Lengths of propositional proofs

Jan Krajíček

A syllabus and references for an advanced logic course,
Michaelmas term 1997, Oxford.

(21.XI.1997 version)

The syllabus is numbered according to the structure of the lectures. Every item ends with a list of related references and a relevant place in [35] (if available). [35] offers a comprehensive introduction into the field and into the closely related theory of bounded arithmetics. However, neither effective interpolation nor algebraic proof systems are covered much in [35]. Introductions to these areas are [36] and [18] respectively. [37, 38, 57, 72] are available survey articles.

1 Motivations, complexity theory, bounded arithmetic. Basic definitions and problems.

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

References: [23], [35, Sec.4.1].

(1.2) NP- and coNP-completeness, Cook's theorem. The P vs. NP and the NP vs. coNP problems. Polynomial hierarchy.

References: [9, 10, 20, 29], [35, Sec.3.1,4.1].

(1.3) Proof systems as non-deterministic acceptors for TAUT.

References: [23], [35, Sec.4.1].

(1.4) The definition of a general propositional proof system.

References: [23], [35, Sec.4.1].

(1.5) "Usual" calculi as general proof systems.

References: [23], [35, Sec.4.1].

(1.6) Cook-Reckhow's theorem about the equivalence of NP = coNP and the existence of polynomially bounded proof system.

References: [23], [35, Sec.4.1].

(1.7) Polynomial simulation.

References: [23], [35, Sec.4.1].

(1.8) Frege systems F.

References: [23], [35, Sec.4.4].

(1.9) Open problem: lower bounds for F. Irrelevance of formats of proofs and of a particular complete language (Spira's theorem, Reckhow's theorem).

References: [33], [23, 64, 70], [35, Sec.4.3,4.4].

(1.10) Remark: a lack of "completeness results" and of "counting arguments" in proof complexity. Problem: find a concrete sequence of tautologies hard for F under some plausible general (complexity-theoretic) conjecture.

(1.11) The extension rule and the substitution rule.

References: [23], [35, Sec.4.5].

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

References: [23, 27, 32, 44, 71], [35, Sec.4.5].

(1.13) Bounded arithmetic (2nd order), language, hierarchy of bounded formulas. Definability and the polynomial-time hierarchy PH.

References: [16], [35, Chpt.5].

(1.14) Theories: BASIC, V_1^i, V_1, $I\Delta_0(\alpha)$. The finite axiomatizability problem.

References: [52], [16], [35, Chpt.5].

(1.15) Known facts about the finite axiomatizability problem.

References: [35, Chpt.10], [48], [49, 55].

(1.16) PHP bounded principle and PHP_n tautologies.

References: [23], [35, Sec.4.2,11.2,12.5,13.1]

(1.17) A translation of arithmetic proofs into propositional proofs. $I\Delta_0(\alpha)$ and constant-depth Frege systems, V_1^1 and EF.

References: [16, 21, 27, 34, 39, 44, 45, 46, 50, 53], [35, Chpt.9].

(1.18) Examples of proof systems: F, EF, SF, F_d. Definition of resolution R.

References: [12, 26, 68], [35, Chpt.4].

2 Effective interpolation

(2.1) Craig's theorem, combinatorial view (separation of disjoint pairs of sets).

References: [25], [35, Sec.4.3].

(2.2) Monotone version: Lyndon's theorem, combinatorial version.

References: [25].

(2.3) Definition of "effective interpolation", a construction of an interpolant from a cut-free proof.

References: [33, 36], [25].

(2.4) From effective interpolation to lower bounds for proof systems.

References: [33, 36].

(2.5) Example: any circuit of size m can be the unique interpolant of an implication with an $m^{O(1)}$ size R-proof.

References: [33].

(2.6) Communication complexity, Karchmer-Wigderson game on disjoint pair U, V.

References: [31].

(2.7) Example: from formulas separating U from V to protocols for K.-W. game.

References: [31].

(2.8) Karchmer-Wigderson theorem.

References: [31], [36, Thm. 2.1].

(2.9) Spira's theorem revisited.

References: [70].

(2.10) Histories of plays and rectangles of inputs.

(2.11) Multifunctions $R \subseteq U \times V \times I$ and their communication complexity $CC(R)$.

References: [31].

(2.12) Example: circuit separating U from V as a protocol for the K.-W. game.

(2.13) The notion of a general protocol for computing a multifunction. Example: the need of the consistency condition.

