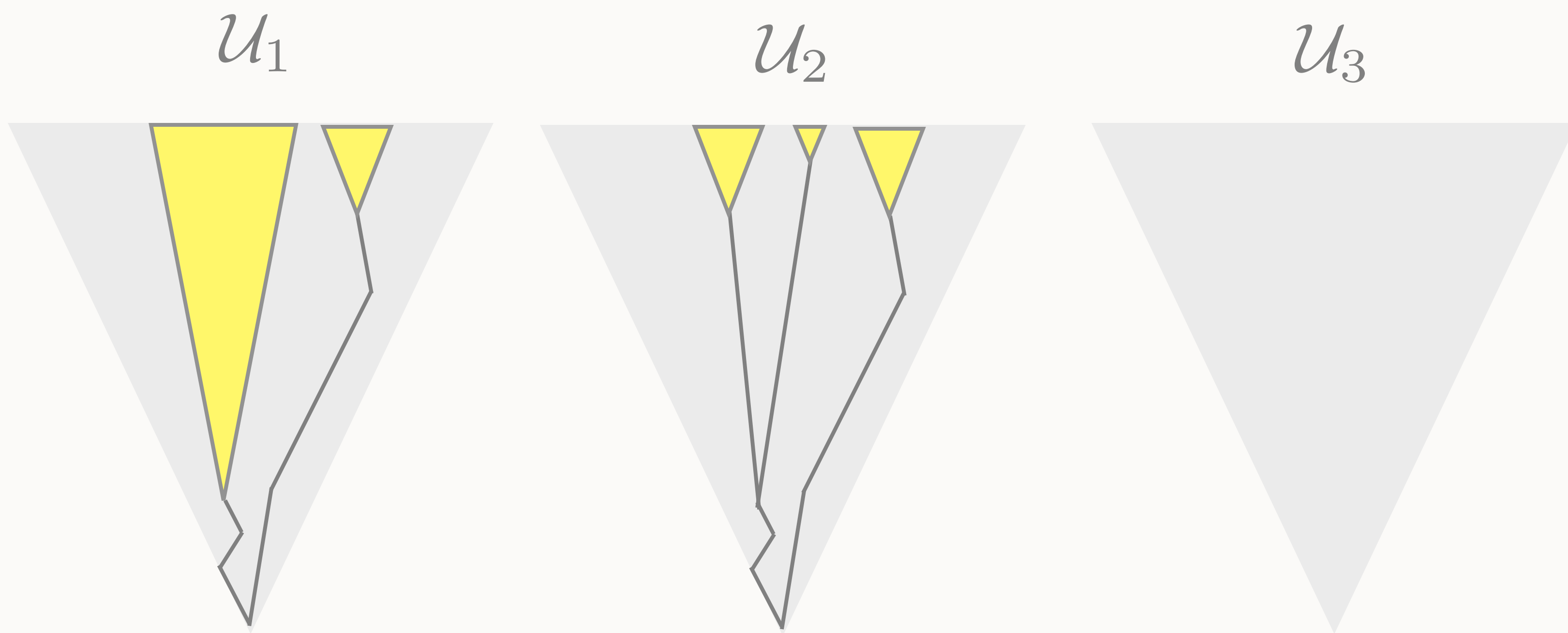
AN ABSTRACT EXAMPLE



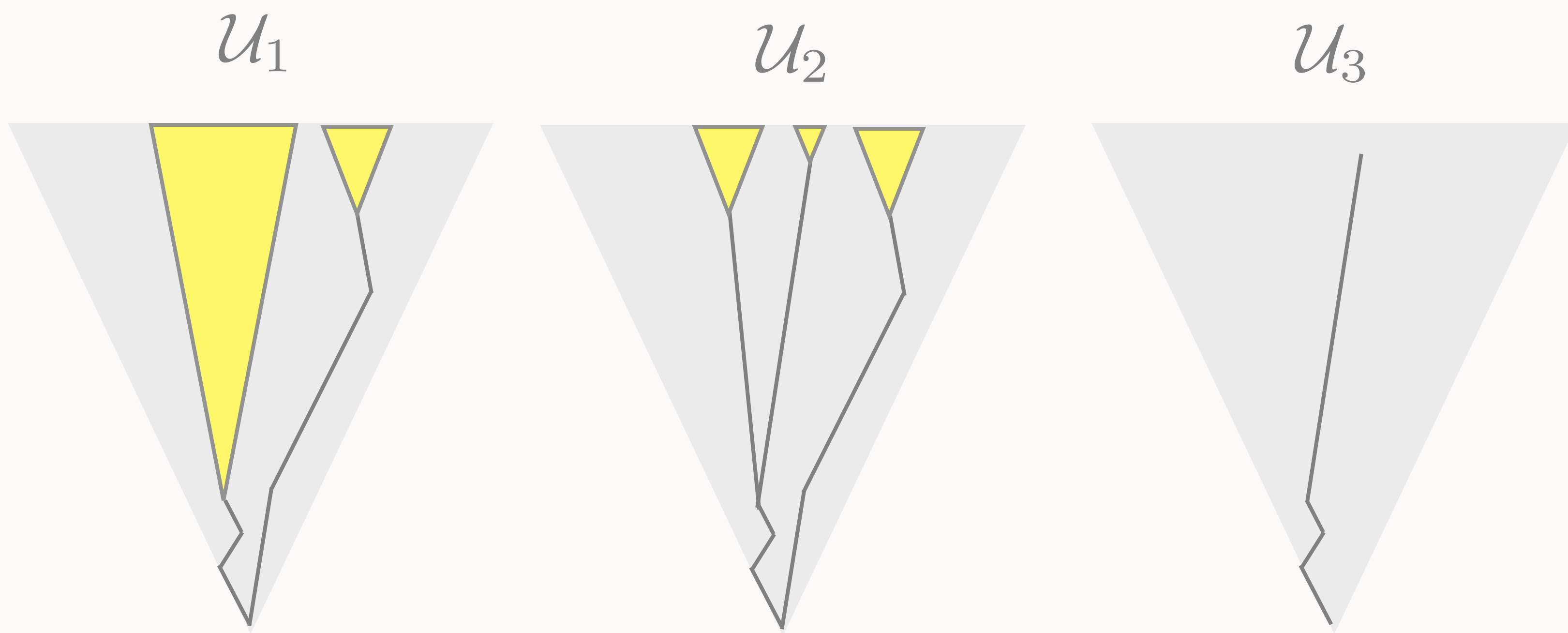
AN ABSTRACT EXAMPLE



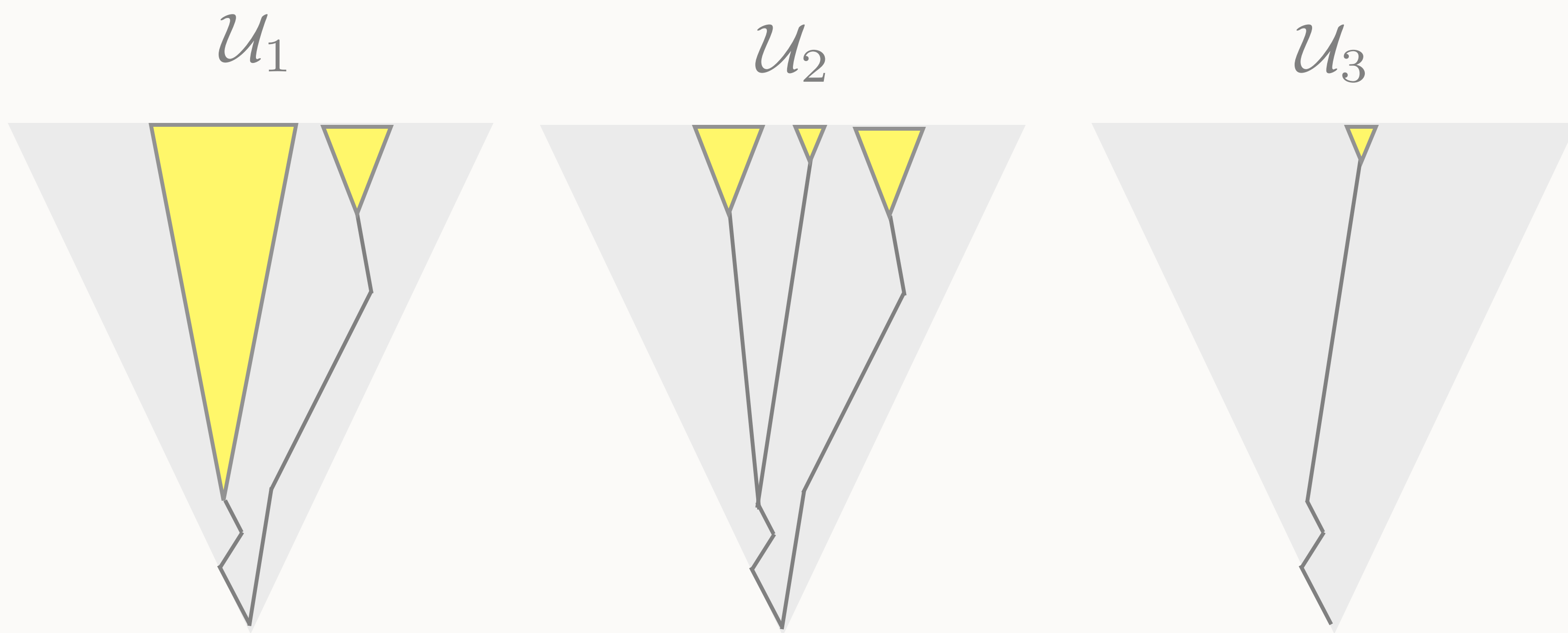
AN ABSTRACT EXAMPLE



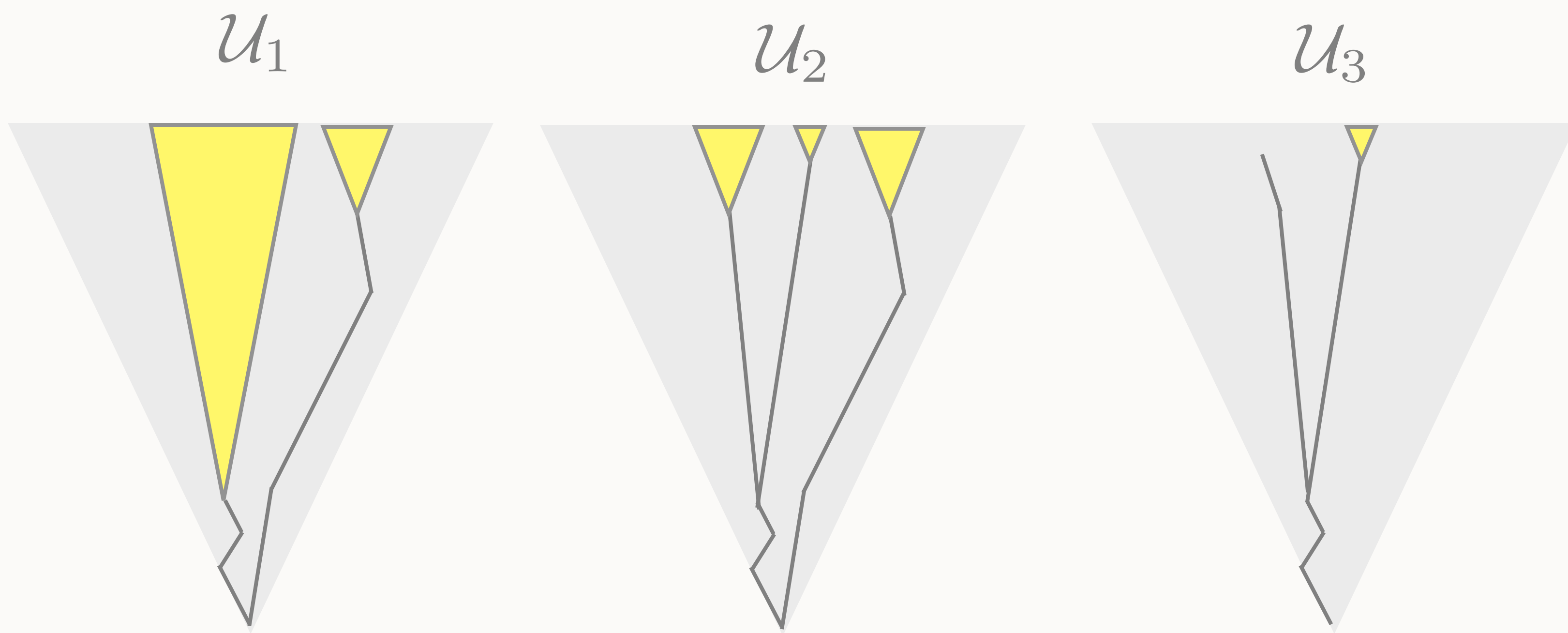
AN ABSTRACT EXAMPLE



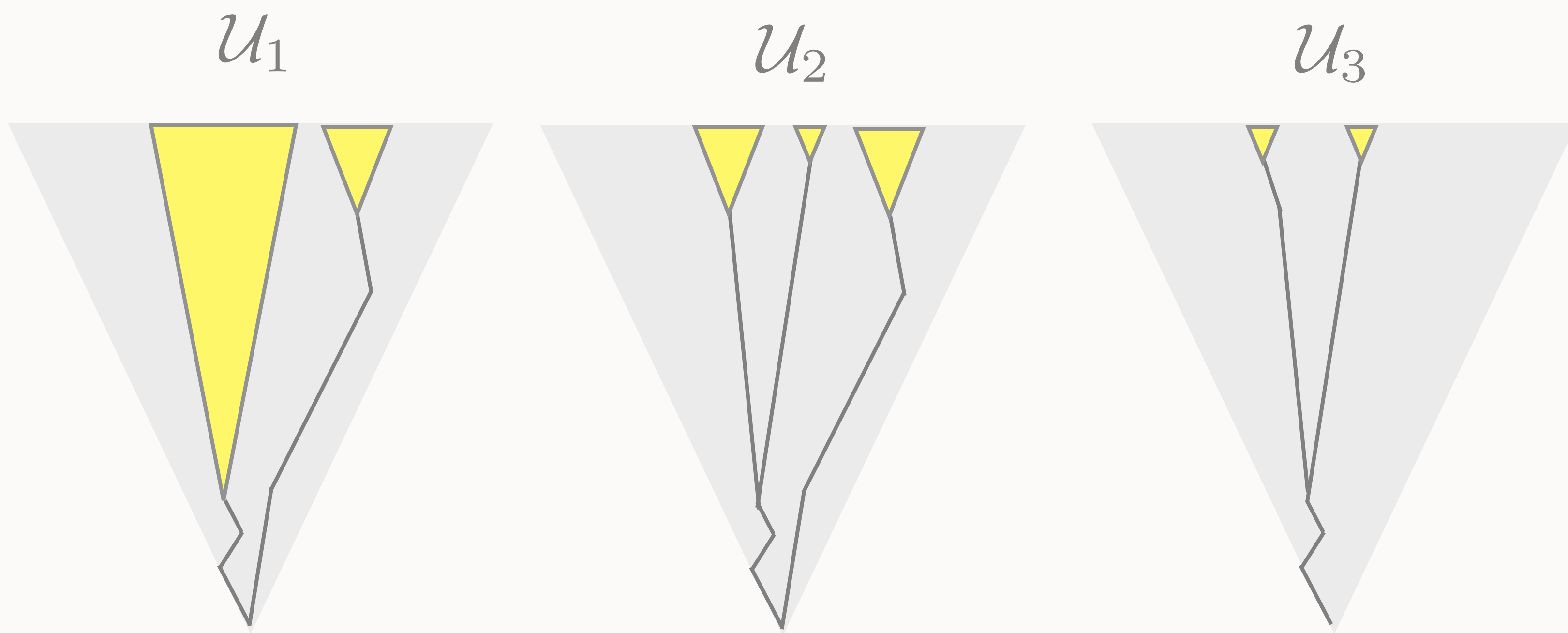
AN ABSTRACT EXAMPLE



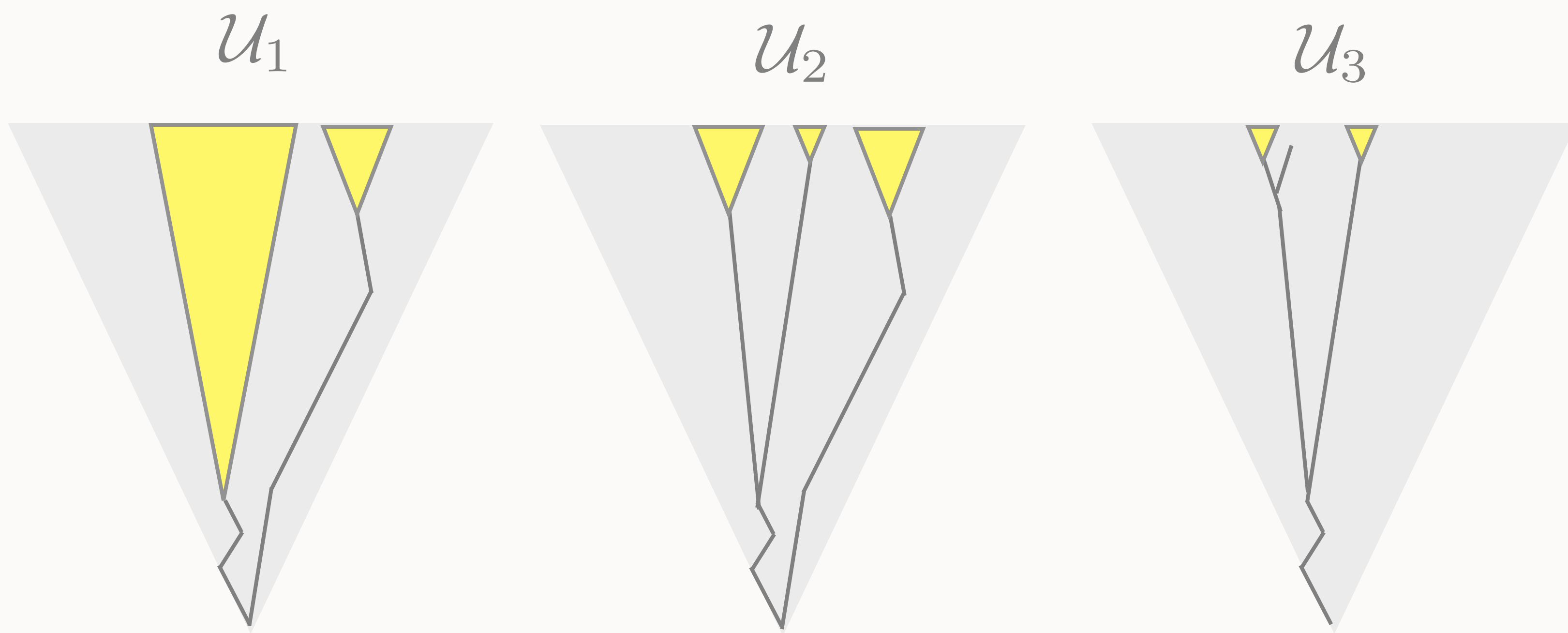
