CURRICULUM VITAE

Pavel Hrubeš

E-mail address: pahrubes@gmail.com
Date of birth: 5/5/1980
Nationality: Czech

EDUCATION

Charles University in Prague 2004-2007
Ph.D. degree in mathematics. The theme of the Ph.D. work was 'proof complexity' and the supervisor Pavel Pudlák.

Charles University in Prague, 1998-2004.
Master's degree in mathematics and philosophy.

EMPLOYMENT AND EXPERIENCE

Institute of Mathematics, Czech Academy of Science, March 2014 - present time.
Researcher.

University of Washington, March 2013 - March 2014.
Postdoctoral fellow in theoretical computer science.

University of Calgary, November 2010 - November 2012.
Postdoctoral fellow in theoretical computer science.

Center for Computational Intractability, Princeton, September 2009 - September 2010.
Postdoctoral fellow in theoretical computer science.

Institute for Advanced Study, Princeton, September 2008- August 2009.
Postdoctoral fellow in theoretical computer science/ discrete mathematics group, headed by Avi Wigderson.

University of Toronto, January 2008 - July 2008. Postdoctoral fellow at the Department of Computer Science, theory group. The supervisor was Stephen Cook.

Czech Academy of Science, 2004 - 2007.
Part-time research position.

Ludwig-Maximilian University, Munich, 2006. Short-term MATHLOGAPS position.

RESEARCH INTERESTS

Proof complexity.
Complexity of proofs in propositional logic, non-classical logics, and algebraic proof systems.

Algebraic circuit complexity.
Sizes of algebraic circuits computing symbolic polynomials.

Mathematical logic and philosophy of mathematics
Questions concerning logical structure of mathematical reasoning.

AWARDS AND INVITED LECTURES

25th International Conference on Computer Aided Verification, Saint Petersburg, Russia, 2013 Invited lecture with title *The interpolation technique in proof complexity.*

Winter meeting of Association for Symbolic Logic, San Diego, USA, 2008 Invited lecture with title *Proof complexity after* $NP \neq coNP$.

Kurt Gödel Centenary Research Prize Fellowship, 2006

PUBLICATIONS

[1] P. Hrubeš and A. Yehudayoff. Shadows of newton polytopes. *ECCC*, 2021.

[2] P. Hrubeš. On the complexity of computing a random Boolean function over the reals. *Theory of Computing*, 16(9):1–12, 2020.

[3] P. Hrubeš and P. Pudlák. Random formulas, monotone circuits, and interpolation. In *FOCS*, pages 121–131, 2017.

[4] P. Hrubeš and P. Pudlák. A note on monotone real circuits. *Information Processing Letters*, 131:15–19, 2018.

[5] B. Shai, P. Hrubeš, S. Moran, A. Shpilka, and A. Yehudayoff. Learnability can be undecidable. *Nature Machine Intelligence*, 1(1):44–49, 2019.

[6] P. Hrubeš. On the distribution of runners on a circle. *European Journal of Combinatorics*, 89, 2020.

[7] P. Hrubeš. On ϵ-sensitive monotone computations. *Computational Complexity*, 29(2), 2020.

[8] P. Hrubeš, S. N. Ramamoorthy, A. Rao, and A. Yehudayoff. Lower bounds for balancing families and depth-two circuits. In *LIPICS*, 2019.

[9] P. Hrubeš and A. Wigderson. Non-commutative circuits with division. *ITCS*, 2014.

[10] P. Hrubeš and I. Tzameret. Short proofs for the determinant identities. *SIAM J. Comput.*, 44(2):193–2012, 2015.

[11] P. Hrubeš. On families of anticommuting matrices. *Linear Algebra and Applications*, 493:494–507, 2016.

[12] P. Hrubeš. On hardness of multilinearization and VNP-completeness in characteristics two. *ACM Transactions on Computation Theory*, 9(1), 2016.

[13] J.R.B. Cockett, P.J.W. Hofstra, and P. Hrubeš. Total maps of turing categories. *Electr. Notes Theor. Comput. Sci.*, 308:129–146, 2014.

[14] P. Hrubeš and A. Rao. Circuits with medium fan-in. *IEEE Conference in Computational Complexity*, 2015.

[15] P. Hrubeš. On the real τ-conjecture and the distribution of complex roots. *Theory of Computing*, 9(10):403–411, 2013.

[16] P. Hrubeš, A. Wigderson, and A. Yehudayoff. An asymptotic bound on the composition number of integer sums of squares formulas. *Canadian Mathematical Bulletin*, 56:70–79, 2013.

[17] P. Hrubeš. On the nonnegative rank of distance matrices. *Information Processing Letters*, 112(11):457–461, 2012.

[18] P. Hrubeš and A. Yehudayoff. Formulas are exponentially stronger than monotone circuits in non-commutative setting. In *Conference on Computational Complexity*, 2013.

[19] R. Cockett, J. Díaz-Boïls, J. Gallagher, and P. Hrubeš. Timed sets, functional complexity, and computability. *Electr. Notes Theor. Comput. Sci.*, 286:117–137, 2012.

[20] P. Hrubeš and I. Tzameret. Short proofs for the determinant identities. In *STOC' 12 Proceedings of the 44th symposium on Theory of Computing*, pages 193–212, 2012.

[21] P. Hrubeš, A. Wigderson, and A. Yehudayoff. Non-commutative circuits and the sum of squares problem. *J. Amer. Math. Soc.*, 24:871–898, 2011.

[22] P. Hrubeš. How much commutativity is needed to prove polynomial identities? *Electronic Colloquium in Computational Complexity*, 2011.

[23] Pavel Hrubeš and Amir Yehudayoff. Homogeneous formulas and symmetric polynomials. *Computational Complexity*, 20(3):559–578, 2011.

[24] P. Hrubeš and A. Yehudayoff. Arithmetic complexity in ring extensions. *Theory of Computing*, 7:119–129, 2011.

[25] P. Hrubeš, A. Wigderson, and A. Yehudayoff. Non-commutative circuits and the sum of squares problem. In *STOC' 10 Proceedings of the 42nd symposium on Theory of Computing*, pages 667–676, 2010.

[26] P. Hrubeš, S. Jukna, A. Kulikov, and P. Pudlák. On convex complexity measures. *Theoretical Computer Science*, 411(16):1842–1854, 2010.

[27] P. Hrubeš, A. Wigderson, and A. Yehudayoff. Relationless completeness and separations. In *IEEE Conference on Computational Complexity*, pages 280–290, 2010.

[28] P. Hrubeš. On lengths of proofs in non-classical logics. *Annals of Pure and Applied Logic*, 157(194-205), 2009.

[29] P. Hrubeš and I. Tzameret. Proof complexity of polynomial identities. *CCC*, pages 41–51, 2009.

[30] P. Hrubeš. Kreisel's conjecture with minimality principle. *Journal of Symbolic logic*, 74(3):976–988, 2009.

[31] P. Hrubeš and A. Yehudayoff. Monotone separations for constant degree polynomials. *Information Processing Letters, 110(1): 1-3*, 2009.

[32] P. Hrubeš. Lower bounds for modal logics. *Journal of Symbolic logic*, 72(3):941–958, 2007.

[33] P. Hrubeš. A lower bound for intuitionistic logic. *Ann. Pure Appl. Logic*, 146:72–90, 2007.

[34] P. Hrubeš. Theories very close to PA where Kreisel's conjecture is false. *Journal of Symbolic logic*, 72:123–137, 2007.