Corrections and clarifications in
J. Krajíček, *Forcing with random variables and proof complexity*, CUP, 2011.

- 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.76 and 96 (first 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 well 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 you can prove in V^0 for any fixed $m \geq 2$ standard that $\forall x Closure(x)$ implies that 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 it is stated 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 would not 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 labelled 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 given 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, *Jan Krajíček's Forcing Construction and Pseudo Proof Systems*, MSc. Thesis, University of Vienna, (2016).

- p.170, line -3: The bound 2^{n^n} is very generous but 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 function 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 exposed in

  – 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.
  DOI: 10.2168/LMCS-8(3:9)2012

  that such a suitable set exists in which the original L.31.2.1 (more precisely, what the lemma actually proves) is used.

  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

     – J.Krajíček, *On the proof complexity of the Nisan-Wigderson generator based on a hard $NP \cap coNP$ function*,
     J. of Mathematical Logic, Vol.11 (1), (2011), pp.11-27.
     DOI: 10.1142/S0219061311000979

  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.

J.K.