AN ABSTRACT EXAMPLE



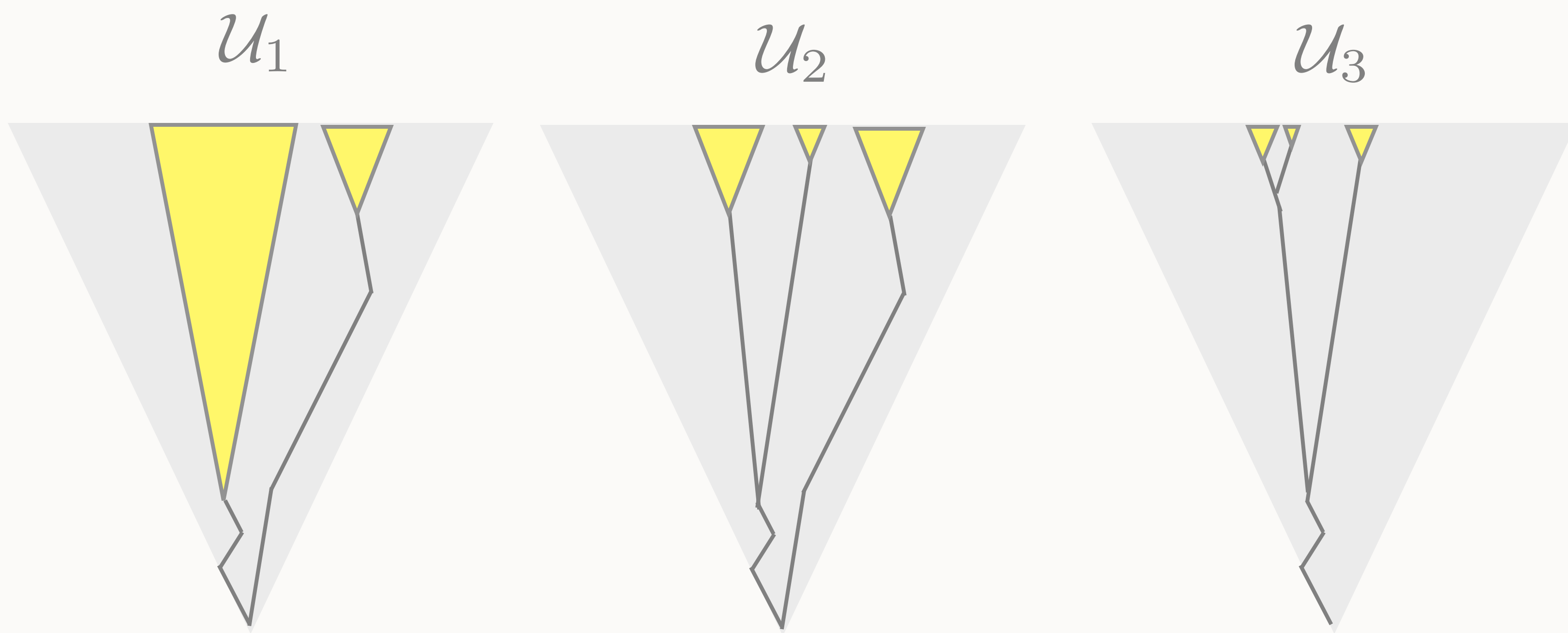
AN ABSTRACT EXAMPLE



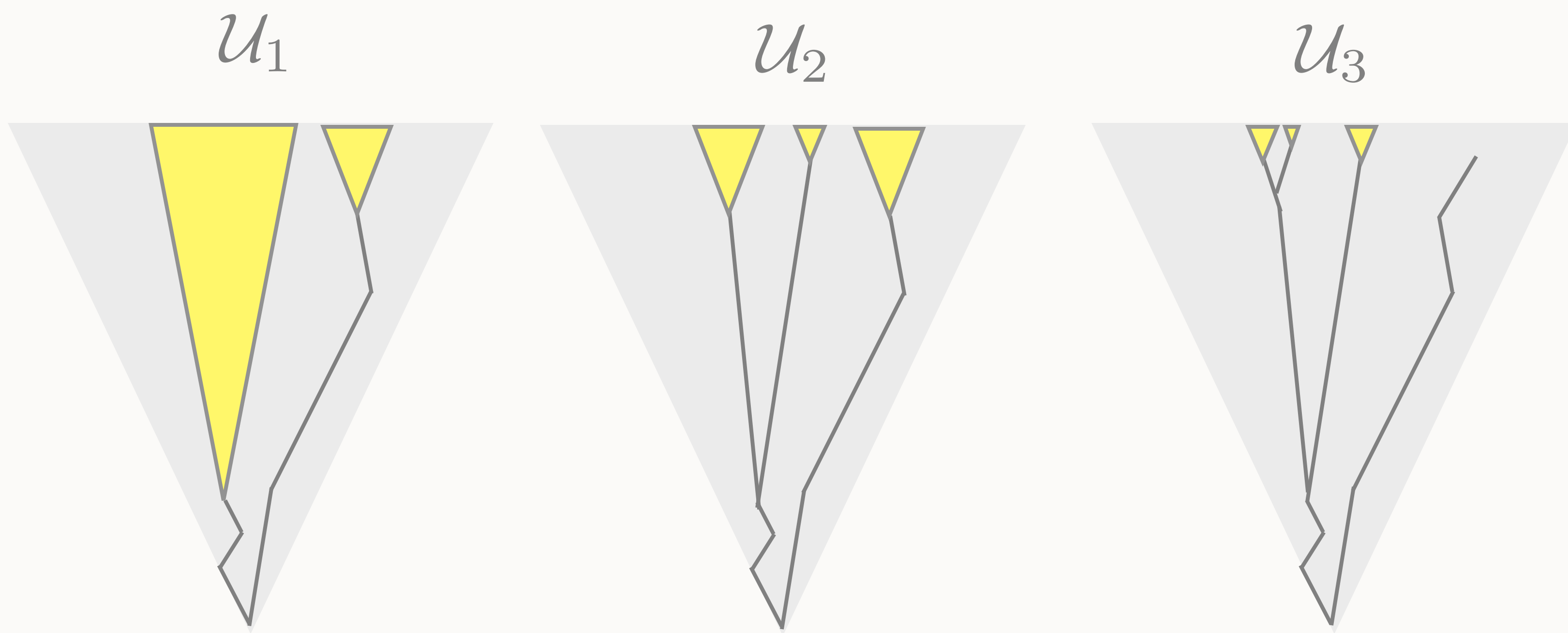
AN ABSTRACT EXAMPLE



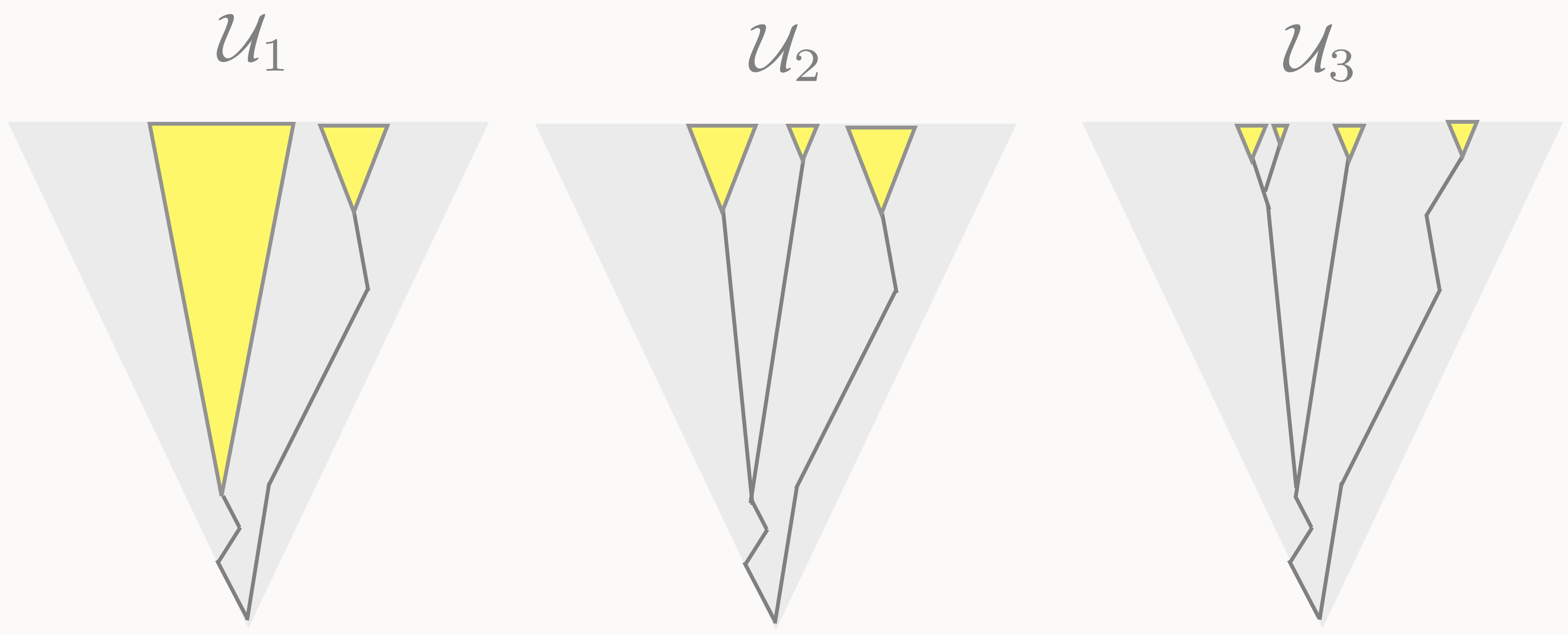
AN ABSTRACT EXAMPLE



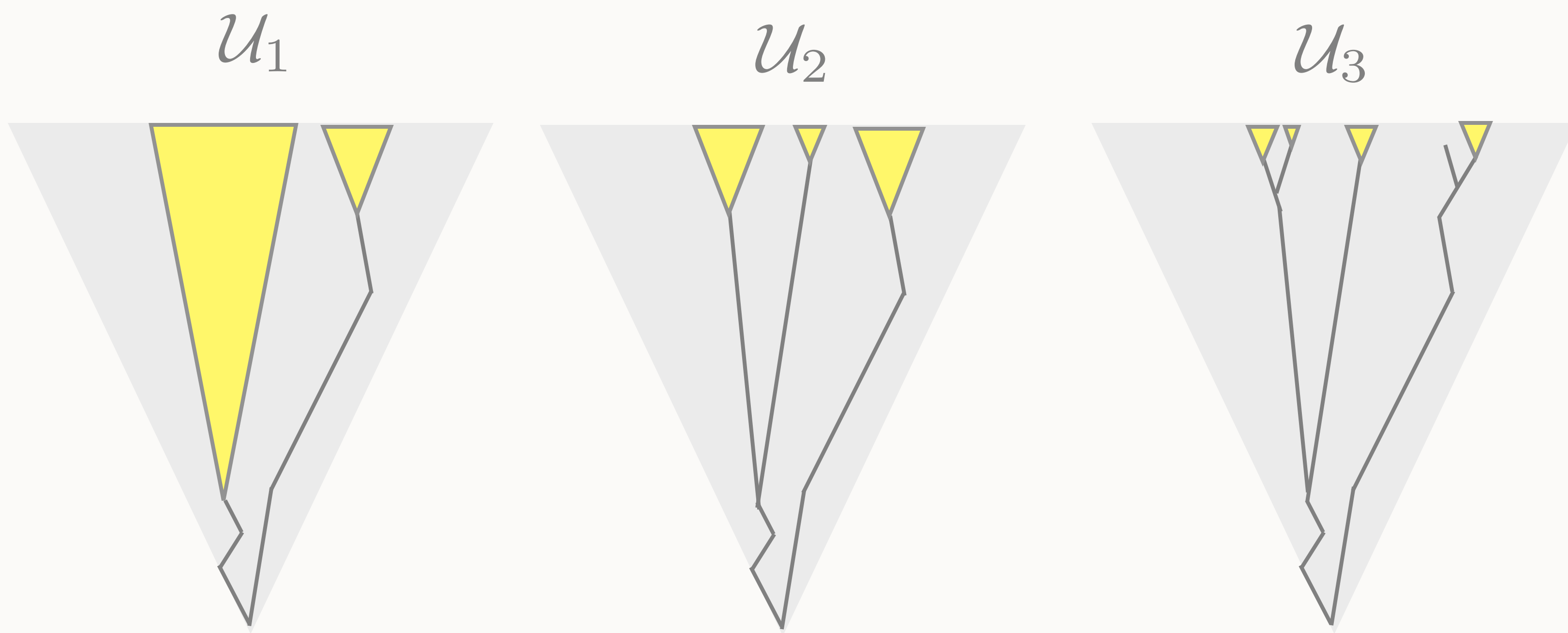
AN ABSTRACT EXAMPLE



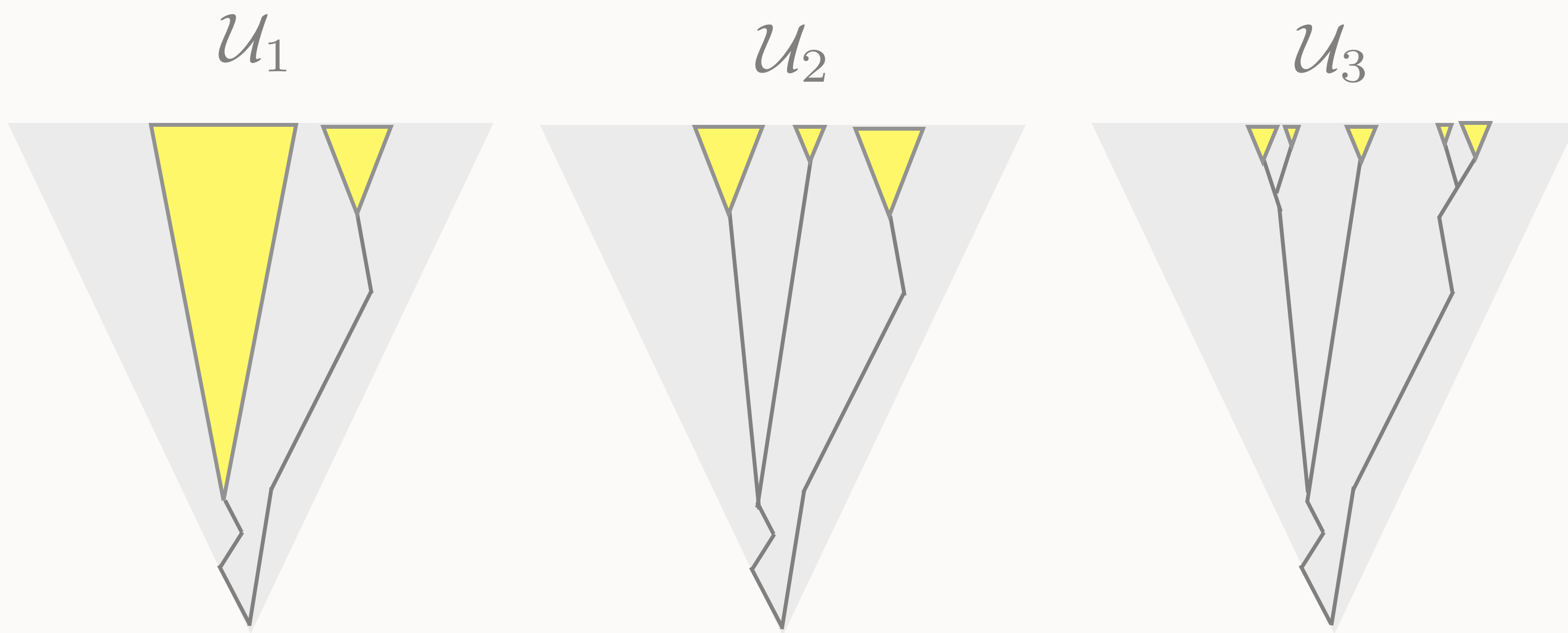
