Errata for my books

Jan Krajíček

Last update: 12.April 2025

This file consists of the errata for my books plus some supplementary material in the appendix. I maintained the errata pages on my web page so far but in the ever-changing digital university space they may not be available in the long-term. It appears that these pages were useful to a number of readers over the years and perhaps will continue to be so. It will be easier to arrange for their archiving in the pdf format. In future only this file will be updated.

The books covered are at present:

1. [1]: *Bounded arithmetic, propositional logic and complexity theory*, 1995,
2. [3]: *Forcing with random variables and proof complexity*, 2011,
3. [5]: *Proof complexity*, 2019.

I expect to add eventually some material related to the fourth one:

4. [6]: *Proof complexity generators*, in press (expected to appear in 2025).

All were (or will be) published with the Cambridge University Press.

The first three sections contain (slightly edited) errata pages for my first three books as they were on my web page in October 2024. In all sections we use the terminology and the notation from the corresponding book without further explanations.

Acknowledgments:

I am indebted to the following colleagues who pointed out some of the errors or issues to clarify:

K.Aehlig (Munich), A. Beckmann (Muenster/Swansea), S.Buss (San Diego), P. Clote (Boston/Munich), S.Cook (Toronto), U.Egly (Wien), Y.Filmus (Toronto), Pietro Galliani (Bolzano), Michal Garlik (St.Petersburg), Raheleh Jalali (Amsterdam), E.Jerabek (Prague), J.Joosten (Amsterdam/Prague), E.Khaniki (Tehran), L.Kolodziejczyk (Warsaw), J.Maly (Vienna) M.Moniri (Tehran), M.Narusevych (Prague), N.Thapen (Oxford), Emre Yolcu (CMU) and Konrad Zdanowski (Warsaw).

1 The 1995 book

- 4.3.10: p.40, the proof of Claim 2: the induction really goes on a part of proofs consisting of ancestors of the end-sequent of the original σ. Hence the induction assumption should rather say: Let any formula in σ either have depth $\leq d$ or be an ancestor of an identical formula in the end-sequent.

- 4.4.8: factor k is obviously missing in part 2.

- 4.6 (pp.57-58): In Def.4.6.2 no variable occurrence free in B should become bounded in $A(B)$. Alternatively, one could allow only quantifier-free B. Another alternative is to introduce bound and free variables in formulas and allow only formulas with no occurrences of bound variables outside the scope of a quantifier.

- 4.6: The proof of L. 4.6.3 uses Π_1^q flas although only Σ_1^q flas are allowed by the definition. Modify the proof of the first part of L. 4.6.3 to use only Σ_1^q-formulas. Namely, simulate EF-proof $\theta_1, \theta_2, \ldots$ by G_1^*-proofs of $\neg\theta_1 \rightarrow, \ldots$ rather than by proofs of $\rightarrow \theta_1, \ldots$. In particular, the substitution rule is simulated than as follows:

$$\frac{\neg\theta(\overline{p}) \rightarrow}{\exists\neg\theta(\overline{p}) \rightarrow}$$

and derive

$$\neg\theta(\overline{\phi}) \rightarrow \neg\theta(\overline{\phi})$$

and thus

$$\neg\theta(\overline{\phi}) \rightarrow \exists\neg\theta(\overline{p})$$

and get but the cut the wanted sequent

$$\neg\theta(\overline{\phi}) \rightarrow$$

Another option (better perhaps): allow in the definition (Def. 4.6.2) of G_i and G_i^* not only Σ_i^b-formulas but also Π_i^b-formulas; that is surely equivalent (w.r.t. p-simulation).

- p.83, l.5: the term $|y|$ in formula $B(s)$ means "cardinality" of y as a set it codes. This should be properly $Numones(y, |y|)$. The LENGTH-MAX principle still obviously applies.

- L. 5.5.7, p.88: in the proof $\Sigma_1^{1,b}$-PIND should be $\Sigma_i^{1,b}$-PIND.

- 7.1: on p. 103 I left out the equality axiom $x = x$.

- In Lemma 7.1.3 the sequents $BASIC^{LK}$ must include all substitution instances of BASIC (unless one wants to allow cuts on their universasl closures).

- 7.1, p.104: the definition of "free" formula should be dual. E.g.: a formula is "free" iff it has no ancestor that is either a principal formula of an induction inference or in an initial sequent.

  An cut inference is "free' iff both occurences of the cut formula in the upper sequents are free.

- In Lemma 7.2.2 (a): ... in S_2^i should be ... in S_2^1.

