Solutions to Nielsen and Chuang

Baptiste Claudon

I. INTRODUCTION AND OVERVIEW

A. Exercise 1.1 (Probabilistic classical algorithm)

Let B denote the event $\{f \text{ is balanced}\}$. Assume that $\mathbb{P}(B) = 1/2$. Then, for $0 \leq k \leq 2^{n-1}$,

$$\mathbb{P}('0' * k|B) = \prod_{j=0}^{k-1} \frac{2^{n-1} - j}{2^n - j}. \tag{1}$$

As a consequence:

$$\mathbb{P}(B|'0'*) = \frac{\mathbb{P}('0' * k|B)\mathbb{P}(B)}{\mathbb{P}('0' * k)} = \frac{1}{1 + \prod_{j=0}^{k-1} \frac{2^n - j}{2^{n-1} - j}}..$$

In particular, if $k > \ln(\ln(1/\epsilon))/\ln(2)$, then $P(B|'0' * k) < \epsilon$.

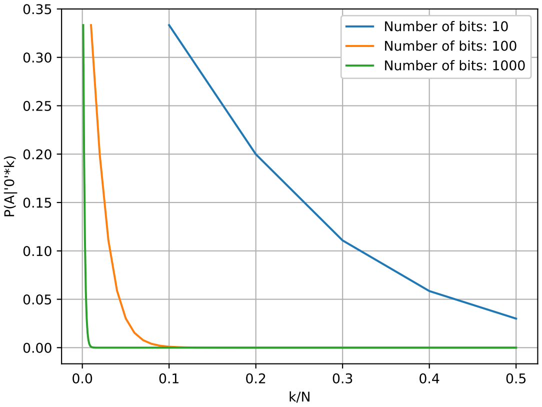


FIG. 1: Probability of f being balanced given the observation of k successive 0's.

II. INTRODUCTION TO QUANTUM MECHANICS

2.1 3 vectors in two-dimensional space. **2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11.** Trivial. **2.12** The algebraic multiplicity of the eigenvalue 1 is two. However, the geometric multiplicity is 1. **2.13, 2.14, 2.15, 2.16.** Trivial. **2.17** If A is normal, it is diagonalizable according to Theorem 2.1. Take λ one of its eigenvalues, $|v\rangle$ the corresponding eigenvector. $\lambda = (v, Av) = (A^\dagger v, v) = \lambda^* \in \mathbb{R}$. The converse is trivial. **2.18** U is normal hence diagonalizable. Then, $1 = (v, v) = (v, u^\dagger U v) = (Uv, Uv) = |\lambda|^2$. **2.19, 2.20 2.21** Again, $M = PMP + QMQ$. Each of these two terms is hermitian. **2.22, 2.23, 2.24, 2.25,..., 2.58** Trivial. **2.60** Characteristic polynomial is $\lambda \mapsto \lambda^2 - 1$. Also, $\mathbf{v} \cdot \sigma P_\pm = (-1)^{\mp 1} P_\pm$. **2.61** $p(+1) = (1 \pm v_3)/3$. The state post-measurement is:

$$\frac{1 + v_3}{2} |0\rangle + \frac{v_1 - iv_2}{2} |1\rangle .$$

Exercise 2.63 Simple corollary from the Polar Decomposition. **Exercise 2.64** For $1 \leq i \leq m$, $E_i = |\psi_i\rangle \langle\psi_i|$. Also, $E_{m+1} = 1 - \sum E_k$. **2.65, 2.66** Trivial. **2.67** Use the existence of the orthogonal complement and complete with the identity restricted to this orthogonal complement. **2.68, 2.69** Trivial. **2.71, 2.72** Trivial. **2.74, 2.75, 2.76** Trivial.

III. INTRODUCTION TO COMPUTER SCIENCE

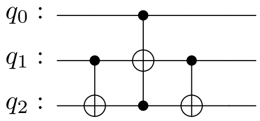
3.9, 3.10, 3.11 Trivial. **3.12** Take $n \geq 2^k$. $n^{\log(n)-k} \to \infty$ for any k. **3.13, 3.14** Trivial. **3.17** Trivial. **3.19** Grow the subgraph of vertices connected to one of the two elements. If it contains the other, done. To know if connected, do this with memory. The number of edges is $\mathcal{O}(n^2)$. **3.20** Since the graph is supposed to be connected, any Euler cycle would pass through a chosen vertex v. Let $e_1 ... e_n$ be the edges which are incident to v. Each edge is visited exactly once. Equivalently, we can separate them into two sets of equal size containing the incident edges and the outgoing edges. **3.21** Polynomial of polynomial is polynomial. **3.22** L is easier than L'. In other words, L' is at least as hard as L. Thus, L' is complete. **3.28** Repeating is efficient. **3.29, 3.30** Trivial. **3.31** A Fredkin can be made from three Toffolis.

