CS 599: The Meta-Complexity Frontier, Fall 2023
Course Project Guidelines

The course project is an opportunity to perform an in-depth exploration of a topic in meta-complexity that interests you. The goals are to gain experience

- Independently reading and synthesizing research papers,
- Presenting research papers to an audience of your peers, and
- Formulating and carrying out a short-term research project.

You are not expected to produce publishable results by the end of the semester, but hopefully you will be able to lay the groundwork for something that can be further developed into publishable research. The main outcomes by the end of the semester will be:

1. A **one-hour presentation** for your classmates about the most interesting paper you encountered, accompanied by **slides** or **typeset lecture notes** if you choose to do a blackboard talk.
2. An **8 to 10 page typeset project report** about your research.

Projects may be done individually or in pairs. Some examples of possible projects include:

- Making progress on an open question in meta-complexity,
- Developing (new) connections between meta-complexity and another area (such as cryptography, learning theory, (uniform) derandomization, proof complexity, etc.) that interests you,
- Synthesizing several papers in the meta-complexity literature (which were not covered in detail in class),
- Something totally different! Be creative!

At the bottom of this document are several broad topic ideas with references to relevant papers. These are only intended for inspiration. You are highly encouraged to come up with your own topics, especially if they relate to your research interests. Please feel free to discuss your ideas with me and with each other throughout the semester, in office hours, or by email. **Auditors are welcome to complete projects and collaborate with registered students.**

To keep you on track with your project, there are several intermediate milestones. If you are working with a partner, you may submit a single set of any of these components.

Topic Ideas (Wednesday Nov. 1): Submit one to three possible topic ideas, with a paragraph describing each. For each topic, include the general question that may like to address, a list of relevant research papers that you plan to read, and one particular paper that you might like to present to the class. Submitting these ideas will encourage you start thinking about your project early, allow you to identify students with similar interests with whom you might like to collaborate, and let me give you preliminary suggestions for how to proceed.

Presentation Sign-Up (Wednesday Nov. 8): Each project group will present a paper or a few very closely related papers to the class. Individuals may choose either a Tuesday slot or a Thursday slot, and pairs should choose a Tuesday slot (with time split evenly between the two group members).

Project Proposal (Wednesday Nov. 15): Submit a page or two outlining what your project will look like. At this stage, you should be able to clearly state your research questions, describe how your project relates to prior work on the topic, and describe your plan of attack for addressing these questions.

Paper Presentation (Roughly Thursday Nov. 30 – Tuesday Dec. 12): Your presentation should clearly explain the main question(s) the paper addresses, provide the context and motivation for studying these questions, state the paper's main result(s), and give as detailed a proof sketch as is reasonable given the time constraints. You should also spend a few minutes describing your project and any new results you have to share. You may either use slides or do a blackboard presentation. A blackboard presentation should be accompanied by a set of typeset lecture notes similar to those appearing on the course website.

Project Report (Wednesday Dec. 13): Submit a paper (about 8 to 10 pages) describing your completed project. The paper should motivate your research questions and results, explain how the project fits into the context of previous work, and present the results in a clear and convincing manner.

These project and presentation guidelines are adapted from those used in other courses, including Jelani Nelson's "Algorithms for Big Data," Toni Pitassi's "Communication Complexity: Applications and New Directions," Salil Vadhan/Jon Ullman's "Mathematical Approaches to Data Privacy," and especially Mark Bun's "Communication Complexity."

Project/Presentation Topic Ideas

Below are a number of suggestions for possible project and presentation topics with a few representative references for each. These are just meant as inspiration to get you started thinking. You are in no way obligated to stick to these topics and are encouraged to explore topics that interest you. The references provided are not exhaustive and you will want to do additional research to find the state-of-the-art on each topic.

Formalizing & Interpreting the Relativization Barrier The relativization barrier we covered in class was not formulated as logical independence — the "gold standard" for precise unprovability results. Furthermore, fixing different oracle access mechanisms can change which statements are considered relativizing, because the contents of a complexity class relative to an oracle can shift. The papers below seek to better understand relativization and develop/debate a logical formulation of the barrier.

- S. Arora, R. Impagliazzo, U. V. Vazirani, Relativizing versus Nonrelativizing Techniques: the Role of Local Checkability.
- Lance Fortnow. "The Role of Relativization in Complexity Theory". In: *Bull. EATCS* 52 (1994), pp. 229–243

Algebrization Barrier The first blatantly non-relativizing separations all used *arithmetization* — a technique that transforms Boolean circuits into polynomials. In class we covered $\mathsf{MA\text{-}EXP} \not\subset \mathsf{P/poly}$ and referenced $\forall k\ \mathsf{MA}/1 \not\subset \mathsf{SIZE}[n^k]$ [BFT98; San09]. The Algebrization Barrier explains why arithmetization alone is not sufficient to solve major open problems in complexity theory, including NEXP vs. $\mathsf{P/poly}$. Many open questions remain about how to best understand and bypass algebrization.

