

Alan Turing in the Twenty-first Century: Normal Numbers, Randomness, and Finite Automata

Jack Lutz

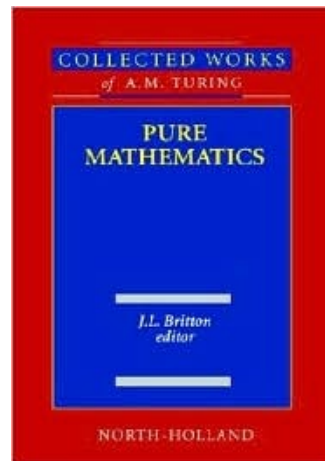
Iowa State University

Main reference

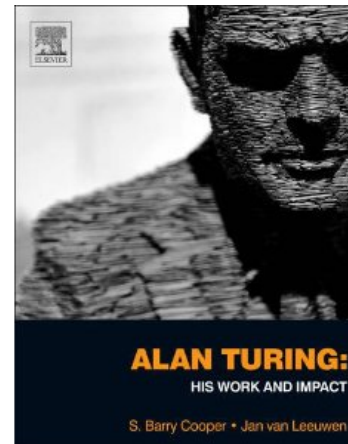


A note on normal numbers

in

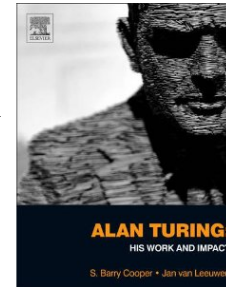


and



Main references on main reference

- V. Becher, Turing's note on normal numbers, in
- V. Becher, S. Figueira, and R. Picchi, Turing's unpublished algorithm for normal numbers, *Theoretical Computer Science* (2007).



Turing's note on normal numbers is over 75 years old.

Turing's note on normal numbers is over 75 years old.

It was not published in his lifetime.

Turing's note on normal numbers is over 75 years old.

It was not published in his lifetime.

We are research scientists, not historians.

Turing's note on normal numbers is over 75 years old.

It was not published in his lifetime.

We are research scientists, not historians.

Why should we care about it?

Turing's note on normal numbers is over 75 years old.

It was not published in his lifetime.

We are research scientists, not historians.

Why should we care about it?

Today's topic: Why we should care.

Outline

1. Normal Numbers
2. Explicit Constructions
3. Normality and Finite Automata
4. Conclusion

Normal Numbers

Definition (Borel 1909). Let $\alpha \in \mathbb{R}$ and $2 \leq b \in \mathbb{N}$.

Normal Numbers

Definition (Borel 1909). Let $\alpha \in \mathbb{R}$ and $2 \leq b \in \mathbb{N}$.

1. α is normal in base b if, for every $m \geq 1$ and every $w \in \{0, \dots, b - 1\}^m$, the asymptotic, empirical frequency of w in the base- b expansion of α is b^{-m} .

Normal Numbers

Definition (Borel 1909). Let $\alpha \in \mathbb{R}$ and $2 \leq b \in \mathbb{N}$.

1. α is normal in base b if, for every $m \geq 1$ and every $w \in \{0, \dots, b - 1\}^m$, the asymptotic, empirical frequency of w in the base- b expansion of α is b^{-m} .
2. α is absolutely normal if it is normal in every base $b \geq 2$.

Theorem (Borel 1909). Almost every real number is absolutely normal.

Theorem (Borel 1909). Almost every real number is absolutely normal.

Question (Steinhaus). Can a number be normal in one base but not in another?

Theorem (Borel 1909). Almost every real number is absolutely normal.

Question (Steinhaus). Can a number be normal in one base but not in another?

Answer (Cassels 1959, Schmidt 1960). Yes!

So absolutely normal numbers are commonplace.

What are some examples?

So absolutely normal numbers are commonplace.

What are some examples?

Widely conjectured natural examples:

$$\pi, e, \sqrt{2}, \ln 2, \zeta(3)$$

So absolutely normal numbers are commonplace.

What are some examples?

Widely conjectured natural examples:

$\pi, e, \sqrt{2}, \ln 2, \zeta(3)$

Every irrational algebraic number

So absolutely normal numbers are commonplace.

What are some examples?

Widely conjectured natural examples:

$$\pi, e, \sqrt{2}, \ln 2, \zeta(3)$$

Every irrational algebraic number

But no natural example has been proven to be normal, even in a single base!

So absolutely normal numbers are commonplace.

What are some examples?