AN ABSTRACT EXAMPLE



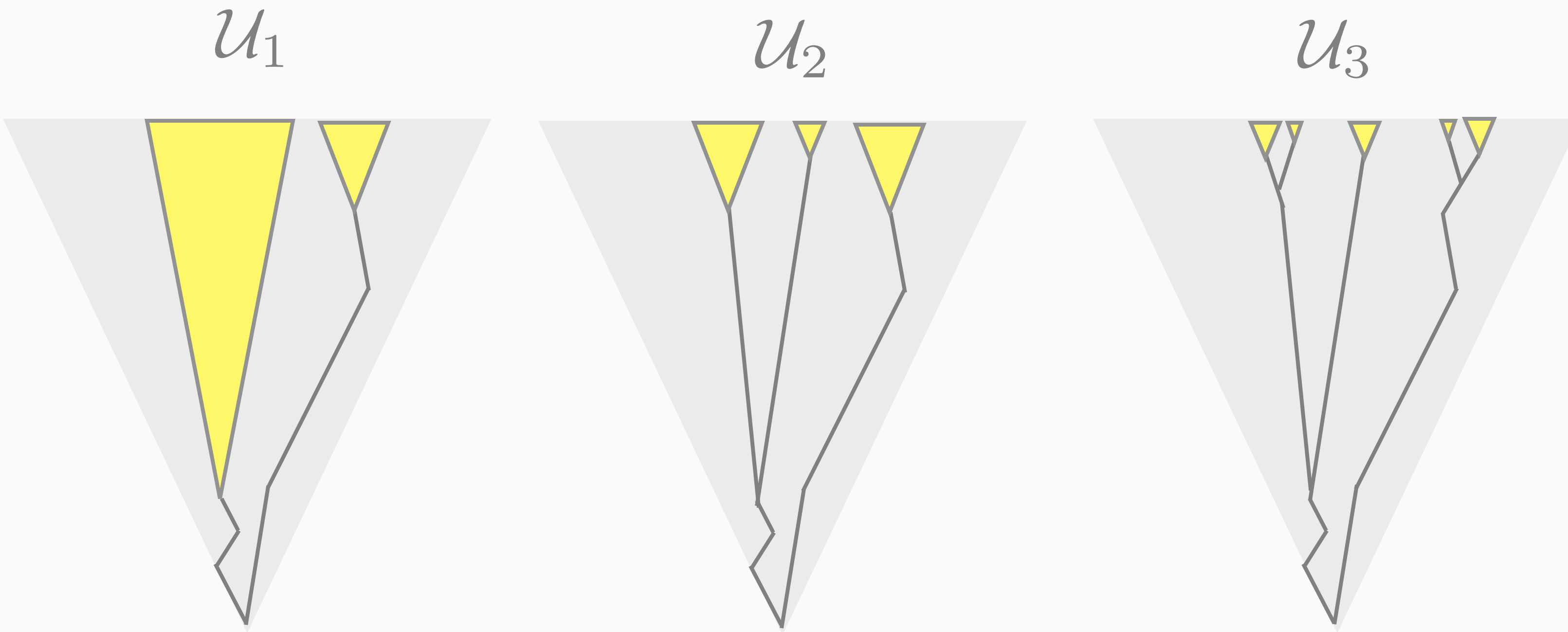
AN ABSTRACT EXAMPLE



AN ABSTRACT EXAMPLE

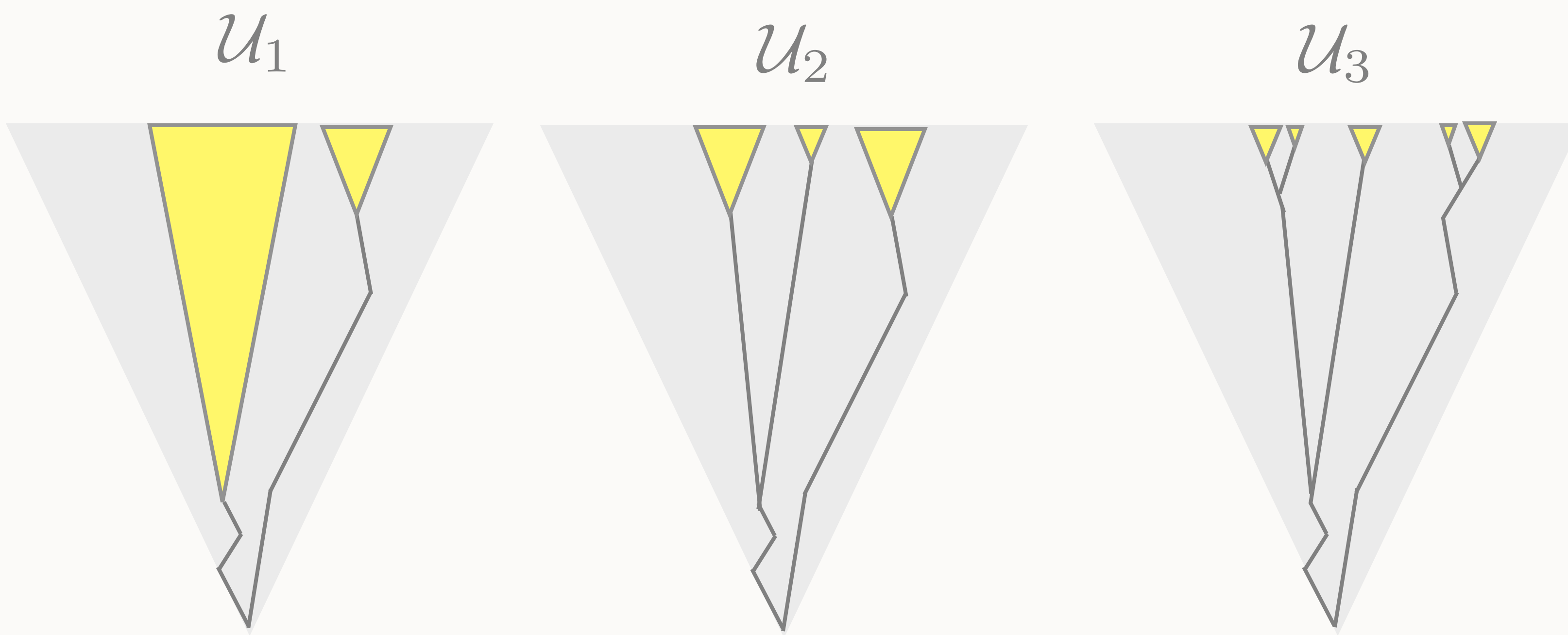


AN ABSTRACT EXAMPLE



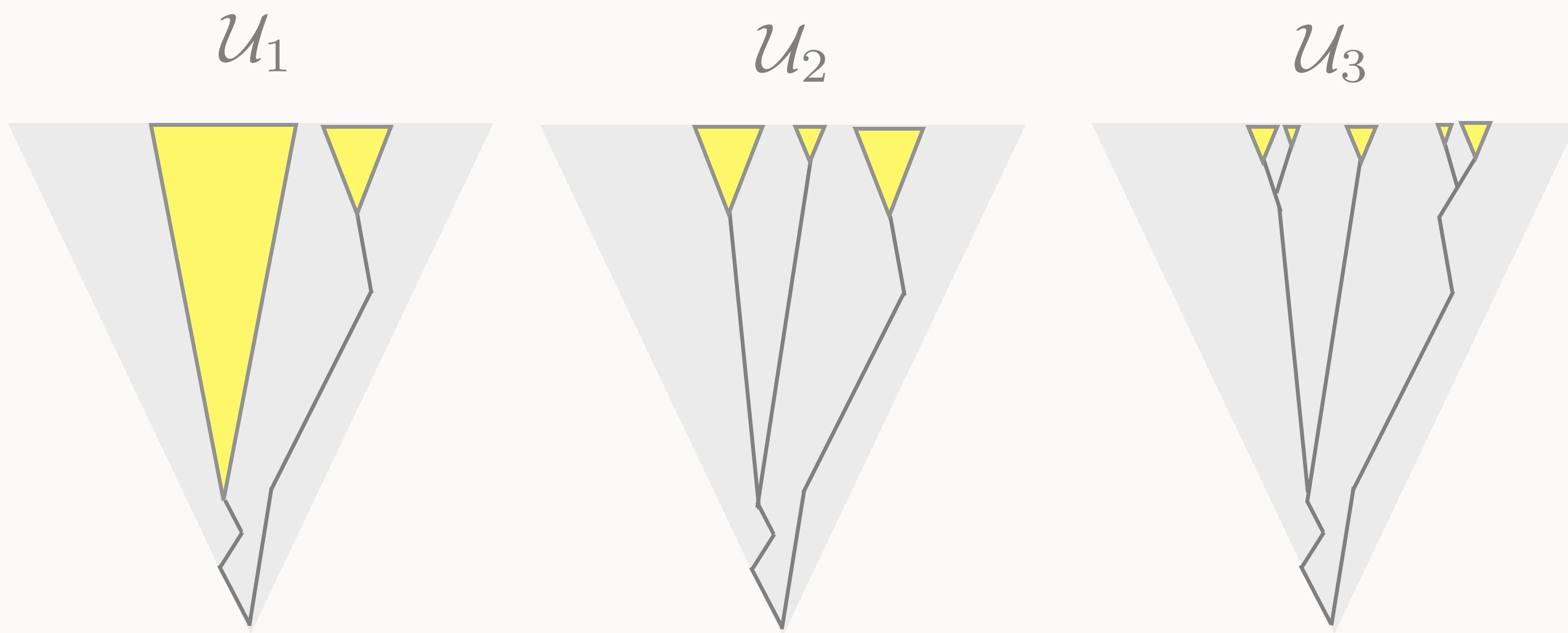
$$\sum_{\sigma \in U_1} 2^{-|\sigma|} \leq \frac{1}{2}$$

AN ABSTRACT EXAMPLE



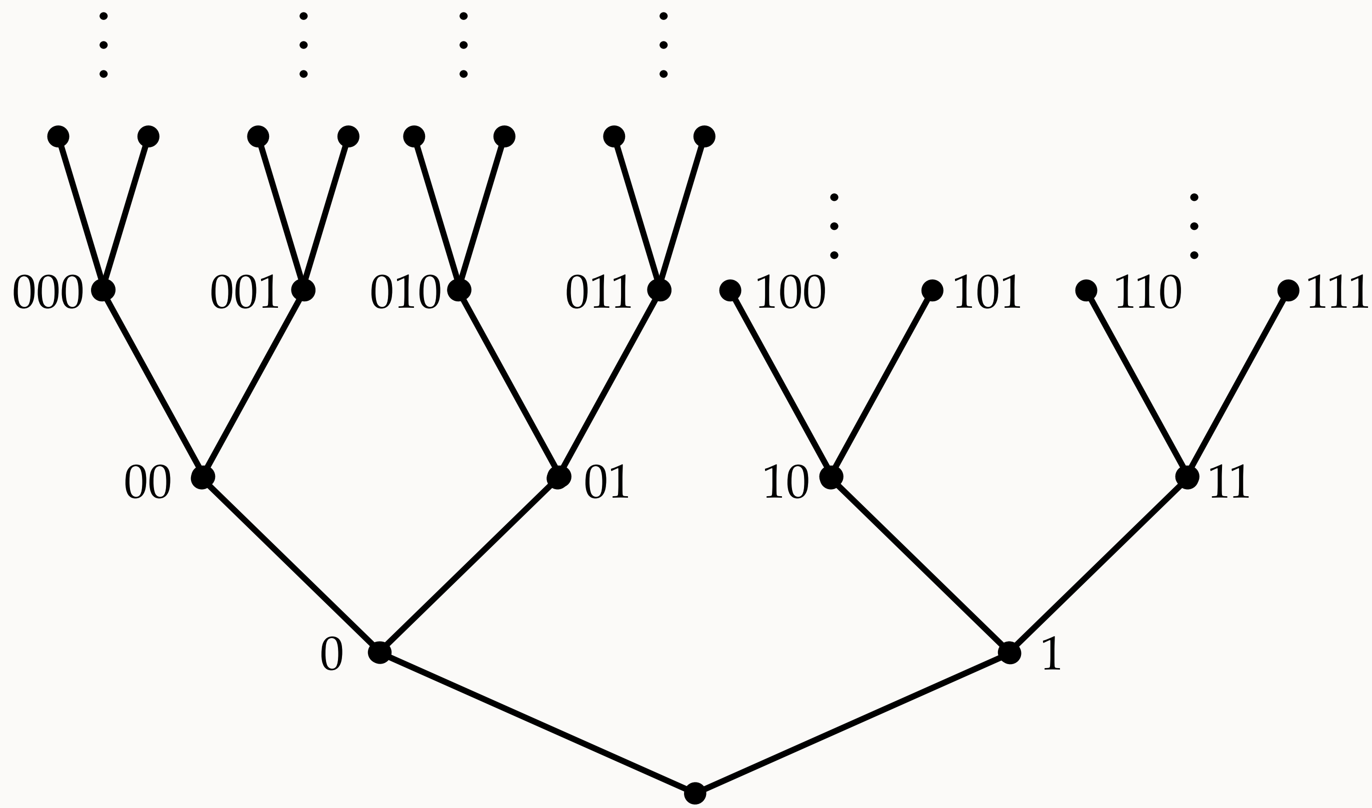
