How Complex Is Complexity?

Eric Allender
Rutgers University

Richard M. Karp Distinguished Lecture

Feb. 8, 2023

How Complex Is Complexity? Or: What's a 'Meta' for?

Eric Allender
Rutgers University

Richard M. Karp Distinguished Lecture

Feb. 8, 2023

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

Goal for Today:

- Give a High-Level Overview of the Simons Institute program on Meta*-Complexity
  - Explain the reasons for excitement and optimism.
  - Illustrate some of the topics involved via examples and metaphors.
  - Apologize for the terrible ‘Meta for’ pun.

    Shockingly, I’m not the first to dive this low.

*No connection to the parent company of Facebook.

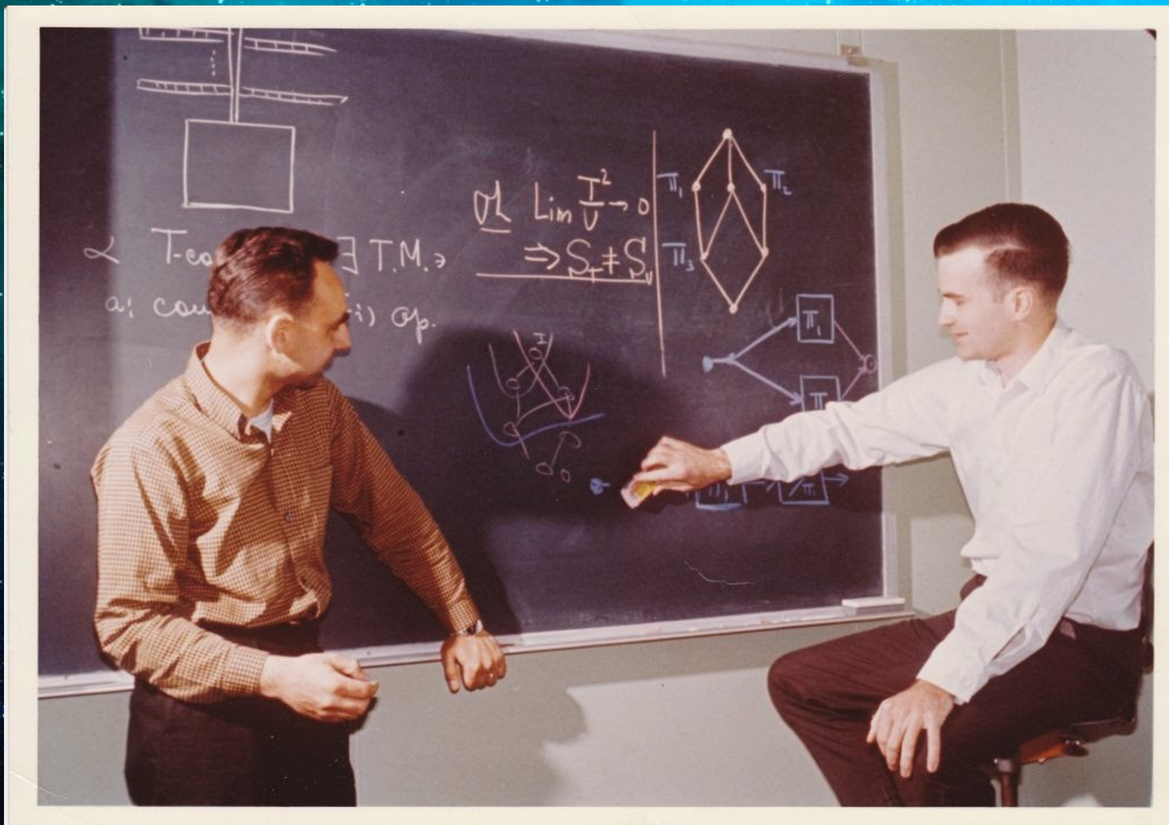
Goal for Today:

- Give a High-Level Overview of the Simons Institute program on Meta*-Complexity
  - Explain the reasons for excitement and optimism.
  - Optimism? Really?

*No connection to the parent company of Facebook.

