List of Errors

October 19, 2006

1. pp. 29 (thanks to Klaus Ambos-Spies). Theorem 2.4.1 does not hold. Klaus Ambos-Spies (personal communication) shows that for any Blum space Φ, there exists a total recursive operator F such that GAP_F^Φ is effectively meager.

   The method in the proof of Theorem 2.4.1 only shows the weaker fact that in any Blum space Φ and for any total recursive operator F, the set $\widehat{\mathrm{GAP}}_F^\Phi$ is effectively of the second category, where $\widehat{\mathrm{GAP}}_F^\Phi = \{t \in \mathrm{COMP} \mid \text{there is no } j \text{ such that } t(x) \leq \Phi_j(x) \leq F(t)(x) \text{ a.e. } x\}$. For this weaker result, the following changes are necessary:

   (a) pp. 41, line 5: "for all $z \leq A_i$ should be changed to "for all z with $A_0 \leq z \leq A_i$"

   (b) pp. 41, line -11: "i.o. x" should be changed to "a.e. x"

   (c) pp. 41, line -9: "for some x" should be changed to "'for all x"

   (d) pp. 41, line -6: "$Lh_{s-1} \leq x < Lh_s$ should be changed to $A_0 \leq x < Lh_s$"

   (e) pp. 42, line 2: "for all $x \leq A_{i_0-1}$" should be changed to "for all $A_0 \leq x \leq A_{i_0-1}$"

2. pp. 44, line 4: change all occurences of y to x.

3. pp. 44, line 5: change $U_{\alpha_n} \subset U_{\alpha_{f(i,n)}}$ to $U_{\alpha_{f(i,n)}} \subset U_{\alpha_n}$.

4. pp. 44, line -10: change $U_{\alpha_n} \subseteq U_{\alpha_{f(<i,m>,n)}}$ to $U_{\alpha_{f(<i,m>,n)}} \subseteq U_{\alpha_n}$.

5. pp. 66 (thanks to Klaus Ambos-Spies). Theorem 3.3.13 is retracted because the proof is incorrect. Specifically, Claim 3.3.18 fails (the construction does not guarantee that for all k, if $i \in \mathrm{TOT}$ and $L(P_k)$ is infinite, then $L(P_k) \cup \overline{L(NP_{s(i)})} \neq \emptyset$).

6. pp. 296, line -7: "the definition of a verifier that runs ..." should be "the definition of a (verifier, prover) pair that run ...".

7. pp. 297, line -10: "the prover still has to check ..." should be "the verifier still has to check ..."

8. pp. 306, line 5: "because the both the verifier and the scribe .." should be "because both the verifier and the scribe ..."

9. pp. 308. Claim 6.9.12 should be replaced with the following claim. This implies that in the continuation of the proof we need to have different values for s and t than those given at page. 309, line -6. For example, we can take $s = 2^{0.1n}$ and $t = 2^{0.8n}$. The pseudo-random generator still passes circuits of size $2^{\Omega(n)}$.

   Revised form of Claim 6.9.12.
   With probability of $R \geq 1 - 2^{-t}$,

$$\mathrm{Prob}_{x \in \Sigma^n}(C^R(x) = R^{-1}(x)) \leq \frac{2est}{2^n}.$$

Proof We can assume that the circuit C on input x queries the oracle R about its output z to check whether $R(z) = x$. Let $\{x_1, \ldots, x_t\} \subseteq \{0,1\}^n$ be a fixed set of size t and let $q(1), q(2), \ldots, q(s \cdot t)$ be the list in chronological order of the queries made by C on inputs $x_1, \ldots, x_t$ in this order. We can assume without loss of generality that C makes exactly s queries on each input and we can also assume that the queries are all distinct (if C actually repeats a question then we modify it so that each duplicate question is replaced with, say, the smallest lexicographically question that has not yet been posed). With these assumptions, the probability that C^R inverts $x_1, \ldots, x_t$ is equal to the probability that there exist $i_1 \in [1, s \cdot t], i_2 \in [1, s \cdot t], \ldots, i_t \in [1, s \cdot t]$, such that $q(i_1), \ldots, q(i_t)$ are mapped by the permutation R onto, respectively, $x_1, \ldots, x_t$. Let us fix distinct indices $i_1 \in [1, s \cdot t]$, $i_2 \in [1, s \cdot t], \ldots, i_t \in [1, s \cdot t]$. It holds that

$$\begin{aligned}\mathrm{Prob}_R(q(i_1), \ldots, q(i_t) &\text{ are mapped, respectively, into } x_1, \ldots, x_t) \\ &\leq \frac{1}{N(N-1)\ldots(N-t+1)},\end{aligned}$$