$$\sum_{\sigma \in U_1} 2^{-|\sigma|} \leq \frac{1}{2} \qquad \sum_{\sigma \in U_2} 2^{-|\sigma|} \leq \frac{1}{4}$$

AN ABSTRACT EXAMPLE

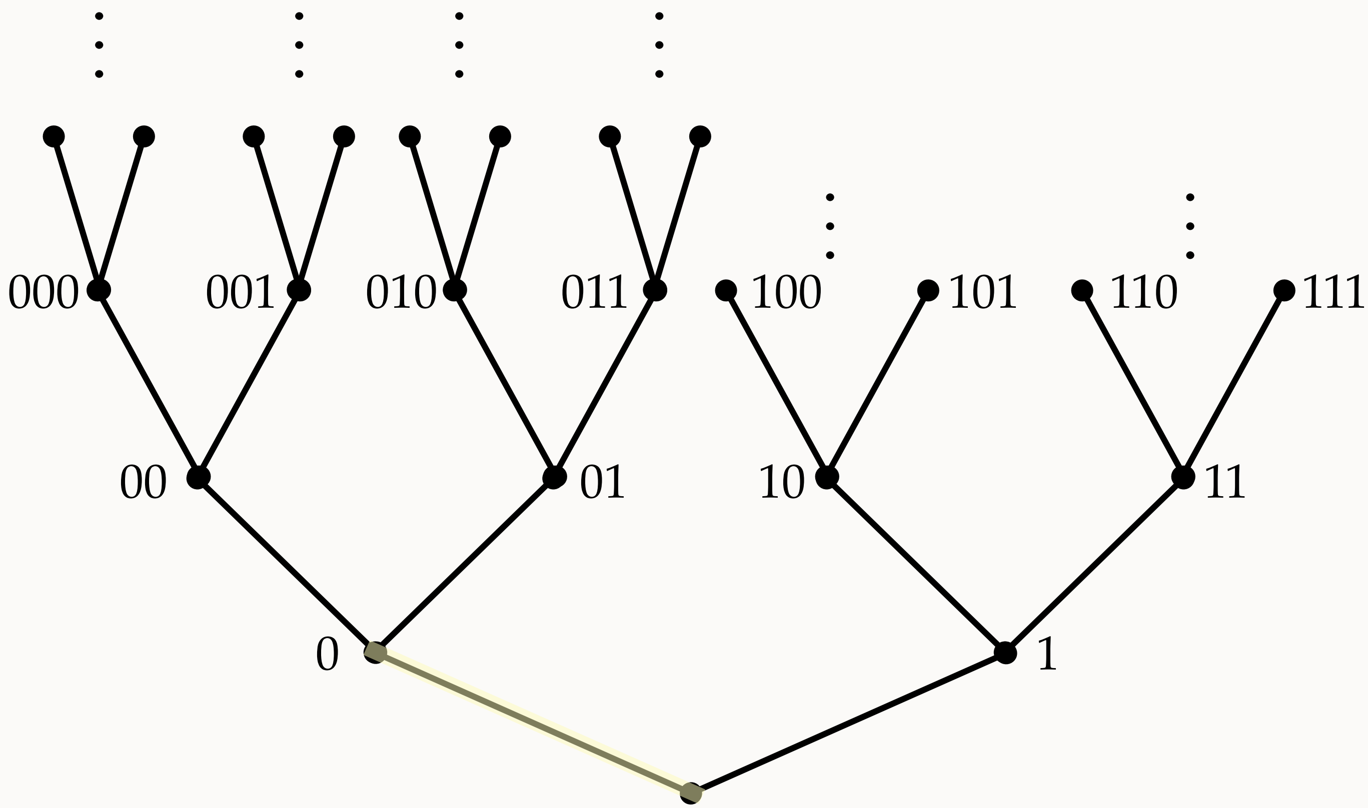


$$\sum_{\sigma \in U_1} 2^{-|\sigma|} \leq \frac{1}{2} \qquad \sum_{\sigma \in U_2} 2^{-|\sigma|} \leq \frac{1}{4} \qquad \sum_{\sigma \in U_3} 2^{-|\sigma|} \leq \frac{1}{8}$$