In the Beginning…

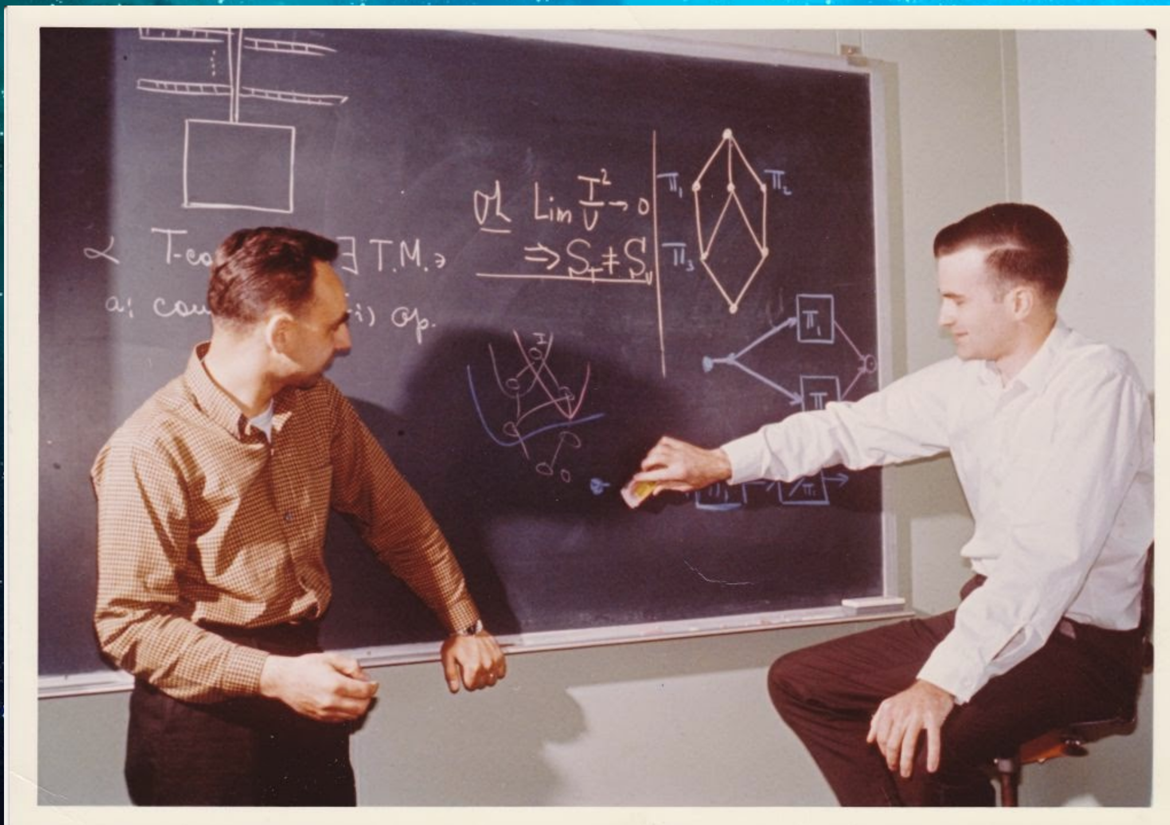
In the Beginning…



1964

Hartmanis and Stearns created complexity theory.

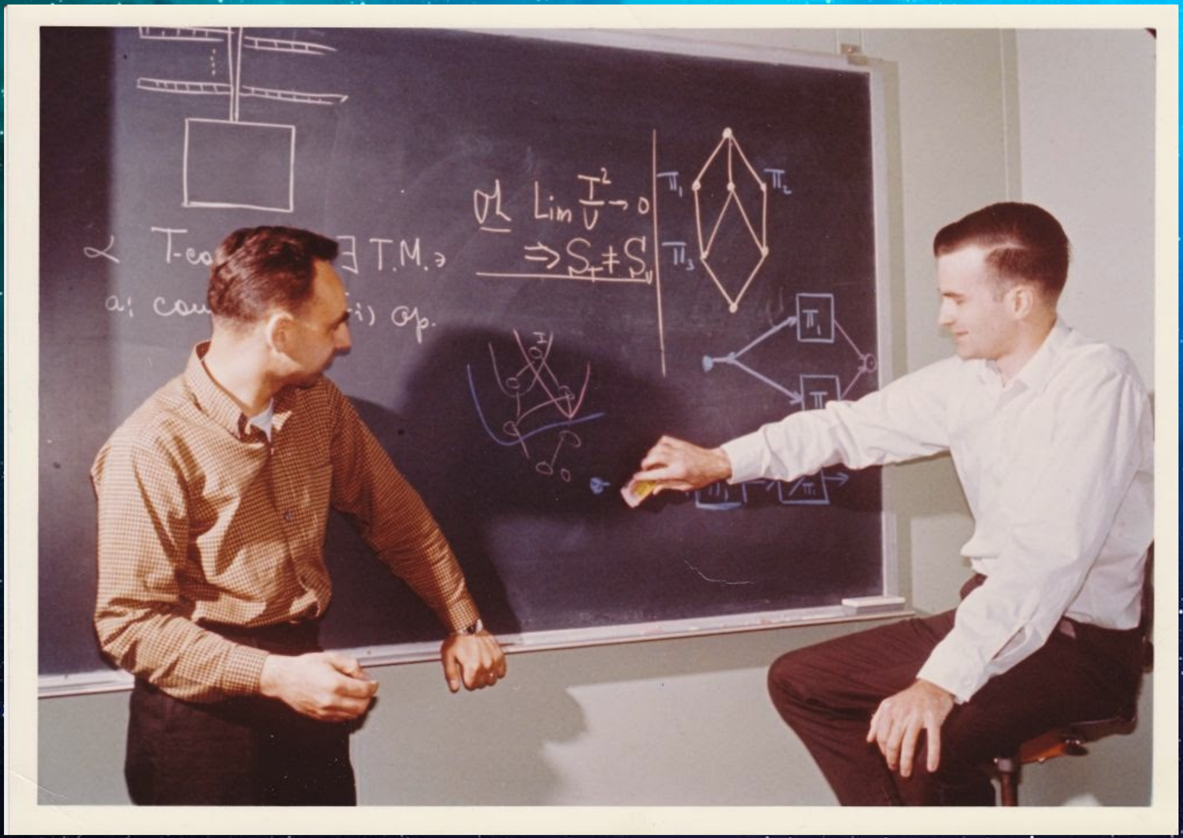
And the critical reaction was…



… mixed.

1964

And the critical reaction was…



1964

We could show that some uninteresting problems require a lot of time … but could say nothing about problems of interest.

