On the Concept of a Random Sequence

Alonzo Church, 1940

Definition 1 (doesn't work)

- An infinite sequence $a_1, a_2, \dots$ of 0's and 1's is random:
  - if $f(r)$ is the number of 1s in the first r terms, then $f(r)/r$ approaches a limit
  - if $a_{n_1}, a_{n_2}, \dots$ is a sub-sequence of a, where a_n is included or not by **some rule** which depends only on n and $a_1, \dots, a_{n-1}$, and if $g(r)$ is the number of 1s in the first r terms of the sub-sequence, then $g(r)/r$ approaches the same limit as $f(r)/r$
  - not precise

Packaging sequences into numbers

- Package $a_1, \ldots, a_n$ into a number
  $b_n = 2^n + a_1 2^{n-1} + a_2 2^{n-2} + \ldots + a_{n-1}$
  - b_n doesn't see a_n but b_{n+1} does
  - latest element a_{n-1} is in lowest value position
  - $\mathbb{N}$: start with a 1 in highest position to mark the beginning
  - $\mathbb{R}$: or, if we start with a decimal point, then the whole infinite sequence b is a single real number

Normal numbers

- A real number is normal in base b if
  - every digit appears with limiting frequency $1/b$
  - every combination of k consecutive digits occurs with limiting frequency $1/b^k$
  - (also covers "admissible" numbers, a term not used these days but was mentioned by Church)
- Examples:
  - 0.1234567891011121314151617181920212223242526272829... in base 10 (Champernowne's constant)
  - 0.23571113171923293137414347535961677173798389... in base 10 (Copeland-Erdös constant)
  - $\sqrt{2}, \pi, e$? Unknown!

Definition 2 (doesn't work)

- A sequence is random if it packages to a normal number.
  - Does let us define probability
  - They can be proven to exist
  - Not really random: includes predictable sequences that can be gamed.

Definition 3 (doesn't work)

- if $\phi : \mathbb{N} \to \mathbb{N}$, form the sub-sequence $a_{n_1}, a_{n_2}, \ldots$ by selecting a_{n_i} if $\phi(b_{n_i}) = 1$
- An infinite sequence $a_1, a_2, \ldots$ of 0's and 1's is random:
  - if $f(r)$ is the number of 1s in the first r terms, then $f(r)/r$ approaches a limit,
  - and for **any** $\phi : \mathbb{N} \to \mathbb{N}$, if $g(r)$ is the number of 1s in $\{a_{n_i}\}$ then $g(r)/r$ has the same limit as $f(r)/r$
  - doesn't rule out an oracular ϕ that selects the 1s anyway

Computable

- Applies to *functions* $f : \mathbb{N} \to \mathbb{N}$
- Formal definition in a moment
- Church deploys these as follows:
  - package the first $n - 1$ digits of the sequence as b_n
  - if $f(b_n) = 1$ then select a_n

Definition 4

- if $\phi : \mathbb{N} \to \mathbb{N}$, form the sub-sequence $a_{n_1}, a_{n_2}, \ldots$ by selecting a_{n_i} if $\phi(b_{n_i}) = 1$

- An infinite sequence $a_1, a_2, \ldots$ of 0's and 1's is random:
    - if $f(r)$ is the number of 1s in the first r terms, then $f(r)/r$ approaches a limit,
    - and for **any computable** $\phi : \mathbb{N} \to \mathbb{N}$, if $g(r)$ is the number of 1s in $\{a_{n_i}\}$ then $g(r)/r$ has the same limit as $f(r)/r$.

Computability

- Intended to capture the idea of a finite algorithm.
- Historically there were several ideas
  - Effectively calculable functions
  - Recursive functions
  - Turing-machine-computable functions
- By 1937 these and others were shown to be equivalent