where $N = 2^n$. We sketch a proof of a slightly stronger claim: For every sequence $1 \leq j_1 < j_2 < \ldots < j_k \leq t \cdot s$, and for every k-tuplet $x_1, \ldots, x_k$, with elements in the tuplet being distinct, $\mathrm{Prob}_R(q(j_1), \ldots, q(j_k)$ are mapped, respectively, into $x_1, \ldots, x_k)$ is at most $1/[N(N-1)\ldots(N-k+1)]$. The proof is by induction on j_k. If $j_k = 1$, then $k = 1$, and clearly, $\mathrm{Prob}(q(j_1)$ is mapped into $x_1) = 1/N$. For the induction step, to keep the notation simple, we present only a concrete particular case, which however illustrates the general argument. Let us thus assume that the assertion holds for $j_k = 3$ and we want to prove it for $j_k = 4$. In our concrete example, we estimate the probability that $q(2)$ is mapped by R into x_2 and that $q(4)$ is mapped by R into x_4. We denote the last event by $q(2) \to x_2, q(4) \to x_4$ (and use the analogue notation for similar events). Then

$$\begin{aligned}&\mathrm{Prob}(q(2) \to x_2, q(4) \to x_4) \\ &\quad = \sum_{a_1, a_3} \mathrm{Prob}(q(1) \to a_1, q(2) \to x_2, q(3) \to a_3, q(4) \to x_4),\end{aligned}$$

where the sum is taken over all strings $a_1, a_3 \in \Sigma^n$, with $a_1 \neq a_3$ and with a_1 and a_3 different from x_2 and x_4. Next,

$$\begin{aligned}&\sum_{a_1, a_3} \mathrm{Prob}(q(1) \to a_1, q(2) \to x_2, q(3) \to a_3, q(4) \to x_4) \\ &\quad = \sum_{a_1, a_3} \mathrm{Prob}(q(1) \to a_1, q(2) \to x_2, q(3) \to a_3) \\ &\qquad \times \mathrm{Prob}(q(4) \to x_4 \mid q(1) \to a_1, q(2) \to x_2, q(3) \to a_3).\end{aligned}$$

By the induction hypothesis,

$$\mathrm{Prob}(q(1) \to a_1, q(2) \to x_2, q(3) \to a_3) \leq \frac{1}{N(N-1)(N-2)}.$$

The value of $\mathrm{Prob}(q(4) \to x_4 \mid q(1) \to a_1, q(2) \to x_2, q(3) \to a_3)$ is either $1/(N-3)$ in case $q(4)$ is different from $q(1), q(2)$ and $q(3)$, or it is 0, otherwise. Therefore the above

probability is at most

$$\begin{aligned}\sum_{a_1,a_3} \frac{1}{N(N-1)(N-2)} \cdot \frac{1}{(N-3)} &= (N-2)(N-3) \cdot \frac{1}{N(N-1)(N-2)(N-3)} \\ &= \frac{1}{N(N-1)}.\end{aligned}$$

There are $(s \cdot t)_t$ tuples $(i_1, \ldots, i_t)$ as above, and, therefore,

$$\begin{aligned}\text{Prob}(C^R \text{ inverts } x_1, \ldots, x_t) &\leq \frac{(s \cdot t)_t}{N(N-1)\ldots(N-t+1)} \\ &= \frac{1}{t!} \cdot \frac{(s \cdot t)_t}{\binom{N}{t}}.\end{aligned}$$

Therefore the expected number of T-subsets that are inverted is at most $\binom{N}{t} \cdot \frac{1}{t!} \cdot \frac{(s \cdot t)_t}{\binom{N}{t}} = \frac{(s \cdot t)_t}{t!}$. Let $u = 2est$. Then,

$$\begin{aligned}&\text{Prob}(\|\{x \mid C^R(R(x)) \in R^{-1}(R(x))\}\| \geq u) \\ &\qquad \leq \text{Prob}(C^R \text{ inverts some } u\text{-subset of } \{0,1\}^n) \\ &\qquad \leq \text{Prob}(C^R \text{ inverts all } t\text{-subsets of some } u\text{-subset of } \{0,1\}^n) \\ &\qquad \leq \text{Prob}(\text{there are } \tbinom{u}{t} \ t\text{-subsets of } \{0,1\}^n \text{ that are inverted}) \\ &\qquad \leq \frac{(s \cdot t)_t / t!}{\binom{u}{t}} \qquad\qquad \text{(by Markov's Inequality)} \\ &\qquad \leq \frac{(st)^t}{\left(\frac{t}{e}\right)^t \cdot \left(\frac{u}{t}\right)^t} = \left(\frac{est}{u}\right)^t = 2^{-t}.\end{aligned}$$