- Scott Aaronson and Avi Wigderson. "Algebrization: A New Barrier in Complexity Theory". In: *ACM Trans. Comput. Theory* 1.1 (2009), 2:1–2:54. DOI: 10.1145/1490270.1490272. URL: https://doi.org/10.1145/1490270.1490272
- Russell Impagliazzo, Valentine Kabanets, and Antonina Kolokolova. "An axiomatic approach to algebrization". In: *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*. Ed. by Michael Mitzenmacher. ACM, 2009, pp. 695–704. ISBN: 978-1-60558-506-2. DOI: 10.1145/1536414.1536509. URL: https://doi.org/10.1145/1536414.1536509

- Baris Aydinlioglu and Eric Bach. "Affine Relativization: Unifying the Algebrization and Relativization Barriers". In: *ACM Trans. Comput. Theory* 10.1 (2018), 1:1–1:67. DOI: 10.1145/3170704. URL: https://doi.org/10.1145/3170704
- Baris Aydinlioglu and Eric Bach. "Corrigendum to Affine Relativization: Unifying the Algebrization and Relativization Barriers". In: *ACM Trans. Comput. Theory* 11.3 (2019), 16:1. DOI: 10.1145/3317693. URL: https://doi.org/10.1145/3317693

Bounded Relativization Barrier We covered only a *small subset* of results about the Bounded Relativization barrier in class, and the paper introduces many interesting open problems. In particular it would be intresting to study the complexity of oracles related to the *algorithmic method*, cited below.

- Shuichi Hirahara, Zhenjian Lu, and Hanlin Ren. "Bounded Relativization". In: *38th Computational Complexity Conference, CCC 2023, July 17-20, 2023, Warwick, UK*. ed. by Amnon Ta-Shma. Vol. 264. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 6:1–6:45. DOI: 10.4230/LIPIcs.CCC.2023.6. URL: https://doi.org/10.4230/LIPIcs.CCC.2023.6
- Nikhil Vyas and Ryan Williams. "On Oracles and Algorithmic Methods for Proving Lower Bounds". In: *14th Innovations in Theoretical Computer Science Conference, ITCS 2023, January 10-13, 2023, MIT, Cambridge, Massachusetts, USA*. ed. by Yael Tauman Kalai. Vol. 251. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 99:1–99:26. ISBN: 978-3-95977-263-1. DOI: 10.4230/LIPIcs.ITCS.2023.99. URL: https://doi.org/10.4230/LIPIcs.ITCS.2023.99

Formalizing the Natural Proofs Barrier Our treatment of the Natural Proofs barrier required a human to "naturalize" each proof by extracting a natural property. In fact, there are formal (logical) characterizations of the Natural Proofs barrier, but they are far from the strongest version of the barrier that one might conjecture — something like "if cryptography exists, then P vs. NP is independent of a rich first-order theory (like Peano Arithmetic)." These papers give increasingly refined logical formulations of the Natural Proofs barrier and related concepts. Especially in the recent papers, there are many open problems about meta-mathematics of complexity and learning theory.

- Razborov, Unprovability of Lower Bounds on the Circuit Size in Certain Fragments of Bounded Arithmetic, in Izvestiya of the Russian Academy of Science, mathematics, Vol. 59, No 1, 1995, pages 201-224.
- Jan Krajicek. "Interpolation Theorems, Lower Bounds for Proof Systems, and Independence Results for Bounded Arithmetic". In: *J. Symb. Log.* 62.2 (1997), pp. 457–486. DOI: 10.2307/2275541. URL: https://doi.org/10.2307/2275541
- Moritz Müller and Ján Pich. "Feasibly constructive proofs of succinct weak circuit lower bounds". In: *Ann. Pure Appl. Log.* 171.2 (2020). DOI: 10.1016/j.apal.2019.102735. URL: https://doi.org/10.1016/j.apal.2019.102735
- Ján Pich. "Learning algorithms from circuit lower bounds". In: *CoRR* abs/2012.14095 (2020). arXiv: 2012.14095. URL: https://arxiv.org/abs/2012.14095
- Ján Pich and Rahul Santhanam. "Learning Algorithms Versus Automatability of Frege Systems". In: *49th International Colloquium on Automata, Languages, and Programming, ICALP 2022, July 4-8, 2022, Paris, France*. Ed. by Mikolaj Bojanczyk, Emanuela Merelli, and David P. Woodruff. Vol. 229. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 101:1–101:20. ISBN: 978-3-95977-235-8. DOI: 10.4230/LIPIcs.ICALP.2022.101. URL: https://doi.org/10.4230/LIPIcs.ICALP.2022.101

Hardness of Proving NP-Hardness of MCSP Beginning with the landmark paper of Kabanets and Cai, the difficulty of proving (NP-)hardness of MCSP using "simple" reductions has been intensively studied. In some cases, it is even *impossible* for MCSP to be hard under "sufficiently weak" reductions. If you select this topic, you must choose a paper *besides* "Circuit minimization problem" by Kabanets and Cai for your in-class presentation.

