Kvantni prstni odtisi

Projekt pri predmetu Kriptografija in teorija kodiranja II

Avtor: Nejc Škofič

Mentor: Aleksandar Jurišić

Kraj in datum: Ljubljana, 29.8.2011

Kazalo

1. Uvod

Zgoščevalne funkcije so funkcije, ki poljubnemu bloku podatkov oziroma sporočilu priredijo običajno krajše zaporedje vnaprej določene dolžine, ki ga imenujemo izvleček. Z izvlečki lako preverjamo enakost dveh blokov podatkov z majhno možnostjo napake. Za dobre kriptografske zgoščevalne funkcije velja, da je poleg učinkovite izračunljivosti za poljuben blok podatkov, tudi težko najti sporočilo, ki nam da iskani prstni odtis (enosmerne funkcije), da je težko najti drugo sporočilo, ki nam da isti prstni odtis kot originalno (šibko brez trčenj) in da je težko najti dve sporočili z enakim prstnim odtisom (krepko brez trčenj).

Primer uporabe je preverjanje enakosti dveh blokov podatkov, kjer je cena komunikacije pri neposredni primerjavi predraga (na primer komunikacija preko omrežja) ali pa je neposreden prenos bloka za primerjavo nezaželen. V tem primeru se lahko generira in pošlje le izvleček, ki se ga uporabi za primerjavo. Drugi primer uporabe je preverjanje integritete podatkov, s katerim lahko zaznamo neželene spremembe. Do teh lahko pride zaradi napak v fizičnem nosilcu na katerem je shranjen podatkovni blok (na primer poškodovana zgoščenka), napak v prenosih podatkov (na primer zaradi izpada omrežja prekinjen prenos podatkov preko mreže) ali pa zaradi aktivne spremembe podatkov s strani tretje osebe. Posebej pozoren mora biti uporabnik pri nameščanju programske opreme iz neznanih virov, kjer lahko tretja oseba programsko opremo prilagodi, in z namestitvijo pri uporabniku namesti zlonamerno kodo. Uporabnik lahko v tem primeru izgubi podatke, lahko pa pride tudi do odtujitve podatkov in njihova uporaba v uporabnikovo škodo. Temu se lahko uporabnik izogne s preverjanjem enakosti izvlečka, ki ga je generiral avtor programske opreme in izvlečka programske opreme v lasti uporabnika.

Kvantno procesiranje je eden izmed alternativnih modelov računanja, ki je zanimiv predvsem zaradi tega, ker naj bi bil računsko močnejši kot so klasični modeli računanja (na primer Turingov stroj). Kvantno procesiranje je skupaj s teorijo kvantne informacije mlada veja znanosti, katere razvoj se je začel s koncem 80. let prejšnjega stoletja in temelji na kvantni mehaniki. To je veja fizike, ki pojasnjuje obnašanje fizikalnih sistemov na subatomskem nivoju. Zakoni, po katerih se ravnajo taki sistemi, so drugačni kot zakoni klasične fizike, zato je bilo potrebno najprej izgraditi teorijo kvantnih informacij in kvantnega procesiranja preden lahko govorimo o kvantnih računalnikih. Ta postopek še vedno poteka. Kljub temu raziskovalci že poskušajo najti algoritme, ki bi jih lahko poganjali s pomočjo kvantnih računalnikov in poskušajo oceniti njihovo izboljšavo glede na klasične algoritme.

Primer takih algoritmov so algoritmi za generiranje kvantnih verzij zgoščevalnih funkcij, poimenovani algoritmi za generiranje kvantnih prstnih odtisov. Njihova privlačnost je v enostavni konfiguraciji problema, kljub temu pa dajo otipljive rezultate o moči kvantnih sistemov. V tem projektu bomo opisali protokol generiranja prstnega odtisa z enim večdimenzionalnim kvantnim stanjem, ki uporablja kvantno prepletenost za izmenjavo ključa in protokol za generiranje prstnega odtisa, ki uporablja ponavljajoče meritve na večjem številu qubitov. Pokazali bomo, da so kvantni algoritmi boljši od klasičnih.

2. Osnove kvantne mehanike

Kot smo omenili že v uvodu je kvantno procesiranje temelji na teoriji kvantne mehanike. Da bi razumeli kako kvantno procesiranje sploh deluje, si moramo najprej ogledati kvantno mehaniko in njene postulate ter lastnosti.

Kvantna mehanika je veja fizike, ki se ukvarja s fizikalnimi lahnostmi in zakoni atomskega in subatomskega sveta. Njen razvoj se je začel v prvi polovici 20. stoletja, ko so znanstveniki začeli opažati razlike med napovedmi, ki jih je dajala klasična fizika in eksperimentalnimi rezultati pri problemih kot so sevanje črnega telesa. Izraz kvantna mehanika je skoval Max Planck, ki je opazil, da se določene fizikalne lastnosti kot so skupna energija črnega telesa ali vrtilna količina elektrona v atomu ne spreminjajo zvezno ampak le v določenih diskretnih vrednostih – kvantih. Kvantna mehanika je uvedla mnoge ideje, ki so se na prvi pogled zdele neintuitivne. Ena izmed njih je dvojnost valovanje-delec, ki je pojasnila odsotnost pojava interference kadar opravljamo meritve na režah, in njegova prisotnost kadar tega ne počnemo[1]. Nekatere izmed ostalih lastnosti kvantne mehanike, kot so nedoločenost, prepletenost kvantnih stanj in nezmožnost popolnega kopiranja kvantnega stanja bom razložil pozneje, saj bo njihovo razumevanje pomembno pri analizi za generiranje kvantnih prstnih odtisov in njihovem preverjanju.

Kvantna mehanika ne podaja direktno zakonov, po katerih se mora fizikalni sistem ravnati, ampak matematično in konceptualno ogrodje za razvoj teh zakonov. To ogrodje sestavljajo štirje postulati, ki si jih bomo podrobneje ogledali.

Postulat št. 1: Z vsakim izoliranim fizikalnim sistemom je povezan kompleksni vektorski prostor s skalarnim produktom (takemu vektorskemu prostoru pravimo tudi *Hilbertov prostor*), poznan tudi kot *prostor stanj sistema*. Sistem je popolnoma opisan z *lastnim vektorjem stanja*, ki je enotski vektor iz prostora stanj sistema.

Kvantna mehanika nam ne pove kako za specifičen fizikalni sistem izpeljati njegov lastni vektor stanja. Pove nam le, da tak vektor obstaja. Najpreprostejši kvantno mehanski sistem s katerim se bomo tudi mi ukvarjali je *qubit*. Qubit predstavlja element iz 2-razsežnega prostora stanj V. Naj $|0\rangle$ in $|1\rangle$[2] sestavljata ortonormirano bazo za ta prostor stanj. V matrični obliki ta lahko ti dve stanji zapišemo kot:

$$|0\rangle: \begin{bmatrix}1\\0\end{bmatrix} \text{ in } |1\rangle: \begin{bmatrix}0\\1\end{bmatrix}. \tag{1}$$

Tedaj lahko poljuben vektor stanja iz tega prostora zapišemo kot njuno linearno kombinacijo:

$$|\psi\rangle = a|0\rangle + b|1\rangle \text{ za } a, b \in \mathbb{C}. \tag{2}$$

[1] Eksperiment je znan pod imenom poskus z dvojno režo (ang. double-slit experiment). Prvi ga je opravil Young v zgodnjem 19. stoletju, kar je uveljavilo teorijo, da je svetloba valovanje. Poznejši poskusi s fotoelektričnim efektom so pokazali, da se svetloba lahko obnaša tako kot valovanje, kot tudi tok delcev.

[2] $|0\rangle$ in $|1\rangle$ sta primer zapisa v Diracovi notaciji in predstavljata prvi in drugi bazni vektor

Ker smo rekli, da je lastni vektor stanja enotski vektor, zanj velja, da je skalarni produkt $\langle\psi|\psi\rangle$ enak 1. $\langle\psi| = |\psi\rangle^{*T} = |\psi\rangle^{\dagger}$ je primer zapisa v Diracovi notaciji *dualnega vektorja* $|\psi\rangle$. Iz skalarnega produkta lahko izpeljemo, da velja pogoj $|a|^2 + |b|^2 = 1$. Qubiti so zanimivi ravno zaradi tega ker lahko poleg osnovnih baznih stanj, kot sta $|0\rangle$ in $|1\rangle$, vsebujejo tudi katerokoli linearno kombinacijo obeh stanj, ki izpolnjuje zgornji pogoj. Pravimo, da je tako kvantno stanje v *superpoziciji* osnovnih stanj.

