Univerzitet u Tuzli
Prirodno-matematički fakultet
Odsjek: Fizika

Sabina Bahić

ZAVRŠNI RAD

prvog ciklusa studija

Kvantna spregnutost i kvantna informacija

Tuzla, april 2019.

Mentor: *dr. sc. Hedim Osmanović, vanredni profesor*

Broj stranica: *43*

Redni broj završnog rada:

Abstract

The fundamental purpose of this thesis is the examination of quantum entanglement and quantum information, in the framework of previous findings within this domain. The Einstein-Podolski-Rosen (EPR) argument is presented in a detailed, as well as in a summarized version, followed by Bell inequalities, in which the paradoxical nature of that argument is visible.

In the context of quantum information, quantum entropy is defined, as well as the qubit, the smallest unit of quantum information, which is of key importance for quantum communication, in a form of comparison to the classical case.

Aiming to present the practical side of this unusual quantum-mechanical behavior, quantum teleportation is described, including the entanglement swapping phenomenon, as well as some of the recent experiments. With the same goal, quantum cryptography is described, within which the BB84 protocol (one of the ways for quantum key distribution-QKD) is presented in a relatively simple way.

Some of the mathematical tools that are necesarry for studying entanglement are decribed as well. Through the separability problem, the difference between entangled and unentangled states is explained. Some of the chapters include simplified summaries of the main subject of the given chapter (EPR paradox), while some of the chapters are completely written in a way that is understadable without a deep knowledge of mathematics behind them (e. g. quantum teleportation, and a significant part of the quantum cryptography chapter).

The desire behind this paper is to present the unusual quantum phenomenon, at least partly in a way to inspire teachers to include a story about quantum mechanics in their plan and programme, which is, without a doubt, achieveable. For example, it is possible to describe many concepts in quantum mechanics, without a need for complicated mathematical tools, by using a qubit. Further, it is possible to present the practical side of quantum mechanics, using the entanglement phenomena, that is, using quantum teleportation, a term that was, not so far in the past, associated only to science fiction. For that reason, it is practical for such a piece of literature to be available in BHS language. The phenomenon of quantum entanglement has brought a lot of things to be questioned, but the doubt is the thing that makes room for growth, and represents the beauty of every natural science.

Keywords: quantum entanglement, quantum information, quantum teleportation, quantum cryptography

Sažetak

Glavni cilj ovog rada je proučavanje teorije kvantne spregnutosti i kvantne informacije, u okviru dosadašnjih saznanja u ovoj oblasti. Predstavljen je Einstein-Podolski-Rosen (EPR) argument u opširnijoj i sažetoj verziji, nakon čega je definisana suština paradoksa tog argumenta, kroz Bell-ove nejednakosti.

Kada je u pitanju kvantna informacija, u formi poređenja sa klasičnim slučajem, obrađena je kvantna entropija, i predstavljen je qubit, najmanja jedinica kvantne informacije, koji je ključan za kvantnu komunikaciju.

S ciljem predstavljanja praktične strane ovog neobičnog kvantnomehaničkog fenomena, opisana je kvantna teleportacija, u sklopu koje je predstavljen i fenomen zamjene spregnutosti, kao i neki od nedavnih eksperimenata, a pored toga i kvantna kriptografija, unutar koje je opisan BB84 protokol, koji predstavlja jedan od načina distribucije kvantnog ključa, na relativno jednostavan način.

Opisani su i neki od matematičkih alata, potrebnih za proučavanje spregnutosti, te je kroz problem separabilnosti pojašnjena razlika između spregnutih i nespregnutih stanja. Neka od poglavlja sadrže sažetke, u kojima je na pojednostavljen način predstavljen glavni problem datog poglavlja (EPR paradoks), a neka poglavlja su u potpunosti opisana na način da ih se može shvatiti i bez dubokog poznavanja matematičkog formalizma (na primjer, kvantna teleportacija, kao i značajan dio o kvantnoj kriptografiji).

Želja, koja se krije iza ovog rada, jeste da se predstave neobični kvantnomehanički fenomeni, barem dijelom na način koji bi potakao nastavnike da u svoj plan i program uvedu i priču o kvantnoj mehanici, što je bez sumnje moguće. Na primjer, pomoću qubita se može pojasniti mnogo toga, bez ikakve potrebe za komplikovanim matematičkim jezikom, a kroz teleportaciju se može predstaviti praktična strana ovog fenomena, donedavno vezanog samo za naučnu fantastiku. Iz tog razloga, praktično je da jedan djelić literature iz ove oblasti bude dostupan i na BHS jeziku. Fenomen kvantne spregnutosti je doveo mnogo toga u pitanje, a sumnja i stvara prostor za rast, i predstavlja raskoš svake prirodne nauke.

Ključne riječi: kvantna spregnutost, kvantna informacija, kvantna teleportacija, kvantna kriptografija

Sadržaj

1 Uvod

1.1 Einstein-Podolski-Rosen argument (EPR argument)

Analizom kvantnih stanja složenih sistema, Albert Eistein, Boris Podolski i Nathan Rosen su predstavili svoj argument, koji se odnosi na nekompletnost kvantnomehaničkog opisa mikroskopskog svijeta. Kvantna mehanika, prema njima, nije potpuna teorija, a za njen potpun opis su potrebne dodatne, skrivene varijable, koje bi u teoriju ponovo uvele kauzalnost i lokalnost. Naglasak je na neobičnoj prirodi spregnutih kvantnomehaničkih stanja. Međutim, ova ideja je nekompatibilna sa statističkim predviđanjima kvantne mehanike. Zahtjeva se lokalnost, odnosno, na rezultat mjerenja na jednom sistemu ne smiju uticati radnje na drugom, udaljenom sistemu (ova dva sistema imaju zajedničku *prošlost*).

Smisao EPR argumenta se može obuhvatiti sljedećim uslovima (pretpostavkama):

(i) Separabilnost: U klasičnoj fizici je poznato samo međudjelovanje objekata u direktnom kontaktu (pod objektima se podrazumijevaju i polja). Stoga, ako su dva objekta razdvojena prostorno, dalje manipulacije na njima su potpuno nezavisne jedna od druge. Jednostavno, *prostorno razdvojeni objekti su, također, i fizički razdvojeni*. Ovo je pretpostavka, ali ona predstavlja temelj EPR argumenta. Separabilnost, stoga, znači da opisi dva prostorno razdvojena kvantna objekta trebaju biti potpuno nezavisna jedan od drugog.

(ii) Realnost: Prema Einsteinu, svaka dobro određena fizička veličina mora imati reprezentaciju u teoriji. Poanta leži u pitanju: Koje osobine su dobro određene? Za razliku od klasične mehanike, u kvantnoj mehanici, u principu, sve mjerljive veličine nemaju dobro određene osobine istovremeno. U kvantnoj mehanici se računaju vjerovatnoće (Richard Feynman: *Priroda nam dozvoljava da računamo samo vjerovatnoće*). Ako je moguće predvidjeti sa pouzdanošću (na primjer, sa vjerovatnoćom jednakoj jedinici) vrijednost fizičke veličine, bez ometanja sistema na bilo koji način, tada postoji element fizičke stvarnosti, koji odgovara ovoj veličini.

(iii) Savršena korelacija: Kada se stanja dva kvantna objekta mjere duž istog pravca, odgovarajući rezultati će biti suprotni.

(iv) Lokalnost: S obzirom na to da za vrijeme mjerenja, dva sistema više ne interaguju, nemoguće je da se dese bilo kakve značajne promjene u drugom sistemu, koje bi mogle biti posljedice bilo čega što bi moglo uticati na prvi sistem.

(v) Kompletnost: Svaki element fizičke stvarnosti mora imati *antielement* u fizičkoj teoriji.

Inicijalni EPR argument je dat u kontekstu kontinualnih osobina kvantnih sistema. Međutim, on se bolje uklapa u kontekst diskretnih osobina.

