

Faglig kontakt under eksamen:
Johannes Skaar

Eksamen i FE8100
KVANTEDATAMASKINER OG KVANTEKOMMUNIKASJON

Tirsdag 22. januar 2008
09:00–13:00

Tillatte hjelpemidler: Alternativ C

Bestemt, enkel kalkulator tillatt. Matematisk formelsamling tillatt.

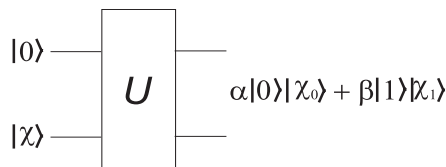
Dette oppgavesettet er på 3 sider.

Oppgave 1

I denne oppgaven skal vi se hvordan man kan kommunisere sikkert uten først å generere en nøkkel.

- a) Vis at alle 4 Bell-tilstander $(|00\rangle \pm |11\rangle)/\sqrt{2}$ og $(|01\rangle \pm |10\rangle)/\sqrt{2}$ kan genereres vha $\beta_{00} = (|00\rangle + |11\rangle)/\sqrt{2}$ og lokale unitære transformasjoner på den ene kvantebiten.
- b) Alice og Bob deler et Bell-par $|\beta_{00}\rangle$. Alice koder inn en klassisk informasjonsbit i sin kvantebit som følger: Hvis informasjonsbiten er “1” anvender hun Pauli-operatoren Z , hvis informasjonsbiten er “0” gjør hun ingenting. Så sender hun kvantebiten til Bob. Forklar hvordan Bob kan dekode meldingen, og konstruer Bobs dekodekrets. Du kan kun bruke projeksjonsmåling av kvantebit i basis $\{|0\rangle, |1\rangle\}$, CNOT og enkeltkvantebitport(er).
- c) Kan en avlytter lese (noe av) meldingen fra Alice ved å måle kvantebiten som Alice sender til Bob? Grunngi svaret.
- d) I resten av oppgaven antar vi at Bob genererer Bell-paret, og sender den ene kvantebiten til Alice. Alice koder så inn informasjonsbiten (som i forrige punkt), og sender kvantebiten tilbake til Bob. En avlytter Eve kopler seg inn i linja (kvantekanal) mellom Alice og Bob. Hun kan gjøre hva hun vil med det som sendes fram og tilbake mellom Alice og Bob, så lenge det ikke bryter med kvantemekanikk.
Sett fra Eves synspunkt, forklar hvorfor vi kan tenke oss at Bob i stedet sender tilstanden $|0\rangle$ med 50% sannsynlighet, og $|1\rangle$ med 50% sannsynlighet.
- e) Jfr. forrige spørsmål antar vi at Bob sender $|0\rangle$ (det andre tilfellet, at han sender $|1\rangle$, blir tilsvarende). Eve kan gjøre to angrep; det første når kvantebiten sendes fra Bob til Alice, og det andre når kvantebiten sendes tilbake fra Alice til Bob. Vi ser nå på det første angrepet.

Det mest generelle angrepet Eve kan gjøre er en kvanteoperasjon, dvs. å sende Bobs kvantebit og en ekstra standardtilstand $|\chi\rangle$ gjennom en unitær kvanteport U , se figur 1. Vis at tilstanden etter dette angrepet kan skrives $\alpha|0\rangle|\chi_0\rangle + \beta|1\rangle|\chi_1\rangle$, der den første kvantebiten referer seg til Bobs kvantebit, $|\chi_0\rangle$ og $|\chi_1\rangle$ er (ikke nødvendigvis ortogonale) tilstander for Eves tilleggsystem og parametrene α og β tilfredsstiller $|\alpha|^2 + |\beta|^2 = 1$.



Figur 1: Første del av Eves angrep.

- f) Alice' informasjonsbit er "0" med sannsynlighet 50% og "1" med sannsynlighet 50%. Etter at Alice har kodet sin informasjonsbit inn på kvantebiten, vis at tilstanden for Alice' og Eves sammensatte system kan skrives

$$\rho = |\alpha|^2|0\rangle|\chi_0\rangle\langle 0|\langle\chi_0| + |\beta|^2|1\rangle|\chi_1\rangle\langle 1|\langle\chi_1| = \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix}, \quad (1)$$

der matriserepresentasjonen er uttrykt i den ortonormale basisen $\{|0\rangle|\chi_0\rangle, |1\rangle|\chi_1\rangle\}$.