References: [36, Def.2.2].

(2.14) Razborov's theorem: a protocol for the K.-W. game on U and V of size S and CC t yields a separating circuit of size $S2^{O(t)}$.

References: [36, Thm.2.3], [62].

(2.15) Idea of getting a protocol from a proof.

References: [36].

(2.16) Semantic derivations.

References: [36, Def.4.1].

(2.17) Set-up; semantic refutations of subsets of $\{0,1\}^N$.

References: [36, Sec.5].

(2.18) Communication complexity of a set.

References: [36, Def.4.3].

(2.19) Example: communication complexity of sets defined by clauses.

References: [36, Thm.6.1: 1st proof].

(2.20) Effective interpolation for semantic derivations. (2.19) revisited.

References: [36, Thm.5.1].

(2.21) Cutting planes: definition and effective interpolation.

References: [24],[13],[36, Thm.6.4].

(2.22) System R(CP), cutting planes with deduction: definition and effective interpolation.

References: [40].

(2.23) LK(CP), discretely ordered modules as a first order extension of CP. Non-monotone effective interpolation.

References: [40].

(2.24) Remark: interpolation for CP independent of the coefficient size.

References: [58], [22].

(2.25) Disjoint pairs of NP-sets.

(2.26) Monotone case: sets $Clique_{n,\omega}$ and $Color_{n,\xi}$, their propositional definitions.

References: [36, Def.7.1].

(2.27) Lower bounds for size of monotone circuits separating the sets from (2.26). Also real monotone case.

References: [59, 7], [58, 22].

(2.28) Separation of the sets from (2.26) follows from PHP, or even from WPHP (if $\omega > 2\xi$). PHP and WPHP have polynomial size proofs in F and quasi-polynomial size proofs in constant-depth F respectively. Hence none of these systems admit monotone effective interpolation.

References: [36, Thm.9.3],[17], [54], [62].

(2.29) Non-monotone case, examples.

References: [36, Sec.9], [61].

(2.30) One-way functions, conjectured examples (factoring, discrete log).

References: [36, Def.9.1].

(2.31) Inverting one-way functions, Beth's theorem.

References: [36, Thm.9.2].

(2.32) RSA encoding scheme, encoding one bit, Alexi et.al. theorem.

References: [67, 6].

(2.33) EF does not admit effective interpolation unless RSA is not secure. Similar for F with Diffie-Hellman in place of RSA.

References: [47], [14].

(2.34) Open problem: primality proofs (not given in the lectures).

References: [47], [42].

3 Constant-depth Frege systems, switching lemmas

(3.1) Definition of the depth, and classes of boolean functions: Σ_s^1, Π_s^1 and Δ_s^1. Example: parity $\oplus_n$ is not in $\Sigma_{n-1}^1 \cup \Pi_{n-1}^1$. Remark: formula- and circuit-size, for fixed depth, are polynomially related.

References: [35, Sec.3.1].

(3.2) Decision trees. Lemma: Any $f \in \Delta_s^1$ has a decision tree of depth $\leq s^2$.

References: [35, L.3.1.3].

(3.3) Collapsing lemma: any f computable by a depth d size S formula, $0 < \delta < 3^{-d}$ and $S < 2^{n^\delta}$, can be restricted by a ρ of size $\leq n - n^{3^{-d}}$ such that f^ρ is computable by a decision tree of depth n^δ. Corollary: parity is not computable by small constant-depth formulas.

References: [1, 28, 73, 30, 62], [35, Secs.3.1 and 15.2], [15].

(3.4) $\mathcal{M}$: partial truth assignments, $S \subseteq \mathcal{M}$ refines $H \subseteq \mathcal{M}$.

References: [35, Def.15.2.1].

(3.5) Reduction of (3.3) to (3.6).

References: [35, Secs.3.1 and 15.2], [15].

(3.6) Switching lemma: Assume that for $\ell \leq S$: $H_\ell \subseteq \mathcal{M}$ and $(\max_{h \in H_\ell} |h|) \leq t$, and $t \leq s$ is small. Let $\epsilon < 1/2$ and

$$S < (\frac{n^{1-\epsilon} - 1}{8t})^s$$

Then there is $\rho \in \mathcal{M}$, $|\rho| \leq n - n^\epsilon$ such that for all $\ell \leq S$ there is a decision tree T_ℓ of depth less than s refining H_ℓ^ρ.