Bohmovo i Aharonovljevo pojednostavljenje

Bohm[1] i Aharonov[2] su posmatrali par čestica spina $\frac{1}{2}$, u singlet stanju koje se kreću slobodno, u suprotnim smjerovima. Singlet stanje ima ključnu ulogu u obradi kvantne informacije, čija je bitna osobina da zadržava isti oblik i kada se izrazi u bilo kojoj ortonormiranoj bazi, koju je moguće dobiti iz kompjutacione baze, tako što se rotira baza podsistema Hilbertovog prostora, za proizvoljan ugao, različit od nule.

Ovim pojednostavljenjem, EPR argument može biti predstavljen na sljedeći način:

- Ako prenosnik može izvršiti operaciju, koja mu dozvoljava da predvidi sa pouzdanošću rezultate mjerenja, bez uticaja na mjerenu česticu, tada mjerenje ima konačan ishod, bilo da je ova operacija zaista izvršena ili ne.

- Za par čestica u singlet stanju, postoji operacija koju prenosnik može izvršiti, dopuštajući da ishod mjerenja jednog podsistema bude određen, bez uticaja na drugu česticu.

Mjerenja se mogu izvršiti pomoću Stern-Gerlach magneta, na odabranim komponentama spina σ_1 i σ_2 . Ako se mjerenjem komponente $\sigma_1 a$ dobije vrijednost $+1$, onda se, prema kvantnoj mehanici, mjerenjem komponente $\sigma_2 a$ mora dobiti vrijednost -1, i obrnuto. Ovdje a predstavlja jedinični vektor. Postavlja se hipoteza: Ako su ova mjerenja izvršena na dva mjesta, koja su udaljena jedno od drugog, orijentacija jednog magneta ne utiče na rezultat dobijen drugim magnetom. S obzirom na to da možemo predvidjeti rezultat mjerenja bilo koje odabrane komponente σ_2, mjereći prije toga istu komponentu σ_1, slijedi da rezultat svakog ovakvog mjerenja mora biti predodređen. Početna talasna jednačina ne određuje rezultat pojedinačnog mjerenja; ova predodređenost nagovještava mogućnost potpunije specifikacije stanja. Sada se uvodi parametar λ, koji će uticati na kompletniju specifikaciju stanja. Parametar λ može biti jedna varijabla, set varijabli, čak

[1] David Bohm (20. 12. 1917.- 27. 10. 1992.), naučnik rođen u SAD, smatra se za najznačajnijeg teorijskog fizičara 20. vijeka. Dao je svoj doprinos neortodoksnoj kvantnoj teoriji, neuropsihologiji i filozofiji uma.

[2] Yakir Aharonov, profesor i kvantni fizičar, rođen 1932. godine, u Izraelu.

i set funkcija, diskretnih, ili kontinualnih. Za ovaj slučaj, pretpostavlja se kontinualna vrijednost parametra λ. Tada su rezultati A i B određeni na sljedeći način:

$$\begin{aligned} A(a,\lambda) &= \pm 1, \\ B(b,\lambda) &= \pm 1, \end{aligned} \tag{1.1.1}$$

gdje su a i b jedinični vektori. Ključno je pretpostaviti da rezultat B za drugu česticu ne zavisi od postavke a magneta za prvu česticu, kao što ni rezultat A za prvu česticu ne zavisi od postavke b magneta za drugu česticu.

Ako je $\rho(\lambda)$ raspodjela vjerovatnoće za parametar λ, onda je očekivana vrijednost proizvoda dvije komponente, $\sigma_1 a$ i $\sigma_2 b$, data sljedećim izrazom

$$P(a,b) = \int \rho(\lambda) A(a,\lambda) B(b,\lambda) d\lambda. \tag{1.1.2}$$

Ovo bi trebalo biti jednako kvantnomehahičkoj očekivanoj vrijednosti, koja za singlet stanje ima sljedeći oblik:

$$\langle \sigma_1 a \, \sigma_2 b \rangle = -ab. \tag{1.1.3}$$

Pokazat će se da je ovo nemoguće. S obzirom na to da je ρ normirana raspodjela vjerovatnoće,

$$\int \rho(\lambda) d\lambda = 1, \tag{1.1.4}$$

zbog osobina (1.1.1) i (1.1.2), vrijednost za očekivanu vrijednost $P(a,b)$ u relaciji (1.1.2) ne može biti manja od -1. Može biti -1 kada je $a = b$ samo ako je

$$A(a,\lambda) = -B(a,\lambda),$$

osim u tačkama nulte vjerovatnoće. Sa ovom pretpostavkom, relacija (1.1.2) se može zapisati na sljedeći način:

$$P(a,b) = -\int \rho(\lambda) A(a,\lambda) A(b,\lambda). \tag{1.1.5}$$

Ako je c jedan jedinični vektor, slijedi

$$\begin{aligned} P(a,b) - P(a,c) &= -\int \rho(\lambda) \left[A(a,\lambda) A(b,\lambda) - A(a,\lambda) - A(c,\lambda) \right] d\lambda \\ &= \int \rho(\lambda) A(a,\lambda) A(b,\lambda) \left[A(b,\lambda) A(c,\lambda) - 1 \right] d\lambda. \end{aligned} \tag{1.1.6}$$

Koristeći relaciju (1.1.2), može se pisati:

$$|P(a,b) - P(a,c)| \leq \int \rho(\lambda) \left[1 - A(b,\lambda) A(c,\lambda) \right] d\lambda. \tag{1.1.7}$$

Drugi član na desnoj strani je upravo $P(b,c)$, pa je

$$1 + P(b,c) \geq |P(a,b) - P(a,c)|\,. \tag{1.1.8}$$

Desna strana je, u opštem slučaju, reda $|b-c|$ za male vrijednosti $|b-c|$, osim u slučaju kada P ima konstantnu vrijednost. Stoga, $P(b,c)$ ne može biti stacionarno na minimalnoj vrijednosti (-1 za $b=c$), te ne može biti jednako kvantnomehaničkoj vrijednosti (1.1.3), niti se (1.1.3) može proizvoljno aproksimirati relacijom (1.1.2). Tehnički, dokaz se može prikazati na sljedeći način. Na izolovanim tačkama postoji mogućnost aproksimiranja, pa će se, umjesto relacija (1.1.2) i (1.1.3), razmatrati $\bar{P}(a,b)$ i $\overline{-a\cdot b}$. Oznakom "bar" je obilježeno nezavisno usrednjavanje $P(a^{'},b^{'})$ i $-a^{'}\cdot b^{'}$ preko vektora $a^{'}$ i $b^{'}$, unutar definisanih malih uglova između a i b. Pretpostavimo da je za svako a i b razlika ograničena sa ε:

$$\left|\bar{P}(a,b) + a\cdot b\right| \leq \varepsilon.$$

Pokazuje se da ε ne može biti proizvoljno malo. Ako se pretpostavi da za svako a i b vrijedi

$$\left|\overline{a\cdot b} - a\cdot b\right| \leq \delta,$$

iz prethodne relacije slijedi da je

$$\left|\bar{P}(a,b) + a\cdot b\right| \leq \varepsilon + \delta.$$

Iz relacije (1.1.2) slijedi

$$\bar{P}(a,b) = \int \rho(\lambda)\bar{A}(a,\lambda)\bar{B}(b,\lambda)d\lambda,$$

gdje su

$$\left|\bar{A}(a,\lambda) \leq 1\right| i\left|\bar{B}(b,\lambda)\right| \leq 1.$$