- g) Vi ser nå på det andre angrepet Eve kan gjøre, dvs. når kvantebiten sendes tilbake fra Alice til Bob. Hva er den maksimale gjensidige informasjonen Eve kan få med Alice (ved å utføre en måling)?
- h) Anta at Bob har mange kopier av $|\beta_{00}\rangle$. Alice og Bob gjentar nå kommunikasjonen ovenfor for mange av disse parene. Anta at Eve oppnår en gjensidig informasjon med Alice som er større enn null. Forklar hvordan Alice og Bob kan finne ut at det er en Eve på linja. (Hint: De kan ofre noen av parene i en test.)

Oppgave 2

- a) Gitt et sammensatt system AB , der A og B er to identiske, n -dimensjonale systemer/tilstandsrom. En tilstand i AB er sammenfiltret dersom den har ikke-klassiske korrelasjoner mellom A og B . I motsatt fall kalles den separabel. For hver av de følgende tilstandene, avgjør om den er sammenfiltret, separabel, produkttilstand, ren, og/eller blandet. Hvis du ikke kan avgjøre dette på grunnlag av den oppgitte informasjonen, si dette. Begrunnelse er kun nødvendig for 3, 5 og 6. (Vi bruker konvensjonen at første (andre) faktor i et tensorprodukt hører til A (B).)

1. $|\psi\rangle \otimes |\psi\rangle$.
2. $\frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}}$, der $\langle 0|1\rangle = 0$.
3. $\frac{|\psi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\phi\rangle}{\sqrt{3}}$, der $\langle \psi|\phi\rangle = \frac{1}{\sqrt{2}}$.
4. $\rho \otimes \rho$, der ρ har spektral dekomposisjon $\rho = \sum_{i=1}^N p_i |i\rangle\langle i|$, $p_i > 0$ for alle $1 \leq i \leq N$, $\sum_{i=1}^N p_i = 1$ og $N > 1$.

5. $\sum_i^N p_i \rho_i \otimes \sigma_i$, der $p_i > 0$ for alle $1 \leq i \leq N$ og $\sum_{i=1}^N p_i = 1$. ρ_i og σ_i er gyldige tilstander for systemene A og B .
 6. $\sum_i p_i \rho_i \otimes \sigma_i$, der ρ_i og σ_i er vilkårlige $n \times n$ -matriser, og p_i vilkårlige komplekse tall, men slik at hele uttrykket er en gyldig tetthetsmatrise.
- b) La en kvantebit representeres med “dual rail” nummertilstander, dvs. logisk $|0\rangle$ representeres ved nummertilstandene $|10\rangle$ and logisk $|1\rangle$ representeres ved $|01\rangle$. Her betyr $|10\rangle \equiv |1\rangle|0\rangle$ ett foton i den første moden og vakuumtilstanden i den andre. Hvordan kan du lage alle slags enkeltkvantebitoperasjoner vha. stråledelere og faseskiftere?
- c) Hvilke(n) av følgende påstander er riktig? Det er ikke nødvendig med begrunnelse.
1. Tilstandsrommet til n kvantebiter er n -dimensjonalt.
 2. En blandet tilstand kan sees på som en ren tilstand i et større tilstandsrom.
 3. To ortogonale kvantebit-tilstander $|\psi\rangle$ og $|\phi\rangle$ er på motsatt side av Blochkula. Dvs. trekk en linje fra $|\psi\rangle$ gjennom sentrum av Bloch-kula. Denne linja skjærer Bloch-kula i $|\phi\rangle$.
 4. Grover's algoritme er en kvantealgoritme for søking i ustrukturerte databaser.

Single qubit operations:

$$\begin{aligned}
 X = \sigma_1 &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, & Y = \sigma_2 &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, & Z = \sigma_3 &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\
 H &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, & T &= \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}, & S &= \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \\
 R_x(\theta) &\equiv e^{-i\theta X/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} X = \begin{bmatrix} \cos \frac{\theta}{2} & -i \sin \frac{\theta}{2} \\ -i \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix} \\
 R_y(\theta) &\equiv e^{-i\theta Y/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Y = \begin{bmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix} \\
 R_z(\theta) &\equiv e^{-i\theta Z/2} = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}
 \end{aligned}$$

