Errata list for "Quantum Computation and Quantum Information"

Michael A. Nielsen and Isaac L. Chuang

October 7, 2004

Thanks to all the people who've contributed to this errata list: Scott Aaronson, Marcus Curty Alonso, Andris Ambainis, Dave Bacon, Mahesh Bandi, Charles Bennett, Mike Brown, Todd Brun, Mark Byrd, Jay Cheng, Andrew Childs, Richard Cleve, Mauro D'Ariano, Jennifer Dodd, Andrew Duggins, Michael Gagen, Ian Glendinning, Ben Gold, Jeroen van de Graaf, Bob Griffiths, Michael Hall, Charles Hill, Gert Ingold, Lawrence Ioannou, Matthew Paul Johnson, Alexei Kaltchenko, Phil Kaye, Yeong Cherng Liang, Naile Liu, Tom Luu, Mark Madden, Ryutaroh Matsumoto, David Meyer, John Obrecht, Ivan Oliveira, Christina Pencarski, Damian Pope, Terry Rudolph, Andy Shiekh, Peter Shor, Alessandro de Sousa Villar, Damonn Sypher, Rob Thew, Julian Ting, Lieven Vandersypen, Xiangbin Wang, and Qianchuan Zhao.

Printing History

The book is now in its fifth printing. Note that the second, fourth and fifth printings contain corrections based on the errata below. The third printing does not contain any corrections beyond those in the second printing.

First, Second, Third, Fourth & Fifth Printing (July, 2002)

pp 4 On page 4, in the first full sentence on the page, there is a missing comma after "qubits".

pp 6 In the errata for the First through Fourth printings there is an error related to page 6, and the Solovay-Strassen test. Namely, "no deterministic test" should be "no efficient deterministic test".

pp 19 The caption for Figure 1.5 should mention that $\overline{x}$ is shorthand for the logical negation of x.

pp 90 Just before Exercise 2.59, "The following two exercises [...]" should be "The following three exercises [...]".

pp 95 Immediately after Exercise 2.67, "Next, suppose we perform ..." should be replaced by "After letting U act on $|\psi\rangle|0\rangle$, suppose we perform ....

pp 95 On the left-hand side of Eq. (2.130), in the denominator $\langle\psi|$ should be $\langle 0|\langle\psi|$, and $|\psi\rangle$ should be $|\psi\rangle|0\rangle$.

pp 141 In Exercise 3.16, $2^n/\log n$ should be $2^n/n$.

pp 144 In Exercise 3.19, the time to solve REACHABILITY ought to be $O(n^2)$, and the time to decide whether a graph is connected $O(n^3)$.

pp 150 In the statement of the graph isomorphism problem, at the top of the page, the final G in the statement of the problem ought to be G'.

Sec 3.2.5 An important lemma is missing from the section. We explain in this section how, given a classical circuit to compute a function $f(x)$ it is possible to produce a reversible circuit using comparably many reversible gates to compute the transformation $(x, y) \rightarrow (x, y \oplus f(x))$. (The proof is given explicitly for functions having a single bit, zero or one, as their output, but obviously holds also for functions with multi-bit outputs, with $\oplus$ denoting bitwise modulo two addition in that case.) The missing lemma is that if $f(x)$ and $f^{-1}(x)$ are permutations which *both* have polynomial-size classical circuits, possibly not reversible, then there is a polynomial size reversible circuit to compute $x \rightarrow f(x)$, with no ancilla bits. The proof is to compute $(x, 0) \rightarrow (x, f(x)) \rightarrow (x \oplus f^{-1}(f(x)), f(x)) = (0, f(x))$, using the already-introduced techniques of reversible computation. This result is implicitly used, for example, in the chapter on Shor's algorithm.