Iz prethodnih relacija, uz $a=b$,

$$\rho(\lambda)\left[\bar{A}(b,\lambda)\bar{B}(b,\lambda)+1\right]d\lambda \leq \varepsilon+\delta,$$

slijedi

$$\begin{aligned}\bar{P}(a,b) - \bar{P}(a,c) &= \int \rho(\lambda)\left[\bar{A}(a,\lambda)\bar{B}(b,\lambda) - \bar{A}(a,\lambda)\bar{B}(c,\lambda)\right]d\lambda \\ &= \int \rho(\lambda)\bar{A}(a,\lambda)\bar{B}(b,\lambda)\left[1+\bar{A}(b,\lambda)\bar{B}(c,\lambda)\right]d\lambda \\ &- \int \rho(\lambda)\bar{A}(a,\lambda)\bar{B}(c,\lambda)\left[1+\bar{A}(b,\lambda)\bar{B}(b,\lambda)\right]d\lambda,\end{aligned}$$

$$\begin{aligned}\bar{P}(a,b) - \bar{P}(a,c) \leq &\int \rho(\lambda)\left[1+\bar{A}(b,\lambda)\bar{B}(c,\lambda)\right]d\lambda \\ &+ \int \rho(\lambda)\left[1 \bar{+} A(b,\lambda)\bar{B}(b,\lambda)\right]d\lambda,\end{aligned}$$

$$\bar{P}(a,b) - \bar{P}(a,c) \leq 1 + \bar{P}(b,c) + \varepsilon + \delta.$$

Konačno

$$|a \cdot c - a \cdot b| - 2(\varepsilon + \delta) \leq 1 - b \cdot c + 2(\varepsilon + \delta),$$

ili

$$4(\varepsilon + \delta) \geq |a \cdot c - a \cdot b| + b \cdot c - 1.$$

Ako je, na primjer, $a \cdot c = 0$, $a \cdot b = b \cdot c = \frac{1}{\sqrt{2}}$, tada je

$$4(\varepsilon + \delta) \geq \sqrt{2} - 1.$$

Dakle, za konačno malo δ, ε ne može biti proizvoljno malo. Stoga, kvantnomehanička očekivana vrijednost ne može biti predstavljena relacijom (1.1.2).

Pretpostavljajući da je bilo koji Hermitski operator sa potpunim setom vlastitih stanja vidljiv (opservabilan), jednostavno je izvršiti generalizaciju, odnosno, proširiti rezultat na druge sisteme. Moguće je posmatrati dvodimenzionalne potprostore, te definisati operatore σ_1 i σ_2 u njihovom izravnom proizvodu, tehnički analogne ranije navedenim operatorima, koji su jednaki nuli za stanja izvan potprostora proizvoda. Tada, za barem jedno kvantnomehaničko stanje, statistička predviđanja kvantne mehanike nisu kompatibilna sa EPR argumentom. U teoriji, u kojoj su kvantnoj mehanici dodani parametri, da bi se odredili rezultati pojedinačnih mjerenja, bez promjena statističkih predviđanja, mora postojati mehanizam po kojem postavka jednog mjernog instrumenta može uticati na očitavanje rezultata na drugom instrumentu, bez obzira na njihovu međusobnu udaljenost. Čak što više, signal se mora trenutno prenositi, tako da ova teorija ne bi mogla biti Lorentz invarijantna. Naravno, situacija je drugačija, ako je validnost kvantnomehaničkih predviđanja ograničena. Predviđanja se mogu odnositi samo na eksperimente u kojima su instrumenti unaprijed podešeni, tako da mogu međusobno razmjenjivati signale brzinom manjom od, ili jednakoj brzini svjetlosti. S tim u vezi, eksperimenti u kojima se postavke mijenjaju dok čestica putuje su od ključne važnosti (Bohm i Aharonov).

Sažetak

Smisao EPR argumenta se ogleda u sljedećem:

-Stanje kvantnog objekta je zadano vektorom stanja, koji sadrži kompletan opis fizičkih osobina kvantnog objekta.

-Svaka fizička veličina je data zajedno sa svim mogućim rezultatima mjerenja te veličine i odgovarajućih vlastitih stanja (sva stanja u kojima kvantni objekat može biti nakon mjerenja). Matematički se to može realizovati matricama.

-Proizvoljna stanja se mogu izraziti u obliku vlastitih stanja ovakvih matrica.

Dakle, dvije čestice su proizvedene u istom procesu (izazvana je njihova interakcija), zbog čega one postaju spregnute, odnosno, dijele zajedničku prošlost. Zatim su odvojene jedna od druge, bez dalje manipulacije (na primjer, jedna je odnesena na Mjesec, a druga je ostala na Zemlji). Zbog zajedničke prošlosti, opisane su jednim, zajedničkim stanjem, ψ, koje nije isto kao i zbir stanja pojedinačnih čestica. Razvoj spregnutih stanja dvije čestice u vlastita stanja, uzimajući u obzir vlastita stanja σ_x (Paulijeva matrica), dat je na sljedeći način

$$\psi(s_1, s_2) = \psi_1(s_1) \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \psi_2(s_1) \begin{pmatrix} 1 \\ -1 \end{pmatrix},$$

i uzimajući u obzir stanja σ_z (Paulijeva matrica):

$$\psi(s_1, s_2) = \phi_1(s_1) \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \phi_2(s_1) \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Prva čestica je opisana drugačije, zavisno od opisa odabranog za drugu česticu, $\psi_i(s_1)$ u jednom slučaju, a $\phi_i(s_1)$ u drugom.

Prema kvantnoj teoriji, informacije o česticama možemo dobiti tek nakon mjerenja. Ako je spin druge čestice mjeren u x pravcu, u istom trenutku stanje spina prve čestice je $\psi_1(s_1)$ ili $\psi_2(s_1)$, prema rezultatu mjerenja vršenom na drugoj čestici. Ukoliko se mjerenje vrši u z pravcu, u istom trenutku stanje spina prve čestice je $\phi_1(s_1)$ ili $\phi_2(s_1)$, prema rezultatu mjerenja vršenom na drugoj čestici. To znači da prva čestica odmah *zna* kakvo je mjerenje izvršeno na drugoj čestici. Ovo predstavlja kvantnu spregnutost. (Einstein je nazvao *spooky action at a distance*). Ona se, prema klasičnim pretpostavkama, ne smije desiti.

Uprkos njihovoj prostornoj udaljenosti, dvije spregnute čestice se ponašaju kao jedan kvantni objekat, postoji samo jedno zajedničko stanje cijelog sistema (koje nije zbir stanja razdvojenih čestica). Rezultat mjerenja pokazuje da se ne smije pretpostaviti da prvi ili drugi foton imaju fiksne vrijednosti smjerova spina prije mjerenja. U ovu svrhu je zgodno koristiti Diracovu notaciju za spregnuto stanje spina:

$$\psi(s_1, s_2) = |1, 0\rangle - |0, 1\rangle.$$

Diracova notacija ima prednost prikaza samo relativnih smjerova spina dvije čestice, što predstavlja jedinu fiksnu, dobro određenu osobinu, dok sami smjerovi nisu određeni, oni se pojave tek nakon mjerenja. U opštem slučaju, fiksne vrijednosti osobina ne postoje, pojave se tek unutar mjerenja (što je od ključnog značaja za praktičnu primjenu spregnutosti).