Postulat št. 2: Sprememba zaprtega kvantnega sistema je opisana z *unitarno transformacijo* (to je bijektivna preslikava med dvema Hilbertovima prostoroma, ki ohranja skalarni produkt). To pomeni, da je stanje sistema $|\psi\rangle$ v času t_1 povezano s stanjem sistema $|\psi'\rangle$ v času t_2 preko unitarnega operatorja *U*, ki je odvisen le od t_1 in t_2,

$$|\psi'\rangle = U|\psi\rangle. \tag{3}$$

Čeprav nam ta postulat pove le to, da obstajajo transformacije kvantnih sistemov, je to že dovolj, saj potrdi eksistenco transformacij, ki jih lahko uporabimo za definicijo operatorjev in s tem postavi temelje za kvantno procesiranje. V primeru qubitov se izkaže, da je vsak unitarni operator lahko realiziran v realnih sistemih.

Poglejmo si operatorja, ki ga bomo uporabili tudi v nadaljevanju. Ta operator so *Hadamardova vrata*, najpogosteje označena s H, ki operirajo na enem qubitu. Pripadajoča transformacijska matrika tega operatorja je

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}. \tag{4}$$

Da je operator unitaren lahko zlahka preverimo:

$$H^{\dagger} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}, \tag{5}$$

$$H^{\dagger}H = I. \tag{6}$$

Na qubitih $|0\rangle$ in $|1\rangle$ naredijo Hadamardova vrata naslednjo transformacijo:

$$|0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \tag{7}$$

$$|1\rangle \mapsto \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{8}$$

S Hadamardovimi vrati lahko qubit, ki je v osnovnem stanju postavimo v superpozicijo osnovnih stanj.

Postulat št. 3: Merjenje kvantnega sistema je opisano z množico $\{M_{m\in\mathbb{N}_0}\}$ *merilnih operatorjev*. Ti operatorji vplivajo na prostor stanj sistema, ki je merjen. Indeks m se nanaša

na rezultat merjenja, ki se lahko pojavi v eksperimentu. Če je stanje kvantnega sistema tik pred meritvijo $|\psi\rangle$, potem je verjetnost, da pride do rezultata m, enaka

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{9}$$

in je stanje sistema po meritvi enako

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} = \frac{M_m|\psi\rangle}{\sqrt{p(m)}}. \tag{10}$$

$M_m^\dagger = (M_m^*)^T$, kjer je M_m^* kompleksna konjugacija elementov matrike M_m, in $(M_m|\psi\rangle)^\dagger = \langle\psi|M_m^\dagger$.

Meritveni operatorji zadoščajo *enačbi popolne verjetnosti* (ang. completeness equation)

$$\sum_m M_m^\dagger M_m = I. \tag{11}$$

Ta nam pove, da se verjetnosti meritve, pri kateri dobimo rezultat m, $p(m)$ seštejejo v ena, saj velja:

$$\sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \left\langle\psi\middle|\left(\sum\nolimits_m M_m^\dagger M_m\right)\middle|\psi\right\rangle = \langle\psi|\psi\rangle = 1. \tag{12}$$

Da nam bo 3. postulat jasnejši, poglejmo njegovo delovanje pri merjenju qubitov. Definirajmo dva meritvena operatorja $M_0 = |0\rangle\langle 0|$ in $M_1 = |1\rangle\langle 1|$. V matrični obliki lahko ta dva operatorja zapišemo kot:

$$M_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ in } M_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}. \tag{13}$$

Oba operatorja sta hermitska[3] in zanju velja $M_0^2 = M_0$ in $M_1^2 = M_1$. Iz tega lahko izpeljemo veljavnost enačbe popolne verjetnosti $I = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1$. Naj bo stanje, ki ga merimo $|\psi\rangle = a|0\rangle + b|1\rangle$. Tedaj je verjetnost, da dobimo meritev 0, enaka

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |a|^2. \tag{14}$$

Podobno dobimo verjetnost, da je meritev 1 enaka $p(1) = |b|^2$. Stanje kvantnega sistema po meritvah pri obeh primerih pa je naslednje:

[3] V Hilbertovem prostoru H, je operator A sam *sebi adjungiran* oziroma *hermitski*, če zanj velja $\forall\, x, y \in H: \langle Ax|y\rangle = \langle x|Ay\rangle$. Ekvivalentni pogoj je, da je operatorjeva matrika hermitska, kar pomeni, da velja $A = A^\dagger$.

$$\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle, \tag{15}$$

$$\frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle. \tag{16}$$

Pokažimo sedaj, da se s stališča opazovalca sistema kvantni stanji $|0\rangle$ in $\frac{a}{|a|}|0\rangle$ ne razlikujeta. Ker je a kompleksno število, nam količnik $\frac{a}{|a|}$ predstavlja točko na enotski krožnici v kompleksni ravnini, ki jo lahko zapišemo tudi kot $e^{i\theta}$, kjer je $\theta \in \mathbb{R}$. Da lahko dve kvantni stanji med seboj razlikujemo, mora obstajati statistična razlika v možnem izidu meritev. Naj bo M_m merilni operator za neko kvantno stanje in $M'_m = e^{i\theta}M_m$. Po enačbi (9), je $p(m) = \langle\phi|M_m^\dagger M_m|\phi\rangle$ in $p'(m) = \langle\phi|M_m'^\dagger M'_m|\phi\rangle = \langle\phi|e^{-i\theta}M_m^\dagger M_m e^{i\theta}|\phi\rangle = \langle\phi|M_m^\dagger M_m|\phi\rangle = p(m)$ za poljuben $|\phi\rangle$. Statistične verjetnosti rezultata meritve za ti dve stanji se ne razlikujeta, zato sta za opazovalca kvantni stanji identični. Za stanji $|\phi\rangle$ in $e^{i\theta}|\phi\rangle$ pravimo, da sta enaki do *globalnega faznega faktorja* $e^{i\theta}$m ki ga lahko pri meritvah zanemarimo. Stanji po meritvi opisani v enačbah (15) oziroma (16) sta tako za opazovalca enaki $|0\rangle$ oziroma $|1\rangle$.

Postulat št. 3 je za nas pomemben iz več vidikov. Prvi in najpomembnejši je, da vsaka meritev kvantnega sistema zmoti ta sistem in spremeni njegovo stanje. Ta lastnost kvantno mehanskim sistemov vodi do problema razločevanja kvantnih stanj. Če je qubit $|0\rangle$ potem bo vsaka meritev dala 0 z verjetnostjo 1 in kvantno stanje bo še vedno $|0\rangle$. Ekvivalentna trditev velja za $|1\rangle$. V tem primeru se kvantni sistem obnaša enako kot klasična bitna logika. Kaj pa se zgodi v primeru stanja $|\psi\rangle = a|0\rangle + b|1\rangle$? Tokrat bomo dobili 0 z verjetnostjo $|a|^2$ ali 1 z verjetnostjo $|b|^2$ in sistem, ki bo bodisi v stanju $|0\rangle$ ali $|1\rangle$. Informacija o a in b se je z meritvijo izgubila. Čeprav je bil pred meritvijo sistem v superpoziciji stanj $|0\rangle$ in $|1\rangle$ je po njej samo v enem stanju in vsaka nadaljnja meritev vrne prejšnji rezultat. Problem se pojavi, ker $|\psi\rangle$ ni bil ortogonalen na bazo v kateri smo merili ($|0\rangle$ in $|1\rangle$). V splošnem lahko dve kvantni stanji razločimo, če sta ortogonalni med seboj.

Postulat št. 4: Prostor stanj sestavljenega fizikalnega sistema je tenzorski produkt prostora stanj komponent tega fizikalnega prostora. Še več, če indeksiramo sisteme z 1 do n in je sistem i pripravljen v stanje $|\psi_i\rangle$, potem je sestavljeno stanje celotnega sistema $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$.