- Valentine Kabanets and Jin-yi Cai. "Circuit minimization problem". In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*. 2000, pp. 73–79. DOI: 10.1145/335305.335314. URL: https://doi.org/10.1145/335305.335314
- Cody D. Murray and R. Ryan Williams. "On the (Non) NP-Hardness of Computing Circuit Complexity". In: *Theory Comput.* 13.1 (2017), pp. 1–22. DOI: 10.4086/toc.2017.v013a004. URL: https://doi.org/10.4086/toc.2017.v013a004
- Michael E. Saks and Rahul Santhanam. "Circuit Lower Bounds from NP-Hardness of MCSP Under Turing Reductions". In: *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*. Ed. by Shubhangi Saraf. Vol. 169. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 26:1–26:13. ISBN: 978-3-95977-156-6. DOI: 10.4230/LIPIcs.CCC.2020.26. URL: https://doi.org/10.4230/LIPIcs.CCC.2020.26
- Eric Allender, Rahul Ilango, and Neekon Vafa. "The Non-hardness of Approximating Circuit Size". In: *Theory Comput. Syst.* 65.3 (2021), pp. 559–578. DOI: 10.1007/s00224-020-10004-x. URL: https://doi.org/10.1007/s00224-020-10004-x

NP-Hardness of MCSP Variants Despite the above, recently there have been exciting breakthroughs showing that *minor variations* on MCSP — such as limiting to weaker classes than general circuits or expanding to consider partial functions — are indeed NP-hard. Are we to a proof that "vanilla" MCSP is NP-hard? Why or why not? Many of the reductions used in these proofs are randomized or adaptive; is that necessary?

- Shuichi Hirahara, Igor C. Oliveira, and Rahul Santhanam. "NP-hardness of Minimum Circuit Size Problem for OR-AND-MOD Circuits". In: *33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA*. ed. by Rocco A. Servedio. Vol. 102. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018, 5:1–5:31. ISBN: 978-3-95977-069-9. DOI: 10.4230/LIPIcs.CCC.2018.5. URL: https://doi.org/10.4230/LIPIcs.CCC.2018.5
- Rahul Ilango, Bruno Loff, and Igor C. Oliveira. "NP-Hardness of Circuit Minimization for Multi-Output Functions". In: *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*. Ed. by Shubhangi Saraf. Vol. 169. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 22:1–22:36. ISBN: 978-3-95977-156-6. DOI: 10.4230/LIPIcs.CCC.2020.22. URL: https://doi.org/10.4230/LIPIcs.CCC.2020.22
- Rahul Ilango. "The Minimum Formula Size Problem is (ETH) Hard". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 427–432. ISBN: 978-1-6654-2055-6. DOI: 10.1109/FOCS52979.2021.00050. URL: https://doi.org/10.1109/FOCS52979.2021.00050
- Shuichi Hirahara. "NP-Hardness of Learning Programs and Partial MCSP". in: *63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 - November 3, 2022*. IEEE, 2022, pp. 968–979. ISBN: 978-1-6654-5519-0. DOI: 10.1109/FOCS54457.2022.00095. URL: https://doi.org/10.1109/FOCS54457.2022.00095

Lower Bounds for MCSP Against Weak Models NP-hardness is still conditional; we do not (yet?) know a separation between P and NP. We can prove *unconditional* lower bounds for simple explicit functions like XOR and MAJORITY against models like bounded-depth circuits — what about MCSP? These results are deeply connected to the theory of pseudorandom generators.

- Alexander Golovnev et al. "$AC^0[p]$ Lower Bounds Against MCSP via the Coin Problem". In: *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Patras, Greece*. Ed. by Christel Baier et al. Vol. 132. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019, 66:1–66:15. ISBN: 978-3-95977-109-2. DOI: 10.4230/LIPIcs.ICALP.2019.66. URL: https://doi.org/10.4230/LIPIcs.ICALP.2019.66
- Mahdi Cheraghchi et al. "Circuit Lower Bounds for MCSP from Local Pseudorandom Generators". In: *ACM Trans. Comput. Theory* 12.3 (2020), 21:1–21:27. DOI: 10.1145/3404860. URL: https://doi.org/10.1145/3404860

