Space-bounded complexity

and inequalities for it

(Andrei Romashchenko, Péter Gács, me)

21 oct 2020

[covid-online talk]

"Laws of information"	Shan.	Kolm	combin.
- information in X	$H(X)$	$C(X)$	logsize X
- information in X about Y	$I(X:Y)$	$I(X:Y)$	logsize$(Y \mid X)$

"The same laws" for all three worlds

$$H(X,Y) \le H(X) + H(Y)$$

X $\quad p_1 \dots p_n \quad H(X) = \sum p_i \log \frac{1}{p_i}$

X $\quad$ min. pr.

Goal: the same laws for "more constructive" (space bounded) complexity

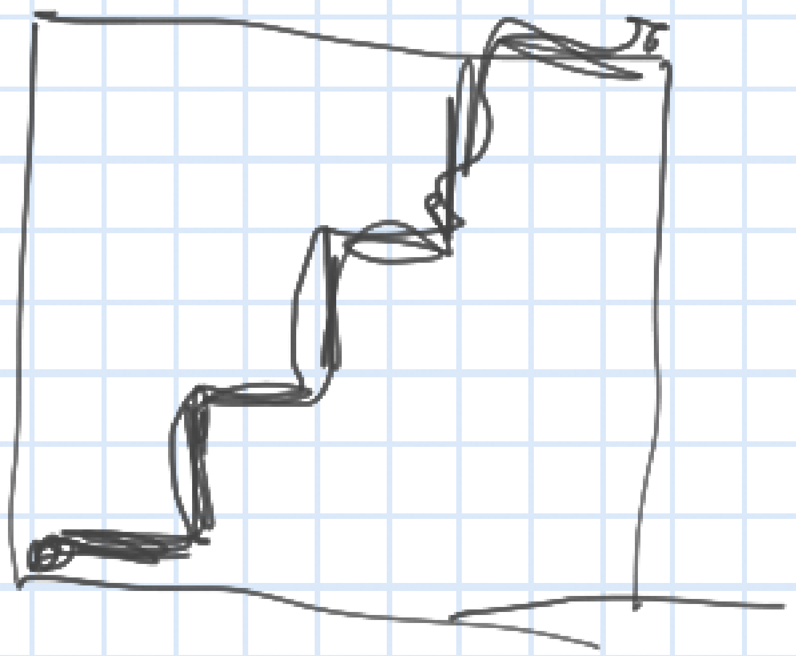
Complexity

using space $\leq S$

$$C^S_I(x) = \min\{\,|p| : I(p) = x\,\}$$

interpreter

$C(x|y)$



- Computational model ?
- Depends on I

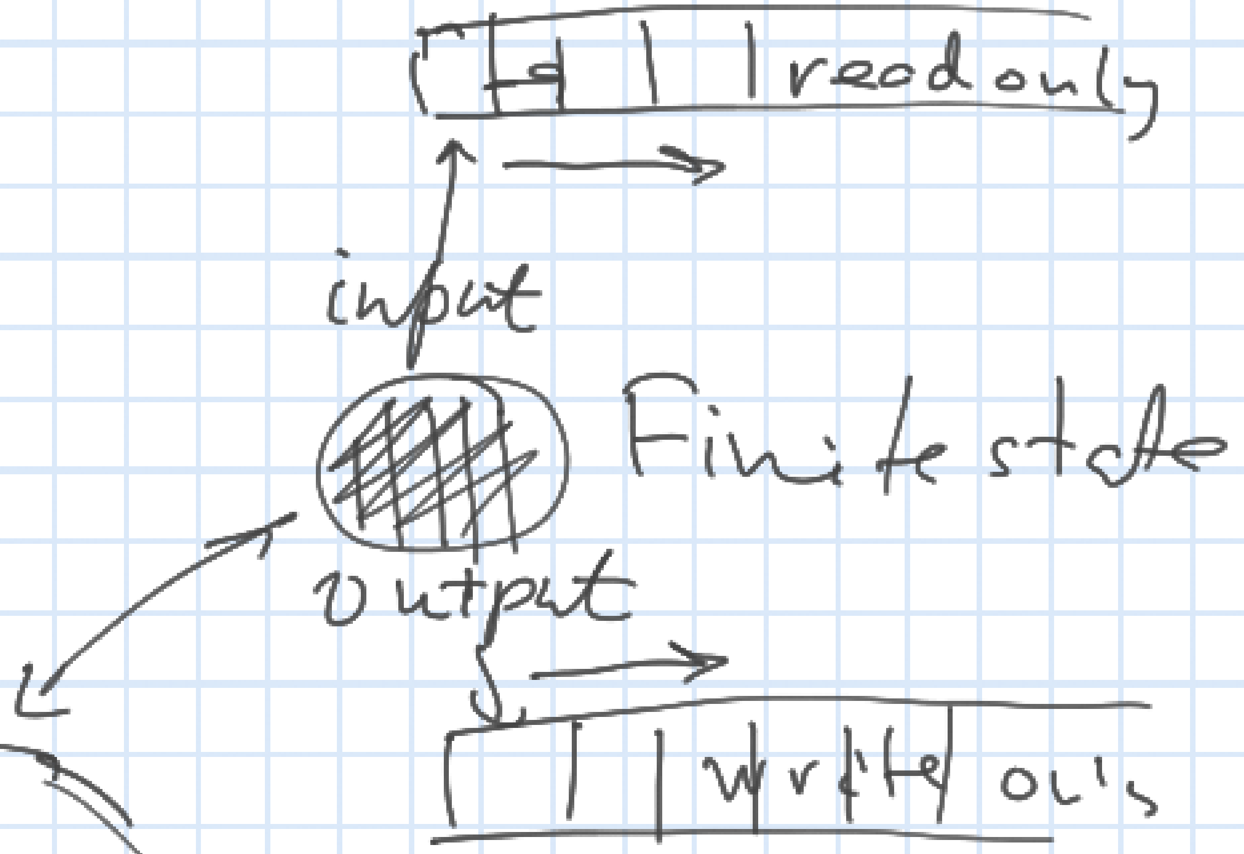
How to measure space?