- p.110: in the proof of the witnessing theorem, in the case of PIND rule one needs to attach to the construction of g a test that looks after each round if a witness to a side formula in the succedent has been found, and if so it stops. This takes care of the case when even the witness for Δ in function g_1 depends on the eigenvariable (which can happen even if the eigenvariable doesn't appear in Δ).

- In the proof of Corollary 7.2.6, p.112, I should appeal first to Parikh's theorem to get rid of unbounded $\exists$ and only then to Theorem 7.2.3. Or extend witnessing to handle unbounded $\exists$ on the right.

- The provability of Δ^b_{i+1} - IND in T^i_2 is stated in Cor. 7.2.7. However, during cross-referencing I have created a vicious circle. Namely:

  1. 6.1.3 follows from 7.2.7

  2. 7.2.7 follows from 5.2.9 and 7.2.4

  3. but 6.1.3 is used (together with 7.2.3) in the proof of 7.2.4.

  One way out is to deduce 6.1.3 directly using Thm. 6.1.2 (and the idea of its proof). One proceeds in two steps:

  1. Show that all f.symbols $f(x) = y$ of PV_{i+1} are definable in T^i_2 in the form

  $$\exists (u, w) \leq t;\ Comp(x, w, u) \wedge Output(x, u) = y \wedge$$

  $$u \text{ correctly encodes the answers of oracle } \phi$$

  where ϕ is a Σ^b_i-oracle.

  2. Having PV_{i+1} symbol $f(x)$ defining predicate $A(x) \equiv_{df} (f(x) = 0)$ such that $A(0)$ and $\neg A(a)$ hold, use binary search to find x smaller than a such that $A(x) \wedge \neg A(x + 1)$.

  The answers to the binary search queries (i.e., $A(a/2)$? etc.) encode by some v. Now combine the query-answers in v together with the strings u encoding the query-answers used in the computation of $A(a/2)$?, etc. into one string $(u_1, u_2, ..., u_\ell, v)$ (actually v is not needed really).

  By the same reasons as in the proof of Thm. 6.1.2 (MAX principle) there is, provably in T^i_2, a string encoding everything correctly, and hence the found x smaller than a witnesses the failure of the induction assumption.

- 7.3, p.119: The last but one paragraph of the proof of Thm.7.3.7 needs a modification.

  For an easier calculation assume that we want to witness by $h(a)$ that f does not map a onto a^3 (this is w.l.o.g. as we may iterate the original f). Put $b_i := 2^{2^i}$, $i = 0, 1, \ldots, t$ such that $b_t \in [2^{p(n)}, 2^{2p(n)})$, i.e. $t = O(\log n)$. In particular, $h(a) =?$ will be ever queried by M only for $a \leq b_t$.

  At the beginning of the computation pick from each interval $I_i := [b_i, 3b_i]$ uniformly at random a representant c_i. Start the computation

of M and whenever $h(a) =?$ is queried for $a \in (b_{i-1}, b_i]$ answer it with $h(a) = c_i$.

Now, $a \leq b_i = |I_i|/2$ so $c_i \notin Rng(f \downarrow a)$ with probability $\geq 1/2$ (on the other hand $c_i \leq 3b_i \leq b_{i-1}^3 \leq a^3$). So with probability $\geq 2^{-t}$ all oracle queries are answered correctly. Hence the probability that M fails to output a correct answer is $\leq (1 - \frac{1}{2p(n)})$.

Repeat the whole computation $4p(n)$ - times, always choosing new random collection of c_i's. the probability that all of these computations fail is at most $(1 - \frac{1}{2p(n)})^{4p(n)} \leq e^{-\frac{4p(n)}{2p(n)}} = e^{-2} < 1/4$.

Note that if the theorem were stated for $PV_1 + WPHP$ rather than for $S_2^1 + WPHP$ the $\Sigma_1^b(h)$-formula in the proof would be witnessed by a term (involving h). Evaluating the term one needs to find only constantly many values $h(a)$; in this case it is not necessary to use the interval I_i but simply pick a random value $\leq 2a$. The probability of failure of one computation is then $\leq 1-\Omega(1)$, i.e. it is enough to repeat the whole process $O(1)$ - times.

- 7.4: p.120 (7th line of the proof of 7.4.1): "... of $\exists z \eta(a, x, y, z)$" should be

  "... of $\exists x \forall y \exists z \eta(a, x, y, z)$".

- In 7.4.2: the function should be not Σ_{i+2}^b-definable but $\exists \forall \Sigma_i^b$-definable (as one would need some BB-scheme, not apparently available, to get it into the $s\Sigma_{i+2}^b$-form).