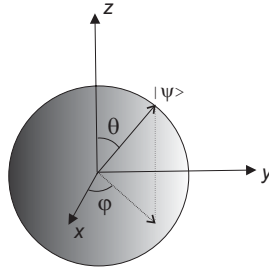
Algebra for the Pauli matrices $\sigma_1 = X$, $\sigma_2 = Y$, and $\sigma_3 = Z$:

$$\begin{aligned}
 [\sigma_1, \sigma_2] &= 2i\sigma_3, & [\sigma_2, \sigma_3] &= 2i\sigma_1, & [\sigma_3, \sigma_1] &= 2i\sigma_2. \\
 \{\sigma_i, \sigma_j\} &\equiv \sigma_i\sigma_j + \sigma_j\sigma_i = 2I\delta_{ij} & \text{for } i, j &= 1, 2, 3.
 \end{aligned}$$

Bloch sphere representation:

$$\begin{aligned}
 |\psi\rangle &= a|0\rangle + b|1\rangle \\
 a &= \cos(\theta/2), & b &= e^{i\varphi} \sin(\theta/2)
 \end{aligned}$$

The state $|\psi\rangle$ has the angular coordinates (θ, ϕ) :

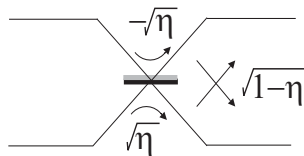


R_x , R_y , and R_z are rotations around the x , y , and z axes on the Bloch sphere.

The Holevo bound: You are given a state ρ_X , where $X = 0, \dots, n$ with associated probabilities p_0, \dots, p_n . For any measurement you can do (with result Y), $H(X : Y) \leq S(\rho) - \sum_{x=1}^n p_x S(\rho_x)$, $\rho = \sum_{x=1}^n p_x \rho_x$.

von Neumann entropy: $S(\rho) = -\text{Tr}\{\rho \log(\rho)\}$.

Beamsplitter: The reflection coefficient from the grey side is $-\sqrt{\eta}$; the reflection coefficient



from the black side is $\sqrt{\eta}$; and both transmission coefficients are $\sqrt{1-\eta}$.

Løsningsforslag

Oppgave 1

- a) Ved å bruke I , Z , X og iY på den ene kvantebiten fås de fire Bell-tilstandene.
- b) Bob dekode meldingen vha. en måling i basisen $(|00\rangle \pm |11\rangle)/\sqrt{2}$. Kretsen består av først en CNOT, deretter en Hadamard-port etterfulgt av en projeksjonsmåling av den første kvantebiten (den som kommer ut av kontrollen til CNOT-porten).
- c) Uavhengig av Alice' informasjonsbit, er tilstanden (tetthetsoperatoren) som Eve ser $I/2$. (Finnes ved å "spore ut" Bob.) Altså kan ikke Eve få noe informasjon om Alice' informasjonsbit.
- d) Tilstanden som Eve ser er $I/2$. Dvs. hun ville ikke se forskjell om Bob i stedet sendte $|0\rangle$ med 50% sannsynlighet og $|1\rangle$ med 50% sannsynlighet, som også gir tetthetsoperatoren $I/2$.
- e) Etter Eves unitære vekselvirkning fås en ny tilstand, som vha. Schmidt-dekomposisjon kan skrives $a|\psi_0\rangle|e_0\rangle + b|\psi_1\rangle|e_1\rangle$. Her er a og b ikke-negative konstanter, mens ψ 'ene refererer seg til kvantebiten og e 'ene refererer seg til Eves ekstrasystem. Tilstandene $|\psi_{0,1}\rangle$ kan uttrykkes som lineærkombinasjoner av $|0\rangle$ og $|1\rangle$: $|\psi_0\rangle = c_{11}|0\rangle + c_{12}|1\rangle$ og $|\psi_1\rangle = c_{21}|0\rangle + c_{22}|1\rangle$. Innsatt i Schmidt-dekomposisjonen fås det ønskede resultatet $\alpha|0\rangle|\chi_0\rangle + \beta|1\rangle|\chi_1\rangle$. Betingelsen $|\alpha|^2 + |\beta|^2$ fås fra normalisering, idet $|0\rangle|\chi_0\rangle$ og $|1\rangle|\chi_1\rangle$ er ortogonale.
- f) Tilstanden før Alice er

$$\rho_0 = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}. \quad (2)$$

Etter Alice fås

$$\rho = \frac{1}{2}\rho_0 + \frac{1}{2}Z\rho_0Z = \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix}. \quad (3)$$