Tape

Several tapes

Inf Memory

$$S \longleftrightarrow S + O(\log S) + O(\text{input} + \text{output})$$



Universality

$\underline{\exists I \; \forall I' \; \exists c_{I'}} \; \forall x$

$$C_I(x) \le C_{I'}(x) + c$$

$$C_I^{s+c}(x) \le C_{I'}^{s}(x) + c$$

$s \to \infty$

$$\lim_{s\to\infty} C^s(x) = C(x)$$

how large should be s $BB(n)$

computable

<u>difference:</u> $C^s(x)$ large while $C(x)$ small?

$C^s(x) \approx |x|$ w $C(x) = \log|x| + \underline{BB^{-1}(\log|s|)}$

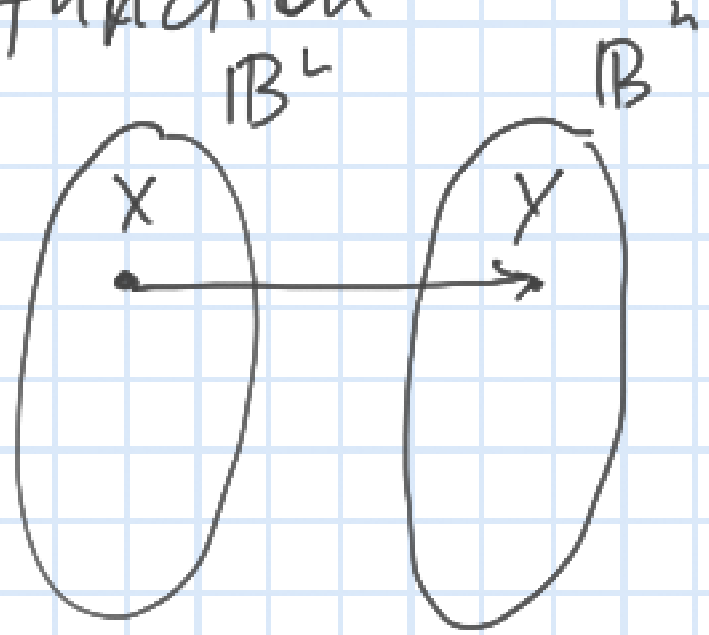
first s-incompr. string

Time: (Luc Longpre) polynomial time bounds

$$I(x:y) \stackrel{?}{=} I(y:x) + O(\log n)$$

$$\begin{array}{ccc} \| & & \| \\ C(y) - C(y|x) & & C(x) - C(x|y) \end{array}$$

one-way function



$C(y|x) \approx 0$

$C(y) \approx n$

if

$C(x|y) \approx O(\log n)$

one of poly(n)

reverts 1/poly(n)

