Effective interpolation

Jan Krajíček
Mathematical Institute, Oxford University
and
Mathematical Institute, Academy of Sciences, Prague

A syllabus and references for a three-lecture course to be given at the **Tohoku University, Sendai**, October 2-4, 1997.

Effective interpolation is a method aimed primarily at proving lower bounds for propositional proof systems. The term "effective interpolation" (for a proof system P) means that it is possible to obtain some information about the computational efficiency of an interpolant of an implication from a proof (in P) of the implication.

We present a communication complexity approach to the effective interpolation and prove several lower bounds for proof systems, and an independence result for bounded arithmetic. We shall also discuss relevant complexity-theoretic topics (cryptography, circuit lower bounds).

The syllabus is divided into (one background section plus) three sections corresponding roughly to the three lectures. Its aim is to help newcomers to orient themselves in the literature. It lists topics that will be covered as well as those that will not be covered but belong to the background. Every item ends with a list of related references and a relevant place in [53]. The monograph [53] offers a comprehensive introduction into the complexity of propositional logic and into the closely related theory of bounded arithmetics. However, effective interpolation is not covered in [53] and the course is based largely on [54]. [55, 56, 77, 100] are survey articles.

Background references

- DeMorgan language, tautologies and satisfiable formulas, the length (i.e., the size) of a formula.

  References: [37], [53, Sec.4.1].

- NP- and coNP-completeness.

  References: [9, 10, 33, 43], [53, Sec.3.1,4.1].

- A Frege system F, F as a non-deterministic acceptor for TAUT.

  References: [37], [53, Sec.4.4].

- The definition of a general propositional proof system, the length-of-proofs function, the main problem.

  References: [37], [53, Sec.4.1].

- Polynomial simulation, speed-up.

  References: [37], [53, Sec.4.1].

- Formats of proofs.

  References: [51], [53, Sec.4.3,4.4].

- Frege systems in other languages, Spira's theorem, Reckhow's theorem.

  References: [37, 88, 94], [53, Sec.4.4].

- Extended Frege systems EF, Frege systems with the substitution rule SF, and their relations. The number of proof-steps versus the length.

  References: [37, 41, 49, 50, 62, 97], [53, Sec.4.5].

- Sequent calculus LK, its relation to F.

  References: [95], [53, Sec.4.3].

- Cut-free LK, resolution R, their relation.

  References: [16, 40, 92, 99], [53, Sec.4.2,4.3].

- Quantified propositional logic G, its relations to F and to predicate calculus.

  References: [63], [53, Sec.4.6].

- PHP_n tautologies and upper bounds for them.

  References: [22, 27], [53, Sec.4.2,11.2,12.5,13.1]

- PHP_n in R.

  References: [28, 29, 45, 96, 98], [53, Sec.4.2].

- Constant-depth Frege systems and PHP_n.

  References: [1, 12, 51, 66, 75], [53, Chpt.12].

- Counting principles $Count_q^N$, their relation to PHP_n and their mutual relations.

  References: [2, 3, 11, 13, 14, 26, 89, 90] [53, Sec.12.5].

- Bounds for F and EF. Connections to bounded arithmetic.

  References: [1, 7, 8, 17, 21, 22, 23, 32, 34, 35, 41, 52, 54, 57, 62, 63, 64, 67, 72, 73], [53, Chpts.9, 13 and 14].

- $Count_q^N$ in constant-depth F with MOD_q.

  References: [53, Sec.12.6].

- Polynomials as formulas, algebraic proof systems.

  References: [26], [53, Sec.12.6].

- Hilbert's Nullstellensatz NS as a proof system.

  References: [11, 26].

- Polynomial calculus PC (a.k.a. Gröbner calculus) and its relation to NS.

  References: [26, 30]

- Equational logic and its relation to NS, PC, and F.

  References: [26].

- Lower bounds and interpolation for NS and PC.

  References: [11, 24, 26, 30, 61, 80, 87].

- An approximation of formulas by low-degree polynomials. Extended Nullstellensatz, its relation to constant-depth Frege systems with modular counting connectives.

  References: [84, 93], [53, Sec.3.1].

- **Open problem**: Lower bounds for constant-depth F with the MOD_q connective.

  References: [26, 60, 68], [53, Sec.12.6].

1 Effective interpolation

- Craig's theorem, a construction of an interpolant from a cut-free proof, Lyndon's theorem.

  References: [39], [53, Sec.4.3].

- From effective interpolation to lower bounds for proof systems.

  References: [51, 54].

- Effective interpolation for R.

  References: [54].