Turing machines

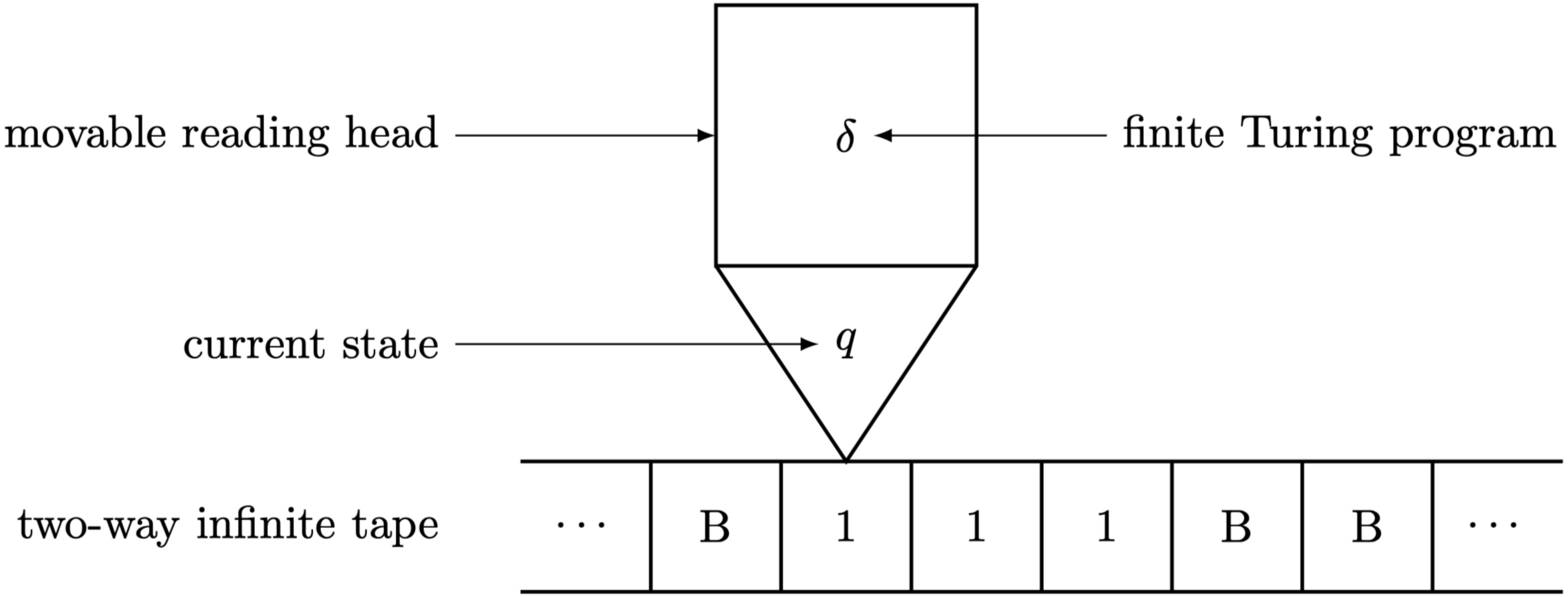

Figure 1.1. Turing machine

From R.I. Soare, Turing Computability, Theory and Applications of Computability, 2016

$$f(x) = x + 3$$

Compile time

in state	if you see	go to state	and write	and move
q_1	1	q_1	1	R
q_1	B	q_2	1	R
q_2	B	q_0	1	R

Run time

1. q_1 1 1 1 B B
2. 1 q_1 1 1 B B
3. 1 1 q_1 1 B B
4. 1 1 1 q_1 B B
5. 1 1 1 1 q_2 B
6. 1 1 1 1 1 q_0

Computable vs random

- Church-random sequences (by definition) defy computable attempts to game them
- So randomness
    - "defeats" or "defies" computability?
    - is invariant under computable alterations?
    - cannot be transformed into non-randomness by computability?
    - is the opposite of computability?

Enumerability

- You can encode the state machine table into a single huge integer.
- Therefore the set of all machines is enumerable.

Existence of random sequences

- The set of probability 1/2 sequences or $\{0,1\}$ is uncountable
    - The set of probability p sequences is uncountable
- If a_n is computable from $a_1, \ldots, a_{n-1}$ then the sequence is not random
    - Is this obvious?
    - Because a computable function based on this function could game it?
    - (Me: what if an infinite number of computable functions are used to generate the sequence? Can a single computable function game it?)
- By comparing sizes, a random sequence exists but is not computable

Existence of random sequences

- Church also concludes that a non-*constructive* argument would be required to produce one
    - The relationship between computable and constructive is interesting! (cf: realizability)