- L. 8.2.3: One needs to assume i ¿ 0. This prevents using the lemma in the proof of the i=0 case in Thm.8.2.4 about a relation of U_2^1 nad PSPACE (other cases are OK). This case is proved via a direct witnessing argument.

- p.152, proof of Thm.9.2.5: In this proof one needs that quantified propositional proof systems G_i and G_i^* (for $i > 0$) allow the substitution rule. I refer to L.4.6.3 where this is shown for G_1^*. However, in the current proof one needs to shown that the quantifier complexity of the simulation does not increase (it does in L.4.6.3). The argument is almost the same but a bit more careful on quantifiers: Assume we want to substitute A (which is q.free!) for p in sequent

(1): $U(p) \longrightarrow V(p)$,

where U, V are Σ_i^q. Proceed as follows. First derive sequents

(2): $p \equiv A, V(p), U(A) \longrightarrow V(A)$

and

(3) $p \equiv A, U(A) \longrightarrow V(A), U(p)$,

both by p-size proofs. Also derive

(4): $\longrightarrow \exists x, x \equiv A$. Apply cut to (1) and (3) getting

(5): $p \equiv A, U(A) \longrightarrow V(A), V(p)$.

Another cut of (5) and (2) yields:

(6): $p \equiv A, U(A) \longrightarrow V(A)$.

Finally existentially quantify x in the antecedent of (6) and cut it out with (4).

- p.155 and other places: Argument is restricted to $s\Sigma_1^{1,b}$-PIND instead to the whole of U_2^1. This is in order to avoid a cumbersome notation in more complex witnessing. To justify this we can add suitable Skolem functions (functionals) to the language and axioms about them - these are universal closures of first-order bounded formulas and easily witnessable. Modulo these axioms we get $\Sigma_1^{1,b}$-AC and hence justify the restriction to the strict class. For V_2^1 this AC is directly proved from induction axioms for $s\Sigma_1^{1,b}$ formulas.

- L.9.3.2 (b), p.164: The closure properties of the proof system should be "provable" in S_2^1.

- L.9.3.4, p.165: ...) bracket is missing before the implication.

- 9.3, p.166, in the Claim: the sign $\equiv$ (twice) should be $=$, and the claim should end with a half-sentence:

  "... thinking of formulas as of Boolean functions and, in particular, of A_j as abbreviating also the value of $A_j(\overline{p})$ on $\overline{p}$."

- 9.4.1, Claim 6, p.174: item (b) should be stated for u bounded by any element (universally quantified) of the cut and not by the cut itself - this violates the required definability of the sets in the forcing notion (the partial ordering $\mathcal{P}$).

- 9.4.2, p.175: The extension $(M', \mathcal{X}')$ is not only $\Sigma_0^{1,b}$-elementary but also a model of V_1^1.

- Proof of Lemma 10.2.2: 1. on p.187, line -3: add conjunct $g(h(|v|), v) \leq v$ (the function $g(u, v)$ actually constructed obviously has this property). 2. on p.189: the last sentence in the proof is redundant (and, in fact, bit confusing).

- p.212, item (ii): function f_j should depend also on t_j.

  Lemma 11.1.2: this lemma appears incorrect (in the proof I implicitly use a universal quantifier over functions h).

- Thm. 11.2.4, p.215: The amplification of $G : 2a \to a$ to $F : a^2 \to a$ works if a is a power of 2. If it is not combine (using G) such an F from maps $G^{(k)} : a \times 2^k \to a$, for k's occurring in the binary expansion of a.

- 11.3.1: Machine gets as the input only a and not whole structure $([0, a], R)$. So the time is $(\log a)^{O(1)}$.

- Thm. 11.4.6: Should be stated only for $i = 2$, not for $i \geq 2$.

- 11.5: p.231: Pudlak (1992a) in paragraph 1 should be Pudlak (1992b).

- 12.1, Thm.12.1.3: Ramsey theorem is provable already in $T_2^4(R)$, by the same argument: on p.235 bottom note that a $\Sigma_2^b(H)$-formula for H being a boolean combination of $\Sigma_2^b(R)$-formulas is $\Sigma_4^b(R)$ and not only $\Sigma_5^b(R)$.

- 12.2: p.239 (last line): $R^{(-1)}(j)$ should be $r^{(-1)}(j)$

- 12.3.1, p.244,l.6: $\alpha = \emptyset$ ought to be $\gamma = \emptyset$

- p.304, line 2: $||0 - RFN(Q)||$ should be just $0 - RFN(Q)$.

- 15.1: The proof of Thm. 15.1.4 contains few typos and inaccuracies.