The Universe of Natural Computational Problems

This universe was without form, and void…

And Cook and Karp said:

Let there be illumination…

And Cook and Karp said:

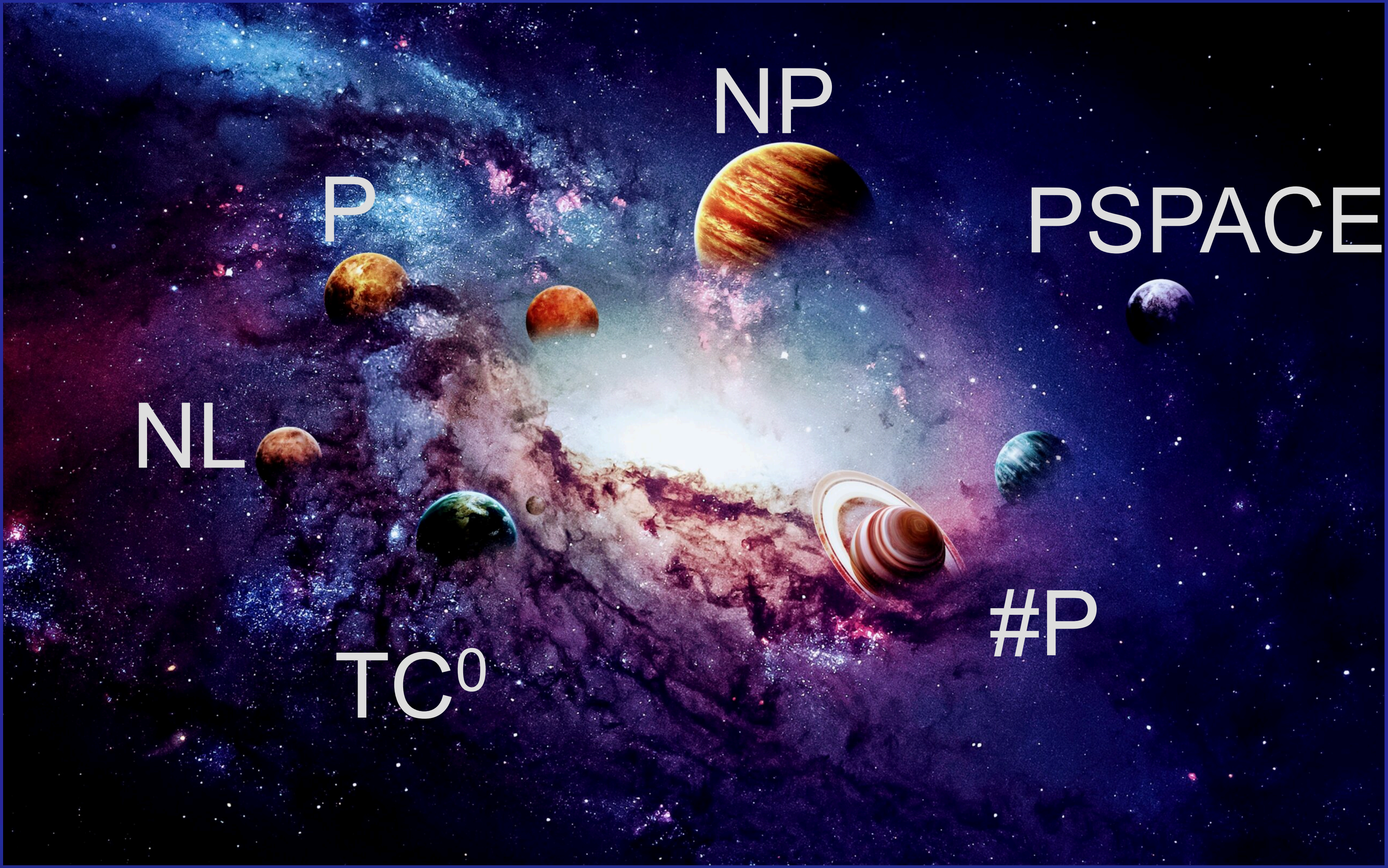
Let there be illumination…

1970

1971

…in the form of efficient reductions.

And the Structure was Revealed!



A Vision of Paradise

- At about this same time, the first positive application of complexity theory arose:
  - *Cryptography*!
- The perceived difference in the complexity of problems now made sense! There was a theoretical framework to support our intuitions! And it promised to be useful in practice!
- We merely needed to prove that the framework was real, and not an illusion.

The Oracular Prohibition

Thou shalt not enter into this paradise by means of any tool at thy disposal.

The Oracular Prohibition

$P^A = NP^A$

$P^B \neq NP^B$

1975

End-Run Around Oracles

- Small circuit classes, where oracle computation might not make sense:
  - AC^0 (1980's) [FSS][A][Y][H]
  - $AC^0[p]$ for prime p (1980's) [R][S]
  - .....
  - NEXP not in $AC^0[6]$ [Williams, 2011]

Frontal Assault against Oracles

- The Theory of Interactive Proofs Leads to Non-relativizing Proof Techniques!
  - $coNP \subseteq IP$ [LFKN 1990]
  - $IP = PSPACE$ [Shamir 1990]
- But this did not usher in a new flood of lower bounds!

Crimes against Nature

Thus spake the nature deities:

If you seek a Natural way to paradise, you must forsake the One Way.

Crimes against Nature

Thus spake the nature deities:

If one-way functions exist, you need a new “un-natural” approach to prove lower bounds.

1994

Pointing the Way to Meta-Complexity

Thus spake the nature deities:

Razborov & Rudich focused on the problem of computation on truth-tables of functions.

1994

Meta-Complexity Is Born [2000]

- The Minimum Circuit Size Problem (MCSP):
- {(f,s) : f has a circuit of size ≤ s, where f is represented by a bit string of length 2^n}
- The complexity question: Show f is hard.
- The Meta-Complexity question: show that it is hard to show that f is hard.

That is: Show MCSP is hard.

Meta-Complexity Is Born [2000]

- The Minimum Circuit Size Problem (MCSP):
- {(f,s) : f has a circuit of size ≤ s, where f is represented by a bit string of length 2^n}
- MCSP is in NP; not in P if one-way functions exist.
- Provably hard to show it's NP-complete.