References: [35, L.15.2.2] (with decision trees in place of complete systems).

(3.7) Proof of (3.3) from (3.6).

(3.8) Proof of switching lemma (3.6).

References: [35, L.15.2.2].

(3.9) Recall the formula PHP_n and the set of clauses $\neg PHP_n$ (cf. **(1.16)**).

(3.10) Idea of lower bounds via k-evaluations.

(3.11) $\mathcal{M}^{PHP_n}$: partial 1-to-1 functions. Definitions of refinement, projection.

References: [35, 12.3] (here and in the rest of part 3. the presentation is after [49]).

(3.12) Definition of PHP_n-decision tree.

References: [55].

(3.13) Restrictions (of formulas, of functions) by $\rho \in \mathcal{M}^{PHP_n}$.

References: [35, 12.3].

(3.14) Definition of k-evaluations.

References: [35, 12.4].

(3.15) Lemma: If $|\rho| + k \leq n$ then restriction of a k-evaluation by ρ is again k-evaluation.

References: [35, L.12.4.7].

(3.16) Theorem on the existence of k-evaluations: If $0 < \delta < 7^{-d}$ and $S < 2^{n^\delta}$ then for any set Γ of depth d formulas, $|\Gamma| \leq S$ there exists ρ of size $\leq n - n^{7^{-d}}$ such that Γ^ρ admits $O(n^\delta)$-evaluation.

References: [35, Thm.12.4.3].

(3.17) Proof of (3.16) from the switching lemma (3.18).

(3.18) Switching lemma (and its proof): Assume that for $\ell \leq S$: $H_\ell \subseteq \mathcal{M}^{PHP_n}$ and $(\max_{h \in H_\ell} |h|) \leq t$, and $t \leq s$. Let $\omega \leq n$. Assume:

$$S < \frac{\omega^s}{(n+1-\omega)^{4s} t^{3s}}$$

Then there is $\rho \in \mathcal{M}^{PHP_n}$, $|\rho| = \omega$, such that for all $\ell \leq S$ there is a decision tree T_ℓ of depth less than $2s$ refining H_ℓ^ρ.

If $0 < \delta < \epsilon < \frac{1}{7}$, $\omega = n - n^\epsilon$, $t = s = n^\delta$, the hypothesis of the lemma is satisfied whenever $S < 2^{n^\delta}$.

References: [35, L.12.3.10].

(3.19) Use of (3.16) for lower bounds.

References: [35, 12.5].

(3.20) Changes needed for $\neg Count_p^n$ in place of $\neg PHP_n$.

References: [35, Secs.12.3,12.5, L.12.3.11].

(3.21) Towards independence of counting module p and q principles over constant depth Frege systems. Generic systems.

References: [35, Secs.12.5,12.6], [4], [11], [66].

(3.22) Reducing the non-existence of a generic system to degree lower bounds for Nullstellensatz.

References: [11], [35, 12.6].

4 Algebraic proof systems, Ajtai's theorem

(4.1) Nullstellensatz proof system NS.

References: [11, 18].

(4.2) System of linear equations related to NS.

References: [11], [43, Ex.2.1].

(4.3) Uniform linear systems, Ajtai's theorem.

References: [4, 5], [42].

(4.4) Lower bound for NS from (4.3).

(4.5) Polynomial calculus PC. Its relation to NS.

References:[18], [19].

(4.6) Linear system related to PC.

References: [42, 43].

(4.7) Lower bound for PC from (4.3).

References: [42]. [63] (not based on (4.3)).

bf (4.8) Open problem: constant-depth Frege systems in the DeMorgan Language together with the MOD_p connectives.

References: [35, Sec.12.6], [18]. Partial result: [41].

Below is an extensive (but not exhaustive) bibliography relevant to the topics treated in the course. Postscript files of my unpublished papers can be found at `http://www.maths.ox.ac.uk/~krajicek`.

References

[1] Ajtai, M. (1983) Σ_1^1 - formulae on finite structures, *Annals of Pure and Applied Logic*, **24** : 1-48.

[2] —— (1988) The complexity of the pigeonhole principle, in: *Proc. IEEE 29th Annual Symp. on Foundation of Computer Science*, pp. 346-355.

[3] —— (1990) Parity and the pigeonhole principle, in: *Feasible Mathematics*, Eds. S.R.Buss and P.J.Scott, pp.1-24. Birkhauser.