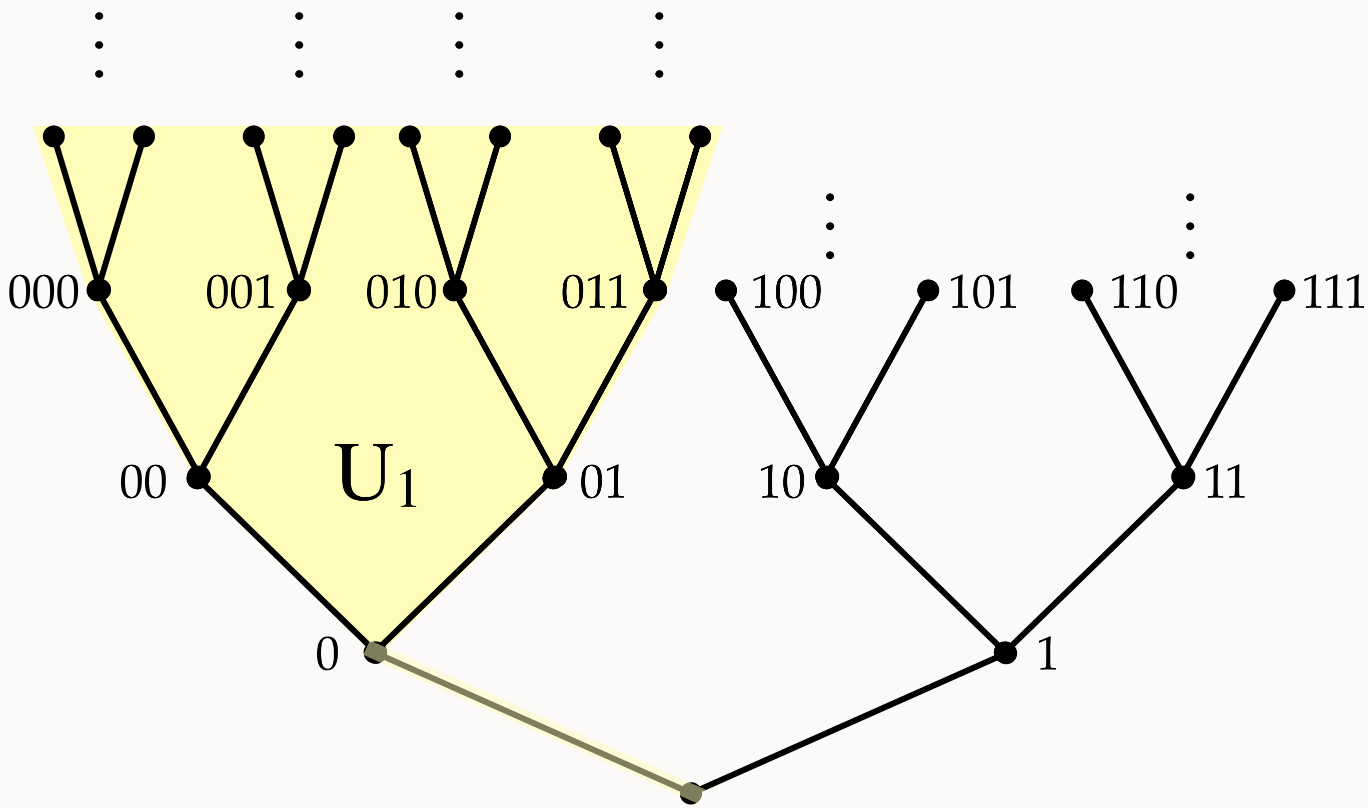
A CONCRETE EXAMPLE



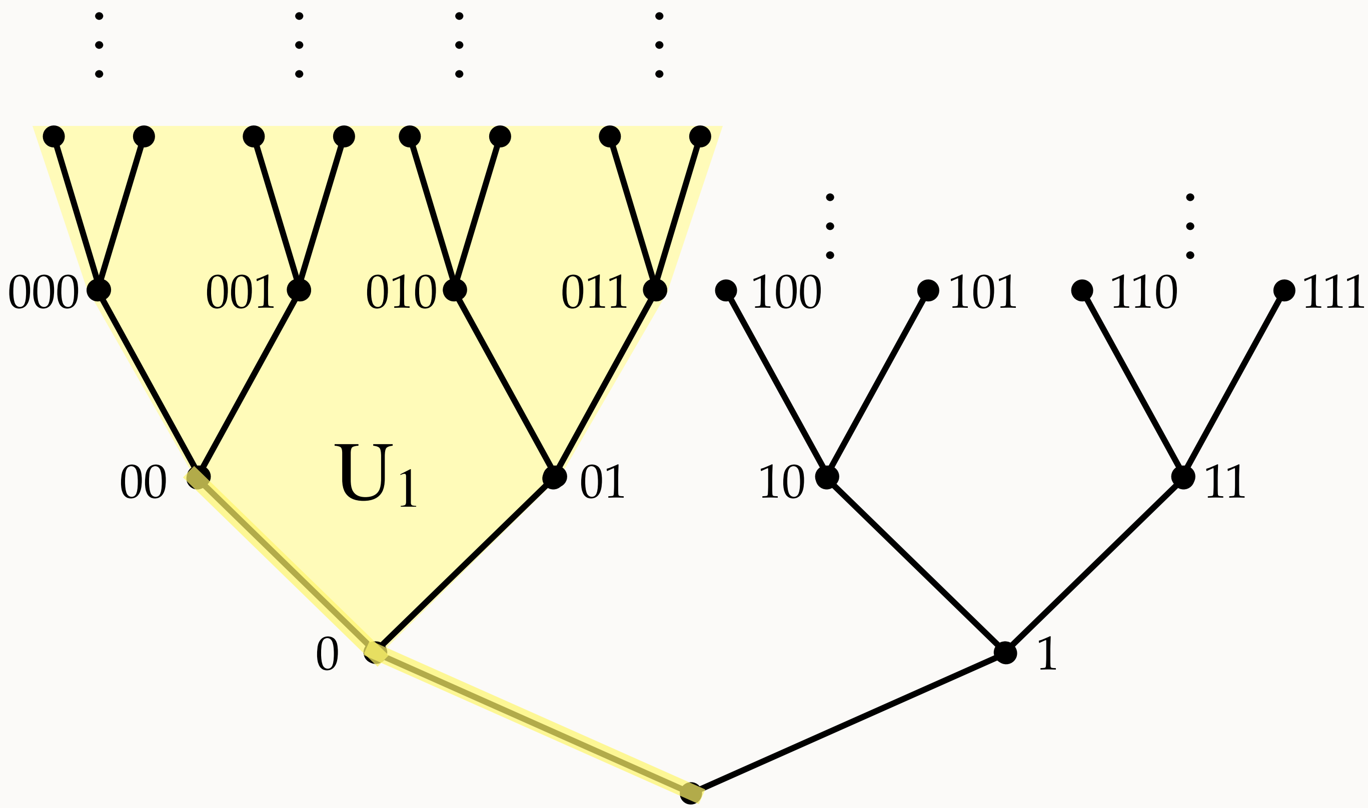
A CONCRETE EXAMPLE



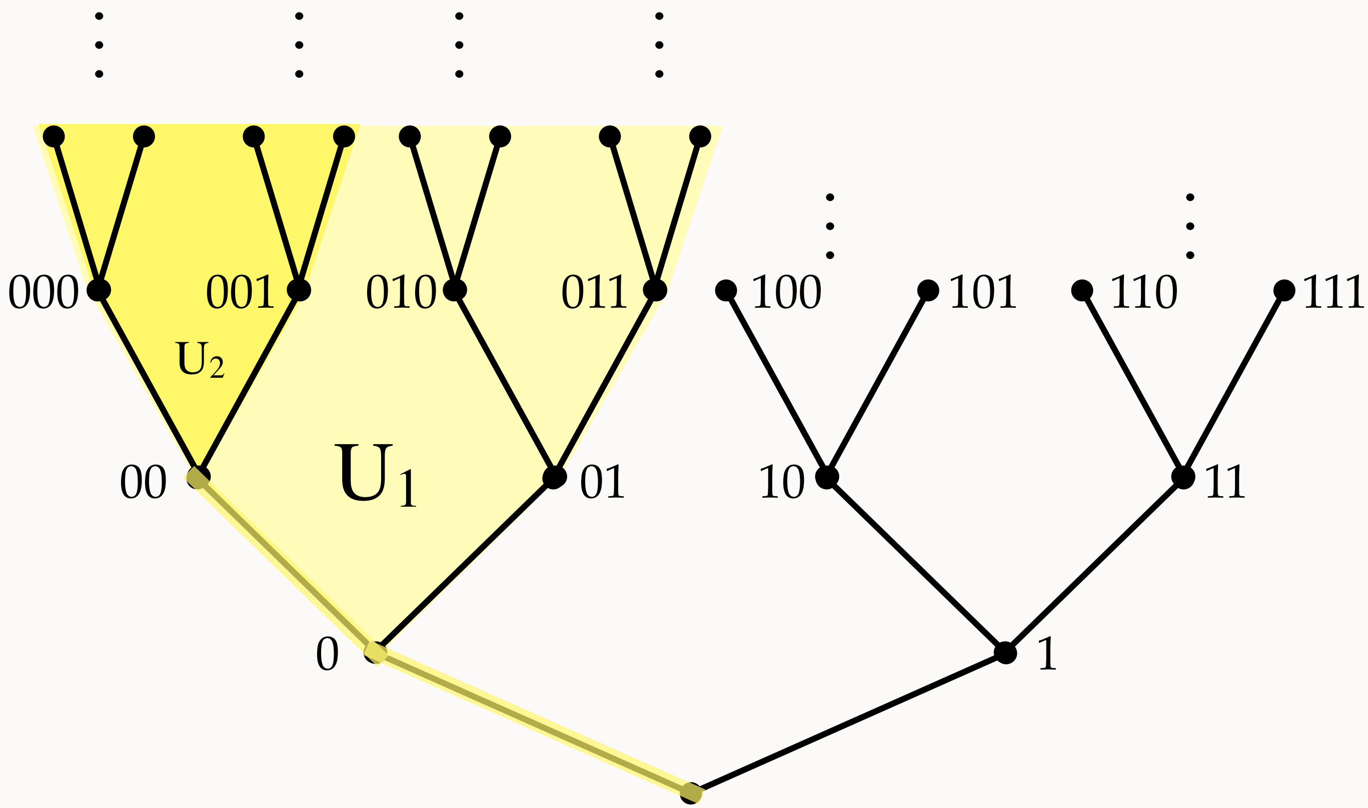
A CONCRETE EXAMPLE



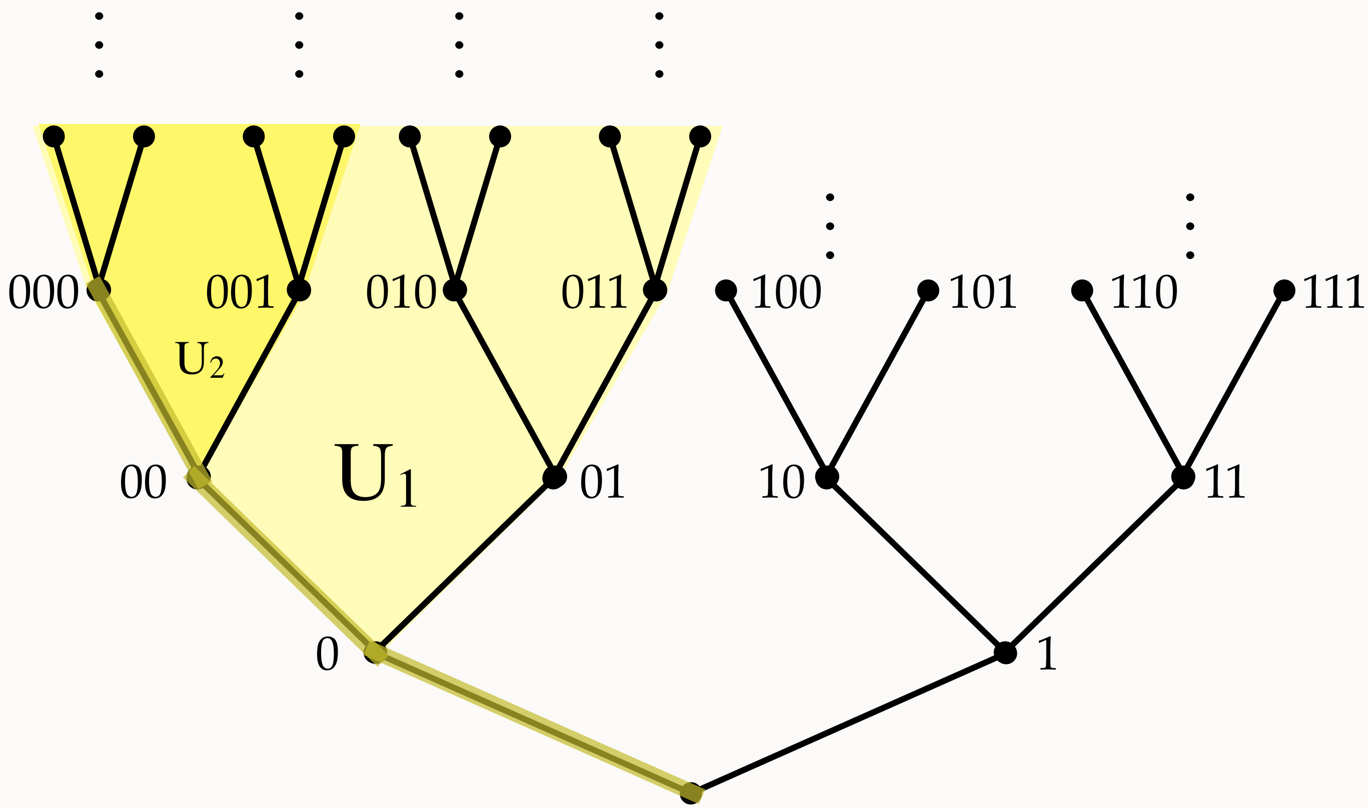
A CONCRETE EXAMPLE



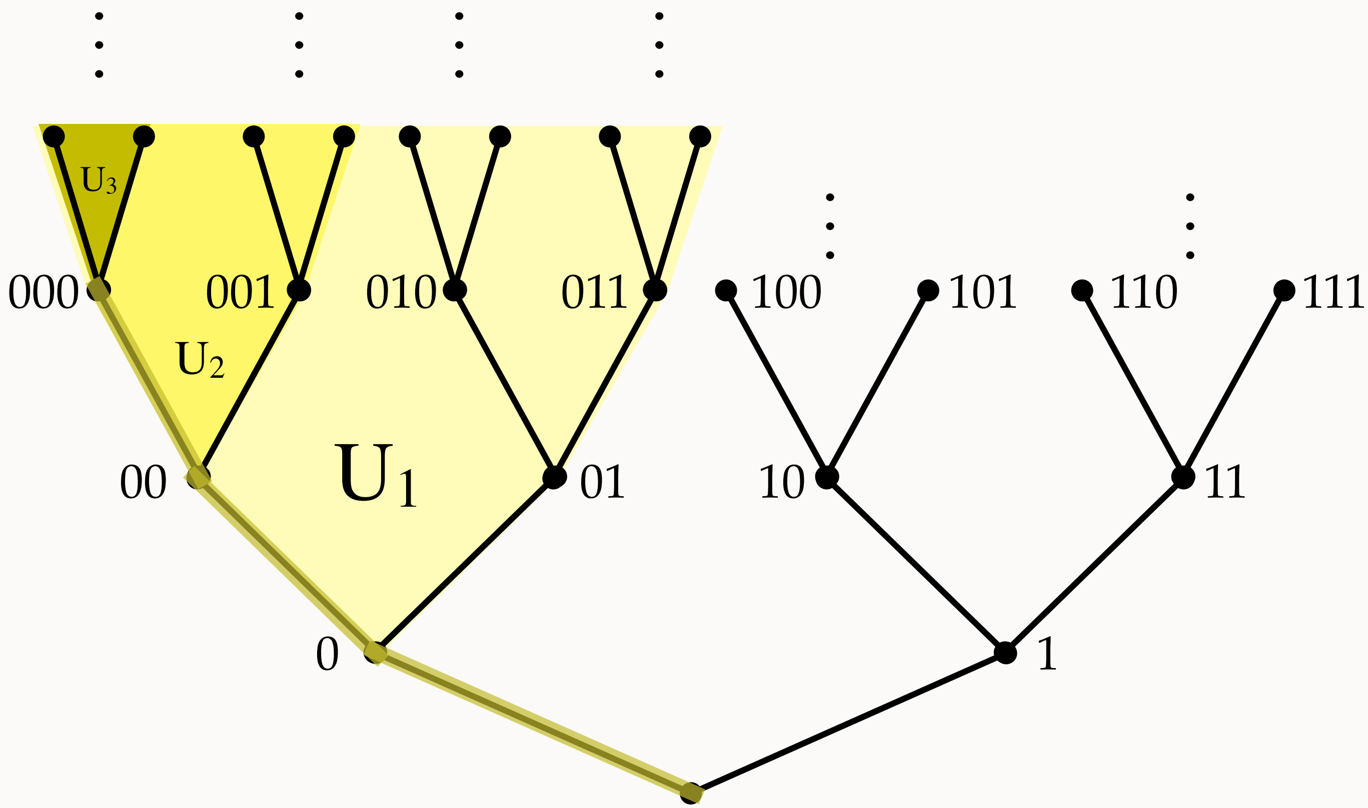
A CONCRETE EXAMPLE



A CONCRETE EXAMPLE



A CONCRETE EXAMPLE



MARTIN-LÖF RANDOMNESS

Let $(\mathcal{U}_n)_{n\in\mathbb{N}}$ be a Martin-Löf test. $X \in 2^\omega$ passes the test if

$$X \notin \bigcap_{i\in\mathbb{N}} \mathcal{U}_i.$$

Further, $X \in 2^\omega$ is ***Martin-Löf random*** if X passes every Martin-Löf test.