Bellova nejednakost

Protoni od nekoliko MeV se sudaraju sa metom, koja je, u ovom slučaju, vodonik, od kojih će se jedan rasijati, uzrokujući uzmak protona mete. Brojači T_1 i T_2 registruju protone, koji se kreću prema udaljenim brojačima, C_1 i C_2. Nakon određenog vremena, ono što registruju brojači T_1 i T_2 će implicirati ono što registruju C_1 i C_2, u idealnoj postavci eksperimenta. Ispred brojača C_1 i C_2 se nalaze filteri, koji propuštaju samo čestice određene polarizacije, na primjer, čestice spinske projekcije $+\frac{1}{2}$, duž z ose. Tada je moguće da jedan ili oba brojača ništa ne registruju. Za protone odgovarajuće energije, samo jedan od ovih brojača će registrovati nešto u skoro svakom slučaju. Razlog tome je što proton-proton rasijanje za male uglove i velike energije uglavnom ide u S-talas. Međutim, antisimetričnost konačne talasne funkcije zahtjeva i antisimetričnost singlet stanja u ovom stanju, jedan spin je *up*, a drugi *down*, što slijedi iz kvantnomehaničke očekivane vrijednosti

$$\langle\psi_s|\,\sigma_z(1)\sigma_z(2)\,|\psi_s\rangle = -1,$$

gdje su $\frac{1}{2}\sigma_z(1)$ i $\frac{1}{2}\sigma_z(2)$ z komponente operatora spina za dvije čestice. Pretpostavlja se da su udaljenosti brojača na izvoru takve da proton koji se kreće prema C_1 stiže prije nego što drugi proton stigne do C_2 . Kada bi neko posmatrao brojač C_1, ne bi mogao znati unaprijed hoće li nešto biti registrovano ili ne. Onog trenutka kada se vidi šta se desilo na brojaču C_1, zna se šta će se desiti na brojaču C_2, bez obzira na njegovu udaljenost. S obzirom na to da je kvantna mehanika nedeterministička teorija, ova situacija je paradoksalna- rezultati mjerenja nepolarizovane čestice nisu konačni, dok se mjerenje ne izvrši. Ali u prethodno opisanoj situaciji, rezultati mjerenja se znaju unaprijed. Nameće se mnoštvo pitanja: Kada su rezultati mjerenja postali poznati? Na koji način tako udaljen događaj može uticati na situaciju ovdje? Da li ima smisla pretpostaviti da su rezultati na neki način predodređeni? Bitno je uzeti u obzir cijelu postavku eksperimenta, ne smije se analizirati dio po dio, sa odvojeno lokalizovanim udjelima neodređenosti.

Einstein predlaže uvođenje skrivenih varijabli, koje bi učinile potpunom, prema njegovom mišljenju, nepotpunu kvantnu teoriju. Međutim, nedeterministički kvantnomehanički fenomeni se mogu simulirati deterministički.

Neka je S varijabla koja poprima vrijednosti ±1, zavisno od toga da li prvi brojač registruje nešto ili ne, i neka je B varijabla koja, također, poprima vrijednosti ±1, zavisno od odgovora drugog brojača. Neka su A i B određene varijablama (koje mogu biti i slučajni brojevi) $\lambda, \mu, \nu, ...$ na sljedeći način:

$$A(\lambda, \mu, \nu, ...),$$

$$B(\lambda, \mu, \nu, ...).$$

Postoji beskonačno mnogo načina odabira ovih varijabli i funkcija, tako da bude B= +1, kad god je A= -1, i obrnuto, što znači da su kvantnomehaničke korelacije reprodukovane.

Sada, umjesto da su filteri usmjereni u z-pravcu, oba su rotirana u nekom drugom pravcu. Neka je filter povezan sa prvim brojačem usmjeren duž nekog jediničnog vektora **a**, a filter povezan sa drugim brojačem duž jediničnog vektora **b**. Za date vrijednosti varijabli $\lambda, \mu, \nu, ...$, rezultat (odgovor) prvog brojača A bi mogao značajno zavisiti od ove orijentacije svoga filtera. Nije za očekivati da će ovaj rezultat zavisiti od orijentacije drugog, udaljenog filtera. Na isti način, odgovor drugog brojača bi mogao zavisiti od orijentacije svog filtera, ali ne i od orijentacije prvog, udaljenog filtera:

$$A(a, \lambda, \mu, \nu, ...),$$
$$B(b, \lambda, \mu, \nu, ...).$$

Neka je funkcija korelacije $P(a, b)$ definisana kao srednja vrijednost proizvoda AB:

$$P(a, b) = \overline{A(a, \lambda, \mu, \nu, ...)B(b, \lambda, \mu, \nu, ...)}. \tag{1.1.9}$$

Za ovaj, uopšteniji slučaj, kvantna mehanika predviđa da je

$$P(a, b) = \langle \psi_s | \, a \cdot \sigma_1 b \cdot \sigma_2 \, | \psi_s \rangle = -\cos\theta, \tag{1.1.10}$$

gdje je θ ugao između a i b. Međutim, *ne postoji* način odabira varijabli $\lambda, \mu, \nu, ...$ i funkcija A i B, takav da prosječna vrijednost (1.1.9) daje vrijednost (1.1.10).

Ako se pretpostavi da su ove dvije relacije jednake kada je $a = b$, odnosno kada je $\theta = 0$, tada je $P(a, b) = -1$, te A i B moraju imati suprotan predznak u cijelom prostoru $\lambda, \mu, \nu, ...$

Ako se a zamijeni nekom novom vrijednošću a', B će ostati isto za date $\lambda, \mu, \nu, ...$, dok će A promijeniti znak u određenim trenutcima (bit će AB=+1, umjesto AB=-1 u prosječnoj vrijednosti). Slijedi:

$$P(a, a') - P(a, a) = 2\rho,$$

gdje ρ predstavlja ukupnu vjerovatnoću svih tačaka $\lambda, \mu, \nu, ...$, u kojima A mijenja znak. Ovaj set tačaka, kada se a zamijeni sa a', ni na kakav način ne zavisi od b. Iz prosječne vrijednosti (1.1.9), te uzimajući da je $B = \pm 1$, slijedi

$$|P(a', b) - P(a, b)| \leq 2\rho.$$

Za vrijednost $b = a$, najizraženija je zavisnost P od a. Za razliku od kvantne relacije (1.1.10), koja je stacionarna u θ za $\theta = 0$, u relaciji skrivenih varijabli mora da postoji neka nelogičnost.

Može se posmatrati i općenitija reprezentacija skrivenih varijabli, gdje bi A zavisilo i od a i od b, kao i B:

$$A(a, b, \lambda, \mu, \nu, ...),$$
$$B(a, b, \lambda, \mu, \nu, ...),$$

što bi značilo da ponašanje brojača zavisi od događaja udaljenog od njega. Ovo ponašanje će biti neuobičajeno i za konstantne vrijednosti a i b. Ako se pretpostavi da se a i b mijenjaju u toku vremena, onda, prema kvantnoj mehanici, relevantne vrijednosti a i b su one koje su dobijene kada čestice prođu kroz odgovarajuće filtere. Ako se podesi da su dva *prolaza* istovremena, tada će A zavisiti od postavke b udaljenog instrumenta (i B od a). Ova zavisnost bi se morala odvijati brzinom većom od brzine svjetlosti.

Iz ovoga slijedi neodrživost Einsteinovog shvatanja stvarnosti, ukoliko priroda slijedi kvantnu mehaniku. Međutim, na mikroskopskim skalama, kvantna mehanika je doživjela veliki uspjeh, ali ovdje su u pitanju fenomeni na makroskopskoj skali.