Widely conjectured natural examples:

$$\pi, e, \sqrt{2}, \ln 2, \zeta(3)$$

Every irrational algebraic number

But no natural example has been proven to be normal, even in a single base!

(Bailey & Crandall 2001 proposed a dynamical hypothesis that implies the base-2 normality of $\pi, \sqrt{2}, \ln 2, \zeta(3)$.)

Explicit Constructions (Non-natural examples)

Explicit Constructions (Non-natural examples)

Sierpinski and Lebesgue 1917: Intricate limiting construction of absolutely normal numbers. No complexity analysis.

Explicit Constructions (Non-natural examples)

Sierpinski and Lebesgue 1917: Intricate limiting construction of absolutely normal numbers. No complexity analysis.

Theorem (Champernowne 1933). The real number whose decimal expansion is $0.1234567891011121314\dots$ is normal in base 10.

Explicit Constructions (Non-natural examples)

Sierpinski and Lebesgue 1917: Intricate limiting construction of absolutely normal numbers. No complexity analysis.

Theorem (Champernowne 1933). The real number whose decimal expansion is $0.1234567891011121314\dots$ is normal in base 10.

This and similar ideas work in any base ...

Explicit Constructions (Non-natural examples)

Sierpinski and Lebesgue 1917: Intricate limiting construction of absolutely normal numbers. No complexity analysis.

Theorem (Champernowne 1933). The real number whose decimal expansion is $0.1234567891011121314\dots$ is normal in base 10.

This and similar ideas work in any base ...

... but not in all bases. How do we explicitly construct absolutely normal numbers?

ALAN TURING YEAR



“Although it is known that almost all numbers are [absolutely] normal no example of [an absolutely] normal number has ever been given. I propose to show how [absolutely] normal numbers may be constructed and to prove that almost all numbers are [absolutely] normal constructively.”



“Although it is known that almost all numbers are [absolutely] normal no example of [an absolutely] normal number has ever been given. I propose to show how [absolutely] normal numbers may be constructed and to prove that almost all numbers are [absolutely] normal constructively.”

So Turing seems not to have known about the constructions by Sierpinski and Lebesgue.



“Although it is known that almost all numbers are [absolutely] normal no example of [an absolutely] normal number has ever been given. I propose to show how [absolutely] normal numbers may be constructed and to prove that almost all numbers are [absolutely] normal constructively.”

So Turing seems not to have known about the constructions by Sierpinski and Lebesgue.

But let's look at that second sentence.

ALAN TURING YEAR



“I propose to show how [absolutely] normal numbers may be constructed and to prove that almost all numbers are [absolutely] normal constructively.”



“I propose to show how [absolutely] normal numbers may be constructed and to prove that almost all numbers are [absolutely] normal constructively.”

What Turing really did was to first
prove that almost all numbers are [absolutely] normal
constructively



“I propose to show how [absolutely] normal numbers may be constructed and to prove that almost all numbers are [absolutely] normal constructively.”

What Turing really did was to first
prove that almost all numbers are [absolutely] normal
constructively

and then trivially derive
how [absolutely] normal numbers may be constructed.



“I propose to show how [absolutely] normal numbers may be constructed and to prove that almost all numbers are [absolutely] normal constructively.”

What Turing really did was to first
prove that almost all numbers are [absolutely] normal
constructively

and then trivially derive
how [absolutely] normal numbers may be constructed.

This is the visionary content of Turing’s note!

For Turing, “constructive” means computable.

For Turing, “constructive” means computable.

His proof — with corrections by Becher, Figueira, and Picchi (2007) — shows that the set of reals that are not absolutely normal has computable measure 0...

For Turing, “constructive” means computable.

His proof — with corrections by Becher, Figueira, and Picchi (2007) — shows that the set of reals that are not absolutely normal has computable measure 0...

... thereby yielding constructions of computable real numbers that are absolutely normal.

Turing's Vision



Placing computability constraints on a nonconstructive theory like Lebesgue measure seems a priori to weaken the theory, but it may strengthen the theory for some purposes

Turing's Vision



Placing computability constraints on a nonconstructive theory like Lebesgue measure seems a priori to weaken the theory, but it may strengthen the theory for some purposes

This vision is crucial for present-day investigations of
individual random sequences,
dimensions of individual sequences,
measure and category in complexity classes,
etc.

What do we know in 2012 about explicit constructions of absolutely normal numbers?

What do we know in 2012 about explicit constructions of absolutely normal numbers?