  In particular:

  – In Claim 1 the size of U is $2^{n(t+1)}$. Also, in the 2nd l. in its proof the number of Ms s.t. $Mx = My$ is $2^{(n-1)(t+1)}$. The needed estimate is, however, correct with these "new" values too.

– Redefine the function F on the bottom of p.310 as follows:

$F(x) := (i, M_i x)$,

where i is the unique s.t. $x \in B_{i+1} \setminus B_i$.

- In L 15.2.2: should be: "..... refines H^{ρ}_{ℓ}" and not just "..... refines H_{ℓ}".
- 15.3.9 and 15.3.10: One should (1) either have strict Σ^b_1 and Π^b_1 formulas, (2) or S^1_2 in place of PV.

  The point is that L. 9.3.12, which they both utilize, uses S^1_2 and that is essential as one needs sharply bounded Σ^b_1-collection scheme: The scheme is available in S^1_2 but not in PV (unless factoring is easy by Cook-Thapen 2004).

2 The 2011 book

Before giving the errata comments let me address the publication year. The publisher displays sometimes 2010 while the printed book shows 2011. The book was published in Europe on 23.December 2010, but in other parts of the world it did not publish until 2011. When books publish towards the end of the calendar year publishers tend to move the copyright year (i.e. the date printed in the book) forward so that the book does not immediately appear out of date. So, as I was told, *neither year is really incorrect.* I stick with what is printed.

- p.30, the last sentence of the proof of L.3.4.2: This proves the statement for non-standard i only but for standard ones it is the hypothesis of the lemma.
- p.44,l.-2: Lower case θ ought to be upper case Θ.
- pp.57-59, Secs.8.2-4: the 2nd order equality sign should be removed from the language $L^2_n(F_{rud}, G_{rud})$ for the statements to hold (it is not decided on samples via shallow tress)
- pp.76 and 96 (1st paragraphs of Sections 12.1 and 16.1): We are using L 3.3.3 even though it applied to first order structures only. Recall from the beginning of Chpt.5 that "second order" is just a misnomer and we treat K(F,G) as first order. On p.45 center it is pointed out that results proved earlier for K(F) hold equally for K(F,G).

- p.80: the definition of Δ is found after L.12.1.2 and not in Thm.12.2.1.

- p.98. A hint for a proof for Theorem 16.1.4: The simplest proof is that in V^0 you can from $\forall x\ Closure(x)$ prove that for any fixed $m \geq 2$ standard there are counting *mod* m functions for all sets. This then gives via simple witnessing a low degree polynomial over $\mathbf{F}_2$ defining counting *mod* 3 with a small error - that is a contradiction.

- p.107: Two lines before 18.1.1 I sloppily state that there is a function symbol for $s(k)$ in L_n. However, the cut $\mathcal{M}_n$ is not necessarily closed under a subexponential $s(k)$ (e.g. $2^{k^{1/t}}$) and hence there is no symbol for the function in L_n. But it is not needed later on: one only needs that $s(n)$ is in the cut (which it is).

  To have the formula Prf_P bounded add a new free variable y to bound Y and in the particular case substitute $s(n)$ for y. (We wouldn't need y if we had in L_2 the symbol $|Y|$ for $\max(Y)+1$ used by Cook and Nguyen in their book).

- p.117: The notation (T, ℓ) is used on line -9 without explaining what ℓ is.

  This follows the notation from 7.1 where labeled trees appeared first.

- pp.154-155: This section is messed up: the notation and the definition of RSA are incorrect and this makes the presentation of Thm.24.1.1 hard to follow. RSA sends x to x^e *mod* N, of course. The sample space should consists of RSA pairs (e, N) (where e, N satisfy the conditions for g, N on p.154) and cipher texts. The construction shadows then the proof of Thm.3 and Cor.4 in [76].

  More details are in J.Maly's MSc. Thesis (Chpt.3) at the Universitat Wien, 2016, available at

  `https://www.dbai.tuwien.ac.at/staff/jmaly/Master.pdf`

- p.170, line -3: the bound 2^{n^n} is just a very generous bound (I prefer simple terms).

- p.198, L.30.1.1, proof sketch:

  If $NE \cap coNE$ have size s circuits then the τ-formula from Possibility A is not a tautology for any L in $NE \cap coNE$ (i.e. the formula determined

by the characteristic string of L restricted to strings of size k) and hence - by Poss.A - the truth-table function with parameter s is hard for every pps P (so $NP \neq coNP$).