IV. QUANTUM CIRCUITS

4.1, 4.2, 4.3 Trivial. **4.5** Trivial. **4.7** Trivial. **4.9** A single-qubit unitary must take $|0\rangle$ and $|1\rangle$ to some normalized states. These two states must be orthogonal in order for U to preserve the inner product. **4.13, 4.14, 4.15, 4.16, 4.17, 4.18** Trivial. **4.21** $|00\rangle|\psi\rangle \mapsto |00\rangle|\psi\rangle$, $|01\rangle|\psi\rangle \mapsto |01\rangle VV^\dagger|\psi\rangle$, $|10\rangle|\psi\rangle \mapsto |10\rangle V^\dagger V|\psi\rangle$ and $|11\rangle|\psi\rangle \mapsto |11\rangle V^2|\psi\rangle$. **4.22** $V = e^{i\alpha}AXBXC$. Figure 4.6 et Figure 4.8. $CC^\dagger = 1$, $A^\dagger = 1$ et deux fois 3 CNOTs deviennent 2 CNOTs. **4.23, 4.24** Trivial.

A. Exercise 4.25 - Fredkin gate construction

(1, 2)The Fredkin gate can be rewritten as:



(3) Use the construction and the fact that $V^4 = I$ and therefore $V^3 = V^\dagger$. (4) Using the circuit from exercise 4.26 yields, up to relative phases, a Fredkin gate with five two-qubit gates.

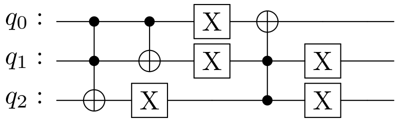
4.26 The overall operation is (with angles π/α):

$$|c_1, c_2, t\rangle \mapsto |c_1, c_2\rangle \otimes (R_y(-\pi/\alpha)X^{c_2}R_y(-\pi/\alpha)X^{c_1}R_y(\pi/\alpha)X^{c_2}R_y(\pi/\alpha))|t\rangle . \tag{2}$$

In particular, $|0,0,t\rangle \mapsto |0,0,t\rangle$ and $|0,1,t\rangle \mapsto |0,1,t\rangle$. If, for example, $4/\alpha = 1/2$ then up to a global phase $|1,0,t\rangle \mapsto |1,0\rangle \otimes Z|t\rangle$. Finally, use:

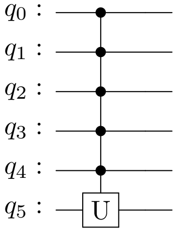
$$R_y(-\pi/\alpha)XR_y(-\pi/\alpha)XR_y(\pi/\alpha)XR_y(\pi/\alpha) = X^2R_y(\pi/\alpha)XR_y(\pi/\alpha) = X.$$

4.27 There are simple X gates but: does the job.

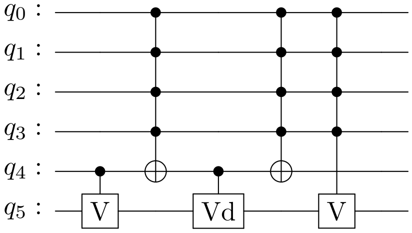


B. Exercise 4.28

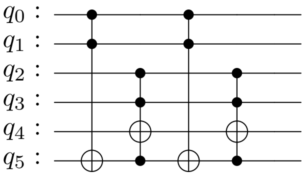
C. U is a single-qubit unitary



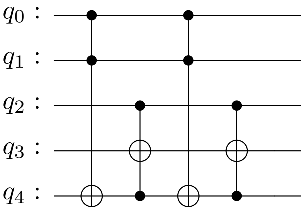
is equal to:



Using, the factorisation $V = e^{i\alpha}AXBXC$, the problem is reduced to writing $C^4(X)$ using Toffolis and $C^1(X)$. First, $C^4(X) =$



Therefore, the final task is to decompose a $C^3(X)$. The decomposition is the following. $C^3(X) =$