Definition. A martingale is a function

$$d: \{0,1\}^* \rightarrow [0, \infty)$$

satisfying

$$d(w) = \frac{d(w0)+d(w1)}{2}$$

for all $w \in \{0,1\}^*$.

What do we know in 2012 about explicit constructions of absolutely normal numbers?

Definition. A martingale is a function

$$d: \{0,1\}^* \rightarrow [0, \infty)$$

satisfying

$$d(w) = \frac{d(w0) + d(w1)}{2}$$

for all $w \in \{0,1\}^*$.

A martingale d succeeds on a sequence $S \in \{0,1\}^\infty$ if

$$\limsup_{w \rightarrow S} d(w) = \infty .$$

Definition. A real $\alpha \in \mathbb{R}$ is polynomial time computable, and we write $\alpha \in P_{\mathbb{R}}$, if there is a function $\hat{\alpha}: \mathbb{N} \rightarrow \mathbb{Q}$ such that

- (i) for all $r \in \mathbb{N}$, $|\hat{\alpha}(r) - \alpha| \leq 2^{-r}$, and
- (ii) $\hat{\alpha}(r)$ is computable in time polynomial in r .

Definition. A real $\alpha \in \mathbb{R}$ is polynomial time computable, and we write $\alpha \in P_{\mathbb{R}}$, if there is a function $\hat{\alpha}: \mathbb{N} \rightarrow \mathbb{Q}$ such that

- (i) for all $r \in \mathbb{N}$, $|\hat{\alpha}(r) - \alpha| \leq 2^{-r}$, and
- (ii) $\hat{\alpha}(r)$ is computable in time polynomial in r .

Definition. A set $X \subseteq \mathbb{R}$ has measure 0 in $P_{\mathbb{R}}$, and we write $\mu(X|P_{\mathbb{R}}) = 0$, if there is a polynomial time computable martingale d that succeeds on (the binary expansion of) every element of X .

Theorem (Lutz 1992, 1998). This makes sense.

Theorem (Lutz 1992, 1998). This makes sense.

It gives a coherent notion of measure in $P_{\mathbb{R}}$. The sets X with $\mu(X|P_{\mathbb{R}}) = 0$ form a “polynomial time ideal” in $P_{\mathbb{R}}$, and this ideal is proper, i.e. $\mu(P_{\mathbb{R}}|P_{\mathbb{R}}) \neq 0$.

Theorem (Lutz 1992, 1998). This makes sense.

It gives a coherent notion of measure in $P_{\mathbb{R}}$. The sets X with $\mu(X|P_{\mathbb{R}}) = 0$ form a “polynomial time ideal” in $P_{\mathbb{R}}$, and this ideal is proper, i.e. $\mu(P_{\mathbb{R}}|P_{\mathbb{R}}) \neq 0$.

The measure conservation theorem that proves $\mu(P_{\mathbb{R}}|P_{\mathbb{R}}) \neq 0$ gives an explicit construction, from any polynomial time computable martingale d , of a real $\alpha \in P_{\mathbb{R}}$ on which d does not succeed.

Theorem (Strauss 1997). Almost every polynomial time computable real number is absolutely normal. That is, if X is the set of reals that are not absolutely normal, then $\mu(X|P_{\mathbb{R}}) = 0$.

Theorem (Strauss 1997). Almost every polynomial time computable real number is absolutely normal. That is, if X is the set of reals that are not absolutely normal, then $\mu(X|P_{\mathbb{R}}) = 0$.

Combining Strauss's proof with the measure conservation theorem gives explicit constructions of reals in $P_{\mathbb{R}}$ that are absolutely normal.

Theorem (Strauss 1997). Almost every polynomial time computable real number is absolutely normal. That is, if X is the set of reals that are not absolutely normal, then $\mu(X|P_{\mathbb{R}}) = 0$.

Combining Strauss's proof with the measure conservation theorem gives explicit constructions of reals in $P_{\mathbb{R}}$ that are absolutely normal.

Theorem (Mayordomo 2012). Explicit constructions of absolutely normal reals α computable in $O(n \log n)$ time.

ALAN TURING YEAR



Question

The above measure is induced on $P_{\mathbb{R}}$ by the binary expansions of reals.

Can this be done (directly) in terms of other representations of reals, e.g., the overlapping intervals representation proposed in Turing's 1937 Correction?

Normal Numbers and Finite Automata

Normal numbers are more closely connected to the theory of computing than was recognized in Turing's time.

Normal Numbers and Finite Automata

Normal numbers are more closely connected to the theory of computing than was recognized in Turing's time.