- Cutting planes CP: the definition, relation to F and effective interpolation. Improved interpolation for CP with small coefficients.

  References: [18, 25, 31, 36, 38, 42, 44, 46, 47, 54, 58, 78], [53, Sec.13.1].

- p-simulation of R by CP.

  References: [38], [53, Sec.13.1].

- Generalizations of CP: LK(CP), Lovász-Schrijver system.

  References: [58, 79].

- Bounded arithmetic theory $S_2^2(\alpha)$ and interpolation.

  References: [21, 54, 86].

2 Communication complexity approach

- Communication complexity, general protocols.

  References: [48, 54, 86].

- Semantic derivations and universal interpolation.

  References: [54].

- Applications to R, CP, LK(CP) and other proof systems.

  References: [54, 58, 59].

3 Disjoint NP-pairs, one-way functions

- Separability of disjoint NP-pairs. Relation of $NP \cap coNP$ to $P/poly$.

  References: [54, 69, 70, 85], [53, Sec.3.1].

- Some monotone Boolean complexity, graphs with k-cliques versus $(k-1)$-colorable graphs.

  References: [5, 6, 20, 74, 83], [53, Sec.3.1].

- Beth's theorem, one-way functions.

  References: [15, 71], [53, Sec.4.3].

- RSA-encryption scheme, limitations of effective interpolation for EF and F.

  References: [4, 19, 65, 71, 91].

- **Open problem**: Proofs of primality.

  References: [65, 76].

Below is an extensive (but not exhaustive) bibliography relevant to the topics treated in the course.

References

[1] Ajtai, M. (1988) The complexity of the pigeonhole principle, in: *Proc. IEEE 29^{th} Annual Symp. on Foundation of Computer Science*, pp. 346-355.

[2] —— (1990) Parity and the pigeonhole principle, in: *Feasible Mathematics*, Eds. S.R.Buss and P.J.Scott, pp.1-24. Birkhauser.

[3] —— (1994) The independence of the modulo p counting principles, in: *Proceedings of the 26th Annual ACM Symposium on Theory of Computing*, pp.402-411. ACM Press.

[4] Alexi, W. B., Chor, B., Goldreich, O., Schnorr, C. P. (1988) RSA and Rabin functions: Certain parts are as hard as the whole, *SIAM J. Comp.*, **17**, pp.194-209.

[5] Alon, N., and Boppana, R. (1987) The monotone circuit complexity of boolean functions, *Combinatorica*, **7(1)** , pp.1-22.

[6] Andreev, A. E. (1985) On a method for obtaining lower bounds for the complexity of individual mnotone functions (in Russian), *Doklady AN SSSR*, **282(5)** , pp.1033-1037.

[7] Arai, T. (1991) Frege system, *ALOGTIME* and bounded arithmetic, manuscript.

[8] Avigad, J. (1996) Plausibly hard combinatorial tautologies, in: Proceedings of the DIMACS workshop on Feasible Arithmetic and Length of Proofs, Eds. P. Beame and S. Buss, submitted.

[9] Balcazár, J. L., Díaz, J., and Gabarró, J. (1988) *Structural complexity I.* Berlin, Springer.

[10] —— (1990) *Structural complexity II.* Berlin, Springer.

[11] Beame, P., Impagliazzo, R., Krajíček, J., Pitassi, T., and Pudlák, P. (1996) Lower bounds on Hilbert's Nullstellensatz and propositional proofs, *Proceedings of the London Mathematical Society*, **(3) 73**, pp.1-26.

[12] Beame, P., Impagliazzo, R., Krajíček, J., Pitassi, T., Pudlák, P., and Woods, A. (1992) Exponential lower bounds for the pigeonhole principle, in: *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, pp.200-221. ACM Press.

[13] Beame, B and Pitassi, T. (1996) An exponential separation between the parity principle and the pigeonhole principle, *Annals of Pure and Applied Logic*, **80**, pp.195-228.

[14] Beame, B and Riis, S. (1996) More on the relative strength of counting principles, preprint.

[15] Beth E. W. (1959) *The foundations of mathematics.* North - Holland, Amsterdam.

[16] Blake, A. (1937) Canonical expressions in boolean algebra, PhD. Thesis, University of Chicago.

[17] Bonet, M., Buss, S. and Pitassi, T. (1995) Are there hard examples for Frege systems?, in: *Feasible Mathematics II*, eds. P. Clote and J. Remmel, pp.30-56. Birkhauser.

[18] Bonet, M. L., Pitassi, T., and Raz, R. (1994) Lower bounds for cutting planes proofs with small coefficients, to appear.