Not hard for RP under $\leq_m^p$ unless EXP ≠ ZPP. [MW][F]

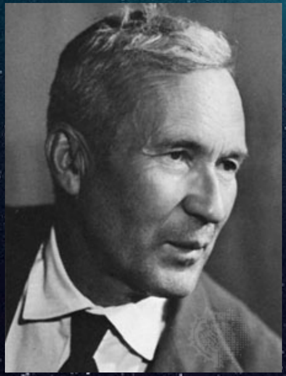
Meta-Complexity Is Born [2000]

- The Minimum Circuit Size Problem (MCSP):
- {(f,s) : f has a circuit of size ≤ s, where f is represented by a bit string of length 2^n}
- MCSP is in NP; not in P if one-way functions exist.
- Provably hard to show it's NP-complete.

Harks back to the pre-history of computational complexity theory.

Before the Beginning…

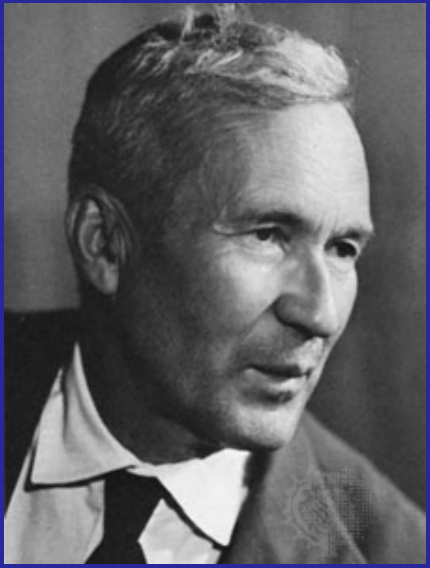
[1959]: Yablonsky announced that MCSP requires exponential time.



And Kolmogorov saw what Yablonsky had written, and saw that it was not good. (Thus sayeth Levin.)

Kolmogorov Complexity

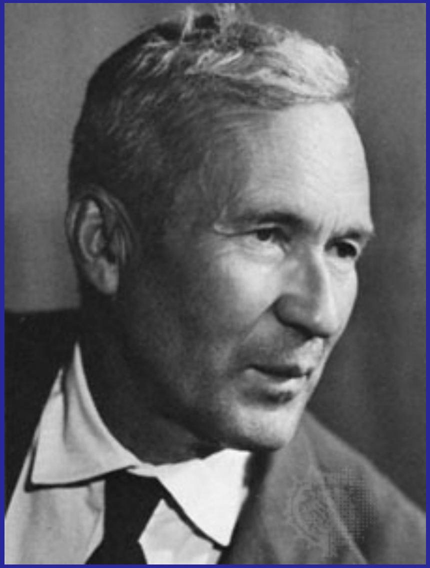
- $C(x) = \min \{|d| : U(d)=x\}$.



Information is best understood via computation; this gives us a definition of randomness.

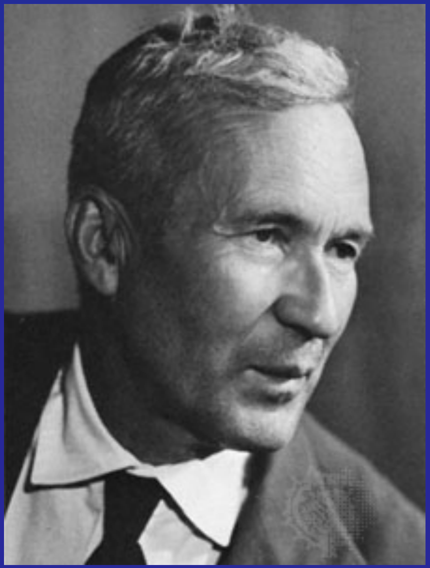
Kolmogorov Complexity

- $C(x) = \min \{|d| : U(d)=x\}$.



Unfortunately, C(x) cannot be computed. This motivates the search for computable variants.

Kolmogorov Complexity



However, Kolmogorov suggested, even before the notions of P, NP, and NP-completeness existed, that lower bound efforts might best be focused on sets that are relatively devoid of simple structure. That is, the NP-complete problems are probably too structured to be good candidates for separating P from NP. One should rather focus on the intermediate less-structured sets that somehow are complex enough to prove separations. As a candidate of such a set he proposed to look at the set of what we call nowadays the resource-bounded Kolmogorov random strings. [Buhrman & Mayordomo, citing Levin]

Time-bounded Kolmogorov Complexity

- Kt(x) = min {|d| + log t : U(d)=x in time t}.

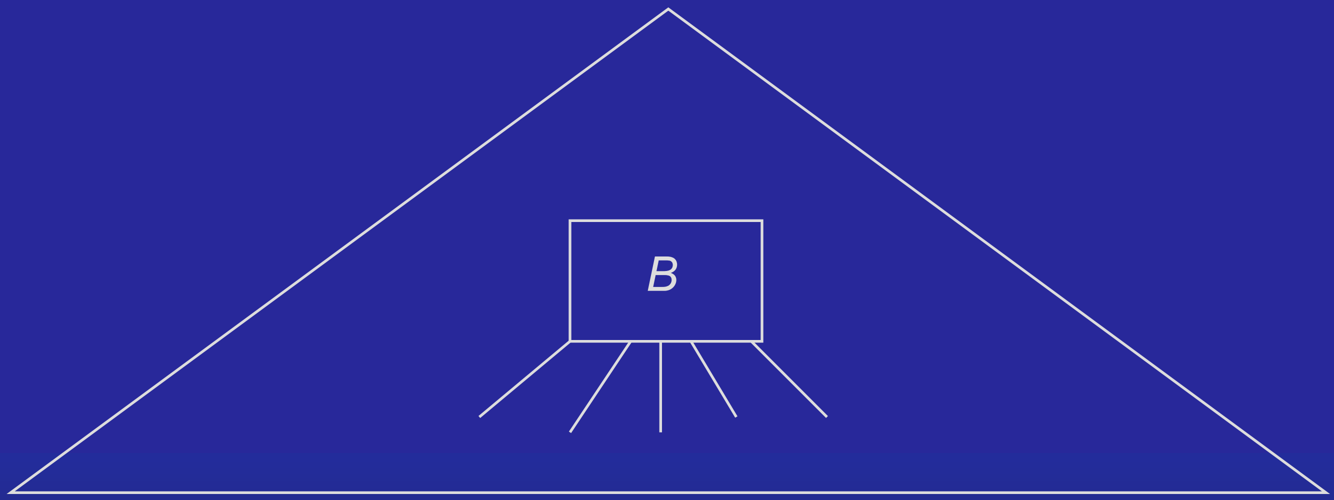
Great for many purposes…
but captures an odd type of
circuit size.