CHSH nejednakost

S ciljem povećavanja praktičnosti u istraživanju problema skrivenih varijabli i lokalnosti, eksperimentalne provjere su inicirali Clauser, Holt, Shimony i Horne. Modifcirali su originalnu Bellovu nejednakost, tako da ona može biti primijenjena na bilo koju eksperimentalnu postavku, koja je dovoljno slična postavci dvo-spinskih atomskih sistema. CHSH nejednakost je data u sljedecem obliku:

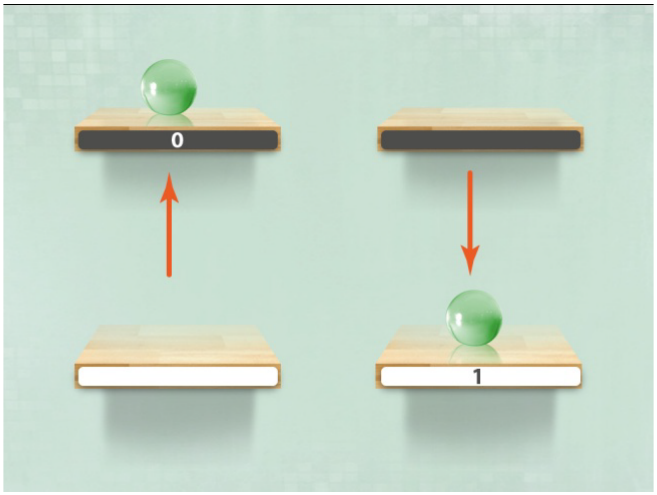
$$|P(a, b) - P(a, b')| + |P(a', b) + P(a', b')| \leq 2$$

2 Kvantna informacija

2.1 Razlika između klasične i kvantne informacije

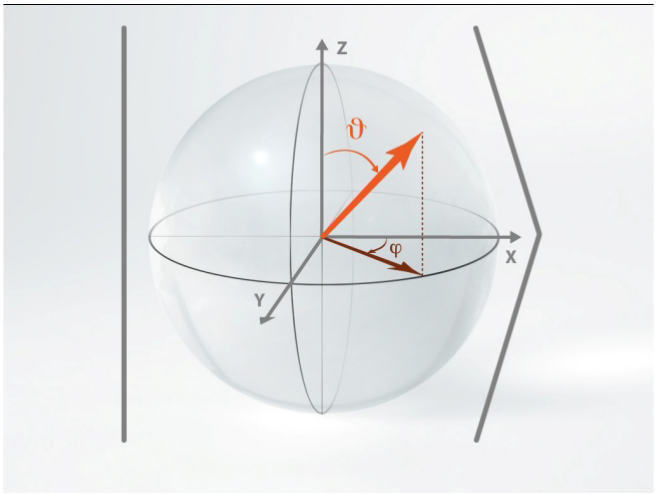
Kvantni bit, ili qubit (QUantum BIT) je osnovna jedinica kvantne informacije. Razlika između kvantne i klasične informacije nastaje upravo zbog razlike između njihovih osnovnih jedinica. Sistem qubita se može nalaziti u jednom od bezbroj signifikantnih stanja (bez obzira na to što može poprimiti dvije vrijednosti u odabranoj računskoj bazi), dok bit može biti u jednom od samo dva signifikantna stanja. U opštem slučaju, sistem qubita se mora posmatrati unutar mogućnosti da istovremeno bude u jednom mjerljivom stanju i/ili drugom, suprotnom stanju, umjesto da je u samo jednom od dva moguća stanja (kao bit). Za razliku od klasičnog stanja, nepoznato stanje sistema qubita se u opštem slučaju ne može dobiti jednim mjerenjem. Umjesto toga, mjerenje se vrši na sistemu ansambla (u ovom slučaju, ansambl je set identično pripremljenih stanja), s ciljem da se otkrije nepoznato stanje koje oni dijele. Superpozicija različitih mogućnosti za dobijanje datog kvantnog stanja u datom trenutku, koje mogu međusobno interferirati, u prirodi je kvantne vjerovatnoće.

Osobine sistema qubita su bivalentne i mogu se predvidjeti samo sa određenom vjerovatnoćom. Ipak, postoji razlika između sistema qubita i probabilističkog klasičnog sistema koji nasumično poprima jednu od dvije kompjutacijski relevantne vrijednosti, jer on i može biti samo u jednom od dva stanja u bilo kojem trenutku, bez obzira na način mjerenja. Vjerovatnoće ishoda mjerenja bilo kojeg klasičnog sistema zavise samo od *neznanja* onoga ko vrši mjerenje stvarnog stanja sistema, a ne od temeljne neodređenosti osobina (što je slučaj kod kvantnih sistema). Kvantni bit se *ne može* redukovati na probabilistički bit.



Slika 2.1.1: Ilustracija klasičnog bita. [3]

Važno je prepoznati razliku između fizičkog sistema, njegove reprezentacije i informacije koju on može da pohrani.



Slika 2.1.2: Grafička reprezentacija mogućih stanja qubita pomoću Blochove sfere. Kvantna stanja su opisana vektorima jedinične dužine u trodimenzionalnom prostoru i uglovima θ i ϕ sfernih koordinata. [3]

Teorija kvantne informacije, prenosa, obrade i pohrane informacija primjenom kvantnih sistema, danas je dobro razvijena. Najvećim dijelom je izgrađena na temelju generalizacije elemenata tradicionalne teorije informacije, koja objašnjava prenos, obradu i pohranu informacija korištenjem klasičnih sistema. Zbog temeljne razlike matematičkog opisa kvantnih sistema od matematičkog opisa klasičnih sistema, njihove osobine se značajno razlikuju. U kvantnomehaničkim sistemima, većina informacija je najčešće pohranjena u obliku korelacija između podsistema, koje znaju biti izuzetno jake. Potpuno spregnuti kvantni sistemi su izvanredni slučajevi. Na primjer, za Bellova stanja, redukovana stanja pojedinačnih qubita su potpuno neodređena, dok je stanje para qubita potpuno korelirano, odnosno, ono što se mjerenjem spoznalo o stanju jednog qubita jednako je onome što se zna o drugom. Postoji razlika u potpunosti klasičnih i kvantnih stanja, i ona se najbolje vidi kada je prisutna spregnutost između komponenti složenih kvantnih sistema. U biparitetnim sistemima, na primjer, spregnutost se manifestuje u narušavanju nejednakosti Bellovog tipa, kao i u vidljivosti samointerferencije podsistema i cjelokupnih sistema. Čak i spregnutost između dva podsistema obezbjeđuje novi izvor obrade informacija, nadopunjavajući one koje omogućavaju biti, ili nespregnuti qubiti.

Ova razlika je još više naglašena u slučaju većih, multi-qubitnih stanja, koja se mogu raspodijeliti između određenog broja razdvojenih strana, koja možda učestvuju u raspodijeljenoj obradi informacija.

2.2 Reprezentacija qubita

Čista stanja qubita mogu se predstaviti vektorima u dvodimenzionalnom kompleksnom Hilbertovom prostoru

$$\mathcal{H} = \mathbb{C}^2.$$

Bilo koja ortonormirana baza za ovaj prostor može korespondirati sa dvije vrijednosti bita, 0 i 1, da bi se ponašala kao jedno-qubitna računarska baza, koja se naziva i pravolinijska baza, i zapisuje kao

$$\{|0\rangle, |1\rangle\}.$$

Elementi odabrane baze se mogu poistovjetiti sa konačnim poljem dva elementa,

$$x_i \in GF(2),$$

zapisujući ih kao $|x_i\rangle$ sa

$$x_i \in \{0, 1\}.$$

Princip superpozicije implicira da je bilo koja kompleksna linearna kombinacija (qubit baza), poput $|0\rangle$ i $|1\rangle$, to jest

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle,$$

sa $a_i \in \mathbb{C}$ i $|a_0|^2 + |a_1|^2 = 1$, također fizičko stanje qubita. Takvo stanje je čisto kvantno stanje. Skalarni koeficijenti a_0 i a_1 predstavljaju kvantne amplitude vjerovatnoće, jer njihove kvadratne vrijednosti predstavljaju vjerovatnoće p_1 i p_2 da se qubit opisan stanjem $|\psi\rangle$ nađe u baznim stanjima $|0\rangle$ i $|1\rangle$. Vektori baze se mogu predstaviti u matričnoj formi, kao

$$|0\rangle \doteq \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

i

$$|1\rangle \doteq \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Dijagonalna baza se, također, često upotrebljava. Ona se zapisuje kao $\{|\nearrow\rangle, |\searrow\rangle\}$, ili kao $\{|+\rangle, |-\rangle\}$. Data je sa

$$|\nearrow\rangle \equiv \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

i

$$|\searrow\rangle \equiv \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle),$$

što je slično sa osnovnom računarskom bazom. Računarska i dijagonalna baza zajedno čine parove stanja, koja se koriste u protokolu BB84 distribucije kvantnog ključa (više o BB84 protokolu u poglavlju 5). Imajući to u vidu, vjerovatnoće da se qubiti u stanjima $|\nearrow\rangle$ i $|\searrow\rangle$ nađu u stanjima $|0\rangle$ i $|1\rangle$ su jednake 0.5, i obrnuto.