pp 195-196 The argument leading to Equation (4.81) needs some modification, in the light of the earlier correction to Exercise 4.11, on page 176. We sketch the modification here. The key is that according to the modified exercise, an arbitrary unitary U can be written as a finite product of rotations about the $\hat{n}$ and $\hat{m}$ axes, up to an unimportant global phase. In particular, for fixed $\hat{n}$ and $\hat{m}$ the number of rotations required is a constant, c, independent of U. Modifying Equation (4.80) and Equation (4.81) appropriately we see that the error in the approximation is $c\epsilon/2$. We could also have modified the choice of n, earlier, so that the right-hand side of Equation (4.76) becomes $2\epsilon/3c$, in which case the bound on the right-hand side of (4.79) would have become $c\epsilon/2$ and that on the right-hand side of (4.81) would have remained ϵ.

pp 177 In Equations (4.20) and (4.22) the minus sign on the right-hand side should be a plus.

pp 203 Theorem 5.3 should be amended so that the lower bound in Eq. (5.60) is $1 - 1/2^{m-1}$. See the discussion below for page 634. Note that, so far as we can see, this error does not propagate to later discussions of the factoring algorithm. (Notifications of places where it does propagate would be welcome!)

pp 207 The reasoning at the end of the proof, after Eq. (4.100), is incorrect. In fact, a conceptually much simpler (and correct) argument may substitue. From Eq. (4.100) we see that $e^{iAt/n}e^{iBt/n} = e^{i(A+B)t/n} + O(1/n^2)$. Raising this to the nth power gives $\left(e^{iAt/n}e^{iBt/n}\right)^n = e^{i(A+B)t} + O(1/n)$, from which the result follows. Note that to understand how the error term scales when raised to a power, we must use an inequality like Eq. (4.69), in Box 4.1, on page 195.

pp 208 In "**Inputs**", the label "(3)" is repeated. The second one should be "(4)".

pp 234 In the exercise on factoring 91, the final gcd should be $\gcd(64-1, 91)$, not $\gcd(64-1, 19)$.

pp 238 In Equation (5.69) the square root should be removed from over N/r.

pp 285 In Box 7.2, just after Eq. (7.8) there is an integral missing a dx.

pp 285 In the third last line of Box 7.2, $\hbar(n+1/2)|n\rangle$ should be $\hbar\omega(n+1/2)|n\rangle$.

pp 286 Just after Equation (7.15), "$t = \pi/\hbar\omega$" should be "$t = \pi/\omega$"..

pp 298 After Equation (7.56), a and $a^\dagger$ should be described as annihilation and creation operators, not creation and annihilation operators.

pp 301 In the third-last line of the first paragraph of Box 7.6, H should be H_A.

pp 326 In the second line of the "Single spin dynamics" section there is a missing vector notation on "$B = B_0\hat{z} + \ldots$".

pp 373 On the first and second line, the sum "$E_i = \sum_{ij} u_{ij}F_j$" should only be over j, not i and j.

pp 392 After Eq. (8.168) there are two places where λ should be $\vec{\lambda}$.

pp 411 In Equation (9.73), the $A^\dagger$ should be A^T. Equation (9.69) on the same page needs to be modified accordingly, with $V_R^\dagger U_R$ inside the trace becoming $V_R^T U_R^*$, and similarly U on the line immediately below needs to become $U \equiv V_Q V_R^T U_R^* U_Q^\dagger$.

450 On the third line prior to Equation (10.66), "$|x+y+e\rangle|H_1e_1\rangle$" should be "$|x+y+e_1\rangle|H_1e_1\rangle$".

pp 464 We state that measurement of observables in the Pauli group may be simulated using $O(n^2)$ operations, provided one is using the stabilizer formalism to describe the quantum state of the system. This is true, but not obvious. The discussion in the book makes clear how the simulation may be performed in $O(n^3)$ time. Scott Aaronson (private communication) has shown how this may be improved to $O(n^2)$ time.

pp 481 Just before Equation (10.114), "Note that we have" should be replaced by "Choosing the smallest k satisfying (10.113), so that the inequality in (10.113) is close to being saturated, and rearranging (10.113), we have:" The equation (10.114) should then be changed so that the first equality sign is replaced by an $\approx$ sign.