- L.31.2.1: There is a gap in Claim 3 in the proof (the argument does not take into account those inputs u to C which determine sample a(u,e) which is in U but not in W) and, in fact, the lemma does not hold as stated (e.g. the region of undefinability of an α querying just one line i and then aborting or stopping with 0 respectively will be almost a half of the sample space).

  To resurrect the lemma one needs to alter the construction just a little bit: take for the sample space not the whole of Ω_b (p.208) but just its suitable subset Ω_b^* (still infinite and an element of the ambient model to conform with Sect.1.2) for which the lemma holds - a sort of "hard-core" of the sample space. There is a simple model-theoretic argument that such suitable set exists in which the original L.31.2.1 (more precisely, what the lemma actually proves) is used. We outline this in Section A here.

  Further remarks:

  (1) The existence of a nonstandard model of T_{PV} in which $\exists x NW_{A,f}(x) = b$ holds and the resulting consistency of Razborov's conjecture and even of the stronger statement (S) (i.e. the context of Sects.31.3 and 31.4) has been also established "classically" (via the KPT witnessing and a version of L.31.2.1 in which the Student-Teacher solve (T) for all inputs, i.e. W is everything, and the problem mentioned above is avoided) in my subsequent paper [2].

  (2) For the program of reducing lower bounds for strong proof systems to circuit hardness assumptions, an acceptable form of the assumption is that every circuit performing some specific task needs to be large (see Chpt.27 and p.175 bottom).

  In particular, form my point of view it would be OK to use an assumption that every circuit computing a strategy of the Student solving task (T) (or some similar task) over a particular sample space with a positive probability needs to be large. The further reduction to the hardness of the function f is "an extra": it is nice if one's assumption follows from a standard one but it is not really that important.

3 The 2019 book

- p.14, Thm.1.1.3: the monotone version should assume that atoms p occur only positively in α or only *positively* in β. The condition that is there (positive in α or negative in β) is good under the assumption that $\alpha \wedge \beta$ is unsatisfiable.

- p.17, proof of Spira's lemma (Lemma 1.1.4): for the first subtree T_a with size $|T_a| \leq (k/(k+1))|T|$ the previous subtree must have size at most $s \leq k|T_a| + 1$ (+1 is missing); the rest of the proof follows as before.

- p.34, line -4: the quantities s_P and s_Q ought to be switched to $s_P(\tau) \leq s_Q(\tau)^c$.

- p.43, Thm.2.2.1: the estimates to the number of steps and the size of the constructed tree-like proofs use implicitly that modus ponens is present or, more generally, that it can be simulated using each premise just once. Jerabek gave a counter-example for a general case: there is no fixed polynomial slow-down that would hold for all Frege systems F (the degree may depend on F).

  He also (cf. ArXiv: 2303.15090) improved a bit bounds to k_{F^*} and s_{F^*} when modus ponens is present in terms of his notion of "inferential size" (of an F-proof) instead of ordinary s_F.

- p.77, L.3.4.5: the proof as given is wrongly organized. An alternative stand-alone argument using the Buss-Pudlak game (Sec.2.2) and DNF-R (Sec.5.7) is in Section B here. It gives only a quasi-polynomial bound but that suffices in all uses of the lemma.

- p.79, definition of the Σ-depth: in item 3 should be inequality $dp(A) \leq d+1$.

  In the definition of $LK_{d+1/2}$ in the 2nd paragraph: allow also $Pi_d^{S,t}$ formulas in π.

- p.191: the notation $X \leq x$ ought to be introduced before the bounded CA axiom and the 2nd order existential quantifier $\exists X$ in it ought to be bounded: $\exists X \leq x$.

Without it we can prove that for each $[0, x]$ there is X having an empty intersection with the interval but not the existence of the empty set (the former suffices for many purposes but it is unintuitive).

- p.206, L.10.5.1: the upper bound to the lengths of propositional simulations of theories $T^i_1(\alpha)$ (in this lemma and others in Sec.10.5) is quasi-polynomial as it uses L.3.4.7 and hence implicitly L.3.4.5 - see the remark about that lemma above.

  There is an additional quasi-poly blow-up when translating sharply bounded formulas into DNF/CNF formulas; this can be remedied, however, posing a restriction on sharply bounded kernels of induction formulas analogous to DNF_1 formulas.

  Polynomial upper bounds hold for the theory defined before L.10.5.2 by the model-theoretic proof in [288]. Analogous theories can be defined for higher $i > 1$. But most natural is to use the quasi-polynomial proof size and theories T^i_2 because all uses of these simulations use theories with the smash function (including the original paper [276]).

- p.240, Cor.12.2.4: the proof is not well-presented (e.g. that h does not occur in T and that axioms of equality are not needed to derive (12.2.9) from (12.2.8) and hence h does not occur in axioms of equality is not stated).