Sestavljeno stanje sistema $|\psi_1\rangle \otimes |\psi_2\rangle$ krajše zapišemo kot $|\psi_1\rangle|\psi_2\rangle$ ali $|\psi_1\psi_2\rangle$.

Ta postulat nam omogoča definirati eno najbolj zanimivih in presenetljivih idej sestavljenih kvantnih sistemov – kvantno prepletenost. Poglejmo si dvo-qubitni sistem

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{17}$$

Opravimo delno meritev na prvem qubitu. Verjetnost, da dobimo meritev 0 je po enačbi (9) enako

$$\mathrm{p_1}(0) = \langle\psi|(\mathrm{M_0} \otimes \mathrm{I})^\dagger(\mathrm{M_0} \otimes \mathrm{I})|\psi\rangle = \frac{1}{\sqrt{2}}\langle 00|\frac{1}{\sqrt{2}}|00\rangle = \frac{1}{2}. \quad (18)$$

Stanje sistema po meritvi v primeru, da smo dobili meritev 0, pa je po enačbi (10) enaka

$$|\psi'\rangle = \frac{(\mathrm{M_0} \otimes \mathrm{I})|\psi\rangle}{\sqrt{\mathrm{p_1}(0)}} = \frac{\frac{1}{\sqrt{2}}|00\rangle}{\frac{1}{\sqrt{2}}} = |00\rangle. \quad (19)$$

Podobno lahko izpeljemo za primer meritve z rezultatom 1.

Opazimo, da so meritve korelirane, saj bo meritev drugega qubita po prvi meritvi vedno vrnila rezultat meritve prvega qubita. V primeru, da je bil rezultat prve meritve 0 je verjetnost, da dobimo 0 tudi za rezultat meritve drugega qubita enaka 1:

$$p_2(0) = \langle\psi'|(I \otimes M_0)^\dagger(I \otimes M_0)|\psi'\rangle = 1\,. \quad (20)$$

S prepletenimi stanji je mogoče opravljati korelirane meritve, čeprav se qubita, ki tvorita prepleteno stanje, nahajata na različnih lokacijah in imamo dostop samo do enega izmed njiju. S kvantno prepletenostjo je mogoče izvesti teleportacijo kvantnega stanja, pri kvantnih prstnih odtisih pa bomo to lastnost uporabili za generiranje skupnega ključa.

Za zaključek si poglejmo še eno osnovno lastnost kvantne mehanike – *nezmožnost kopiranja kvantnega stanja*. Postulat št. 3 nam že daje slutiti, da bi pri morebitnem poskusu kloniranja kvantnega stanja lahko imeli probleme. Če poskusimo izmeriti stanje v neki ortogonalni bazi bomo uspeli le, če bo kvantno stanje del te baze, kot je že bilo opisano. V splošnem si torej z meritvijo ne moremo pomagati pri kopiranju. Preostane nam le še manipulacija kvantnega stanja z operatorji. Sestavimo sestavljen kvantni sistem iz dveh qubitov. Prvi qubit naj bo stanje $|\psi\rangle$, ki ga želimo kopirati, drugi pa neko osnovno stanje $|e\rangle$ izbrano neodvisno od stanja $|\psi\rangle$. Tedaj imamo sestavljen sistem $|\psi\rangle|e\rangle$. Zanima nas operator *U*, tako da bo veljalo:

$$U|\psi\rangle|e\rangle = |\psi\rangle|\psi\rangle \text{ in } U|\phi\rangle|e\rangle = |\phi\rangle|\phi\rangle \quad (21)$$

za poljubni kvantni stanji $|\psi\rangle$ in $|\phi\rangle$. Ker je *U* unitarni operator (postulat št. 2), ohranja skalarni produkt in velja:

$$\langle e|\langle\phi|U^\dagger U|\psi\rangle|e\rangle = \langle\phi|\langle\phi|\psi\rangle|\psi\rangle \quad (22)$$

iz česar izpeljemo, da je $\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$. To pa velja le, če sta $|\phi\rangle$ in $|\psi\rangle$ enaka, ali pa ortogononalna, kar pa v splošnem ni res. Zato torej operator *U* ne more klonirati kvantnih stanj in kloniranje ni mogoče.

Namen tega poglavja je podati dovolj matematičnih osnov kvantne mehanike, da bo bilo preostanku projekta mogoče brez težav slediti. Podrobnejše definicije, implikacije postulatov in njihova uporaba v kvantnem procesiranju so opisane v [3].

3. Primeri algoritmov

V tem poglavju bom predstavil dva različna protokola za generiranje kvantnih prstnih odtisov. Prvi protokol izkorišča kvantno prepletenost za svoje delovanje. Pokazal bom optimalno delovanje in izboljšanje v primerjavi s klasičnim protokolom z skupnim ključem. Drugi opisani protokol izkorišča ponavljajoče meritve za zmanjšanje napake v meritvah. Primerjali bomo velikost prstni odtisov generiranih s tem protokolom in pokazali kakšna je verjetnost napake.

3.1 Konfiguracija problema

Osredotočili se bomo na model SMP (ang. simultaneous message passing). V tem modelu imata dva udeleženca, ki ju bomo imenovali Alica in Bob, vhod x in y, ki predstavljata dve ne nujno različni sporočili. Obadva hkrati pošljeta prstna odtisa x' in y' tretji osebi, ki jo bomo imenovali sodnik. Sodnik nima lastnega sporočila ampak le funkcijo, ki jo izvede nad prejetima sporočiloma. V našem primeru bo ta funkcija kar enakost obeh vhodov:

$$EQ(x', y') = \begin{cases} 0, \text{če } x' \neq y' \\ 1, \text{če } x' = y' \end{cases} \tag{23}$$

Sodnik je uspešen tedaj, ko za par (x', y') vrne 1 natanko tedaj, ko sta sporočili x in y enaki, ter 0 natanko tedaj, ko sta sporočili x in y različni. V ostalih primerih je sodnik naredil napako. Naš cilj je minimizirati komunikacijo pri najslabšem paru sporočil (x, y) pri dovolj majhni verjetnosti napake sodnika. Ker gre za hkratno pošiljanje sporočil pri katerem udeleženca ne komunicirata neposredno med seboj, se ta model imenuje *simultano pošiljanje sporočil* ali *SMP* (ang. *simultaneous message passing*).

3.2 Klasični algoritmi z skupno naključnostjo proti kvantnim algoritmom s prepletenostjo

3.2.1 Klasični protokol z skupno naključnostjo

Najprej si poglejmo klasični protokol za izdelavo prstnih odtisov. Naj obstaja *n* različnih sporočil in *m* različnih prstnih odtisov. Zaradi definicije prstnega odtisa mora nujno veljati, da je *n* > *m*. Alica in Bob na podlagi svojega zasebnega ključa razdelita množico *n* sporočil na *m* skoraj enako velikih podmnožic tako, da velja: *k* skupin vsebuje $\lceil n/m \rceil$ sporočil in *m*-*k* skupin vsebuje $\lfloor n/m \rfloor$ sporočil, kjer je $k = n \bmod m$. Elementi podmnožice se preslikajo v isti prstni odtis. Vpeljemo še zlonamernega udeleženca Sabino, ki razdeljuje sporočila Alici in Bobu. Njen namen je maksimizirati verjetnost, da bo sodnik, ki ga imenujmo Roger, na podlagi prstnih odtisov Alice in Boba sporočil, da sta sporočili enaki, čeprav bosta v resnici sporočili različni. Na voljo ima $k\lceil n/m \rceil^2 + (m-k)\lfloor n-m \rfloor^2 - n$ izbir od skupno $n^2 - n$ neenakih parov. Ker pa Sabina ne pozna algoritma, ki razdeli sporočila v množice z enakimi prstnimi odtisi, bo poslala kar dve neenaki sporočili. V najslabšem primeru bo tedaj verjetnost napake kar

$$P_e = \frac{k\lceil n/m \rceil^2 + (m-k)\lfloor n-m \rfloor^2 - n}{n^2 - n}. \tag{24}$$

V nadaljevanju bomo pokazali tudi, da je tak protokol optimalen.