pp 487 Exercise 10.66 has an error. The relation $TX = \exp(-i\pi/4)SX$ should read $TXT^\dagger = \exp(-i\pi/4)SX$.

pp 521 In Equation (11.104) there is a ρ_{AB} that should be ρ^{AB}.

pp 544 Just after Equation (12.49) there is a $\rho^{\otimes}$ that should be $\rho^{\otimes n}$. In the couple of lines following this, dedicated parentheses watchers will find two missing right parentheses.

pp 629 In Equation (A.4.12) and in the line immediately following, "37" should be "43".

pp 634 In the statement of Theorem A4.13, the probability in Eq. (A4.32) should be bounded below by $1 - 1/2^{m-1}$, not $1 - 1/2^m$. The proof of the theorem also needs some modification, which we sketch here. The proof as written shows that all the d_j must take the same value in order to have r odd or $x^{r/2} = -1(\text{mod}N)$. This part of the proof is correct. The error is to assume that this implies, based on Lemma A4.12, that the probability that r is odd or $x^{r/2} = -1(\text{mod}N)$ is at most $1/2^m$. In fact, there is no constraint on d_1 implied by Lemma A4.12, it is only $d_2, \ldots, d_m$ that are constrained to be equal to d_1, each contributing a factor $1/2$ to the decrease in probability, by Lemma A4.12. As a result, Eq. (A4.33) should also be amended so the right-hand side is $1/2^{m-1}$.

pp 638 In Equation (A4.55), $2 - 1 > 1$ should be $2 - 1 \geq 1$.

pp 661 In the Bilbiography entry for [Sho96], Shor's paper on fault-tolerant quantum computing, the symposium name "Fundamentals of Computer Science" should be "Foundations of Computer Science".

pp 663 In the Bibliography entry for [VR89] the correct journal informamtion is *Phys. Rev. A*, 40 (5): 2847–2849, 1989.

First, Second, Third & Fourth Printing (October, 2001)

pp 2 One the first line of Section 1.1.1, "a unheralded" should be "an unheralded".

pp 4 On line 2, "qubits" should be "quantum bits (or *qubits*)".

pp 6 The sentence beginning "Of especial interest at the time the Solovay-Strassen..." is somehwat ambiguous. It should be replaced by: "The Solovay-Strassen test was of especial significance at the time it was proposed as no deterministic test for primality was then known, nor is one known at the time of this writing."

pp 12 In the first line of Section 1.1.2, "some at the history" should read "some of the history".

pp 19 The geometric description of the Hadamard gate is incorrect. To correct the description, note that a Hadamard gate corresponds to a rotation of the Bloch sphere by 90 degrees about the $\hat{y}$ axis, followed by a 180 degree rotation about the $\hat{x}$ axis. Equivalently, it can be described by a 180 degree rotation about the axis $(\hat{x}+\hat{z})/\sqrt{2}$.

pp 61 On the second line of the second paragraph, "but rather the rather" should be "but rather the".

pp 88 Four lines below Eq(2.115), the formula in the text should read $\Delta(M) = \sqrt{\langle M^2 \rangle - \langle M \rangle^2}$.

pp 105 In fixing Exercise 2.73 for the fourth printing, we inadvertently took out the definition of the support for a Hermitian operator. The exercise should be amended to include this definition: "The *support* of a Hermitian operator A is the vector space spanned by the eigenvectors of A with non-zero eigenvalues."

pp 169 Fourth line from top: 2^{17} should be 2^{13}.

pp 205 The first differential in Eq. (4.88) should be with respect to time t, not to x.

pp 218 Equation (5.9) should have a base of e instead of 2 for the exponential multiplying $|1\rangle$.

pp 254 Line 3 of the quantum search algorithm has a superscript $\otimes R$ which should be just R, denoting application of the operator R times.

pp 276 The [Zal98] should instead refer to [Zal99], C. Zalka. Grover's quantum searching algorithm is optimal. Physical review A, 60:2746-2751, 1999.