Circuit Complexity

- Let D be a circuit of AND and OR gates (with negations at the inputs). Size(D) = # of wires in D.
- Size(f) = min{Size(D) : D computes f}
- We may allow oracle gates for a set A, along with AND and OR gates.
- $Size^A$(f) = min{Size(D) : D^A computes f}

What is an Oracle Gate?

- An oracle gate for oracle *B* is a piece of hardware with *k* wires coming in (for some *k*). If those wires take on the value *x*, then the gate outputs 1 if *x* is in *B*, and 0 otherwise.



Time-Bounded Kolmogorov Complexity

- Levin's definition:
- $Kt(x) = \min\{|d|+\log t : U(d) = x \text{ in time } t\}$.
- …but captures an odd type of circuit size.
- Let A be complete for $E = Dtime(2^{O(n)})$.
  - Then $Kt(x) \approx Size^A(x)$.

Time-Bounded Kolmogorov Complexity

- Levin's definition:
- $Kt(x) = \min\{|d|+\log t : U(d) = x \text{ in time } t\}$.
- Why log t?
  - This gives an optimal search order for NP search problems.
  - Adding t instead of log t would give every string complexity $\geq |x|$.
- …So let's look at how to make the run-time be much smaller.

Revised Kolmogorov Complexity

- $C(x) = \min\{|d| : \text{for all } i \leq |x| + 1, U(d,i,b) = 1 \text{ iff } b \text{ is the } i\text{-th bit of } x\}$ (where bit # i+1 of x is *).
  - This is identical to the original definition.
- $Kt(x) = \min\{|d|+\log t : \text{for all } i \leq |x| + 1, U(d,i,b) = 1 \text{ iff } b \text{ is the } i\text{-th bit of } x, \text{ in time } t\}$.
  - The new and old definitions are within O(log |x|) of each other.
- Define $KT(x) = \min\{|d|+t : \text{for all } i \leq |x| + 1, U(d,i,b) = 1 \text{ iff } b \text{ is the } i\text{-th bit of } x, \text{ in time } t\}$.

Kolmogorov Complexity is Circuit Complexity

- $KT(x) \approx Size(x)$.
- $C(x) \approx KT^H \approx Size^H(x)$.
- $Kt(x) \approx KT^E \approx Size^E(x)$.
- Other measures of complexity can be captured in this way, too:
  - Branching Program Size $\approx KB(x) = \min\{|d|+2^s : \text{for all } I \leq |x| + 1, U(d,i,b) = 1 \text{ iff } b$ is the i-th bit of x, in space s$\}$.

Kolmogorov Complexity is Circuit Complexity

- $KT(x) \approx Size(x)$.
- $C(x) \approx KT^H \approx Size^H(x)$.
- $Kt(x) \approx KT^E \approx Size^E(x)$.
- Other measures of complexity can be captured in this way, too:
  - Formula Size ≈ $KF(x) = \min\{|d|+2^t : \text{for all } I \leq |x| + 1, U(d,i,b) = 1 \text{ iff } b$ is the i-th bit of x, in time t}, for an alternating Turing machine U.

Kolmogorov Complexity is Circuit Complexity

- $KT(x) \approx Size(x)$.
- $C(x) \approx KT^{H} \approx Size^{H}(x)$.
- $Kt(x) \approx KT^{E} \approx Size^{E}(x)$.
- In particular, MCSP "morally" has the same complexity as computing KT complexity.
- Frequently, MKTP is easier to work with.
- Other versions of time-bounded K-complexity (such as K^{poly}) also figure prominently in recent work. In this overview, we'll ignore the differences.

The Mother of All One Way Functions

- [Liu, Pass 2020] Cryptographically Secure One-Way Functions exist if and only if K^{poly} is hard on average.
- Thus, if you want to base cryptography on the assumption that NP is hard (in the worst case), this is equivalent to showing:
  - NP not in BPP implies $K^{poly} \notin$ BPP, and
  - $K^{poly} \notin$ BPP implies K^{poly} is hard on average.
  - [Hirahara 2018] "nearly" shows the 2nd implication.

Pass & Hirahara: Destroyers of Worlds

Heuristica

NP easy on average

Note: Destruction is not yet complete … but off to a good start.

Pessiland

NP hard on average but no crypto.

Worst-Case vs Average Case

- [Hirahara 2020] (paraphrased): There is something in the polynomial hierarchy that is hard on average
- If and only if
- $K^{poly,PH}$ is not in P.
- This is just a sample. Much more has been done in this direction.

Meta-Logic and Meta-Complexity

- A major theme of the Meta-Complexity semester explores how Meta-Complexity provides new insight into the field of Proof Complexity (lower bounds on the length required to prove that a formula is a tautology).
- Rahul Santhanam will be giving a talk on this topic later in the Karp Distinguished Lecture series.