D. Why is it nos possible to use only $C^1(V)$ and $C^1(V^\dagger)$?

4.29 Use the same trick as in exercise 4.28 to express a n-control in terms of $(n-1)$-controls and liberate a borrowable qubit. **4.30** It is a corollary from exercise 4.29 because of the $U = e^{i\alpha}AXBXC$ factorisation of an arbitrary single-qubit gate. **4.31** Trivial. **4.32** First question follows from measurement definition. $\mathrm{tr}_2(\rho') = \mathrm{tr}_2(\rho P_0) + \mathrm{tr}_2(\rho P_1)) = \mathrm{tr}_2(\rho(P_0 + P_1)) = \mathrm{tr}_2(\rho)$. **4.34, 4.35** Trivial. **4.42** Trivial. **4.46, 4.47, 4.48, 4.49, 4.50, 4.51** Trivial.

V. THE QUANTUM FOURIER TRANSFORM AND ITS APPLICATIONS

5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 Trivial. **5.10** $5^2 = 4$, $5^3 = 20$, $5^4 = 16$, $5^5 = 17$ and $5^6 = 1$. **5.11** The subgroup generated by any element is of size r, and its size (r) must divide N. In particular, $r \leq N$. **5.12** $xy = xz$ implies $y = z$ so $\langle xz|U^\dagger U|xy\rangle = \delta_{xy}$. **5.15** Trivial. **5.16**

$$\int_x^{x+1} \frac{1}{y^2} = \frac{1}{x(x+1)} = \frac{x}{x^2(x+1)} \geq \frac{2}{3x^2}.$$

Then,

$$\sum_{q\in\mathbb{P}} \frac{1}{q^2} \leq \sum_{q\in\mathbb{P}} \frac{3}{2}\int_q^{q+1} \frac{1}{y^2} \leq \frac{3}{4}.$$

5.15, 5.20 Trivial.

VI. PROBLEM 5.3: KITAEV'S ALGORITHM

The output state is:

$$\frac{(1+e^{2\pi i\varphi})\left|0\right\rangle\left|u\right\rangle + (1-e^{2\pi i\varphi})}{\sqrt{2}},$$

hence one easily recovers the probability of measuring 0 to be $\cos^2(\pi\varphi)$. Write $\varphi = \sum_{k=0}^t \varphi_k 2^{-k}$. Then, $\cos^2(\pi 2^j\varphi) = \cos^2(\pi 2^j \sum_{k=j}^t \varphi_k 2^{k-j})$.

VII. PROBLEM 5.6: ADDITION BY FOURIER TRANSFORM

Let $|j\rangle$ be a computational basis state. Compute:

$$\begin{aligned} QFT^\dagger\left|j\right\rangle &= \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{-2\pi ijk/N}\left|k\right\rangle \\ \Sigma QFT^\dagger\left|j\right\rangle &= e^{2\pi ij/N} QFT^\dagger\left|j\right\rangle \\ QFT\Sigma QFT^\dagger\left|j\right\rangle &= e^{2\pi ij/N}\left|j\right\rangle. \end{aligned} \tag{3}$$

As a consequence:

$$\Sigma = QFT^\dagger \bigotimes_{k=0}^{n-1} \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i 2^{k-n}} \end{pmatrix} QFT. \tag{4}$$

VIII. QUANTUM SEARCH ALGORITHMS

6.1, 6.2, 6.3 Trivial. **6.4** Only change the number of repetitions. **6.5** Control the oracle on the state 0 for the added qubit. **6.6** There is a CZ in the middle of the $X^{\otimes 2}$ change of basis. The unimportant global phase is -1. **6.7** The circuit proceeds to $\left|y\right\rangle\left|0\right\rangle \to \left|y\right\rangle\left|f(y)\right\rangle \to \left|y\right\rangle e^{i\Delta t f(y)}\left|f(y)\right\rangle \to e^{i\Delta t f(y)}\left|y\right\rangle\left|0\right\rangle$. On the other hand, for any projector P (such as $\left|x\right\rangle\left\langle x\right|$ or $\left|\psi\right\rangle\left\langle\psi\right|$ for the next question):