pp 321 "basic" is misspelled in the caption of Fig 7.12

pp 323 End of second paragraph: "between" is misspelled.

pp 330-331 In (7.144), $T_2/2$ should be replaced by T_2. And at the end of the first paragraph on page 331, the exponent is missing a minus sign, and should read $M = M_0 e^{-k\tau/T_2}$.

pp 363 In (8.27), P_0 should be replaced by E_0 and P_1 by E_1.

pp 382 In the last line of Exercise 8.25 k_{rmB} should read $k_{\rm B}$.

pp 386 In Exercise 8.30, T_2 should be replaced by $2T_2$, so that it reads as follows:

> **Exercise 8.30: ($T_2 \leq T_1/2$)** The T_2 phase coherence relaxation rate is just the exponential decay rate of the off-diagonal elements in the qubit density matrix, while T_1 is the decay rate of the diagonal elements (see Equation (7.144)). Amplitude damping has *both* nonzero T_1 and T_2 rates; show that for amplitude damping $T_2 = T_1/2$. Also show that if amplitude and phase damping are *both* applied then $T_2 \leq T_1/2$.

pp 412 In Equation (9.75) and subsequently an unexplained "U" suddenly appears in the proof. This U arises from the polar decomposition, $\sqrt{\rho^{1/2}\sigma\rho^{1/2}} = \sqrt{\rho}\sqrt{\sigma}U$.

pp 418 In Exercise 9.22 we need to add the assumption that the metric be unitarily invariant, that is, $d(U\rho U^\dagger, U\sigma U^\dagger) = d(\rho, \sigma)$ for all density matrices ρ and σ and unitary matrices U.

pp 423 An unfortunate transposition occurred during final typesetting of the book: the square root appearing on the right-hand side of (9.144) should be removed, and placed instead over the quantity on the right-hand side of (9.145).

pp 423 In the statement of Problem 9.2 "Show that there is a set [...]" should be replaced by "Show that for each ρ there is a set [...]".

pp 424 The "History and further reading" section should include a citation to C. A. Fuchs and J. van de Graaf, "Cryptographic distinguishability measures for quantum-mechanical states", IEEE Transactions on Information Theory **45** (4), 1216-1227 (1999). This paper is the origin of the inequality (9.110), and is also a good overview of distance measures for quantum information, especially in the context of quantum cryptography.

pp 449 Eq.(10.63) should have $H(2t/n)$ instead of $H(t/n)$.

pp 532 In the second-last line of Box 12.1, "mean" should be "meant".

pp 600 In equation (12.206) the two instances of w on the r.h.s. should be w_1 and w_2, respectively. There should also be a sum over z.

pp 654 The citation for [EJ96] states that the article in question begins on page 1, when it actually begins on page 733.

First & Second Printing (January, 2001)

pp 20 Equation (1.17) contains an extra comma between the second and third matrices on the right hand side.

pp 36 In step 3 of the Deutsch-Jozsa algorithm, a normalization factor of $1/\sqrt{2^n}$ is missing.

pp 36 In step 4 of the Deutsch-Jozsa algorithm, the normalization factor in the denominator should be 2^n rather than $\sqrt{2^n}$.

pp 48 On line 8, "procotols" should be "protocols".

pp 88 In Equation (2.114), $\Delta(M)$ should be $[\Delta(M)]^2$.

pp 105 Michael Hall has pointed out that Exercise (2.73) needs to be replaced, as follows:

Exercise 2.73: Let ρ be a density operator. A *minimal ensemble* for ρ is an ensemble $\{p_i, |\psi_i\rangle\}$ containing a number of elements equal to the rank of ρ. Let $|\psi\rangle$ be any state in the support of ρ. Show that there is a minimal ensemble for ρ that contains $|\psi\rangle$, and moreover that in any such ensemble $|\psi\rangle$ must appear with probability

$$p_i = \frac{1}{\langle\psi_i|\rho^{-1}|\psi_i\rangle},$$

where ρ^{-1} is defined to be the inverse of ρ, when ρ is considered as an operator acting only on the support of ρ. (This definition removes the problem that ρ may not have an inverse.)