[19] Bonet, M. L., Pitassi, T., and Raz, R. (1997) No feasible interpolation for TC^0-Frege proofs, preprint.

[20] Boppana, R., and Sipser, M. (1990) Complexity of finite functions. in: *Handbook of Theoretical Computer Science*, ed. J. van Leeuwen, pp.758-804.

[21] Buss, S. R. (1986) *Bounded Arithmetic.* Naples, Bibliopolis.

[22] —— (1987) The propositional pigeonhole principle has polynomial size Frege proofs, *J. Symbolic Logic*, **52**, pp.916-927.

[23] —— (1991) Propositional consistency proofs, *Annals of Pure and Applied Logic*, **52**, pp.3-29.

[24] Buss, S. (1996) Lower bounds on Nullstellensatz proofs via designs, preprint.

[25] Buss, S., and Clote, P. (1986) Cutting planes, connectivity, and threshold logic, Archiv for math.Logic, 35, pp.33-62.

[26] Buss, S., Impagliazzo, R., Krajíček, J., Pudlák, P., Razborov, A. A., and Sgall, J. (1996) Proof complexity in algebraic systems and constant depth Frege systems with modular counting, *Computational Complexity*, to appear.

[27] Buss, S., and Pitassi, T.: Resolution and the weak pigeonhole principle, preprint, (1996).

[28] Buss, S. R., and Turán, G. (1988) Resolution proofs of generalized pigeonhole principles, *Theoretical Computer Science* **62**, pp.311-317.

[29] Chvátal, V., and Szemerédi, E. (1988) Many hard examples for resolution, *J. of ACM*, **35(4)** , pp.759-768.

[30] Clegg, M., Edmonds, J., and Impagliazzo, R. (1996) Using the Groebner basis algorithm to find proofs of unsatisfiability, in: *Proc. ACM Symp. on Theory of Computing*, ACM Press, pp.174-183.

[31] Clote, P. (1995) Cutting planes and Frege proofs, Information and Computation, 121(1), pp.103-122.

[32] Clote, P., and Krajíček, J. (1993) Open problems, in: *Arithmetic, Proof Theory and Computational Complexity*, eds.P. Clote and J. Krajíček, pp.1-19, Oxford Press.

[33] Cook, S A. (1971) The complexity of theorem proving procedures, in: *Proc. 3^{rd} Annual ACM Symp. on Theory of Computing*, pp. 151-158. ACM Press.

[34] —— (1975) Feasibly constructive proofs and the propositional calculus, in: *Proc. 7^{th} Annual ACM Symp. on Theory of Computing*, pp. 83-97. ACM Press.

[35] —— (1997) Relating provable collapse of P to NC^1 and the power of logical theories, in: Proceedings of the DIMACS workshop on Feasible Arithmetic and Length of Proofs, Eds. P. Beame and S. Buss, to appear.

[36] Cook, S.A. and Haken, A. (1995) An exponential lower bound for the size of monotone real circuits, preprint.

[37] Cook, S. A., and Reckhow, A. R. (1979) The relative efficiency of propositional proof systems, *J. Symbolic Logic*, **44(1)**, pp.36-50.

[38] Cook, W., Coullard, C. R., and Turán, G. (1987) On the complexity of cutting plane proofs, *Discrete Applied Mathematics*, **18**, pp.25-38.

[39] Craig, W. (1957) Three uses of the Herbrand-Gentzen theorem in relating model theory and proof theory, *Journal of Symbolic Logic*, **22(3)**, pp.269-285.

[40] Davis, M., and Putnam, H. (1960) A computing procedure for quantification theory, *Journal of the ACM*, **7(3)**, pp.210-215.

[41] Dowd, M. (1979) Propositional representations of arithmetic proofs, PhD Thesis, University of Toronto.

[42] Fu, X. (1996) Modular coloring formulas are hard for cutting planes proofs, in: Proc. ACM Symp. on Theory of Computing, ACM Press, pp.595-602.

[43] Garey, M.R., and Johnson, D. S. (1979) *Computers and intractability.* New York, W.H.Freeman and Co..

[44] Goerdt, A. (1990) Cutting plane versus Frege proof systems, in: *Computer Science Logic' 90*, LNCS 533, pp.174-194. Springer-Verlag.

[45] Haken,A. (1985) The intractability of resolution, *Theoretical Computer Science*, **39**, pp.297-308.

[46] Impagliazzo, R., Pitassi, T., and Urquhart, A. (1994) Upper and lower bounds for tree-like cutting planes proofs, in: Proc. of the 9th Annual IEEE Symposium on *Logic in Computer Science.* Piscataway, NJ, IEEE Computer Science Press. pp.220-228.