Predstavljajmo si, da Alice, Bob in Roger pripadajo ekipi s ciljem maksimizirati verjetnost Rogerjevega uspeha, medtem ko njihov nasprotnik Sabina želi maksimizirati napako. Ta ekipa se ravna po vnaprej dogovorjeni in znani strategiji, kjer imata Alica in Bob za vsak par sporočil, ki jih prejmeta od Sabine verjetnost, da generirata par prstnih odtisov (a, b) in kjer Roger za vsak par (a, b), ki ga prejme od Alice in Boba napove, da sta sporočili enaki z neko verjetnostjo. Tako lahko vsako strategijo opišemo s trojčkom (p, q, r), kjer je $p, q: \{1, \dots, m\} \times \{1, \dots, n\} \times \mathbb{Z}^+ \to [0, 1]$ in $r: \{1, \dots, m\} \times \{1, \dots, m\} \to [0, 1]$. Funkcija $p(a|x, \xi)$ poda verjetnost, da bo Alica poslala prstni odtis a na prejeto sporočilo x pri skupnem ključu $\xi \in \mathbb{Z}^+$, funkcija $q(b|y, \xi)$ poda verjetnost, da bo Bob poslal prstni odtis b na prejeto sporočilo y pri skupnem ključu ξ in funkcija $r(a, b)$ poda verjetnost, da bo Roger na prejeti par (a, b) odgovoril $z = 1$ (sporočili sta enaki). Kadar vse tri funkcije slikajo le v vrednosti 0 in 1 pravimo, da je strategija deterministična. Velja

$$\sum_{a=1}^{m} p(a|x, \xi) = \sum_{b=1}^{m} q(b|y, \xi) = 1 \tag{25}$$

za vse vrednosti x, y in ξ. Vir skupne naključnosti, je izražen s funkcijo $\sigma: \mathbb{Z}^+ \to [0, 1]$, kjer je $\sigma(\xi)$ verjetnost, da si Alica in Bob delita ključ ξ. Velja

$$\sum_{\xi=1}^{\infty} \sigma(\xi) = 1. \tag{26}$$

Dovolimo, da si Alica in Bob izbereta funkcijo σ. Trojček (p, q, r) je tako strategija s skupno naključnostjo. Če Alica in Bob uporabljata algoritem, ki je neodvisen od ξ, je to strategija brez skupne naključnosti.

Pri podani strategiji (p, q, r) s skupno naključnostjo ξ je verjetnost, da Roger vrne 1, kadar Sapna pošlje sporočilo x Alici in y Bobu enaka

$$P_1^{(p,q,r)}(x, y) = \sum_{\xi=0}^{\infty} \sum_{a,b=0}^{m} p(a|x, \xi) q(b|y, \xi) r(a, b) \sigma(\xi). \tag{27}$$

Napaka je enaka

$$P_e^{(p,q,r)}(x, y) = \begin{cases} 1 - P_1^{(p,q,r)}(x, x); & x = y \\ P_1^{(p,q,r)}(x, y); & x \neq y \end{cases} \tag{28}$$

in napaka v najslabšem primeru je kar največja možna napaka, ki jo Sabina lahko doseže

$$P_{wce}^{(p,q,r)}(x, y) = \max_{x,y} P_e^{(p,q,r)}(x, y) \tag{29}$$

Optimalna strategija je torej tista, ki minimizira napako v najslabšem primeru:

$$\min_{(p,q,r)} P_{wce}^{(p,q,r)}(x,y) \tag{30}$$

Ogledal si bomo strategije z enostransko napako, kjer je $P_1^{(p,q,r)}(x,y) = 1$. V tem primeru Roger nikoli ne bo mogel odgovoriti z 0 na sporočili, ki sta enaki.

Lema 1: Naj bo (p,q,r) strategija za generiranje prstnih odtisov z skupno naključnostjo σ in enostransko napako. Tedaj velja

$$P_e^{(p,q,r)}(x,y) \geq P_e^{(p,q,r')}(x,y) \tag{31}$$

za vse x in y, kjer je

$$r'(a,b) = \begin{cases} 1; \exists x,\xi: p(a|x,\xi) > 0 \wedge q(b|y,\xi) > 0 \\ 0; \text{sicer} \end{cases} \tag{32}$$

Dokaz: Da zadostimo omejitvi o enostranski napaki, moramo za nek p in q nujno imeti $r(a,b) = 1$ za vsak x in ξ, pri katerih velja $p(a|x,\xi) > 0$ in $q(b|y,\xi)$. Ker želimo minimizirati $P_1(x,y)$, kadar sta x in y med seboj različna, izberemo $r(a,b) = 0$ v teh primerih. ■

Z lemo 1 se lahko omejimo na strategije, kjer je Rogerjeva izbira deterministična. Definirajmo

$$N_e^{(p,q,r)} = \sum_{x,y} P_e^{(p,q,r)}(x,y). \tag{33}$$

Za deterministične strategije z enostransko napako in brez skupne naključnosti nam ta vrednost pove število parov (x,y), pri katerih pride do napake.

Lema 2: Naj bo (p,q,r) strategija za generiranje prstnih odtisov z skupno naključnostjo σ in enostransko napako. Potem obstaja deterministična strategija za generiranje prstnih odtisov (p',q',r') brez skupne naključnosti in z enostransko napako, da velja:

$$N_e^{(p,q,r)} \geq N_e^{(p',q',r')}. \tag{34}$$

Dokaz: Po lemi 1 velja

$$N_e^{(p,q,r)} \geq N_e^{(p,q,r')}, \tag{35}$$

kjer je r' Rogerjeva deterministična strategija. Definirajmo strategiji Alice in Boba brez skupne naključnosti: $p_\xi(a|x) \equiv p(a|x,\xi)$ in $q_\xi(b|y) \equiv q(b|y,\xi)$. Tedaj velja

$$N_e^{(p,q,r\prime)} = \sum_{\xi} N_e^{(p,q,r')}\sigma(\xi) \geq \min_{\xi} N_e^{(p_\xi,q_\xi,r')} = N_e^{(p_{\xi\prime},q_{\xi\prime},r')}, \tag{36}$$

kjer je $(p_{\xi\prime}, q_{\xi\prime}, r')$ strategija brez skupne naključnosti, ki doseže minimum. Funkciji $p_{\xi\prime}$ in $q_{\xi\prime}$ sta probabilistični zasebni strategiji brez skupne naključnosti. Zaradi normalizacije je množica vseh takih funkcij konveksna in kompaktna z ekstremnimi točkami iz množice m^n različnih deterministčnih strategij. Vsako probabilistično strategijo lahko opišemo z deterministčnimi na sledeč način:

$$p_{\xi'}(a|x) = \sum_i \phi_i \hat{p}_i(a|x) \text{ in } q_{\xi'}(b|y) = \sum_j \theta_j \hat{q}_j(b|y), \tag{37}$$

kjer sta $\phi_i, \theta_j \geq 0$, $\sum_i \phi_i = \sum_i \theta_i = 1$ in sta strategiji $\hat{p}_i(a|x)$ in $q_{\xi'}(b|y)$ deterministični. Tedaj velja

$$N_e^{(p,q,r\prime)} = \sum_{i,j} \phi_i\theta_j N_e^{(\hat{p}_i,\hat{q}_j,r')} \geq \min_{i,j} N_e^{(\hat{p}_i,\hat{q}_j,r')} = N_e^{(p\prime,q\prime,r\prime)} \ \blacksquare \tag{38}$$

Z lemo 2 pokažemo, da za minimizacijo zadošča deterministična strategija brez skupne naključnosti.

