L211 Logic and Mathematics

13. Lecture

Norbert PREINING
preining@jaist.ac.jp

http://www.preining.info/jaist/l211/2015e/

Last lecture

(Non-)Euclidean geometry, functions, sequence, convergence, continuity

Important points

- (Non-)Euclidean geometry: hyperbolic, elliptic
- ϵ-δ definitions
- sequence, series
- convergence, continuity
- graphs, functions, inverse functions, domain, range
- power series

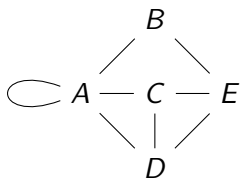
What is a graph?

Graph $G = (V, E)$

- V: set of nodes
- $E \subseteq V \times V$: set of edges

Example:

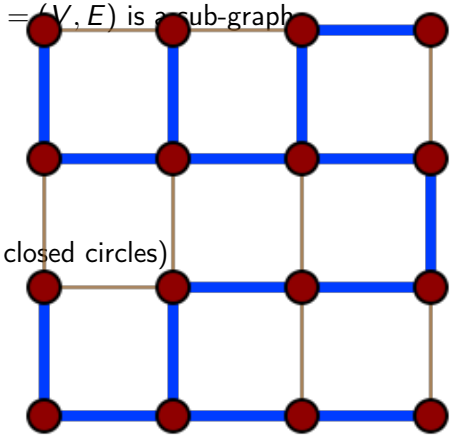
$V = \{A, B, C, D, E\}$
$E = \{(A, A), (A, B), (A, C), (A, D), (B, E), (C, D), (C, E), (D, E)\}$



Spanning Tree

The spanning tree of a graph $G = (V, E)$ is a sub-graph $G' = (V', E')$ of G such that:

- $V' = V$
- $E' \subseteq E$
- $G' = (V', E')$ is a tree (no closed circles)

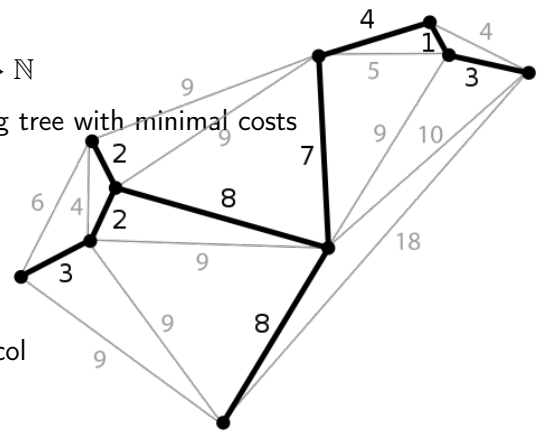


Minimal spanning tree

- Graph $G = (V, E)$
- Cost function $f : E \to \mathbb{N}$
- Requested: a spanning tree with minimal costs