The development of this definition was considered to be a significant achievement.

But how does it relate to Kolmogorov complexity?

A PARTIAL RESULT

Recall that Martin-Löf proved that for every $X \in 2^\omega$, there are infinitely many n such that

$$C(X\restriction n) \leq n - log(n).$$

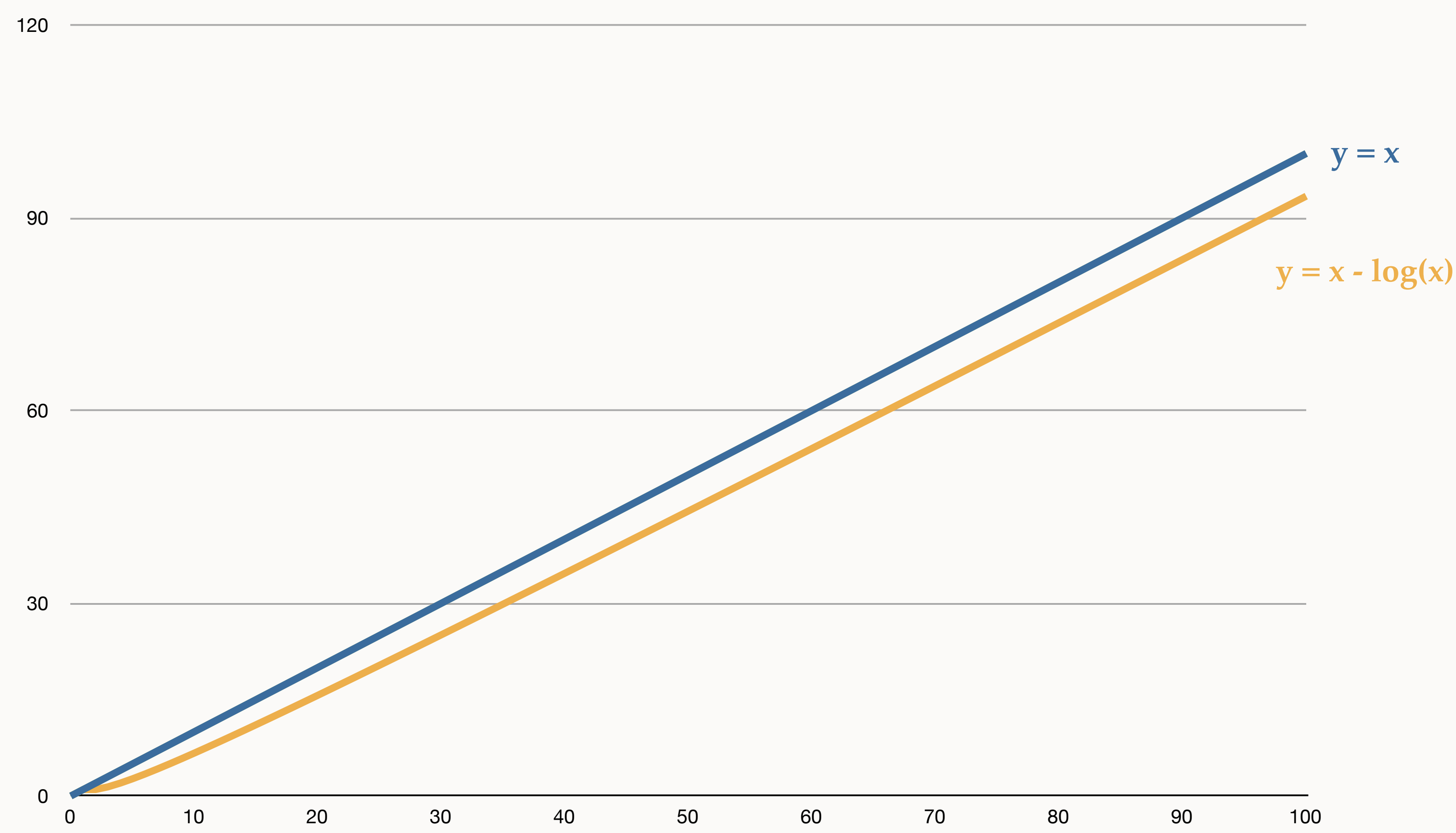
However, he also proved:

Theorem: For $X \in 2^\omega$, if there is some c such that

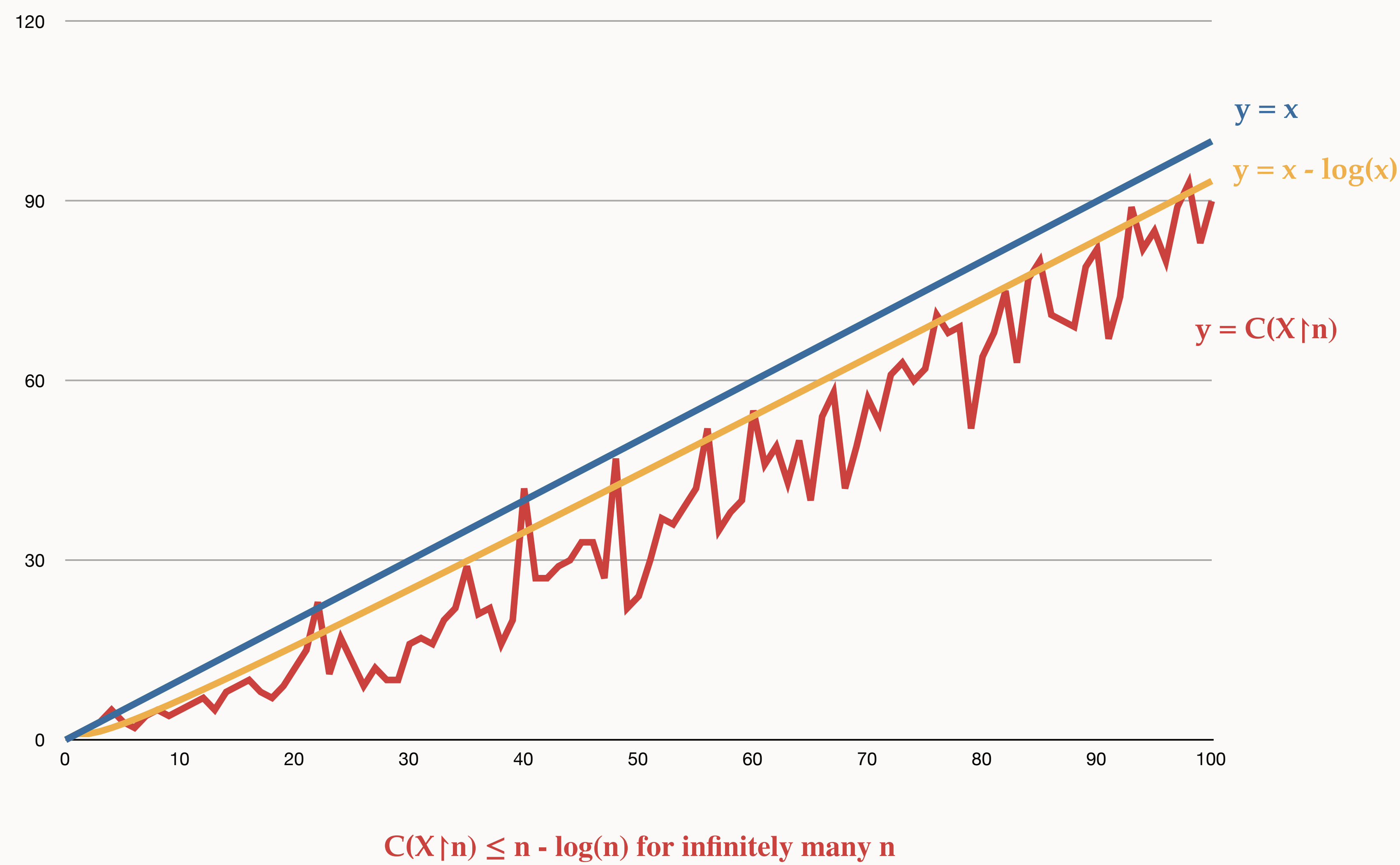
$$C(X\restriction n) \geq n - c$$

for infinitely many n, then X is Martin-Löf random.

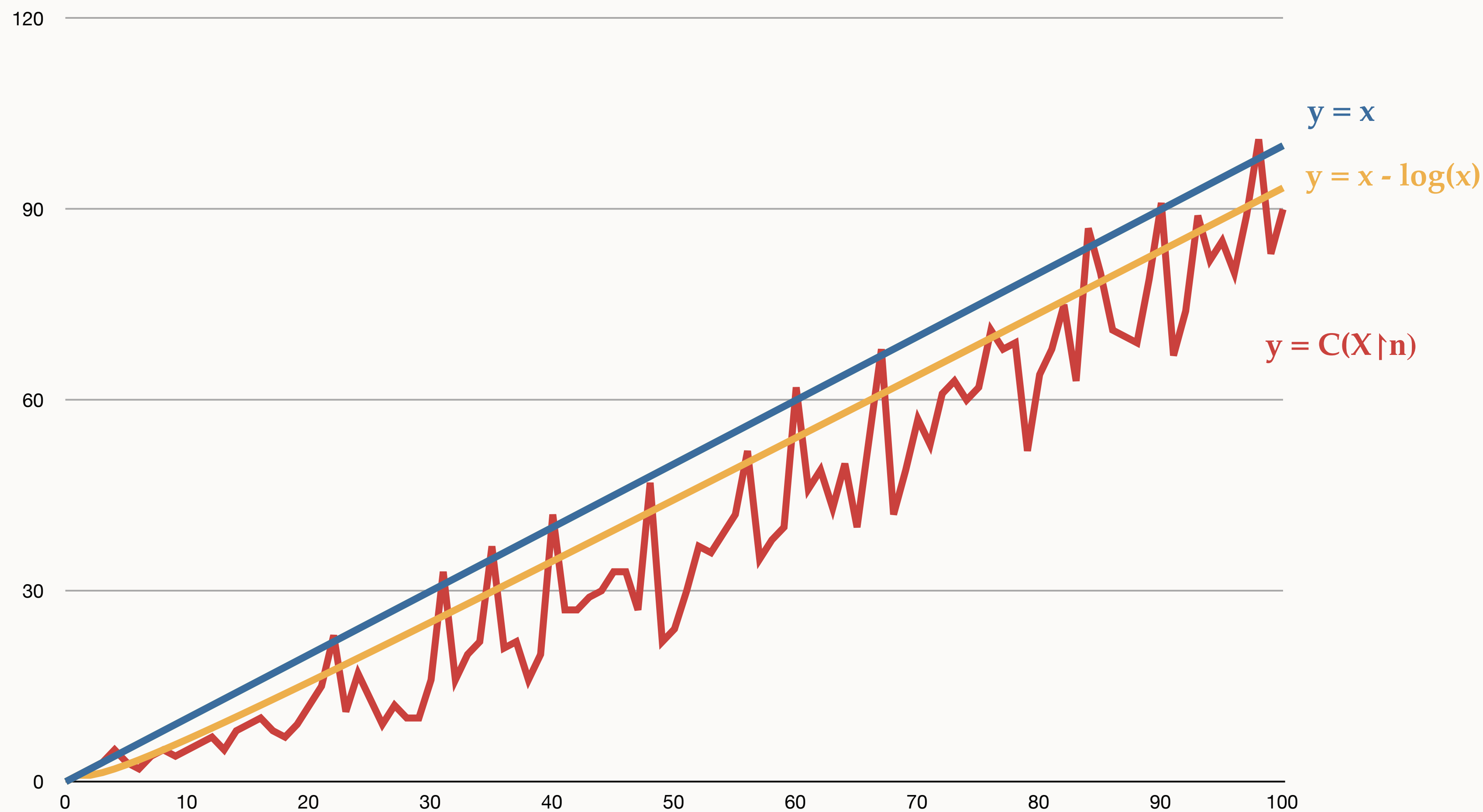
He was unable to prove the converse.