- See Theorem 1.6 of Rahul Ilango. “Approaching MCSP from Above and Below: Hardness for a Conditional Variant and AC0p”. In: *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA*. ed. by Thomas Vidick. Vol. 151. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 34:1–34:26. ISBN: 978-3-95977-134-4. DOI: 10.4230/LIPIcs.ITCS.2020.34. URL: https://doi.org/10.4230/LIPIcs.ITCS.2020.34
- Mahdi Cheraghchi et al. “One-Tape Turing Machine and Branching Program Lower Bounds for MCSP”. in: *38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021, March 16-19, 2021, Saarbrücken, Germany (Virtual Conference)*. Ed. by Markus Bläser and Benjamin Monmege. Vol. 187. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 23:1–23:19. ISBN: 978-3-95977-180-1. DOI: 10.4230/LIPIcs.STACS.2021.23. URL: https://doi.org/10.4230/LIPIcs.STACS.2021.23

Meta-Complexity in Relativized Worlds How does the relativization barrier impede progress in meta-complexity? These papers construct oracles to show that key conjectures in meta-complexity are non-relativizing statements.

- Ker-I Ko. “On the Complexity of Learning Minimum Time-Bounded Turing Machines”. In: *SIAM J. Comput.* 20.5 (1991), pp. 962–986. DOI: 10.1137/0220059. URL: https://doi.org/10.1137/0220059
- Shuichi Hirahara and Osamu Watanabe. “Limits of Minimum Circuit Size Problem as Oracle”. In: *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan.* Ed. by Ran Raz. Vol. 50. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016, 18:1–18:20. ISBN: 978-3-95977-008-8. DOI: 10.4230/LIPIcs.CCC.2016.18. URL: https://doi.org/10.4230/LIPIcs.CCC.2016.18
- Hanlin Ren and Rahul Santhanam. “A Relativization Perspective on Meta-Complexity”. In: *39th International Symposium on Theoretical Aspects of Computer Science, STACS 2022, March 15-18, 2022, Marseille, France (Virtual Conference)*. Ed. by Petra Berenbrink and Benjamin Monmege. Vol. 219. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 54:1–54:13. ISBN: 978-3-95977-222-8. DOI: 10.4230/LIPIcs.STACS.2022.54. URL: https://doi.org/10.4230/LIPIcs.STACS.2022.54

Learning Theory See:

- Marco L. Carmosino et al. “Learning Algorithms from Natural Proofs”. In: *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan.* Ed. by Ran Raz. Vol. 50. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016, 10:1–10:24. DOI: 10.4230/LIPIcs.CCC.2016.10. URL: https://doi.org/10.4230/LIPIcs.CCC.2016.10
- Shuichi Hirahara and Mikito Nanashima. “On Worst-Case Learning in Relativized Heuristica”. In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022.* IEEE, 2021, pp. 751–758. ISBN: 978-1-6654-2055-6. DOI: 10.1109/FOCS52979.2021.00078. URL: https://doi.org/10.1109/FOCS52979.2021.00078
- Shuichi Hirahara and Mikito Nanashima. “Learning in Pessiland via Inductive Inference”. In: *Electron. Colloquium Comput. Complex.* TR23-100 (2023). ECCC: TR23-100. URL: https://eccc.weizmann.ac.il/report/2023/100
- Halley Goldberg and Valentine Kabanets. “Improved Learning from Kolmogorov Complexity”. In: *38th Computational Complexity Conference, CCC 2023, July 17-20, 2023, Warwick, UK*. ed. by Amnon Ta-Shma. Vol. 264. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 12:1–12:29. ISBN: 978-3-95977-282-2. DOI: 10.4230/LIPIcs.CCC.2023.12. URL: https://doi.org/10.4230/LIPIcs.CCC.2023.12

Cryptography See:

- Yanyi Liu and Rafael Pass. "On One-way Functions and Kolmogorov Complexity". In: *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020*. Ed. by Sandy Irani. IEEE, 2020, pp. 1243–1254. ISBN: 978-1-7281-9621-3. DOI: 10.1109/FOCS46700.2020.00118. URL: https://doi.org/10.1109/FOCS46700.2020.00118
- Hanlin Ren and Rahul Santhanam. "Hardness of KT Characterizes Parallel Cryptography". In: *36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference)*. Ed. by Valentine Kabanets. Vol. 200. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 35:1–35:58. ISBN: 978-3-95977-193-1. DOI: 10.4230/LIPIcs.CCC.2021.35. URL: https://doi.org/10.4230/LIPIcs.CCC.2021.35
- Yanyi Liu and Rafael Pass. "On One-Way Functions from NP-Complete Problems". In: *37th Computational Complexity Conference, CCC 2022, July 20-23, 2022, Philadelphia, PA, USA*. ed. by Shachar Lovett. Vol. 234. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 36:1–36:24. ISBN: 978-3-95977-241-9. DOI: 10.4230/LIPIcs.CCC.2022.36. URL: https://doi.org/10.4230/LIPIcs.CCC.2022.36
- Shuichi Hirahara et al. "A Duality between One-Way Functions and Average-Case Symmetry of Information". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*. Ed. by Barna Saha and Rocco A. Servedio. ACM, 2023, pp. 1039–1050. ISBN: 978-1-4503-9913-5. DOI: 10.1145/3564246.3585138. URL: https://doi.org/10.1145/3564246.3585138