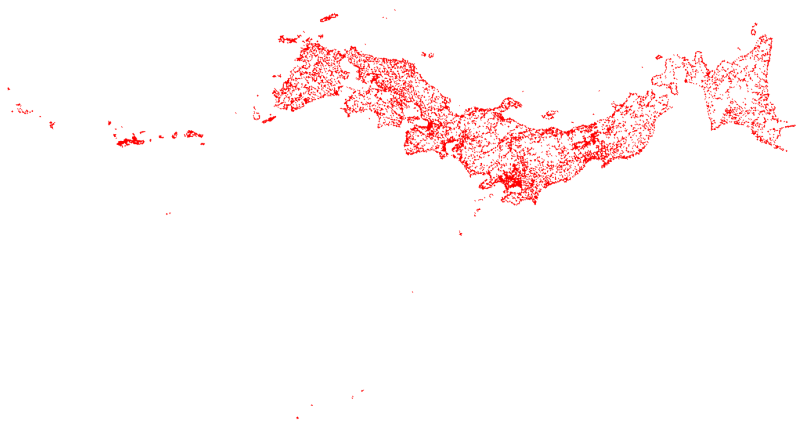
Minimal costs: 38

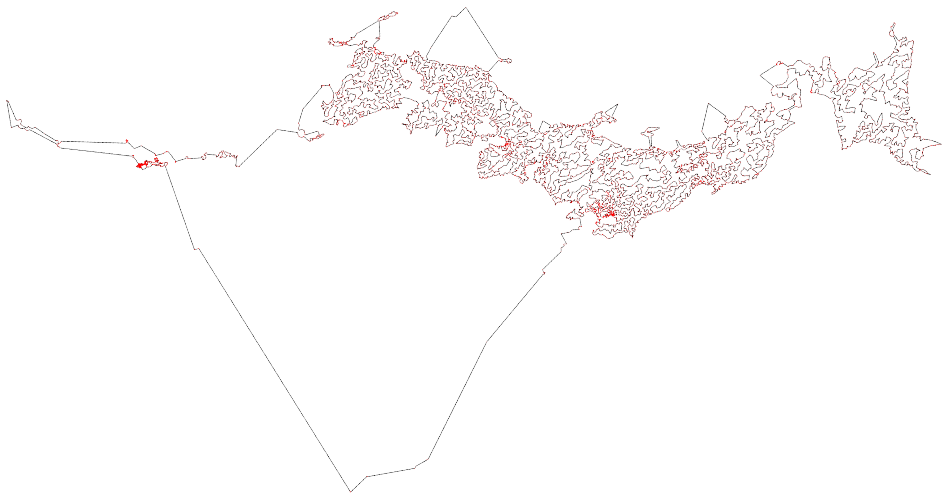
STP Spanning Tree Protocol
bridged Ethernet LAN



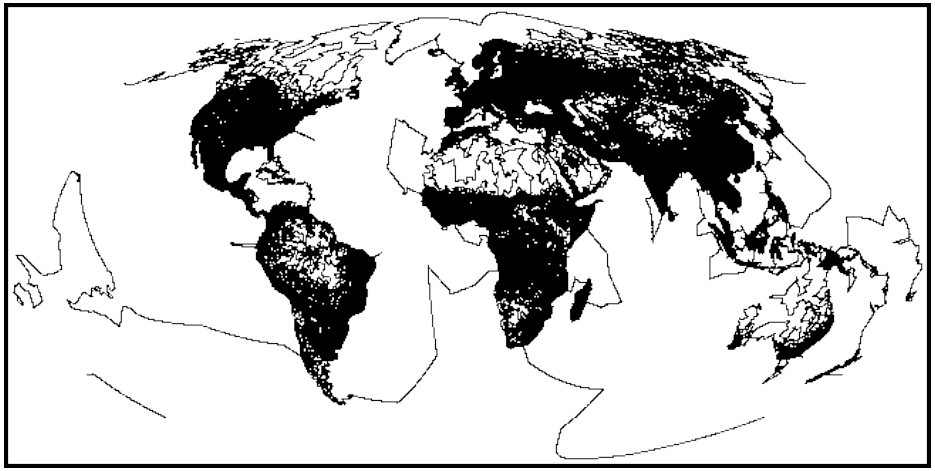
Travelling salesman problem

Find the path with the least costs for a traveling salesman such that he visits every place (township) exactly once.





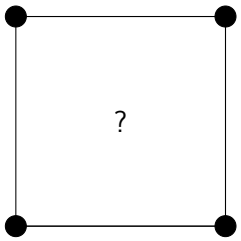
length: 7,516,353,779



Old ladies' houses

Four old ladies live in their respective houses in the corner of a square of 1km side, and want to build connecting streets.

What is the shortest street that connects all four?



Length: 3.457... km

Steiner tree: NP-hard problem

Models of computations

Primitive recursive functions

$f : \mathbb{N}^n \to \mathbb{N}$

- Constant functions $0 : \{\} \to \mathbb{N}$
- Successor function: $S : \mathbb{N} \to \mathbb{N}$
- Projection functions: $P_i^n : \mathbb{N}^n \to \mathbb{N} \quad P_i^n(x_1, \ldots, x_n) = x_i$
- Composition: If f (k-ary) and g_i (m-ary) are prf, then also $f(g_1(x_1, \ldots, x_m), \ldots, g_k(x_1, \ldots, x_m)) : \mathbb{N}^m \to \mathbb{N}$
- primitive recursion: if f (k-ary), g ($k+2$-ary) are prf, then also

$$h(0, x_1, \ldots, x_k) = f(x_1, \ldots, x_k)$$
$$h(S(y), x_1, \ldots, x_k) = g(h(y, x_1, \ldots, x_k), y, x_1, \ldots, x_k)$$

Examples of prf

Addition

$$\begin{aligned}\mathrm{add}(0,x) &= P_1^1(x)\\ \mathrm{add}(S(n),x) &= S(P_1^3(add(n,x),n,x)) = S(add(n,x))\end{aligned}$$

$h = \mathrm{add}$, $f = P_1^1$, $g = S \circ P_1^3$,

Examples of prf cont.