Lema 3: Naj bo (p, q, r) deterministična strategija za generiranje prstnih odtisov brez skupne naključnosti in z enostransko napako. Potem

$$N_e^{(p,q,r)} \geq \ k\lceil n/m\rceil^2 + (m-k)\lfloor n-m\rfloor^2 - n, \tag{39}$$

kjer je $k = n \bmod m$. Enakost velja za strategijo:

$$r(a,b) = \delta(a,b), p(a|x) = q(b|y) = \begin{cases} 1; \ a-1 \equiv x-1 \bmod m \\ 0; \ \text{sicer} \end{cases} \tag{40}$$

Dokaz: Za Rogerja je optimalno, če uporabi strategijo opisano v lemi 1. Naj Alica in Bob uporabljata deterministični strategiji. Sprememba sporočila v prstni odtis je opisana s funkcijo $f\colon\{1,\dots,n\} \to \{1,..,m\}$. Natančneje $p(a|x) \equiv \delta(f^{(p)}(x), a)$ in $q(b|y) \equiv \delta(f^{(q)}(y), b)$, kjer sta $f^{(p)}$ in $f^{(q)}$ Alicini in Bobovi funkciji za generiranje prstnih odtisov. Tedaj je Rogerjeva strategija

$$r(a,b) = \begin{cases} 1;\ \exists x\colon f^{(p)}(x) = a\ \wedge\ f^{(q)}(x) = b \\ 0;\ \text{sicer} \end{cases} \tag{41}$$

Definirajmo sledeči množici sporočil:

$$M_a^{(p)} \equiv \left\{x \middle| f^{(p)}(x) = a\right\} \text{ in } M_b^{(q)} \equiv \left\{y \middle| f^{(q)}(y) = b\right\}. \tag{42}$$

Tedaj naj bo

$$s_{ab} \equiv \left|M_a^{(p)} \cap M_b^{(q)}\right| \text{ in } d_{ab} \equiv \left|M_a^{(p)}\right|\left|M_b^{(q)}\right| - s_{ab} \tag{43}$$

Ker $\{M_a^{(p)}\}_{a=1}^m$ in $\{M_b^{(q)}\}_{b=1}^m$ razdelijo množico $\{1, \dots, n\}$ na particije, veljajo naslednje enakosti:

$$\sum_a s_{ab} = \left|M_b^{(q)}\right|, \sum_b s_{ab} = \left|M_a^{(p)}\right|, \sum_{a,b} s_{ab} = n \tag{44}$$

in zato velja naslednja enačba:

$$d_{ab} \equiv \left(\sum_{i,j} s_{ai} s_{jb}\right) - s_{ab}. \tag{45}$$

Število vseh parov sporočil, ki katerih pride do napake je tedaj:

$$N_e^{(p,q,r)} = \sum_{a,b} d_{ab} r(a,b) = \left(\sum_{a,b,i,j} s_{ai} s_{jb} r(a,b)\right) - n = F(s) - n. \tag{46}$$

Minimizirajmo matriko $F(s)$ med vsemi $m \times m$ matrikami z nenegativnimi celoštevilskimi elementi za katere velja, da je $\sum_{a,b} s_{ab} = n$. Privzemimo, da je s diagonalen [2]. Če je s diagonalen, potem pridemo do minimuma $F(s) = \sum_a s_{aa}^2$ pri pogoju $\sum_a s_{aa} = n$, če $s_{aa} = \lceil n/m \rceil$ za k vnosov in $s_{aa} = \lfloor n/m \rfloor$ za $m - k$ vnosov, iz česar lahko izpeljemo originalno enačbo. ■

Izrek 4: Naj bo (p, q, r) strategija za generiranje prstnega odtisa z skupno naključnostjo in enostransko napako. Potem velja

$$P_{wce}^{(p,q,r)} \geq \frac{k\lceil n/m \rceil^2 + (m-k)\lfloor n-m \rfloor^2 - n}{n^2 - n}, \tag{47}$$

kjer je $k = n \bmod m$. Enakost velja v primeru, ko Alica in Bob uporabljata deterministično strategijo iz leme 3 potem, ko nad sporočilom, prejetim od Sabine, izvedeta naključno permutacijo vseh možnih sporočil. Katero permutacijo bosta uporabila, je odvisno od skupne naključnosti. Strategija, je tedaj:

$$\begin{gathered} r(a,b) = \delta(a,b) \text{ in} \\ p(a|x,\xi) = q(b|y,\xi) = \begin{cases} 1; & \text{če } \pi_\xi(a) - 1 \equiv x - 1 \bmod m \\ 0; & \text{sicer} \end{cases} \end{gathered} \tag{48}$$

kjer je π_ξ ena od $n!$ različnih permutacij vseh možnih sporočil, in za skupno naključnost velja $\sigma(\xi) = 1/n!$ za $1 \leq \xi \leq n!$ (0 v drugih primerih).

Dokaz: Povprečno verjetnost napake pri strategiji z enostransko napako pri vseh neenakih parih sporočil definiramo z $N_e^{(p,q,r)}/(n^2 - n)$. Ta vrednost nam poda spodnjo mejo napake v najslabšem primeru in zato po lemi 2 in 3 velja:

$$P_{wce}^{(p,q,r)} \geq \frac{N_e^{(p,q,r)}}{(n^2 - n)} \geq \frac{k\lceil n/m \rceil^2 + (m-k)\lfloor n-m \rfloor^2 - n}{n^2 - n} \tag{49}$$

Prva neenakost velja, če Alica in Bob permutirata x in y z naključno permutacijo preden generirata prstne odtise, druga neenakost pa če uporabljata deterministično strategijo iz leme 3. ■

Poglejmo si še zahtevnost komunikacije v primeru, ko drži enakost enačbe (47). Potem je $P_{wce} < 1/m$ in posledično $\log_2(1/\epsilon) = O(1)$ bitov za prstni odtis je potrebnih, da omejimo napako $P_{wce} < \epsilon$ za katerikoli $\epsilon > 0$. Zgornji protokol zahteva $\log_2(n!) = O(2^N N)$ bitov skupne naključnosti, kjer je $N = \log_2 n$. Za zmanjšanje potrebne skupne naključnosti si poglejte [2].

3.2.2 Kvantni protokol s prepletenostjo

Zamenjajmo Alicin in Bobov prstni odtis a in b ter verjetnostni porazdelitvi $p(a|x,\xi)$ in $q(b|y,\xi)$ s kvantnima stanjema $\hat{\rho}(x,\hat{\sigma})$ in $\hat{\tau}(y,\hat{\sigma})$ m dimenzionalnega Hilbertovega prostora $\mathcal{H}_m$. Skupno naključnost $\sigma(\xi)$ zamenjamo z prepletenim kvantnim stanjem $\hat{\sigma}$, ki pripada tenzorskemu produktu prostorov $\mathcal{H}_{d_A} \otimes \mathcal{H}_{d_B}$, kjer $\mathcal{H}_{d_A}$ pripada Alici in $\mathcal{H}_{d_B}$ Bobu. Naj bosta $d_a = d_b = d$ in definirajmo maksimalno prepleteno stanje v prostoru $\mathcal{H}_d \otimes \mathcal{H}_d$ kot $|\psi_+^{(d)}\rangle = d^{-1/2} \sum_{k=1}^{d} |k_A\rangle \otimes |k_B\rangle$, kjer so $|k_A\rangle$ in $|k_B\rangle$ osnovne baze za Alico in Boba. Ker uporabljata enake baze, bomo pisali kar $|k\rangle$.

Izrek 5: Kadar je $n \leq m^2$ obstaja strategija generiranja kvantnih prstnih odtisov brez napake s prepletenostjo $\hat{\sigma} = |\psi_+^{(d)}\rangle\langle\psi_+^{(d)}|$.

Dokaz: Naj bo $\{U_x\}_{x=1}^{m^2}$ baza ortonormiranih unitarnih operatorjev nad $End(\mathcal{H}_m)$ - prostorom vseh linearnih operatorjev nad $\mathcal{H}_m$. Velja $tr(U_x^\dagger U_y) = m\delta_{xy}$. Primer take baze je (54)kjer je $n = m^2$. Ko Alica in Bob prejmeta Sabinini sporočili x in y, vsak izvede na svojem delu $|\psi_+^{(d)}\rangle$ unitarni operaciji U_x^* in U_y, kjer je konjugacija narejena v računski bazi, ter pošljeta rezultat Rogerju. Ker velja

$$\begin{aligned}\left\langle\psi_+^{(m)}\middle|U_x^* \otimes U_y\middle|\psi_+^{(m)}\right\rangle &= \frac{1}{m}\sum_{j,k}\langle j|U_x|k\rangle^*\langle k|U_y|j\rangle \\ &= \frac{1}{m}\sum_{j,k}\langle j|U_x^\dagger|k\rangle\langle k|U_y|j\rangle \\ &= \frac{1}{m}\mathrm{tr}(U_x^\dagger U_y) \\ &= \delta_{xy}\end{aligned} \tag{50}$$

je stanje, ki ga prejme Roger, enako $|\psi_+^{(m)}\rangle$ natanko tedaj, ko je $x = y$, in ortogonalno na $|\psi_+^{(m)}\rangle$, ko je $x \neq y$. Z meritvijo s projekcijo na $\{P_1 = |\psi_+^{(d)}\rangle\langle\psi_+^{(d)}|, P_0 = 1 - P_1\}$ lahko Roger brez napake ugotovi enakost. ■

Kvantni protokol za generiranje prstnih odtisov uporabljen pri izreku 5 lahko razširimo tudi na primer, kjer je $n > m^2$ z reformulacijo klasične strategije, uporabljene v prejšnjem poglavju, kjer je število skupin m^2 namesto m. Verjetnost napake v najslabšem primeru za ta protokol je

$$P_{wce} = \frac{k\lceil n/m^2\rceil^2 + (m^2 - k)\lfloor n - m^2\rfloor^2 - n}{n^2 - n}, \tag{51}$$

kjer je $k = n \bmod m^2$.