Pathetic Lower Bounds

- The Goal is to prove superpolynomial circuit size bounds.
- Our current best efforts fall far short.
  - For circuits: nothing superlinear.
  - For (De Morgan) formulas: approximately n^3.
  - For Branching Programs: approximately n^2.
- Lower bounds for MCSP on these models essentially match the best known for any explicit problem. [CKLM]

Lower Bounds and Magnification

- Define MCSP[s] = {f : (f,s) is in MCSP}
- [CHMY]: MCSP[N^{ϵ}] is not in probabilistic 1-tape TM time $N^{1.99}$.
- [MMW]: If MCSP[N^{β}] is not in 1-tape TM time $N^{1.01}$, then P ≠ NP.
  – Note: $\beta<\epsilon$…
- General theme of Magnification: modest-sounding lower bounds can have huge consequences.

Lower Bounds and Magnification

- Another example:
- Recall: MCSP is not in De Morgan Formula Size $n^{3-\epsilon}$ [CKLM]
- This holds also for MKTP and MKtP.
- If MKtP[N^{ϵ}] is not in De Morgan Formula Size $n^{3.001}$, then EXP is not in NC^1 [OPS].
- …but perhaps you're thinking: We don't have ANY formula size lower bounds that big. Then consider this…

Lower Bounds and Magnification

Yet another example:

- If MKtP[N^{ϵ}] is not in De Morgan Formula of PARITY Size $n^{1.1}$, then EXP is not in NC^1 [OPS].
- …and we *do* know problems in P that require size $n^{1.99}$ in this model [Tal].
- For more on magnification, see [CHOPRS].

Meta-Complexity Is Born [2000]

- The Minimum Circuit Size Problem (MCSP):
- {(f,s) : f has a circuit of size ≤ s, where f is represented by a bit string of length 2^n}
- MCSP is in NP; not in P if one-way functions exist.
- Provably hard to show it's NP-complete.

Not hard for RP under $\leq_m^p$ unless EXP ≠ ZPP. [MW][F]

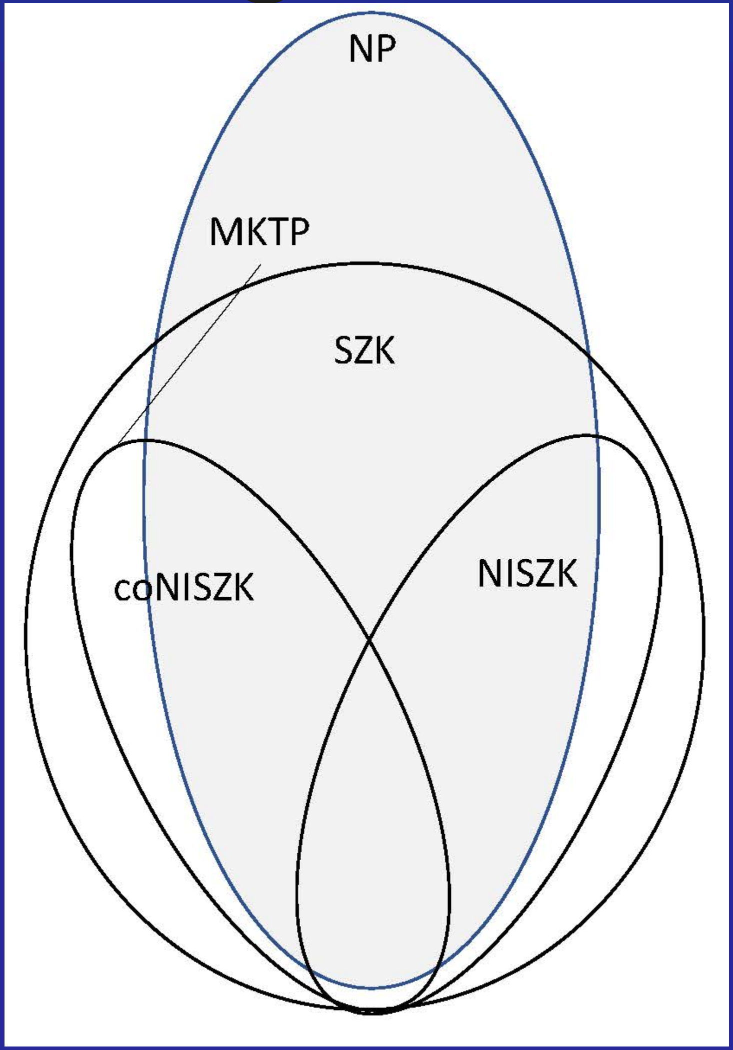
Randomized Reductions

- Let A and B be languages.
- We say A $\leq_m^{BPP}$ B if there is a polynomial-time-computable f such that
  - x ∈ A implies for most r, f(x,r) ∈ B
  - x ∉ A implies for most r, f(x,r) ∉ B
- Several close relatives of MCSP have been shown to be NP-complete under randomized reductions.