Derandomization See:

- Eric Allender et al. "Power from Random Strings". In: *SIAM J. Comput.* 35.6 (2006), pp. 1467–1493. DOI: 10.1137/050628994. URL: https://doi.org/10.1137/050628994

First-Order Proof Complexity Meta-mathematics of computational complexity — both lower and upper bounds.

- Stephen A. Cook and Jan Krajicek. "Consequences of the provability of $NP \subseteq P/poly$". In: *J. Symb. Log.* 72.4 (2007), pp. 1353–1371. DOI: 10.2178/jsl/1203350791. URL: https://doi.org/10.2178/jsl/1203350791
- Jan Krajicek and Igor C. Oliveira. "Unprovability of circuit upper bounds in Cook's theory PV". in: *Log. Methods Comput. Sci.* 13.1 (2017). DOI: 10.23638/LMCS-13(1:4)2017. URL: https://doi.org/10.23638/LMCS-13(1:4)2017
- Marco Carmosino et al. "LEARN-Uniform Circuit Lower Bounds and Provability in Bounded Arithmetic". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 770–780. ISBN: 978-1-6654-2055-6. DOI: 10.1109/FOCS52979.2021.00080. URL: https://doi.org/10.1109/FOCS52979.2021.00080
- Ján Pich and Rahul Santhanam. "Strong co-nondeterministic lower bounds for NP cannot be proved feasibly". In: *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*. Ed. by Samir Khuller and Virginia Vassilevska Williams. ACM, 2021, pp. 223–233. ISBN: 978-1-4503-8053-9. DOI: 10.1145/3406325.3451117. URL: https://doi.org/10.1145/3406325.3451117
- Jiatu Li and Igor C. Oliveira. "Unprovability of Strong Complexity Lower Bounds in Bounded Arithmetic". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*. Ed. by Barna Saha and Rocco A. Servedio. ACM, 2023, pp. 1051–1057. ISBN: 978-1-4503-9913-5. DOI: 10.1145/3564246.3585144. URL: https://doi.org/10.1145/3564246.3585144

References

[22] *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2022. ISBN: 978-1-6654-2055-6. DOI: 10.1109/FOCS52979.2022. URL: https://doi.org/10.1109/FOCS52979.2022.

[AB18] Baris Aydinlioglu and Eric Bach. "Affine Relativization: Unifying the Algebrization and Relativization Barriers". In: *ACM Trans. Comput. Theory* 10.1 (2018), 1:1–1:67. DOI: 10.1145/3170704. URL: https://doi.org/10.1145/3170704.

[AB19] Baris Aydinlioglu and Eric Bach. "Corrigendum to Affine Relativization: Unifying the Algebrization and Relativization Barriers". In: *ACM Trans. Comput. Theory* 11.3 (2019), 16:1. DOI: 10.1145/3317693. URL: https://doi.org/10.1145/3317693.

[AIV21] Eric Allender, Rahul Ilango, and Neekon Vafa. "The Non-hardness of Approximating Circuit Size". In: *Theory Comput. Syst.* 65.3 (2021), pp. 559–578. DOI: 10.1007/s00224-020-10004-x. URL: https://doi.org/10.1007/s00224-020-10004-x.

[All+06] Eric Allender et al. "Power from Random Strings". In: *SIAM J. Comput.* 35.6 (2006), pp. 1467–1493. DOI: 10.1137/050628994. URL: https://doi.org/10.1137/050628994.

[AW09] Scott Aaronson and Avi Wigderson. "Algebrization: A New Barrier in Complexity Theory". In: *ACM Trans. Comput. Theory* 1.1 (2009), 2:1–2:54. DOI: 10.1145/1490270.1490272. URL: https://doi.org/10.1145/1490270.1490272.

[BFT98] Harry Buhrman, Lance Fortnow, and Thomas Thierauf. "Nonrelativizing Separations". In: *Proceedings of the 13th Annual IEEE Conference on Computational Complexity, Buffalo, New York, USA, June 15-18, 1998*. IEEE Computer Society, 1998, pp. 8–12. DOI: 10.1109/CCC.1998.694585. URL: https://doi.org/10.1109/CCC.1998.694585.