[47] Johannsen, J. (1997) Simple lower bounds for monotone real circuit depth and formula size and tree-like cutting planes proofs, preprint.

[48] Karchmer, M., and Wigderson, A. (1988) Monotone circuits for connectivity require super - logarithmic depth, in: *Proc.* 20^{th} *Annual ACM Symp. on Theory of Computing*, pp.539-550. ACM Press.

[49] Krajíček, J. (1989) On the number of steps in proofs, *Annals of Pure and Applied Logic*, **41**, pp.153-178.

[50] —— (1989) Speed-up for propositional Frege systems via generalizations of proofs, *Commentationes Mathematicae Universitas Carolinae*, **30(1)**, pp.137-140.

[51] —— (1994) Lower bounds to the size of constant-depth propositional proofs, *Journal of Symbolic Logic*, **59(1)**, pp.73-86.

[52] —— (1995) On Frege and Extended Frege proof systems, in: *Feasible Mathematics II*, eds. P. Clote and J. Remmel, Birkhauser, pp. 284-319.

[53] —— (1995) *Bounded arithmetic, propositional logic and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, Cambridge - New York - Melbourne.

[54] —— (1997) Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, *J. of Symbolic Logic*, **62(2)**, pp.457-486.

[55] —— (1995) "On methods for proving lower bounds in propositional logic", in: *Logic and Scientific Methods* Eds. M. L. Dalla Chiara et al., (Vol. 1 of Proc. of the Tenth International Congress of Logic, Methodology and Philosophy of Science, Florence (August 19-25, 1995)), Synthese Library, Vol.259, Kluwer Academic Publ., Dordrecht, (1997), pp.69-83.

[56] —— (1996) A fundamental problem of mathematical logic, *Annals of the Kurt Gödel Society*, Springer-Verlag, Collegium Logicum, Vol.2, pp.56-64.

[57] —— (1996) Extensions of models of PV, in: *Proc. Logic Colloquium 1995 (Haifa)*, Eds. V. Harnik and J. Makowsky, Springer-Verlag, to appear.

[58] —— (1996) Discretely ordered modules as a first-order extension of the cutting planes proof system, *J. Symbolic Logic*, to appear.

[59] —— (1996) Interpolation by a game, *Mathematical Logic Quaterly*, to appear.

[60] —— (1997) Lower bounds for a proof system with an exponential speed-up over constant-depth Frege systems and over polynomial calculus, in: Eds. I.Prívara, P. R˚užička, 22nd Inter. Symp. *Mathematical Foundations of Computer Science* (Bratislava, August '97), Lecture Notes in Computer Science 1295, Springer-Verlag, pp.85-90.

[61] —— (1997) On the degree of ideal membership proofs from uniform families of polynomials over a finite field, preprint.

[62] Krajíček, J., and Pudlák, P. (1989) Propositional proof systems, the consistency of first order theories and the complexity of computations, *J. Symbolic Logic*, **54(3)**, pp.1063-1079

[63] —— (1990) Quantified propositional calculi and fragments of bounded arithmetic, *Zeitschrift f. Mathematikal Logik u. Grundlagen d. Mathematik*, **36**, pp.29-46.

[64] —— (1990) Propositional provability in models of weak arithmetic, in: *Computer Science Logic (Kaiserlautern, Oct. '89)*, eds.E.Boerger, H.Kleine-Bunning and M.M. Richter, LNCS 440, pp.193-210. Springer-Verlag.

[65] —— (1995) Some consequences of cryptographical conjectures for S^1_2 and EF, in: *Logic and Computational Complexity* (Proc. of the meeting held in Indianapolis, October 1994), Ed. D. Leivant, Springer-Verlag, Lecture Notes in Computer Science, Vol. **960**, pp.210-220.

[66] Krajíček, J.,Pudlák, P. and Woods, A. (1995) Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle, *Random Structures and Algorithms*, **7(1)**, pp.15-39.

[67] Krajíček, J., and Takeuti, G. (1990) On bounded $\sum^1_1$-polynomial induction, in: *Feasible Mathematics*, eds. S.R. Buss and P.J. Scott, pp.259-280. Birkhauser.

[68] Maciel, A., and Pitassi, T. (1997) On $ACC^0[p^k]$ Frege proofs, 29th STOC, pp. 720-729.

[69] Mundici, D. (1983) A lower bound for the complexity of Craig's interpolants in sentential logic, *Archiv fur Math. Logik*, **23** , pp.27-36.

[70] —— (1984) NP and Craig's interpolation theorem, Proc. *Logic Colloquium 1982*, North-Holland, pp. 345-358.