  It is much clearer to base the proof on "propositional" Cor.12.2.2: (12.2.6) is a tautology and after replacing everywhere $h(t'_k)$ by z_k same atoms (= atomic formulas) remain same and hence (12.2.6) remains a tautology.

  (See references in the book for further alternative proofs.)

- p.288, Cor.13.5.4: constant c is redundant

- p.300, Thm.14.3.1: using the lower bound for R-refutations of $\neg WPHP^{n^2}_n$ instead of lower bounds for $R^*(\log)$ we can strengthen a bit the base case of Thm.14.3.1 to the separation of $LK_{1/2}$ from LK_0 and hence from LK^*_1 (by L.3.4.4). This then implies a separation of $LK_{d+1/2}$ vs. LK_d or equivalently vs. LK^*_{d+1}. I do not know if this improvement has some immediate bounded arithmetic relevance.

- p.375, Subsec.17.6.2: the bound to CC and MCC is $2 \log n$ rather than just $\log n$ as in 17.6.1 (both players need to send their partial sums in the binary search).

- p.433/ definition of $s(n)$-iterability before Thm.19.5.3: this definition using g_n-circuits is not the right one (the thm is still correct but useless).

  Use instead the original definition from Sec.3 of [291] (= J.K., "Dual weak ...") using the notion of an "iteration protocol".

- p.468, Problem 21.5.3: for a fixed P there is such time-optimal (A, P), with A constructed as in universal search (for $i = 1, 2, \ldots$ try first i algorithms for i steps until you find a P-proof of the formula). Here set E can be empty.

  Further: it can be proved that some (A, P) is time-optimal iff P is p-optimal, for P containing R and satisfying the technical condition in Lemma 21.1.1.

  An augmented definition of the quasi-ordering of proof search algorithms was proposed in my Oberwolfach 2020. However, I now look at it a bit differently: see my 2020 JSL paper *Information in propositional proofs and algorithmic proof search.*

- p.468 bottom (remarks for Sec.21.1): the results of [353,269,64] mentioned relate to the existence of an optimal proof system, not p-optimal.

- p.470: the weak set theory I write about in the second paragraph is called "adjunctive set theory" and was discussed already in 1950s by W.Szmielew, A.Tarski and others.

Michal Garlík wrote a 3-page list of minor errors and misprints he noted while using the book in his St.Petersburg course in Fall 2020. It is, at least for now, available at:

`https://www.karlin.mff.cuni.cz/~krajicek/garlik-comments.pdf`

Appendix

A The local witness model

In this section we expand upon the comment concerning L.31.2.1 in Section 2, which was used in the construction of the local witness model in [3, Chpt.31]. To find the suitable hard-core of the original sample space we may proceed as follows. A more detailed (and general) presentation is in [4]. We use the notation from [3, Sec.31.2.].

In the proof of Lemma 31.2.1 we pick by averaging e s.t. at least a fraction of $\delta\frac{1}{(3m)^k}$ more inputs u to C (and f) yield a sample $a(u,e) \in W$ whose trace is exactly $\bar{i}$ than those which do yield $a(u,e) \in W$ whose trace properly contains $\bar{i}$ (Claims 1 and 2). The error in the argument for Claim 3 is that we have no control over the number of u for which $a(u,e) \notin W$ but its trace contains $\bar{i}$, i.e. of the size of the set $U \setminus W$.

However, if we knew that the size of the complement of W is at most e.g.

$$w_c := \frac{1}{2}2^{n^{1/3}}\frac{1}{(3m)^c}$$

then the argument works: w_c bounds the number of bad u and the algorithm constructed in Claim 3 gets the advantage at least (we ignore δ now)

$$\frac{1}{(3m)^k} - \frac{1}{2}\frac{1}{(3m)^c} \geq \frac{1}{2}\frac{1}{(3m)^k}$$

and the rest of the proof (bottom p.212, top p.213) remains the same.

Hence what is established in [3, Sec.31.2] is the following statement.

Lemma A.1 *Under the same hypothesis as in [3, L.31.2.1], the number of samples $\omega \in \Omega$ for which $\alpha(\omega)$ is defined is at least*

$$w_c := \frac{1}{2}2^{n^{1/3}}\frac{1}{(3m)^c}$$

where c bounds the number of queries can ask on any sample.

Note that w_c is a nonstandard number for any $m \in \mathcal{M}_n$ and any standard c.