$$e^{-i\Delta t P} = 1 + P(e^{-i\Delta t} - 1). \tag{5}$$

Thus, we can conclude. The second circuit proceeds to $\left|y\right\rangle\left|0\right\rangle \to \sum_x (-1)^{x\cdot y}\left|x\right\rangle\left|0\right\rangle \to \left|0\right\rangle\left|1\right\rangle + \sum_{x\neq 0}(-1)^{x\cdot y}\left|x\right\rangle\left|0\right\rangle \to e^{i\Delta t}\left|0\right\rangle\left|1\right\rangle + + \sum_{x\neq 0}(-1)^{x\cdot y}\left|x\right\rangle\left|0\right\rangle \to e^{i\Delta t}\left|0\right\rangle\left|0\right\rangle + + \sum_{x\neq 0}(-1)^{x\cdot y}\left|x\right\rangle\left|0\right\rangle \to (e^{i\Delta t} - 1)\left|\psi\right\rangle\left|0\right\rangle + \left|y\right\rangle\left|0\right\rangle$. **6.8** The error is of order $\frac{t}{\Delta t} \times \Delta t^r = \mathcal{O}(N^{1/2})\Delta t^{r-1}$. To make this error constant, we need $\Delta t = \mathcal{O}((N^{-1/2})^{\frac{1}{r-1}})$. There is a constant number of oracle calls per time step so the number of oracle calls is $\mathcal{O}(t/\Delta t) = \mathcal{O}(N^{1/2}/(N^{-1/2})^{\frac{1}{r-1}}) = \mathcal{O}(N^{1/2+\frac{1}{2(r-1)}}) = \mathcal{O}(N^{\frac{r}{2(r-1)}})$. **6.9** Exercise 4.15 (2).

IX. QUANTUM COMPUTERS: PHYSICAL REALIZATION

7.1, 7.2, 7.3, 7.4, 7.5 Trivial. **7.6** $a\left|\alpha\right\rangle = \alpha\left|\alpha\right\rangle$.

X. QUANTUM NOISE AND QUANTUM OPERATIONS

8.1, 8.2 Trivial. **8.3** $E_k = I_A \otimes \langle k|$, over all the basis vectors $\{|k\rangle\}$ for B. **8.4** $E_0 = \frac{1}{\sqrt{2}}\langle 0| \otimes I$ and $E_1 = \frac{1}{\sqrt{2}}\langle 1| \otimes X$. **8.5** $E_0 = \frac{1}{\sqrt{2}}|1\rangle \otimes (I - iX)$ and $E_1 = \frac{1}{\sqrt{2}}|0\rangle \otimes (I + iX)$. **8.6** Trivial. **8.10** Trivial.

XI. DISTANCE MEASURES FOR QUANTUM INFORMATION

9.1, 9.2, 9.3 Trivial. **9.5** For any subset S, $p(S) - q(S) = q(S^c) - p(S^c)$. Hence, the absolute value does not matter. **9.6** Trivial. **9.7** Take Q to be $\rho - \sigma$ with 0 cut-off on the eigenvalues. Similar for S. **9.8** Trivial. **9.9** In finite dimensions, the closed unit ball in which the states live is compact. Hence the result follows. **9.10** Assume there are two fixed points ρ and σ. By definition, $\mathcal{E}(\rho) = \rho$ and $\mathcal{E}(\sigma) = \sigma$. However, $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) < D(\rho, \sigma)$, a contradiction. **9.11** $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq pD(\rho_0, \rho_0) + (1-p)D(\mathcal{E}'(\rho), \mathcal{E}'(\sigma)) < D(\mathcal{E}'(\rho), \mathcal{E}'(\sigma)) \leq D(\rho, \sigma)$. **9.12** $\mathcal{E}(\rho) = \frac{I + (1-p)n\cdot\sigma}{2}$ so $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) = (1-p)D(\rho, \sigma)$. **9.13** $\rho = X$ for example. All ρ that commutes with X. **9.14** Trivial. **9.17, 9.18, 9.19, 9.20** Trivial. **9.23** Trivial.