Verjetnost napake lahko izboljšamo, če za vsak $\epsilon > 0$ ugotovimo, koliko unitarnih operatorjev U_x lahko skonstruiramo, da velja $\sum_{x,y}\left|tr(U_x^\dagger U_y)\right|^2 \leq \varepsilon$. Pokažemo lahko, da velja

$$\sum_{x,y=1}^{n}\left|\mathrm{tr}(E_x^\dagger E_y)\right|^2 \geq n^2 \tag{52}$$

za katerokoli množico $\{E_x\}_{x=1}^n \subset End(\mathcal{H}_m)$ za $n \geq m^2$ linearnih operatorjev, za katere velja $\forall\, x\colon tr(E_x^\dagger E_x) = m$. Dokaz je osnovan na obstoju unitarnih operatorjev, ki dosežejo to mejo. Kadar velja $n = lm^2$, kjer je $l \in \mathbb{Z}^+$, se napaki pri enačbi (51) in enačbi (53) ujemata zaradi dejstva, da l kopij ortonormirane baze unitarnih operatorjev zasiči neenakost.

Izrek 6: Kadar $n \geq m^2$, obstaja strategija za generiranje kvantnih prstnih odtisov z prepletenstjo $\hat{\sigma} = |\psi_+^{(m)}\rangle\langle\psi_+^{(m)}| \otimes |\psi_+^{(n!)}\rangle\langle\psi_+^{(n!)}|$ in z verjetnostjo napake v najslabšem primeru enako

$$P_{wce} = \frac{n/m^2 - 1}{n - 1} \tag{53}$$

Dokaz: Za $n \geq m^2$ definirjamo množico $\{U_x\}_{x=1}^{n} \subset End(\mathcal{H}_m)$ unitarnih operatorjev z komponentami matrike

$$\langle j|U_x|k\rangle = \frac{1}{\sqrt{m}} \exp\left[\frac{2\pi ijk}{m} + \frac{2\pi i(j + mk)x}{n}\right], \tag{54}$$

kjer je $i = \sqrt{-1}$. Kadar je $n = m^2$, $\{U_x\}_{x=1}^{m^2}$ tvori ortonormalno bazo unitarnih operatojev. Pokažemo lahko, da velja unitarnost operatorjev

$$\begin{aligned} \left\langle j\middle|U_x^\dagger U_x\middle|k\right\rangle &= \sum_{l=1}^{m} \langle l|U_x|j\rangle^* \langle l|U_x|k\rangle \\ &= \frac{1}{m}\sum_{l=1}^{m} \exp\left[\frac{2\pi i(k-j)l}{m} + \frac{2\pi im(k-j)x}{n}\right] \\ &= \delta_{jk} \end{aligned} \tag{55}$$

ortogonalnost kadar je $n = m^2$

$$\begin{aligned} tr\left[U_x^\dagger U_y\right] &= \sum_{j,k=1}^{m} \langle j|U_x|k\rangle^* \left\langle j\middle|U_y\middle|k\right\rangle \\ &= \frac{1}{m}\sum_{j,k=1}^{m} \exp\left[\frac{2\pi i(j + mk)(x - y)}{n}\right] \\ &= \frac{1}{m}\sum_{l=1}^{m} \exp\left[\frac{2\pi i(l + m)(x - y)}{m^2}\right] \\ &= m\delta_{xy} \end{aligned} \tag{56}$$

in da velja

$$\begin{aligned}\sum_{x,y=1}^{n}\left|tr\left[U_x^{\dagger}U_y\right]\right|^2 &= \sum_{x,y=1}^{n}\sum_{j,k,p,q=1}^{m}\langle j|U_x|k\rangle^{*}\langle j|U_y|k\rangle\langle p|U_x|q\rangle\langle p|U_y|q\rangle^{*}\\ &= \frac{1}{m^2}\sum_{x,y=1}^{n}\sum_{j,k,p,q=1}^{m}\exp\left[\frac{2\pi i\big(p-j+m(q-k)\big)(x-y)}{n}\right]\\ &= \frac{n^2}{m^2}\sum_{j,k,p,q=1}^{m}\delta_{jp}\delta_{qk}\\ &= n^2\end{aligned} \tag{57}$$

kadar je $n \geq m^2$.

Da dosežemo mejo podano v enačbi (53), Alica in Bob najprej pretvorita prepleteno kvantno stanje $|\psi_+^{(n!)}\rangle$ v skupen ključ $\xi \in \{1, \dots, n!\}$ z lokalnimi meritvami v računski bazi. Nato uporabita ξ, da izbereta eno izmed $n!$ različnih permutacij Sabininih sporočil π_ξ. Prepleteno stanje $|\psi_+^{(m)}\rangle$ se uporabi na podoben način kot pri izreku 5. Alica in Bob izvedeta lokalni operaciji $U^*_{\pi_\xi(x)} \otimes U_{\pi_\xi(y)}$ nad $|\psi_+^{(m)}\rangle$, kjer je U_x definiran z enačbo (54) in pošljeta rezultat Rogerju. Roger izvede projekcijsko meritev $\left\{P_1 = \left|\psi_+^{(m)}\right\rangle\!\left\langle\psi_+^{(m)}\right|, P_0 = 1 - P_1\right\}$ z rezultatom 1 z verjetnostjo

$$\begin{aligned}p(1) &= \frac{1}{n^2-n}\sum_{x\neq y}\left|\left\langle\psi_+^{(m)}\middle|U^*_{\pi_\xi(x)}\otimes U_{\pi_\xi(y)}\middle|\psi_+^{(m)}\right\rangle\right|^2\\ &= \frac{1}{n^2-n}\left(\frac{1}{m^2}\sum_{x,y}\left|tr\left[U_x^{\dagger}U_y\right]\right|^2 - n\right)\\ &= \frac{n^2/m^2-n}{n^2-n}\end{aligned} \tag{58}$$

kadar $x \neq y$, in

$$\begin{aligned}p(1) &= \frac{1}{n}\sum_{x}\left|\left\langle\psi_+^{(m)}\middle|U^*_{\pi_\xi(x)}\otimes U_{\pi_\xi(x)}\middle|\psi_+^{(m)}\right\rangle\right|^2\\ &= \frac{1}{n}\left(\frac{1}{m^2}\sum_{x}\left|tr\left[U_x^{\dagger}U_x\right]\right|^2\right)\\ &= 1\end{aligned} \tag{59}$$

kadar $x = y$. ■

3.3 Kvantni protokol za generiranje prstnih odtisov s ponavljanjem

Poglejmo si še primer protokola, ki ne uporablja prepletenosti. Pokažemo lahko, da je za tak protokol potrebno $O(log_2 n)$ qubitov za prstni odtis, kar je eksponentno boljše od klasičnih

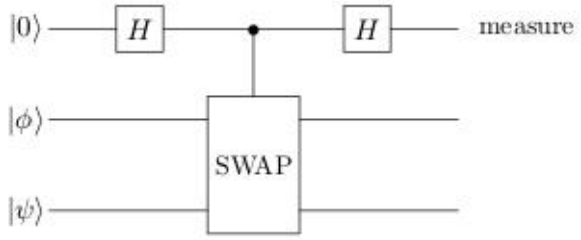
protokolov, za katere vemo, da je potrebno $\Theta(\sqrt{n})$ bitov glede na velikost vhoda [1]. Spodaj opisana metoda temelji na klasičnih kodih za odpravljanje napak.