We would like to use Lemma A.1 to establish

Lemma A.2 *There exists an infinite set $\Omega^* \subseteq \Omega_b$, $\Omega^* \in \mathcal{M}$, such that each $\alpha \in F_b$ is defined on all but an infinitesimal fraction of samples from Ω^*.*

Taking F_b^*, the family of random variables defined as F_b but restricted to Ω^*, determines model $K(F_b^*)$ for which the analogous statement to [3, L.31.2.1] holds and it can be used in place of $K(F_b)$.

Lemma A.2 can be derived by a combinatorial argument for small $m > n$ but here we shall give a model-theoretic argument which has the advantage 1of being much simpler and working for any m, using a smaller set of random variables.

Namely, for any string $w \in \mathcal{M}_n$ let $F_{b,w}^{unif}$ be the family of partial random variables on Ω_b defined as F_b but allowing the algorithms computing the random variables to use as an advice only the triple (A, b, w). This is perfectly sufficient for any application of the eventual model in Secs.31.3. and 31.4 of [3]: w can contain e.g. a proof of the τ-formula or a witness of the membership of b in an NP set R, etc., and has the great advantage that the family $F_{b,w}^{unif}$ is now countable.

Lemma A.3 *Let $w \in \mathcal{M}_n$ be arbitrary. Then there exists an infinite set $\Omega^* \subseteq \Omega_b$, $\Omega^* \in \mathcal{M}$, such that each $\alpha \in F_{b,w}^{unif}$ is defined on all samples from Ω^*.*

Proof :

Enumerate $\alpha_1, \alpha_2, \ldots$ the set $F_{b,w}^{unif}$ in such a way that the algorithm defining α_k runs in time $\leq m^k$ and ask at most k queries, for all $k \geq 1$.

Let $\{\alpha_i\}_{i<t} \in \mathcal{M}$ be its non-standard extension obtained via the $\aleph_1$-saturation (see [3, p.9]).

If we take $\alpha_1, \ldots, \alpha_k$ we can compose the programs defining the αs by first running α_1, if it is not aborted then instead of outputting a value run α_2, etc. , and output (arbitrary) values only at the end, if the computation is not aborted earlier. The resulting function is computed in time $O(km^k)$ using at most $k(k+1)/2 \leq k^2$ queries. Hence by Lemma A.1 it is defined on at least w_{k^2} samples from Ω_b. This yields the following

Claim: *For each standard $k \geq 1$ there exists definable subset $\Omega^k \subseteq \Omega_b$ of size at least w_{k^2} such that all $\alpha_1, \ldots, \alpha_k$ are defined on all samples from Ω^k.*

By Overspill the statement of the Claim holds also for the sequence $\{\alpha_i\}_{i<t}$ for some non-standard $s < t$, and we can take s small enough (but still non-standard) such that $\Omega^* := \Omega^s$ satisfies the statement of the lemma.

q.e.d.

B Tree-like LK-proofs

In this section we give the construction promised in the remark concerning p.77/[5, L.3.4.5] in Section 3 in the 2019 book.

(1) Set-up:

n: number of atoms
$\mathcal{C}$: a set of clauses in n variables
π: a tree-like DNF-R refutation (i.e. $R^*(id)$-refutation) of $\mathcal{C}$
k: the number of steps in π
s: size of π
c: a parameter bounding the number of conjunctions in any line in π
We allow as initial clauses also all clauses containing some $\{\ell, \neg\ell\}$.

(2) Lemma: *Assume the set-up (1). Then $\mathcal{C}$ has an R^*-refutation π^* (i.e. tree-like R) with at most $n^{O(c \log k)}$ steps.*

The lemma follows from Lemmas (5) and (6) below. Note that it is not claimed that π^* is balanced.

(3) Remark: Lemma (2) implies an analogous statement about depth $d+1$ LK refutations with k and n in the estimate replaced by $O(s)$: use limited extension for all depth $\leq d$ formulas in π to reduce to $R^*(id)$. Then substitute in π^* back formulas for the corresponding extension atoms (this changes n by adding the number of extension atoms and k when deriving a formula from the associated extension atom - in both case it is bounded above by $O(s)$).

(4) Game: Consider the Prover-Liar game where Prover asks for the truth-value of a clause D and the Liar either replies *true*, in which case D is added to his set $\mathcal{D}$ of replies, or *false*, in which case all singleton clauses $\{\neg\ell\}$, all $\ell \in D$, are added. The game stops with Prover winning the moment $\mathcal{C} \cup \mathcal{D}$ contains some clause D and at the same time also all $\{\neg\ell\}$, all $\ell \in D$.