XII. QUANTUM ERROR-CORRECTION

10.1 Trivial. **10.2** Use $I = P_+ + P_-$ and $X = P_+ - P_-$. **10.3, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9** Trivial. **10.12** $\mathcal{E}(|0\rangle\langle 0|) = (1 - 2p/3)|0\rangle\langle 0| + 2p/3|1\rangle\langle 1|$. **10.13** Compute for $|\psi\rangle = a|0\rangle + b|1\rangle$:

$$\langle\psi|\mathcal{E}(|\psi\rangle\langle\psi|)|\psi\rangle = |a|^2(1 + |b|^2\sqrt{1-\gamma}) + |b|^2(|a|^2\sqrt{1-\gamma} + |b|^2(1-\gamma)) \geq 1 - \gamma,$$

where the minimum is reached for $|\psi\rangle = |1\rangle$. **10.14** Trivial. **10.15** $(a+b)x_1 + bx_2 = ax_1 + b(x_1 + x_2)$. It maps $(0,0)$ to 0, $(0,1)$ to b, $(1,0)$ to $a+b$ and $(1,1)$ to a. **10.16** Trivial. **10.17**

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

10.18 Trivial. **10.19** Clearly, $\mathrm{Im}(G) \subseteq \mathrm{Ker}(H)$. So the code of G is contained in the code of H. Now, the range of H is at least of dimension $n-k$. Hence the kernel of H is at most of dimension k. By dimensionality analysis, we can conclude. **10.20** Take any non-zero vector in the code of weight strictly less than d. By hypothesis, $Hx \neq 0$. Therefore, the code distance is at least d. Since there exist d columns $h_{i_1}...h_{i_d}$ such that $\sum_{j=1}^{d} h_{i_j} = 0$, there exists a codeword with weight d. Hence, the code distance is d. **10.21** Assume H to be in standard form. The right-most $n-k$ columns are linearly independent. Hence, $d - 1 \leq n - k$. **10.22** Again, any two columns are different, hence linearly independent. The code distance is at least 3. Summing the first two columns yields the third column. Hence, by exercise 10.20, the code distance is 3. **10.24** Trivial. **10.26** Standard chain of multi-control gates. Use results from chapter 4 to decompose the $C^n(X)$ into $CNOT$s. **10.27** Instead of comparing the ancilla measurements with 0, compare it with u and v. Perform the recovery operations accordingly. **10.28** Transpose the matrix. Apply it to H. We get 0. **10.29** Trivial. **10.30** Assume that $\pm iI \in S$. Then, $(\pm iI)^2 = -I \in S$. A contradiction. **10.31** Trivial. **10.32** We have $|0 + C_2\rangle \propto \sum y \in C_2 |y\rangle$. Since $C_2 \subseteq C_1$, applying the generators from the first lines to each term $|x+y\rangle$ yields another term of the form $|x+y'\rangle$. By remembering the definition of $H(C_2)$, applying the generators from the last lines apply an even number of phases on each term. **10.33** Two Pauli elements commute if they non-trivially differ on an even number of positions. If X meets X, add 0, if X meets Y, add 1, if X meets 2, add 1 and so on... Hence, $r(g)\Lambda r(g')^T$ counts precisely that. **10.34** Trivial. **10.35** Write g as a finite product. By using that Pauli tensor products either commute or anti-commute, swap (with a phase) each pair of terms until two similar terms are grouped together. Their square is the identity. The final result cannot be $-I$ by hypothesis. Hence it is I. **10.36** Trivial. **10.37** $UY_1U^\dagger = -iUZ_1X_1U^\dagger = -iZ_1X_1X_2 = Y_1X_2$. **10.38** From these circuits, we can deduce the effect of conjugation by U of any two-qubit operators. **10.39** Trivial. **10.41** Trivial. **10.43, 10.44** Trivial. **10.46, 10.47, 10.48** Trivial. **10.49** X and Z type of errors anti-commute with at least one of the generators. **10.50** $t = 1, k = 1, n = 5$ so $2^1(1 + 5 \times 3) = 2^5$. **10.52** Trivial. **10.58, 10.59** Trivial.

XIII. ENTROPY AND INFORMATION

11.1 Trivial. **11.3, 11.4, 11.5** Trivial. **11.6** Using the inequality $\log(x) \leq (x-1)/\ln 2$,

$$\begin{aligned} H(X,Y,Z) + H(Y) - H(X,Y) - H(Y,Z) &= \sum_{x,y,z} p(x,y,z) \log\left(\frac{p(x,y)p(y,z)}{p(y)p(x,y,z)}\right) \\ &\leq \frac{1}{\ln 2}\sum_{x,y,z} p(x,y,z)\left(\frac{p(x,y)p(y,z)}{p(y)p(x,y,z)} - 1\right) \\ &= \frac{1}{\ln 2}(1-1) = 0. \end{aligned} \tag{6}$$