fraction

Space

$$\underline{C^{s'}(x,y) \le C^{s}(x) + C^{s}(y|x) + O(\log n)}$$

$$|x| = |y| = n$$

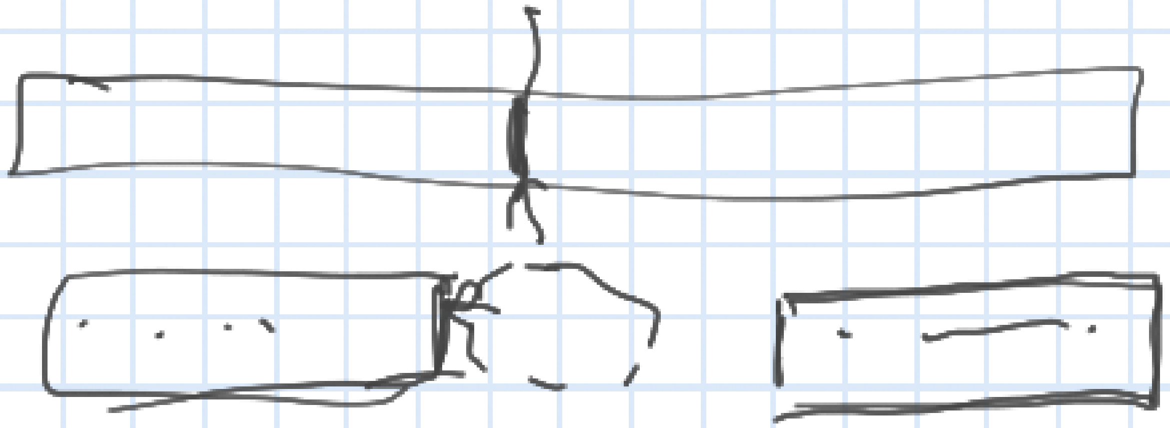
how to make a space-bounded version

$s' = ?$

$$s' = \underline{s + O(n)} \quad [+ O(\log s)]$$

Easy direction

two stacks



$$C^{\cancel{s}\,s'}(x) + C^{\cancel{s}\,s'}(y|x) \le C^{s}(x,y) + \underline{O(\log n)}$$