Cirkularna baza, $\{|r\rangle, |l\rangle\}$ (ponekad zapisana i u obliku $\{|\circlearrowright\rangle, |\circlearrowleft\rangle\}$),

$$|r\rangle \equiv \frac{1}{\sqrt{2}} (|0\rangle + i\,|1\rangle),$$

$$|l\rangle \equiv \frac{1}{\sqrt{2}} (|0\rangle - i\,|1\rangle),$$

također je korisna u kvantnoj kriptografiji. Srodna je sa računarskom i dijagonalnom bazom. Sve tri navedene, međusobno srodne baze, koriste se za dobijanje tri para stanja u protokolu za distribuciju kvantnog ključa. Vjerovatnoće da se qubiti u stanjima $|r\rangle$ i $|l\rangle$ nađu u stanjima $|0\rangle$, $|1\rangle$, $|\nearrow\rangle$, i $|\searrow\rangle$, redom su jednake 0.5. Vrijedi i obrnuto. Spinorska reprezentacija uopštenog čistog stanja qubita je data sa

$$|\psi(\theta, \phi)\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \doteq \begin{pmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{pmatrix},$$

gdje je $0 \leq \theta \leq \pi$, i $0 \leq \phi \leq 2\pi$, kada je $\theta = 0$ i π, za ϕ se uzima da je nula. Stoga je ϕ relativna faza između jednokubitnih baznih stanja. Sa ovom parametrizacijom, uopšteno stanje qubita se prirodno vizualizira u Blochovoj lopti, čija je granica Poincare-Bloch sfera, sačinjena isključivo od čistih stanja $|\psi(\theta, \phi)\rangle$.

3 Kvantna entropija

3.1 Von Neumannova entropija

Standardna mjera za informaciju sadržanu u kvantnim sistemima, opisanu statističkim operatorom ρ, jeste von Neumannova[1] entropija

$$S(\rho) = -tr(\rho log_2 \rho) = -\sum_i \lambda_i log_2 \lambda_i,$$

gdje su λ_i članovi skupa vlastitih vrijednosti ρ i $0log0 \equiv 0$. $S(\rho)$ je nenegativno, postiže maksimalnu vrijednost za maksimalno miješano stanje i jednako je nuli ako i samo ako ρ opisuje čisto stanje. Za sisteme opisane stanjima u d-dimenzionalnim Hilbertovim prostorima,

$$0 \leq S(\rho) \leq log_2 d,$$

tako da za qubite vrijedi

$$0 \leq S(\rho) \leq 1.$$

$S(\rho)$ obezbjeđuje mjeru informacija u jedinicama qubita. Von Neumannova entropija ima ulogu u teoriji kvantne informacije analognu onoj koju ima Shannonova[2] entropija u teoriji klasične informacije. $S(\rho)$ mjeri neodređenost kvantnog stanja, povezanu sa kvantnom raspodjelom vjerovatnoće. U klasičnom sistemu, entropija se može posmatrati kao informacija dobijena identifikacijom stanja sistema, dok, u opštem slučaju, ρ ne može biti potpuno identificirano opservacijom događaja, tako da $S(\rho)$ osigurava samo labavo ograničenje. Kvantne pridružene entropije su:

$$S(A, B) \equiv S(\rho_{AB}),$$

$$S(A, B, C) \equiv S(\rho_{ABC}).$$

Zbog uniformnosti zapisa, uzima se i

$$S(A) \equiv S(\rho_A).$$

[1] John von Neumann (28. 12. 1903.- 8. 2. 1957.), polimat rođen u Mađarskoj. Pionir je primjene teorije operatora u kvantnoj mehanici u razvoju funkcionalne analize. Imao je ključnu ulogu u razvoju teorije igara i ćelijskog automata. Bio je uključen u razvoj prvog elektronskog računara, ENIAC-a.

[2] Claude Elwood Shannon (30. 4. 1916.- 24. 2. 2001.), matematičar, inžinjer elektrotehnike, kriptograf, rođen u SAD. Osnivač je teorije dizajna digitalnih kola. Poznat je kao "otac teorije informacije".

Iz ovakvog zapisa proizilaze sljedeće osobine von Neumannove entropije:

- Aditivnost za proizvode stanja (također osobina klasičnih stanja):

$$S(\rho_A \otimes \rho_B) = S(A) + S(B).$$

- Subaditivnost za sva kvantna stanja:

$$S(A, B, C) + S(B) \leq S(A, B) + S(B, C).$$

- Konkavnost:

$$S(\sum_i p_i \rho_i) \geq \sum_i p_i S(\rho_i).$$

- Invarijantnost prema unitarnim transformacijama kvantnih stanja:

$$S(U \rho U^\dagger) = S(\rho).$$

Vjerovatnoće da se sistem nalazi u odgovarajućem stanju ρ_i (čija je suma jednaka jedinici) su označene sa p_i. Posljednja osobina je povezana sa očuvanjem čistoće stanja. Shannonova entropija i von Neumannova entropija se podudaraju samo za ansambl koji formiraju zajednički ortonormirana čista kvantna stanja. Stoga, ako se želi poslati poruka, koja je kodirana unutar seta ortogonalnih čistih stanja qubita, koji se mogu opisati tenzorom produkta stanja, prenos bi bio ekvivalentan stanju iste informacije kao seta klasičnih bita, jer se svaki qubit razlikuje jedan od drugog, kada se odredi baza kodiranja. Kvantna entropija je prema unitarnim transformacijama invarijantna. Međutim, mjerenja se itekako mogu promijeniti. Na primjer, za sistem u početnom trenutku opisan statističkim operatorom ρ, a nakon mjerenja operatorom ρ', konačna entropija će biti manja ili jednaka početnoj:

$$S(\rho') \leq S(\rho).$$

Araki-Lieb[3][4] nejednakost povezuje pridruženu entropiju i entropiju podsistema:

$$S(A, B) \geq |S(A) - S(B)|.$$

Za složeni sistem u čistom stanju $|\psi\rangle$, $\rho_{AB} = P(|\psi\rangle)$, pa je $S(A, B) = 0$, iz čega slijedi da mora vrijediti $S(A) = S(B)$ za bilo koji ovakav sistem. Prema tome, za dvije individualne čestice u singlet stanju $|\psi^-\rangle$, $S(A, B) = 0$, gdje je $S(A) = S(B) = 1$, to jest, uzajamnost između stanja podsistema A i B je potpuno određena, dok su pojedinačna

[3] Huzihiro Araki, japanski matematičar i fizičar, rođen 1932. godine. Diplomirao je pod mentorstvom Hidekija Yukawe. Doktorirao je na Princeton Univerzitetu.