[71] Papadimitriou, A. (1994) *Computational complexity*, Addison-Wesley.

[72] Parikh, R. (1971) Existence and feasibility in arithmetic, *Journal of Symbolic Logic*, **36**, pp.494-508.

[73] Paris, J., and Wilkie, A. J. (1985) Counting problems in bounded arithmetic, in: *Methods in Mathematical Logic*, LNM 1130, pp.317-340.Springer.

[74] Paris, J. B., Wilkie, A. J., and Woods, A. R. (1988) Provability of the pigeonhole principle and the existence of infinitely many primes, *Journal of Symbolic Logic*, **53**, pp.1235–1244.

[75] Pitassi, T., Beame, P., and Impagliazzo, R. (1993) Exponential lower bounds for the pigeonhole principle, *Computational complexity*, **3**, pp.97-308.

[76] Pratt, V.R. (1975) Every prime has a succinct certificate, *SIAM J. Computing*, **4**, pp.214-220.

[77] Pudlák, P. (1996) The lengths of proofs, in: *Handbook of Proof Theory*, Ed. S. Buss, to appear.

[78] —— (1996) Lower bounds for resolution and cutting planes proofs and monotone computations, to appear.

[79] —— (1997) On the complexity of propositional calculus, preprint.

[80] Pudlák, P., and Sgall, J. (1996) Algebraic models of computation and interpolation for algebraic proof systems, preprint.

[81] Raz, R., and Wigderson, A. (1989) Probabilistic communication complexity of Boolean relation, in: *Proc. IEEE 30th Annual Symp. on Foundation of Computer Science*, pp.562-567.

[82] —— (1992) Monotone circuits for matching require linear depth, *J. of Assoc. for Computing Machinery*, **39(3)**, pp.736-744.

[83] Razborov, A. A. (1985) Lower bounds on the monotone complexity of some Boolean functions, *Soviet Mathem. Doklady*, **31**, pp.354-357.

[84] —— (1987) Lower bounds on the size of bounded depth networks over a complete basis with logical addition, *Matem. Zametki*, **41(4)**, pp.598-607.

[85] —— (1994) On provably disjoint NP-pairs, Basic Research in Computer Science Center, Aarhus, RS-94-36, preprint.

[86] —— (1995) Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic, *Izvestyia of the R.A.N.*, **59(1)**, pp.201-244.

[87] —— (1996) Lower bounds for the polynomial calculus, *Computational Complexity*, to appear.

[88] Reckhow, R. A. (1976) On the lengths of proofs in the propositional calculus, PhD.Thesis, Dept. of CS, University of Toronto. Technical Report No.87.

[89] Riis, S. (1993) Independence in bounded arithmetic, PhD. Thesis, Oxford University.

[90] —— (1994) $Count(q)$ does not imply $Count(p)$, to appear.

[91] Rivest, M., Shamir, A., and Adleman, L. (1978) A method of obtaining digital signatures and public-key cryptosystems, *ACM Communications*, **21**, pp. 120-126.

[92] Robinson, J., A. (1965) A machine-oriented logic based on the resolution principle, *Journal of the ACM*, **12(1)**, pp.23-41.

[93] Smolensky, R (1987) Algebraic methods in the theory of lower bounds for Boolean circuit complexity, in: *Proc. 19th Ann. ACM Symp. on Th. of Computing*, pp. 77-82.

[94] Spira, P. M. (1971) On time-hardware complexity of tradeoffs for Boolean functions, in: *Proc. 4^{th} Hawaii Symp. System Sciences*, pp. 525-527.North Hollywood, Western Periodicals Co..

[95] Takeuti, G. (1975) *Proof theory*, North-Holland.

[96] Tseitin, G. C. (1968) On the complexity of derivations in propositional calculus, in: *Studies in mathematics and mathematical logic, Part II*, ed. A.O.Slisenko, pp.115-125.

[97] Tseitin, G. C., and Choubarian, A. A. (1975) On some bounds to the lengths of logical proofs in classical propositional calculus" (Russian), *Trudy Vyčisl Centra AN Arm SSR i Erevanskovo Univ.*, **8**, pp.57-64.

[98] Urquhart, A. (1987) Hard examples for resolution, *Journal of the ACM*, **34**, pp.209-219.

[99] —— (1992) The relative complexity of resolution and cut-free Gentzen systems, *Annals of Mathematics and Artificial Inteligence*, **6**, pp.1157-168.

[100] —— (1995) The complexity of propositional proofs, *Bull. of Symbolic Logic*, **1(4)**, pp.425-467.