[Car+16] Marco L. Carmosino et al. "Learning Algorithms from Natural Proofs". In: *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*. Ed. by Ran Raz. Vol. 50. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016, 10:1–10:24. DOI: 10.4230/LIPIcs.CCC.2016.10. URL: https://doi.org/10.4230/LIPIcs.CCC.2016.10.

[Car+21] Marco Carmosino et al. "LEARN-Uniform Circuit Lower Bounds and Provability in Bounded Arithmetic". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 770–780. ISBN: 978-1-6654-2055-6. DOI: 10.1109/FOCS52979.2021.00080. URL: https://doi.org/10.1109/FOCS52979.2021.00080.

[Che+20] Mahdi Cheraghchi et al. "Circuit Lower Bounds for MCSP from Local Pseudorandom Generators". In: *ACM Trans. Comput. Theory* 12.3 (2020), 21:1–21:27. DOI: 10.1145/3404860. URL: https://doi.org/10.1145/3404860.

[Che+21] Mahdi Cheraghchi et al. "One-Tape Turing Machine and Branching Program Lower Bounds for MCSP". In: *38th International Symposium on Theoretical Aspects of Computer Science, STACS 2021, March 16-19, 2021, Saarbrücken, Germany (Virtual Conference)*. Ed. by Markus Bläser and Benjamin Monmege. Vol. 187. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 23:1–23:19. ISBN: 978-3-95977-180-1. DOI: 10.4230/LIPIcs.STACS.2021.23. URL: https://doi.org/10.4230/LIPIcs.STACS.2021.23.

[CK07] Stephen A. Cook and Jan Krajicek. "Consequences of the provability of $NP \subseteq P/poly$". In: *J. Symb. Log.* 72.4 (2007), pp. 1353–1371. DOI: 10.2178/jsl/1203350791. URL: https://doi.org/10.2178/jsl/1203350791.

[For94] Lance Fortnow. "The Role of Relativization in Complexity Theory". In: *Bull. EATCS* 52 (1994), pp. 229–243.

[GK23] Halley Goldberg and Valentine Kabanets. "Improved Learning from Kolmogorov Complexity". In: *38th Computational Complexity Conference, CCC 2023, July 17-20, 2023, Warwick, UK*. Ed. by Amnon Ta-Shma. Vol. 264. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 12:1–12:29. ISBN: 978-3-95977-282-2. DOI: 10.4230/LIPIcs.CCC.2023.12. URL: https://doi.org/10.4230/LIPIcs.CCC.2023.12.

[Gol+19] Alexander Golovnev et al. "$AC^0[p]$ Lower Bounds Against MCSP via the Coin Problem". In: *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Patras, Greece*. Ed. by Christel Baier et al. Vol. 132. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019, 66:1–66:15. ISBN: 978-3-95977-109-2. DOI: 10.4230/LIPIcs.ICALP.2019.66. URL: https://doi.org/10.4230/LIPIcs.ICALP.2019.66.

[Hir+23] Shuichi Hirahara et al. "A Duality between One-Way Functions and Average-Case Symmetry of Information". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*. Ed. by Barna Saha and Rocco A. Servedio. ACM, 2023, pp. 1039–1050. ISBN: 978-1-4503-9913-5. DOI: 10.1145/3564246.3585138. URL: https://doi.org/10.1145/3564246.3585138.

[Hir22] Shuichi Hirahara. "NP-Hardness of Learning Programs and Partial MCSP". In: *63rd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2022, Denver, CO, USA, October 31 - November 3, 2022*. IEEE, 2022, pp. 968–979. ISBN: 978-1-6654-5519-0. DOI: 10.1109/FOCS54457.2022.00095. URL: https://doi.org/10.1109/FOCS54457.2022.00095.

[HLR23] Shuichi Hirahara, Zhenjian Lu, and Hanlin Ren. "Bounded Relativization". In: *38th Computational Complexity Conference, CCC 2023, July 17-20, 2023, Warwick, UK*. Ed. by Amnon Ta-Shma. Vol. 264. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 6:1–6:45. DOI: 10.4230/LIPIcs.CCC.2023.6. URL: https://doi.org/10.4230/LIPIcs.CCC.2023.6.

[HN21] Shuichi Hirahara and Mikito Nanashima. "On Worst-Case Learning in Relativized Heuristica". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 751–758. ISBN: 978-1-6654-2055-6. DOI: 10.1109/FOCS52979.2021.00078. URL: https://doi.org/10.1109/FOCS52979.2021.00078.

[HN23] Shuichi Hirahara and Mikito Nanashima. "Learning in Pessiland via Inductive Inference". In: *Electron. Colloquium Comput. Complex.* TR23-100 (2023). ECCC: TR23-100. URL: https://eccc.weizmann.ac.il/report/2023/100.

