ERRATA AND COMMENTS ON "QUANTUM COMPUTATION AND QUANTUM INFORMATION" AMS GSM 243

J. M. LANDSBERG

Errata begin with (E)

(1) p24 Motivated by the DFT, one could replace 3) on the wish list by asking to allow complex numbers and get the same effect.

(2) (E) p36 display in middle of page is missing $\frac{1}{\sqrt{2}}$.

(3) (E) p45 L5 $\oplus$ should be $\underline{\oplus}$

(4) p48 Prop. 3.3.4: the $O(\log(a)^3)$ is because there are $O(\log(a))$ steps, each of cost $O(\log(a)^2)$.

(5) p54 L-6 $b^{2j_0\ell}$ should be $b^{2^{j_0}\ell}$

(6) p57 Def. 3.5.3: to clarify: $\max_{|\xi|_A=1} |X|\xi\rangle|_B$

(7) p63: §3.6.3 This section follows Chap. 10 of [1].

(8) p60 (E) The argument that $s_1 = s_2$ happens with probability at most $\frac{1}{2}$ is muddled. Here is a cleaner argument (thanks to Chun-Hung Liu):

By the CRT we associate to $a \in (\mathbb{Z}/N\mathbb{Z})^*$ $(a_1, a_2) \in (\mathbb{Z}/p_1\mathbb{Z})^* \times (\mathbb{Z}/p_2\mathbb{Z})^*$ with r_j order of a_j in $(\mathbb{Z}/p_j\mathbb{Z})^*$, and $r_j = 2^{s_j} r'_j$ with r'_j odd.

We want to show the probability that $s_1 = s_2$ is at most $\frac{1}{2}$. Again by the CRT, each a_j is chosen uniformly from $(\mathbb{Z}/p_j\mathbb{Z})^*$ and the choices are independent. So it suffices to show that for any fixed b, the probability that $s_2 = b$ is at most $\frac{1}{2}$.

The choice of a_2 is equivalent to choosing an integer x_2 between 1 and $p_2 - 1$ (the order of $(\mathbb{Z}/p_2\mathbb{Z})^*$) uniformly at random because for each $a_2 \in (\mathbb{Z}/p_2\mathbb{Z})^*$ there exists x_2 such that $a_2 = g^{x_2}$ where g is the generator of $(\mathbb{Z}/p_2\mathbb{Z})^*$.

The order of a_2 is $\frac{p_2-1}{gcd(x_2,p_2-1)}$. Let t_2 be the largest integer such that 2^{t_2} divides x_2 and let s be the largest integer such that 2^s divides $p_2 - 1$. Then $s_2 = s - t_2$. So for any fixed b, the probability that $s_2 = b$ equals the probability that $t_2 = s - b$.

If $b = 0$, then for each x_2 with $s_2 = 0 = b$, $t_2 = s \geq 1$ so x_2 is even and between 1 and $p_2 - 1$, which occurs at most half the time. Similarly if $b > 0$, for each x_2 with $s_2 = b$, $t_2 < s$ so $2x_2$ will be such that the equality fails, so this can occur at most half the time as well.

(9) p64 (E) The proof of Prop. 3.6.15 is incorrect. Here is a correct proof:

First a preliminary result:

Proposition 0.1. *Write* $\frac{p}{q} = [\alpha_1, \dots, \alpha_N] = [\alpha_1, \dots, \alpha_{k-1}, \alpha'_k]$ *where* $\alpha'_k = [\alpha_k, \dots, \alpha_N]$ *is rational. Then* $\alpha_k = \lfloor \alpha'_k \rfloor$ *except if* $k = N - 1$ *and* $\alpha_N = 1$, *in which case* $\alpha_{N-1} = \lfloor \alpha'_N \rfloor - 1$.

Proof. Use induction. When $k = 1$, we indeed have $\alpha_1 = \lfloor \frac{p}{q} \rfloor$. Now say $k > 1$. $\alpha'_k = \alpha_k + \frac{1}{\alpha'_{k+1}}$ and if $k+1 \neq N$ or $\alpha_N > 1$, then $\alpha'_{k+1} > 1$, so $\alpha_k < \alpha'_k < \alpha_k + 1$. Thus $\alpha_k = \lfloor \alpha'_k \rfloor$. □

Proof of 3.6.15. Write $\frac{a}{b} = [\alpha_1, \dots, \alpha_n] = [\beta_1, \dots, \beta_m]$ with $\alpha_j, \beta_j \geq 1$ for all $j > 1$, and $\alpha_n, \beta_m > 1$. To show: $m = n$ and $\alpha_k = \beta_k$ for all k. Proof by induction. Again the case $k = 1$ is ok. Say it is true for all $j < k$. Write $\frac{p}{q} = [\alpha_1, \dots, \alpha_{k-1}, \alpha'_k] = [\alpha_1, \dots, \alpha_{k-1}, \beta'_k]$. Then

$$\frac{p_k}{q_k} = \frac{\alpha'_k p_{k-1} + p_{k-2}}{\alpha'_k q_{k-1} + q_{k-2}} = \frac{\beta'_k p_{k-1} + p_{k-2}}{\beta'_k q_{k-1} + q_{k-2}}$$

i.e., $(\alpha'_k - \beta'_k)(p_{k-1}q_{k-2} - p_{k-2}q_{k-1}) = 0$, so by Cor. 3.6.12, $\alpha'_k = \beta'_k$ and if $k \neq N-1$ or $\alpha_N > 1$, by the proposition above $\alpha_k = \beta_k$. The rest of the proof is as before. □

(10) (E) p190 3.3.3 α_{n+2} should be α_{n+3}.

References

1. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles. MR 2445243

Department of Mathematics, Texas A&M University, College Station, TX 77843-3368, USA

Email address, J.M. Landsberg: jml@math.tamu.edu