120
90
60
30
0
0
10
20
30
40
50
60
70
80
90
100
y = x
y = x - log(x)



120
90
60
30
0
0
10
20
30
40
50
60
70
80
90
100
y = x
y = x - log(x)
y = C(X↾n)
C(X↾n) ≤ n - log(n) for infinitely many n



$C(X\upharpoonright n) \geq n - c$ for infinitely many n

THE LEVIN-SCHNORR THEOREM

THE NEXT STEP

To determine the exact relationship between Kolmogorov complexity and Martin-Löf randomness, progress was made by slightly modifying the definition of Kolmogorov complexity.

Instead of defining Kolmogorov complexity in terms of *all* machines, the key step was to restrict the collection to some proper sub-collection.

Both Levin and Schnorr took this approach.

PREFIX-FREE MACHINES

A machine $M : 2^{<\omega} \to 2^{<\omega}$ is ***prefix-free*** if for every $\sigma, \tau \in 2^{<\omega}$, if $\sigma \prec \tau$ and $M(\sigma)\downarrow$, then $M(\tau)\uparrow$.

Let $(M_i)_{i\in\mathbb{N}}$ be an effective enumeration of all prefix-free machines.

We can define a universal prefix-free machine $U : 2^{<\omega} \to 2^{<\omega}$ as before:

$$U(1^i 0\sigma) \simeq M_i(\sigma)$$

The optimality theorem and the invariance theorem also hold for universal prefix-free machines.

PREFIX-FREE KOLMOGOROV COMPLEXITY

Now we can define prefix-free Kolmogorov complexity:

Let U be a universal prefix-free machine.

Then the ***prefix-free Kolmogorov complexity*** of τ is defined to be

$$K(\tau) = \min\{|\sigma| : U(\sigma)\downarrow = \tau\}.$$

SEVERAL IMPORTANT FACTS

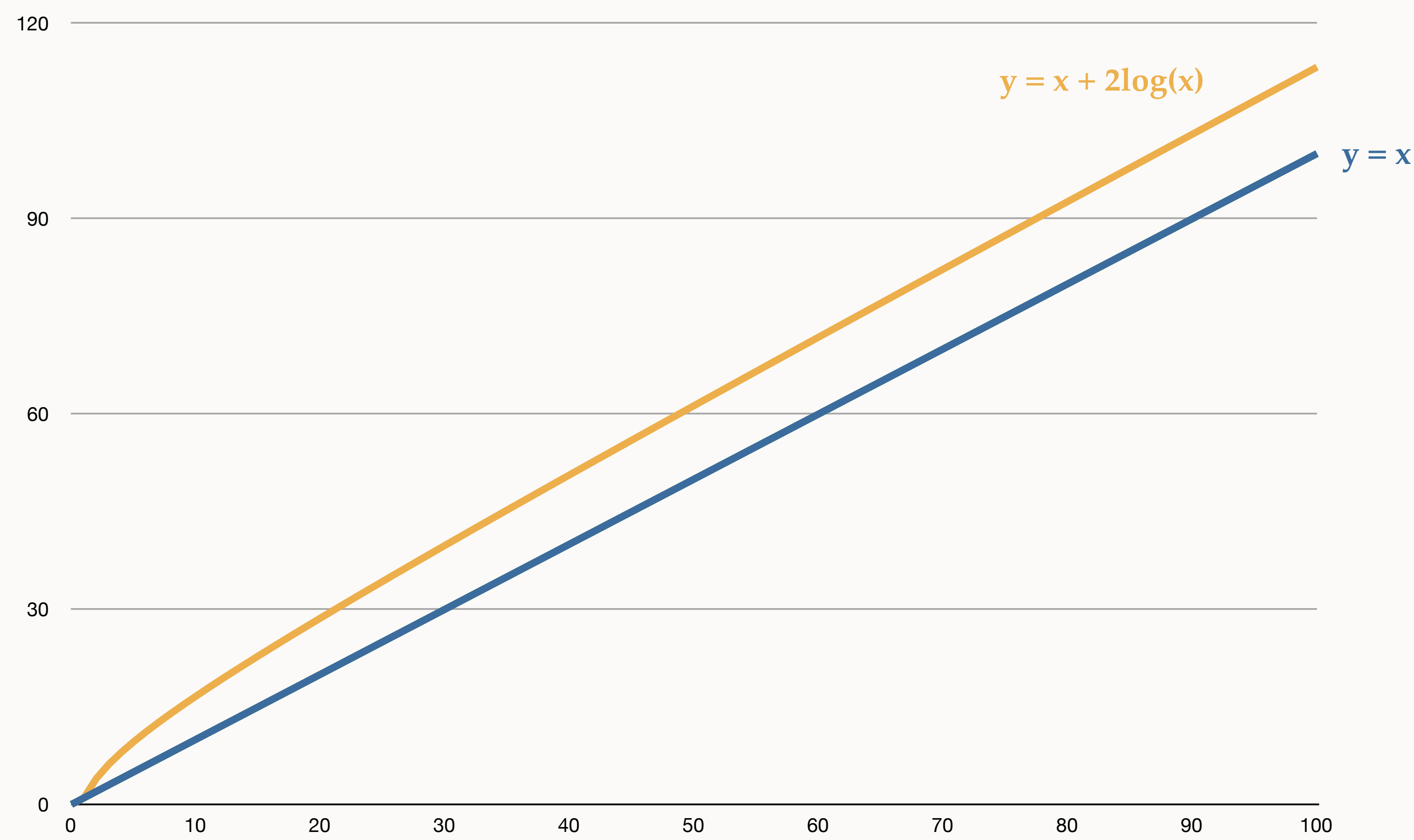
There exists some constant c such that for every $\sigma \in 2^{<\omega}$,

$$K(\sigma) \leq |\sigma| + 2\log(|\sigma|) + c.$$

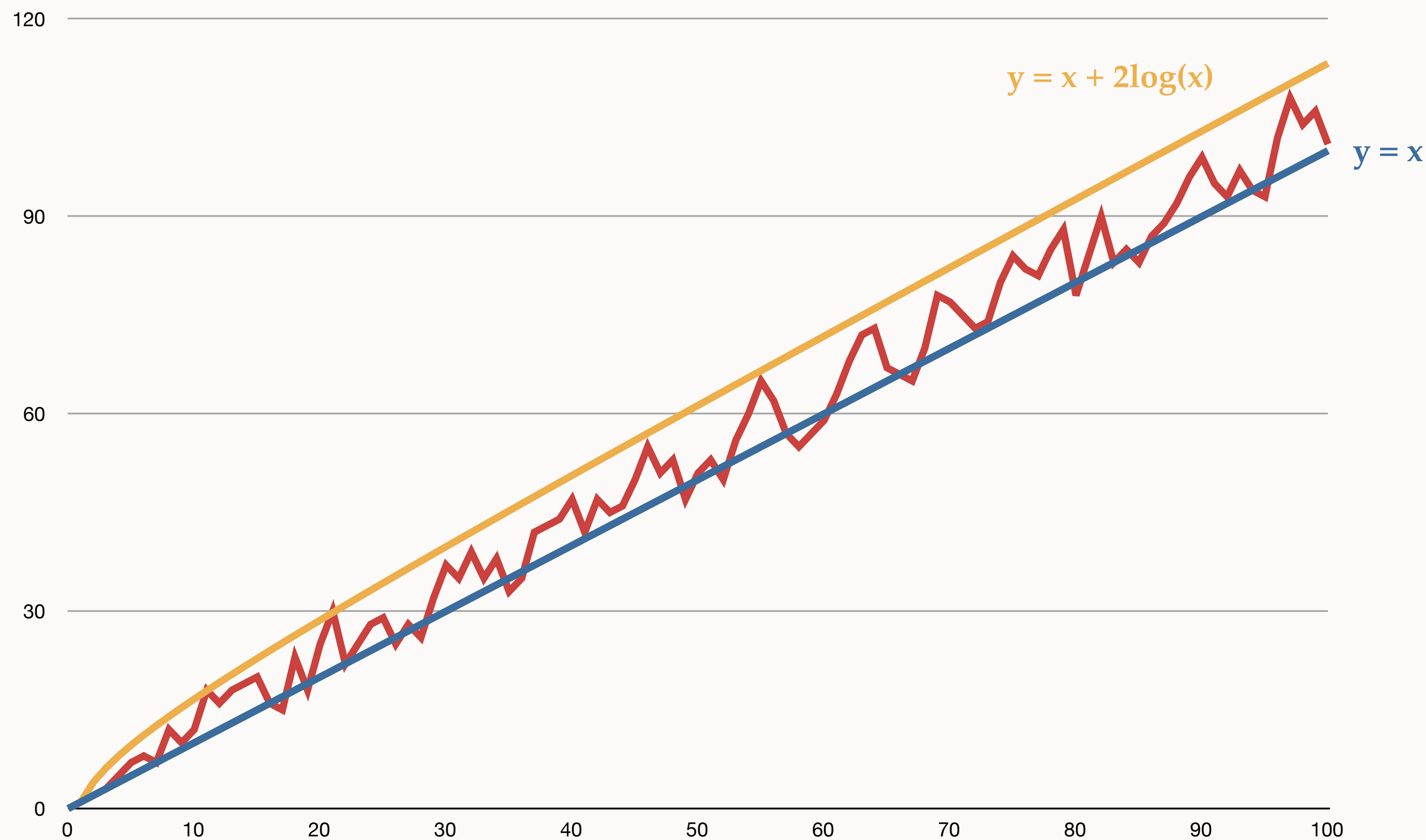
Further, the collection of $X \in 2^{\omega}$ such that

$$(\exists c)(\forall n) K(X \upharpoonright n) \geq n - c$$

is non-empty.



y = x + 2log(x)
y = x
120
90
60
30
0
0
10
20
30
40
50
60
70
80
90
100



K(X↾n) ≥ n-3 for all n

THE LEVIN-SCHNORR THEOREM

Theorem: For $X \in 2^\omega$,

$$(\exists c)(\forall n) K(X \upharpoonright n) \geq n - c$$

if and only if X is Martin-Löf random.

COMPRESSIBLE $\Rightarrow$ ATYPICAL

Suppose we have a sequence X such that for every *c*, at least one initial segment of *X* is *c*-compressible.

That is, for every *c* there is some *n* such that

$$K(X \upharpoonright n) < n - c.$$

Then we define a sequence $(\mathcal{U}_n)_{n \in \mathbb{N}}$ of subsets of 2^ω as follows:

$$\mathcal{U}_c = \{X \in 2^\omega : (\exists k)[K(X \upharpoonright k) \leq k - c]\}$$

Key insight: $(\mathcal{U}_n)_{n \in \mathbb{N}}$ is a Martin-Löf test.

ATYPICAL $\Rightarrow$ COMPRESSIBLE, 1

For $X \in 2^\omega$, suppose there is some Martin-Löf test $(\mathcal{U}_n)_{n\in\mathbb{N}}$ such that

$$X \in \bigcap_{i\in\mathbb{N}} \mathcal{U}_i.$$

It is not obvious how to proceed here.

- We'd like to show that sequences that are contained in $\bigcap_{i\in\mathbb{N}} \mathcal{U}_i$ can be compressed.
- The problem is that it's not clear which machine we should use to compress these sequences.

ATYPICAL $\Rightarrow$ COMPRESSIBLE, 2

The solution: We build the machine ourselves!

By the definition $(\mathcal{U}_n)_{n\in\mathbb{N}}$, the finite sequences that determine each $\mathcal{U}_i$ must be getting longer and longer.

Note that if $X \in \mathcal{U}_i$, then this is due to some $X\restriction k$ being enumerated in the corresponding critical region.

Thus, for any $Y \in 2^\omega$ such that $X\restriction k \prec Y$, it follows that $Y \in \mathcal{U}_i$.

