Corrections and clarifications in
J. Krajíček, *Bounded arithmetic, propositional logic, and complexity theory*, CUP, 1995.

- 4.3.10, p.40, the proof of Claim 2: The induction really goes on a part of a proof 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 occurring 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 to allow only formulas with all occurrences of a bound variable inside the scope of a quantifier.

- 4.6: The proof of L. 4.6.3 uses Π^q_1-formulas although only Σ^q_1-formulas are allowed by the definition. Modify the proof of the first part of L. 4.6.3 to use only Σ^q_1-formulas. Namely, simulate EF-proof $\theta_1, \ldots$ 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 as follows:

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

  and derive

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

  and from it

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

  and get the wanted sequent

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

  by a cut. Another option (better perhaps): allow in the definition (Def. 4.6.2) of G_i and G^*_i not only Σ^b_i-formulas but also Π^b_i-formulas; that is equivalent (w.r.t. p-simulation).

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

- L. 5.5.7, p.88: In the proof the scheme $\Sigma^{1,b}_1$-PIND should be $\Sigma^{1,b}_i$-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 universal 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.

  A cut inference is free iff both occurrences 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, the proof of the witnessing theorem: In the case of the 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 does not 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 the 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 the cross-referencing I have created a vicious circle. Namely: 6.1.3 follows from 7.2.7, 7.2.7 follows from 5.2.9 and 7.2.4 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 for all f.symbols f of PV_{i+1} the atomic formula $f(x) = y$ is definable in T^i_2 in the form

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

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

     where ϕ is a Σ^b_i-oracle.

  2. Having a PV_{i+1} f.symbol f defining the predicate

     $$A(x) \equiv_{df} (f(x) = 0)$$

     such that $A(0)$ and $\neg A(a)$ hold, use a binary search to find $x < a$ such that $A(x) \wedge \neg A(x + 1)$.

     Encode the answers to the binary search queries (e.g. $A(a/2)$? etc.) 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).

     By the same reasoning 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 $x < a$ thsi process finds 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 not be 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 case $i = 0$ in Thm.8.2.4 about a relation of U_2^1 and 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 with the use of 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) to get

(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 p in the antecedent of (6) and cut it out with (4).

- p.155 and other places: Argument is restricted to (strict) $s\Sigma_1^{1,b}$-PIND and does not apply to all PIND axioms 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:

  - on p.187, line -3: add as conjunct $g(h(|v|), v) \leq v$ (the function $g(u, v)$ actually constructed obviously has this property),

- on p.189: the last sentence in the proof is redundant (and, in fact, a bit confusing).

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

  Lemma 11.1.2: This lemma appears to be incorrect (in the proof I implicitely 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 the values k occurring in the binary expansion of a.

- 11.3.1: Machine gets as the input only a and not the 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 the first paragraph should be Pudlak (1992b).

- 12.1, Thm.12.1.3: Ramsey theorem is provable already in $T^4_2(R)$, by the same argument: on p.235 bottom note that a $\Sigma^b_2(H)$-formula for H being a boolean combination of $\Sigma^b_2(R)$-formulas is $\Sigma^b_4(R)$ and not only $\Sigma^b_5(R)$.

- 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 second line 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 either have strict Σ^b_1 and Π^b_1 formulas, or use S^1_2 in the place of PV. The point is that L. 9.3.12, which both statements 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).

J.K.