- g) Holevos grense gir at for enhver måling Eve kan utføre, blir den gjensidige informasjonen mellom Eve og Alice mindre enn $S(\rho) - \frac{1}{2}S(\rho_0) - \frac{1}{2}S(Z\rho_0Z) = S(\rho) = h(|\beta|^2)$, der h er den binære Shannon-entropien. Merk at hvis Eve gjør et angrep som gir henne gjensidig informasjon med Alice større enn null, må $|\beta|^2$ være større enn null. Hvis Eve ikke er tilstede, er $|\beta|^2 = 0$.
- h) Alice kan ofre en viss andel av kvantebitene som sendes til henne. Hvis hun bestemmer seg for å ofre en gitt kvantebit, måler hun den i basisen $\{|0\rangle, |1\rangle\}$. Etterpå forteller hun åpent til Bob at hun har ofret biten og ber han om å måle sin kvantebit i tilsvarende basis. Deretter kan de åpent sammenlikne sine resultater. Sannsynligheten for at de får ulike resultater for et gitt par er $|\beta|^2$. Ved å ofre tilstrekkelig mange par finner de til slutt et rimelig nøyaktig estimat av $|\beta|^2$, og kan avbryte protokollen dersom $|\beta|^2$ er større enn en gitt toleranse. Med andre ord, Eve kan detekteres!

Oppgave 2

a) Ren er motsatt av blandet. Separabel er motsatt av sammenfiltret. Angir derfor bare den ene av disse parene av begreper.

- (a) $|\psi\rangle \otimes |\psi\rangle$ er en ren, separabel produkttilstand.
- (b) $\frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}}$ er en ren, sammenfiltret tilstand. Ikke produkttilstand.
- (c) $\frac{|\psi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\phi\rangle}{\sqrt{3}}$ er en ren, sammenfiltret tilstand. Ikke produkttilstand. Man kan vise at den er sammenfiltret f.eks. ved å regne ut tetthetsoperatoren for A , ρ_A , og sjekke at ρ_A er blandet (kontroller at $\text{Tr}(\rho_A^2) \neq 1$). Evt. kan man sammenlikne $\rho_A \otimes \rho_A$ med den totale tetthetsoperatoren.
- (d) $\rho \otimes \rho$ er en blandet, separabel produkttilstand.
- (e) $\sum_i p_i \rho_i \otimes \sigma_i$, der $p_i > 0$, $\sum_i p_i = 1$ og ρ_i og σ_i er gyldige tilstander for systemene A og B : Denne tilstanden kan genereres uten at A og B vekselvirker kvantemekanisk. (Med sannsynlighet p_i får Charlie resultatet i , og sier fra til Alice og Bob at de skal preparere sitt system i hhv. ρ_i og σ_i . For en som ikke kjenner i , bare sannsynlighetene p_i , er tilstanden den oppgitte.). Den er altså separabel. Generelt er den blandet og ikke en produkttilstand, men for spesielle valg av p_i , ρ_i og σ_i kan den bli ren og/eller en produkttilstand.
- (f) $\sum_i p_i \rho_i \otimes \sigma_i$, der ρ_i og σ_i er vilkårlige $n \times n$ -matriser, og p_i vilkårlige komplekse tall, men slik at hele uttrykket er en gyldig tetthetsmatrise: Dette er en helt vilkårlig tetthetsmatrise for det sammensatte systemet. Man kan f.eks. velge matrisene til å ha kun ett enkelt element ulikt null. Hvilket element som er ulikt null kan være avhengig av i . På denne måten kan man generere en vilkårlig matrise. Man kan altså ikke avgjøre hvilke egenskaper tilstanden har.

b) A beamsplitter gives the transformation

$$\begin{bmatrix} \cos \theta/2 & \sin \theta/2 \\ \sin \theta/2 & -\cos \theta/2 \end{bmatrix}, \quad (4)$$

on the logical qubit. Here the beamsplitter reflectivity is $\eta = \cos^2(\theta/2)$. A phase shifter in the one of the modes leads to

$$R_z(\phi) = \begin{bmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{bmatrix}, \quad (5)$$

up to a global phase. Using a beamsplitter and a phase shifter with $\phi = \pi$ we obtain the rotation $R_y(\theta)$. With the rotations R_y and R_z , any single qubit rotation can be obtained: First you rotate with R_z to transfer the state to the xz -plane of the Bloch sphere. Then you rotate with R_y to obtain the desired latitude, and with R_z to obtain the desired longitude.

c) 2,3,4 er riktige; 1 er gal.