The equality is satisfied if:

$$\forall x, y, z : p(y)p(x,y,z) = p(x,y)p(y,z).$$

This is equivalent to $p(z|x,y) = p(x,y,z)/p(x,y) = p(x,y)p(y,z)/p(y)/p(x,y) = p(y,z)/p(y) = p(z|y)$. Moreover, if the equality is satisfied:

$$H(Z|X,Y) = X(X,Y,Z) - H(X,Y) = H(Z|Y)$$

and $Z \to Y \to X$ is a Markov chain. **11.7** $H(Y|X) = H(p(x,y)||q(x,y))$ where $q(x,y) \equiv p(y)$. The equality condition is the independence of X and Y. **11.8** On the one hand, $H(X,Y:Z) = H(X,Y) + H(Z) - H(X,Y,Z) = 2H(X) + H(Z) - H(X,Y,Z) = \log(2)$. On the other, $H(X:Z) = H(X) - H(X,Z) = 2\log 2 - \log 4 = 0$ and therefore the right-hand side is 0. **11.9** The left is $2H(X_1) = 2\log 2$ and the right is $\log 2$. **11.10** Assume that $X \to Y \to Z$ is a Markov chain. Then,

$$p(z|x,y) = \frac{p(x,y,z)}{p(x,y)} = \frac{p(x|y,z)p(y,z)}{p(x|y)p(y)} = \frac{p(y,z)}{p(y)} = p(z|y).$$

In words, $Z \to Y \to X$ is also a Markov chain. **11.11, 11.12** Trivial. **11.13** Using the joint entropy theorem with $\rho = \sum_i p_i |i\rangle\langle i|$ and $\rho_i = \sigma \forall i$:

$$S(\rho \times \sigma) = H(p_i) + \sum_i p_i S(\sigma) = S(\rho) + S(\sigma).$$

Without using this theorem, use the form of the eigenvalues of a tensor product. **11.14** If $|AB\rangle$ is not entangled, it is of the form $\rho \otimes \sigma$. Applying exercise 11.13 allows to conclude that $S(B|A) > 0$ implies entanglement between A and B. Since $|AB\rangle$ is assumed to be a pure state, $S(B|A) = -S(A)$. If we further ask for entanglement, system A must have a density operator with at least two strictly positive eigenvalues, and therefore $S(A) > 0$. **11.15** The entropy of the system afterwards is 0. Any non-zero entropy starting state provides a counter-example (I/2 for example). **11.17** Take AB to be in the state $(|00\rangle + |11\rangle)/\sqrt{2}$. Then, $S(AB) = 0 = 1 - 1 = S(B) - S(A)$. **11.18** If the ρ_i are the same, equality is clearly satisfied. Otherwise, ρ^{AB} must factorize into $\rho^A \otimes \rho^B$. Hence, the condition. **11.21** Take a diagonal density matrix. **11.23** Take $B_1 = B_2$. $f : \mathbb{R} \to \mathbb{R}, (x1, x2) \mapsto x_1 x_2$.

XIV. QUANTUM INFORMATION THEORY

12.1 Suppose we know the quantum circuits U and V such that $U|0\rangle = |\psi\rangle$ and $V|0\rangle = |\varphi\rangle$ (one-qubit gates so reasonable). Then, apply $U^\dagger$ on the data, a $C^0 - U$ with control the data qubit and target the target qubit. A $C - V$ controlled on the data on the target qubit and finally U on the target. **12.2** Trivial. **12.3** Trivially, the Holevo χ quantity is bounded by $S(\rho) = -\mathrm{tr}(\rho\log(\rho)) \leq n$. **12.4** The density matrix is in fact $\rho = 0.5|0\rangle\langle 0| + 0.5|1\rangle\langle 1|$. Hence the Holevo χ quantity is $\log(2) = 1$.

XV. NOTES ON BASIC PROBABILITY THEORY

Exercises A1.1, A1.2, A1.3, A1.4, A1.5, A1.6 Trivial.