This connection is made via [finite-state compressors](#) and [finite-state gamblers](#).

Definition (Shannon 1948). Fix a finite alphabet Σ .

1. A finite-state compressor (FSC) is a 4-tuple

$$C = (Q, \delta, q_0, \nu),$$

where Q, δ, q_0 form a finite-state automaton, and $\nu: Q \times \Sigma \rightarrow \{0, 1\}^*$ is the output function.

Definition (Shannon 1948). Fix a finite alphabet Σ .

1. A finite-state compressor (FSC) is a 4-tuple

$$C = (Q, \delta, q_0, \nu),$$

where Q, δ, q_0 form a finite-state automaton, and $\nu: Q \times \Sigma \rightarrow \{0, 1\}^*$ is the output function.

2. The output of C on input $w \in \Sigma^*$ is the string $C(w) \in \{0, 1\}^*$ defined by

$$C(\lambda) = \lambda; \quad C(wa) = C(w)\nu(\delta(w), a).$$

Definition (Shannon 1948). Fix a finite alphabet Σ .

1. A finite-state compressor (FSC) is a 4-tuple

$$C = (Q, \delta, q_0, \nu),$$

where Q, δ, q_0 form a finite-state automaton, and $\nu: Q \times \Sigma \rightarrow \{0, 1\}^*$ is the output function.

2. The output of C on input $w \in \Sigma^*$ is the string $C(w) \in \{0, 1\}^*$ defined by

$$C(\lambda) = \lambda; \quad C(wa) = C(w)\nu(\delta(w), a).$$

3. An information-lossless FSC (ILFSC) is an FSC for which the function

$$w \mapsto (C(w), \delta(w))$$

is one-to-one.

Definition (Schnorr and Stimm 1972).

1. A finite-state gambler (FSG) is a 4-tuple

$$G = (Q, \delta, q_0, B)$$

where Q, δ, q_0 form a finite-state automaton, and $B: Q \rightarrow \Delta_{\mathbb{Q}}(\Sigma)$ is the betting function.

($\Delta_{\mathbb{Q}}(\Sigma) = \{\text{rational-valued probability measures on } \Sigma\}$)

Definition (Schnorr and Stimm 1972).

1. A finite-state gambler (FSG) is a 4-tuple

$$G = (Q, \delta, q_0, B)$$

where Q, δ, q_0 form a finite-state automaton, and $B: Q \rightarrow \Delta_{\mathbb{Q}}(\Sigma)$ is the betting function.

($\Delta_{\mathbb{Q}}(\Sigma) = \{\text{rational-valued probability measures on } \Sigma\}$)

2. The martingale of G is the function

$$\begin{aligned} d_G: \Sigma^* &\rightarrow [0, \infty) \\ d_G(\lambda) &= 1 \\ d_G(wa) &= |\Sigma| d_G(w) B(\delta(w))(a). \end{aligned}$$

Definition (Schnorr and Stimm 1972).

1. A finite-state gambler (FSG) is a 4-tuple

$$G = (Q, \delta, q_0, B)$$

where Q, δ, q_0 form a finite-state automaton, and $B: Q \rightarrow \Delta_{\mathbb{Q}}(\Sigma)$ is the betting function.

($\Delta_{\mathbb{Q}}(\Sigma) = \{\text{rational-valued probability measures on } \Sigma\}$)

2. The martingale of G is the function

$$\begin{aligned} d_G: \Sigma^* &\rightarrow [0, \infty) \\ d_G(\lambda) &= 1 \\ d_G(wa) &= |\Sigma| d_G(w) B(\delta(w))(a). \end{aligned}$$

3. For $s \in [0, \infty)$, the s-gale of G is the function

$$d_G^{(s)}(w) = 2^{(s-1)|w|} d_G(w).$$

Definition. Let d be a gale, and let $S \in \Sigma^\infty$.

1. d succeeds on S if $\limsup_{w \rightarrow S} d(w) = \infty$.
2. d succeeds strongly on S if $\liminf_{w \rightarrow S} d(w) = \infty$.

Definition and Theorem Let $S \in \Sigma^\infty$.

1. (Dai, Lathrop, Lutz, and Mayordomo 2004). The finite-state dimension of S is

$$\begin{aligned} \dim_{FS}(S) &= \inf \left\{ s \in [0, \infty) \mid (\exists \text{ FSG } G) d_G^{(s)} \text{ succeeds on } S \right\} \\ &= \inf_{\text{ILFSC}} \liminf_{w \rightarrow S} \frac{|C(w)|}{|w| \log |\Sigma|}. \quad \text{"compression ratio"} \end{aligned}$$

Definition and Theorem Let $S \in \Sigma^\infty$.