[4] Elliott Hershel Lieb, američki matematičar i fizičar, rođen 1932. godine. Profesor je na Princeton Univerzitetu. Poznat je po istraživanju u oblasti statističke fizike, teorije kondenzovane materije, i funkcionalne analize.

stanja tih podsistema potpuno neodređena. U tome se ogleda smisao von Neumannove entropije pri opisivanju spregnutosti. Teorema o pridruženoj entropiji također vrijedi za set ortogonalnih stanja $\{|i\rangle\}$ sistema A, i n statističkih operatora ρ_i drugog sistema B, pri čemu su p_i vjerovatnoće za oba:

$$S(\sum_{i=1}^{n} p_i P(|i\rangle) \otimes \rho_i) = \mathcal{H}(\{p_i\}) + \sum_{i=1}^{n} p_i S(\rho_i).$$

3.2 Kvantna relativna i uslovljena entropija

Kvantna uslovljena entropija je, analogno odgovarajućoj klasičnoj veličini, data sa

$$S(A \mid B) \equiv S(A,B) - S(B) = S(\rho_{AB}) - S(\rho_B),$$

dok u kvantnoj mehanici, ova veličina može biti negativna. To znači da kvantni sistemi mogu da budu "određeniji" u pridruženom stanju dvokomponentnih sistema, nego u stanjima njegovih pojedinačnih komponenti (što je vidljivo u slučaju singlet stanja $|\psi^-\rangle$). Kvantna relativna entropija (između) dva stanja, ρ i σ , kvantnih sistema, data je sa

$$S(\rho \parallel \sigma) \equiv tr(\rho(log_2\rho - log_2\sigma)).$$

Ova veličina zadovoljava relaciju

$$S(\rho \parallel \sigma) \geq 0,$$

koja se naziva Kleinova[5] nejednakost i prelazi u jednakost ako i samo ako je $\rho = \sigma$ (analogna nejednakost za klasičnu relativnu entropiju je Gibbsova nejednakost). Ni ova veličina nije normirana zbog nedostatka simetrije u odnosu na svoje argumente, kao ni odgovarajuća klasična veličina. Kvantna relativna entropija opisuje mogućnost razlikovanja stanja definisanih u istom Hilbertovom prostoru.

3.3 Kvantna zajednička informacija

Kvantna zajednička informacija između dva podsistema, ρ_A i ρ_B i složenog sistema, opisanog pridruženim stanjima ρ_{AB}, data je sa

$$I(A:B) \equiv S(A) + S(B) - S(A,B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}),$$

[5] Oskar Benjamin Klein (15. 9. 1894.-5. 2. 1977.), švedski teorijski fizičar. Pripisuju mu se temeljne ideje teorije struna.

također po analogiji sa odgovarajućom klasičnom veličinom. Međutim, kvantna zajednička informacija prelazi klasična ograničenja. Ona može doseći dva puta veću maksimalnu vrijednost od vrijednosti dobijene u odgovarajućem klasičnom slučaju:

$$I(A:B) \leq 2 \cdot min\left\{S(A), S(B)\right\}.$$

Ovo je posljedica Araki-Lieb nejednakosti, koja implicira da kvantni sistemi mogu biti superkorelirani. Ukupan iznos uzajamnosti, mjeren pri minimalnoj stopi nasumičnosti, koja je potrebna za potpuno brisanje svih korelacija u stanju ρ_{AB}, jednak je kvantnoj zajedničkoj informaciji, što vodi do jake subaditivnosti von Neumannove entropije. Kvantna zajednička informacija se također može posmatrati kao tip relativne entropije:

$$I(A:B) = S(\rho_{AB} \parallel \rho_A \otimes \rho_B).$$

Kao u slučaju klasične entropije, kvantna entropija se može zadati za multiparitetne sisteme. Na primjer, kvantna uslovljena zajednička informacija unutar triparitetnih sistema se može zapisati kao

$$I(A:B \mid C) = S(A \mid C) - S(A \mid B,C) = S(A \mid C) + S(B \mid C) - S(A,B \mid C).$$

Također, postoje kvantna pravila lanca za entropiju, analogno klasičnim. Važna teorema, poznata pod imenom Liebova teorema, baza je mnogih rezultata povezanih sa mjerenjima kvantne entropije. Na primjer, nejednakost jake subaditivnosti, druga osobina von Neumannove entropije, veoma je koristan rezultat, koji se može dokazati koristeći ovu teoremu. Osobina jake subaditivnosti von Neumannove entropije dozvoljava demonstraciju nekoliko korisnih osobina entropija iz ovog poglavlja, koje također poprimaju formu nejednakosti. Na primjer, važno je primijetiti da uslovljavanje smanjuje entropiju u kontekstu triparitetne podjele složenog sistema

$$S(A \mid B,C) \leq S(A \mid B).$$

Pored toga, odbacivanje komponenti složenog sistema može smanjiti, a nikada povećati kvantnu zajedničku informaciju

$$I(A:B) \leq I(A:B,C),$$

što je možda najznačajnija manifestacija jake subaditivnosti kvantne entropije. U sistemu sačinjenom od četiri komponente, A, B, C, i D, kvantna uslovljena entropija je subaditivna

$$S(A,B \mid C,D) \leq S(A \mid C) + S(B \mid D),$$

dok kvantna zajednička informacija nije.

3.4 Vjernost i koherentna informacija

Mjera vjernosti prenosa ulazne informacije čistog stanja $|\psi\rangle$, koje proizvodi konačno stanje σ_i sa vjerovatnoćama p_i u statističkom stanju $\rho = \sum_i p_i \sigma_i$, data je sa

$$F(P(|\psi\rangle), \rho) = \langle\psi| \rho |\psi\rangle ,$$

a u slučaju unosa miješanog stanja ω,

$$F(\rho, \omega) = \left[tr\left(\sqrt{\sqrt{\omega}\rho\sqrt{\omega}} \right) \right]^2 .$$

Ova veličina je ključna u izučavanju kvantne komunikacije i predstavlja maksimalnu vrijednost, dobijenu iz čistog stanja, izraženog preko skupa čistih stanja u Hilbertovom prostoru. Relacija

$$S(\rho, \varepsilon) \leq H_{bin}(\tilde{F}(\rho, \varepsilon)) + (1 - \tilde{F}(\rho, \varepsilon)) log_2(d^2 - 1)$$

predstavlja kvantnu Fano[6] nejednakost, za kvantnu operaciju ε na sistemu, u Hilbertovom prostoru dimenzije $d \geq 2$, gdje je izmjena entropije

$$S_e(\rho, \varepsilon) = -tr(W log W).$$

Elementi matrice W:

$$[W]_{ij} \equiv tr(E_i \rho E_j^\dagger)/tr\varepsilon(\rho).$$

E_i su elementi reprezentacije operatora sume ε. $S_e(\rho, \varepsilon)$ određuje količinu kvantne entropije uvedene u sistem kao rezultat operacije ε izvršene na njemu. $\tilde{F}(\rho, \varepsilon)$ predstavlja *vjernost spregnutosti,* koja određuje stepen očuvanja spregnutosti, pod operacijom ε, između jednog i drugog sistema potrebnog za formiranje čistog cijelog stanja, odnosno, vjernost stanja

$$\tilde{F}(\rho, \varepsilon) = \langle\psi_{PQ}| \rho_{PQ'} |\psi_{PQ}\rangle$$

između početnih i konačnih čistih stanja ovakvog cijelog sistema, gdje je $|\psi_{PQ}\rangle$ čisto stanje sistema kombinovanog od ulaznog sistema Q i *referentnog* sistema P, iz čega proizilazi ρ kao redukovano stanje sistema Q i $\rho_{PQ'}$ stanje, kao rezultat operacije ε na sistemu Q. U slučaju ovakvog para sistema, koji formira potencijalno spregnut pridruženi sistem, podsistem Q bi mogao biti djelomično izolovan od svoje okoline (ovaj efekat je opisan operacijom ε). Na primjer, Q se može poslati kroz kvantni kanal. Izlazno stanje

[6] Roberto Mario "Robert" Fano (11. 11. 1917.-13. 7. 2016.), talijansko-američki informatičar. Profesor je elektrotehnike na MIT-u (Massachusetts Institute of Technology). Značajan je njegov doprinos razvoju teorije informacije. Poznat je i po Shannon-Fano kodiranju.