XVI. GROUP THEORY

A2.1 The set $(g^r)_{r\in\mathbb{N}}$ must take finitely many different values, since $|G| < \infty$. Therefore, there must by $j \in \mathbb{N}$ such that for infinitely many $r \in \mathbb{N}$, $g^r = g^j$. Choose one such r, strictly larger then j. Then $g^r = g^j$. In particular, $g^{r-j} = e$. Choosing the smallest such positive k yields the order of j. **A2.3** Apply A2.2 to the subgroup generated by g. **A2.4, A2.5** Trivial. **A2.6** The order of the subgroup generated by any element must divide this prime order. **A2.7** Let I be a set of index such that:

$$H = \{e\} \cup \{g^i : i \in I\}.$$

Let $a = \min(I)$. Then, $\langle g^a\rangle \subseteq H$. Let $b \in I\backslash\{\mathbb{Z}a\}$ and suppose $g^b \in H$. Let the euclidean division of b by a give $b = ma + r$. Then, $g^r = g^b g^{-ma} \in H$ but $0 < r < a$. This contradicts $a = \min(I)$. Hence $I\backslash\{\mathbb{Z}a\} =$ and H is cyclic. **A2.8** Trivial. **A2.9** Assume that $g_1, g_2 \in gH$. Then, for some $h, l \in H$, $g_1 = gh$ and $g_2 = gl$. In particular, $g_1 = gll^{-1}h = g_2 l^{-1}h$. The other direction is as simple. **A2.11** (1) is clear. (2) and (3) results from the fact there exists an integer r such that $\chi(g^r) = \chi(g)^r = n$. (4) results from the cyclic property of the trace. (5) and (6) are clear.**A2.15** First,

$$\sum_{i=1}^{r} r_i(\chi_i^p)^*(\chi_i^q) = \sum_{g\in G}(\chi^p(g))^*(\chi^q(g)) = \sum_{g\in G}(\chi^p(g))^{-1}(\chi^q(g)) = \frac{|G|\delta_{pq}}{1} = |G|\delta_{pq}.$$

Summing both sides of the second equation to prove yields $r|G|\delta_{ij}$ in both cases. **A2.16** Trivial. **A2.18** Let $g \neq e$. Then,

$$\chi(g) = \#\{h \in G : gh = h\} = 0.$$

A2.19 The conjugacy class of the identity only contains the identity. Using exercise A2.18, the only non-zero term in the sum is $\chi^p(I)^*\chi(I) = d_{\rho^p}|G|$. **A2.20** $\sum_{\rho\in\hat{G}} d_\rho \chi^\rho(g) = \chi^R(g) = N\delta_{ge}$.**A2.21**

$$|G| = \chi^R(I) = \sum_{\rho\in\hat{G}} d_\rho \chi^\rho(I) = \sum_{\rho\in\hat{G}} d_\rho^2.$$

A2.22 First,

$$f(g)\rho(g) = \frac{1}{\sqrt{N}} \sum_{\sigma\in\hat{G}} \sqrt{d_\sigma}\,\mathrm{tr}(\hat{f}(\sigma)\sigma(g^{-1}))\rho(g).$$

Moreover, according to the Fundamental Theorem,

$$\sum_{g\in G} \chi^\sigma(g)^* \rho(g)_{ij} = \frac{N}{d_\rho}\delta_{\sigma\rho}\delta_{1i}\delta_{1j}.$$

Hence, the right-hand side of equation $A2.9$ becomes:

$$\frac{\sqrt{d_\rho}}{N}\sqrt{d_\rho}\hat{f}(\rho)\frac{N}{d_\rho} = \hat{f}(\rho).$$

A2.23 The first equation is a simple application of the definition. Then, it is easy to see that the second equation is the well-defined inverse of the first. **A2.24** First, notice that $1 + 1 + 2^2 = 6$. Therefore, we already have all the irreducible representations. Let ρ^0 be the trivial representation, ρ^1 be the non-trivial one-dimensional representation and ρ^2 be the two-dimensional representation. Then,

$$\hat{f}(\rho^0) = \frac{1}{\sqrt{6}} \sum_{g\in G} f(g).$$

Also,

$$\hat{f}(\rho^1) = \frac{1}{\sqrt{6}}(f(123) + f(231) + f(312) - f(213) - f(132) - f(321))$$

and without copying the matrices defined in equation A2.5 from the book:

$$\hat{f}(\rho^2) = \frac{1}{\sqrt{6}}\left(\sum_{g\in G} f(g)\rho^2(g).\right)$$

The dimension of the Fourier Transform depends on the representation it is applied to.