[HOS18] Shuichi Hirahara, Igor C. Oliveira, and Rahul Santhanam. "NP-hardness of Minimum Circuit Size Problem for OR-AND-MOD Circuits". In: *33rd Computational Complexity Conference, CCC 2018, June 22-24, 2018, San Diego, CA, USA*. Ed. by Rocco A. Servedio. Vol. 102. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018, 5:1–5:31. ISBN: 978-3-95977-069-9. DOI: 10.4230/LIPIcs.CCC.2018.5. URL: https://doi.org/10.4230/LIPIcs.CCC.2018.5.

[HW16] Shuichi Hirahara and Osamu Watanabe. "Limits of Minimum Circuit Size Problem as Oracle". In: *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*. Ed. by Ran Raz. Vol. 50. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016, 18:1–18:20. ISBN: 978-3-95977-008-8. DOI: 10.4230/LIPIcs.CCC.2016.18. URL: https://doi.org/10.4230/LIPIcs.CCC.2016.18.

[IKK09] Russell Impagliazzo, Valentine Kabanets, and Antonina Kolokolova. "An axiomatic approach to algebrization". In: *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*. Ed. by Michael Mitzenmacher. ACM, 2009, pp. 695–704. ISBN: 978-1-60558-506-2. DOI: 10.1145/1536414.1536509. URL: https://doi.org/10.1145/1536414.1536509.

[Ila20] Rahul Ilango. "Approaching MCSP from Above and Below: Hardness for a Conditional Variant and AC0p". In: *11th Innovations in Theoretical Computer Science Conference, ITCS 2020, January 12-14, 2020, Seattle, Washington, USA*. Ed. by Thomas Vidick. Vol. 151. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 34:1–34:26. ISBN: 978-3-95977-134-4. DOI: 10.4230/LIPIcs.ITCS.2020.34. URL: https://doi.org/10.4230/LIPIcs.ITCS.2020.34.

[Ila21] Rahul Ilango. "The Minimum Formula Size Problem is (ETH) Hard". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 427–432. ISBN: 978-1-6654-2055-6. DOI: 10.1109/FOCS52979.2021.00050. URL: https://doi.org/10.1109/FOCS52979.2021.00050.

[ILO20] Rahul Ilango, Bruno Loff, and Igor C. Oliveira. "NP-Hardness of Circuit Minimization for Multi-Output Functions". In: *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*. Ed. by Shubhangi Saraf. Vol. 169. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 22:1–22:36. ISBN: 978-3-95977-156-6. DOI: 10.4230/LIPIcs.CCC.2020.22. URL: https://doi.org/10.4230/LIPIcs.CCC.2020.22.

[KC00] Valentine Kabanets and Jin-yi Cai. "Circuit minimization problem". In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*. 2000, pp. 73–79. DOI: 10.1145/335305.335314. URL: https://doi.org/10.1145/335305.335314.

[KO17] Jan Krajicek and Igor C. Oliveira. "Unprovability of circuit upper bounds in Cook's theory PV". In: *Log. Methods Comput. Sci.* 13.1 (2017). DOI: 10.23638/LMCS-13(1:4)2017. URL: https://doi.org/10.23638/LMCS-13(1:4)2017.

[Ko91] Ker-I Ko. "On the Complexity of Learning Minimum Time-Bounded Turing Machines". In: *SIAM J. Comput.* 20.5 (1991), pp. 962–986. DOI: 10.1137/0220059. URL: https://doi.org/10.1137/0220059.

[Kra97] Jan Krajicek. "Interpolation Theorems, Lower Bounds for Proof Systems, and Independence Results for Bounded Arithmetic". In: *J. Symb. Log.* 62.2 (1997), pp. 457–486. DOI: 10.2307/2275541. URL: https://doi.org/10.2307/2275541.

[LO23] Jiatu Li and Igor C. Oliveira. "Unprovability of Strong Complexity Lower Bounds in Bounded Arithmetic". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*. Ed. by Barna Saha and Rocco A. Servedio. ACM, 2023, pp. 1051–1057. ISBN: 978-1-4503-9913-5. DOI: 10.1145/3564246.3585144. URL: https://doi.org/10.1145/3564246.3585144.

[LP20] Yanyi Liu and Rafael Pass. "On One-way Functions and Kolmogorov Complexity". In: *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS 2020, Durham, NC, USA, November 16-19, 2020*. Ed. by Sandy Irani. IEEE, 2020, pp. 1243–1254. ISBN: 978-1-7281-9621-3. DOI: 10.1109/FOCS46700.2020.00118. URL: https://doi.org/10.1109/FOCS46700.2020.00118.