Sets NP-complete under $\leq_m^{BPP}$

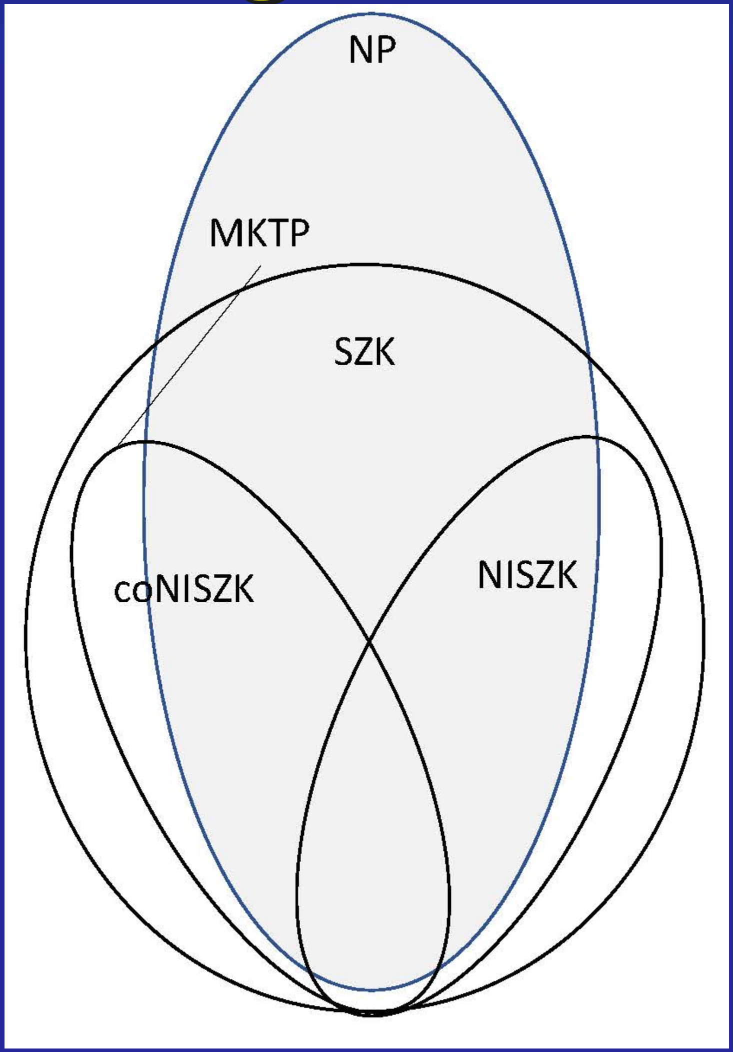
- Multi-Output MCSP [ILO 2020]
- Conditional KT complexity McKTP = {(x,y,i) : KT(x|y) ≤ i} [ACMTV] [Ilango 2020]
- MCSP* [Hirahara 2022]
- Can MCSP be far behind??

Zero Knowledge & K-Complexity



Non-Interactive Statistical Zero Knowledge

Zero Knowledge & K-Complexity



[GSV]: SZK $\leq_{tt}^{AC^0}$ NISZK (so NISZK is hard iff SZK is).

Approximating K-Complexity

- Let R denote the following promise problem:
- $R_Y = \{x : K(x) \geq |x|/2\}$
- $R_N = \{x : K(x) < |x|/2 - e(|x|)\}$
- …where e(|x|) is the "approximation error" term. Our results hold for any e(n) such that
- $\omega(\log n) < e(n) < n^{o(1)}$.
- For K-complexity experts: Our results hold for both plain and prefix-free K-complexity.

Zero Knowledge Characterized

- Let A be any decidable promise problem. Then the following are equivalent:
  - A is in NISZK
  - $A \leq_m^{BPP} R$
- This is the first time a well-studied complexity class has been characterized in terms of efficient reducibility to an undecidable problem!

Zero Knowledge Characterized

- Let A be any decidable promise problem. Then the following are equivalent:
  - A is in NISZK
  - A $\leq_m^{BPP}$ R
- Let A be any decidable promise problem. Then the following are equivalent:
  - A is in $NISZK_L$
  - A $\leq_m^{BPL}$ R
  - A $\leq_m^{BPNC^0}$ R

Why care about $NISZK_L$?

- Let A be any decidable promise problem. Then the following are equivalent:
  - A is in $NISZK_L$
  - $A \leq_m^{BPL} R$
  - $A \leq_m^{BPNC^0} R$
- Because we get projections!
  - For every A in $NISZK_L$
  - $A \leq_m^{proj} R$
  - $A \leq_m^{proj} R_{KT}$

What are projections?

Input

$x_1 \ \overline{x}_1 \quad x_2 \ \overline{x}_2 \quad \ldots \quad x_n \ \overline{x}_n$

$x_{34}\ 001\overline{x_{103}}\ 1110\ \ldots\ \overline{x_{n18}}$

Output

No gates! Just wires!

Why care about NISZK_L?

For every A in NISZK_L

– A $\leq_m^{proj}$ R

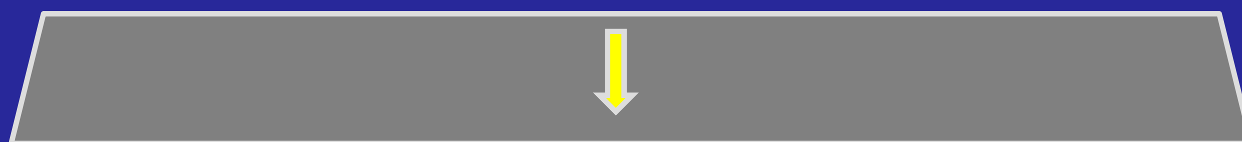
– A $\leq_m^{proj}$ R_{KT}

- R_{KT} is in coNP, and NL is contained in NISZK_L.
- Thus if NP=NL, there is a projection f, where
- f(000000…0) has high K-complexity, and
- f(anything random) has low K-complexity.

Transmutation

Input

$low\ information$



$high\ information$

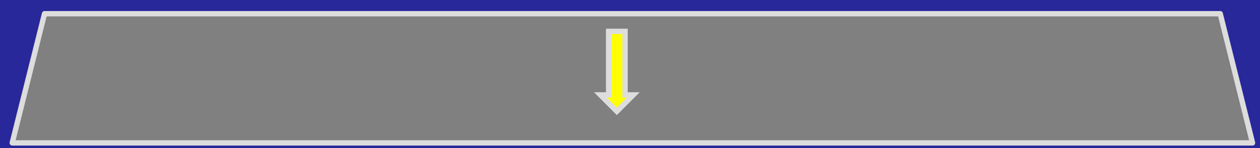
Output

No gates! Just wires!

