Classical propositional logic and its complexity

Jan Krajíček
Mathematical Institute and Institute of Computer Science
Academy of Sciences, Prague

A syllabus and references for an advanced logic course (five 90-minutes lectures) given at the **Eight European Summer School in Logic, Language and Information** held in Prague, August 12-23, 1996

The syllabus is divided into five sections corresponding to the five lectures. Every item ends with a list of related references and a relevant place in [41]. The monograph [41] offers a comprehensive introduction into the field and into the closely related theory of bounded arithmetics. The second half of the course contains some of the recent developments not covered in [41]. [43, 44, 61, 78] are available survey articles.

1 Basic notions and facts

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

  References: [29], [41, Sec.4.1].

- NP- and coNP-completeness.

  References: [8, 9, 26, 34], [41, Sec.3.1,4.1].

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

  References: [29], [41, Sec.4.4].

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

  References: [29], [41, Sec.4.1].

- Polynomial simulation, speed-up.

  References: [29], [41, Sec.4.1].

- Formats of proofs.

  References: [39], [41, Sec.4.3,4.4].

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

  References: [29, 66, 72], [41, 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: [29, 33, 37, 38, 47, 75], [41, Sec.4.5].

- Sequent calculus LK, its relation to F.

  References: [73], [41, Sec.4.3].

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

  References: [14, 32, 70, 77], [41, Sec.4.2,4.3].

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

  References: [48], [41, Sec.4.6].

- **HW:** PHP_n tautologies.

  References: [36], [41, Sec.4.2,11.2,12.5,13.1]

2 Known bounds

- PHP_n in R.

  References: [22, 23, 36, 74, 76], [41, Sec.4.2].

- Constant-depth Frege systems and PHP_n.

  References: [1, 11, 39, 51, 59], [41, Chpt.12].

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

  References: [2, 3, 10, 12, 21, 67, 68] [41, Sec.12.5].

- Languages with the equivalence connective and with modular counting connectives. An open problem.

  References: [21], [41, Sec.12.6].

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

  References: [1, 7, 15, 18, 19, 20, 25, 27, 33, 40, 42, 45, 47, 48, 49, 52, 56, 57], [41, Chpts.9, 13 and 14].

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

  References: [41, Sec.12.6].

3 Effective interpolation

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

  References: [31], [41, Sec.4.3].

- From effective interpolation to lower bounds for proof systems.

  References: [39, 42].

- Effective interpolation for R.

  References: [42].

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

  References: [16, 28, 30, 35, 42, 46, 62], [41, Sec.13.1].

- **HW:** p-simulation of R by CP.

  References: [30], [41, Sec.13.1].

4 Disjoint NP-pairs, one-way functions

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

  References: [42, 53, 54, 65], [41, Sec.3.1].

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

  References: [5, 6, 17, 58, 63], [41, Sec.3.1].

- Beth's theorem, one-way functions.

  References: [13, 55], [41, Sec.4.3].

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

  References: [4, 50, 55, 69].

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

  References: [50, 60].

5 Algebraic proof systems

- Polynomials as formulas.

  References: [21], [41, Sec.12.6].

- Hilbert's Nullstellensatz NS as a proof system.

  References: [10, 21].

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

  References: [21, 24]

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

  References: [21].

- Lower bounds for NS, interpolation for PC.

  References: [10, 21, 24]

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

  References: [64, 71], [41, Sec.3.1].

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

Below is an extensive (but not exhaustive) bibliography relevant to the topics treated in the course. Postscript files of my unpublished papers can be requested at `krajicek@mbox.cesnet.cz`.

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

[9] —— (1990) *Structural complexity II.* Berlin, Springer.

[10] 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.

[11] 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.

[12] 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.

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

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

[15] 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.

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

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

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

[19] —— (1987) The propositional pigeonhole principle has polynomial size Frege proofs, *J. Symbolic Logic*, **52**, pp.916-927.

[20] —— (1991) Propositional consistency proofs, *Annals of Pure and Applied Logic*, **52**, pp.3-29.

[21] 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*, submitted.

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

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

[24] 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.

[25] 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.

[26] 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.

[27] —— (1975) Feasibly constructive proofs and the propositional calculus, in: *Proc. 7^{th} Annual ACM Symp. on Theory of Computing*, pp. 83-97. ACM Press.

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

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

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

[31] 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.

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

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

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

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

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

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

[38] —— (1989) Speed-up for propositional Frege systems via generalizations of proofs, *Commentationes Mathematicae Universitas Carolinae*, **30(1)**, pp.137-140.

[39] —— (1994) Lower bounds to the size of constant-depth propositional proofs, *Journal of Symbolic Logic*, **59(1)**, pp.73-86.

[40] —— (1995) On Frege and Extended Frege proof systems, in: *Feasible Mathematics II*, eds. P. Clote and J. Remmel, Birkhauser, pp. 284-319.

[41] —— (1995) *Bounded arithmetic, propositional logic and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, Cambridge - New York - Melbourne.

[42] —— (1995) Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, *J. of Symbolic Logic*, to appear.

[43] —— (1995) On methods for proving lower bounds in propositional logic, Proceedings of the Tenth International Congress *Logic, Methodology and Philosophy of Science*, International Union of History and Philosophy of Science, Florence (August 19-25, 1995), Eds. M. L. Dalla Chiara, K. Doets, D. Mundici, J. van Benthem, to appear.

[44] —— (1996) A fundamental problem of mathematical logic, *Annals of the Kurt Gödel Society*, Springer-Verlag, Collegium Logicum, Vol.2, pp.56-64.

[45] —— (1996) Extensions of models of PV, in: *Proc. Logic Colloquium 1995 (Haifa)*, Eds. V. Harnik and J. Makowsky, Springer-Verlag, submitted.

[46] —— (1996) Discretely ordered modules as a first-order extension of the cutting planes proof system, submitted.

[47] 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

[48] —— (1990) Quantified propositional calculi and fragments of bounded arithmetic, *Zeitschrift f. Mathematikal Logik u. Grundlagen d. Mathematik*, **36**, pp.29-46.

[49] —— (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.

[50] —— (1995) Some consequences of cryptographical conjectures for S_2^1 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.

[51] 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.

[52] 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.

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

[54] —— (1984) NP and Craig's interpolation theorem, Proc. *Logic Colloquium 1982*, North-Holland, pp. 345-358.

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

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

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

[58] 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.

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

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

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

[62] —— (1996) Lower bounds for resolution and cutting planes proofs and monotone computations, to appear.

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

[64] —— (1987) Lower bounds on the size of bounded depth networks over a complete basis with logical addition, *Matem. Zametki*, **41(4)**, pp.598-607.

[65] —— (1994) On provably disjoint NP-pairs, Basic Research in Computer Science Center, Aarhus, RS-94-36, preprint.

[66] 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.

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

[68] —— (1994) $Count(q)$ does not imply $Count(p)$, to appear.

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

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

[71] 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.

[72] 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..

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

[74] 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.

[75] 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.

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

[77] —— (1992) The relative complexity of resolution and cut-free Gentzen systems, *Annals of Mathematics and Artificial Inteligence*, **6**, pp.1157-168.

[78] —— (1995) The complexity of propositional proofs, *Bull. of Symbolic Logic*, **1(4)**, pp.425-467.