3.3.1 Preverjanje enakosti kvantnih stanj

V uvodu smo pri postulatu št. 3 smo pokazali, da je razločevanje kvantnih stanj netrivialen problem. Pokazali smo tudi, da je neortogonalna stanja nemogoče popolnoma ločiti med seboj. Kljub temu obstaja kvantno vezje, ki nam omogoča ločevanje med kvantnimi stanji z enostransko napako. Preden si pogledamo to vezje in njegove lastnosti je potrebno povedati še nekaj v kvantnih vezjih.

Klasična vezja so sestavljena iz vodil, ki prenašajo informacijo in logičnih vrat, ki manipulirajo informacijo – spreminjajo jo iz ene oblike v drugo. Kvantna vezja so sestavljena na podoben način. Tudi v kvantnih vezjih je prisotno *vodilo*, ki pa ne nujno predstavlja fizičnega vodila. Lahko predstavlja tok časa, ali premik fizičnega delca (npr. fotona) skozi prostor. Namesto logičnih vrat imamo qubitna vrata, ki lahko operirajo nad enim ali več qubitov. Kot smo že v postulatu št. 2 omenili, je edini pogoj za veljavnost qubitnih vrat to, da je operator unitaren. Kvantna vezja imajo tudi nekaj omejitev, ki niso prisotne v klasičnih vezjih. Ne moremo ustvarjati ciklov, ni dovoljeno združevanje vodil (s tem lahko realiziramo v klasičnem vezju bitni ali) in ne moremo razcepiti vodil (v klasičnih vezjih lahko s tem dobimo kopje bita, kar pa kvantna mehanika prepoveduje). Velja omeniti tudi, da se sheme kvantnih vezij bere od leve proti desni in da so začetna stanja vhodov $|0\rangle$, če ni drugače omenjeno.

Vezje s katerim je mogoče preveriti enakost kvantnih stanj z enostransko napako se imenuje QSTC (ang. quantum swap test circuit). Njegova shema je sledeča:



Sestavljeno je iz dveh različnih kvantnih vrat – *Hadamardovih* (simbol *H*) in *Fredkinovih vrat* (SWAP simbol).

Hadamardova vrata so že bila omenjena v poglavju o osnovah kvantne mehanike, zato samo spomnimo, da je transformacijka matrika enaka

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{60}$$

Fredkinova vrata so 3-qubitna vrata, ki opravijo nadzorovano zamenjavo zadnjih dveh qubitov glede na stanje prvega (ang. CSWAP gate). Ker ta vrata operirajo na treh qubitih, je prostor stanj vhoda in izhoda enak $V \otimes V \otimes V$ s pripadajočo ortonormirano bazo

$\{|0\rangle|0\rangle|0\rangle, |0\rangle|0\rangle|1\rangle, |0\rangle|1\rangle|0\rangle, \dots, |1\rangle|1\rangle|0\rangle, |1\rangle|1\rangle|1\rangle\}$. Prostor stanj je dimenzije 8. Transformacijska matrika, ki pripada temu operatorju je:

$$F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{61}$$

Ker je $F^\dagger = F$, lahko brez težav preverimo da je matrika unitarna.

S Fredkinovimi vrati opravimo sledečo transformacijo glede na prvi qubit:

$$|0\rangle|\varphi\rangle|\phi\rangle \rightarrow |0\rangle|\varphi\rangle|\phi\rangle, \tag{62}$$

$$|1\rangle|\varphi\rangle|\phi\rangle \rightarrow |0\rangle|\phi\rangle|\varphi\rangle. \tag{63}$$

Sedaj si poglejmo še delovanje celotnega QSTC vezja. Začetno stanje sistema je

$$|\psi\rangle = |0\rangle|\varphi\rangle|\phi\rangle, \tag{64}$$

kjer sta $|\varphi\rangle$ in $|\phi\rangle$ stanji, ki ju želimo primerjati med seboj. Po prvih Hadamardovih vratih je sistem v stanju

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\varphi\rangle|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\varphi\rangle|\phi\rangle + |1\rangle|\varphi\rangle|\phi\rangle) \tag{65}$$

Po prehodu skozi Fredkinova vrata sistem preide v stanje

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\varphi\rangle|\phi\rangle + |1\rangle|\phi\rangle|\varphi\rangle) \tag{66}$$

Po prehodu prvega qubita skozi zadnja Hadamardova vrata je končno stanje sistema

$$\begin{aligned} |\psi\rangle &= \frac{1}{2}[(|0\rangle + |1\rangle)|\varphi\rangle|\phi\rangle + (|0\rangle - |1\rangle)|\phi\rangle|\varphi\rangle)] \\ &= \frac{1}{2}[|0\rangle(|\varphi\rangle|\phi\rangle + |\phi\rangle|\varphi\rangle) + |1\rangle(|\varphi\rangle|\phi\rangle - |\phi\rangle|\varphi\rangle)] \end{aligned} \tag{67}$$

Ko je sistem v tem stanju, izmerimo njegov prvi qubit v bazi $|0\rangle$, $|1\rangle$. Iz enačbe končnega stanja brez težav vidimo, da bo v primeru, da sta stanji $|\varphi\rangle$ in $|\phi\rangle$ enaki, rezultat meritve vedno 1, v nasprotnem primeru pa bo 0 ali 1. Verjetnost, da izmerimo1, je enaka:

$$p(1) = \frac{1}{2} + \frac{|\langle\varphi|\phi\rangle|^2}{2} \tag{68}$$

Če sta $|\varphi\rangle$ in $|\phi\rangle$ ortogonalna, je verjetnost, da izmerim 1 natanko $\frac{1}{2}$. Algoritem, ki ga izvede to vezje je primer algoritma Monte Carlo z enostransko napako. Verjetnost napake pri različnih kvantnih stanjih je na intervalu $\left[\frac{1}{2}, 1\right)$.

3.3.2 Algoritem za kvantne prstne odtise s ponavljanjem

Naj bo kod za odpravljanje napak podan z $E: \{0,1\}^n \to \{0,1\}^m$ za vsak n, kjer je $m = cn$ za konstanten $c > 1$ in je razdalja med $E(x)$ in $E(y)$ vsaj $(1 - \varepsilon)m$ za različna x in y ter $\varepsilon < 1$. Primer takega koda je Justesenov kod, za katerega velja $\epsilon < 9/10 + 1/(15c)$ za katerikoli izbrani $c > 2$. Definirajmo za kakršenkoli n $(log_2 m + 1)$ qubitno stanje

$$|h_x\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle|E_i(x)\rangle \tag{69}$$

za vsak $x \in \{0,1\}^n$. Ker sta dve kodni besedi lahko enaki na največ εm mestih za vsak $x \neq y$, velja $\langle h_x | h_y \rangle \leq \varepsilon m/m = \varepsilon$. Tako imamo 2^n različnih $(log_2 n + O(1))$ qubitnih stanj in vsak par med njimi ima skalarni produkt največ ε.

Ko Alica in Bob prejmeta sporočili x in y, pošljeta $|h_x\rangle$ in $|h_y\rangle$ sodniku, ki nad prejetima kvantnima stanjema izvede QSTC opisan v prejšnjem poglavju. Meritev prvega qubita bo vrnila 1 z verjetnostjo $p(1) = \frac{1}{2} - \frac{|\langle\varphi|\phi\rangle|^2}{2}$. Ta verjetnost je 0 kadar $x = y$ in vsaj $\frac{1}{2}(1 - \varepsilon^2) > 0$ kadar $x \neq y$. Test tako določi enakost z enostransko napako $\frac{1}{2}(1 - \varepsilon^2)$.

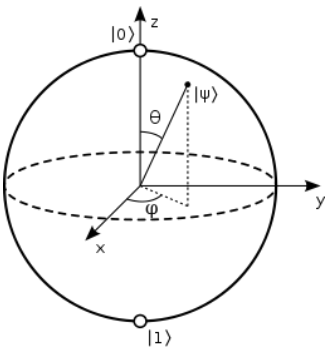
Verjetnost napake lahko zmanjšamo na katerikoli $\delta > 0$, če prstni odtis za $x \in \{0,1\}^n$ na $|h_x\rangle^{\otimes k}$ za ustrezen $k \in O(\log_2(1/\delta))$. S takim prstnim odtisom lahko sodnik izvede k neodvisnih testov, zaradi česar dobimo verjetnost napake manjšo od δ. V tem primeru je velikost kvantnih prstnih odtisov $O((\log_2 n)(\log_2(1/\delta))$.

