Rounding-up the seminar

16.XII.2020

why lower bounds

A large part of the research into circuit lower bounds is motivated by the possibility to prove

$$P \neq NP$$

in that way:

- by Savage's thm $P \subseteq P/poly$
- hence $NP \not\subseteq P/poly \Rightarrow P \neq NP$.

But how good this strategy really is?

PH

prerequisite:
NP ($= \Sigma_1^p$): defined by $\exists y(|y| \leq |x|^{O(1)})R(x,y)$
where R is p-time decidable

coNP ($= \Pi_1^p$): defined by $\forall y(|y| \leq |x|^{O(1)})R(x,y)$

and then allow longer prefixes of bounded quantifiers
Σ_2^p: defined by

$$\exists y_1(|y_1| \leq |x|^{O(1)})\forall y_2(|y_2| \leq |x|^{O(1)})R(x,y_1,y_2)$$

Π_2^p: defined by

$$\forall y_1(|y_1| \leq |x|^{O(1)})\exists y_2(|y_2| \leq |x|^{O(1)})R(x,y_1,y_2)$$

and analogously $\Sigma_3^p, \Pi_3^p, \dots$ and eventually:

$$PH := \bigcup_i \Sigma_i^p = \bigcup_i \Pi_i^p \ .$$

pluses

On the plus side of the strategy are:

- It replaces Turing machines by seemingly simpler combinatorial objects - circuits - and it ought to be susceptible to combinatorial methods.
- Some early successes for restricted classes of circuits: e.g. monotone, constant-depth in various languages.
- Karp-Lipton's thm: $NP \subseteq P/poly \;\Rightarrow\; PH = \Sigma_2^p$
  which most experts deem unlikely.

minuses

Same items also illustrate the failure of the approach:

- No non-trivial lower bounds for general circuits for SAT: even $1.1n$ is unknown.
- No significant progress on restricted classes (as are e.g. $AC^0(6)$ or formulas) in last 30+ years.
- There is no really good argument why PH could not collapse to Σ_2^p, only analogy with the arithmetical hierarchy.

In addition, several deeper thms in complexity theory in the last several decades have the form of establishing upper bounds or constructing new algorithms that show that some complexity classes expected to be different are actually the same:

Toda's thm: $PH \subseteq P^{\oplus}$.
the Szelepcsényi-Immermann thm: $NL = coNL$.

an alternative

It is important to keep an open mind and not to listen to experts too much: some of them sound as if they had a direct line to God who tells them what is and what is not true.

An alternative approach to P vs. NP - still using circuits - was contemplated by A.N.Kolmogorov, on of the most influential mathematician of the 20th century contributing to a number of diverse fields. Ex's in complexity th.: Kolmogorov complexity of strings and algorithmic randomness.
Kolmogorov considered that it is possible that

$$P \subseteq Size(O(n))$$

i.e. all p-time decidable languages have linear size circuits. This is sometimes called Kolmogorov's conjecture.
(Ref: Jukna's book on circuit complexity.)

KC consequence

Theorem

Kolmogorov's conjecture implies that $P \neq NP$.

Prf.:

If $P = NP$ then $P = PH$. But by Kannan's thm for every $k \geq 1$ there is $L \in \Sigma_2^p \subseteq PH$ such that $L \notin Size(n^k)$.

$\square$

So, in principle, we can prove $P \neq NP$ by proving upper bounds on circuits.

Remark: the Karp-Lipton thm and Kannan's thm are fairly easy to prove, see the 3-page lecture notes of P.Beame on the seminar web page.