Transmutation

Input

high information



low information

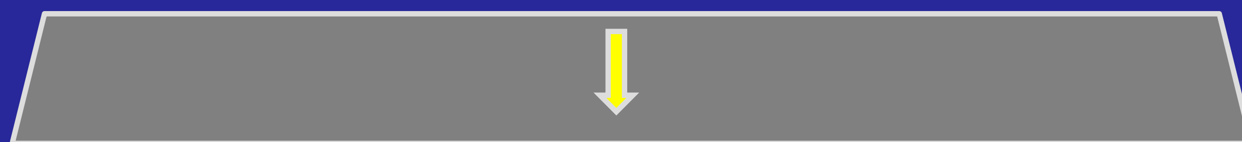
Output

No gates! Just wires!

Transmutation

Input

$high\ information$



$low\ information$

Such transmutation seems impossible.
Proving it's impossible shows NP≠NL.

More to the Meta-Complexity Saga

- Many exciting developments were not covered:
  - Connections to maching learning.
  - Probabilistic Kolmogorov Complexity.
  - …

A Pathway to Paradise?

- Is there really optimism that meta-complexity will help solve the long-standing open questions of complexity theory?
- Perhaps a little…
- Recent work has already overcome many apparent barriers. And Meta-Complexity has – at least – given us some new approaches.

A Pathway to Paradise?

- Is there really optimism that meta-complexity will help solve the long-standing open questions of complexity theory?

- Perhaps a little…
- We definitely expect further developments to bring us further along the road to true enlightenment.

References

- Ajtai, M. Sigma^1_1-formulae on finite structures. Annals of Pure and Applied Logic 24, 1983.
Allender, E., Mahdi Cheraghchi, Dimitrios Myrisiotis, Harsha Tirumala, and Ilya Volkovich. One-way functions and a conditional variant of MKTP. FSTTCS 2021.
Allender, E., Shuichi Hirahara, and Harsha Tirumala. Kolmogorov complexity characterizes statistical zero knowledge. ITCS 2023.
Baker, T., J. Gill, and R. Solovay. Relativizations of the P =? NP Question. SIAM J. Comput. (1975)
Buhrman, H. and Elvira Mayordomo. An excursion to the Kolmogorov random strings. Journal of Computer and System Sciences 54, 1997.
Chen, L., Hirahara, S., Oliveira, I.C., Pich, J., Rajgopal, N., Santhanam, R.: Beyond natural proofs: Hardness magnification and locality. ITCS 2020.
Cheraghchi, M., Hirahara, S., Myrisiotis, D., Yoshida, Y.: One-tape Turing machine and branching program lower bounds for MCSP. STACS 2021.
Cheraghchi, M., Kabanets, V., Lu, Z., Myrisiotis, D.: Circuit lower bounds for MCSP from local pseudorandom generators. ACM Trans. Comput. Theory 12, 2020.
Cook, S. The Complexity of Theorem-Proving Procedures. STOC 1971.
Fu, B.: Hardness of sparse sets and minimal circuit size problem. COCOON 2020.

References

- Furst, M., J. Saxe, and M. Sipser. Parity, circuits, and the polynomial-time hierarchy. Mathematical Systems Theory 17, 1984.
  Goldreich, O., Amit Sahai, and Salil Vadhan. Can statistical zero knowledge be made non-interactive? or On the relationship of SZK and NISZK. Crypto 1999.
  Hartmanis, J. and Richard E Stearns. On the computational complexity of algorithms. Transactions of the American Mathematical Society, 117:285–306, 1965.
  Hastad, J. Computational Limitations for Small Depth Circuits. MIT Press, Cambridge, MA, 1987.
  Hirahara, S. NP-hardness of learning programs and partial MCSP. FOCS 2022.
  Hirahara, S. Characterizing Average-Case Complexity of PH by Worst-Case Meta-Complexity. FOCS 2020.
  Hirahara, S.: Non-black-box worst-case to average-case reductions within NP. FOCS 2018.
  Ilango, R., Loff, B., Oliveira, I.C.: NP-hardness of circuit minimization for multioutput functions. CCC 2020.
  Ilango, R.: Constant depth formula and partial function versions of MCSP are hard. FOCS 2020.
  Impagliazzo, R. A personal view of average-case complexity. Structure in Complexity Theory. 1995.
  Kabanets, V. and J.-Y. Cai. Circuit minimization problem. In STOC, 2000.
  Karp, R. Reducibility among Combinatorial Problems. Complexity of Computer Computations 40, 1972.

References

- Levin, L. https://www.cs.bu.edu/fac/lnd/research/hard.htm
  Liu, Y., Pass, R.: On one-way functions and Kolmogorov complexity. FOCS 2020.
  Lund, C., Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. JACM, 39, 1992.
  McKay, D.M., Murray, C.D., Williams, R.R.: Weak lower bounds on resource-bounded compression imply strong separations of complexity classes. STOC, 2019.
  Murray, C., Williams, R.: On the (non) NP-hardness of computing circuit complexity. Theory of Computing 13, 2017.
  Oliveira, I.C., Pich, J., Santhanam, R.: Hardness magnification near state-of the-art lower bounds. CCC 2019.
  Razborov, A. Lower bounds on the size of bounded depth networks over a complete basis with logical addition. Mathematicheskie Zametki 41, 1987.
  Shamir, A. IP = PSPACE. JACM, 39, 1992.
  Smolensky, R. On representations by low-degree polynomials. FOCS, 1993.
  Tal, A.: The bipartite formula complexity of inner-product is quadratic. ECCC Report 16-181.
  Williams, R.R. Nonuniform ACC Circuit Lower Bounds. JACM 61, 2014.
  Yablonsky, S. On the Impossibility of Eliminating PEREBOR in Solving Some Problems of Circuit Theory, Doklady Akademii Nauk SSSR 124, 1959.
  Yao, A. Separating the polynomial-time hierarchy by oracles. FOCS, 1985.