pp 106 Equation (2.189) should read:

$$\frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \tag{2.189}$$

pp 214-215 The "History and further reading" section should acknowledge that the suggestion (made in Section 4.6) that it may be possible to use non-computational basis starting states to obtain computational power beyond the quantum circuits model was made by Daniel Gottesman and Michael Nielsen (private communication).

pp 225 In the line beginning **Inputs:**, "wich" should be "which".

pp 267 On the first line of the last paragraph "the principle use" should be "the principal use".

pp 280 Just after Equation(7.1) it is stated that $E_n = n^2\pi^2 m/2L^2$. The correct expression is $E_n = n^2\pi^2/2mL^2$.

pp 291-292 At the bottom of p291, G is defined incorrectly; it should be $G = ab^\dagger - a^\dagger b$ (to be consistent with (7.24)). This change introduces a minuns sign which propagates through (7.33), giving the new text and equations:

> Since it follows from $[a, a^\dagger] = 1$ and $[b, b^\dagger] = 1$ that $[G, a] = b$ and $[G, b] = -a$, for $G \equiv ab^\dagger - a^\dagger b$, we obtain for the expansion of $BaB^\dagger$ the series coefficients $C_0 = a$, $C_1 = [G, a] = b$, $C_2 = [G, C_1] = -a$, $C_3 = [G, C_2] = -[G, C_0] = -b$, which in general are
>
> $$C_{n \text{ even}} = i^n a \tag{7.28}$$
> $$C_{n \text{ odd}} = -i^{n+1} b\,. \tag{7.29}$$
>
> From this, our desired result follows straightforwardly:
>
> $$BaB^\dagger = e^{\theta G} a e^{-\theta G} \tag{7.30}$$

$$
\begin{aligned}
&= \sum_{n=0}^{\infty} \frac{\theta^n}{n!} C_n && (7.31)\\
&= \sum_{n \text{ even}} \frac{(i\theta)^n}{n!} a - i \sum_{n \text{ odd}} \frac{(i\theta)^n}{n!} b && (7.32)\\
&= a\cos\theta + b\sin\theta\,. && (7.33)
\end{aligned}
$$

pp 303 In Equation (7.78), sin and cos should be interchanged.

pp 309 The static potential on the third last line of the page should read "$\Phi_{\rm dc} = \kappa U_0 \left[z^2 - (x^2+y^2)/2\right]$". That is, the factor 2 is now inside the square brackets.

pp 316 In Equation (7.110) the term $(\omega - \omega_0)^2$ appearing in the argument of sin should not be squared.

pp 320 The S_+ and S_- operators in (7.124) are not the same as those appearing in (7.122) and earlier; they should appear as S'_+ and S'_- and denote transitions between $|20\rangle$ and $|11\rangle$. This text should appear after (7.124):

> where S'_+ and S'_- denote transitions between $|20\rangle$ and $|11\rangle$, and we assume that higher order motional states are unoccupied.

pp 370 Equation (8.61) should have a sum over the i index on the right hand side.

pp 380 The right hand side of Equation (8.107) should read "$E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger$".

pp 407 On the first line there is a right parenthesis missing from $\mathrm{tr}(\mathcal{E}(Q))$.

pp 417 Equation (9.118) should have $\sqrt{p}$ on the right hand side, not $\sqrt{1-p}$.

pp 418 Equation (9.124) is missing a p: it should read $\min_{|\psi\rangle} \sqrt{(1-p) + p\langle\psi|Y|\psi\rangle^2}$.

pp 455 Just before Exercise 10.31, "To establish condition (b), that $I \notin S$" should be "To establish condition (b), that $-I \notin S$".