Predecessor

$$\begin{aligned}\mathrm{pred}(0) &= 0\\ \mathrm{pred}(S(n)) &= P_2^2(\mathrm{pred}(n),n) = n\end{aligned}$$

Subtraction

$$\begin{aligned}\mathrm{sub}(0,x) &= P_1^1(x)\\ \mathrm{sub}(S(n),x) &= \mathrm{pred}(P_1^3(\mathrm{sub}(n,x),n,x))\end{aligned}$$

Are these all the functions that are computable?

Ackermann function

$$\mathrm{Ack}(m,n) = \begin{cases} n+1, & \text{if } m=0\\ \mathrm{Ack}(m-1,1), & \text{if } n=0\\ \mathrm{Ack}(m-1,\mathrm{Ack}(m,n-1)), & \text{otherwise}\end{cases}$$

$\mathrm{Ack}(4,2) = 2^{265536} - 3 = 2^{2^{2^{2^2}}} - 3$

It is computable, but not primitive recursive.

μ-recursive functions

primitive recursive functions plus

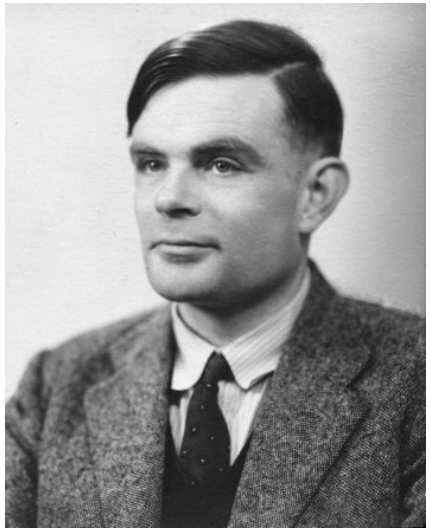
- μ operator: f ($k+1$-ary)

$$\begin{gathered}\mu(f)(x_1,\ldots,x_k) = z\\ \Updownarrow\\ f(z,x_1,\ldots,x_k) = 0 \quad \text{and}\\ f(i,x_1,\ldots,x_k) > 0 \quad i = 0,\ldots,z-1\end{gathered}$$

Example

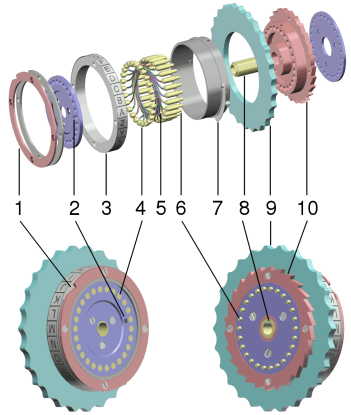
$$\begin{aligned}f(z,x) &= \mathrm{sub}(\mathrm{add}(z,x), S(S(S(S(S(S(S(0))))))))\\ g(x) &= \mu(f)(x)\\ g(4) &= ? \quad g(8) = ?\end{aligned}$$

Alan Turing



- 1912–1954
- English mathematician
- Cryptology
- Models of computation
- Turing machine
- 1952 imprisoned for homosexuality
- 1954 died, probably suicide
- 2013-12-24 pardoned by the Queen

Enigma



Enigma

- Rotor cipher machine
- Code: NIBLFMYMLLUFWCASCSSNVHAZ
- Meaning: THEXRUSSIANSXAREXCOMINGX