4. Eksperimentalni rezultati z generiranjem kvantnih prstnih odtisov

Na inštitutu za kvantno informacijsko znanost, univerza Calgary s sedežem v Kanadi, so izvedli poskus eno qubitnega protokola za generiranje prstnih odtisov s fotoni. V tej optični shemi imata Alica in Bob enotni skupni vir fotonov, sporočilo Sabine pa se interpretira kot navodilo spremembe polarizacije teh fotonov.

4.1 Kvantno enkodiranje

Kvantno enkodiranje je protokol po katerem zapisujemo informacijo v qubite. Kot smo omenili že v uvodu je vsak qubit sestavljen iz superpozicije dveh vektorjev v Hilbertovem prostoru, označenih z $|0\rangle$ in $|1\rangle$, kar lahko zapišemo tudi kot $|\theta,\phi\rangle = \cos\theta|0\rangle + e^{i\phi}|1\rangle$. Če si to stanje predstavljamo kot točke na sferi, potem je θ polarni kot in ϕ azimutni kot, stanje $|0\rangle$ ustreza $\theta = 0$ in stanje $|1\rangle$ ustreza $\theta = \pi/2$.



Omenili smo že, da je mogoče popolnoma razločiti le ortogonalna kvantna stanja. Ortogonalnost v zgornjem zapisu izrazimo s funkcijo prekrivanja[4]

$$\delta = |\langle\theta',\phi'|\theta,\phi\rangle|^2 = \left|\cos\frac{\theta'}{2}\cos\frac{\theta}{2} + e^{i(\phi-\phi')}\sin\frac{\theta'}{2}\sin\frac{\theta}{2}\right|^2 \tag{70}$$

ki vrne 1 za identična stanja in 0 za ortogonalna stanja.

Za protokol so uporabili tetraederno kodiranje s štirimi kvantnimi stanji $|0,0\rangle$ in $|2\cos^{-1}\left(3^{-\frac{1}{2}}\right), 2\pi l/3\rangle$, kjer je $l = \{1,2,3\}$. Ta stanja so maksimalno oddaljena med seboj na sferi in funkcija prekrivanja $\delta = 1/3$ za vsak par stanj. Ker med seboj niso ortogonalna je razlikovanje med stanji omejeno.

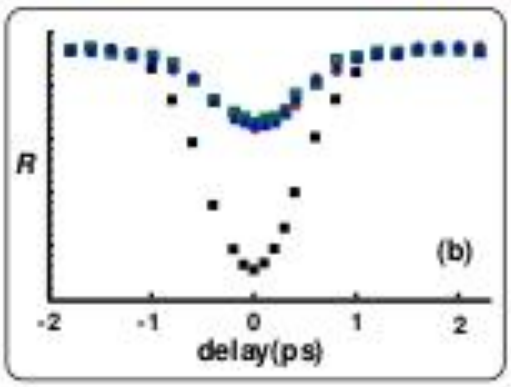
4.2 Enostranska napaka

Teoretično enostransko napako v najslabšem primeru lahko enostavno izračunamo, če sledimo postavitvi protokola iz poglavja 2 o kvantnih algoritmih s prepletenostjo in uporabimo QSTC za meritev. Zlobna Sabina bo vedno odposlala različni sporočili in v primeru, da Alica in Bob uporabljata prstne odtise s štirimi možnimi stanji in kodirata v qubit z uporabo tetraedernega kodiranja bo Roger vrnil 1 z verjetnostjo $2/3$ (verjetnost lahko izračunamo z uporabo enačbe (68)).

[4] Funkcijo prekrivanja smo že zasledili kot del enačbe (68) pri QSTC

4.3 Optična shema

Alica in Bob glede na prejeti sporočili spremenita polarizacijo svojih fotonov in ju pošljeta Rogerju. Njegova naloga je preveriti enakost polarizacije. V idealni shemi se uporablja QSTC za preverjanje enakosti, vendar je optična realizacija takega sistema prezapletena. Namesto teoretičnega vezja so tako uporabili kar cepilec svetlobnega žarka (ang. beam splitter). Primer takega cepilca je pol posrebreno steklo. Roger usmeri fotona skozi cepilec, ki usmeri foton v eno izmed dveh smeri z verjetnostjo $1/2$. Če sta fotona enaka, bosta oba izšla iz cepilca na isti strani in ne bosta generirala skupnega dogodka na detektorjih na vsakem izhodu cepilca. Roger bo tako vrnil 1, če skupnega dogodka ne zabeleži in 0, če detektorji zaznajo oba fotona.



Teoretična napaka je $2/3$ in je identična za QSTC in optični test. V eksperimentu se je sicer pojavila dvostranska napaka zaradi omejitev Hong-ou-Mandel dip naprave (naprava, ki opravi optični test). Vseeno se jasno vidi meja med enakimi in različnimi kvantnimi stanji: globina pri različnih stanjih je vsaj 88% in globina pri različnih je blizu pričakovane $1/3$. Omejitev je sicer v tem, da trenutno še ni mogoče opremiti Alice in Boba z samostojnimi viri posamičnih fotonov na zahtevo. V tem poskusu so uporabili SPDC kristal (ang. spontaneous parametric down converter crystal), ki sočasno proizvede par fotonov za Alico in Boba, vendar je čas emisije naključen.

5. Zaključek

V tem projektu sem pokazal dva algoritma za generiranje kvantnih prstnih odtisov in njuni verjetnosti napake v najslabšem primeru. V protokolu s prepletenostjo smo pokazali obstoj kvantnega stanja dimenzije m, kje je $m < n$ in je n število vseh mogočih sporočil. Za dimenzijo m velja, da če je velikosti $\sqrt[2]{m'}$, kjer je m' dolžina klasičnega algoritma, dobimo isto napako. Kvantno algoritem tako omogoča večjo kompresijo informacije, vendar je trenutno še nemogoče sestaviti kvantno stanje, ki bi ustrezalo pogojem za poljuben m. Drugi protokol, ki uporablja večkratne meritve uporablja qubite, ki so dvodimenzionalna kvantna stanja. Pokazali smo, da zadošča za tak prstni odtis $O(\log_2 n)$ qubitov v primerjavi s $\Theta(\sqrt[2]{n})$ navadnih bitov a klasičnih protokolih, kjer je n velikost vhoda. Velja pa poudariti, da ima ta protokol enostransko napako pri preverjanju enakosti kvantnih stanj. Razlog za to je v naravi kvantne fizike, v kateri je nemogoče popolnoma razločevati kvantna stanja, ki niso med seboj ortogonalna. Zaradi te lastnosti lahko preverjanje vrne, da prstna odtisa nista enaka, čeprav sta z verjetnostjo $p > 0$.

Poleg modela SMP obstajata še dva druga modela, enosmerno komuniciranje in večpotezno dvostransko komuniciranje za katera bi si bilo zanimivo pogledati lastnosti kvantnih prstnih odtisov. Vsi ti model so teoretični in primanjkuje jim eksperimentalnih potrditev. Težava je namreč v tem, da s trenutno tehnologijo lahko realiziramo le najpreprostejše kvantne sisteme. Zato za dokončno potrditev matematičnih modelov kvantne mehanike in moči kvantnega procesiranja še čakamo. Upamo, da bomo nekoč v prihodnosti lahko uporabljali kvantno procesiranje in z njim kvantne prstne odtise tako, kot danes uporabljamo klasične algoritme.

6. Literatura

[1] Buhrman, H. a. (2001). Quantum Fingerprinting. *Phys. Rev. Lett. , 87* (16), 167902.

[2] Horn, R. T. (2005). Classical and quantum fingerprinting with shared randomness and one-sided error. *Quantum Info. Comput. , 5* (3), 258-271.

[3] Nielsen, M. A. (2000). *Quantum Computation and Quantum Information.* Cambridge: Cambridge University Press.

[4] Sanders, B., & Inst. for Quantum Inf. Sci., C. U. (2005). Classical vs Quantum Fingerprinting. *Proceedings of the 35th International Symposium on Multiple-Valued Logic* (str. 2-5). Washington, DC: IEEE Computer Society.