(5) Lemma: *Assume that Prover has a winning strategy S that wins over each Liar in at most r rounds. Then $\mathcal{C}$ has an R^*-refutation with at most $(n+1)^{r+1}$ steps.*

Proof :

Think of S as of a binary tree branching according to Liar's answers. For a partial path σ in S ending in vertex v_σ denote:

S_σ: the subtree with root v_σ,
$\mathcal{D}_\sigma$: Liar's answers given on path σ,
r_σ: the height of S_σ.

Note that for the empty path Λ, $S_\Lambda = S$, $\mathcal{D}_\Lambda = \emptyset$ and $r_\Lambda = r$.

We shall prove by induction on r_σ the following

Claim: *$\mathcal{C} \cup \mathcal{D}_\sigma$ has an R^*-refutation ρ_σ with at most $(n+1)^{r_\sigma+1}$ steps.*

Assume $r_\sigma = 0$, i.e. σ is a complete path in S. By the definition of the game the set $\mathcal{D}_\sigma$ contains some clause D and also all singleton clauses $\{\neg\ell\}$, all $\ell \in D$. Define ρ_σ to be $|D| \leq n$ resolutions removing from D subsequently all literals.

Assume $r_\sigma > 0$. Let D be the clause S asks at node v_σ and denote by $S_{\sigma 1}$ the subtree corresponding to the positive answer (hence $D \in \mathcal{D}_{\sigma 1}$) and by $S_{\sigma 0}$ the negative subtree (hence $\{\neg l\} \in \mathcal{D}_{\sigma 0}$ for all $\ell \in D$). Let ρ_1 and ρ_0, resp., be the two R^*-refutations attached to the two subtrees satisfying the induction assumption, having k_0 and k_1 steps, respectively.

Change in ρ_0 all $\{\neg\ell\}$, $\ell \in D$, into $\{\neg\ell, \ell\}$ and carry the extra literals along the whole ρ_0: this yields an R^*-derivation ρ_0' of D from $\mathcal{C} \cup \mathcal{D}_{\sigma 0}$ with the same number of steps as in ρ_0.

For all $\ell \in D$ construct an R^*-derivation $\rho_{1,\ell}$ of $\{\neg\ell\}$ from $\mathcal{C} \cup \mathcal{D}_\sigma$ as follows: add to each occurrence of D as initial clause in ρ_1 literal $\neg\ell$ (hence the clause becomes an instance of free logic initial clauses - see (1)) and carry it along. Note that all $\rho_{1,\ell}$ have the same number of steps as ρ_1.

The resulting R^*-refutation ρ_σ starts as ρ_0' deriving D and the using subsequently all subproofs $\rho_{1,\ell}$ ($|D|$ of them) to cut out all literals $\ell \in D$. The number of steps in ρ_σ is bounded above by

$$|D| \cdot k_1 + k_0 \leq nk_1 + k_0 \leq n(n+1)^{\rho_\sigma} + (n+1)^{\rho_\sigma} \leq (n+1)^{\rho_\sigma+1} \ .$$

This proves the claim.

The lemma follows from the claim for $\sigma := \Lambda$.

q.e.d.

(6) Lemma: *Under the set-up (1) there is a winning strategy for Prover that wins over any Liar in at most $O(c \log k)$ rounds.*

Proof :

Note that Prover can find the truth value of a DNF-clause by asking separately for the truth values of all (clauses that are negations of) conjunctions in the clause (at most c) and then for the truth value of the sub-clause consisting of the remaining literals. Use this to navigate in π in a Spira-like fashion. Hence Prover needs to ask for the values of $O(\log k)$ DNF-clauses, getting each by asking for the values of $\leq c+1$ ordinary clauses.

q.e.d.

References

[1] J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, Encyclopedia of Mathematics and Its Applications, Vol. **60**, Cambridge University Press, (1995).

[2] J. Krajíček, On the proof complexity of the Nisan-Wigderson generator based on a hard NP $\cap$ coNP function, *J. of Mathematical Logic*, **11(1)**, (2011), pp.11-27.

[3] J. Krajíček, *Forcing with random variables and proof complexity*, London Mathematical Society Lecture Note Series, **382**, Cambridge University Press, (2011).

[4] J. Krajíček, Pseudo-finite hard instances for a student-teacher game with a Nisan-Wigderson generator, Logical methods in Computer Science, Vol. 8 (3:09) 2012, pp.1-8.

[5] J. Krajíček, *Proof complexity*, Encyclopedia of Mathematics and Its Applications, Vol. **170**, Cambridge University Press, (2019).

[6] J. Krajíček, *Proof complexity generators*, London Mathematical Society Lecture Note Series, Cambridge University Press, in press.