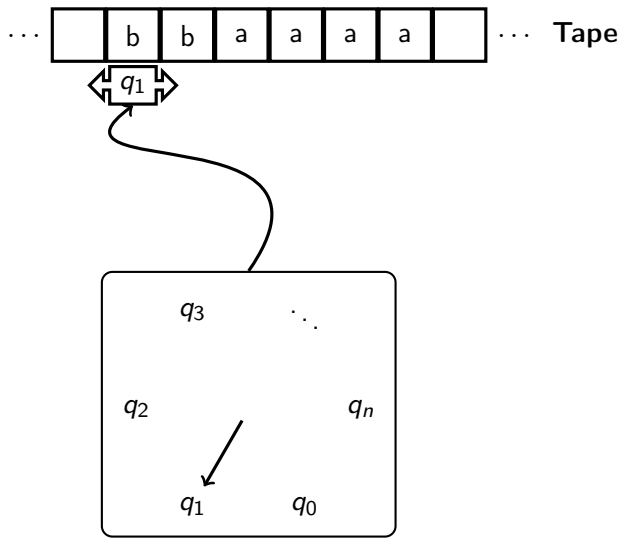
Turing machine

Parts of the machine

- infinite tape
- read-write head
- memory for internal states

Operations

- head can read/write to/from the tape at the current position
- state of the machine can be changed
- head can be moved left or right



Formalization

- Q: set of states
- Σ: input alphabet
- $\sqcup$: empty/space symbol
- Γ: tape alphabet $\Gamma \supseteq \Sigma \cup \{\sqcup\}$
- q_0: initial state $q_0 \in Q$
- q_a: accepting state $q_a \in Q$
- $\delta : Q \times \Gamma \to Q \times \Gamma \times \{\mathrm{L}, \mathrm{R}\}$

Example: $Q = \{q_0, q_a\}$, $\Sigma = \{a\}$, $\Gamma = \{a, \sqcup\}$

$\delta(q_0, a) = (q_0, a, \mathrm{R})$, $\delta(q_0, \sqcup) = (q_a, \sqcup, \mathrm{R})$

Computations

$f(n_1, \ldots, n_k) = m$

- $\Sigma = \{1\}$
- Input: $\sqcup^*(n_1)\sqcup(n_2)\sqcup\ldots\sqcup(n_k)\sqcup^*$
- Output: $\sqcup^*(m)\sqcup^*$

$f(n, m) = n + m$

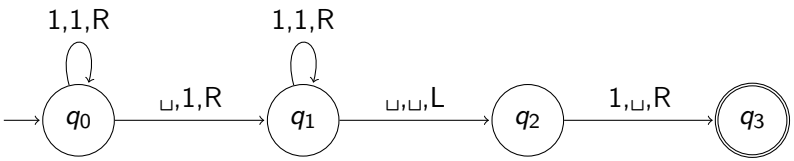
Input: $\cdots$ | $\sqcup$ | 1 | 1 | $\sqcup$ | 1 | 1 | 1 | 1 | $\sqcup$ | $\cdots$

Output: $\cdots$ | $\sqcup$ | 1 | 1 | 1 | 1 | 1 | 1 | $\sqcup$ | $\sqcup$ | $\cdots$

Program

$$\delta(q_0, 1) = (q_0, 1, \mathrm{R})$$
$$\delta(q_0, \sqcup) = (q_1, 1, \mathrm{R})$$
$$\delta(q_1, 1) = (q_1, 1, \mathrm{R})$$
$$\delta(q_1, \sqcup) = (q_2, \sqcup, \mathrm{L})$$
$$\delta(q_2, 1) = (q_a, \sqcup, \mathrm{R})$$

Automaton



$\delta(q_0, 1) = (q_0, 1, \mathrm{R})$ $\delta(q_1, 1) = (q_1, 1, \mathrm{R})$ $\delta(q_2, 1) = (q_a, \sqcup, \mathrm{R})$
$\delta(q_0, \sqcup) = (q_1, 1, \mathrm{R})$ $\delta(q_1, \sqcup) = (q_2, \sqcup, \mathrm{L})$

Example of a program

- acceptance of words a^*ba^*
- Palindrom
- addition in binary

Power of the Turing machine

- μ-recursive functions
- all programming languages

What functions are computatble?

Church–Turing Thesis

Sources

Wikimedia
Turing machine: `http://morphett.info/turing/turing.html`
Enigma rotor, Enigma: WikiCommons, GFDL