pp 468 In Figure 10.11 the eighth generator of the stabilizer for the Shor code should be $IIIXXXXXX$, not $XIIIXXXXX$.

pp 573 Six lines after Equation (12.154), "$\cos\theta|11\rangle + \sin\theta|00\rangle$" should be "$\cos\theta|00\rangle + \sin\theta|11\rangle$".

pp 588 Item 7 in Figure 12.13, "... will to serve as a check..." should omit the "to".

pp 650 Reference [BFC+96] should have page 2818, not 2828.

pp 652 Entry [BS98] should read *IEEE Trans. Inf. Theory* instead of *itit*.

pp 667 Index entry for "element of reality" should point to page 112, not page 111.

pp 670 There should be an index entry "majorization, 573".

First Printing (September, 2000)

Cover blurb "quatum teleportation" should be "quantum teleportation".

pp xvii (line 21) "Apendix 2" should be "Appendix 2".

pp 112 (9th line from bottom) "co-authored with Nathan Rosen and Boris Podolsky" should be "co-authored with Boris Podolsky and Nathan Rosen".

pp 121 (20 lines from bottom) "[...] instinctively know what problems, what techniques, and most importantly what problems are of greatest interest to a computer scientist." should be "[...] instinctively know what techniques and, more importantly, what problems are of greatest interest to a computer scientist."

pp 176 Exercise 4.11 should be replaced by

> Suppose $\hat{m}$ and $\hat{n}$ are non-parallel real unit vectors in three dimensions. Show that an arbitrary single qubit unitary U may be written as
>
> $$U = e^{i\alpha} R_{\hat{n}}(\beta_1) R_{\hat{m}}(\gamma_1) R_{\hat{n}}(\beta_2) R_{\hat{m}}(\gamma_2) \ldots, \tag{4.13}$$
>
> for appropriate choices of α and β_k, γ_k.

pp 168 (15th line from bottom) The first reference to Bennett's work on Maxwell's Demon should be amended. It currently is to the paper [BBBW82], which is actually about quantum cryptography. The correct reference is:

[Ben82a] C. H. Bennett, "The thermodynamics of computation – A review", Int. J. Theor. Phys. **21**, 905–940 (1982).

pp 202 In equation (4.87), $U_{p(n)-2}$ should be $U_{p(n)-1}$.

pp 202 (5th last line of section 4.5.5) The text "[...] this means that quantum computers do not violate the Church-Turing thesis that any algorithmic process can be simulated efficiently using a Turing machine" should not include the word "efficiently".

pp 325 In the second paragraph "11.8 tesla" should read "11.7 Tesla".

pp 424 (5th line from the top) The term "monotonicity of the trace distance" should be replaced by "contractivity of the trace distance". Note that these two terms are often used interchangeably in quantum computation and quantum information, however in our presentation in the book we prefer the latter.

pp 521 Exercise 11.25 has a couple of typos in the first two sentences. They should read as follows:

"We obtained strong subadditivity as a consequence of the concavity of the conditional entropy, $S(A|B)$. Show that the concavity of the conditional entropy may be deduced from strong subadditivity."

pp 570 In Figure 12.9, there are missing boxes around ρ' and ρ''_m, at the top and bottom of the figure, respectively.

pp 621 In Equation (A3.7) the two σs on the left hand side should be $\vec{\sigma}$.

pp 622 In Equation (A3.16) there is a missing right parenthesis just before the plus sign on the right hand side of the equation.

pp 653 The reference [DiV95a] should have the arXive number removed, as it did not appear as a preprint at the archive.

pp 663 The reference [VR89] is incorrect. The given issue and page numbers are for a different article, "k-photon Jaynes-Cummings model with coherent atomic preparation: Squeezing and coherence," by W. Vogel and D.-G. Welsch. The correct citation is

K. Vogel and H. Risken, Phys. Rev. A **40**(5): 2847-2849, 1989.

This page last modified

$$Id : errata.tex, v1.472002/09/3001 : 59 : 14mnielsenExpmnielsen$$

.