XVII. THE SOLOVAY–KITAEV THEOREM

A3.1 First, notice that for any unitaries U and V: $E(U,V) = E(I, U^\dagger V)$ and $D(I, U^\dagger V) = D(U,V)$. Therefore, it is sufficient to prove that for any unitary U, $E(I,U) = \frac{1}{2}D(I,U)$. Moreover, assume without loss of generality that $U = \cos(\theta) - i\sin(\theta)\mathbf{n}$ for some angle θ and axis $\mathbf{n}$. Now,

$$D(U,I) = \frac{1}{2}\mathrm{tr}\sqrt{(U-I)^\dagger(U-I)} = \frac{1}{2}\mathrm{tr}\sqrt{(\cos(\theta)-1)^2+\sin(\theta)^2} = \sqrt{(\cos(\theta)-1)^2+\sin(\theta)^2} = \sqrt{\max_{|\psi\rangle}\|(U-I)\,|\psi\rangle\,\|^2}.$$

A3.2 Let $U = e^{-iA}, V = e^{-iB}$. Expand:

$$UVU^\dagger V^\dagger = 1 - AB + A^2 + AB + BA + B^2 - AB - A^2/2 - B^2/2 - A^2/2 - B^2/2 + \mathcal{O}(\epsilon^3).$$

A3.3 Notice that $D(u(\vec{x}), u(\vec{y})) = D(I, u^\dagger(\vec{x})u(\vec{y}))$ and apply equation 4.19 from the book. (If needed, redo the computation from exercise A3.1.)**A3.4** Trivial.

XVIII. NUMBER THEORY

A4.1, A4.2, A4.3 Trivial. **A4.4** $36300 = 2^2 \times 3 \times 5^2 \times 11^2$. $697 = 17 \times 41$. **A4.5** The first statement is easy enough. Integers $1 \leq a \leq p^2 - 1$ have an inverse modulo p^2 if and only if $\gcd(a, p^2) = 1$. Using the factorisation theorem, all but numbers of the form $a = \alpha p$ have an inverse modulo p^2. **A4.6** Trivial. **A4.7** $1 - n + n^2$. **A4.8** Contrapositive is easy enough. **A4.9, A4.10** Trivial.

A. Exercise A4.11

Assume that $n = p^\alpha$, for some $\alpha \in \mathbb{N}$ and p prime. If $\alpha = 0, 1$, the claim is trivial. Assume $\alpha \geq 2$. Then:

$$\sum_{d|n}\varphi(d) = 1 + p - 1\sum_{k=2}^{\alpha}\varphi(p^k) = p + p(p-1)\sum_{k=0}^{\alpha-2}\varphi(p^k) = p + \sum_{k=2}^{\alpha}p^{k-1}(p-1) = p^\alpha. \tag{7}$$

Let $n = p_1^{\alpha_1}...p_l^{\alpha_l}$ be the prime factorization of an arbitrary n. Then:

$$\sum_{d|n}\varphi(d) = \prod_{j=1}^{l}\sum_{k_j=0}^{\alpha_j}\varphi(p_j^{k_j}) = n. \tag{8}$$

Exercise A4.12, A4.13, A4.14 Trivial. **A4.15** Take a non-trivial element a. The subgroup generated by a has order $r > 1$. By Lagrange's theorem, $r|\varphi(n)$. In other words, there is an integer α such that $\varphi(n) = r\alpha$. Thus, $a^{\varphi(n)} = (a^r)^\alpha = 1^\alpha = 1[n]$.**A4.16, A4.17, A4.18, A4.19** Trivial.

XIX. PUBLIC KEY CRYPTOGRAPHY AND THE RSA CRYPTOSYSTEM [V]

A5.1, A5.2 Trivial.

XX. PROOF OF LIEB'S THEOREM [V]

A6.1 $A \leq B$ means that $\forall x : \langle x, (A-B)x\rangle \geq 0$ which implies that $\forall X \forall x : 0 \leq \langle Xx, (A-B)Xx\rangle = \langle x, (X^\dagger AX - X^\dagger BX)x\rangle$. **A6.2, A6.3** Trivial. **A6.4** (1) $\exists\,|\psi\rangle : \|A\,|\psi\rangle\,\| = |\lambda|$. (2) Decompose in the eigenbasis $|\psi\rangle = \sum_i c_i\,|\phi_i\rangle$. **A6.5** $\det(xI - AB) = \det(A(xA^{-1} - B)) = \det((xA^{-1} - B)A) = \det(xI - BA)$. A6.6 Use A6.4 (1). **A6.7, A6.8** Trivial.