1. (Dai, Lathrop, Lutz, and Mayordomo 2004). The finite-state dimension of S is

$$\begin{aligned} \dim_{FS}(S) &= \inf \left\{ s \in [0, \infty) \mid (\exists \text{ FSG } G) d_G^{(s)} \text{ succeeds on } S \right\} \\ &= \inf_{\text{ILFSC}} \liminf_{w \rightarrow S} \frac{|C(w)|}{|w| \log |\Sigma|}. \quad \text{"compression ratio"} \end{aligned}$$

2. (Athreya, Hitchcock, Lutz, and Mayordomo 2007). The finite-state strong dimension of S is

$$\begin{aligned} \text{Dim}_{FS}(S) &= \inf \left\{ s \in [0, \infty) \mid (\exists \text{ FSG } G) d_G^{(s)} \text{ succeeds strongly on } S \right\} \\ &= \inf_{\text{ILFSC}} \limsup_{w \rightarrow S} \frac{|C(w)|}{|w| \log |\Sigma|}. \end{aligned}$$

Definition. For $\alpha \in \mathbb{R}$ and $2 \leq b \in \mathbb{N}$, the base- b finite-state dimension and finite-state strong dimension of α are

$$\dim_{\text{FS}}^{(b)}(\alpha) = \dim_{FS}(S),$$

$$\text{Dim}_{\text{FS}}^{(b)}(\alpha) = \text{Dim}_{FS}(S),$$

where S is “the” base- b expansion of α .

The connection between normality and finite automata:

Theorem (Schnorr and Stimm 1972; Bourke, Hitchcock, and Vinodchandran 2005). A real $\alpha \in \mathbb{R}$ is normal in base b if and only if $\dim_{\text{FS}}^{(b)}(\alpha) = 1$.

Question: How true is the following statement?

Question: How true is the following statement?

Every theorem about normal numbers is the dimension-1 special case of a more general theorem about finite-state dimension.

Question: How true is the following statement?

Every theorem about normal numbers is the dimension-1 special case of a more general theorem about finite-state dimension.

The known instances of this phenomenon are interesting, because the generalizations require new methods.

Instance 1: Real arithmetic

Theorem (Wall 1949). For every $\alpha \in \mathbb{R}$ and $0 \neq q \in \mathbb{Q}$, if α is normal in base b , then so are $q + \alpha$ and $q\alpha$.

Instance 1: Real arithmetic

Theorem (Wall 1949). For every $\alpha \in \mathbb{R}$ and $0 \neq q \in \mathbb{Q}$, if α is normal in base b , then so are $q + \alpha$ and $q\alpha$.

Theorem (Doty, Lutz, and Nandakumar 2007) For every $\alpha \in \mathbb{R}$ and $0 \neq q \in \mathbb{Q}$,

$$\dim_{\text{FS}}^{(b)}(q + \alpha) = \dim_{\text{FS}}^{(b)}(q\alpha) = \dim_{\text{FS}}^{(b)}(\alpha)$$

and

$$\text{Dim}_{\text{FS}}^{(b)}(q + \alpha) = \text{Dim}_{\text{FS}}^{(b)}(q\alpha) = \text{Dim}_{\text{FS}}^{(b)}(\alpha).$$

Instance 2. Copeland-Erdős sequences

Definition. The base- b Copeland-Erdős sequence of an infinite set $A \subseteq \mathbb{Z}^+$ is

$CE_b(A)$ = the concatenation of the base- b expansions of the elements of A in order.

Instance 2. Copeland-Erdős sequences

Definition. The base- b Copeland-Erdős sequence of an infinite set $A \subseteq \mathbb{Z}^+$ is

$CE_b(A)$ = the concatenation of the base- b expansions of the elements of A in order.

E.g., Champernowne proved that $CE_{10}(\mathbb{Z}^+)$ is normal in base 10.

Instance 2. Copeland-Erdős sequences

Definition. The base- b Copeland-Erdős sequence of an infinite set $A \subseteq \mathbb{Z}^+$ is

$CE_b(A)$ = the concatenation of the base- b expansions of the elements of A in order.

E.g., Champernowne proved that $CE_{10}(\mathbb{Z}^+)$ is normal in base 10.

Champernowne also conjectured that $CE_{10}(\text{PRIMES})$ is normal in base 10.