[4] —— (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.

[5] —— (1994) Symmetric systems of linear equations modulo p, a preprint. Available as a report number TR94-015 of the *Electronic Colloquium on Computational Complexity*, http://www.eccc.uni-trier.de/pub/eccc

[6] 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.

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

[8] 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.

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

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

[14] —— (1997) No feasible interpolation for TC^0 proofs, preprint.

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

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

[17] —— (1987) The propositional pigeonhole principle has polynomial size Frege proofs, *J. Symbolic Logic*, **52**: 916-927.

[18] 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.

[19] Clegg, M, Edmonds, J., and Impagliazzo, R. (1996) Using the Groebner basis algorithm to find proofs of unsatisfiability, in: *Proceedings of the 28th ACM Symposium on Theory of Computing*, ACM Press. pp.174-183.

[20] 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.

[21] —— (1975) Feasibly constructive proofs and the propositional calculus, in: *Proc. 7^{th} Annual ACM Symp. on Theory of Computing*, pp. 83-97. ACM Press.

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

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

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

[25] 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.

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

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

[28] Furst, M., Saxe, J., B., and Sipser, M. (1984) Parity, circuits and the polynomial-time hierarchy, *Math. Systems Theory*, **17**: 13–27.

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

[30] Hastad, J. (1989) Almost optimal lower bounds for small depth circuits. in: *Randomness and Computation*, ed. S.Micali, Ser.Adv.Comp.Res. **5**: 143-170. JAI Pres.

[31] 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.

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

[33] —— (1994) Lower bounds to the size of constant-depth propositional proofs, *Journal of Symbolic Logic*, **59(1)**, pp.73-86.

[34] —— (1995) On Frege and Extended Frege proof systems, in: *Feasible Mathematics II*, eds. P. Clote and J. Remmel, Birkhauser, pp. 284-319.

[35] —— (1995) *Bounded arithmetic, propositional logic and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, Cambridge - New York - Melbourne.

[36] —— (1997) Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, *J. of Symbolic Logic*, **62(2)**, pp.457-486.

[37] —— (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.

[38] —— (1996) A fundamental problem of mathematical logic, *Annals of the Kurt Gödel Society*, Springer-Verlag, Collegium Logicum, Vol.2, pp.56-64.

[39] —— (1996) Extensions of models of PV, in: *Proc. Logic Colloquium 1995 (Haifa)*, Eds. V. Harnik and J. Makowsky, Springer-Verlag, submitted.

[40] —— (1996) Discretely ordered modules as a first-order extension of the cutting planes proof system, submitted.

[41] —— (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.

[42] —— (1997) On the degree of ideal membership proofs from uniform families of polynomials over a finite field, submitted.

[43] —— (1997) Uniform families of polynomial equations over a finite field and structures admitting an Euler characteristic of definable sets, preprint.

[44] 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

[45] —— (1990) Quantified propositional calculi and fragments of bounded arithmetic, *Zeitschrift f. Mathematikal Logik u. Grundlagen d. Mathematik*, **36**, pp.29-46.

[46] —— (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.

[47] —— (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.

[48] Krajíček, J, Pudlák, P, and Takeuti, G. (1991) Bounded arithmetic and the polynomial hierarchy, *Annals of Pure and Applied Logic*, **52**: 143–153.

[49] 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.

[50] 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.

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

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

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

[54] 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.

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

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

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

[58] —— (1996) Lower bounds for resolution and cutting planes proofs and monotone computations, to appear.

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

[60] —— (1987) Lower bounds on the size of bounded depth networks over a complete basis with logical addition, *Matem. Zametki*, **41(4)**, pp.598-607.

[61] —— (1994) On provably disjoint NP-pairs, Basic Research in Computer Science Center, Aarhus, RS-94-36, preprint.

[62] —— (1995) Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic, *Izvestiya of the R.A.N.*, **59(1)**, pp.201-224.

[63] —— (1997) Lower bounds for the polynomial calculus, *Computational Complexity*, to appear.

[64] 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.

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

[66] —— (1994) $Count(q)$ does not imply $Count(p)$, to appear.

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

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

[69] 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.

[70] 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..

[71] 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.

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

[73] Yao, Y. (1985) Separating the polynomial-time hierarchy by oracles, in: *Proc. 26th Ann. IEEE Symp. on Found. of Comp. Sci.*, pp. 1-10.