$s \to \infty$

$s' \to \infty$

for $|x| = |y| = n$

$$\underline{s' = s + O(n) + O(\log s)}$$

no s

$s \to \infty$

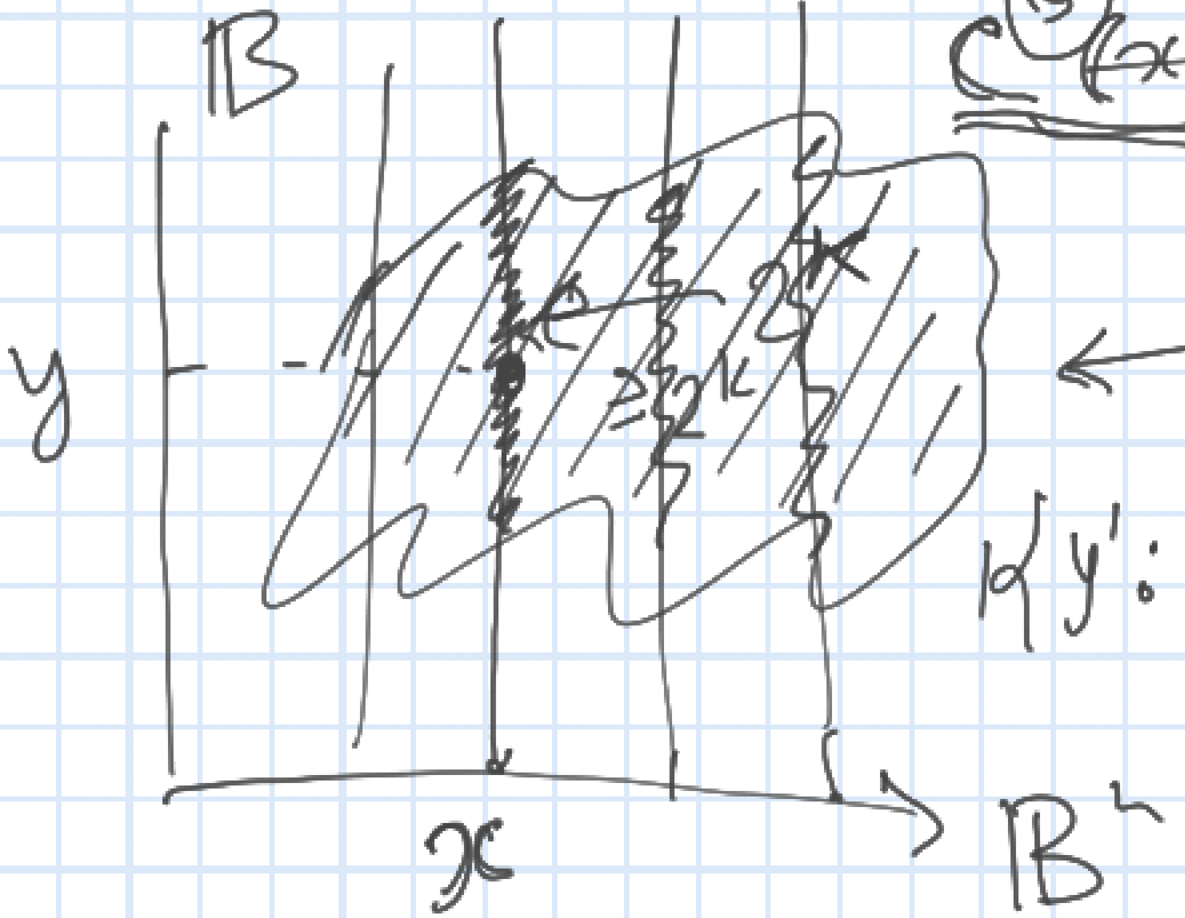
Longpre: $s' = 2s + O(n) + O(\log s)$

$3s$

Proof sketch

$C(y|x) \le k$

$C(x) \le n - k$



$\underline{C^{s}(x,y) \le n}$

try all programs of length $\le n$, s

2^n of them

$|\{y' : C(x,y') \le n\}| = 2^k$

2^{n-k} large lines

Sipser's trick

M - machine, input x for M (when $M(x)$ terminates in space s)
fixed

$\bar{M}$ - input x, s : [does M terminate on x in space s?

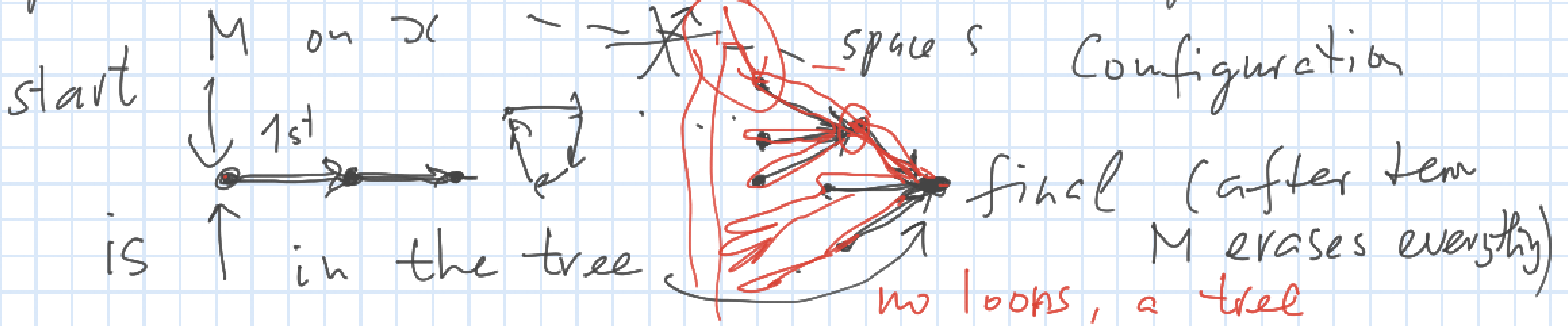
after $\boxed{2^{s\ldots} \text{ steps}}$ no chance

standard $\boxed{2^{s} + O(\log s) + O(|x|)}$ — counter for space

$s + s$ — to avoid loops
for simulation

Sipser: $s + O(\log s) + O(|x|)$

M on x — space s Configuration



Why important? Iterations $s \to 2s$

$4s$

$$+\left\{ \underline{C^{s'}(\ldots) + C^{s'}(\ldots)} \le \ldots \underline{C^{s}(\ldots) + C^{s}(\ldots)} \ldots \right.$$

$O(n)$

$C^{s'} \ldots \cancel{C^{s'}} \ldots \le \cancel{C^{s}} + \ldots C^{s}$

can be smaller cancellation?

$A^{s''} \le B^{s'}$

$B^{s'} \le C^{s}$

$A \le C$

$s \xrightarrow{f} s + O(\log s) + O(n)$

$s \to s' \to s'' \to \ldots s^{k} \to s^{k+1}$

n-th iteration of

$O(n)$ steps

$s \to 2s$

$s \to s + \underline{O(\log s)} + O(n)$

$s' = f^{(n)}(s)$

$s' \le s + O(n^2 \log n) + O(n \log s)$

$s' \sim 2^n s$

General result

Any linear inequality that is true for $\overbrace{\text{complexity}}^{\text{entropy, subgroup size}}$ is true for space-bounded complexities

$$C^{s'}\ldots + C^{s'}\ldots \le C^{s}\ldots + C^{s}\ldots$$

$$s' = s + O(n \log s) + O(n^2 \log n)$$

$n =$ max length of strings

$$s \to \infty \qquad s' \to \infty$$

THANKS!

$P = NP \longrightarrow$ polynomial-time symmetry

$\overset{?}{\searrow}$ all standard inequalities?

$$\underline{I(x:y)} \;\underset{\geq}{\leq}\; C^s(y) - C^s(y|x)$$