Theorem (Copeland and Erdős 1946) If $A \subseteq \mathbb{Z}^+$ is “sufficiently dense”, then $CE_b(A)$ is normal in base b . (And PRIMES is sufficiently dense by the Prime Number Theorem)

Definition. Let $A \subseteq \mathbb{Z}^+$.

1. The A -zeta function $\zeta_A: [0, \infty) \rightarrow [0, \infty]$ is defined by

$$\zeta_A(s) = \sum_{n \in A} n^{-s}.$$

Definition. Let $A \subseteq \mathbb{Z}^+$.

1. The A-zeta function $\zeta_A: [0, \infty) \rightarrow [0, \infty]$ is defined by

$$\zeta_A(s) = \sum_{n \in A} n^{-s}.$$

2. The zeta-dimension of A is

$$\begin{aligned} \text{Dim}_\zeta(A) &= \inf\{s \mid \zeta_A(s) < \infty\} \\ &= \limsup_{n \rightarrow \infty} \frac{\log|A \cap \{1, \dots, n\}|}{\log n}. \end{aligned}$$

Definition. Let $A \subseteq \mathbb{Z}^+$.

1. The A-zeta function $\zeta_A: [0, \infty) \rightarrow [0, \infty]$ is defined by

$$\zeta_A(s) = \sum_{n \in A} n^{-s}.$$

2. The zeta-dimension of A is

$$\begin{aligned} \text{Dim}_\zeta(A) &= \inf\{s \mid \zeta_A(s) < \infty\} \\ &= \limsup_{n \rightarrow \infty} \frac{\log|A \cap \{1, \dots, n\}|}{\log n}. \end{aligned}$$

3. The lower zeta-dimension of A is

$$\dim_\zeta(A) = \liminf_{n \rightarrow \infty} \frac{\log|A \cap \{1, \dots, n\}|}{\log n}.$$

Theorem, restated (Copeland and Erdős 1946). If $\dim_{\zeta}(A) = 1$, then $CE_b(A)$ is normal in base b .

Theorem, restated (Copeland and Erdős 1946). If $\dim_{\zeta}(A) = 1$, then $CE_b(A)$ is normal in base b .

Theorem (Gu, Lutz, and Moser 2007).

$$\begin{array}{ccc} \dim_{FS}(CE_b(A)) & \geq & \dim_{\zeta}(A) \\ | \wedge & & | \wedge \\ \text{Dim}_{FS}(CE_b(A)) & \geq & \text{Dim}_{\zeta}(A) \end{array}$$

and that's all.

Theorem, restated (Copeland and Erdős 1946). If $\dim_{\zeta}(A) = 1$, then $CE_b(A)$ is normal in base b .

Theorem (Gu, Lutz, and Moser 2007).

$$\begin{array}{ccc} \dim_{FS}(CE_b(A)) & \geq & \dim_{\zeta}(A) \\ \text{|\wedge} & & \text{|\wedge} \\ \text{Dim}_{FS}(CE_b(A)) & \geq & \text{Dim}_{\zeta}(A) \end{array}$$

and that's all.

Note:

$$\dim_{FS}(CE_b(\text{SQUARES})) = 1 > \frac{1}{2} = \dim_{\zeta}(\text{SQUARES})$$

Besicovitch 1936; Davenport and Erdős 1952

Generalizing theorems about normal numbers to theorems about finite-state dimension is a fun, challenging, and productive line of inquiry.

Generalizing theorems about normal numbers to theorems about finite-state dimension is a fun, challenging, and productive line of inquiry.

But Turing, hypothetically apprised of these developments, might well ask a different, more specific question.

Definition. A real number α is absolutely dimensioned if

$$\dim_{FS}(\alpha) = \dim_{FS}^{(b)}(\alpha)$$

does not depend on b .

Definition. A real number α is absolutely dimensioned if

$$\dim_{FS}(\alpha) = \dim_{FS}^{(b)}$$

does not depend on b .



Is there an absolutely dimensioned real number α with

$$0 < \dim_{FS}(\alpha) < 1 \quad ?$$

If so, can we explicitly construct such numbers?

Conclusion

Turing's note on normal numbers was not published in his lifetime, but it has been published now.

Conclusion

Turing's note on normal numbers was not published in his lifetime, but it has been published now.

Its ultimate impact will depend on how it affects 21st century research.

Conclusion

Turing's note on normal numbers was not published in his lifetime, but it has been published now.

Its ultimate impact will depend on how it affects 21st century research.

Thank you!