ATYPICAL $\Rightarrow$ COMPRESSIBLE, 3

The idea, then, is to define a machine that compresses any sequence the initial segments of which appear in each of the $\mathcal{U}_i$'s.

In fact, for every sequence $X \in \mathcal{U}_{2i}$, our machine will compress some initial segment of X by roughly i bits.

ATYPICAL $\Rightarrow$ COMPRESSIBLE, 4

We appeal to a more general result:

Suppose we can effectively list a sequence of pairs (n, σ), where each pair can be seen as a request. For the pair (n, σ), we are requesting that a sequence of length n be mapped to σ.

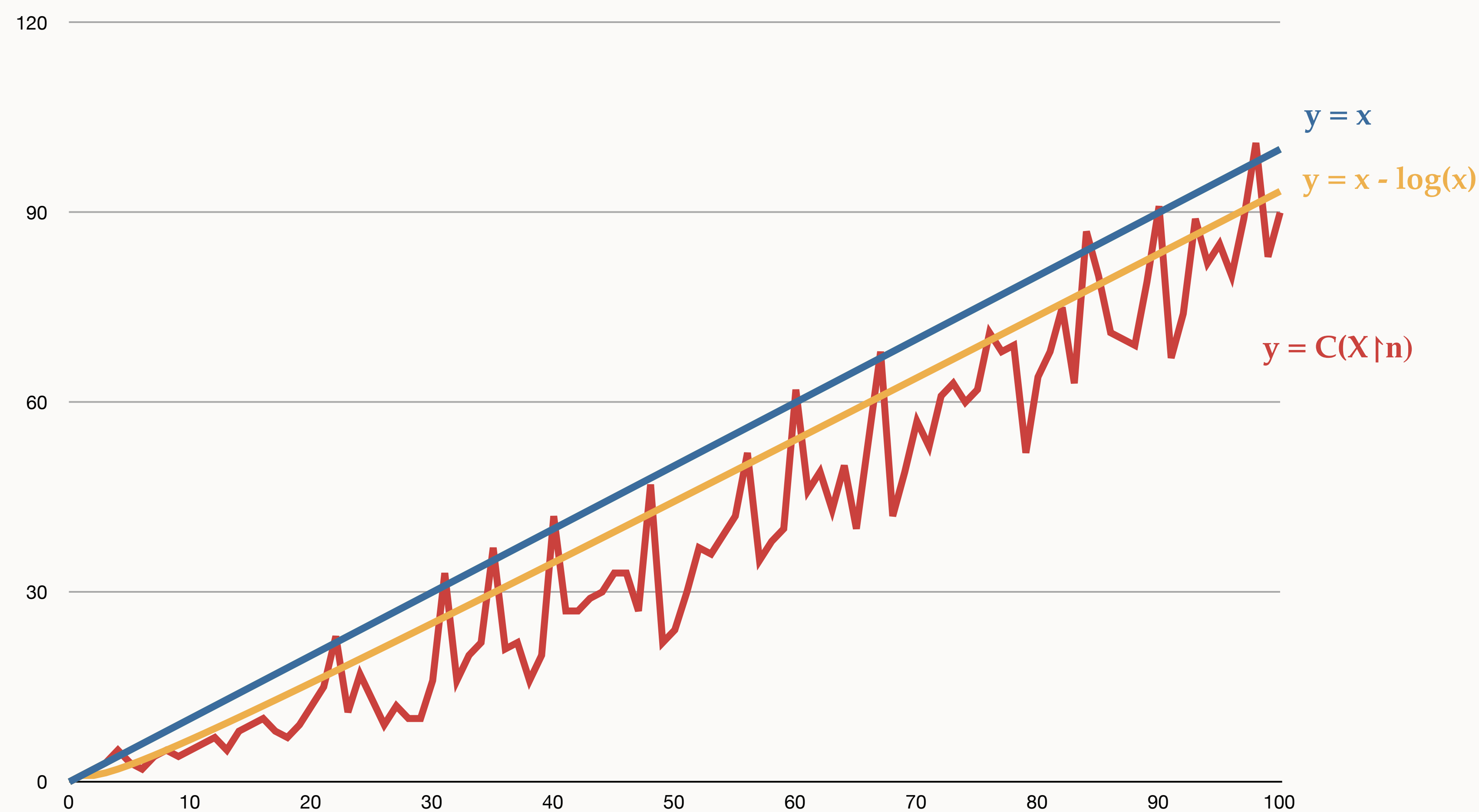
Then as long as our requests satisfy a certain technical condition, then we can build a machine that meets all of our requests.

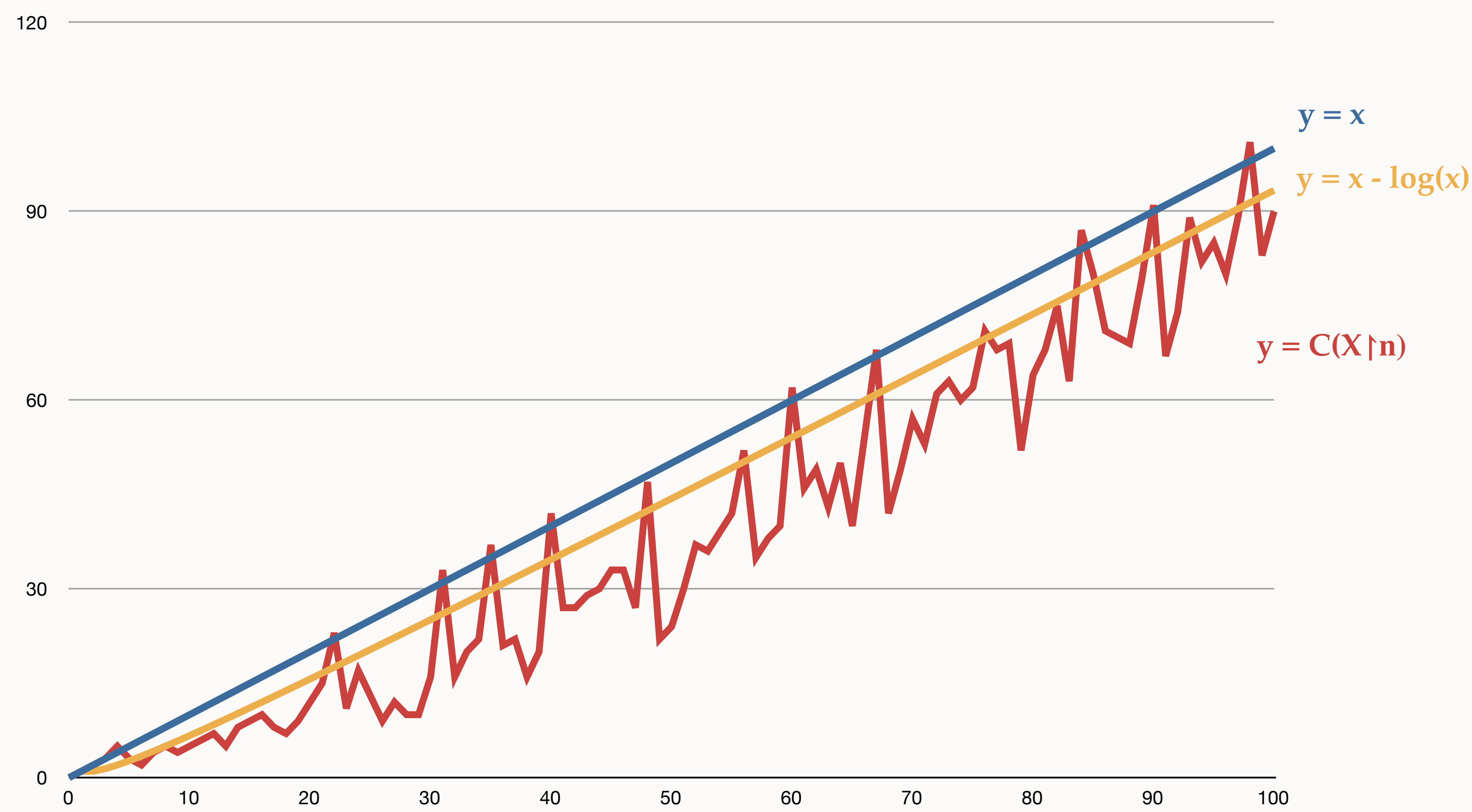
ONE LAST MATTER

What about the sequences $X \in 2^\omega$ for which there is some c such that

$$C(X\restriction n) \geq n - c$$

for infinitely many n?


120
90
60
30
0
0
10
20
30
40
50
60
70
80
90
100
y = x
y = x - log(x)
y = C(X↾n)



C(X↾n) ≥ n - c for infinitely many n

ONE LAST MATTER

What about the sequences $X \in 2^\omega$ for which there is some c such that

$$C(X{\upharpoonright}n) \geq n - c$$

for infinitely many n?

This condition determines a *stronger* notion of randomness: If we define Martin-Löf randomness relative to the halting set $K = \{e : \phi_e(e)\downarrow\}$ as an oracle, we have what is known as ***2-randomness***.

CHARACTERIZING 2-RANDOMNESS

Theorem: (Nies, Stephan, Terwijn; Miller) For $X \in 2^\omega$, there is some c such that

$$C(X \restriction n) \geq n - c$$

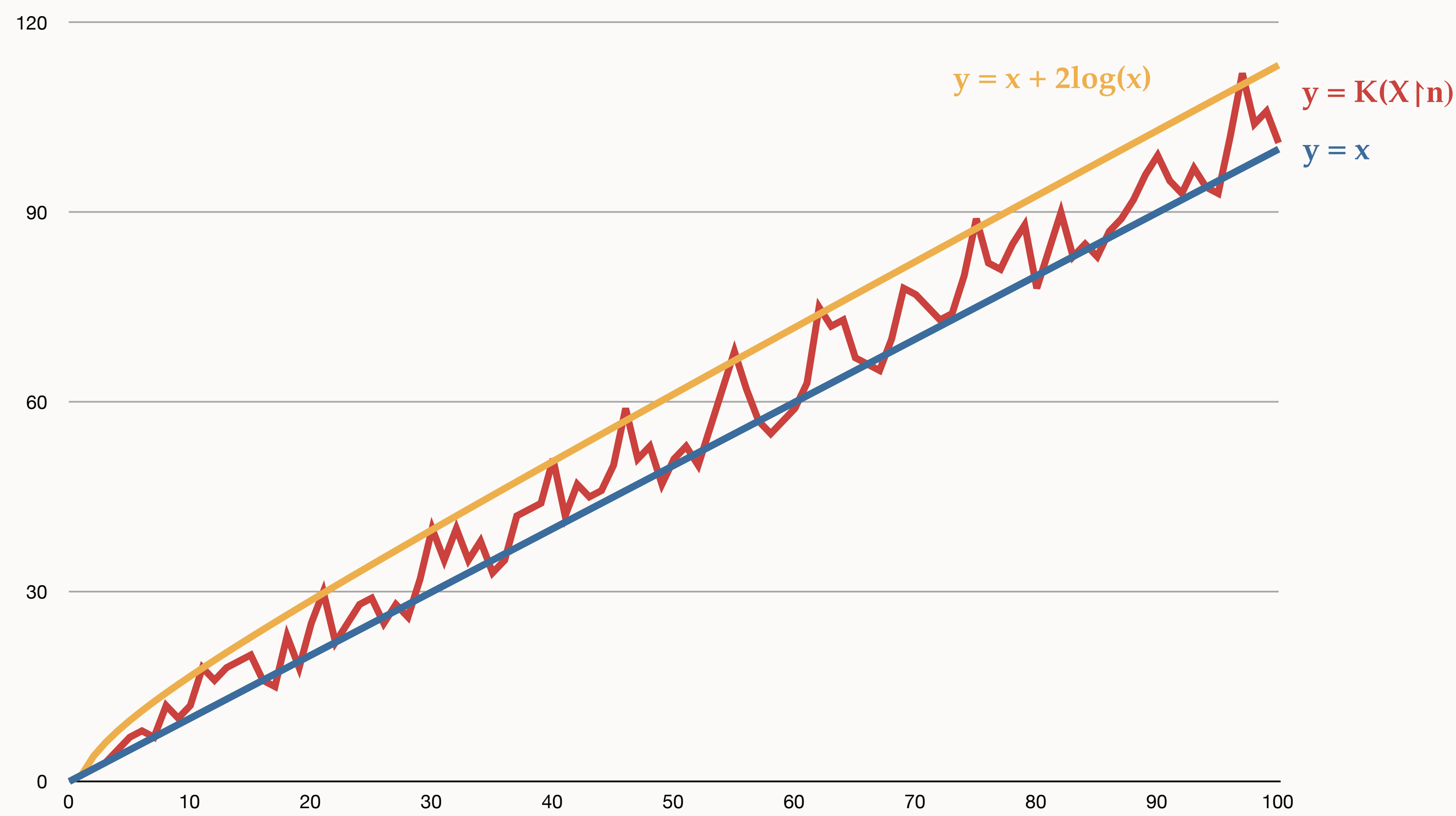
for infinitely many n if and only if X is 2-random.

ANOTHER CHARACTERIZATION

Theorem: (Miller) For $X \in 2^\omega$, there is some c such that

$$K(X\restriction n) \geq n + K(n) - c$$

for infinitely many n if and only if X is 2-random.



120
90
60
30
0
0
10
20
30
40
50
60
70
80
90
100
y = x + 2log(x)
y = K(X↾n)
y = x

Thank you for your attention!