[LP22] Yanyi Liu and Rafael Pass. "On One-Way Functions from NP-Complete Problems". In: *37th Computational Complexity Conference, CCC 2022, July 20-23, 2022, Philadelphia, PA, USA*. Ed. by Shachar Lovett. Vol. 234. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 36:1–36:24. ISBN: 978-3-95977-241-9. DOI: 10.4230/LIPIcs.CCC.2022.36. URL: https://doi.org/10.4230/LIPIcs.CCC.2022.36.

[MP20] Moritz Müller and Ján Pich. "Feasibly constructive proofs of succinct weak circuit lower bounds". In: *Ann. Pure Appl. Log.* 171.2 (2020). DOI: 10.1016/j.apal.2019.102735. URL: https://doi.org/10.1016/j.apal.2019.102735.

[MW17] Cody D. Murray and R. Ryan Williams. "On the (Non) NP-Hardness of Computing Circuit Complexity". In: *Theory Comput.* 13.1 (2017), pp. 1–22. DOI: 10.4086/toc.2017.v013a004. URL: https://doi.org/10.4086/toc.2017.v013a004.

[Pic20] Ján Pich. "Learning algorithms from circuit lower bounds". In: *CoRR* abs/2012.14095 (2020). arXiv: 2012.14095. URL: https://arxiv.org/abs/2012.14095.

[PS21] Ján Pich and Rahul Santhanam. "Strong co-nondeterministic lower bounds for NP cannot be proved feasibly". In: *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*. Ed. by Samir Khuller and Virginia Vassilevska Williams. ACM, 2021, pp. 223–233. ISBN: 978-1-4503-8053-9. DOI: 10.1145/3406325.3451117. URL: https://doi.org/10.1145/3406325.3451117.

[PS22] Ján Pich and Rahul Santhanam. “Learning Algorithms Versus Automatability of Frege Systems”. In: *49th International Colloquium on Automata, Languages, and Programming, ICALP 2022, July 4-8, 2022, Paris, France*. Ed. by Mikolaj Bojanczyk, Emanuela Merelli, and David P. Woodruff. Vol. 229. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 101:1–101:20. ISBN: 978-3-95977-235-8. DOI: 10.4230/LIPIcs.ICALP.2022.101. URL: https://doi.org/10.4230/LIPIcs.ICALP.2022.101.

[RS21] Hanlin Ren and Rahul Santhanam. “Hardness of KT Characterizes Parallel Cryptography”. In: *36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference)*. Ed. by Valentine Kabanets. Vol. 200. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 35:1–35:58. ISBN: 978-3-95977-193-1. DOI: 10.4230/LIPIcs.CCC.2021.35. URL: https://doi.org/10.4230/LIPIcs.CCC.2021.35.

[RS22] Hanlin Ren and Rahul Santhanam. “A Relativization Perspective on Meta-Complexity”. In: *39th International Symposium on Theoretical Aspects of Computer Science, STACS 2022, March 15-18, 2022, Marseille, France (Virtual Conference)*. Ed. by Petra Berenbrink and Benjamin Monmege. Vol. 219. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022, 54:1–54:13. ISBN: 978-3-95977-222-8. DOI: 10.4230/LIPIcs.STACS.2022.54. URL: https://doi.org/10.4230/LIPIcs.STACS.2022.54.

[San09] Rahul Santhanam. “Circuit Lower Bounds for Merlin–Arthur Classes”. In: *SIAM J. Comput.* 39.3 (2009), pp. 1038–1061. DOI: 10.1137/070702680. URL: https://doi.org/10.1137/070702680.

[Sar20] Shubhangi Saraf, ed. *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*. Vol. 169. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. ISBN: 978-3-95977-156-6. URL: https://www.dagstuhl.de/dagpub/978-3-95977-156-6.

[SS20] Michael E. Saks and Rahul Santhanam. “Circuit Lower Bounds from NP-Hardness of MCSP Under Turing Reductions”. In: *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*. Ed. by Shubhangi Saraf. Vol. 169. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 26:1–26:13. ISBN: 978-3-95977-156-6. DOI: 10.4230/LIPIcs.CCC.2020.26. URL: https://doi.org/10.4230/LIPIcs.CCC.2020.26.

[SS23] Barna Saha and Rocco A. Servedio, eds. *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*. ACM, 2023. ISBN: 978-1-4503-9913-5. DOI: 10.1145/3564246. URL: https://doi.org/10.1145/3564246.

[VW23] Nikhil Vyas and Ryan Williams. “On Oracles and Algorithmic Methods for Proving Lower Bounds”. In: *14th Innovations in Theoretical Computer Science Conference, ITCS 2023, January 10-13, 2023, MIT, Cambridge, Massachusetts, USA*. Ed. by Yael Tauman Kalai. Vol. 251. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 99:1–99:26. ISBN: 978-3-95977-263-1. DOI: 10.4230/LIPIcs.ITCS.2023.99. URL: https://doi.org/10.4230/LIPIcs.ITCS.2023.99.