bi bilo $\rho_{PQ'}$. Ako je ulazno stanje čisto, izlazno, u opštem slučaju, neće biti. Tada se može uvesti koherentna informacija između podsistema

$$I_{coh}(\rho, \varepsilon) = S(Q') - S(P, Q').$$

Na desnoj strani posljednje relacije su von Neumannove entropije za preneseni podsistem i cijeli sistem, respektivno. Koherentna kvantna informacija, koja može imati bilo koji predznak, ima neke jako korisne osobine. Ako je izlazno stanje spregnuto, ova veličina je pozitivna i može se posmatrati kao mjera neklasičnih svojstava, preko očuvanja kvantne koherentnosti (opisanog sa ε). Koherentna informacija se ne može povećavati pod lokalnim operacijama na Q, tako da je

$$I_{coh}(\rho, \varepsilon) \leq S(Q),$$

nakon uticaja okoline na Q. S obzirom na to da je smanjenje koherentne informacije zbog efekta okoline nepovratan proces, potreban i dovoljan uslov za mogućnost izvođenja savršene ispravke pogrešaka, koje su nastale interakcijom Q sa okolinom, je

$$I_{coh}(\rho, \varepsilon) = S(Q).$$

Ako se posmatra proces u dvije faze, nastao iz dva potprocesa, ε_1 i ε_2 zaredom, te se kao rezultat prvog procesa dobije

$$\rho \to \rho_{Q'} = \varepsilon_1(\rho_Q),$$

tada je rezultat drugog procesa

$$\rho_{Q'} \to \rho_{Q''} = \varepsilon_2(\rho_{Q'}) = \varepsilon_{12}(\rho_Q),$$

gdje je

$$\varepsilon_{12} = (\varepsilon_2 \circ \varepsilon_1)(\rho_Q).$$

Tada koherentna informacija zadovoljava nejednakost obrade kvantne informacije

$$S(Q) \geq I_{e_1}(\rho_Q, \varepsilon_1) \geq I_{e_{12}}(\rho_Q, \varepsilon_{12}),$$

gdje je

$$I_{e_1}(\rho_Q, \varepsilon_1) = S(Q') - S_{e_1}(Q)$$

i

$$I_{e_{12}}(\rho_Q, \varepsilon_{12}) = S(Q'') - S_{e_{12}}(Q),$$

gdje je $S_{e_1}(Q)$ izmjena entropije u prvoj fazi procesa, a $S_{e_{12}}(Q)$ izmjena entropije kompozicije dva procesa, koji čine cijeli proces ε_{12}.

4 Kvantna spregnutost

4.1 *Ipak se spreže* (Historijski uvod)

Kada se ne mogu razlikovati alternativne mogućnosti za proizvodnju zajedničkih događaja, tada se, vjerovatno, *desila* spregnutnost. Pojam spregnutost (njemački - Verschränkung, engleski - entanglement) je prvi puta upotrijebio Ervin Schrödinger, opisujući je kao osobinu svojstvenu kvantnoj mehanici. Zbog nemogućnosti razlikovanja alternativnih redova stanja kvantnog sistema (koji počinju datim početnim stanjem i završavaju odgovarajućim konačnim stanjem), preciznim mjerenjem, u određenom konačnom trenutku vremena, nastaje kvantna interferencija. Izvanredna uzajamnost stanja kvantnih podsistema, povezanih spregnutošću, može se koristiti u algoritmima kvantnog računanja, koji rade na principu interferencije, što je mnogo efikasnije od načina koji nude klasične metode.

Spregnuta stanja se mogu primijeniti i u jedinstvenim protokolima kvantne komunikacije (kvantna teleportacija, kvantno kodiranje, napredni oblici distribucije kvantnog ključa, korištenjem LOCC). Zbog ponašanja koje nije intuitivno, radi jake uzajamnosti koju spregnutost povlači za sobom, izučavanje spregnutosti je od trajnog, esencijalnog značaja. Einstein, Podolski i Rosen su, u svom argumentu, iznijeli stav da je kvantna mehanika nepotpuna, ako se na nju gleda kao na lokalnu realističku teoriju, zasnovanu na razmatranju spregnutih kvantnih stanja, u obliku

$$|\Psi(x_1, x_2)\rangle = \sum_{i=1}^{\infty} a_i \left|\psi(x_1)_i \, \phi(x_2)_i\right\rangle .$$

Poslije je David Bohm istražio spregnutost na mnogo jednostavniji način (spinski par u singlet stanju):

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right),$$

što je, od tada, centralni način istraživanja osnova kvantne mehanike i kvantne informacije, gdje su $\{|\uparrow\rangle, |\downarrow\rangle\}$ uzeti kao vektori baze, i pišu se kao $\{|0\rangle, |1\rangle\}$.

Prateći ovaj razvoj, John Bell je značajno unaprijedio istraživanje kvantne spregnutosti. On je postavio jasnu granicu između lokalnog ponašanja, koje se može objasniti klasičnim metodama, i nelokalnih, manje intuitivnih oblika ponašanja, izvodeći nejednakost, koju lokalne realističke teorije, koje bi trebale objasniti jaku uzajamnost između dva

udaljena podsistema, koji formiraju složen sistem (poput onih koji nastaju u sistemima koji su u kvantnoj mehanici opisani singlet stanjem) moraju zadovoljavati. Istraživanje ovog neobičnog ponašanja među podsistemima unutar većih sistema i dalje je u toku. U toku su i istraživanja mogućnosti primjene istog.

4.2 Problem separabilnosti

Spregnuta kvantna stanja su, jednostavno, ona koja su neseparabilna. Prema Schrödingerovoj definiciji, spregnuta čista stanja multiparitetnih sistema su ona koja se ne mogu predstaviti u formi jednostavnog tenzorskog proizvoda stanja podsistema:

$$|\Psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \otimes ... \otimes |\psi_n\rangle \,,$$

gdje su $|\psi_i\rangle$ stanja lokalnih podsistema (na primjer, spinska stanja fundamentalnih čestica). Ostala čista stanja multiparitetnih sistema, koja se *mogu* predstaviti jednostavnim tenzorskim proizvodom stanja nezavisnih podsistema, nazivaju se stanja proizvoda.

Definicija spregnutosti se može proširiti i na miješana stanja. Kvantna miješana stanja, unutar kojih je najlakše shvatiti spregnutost, jesu stanja biparitetnih sistema ρ_{AB}, koja se najčešće označavaju sa AB, čije su komponente označene sa A i B, u korespondenciji sa laboratorijama u kojima su locirane. Miješana stanja se nazivaju separabilnim (ili faktorabilnim) onda, kada se mogu zapisati u obliku konveksne kombinacije proizvoda:

$$\rho_{AB} = \sum_i p_i \rho_{Ai} \otimes \rho_{Bi},$$

gdje je $p_i \in [0,1]$ i $\sum_i p_i = 1$, a ρ_A i ρ_B su statistički operatori na podsistemima Hilbertovih prostora, $\mathcal{H}_\mathcal{A}$ i $\mathcal{H}_\mathcal{B}$, respektivno.

Dakle, spregnuta stanja su neseparabilna, dok separabilna miješana stanja ne mogu biti spregnuta. Prema definiciji, to su mješavine produkt stanja, te mogu biti kreirana lokalnim operacijama i klasičnom komunikacijom (LOCC) od čistih produkt stanja. Da bi nastalo separabilno stanje, prenosnik u jednoj laboratoriji samo mora uzeti uzorak raspodjele vjerovatnoće $\{p_i\}$, i podijeliti odgovarajuće rezultate mjerenja sa drugim prenosnikom. Tada ova dva prenosnika mogu stvoriti sopstvene setove pogodnih lokalnih stanja ρ_i, u svojim razdvojenim laboratorijama. Međutim, nije moguće konvertovati sva spregnuta stanja jedno u drugo na ovaj način. To dovodi do različitih klasa spregnutih stanja, odnosno, do različitih tipova spregnutosti. Pored toga, u opštem slučaju, nije uvijek moguće odrediti da li je dati statistički operator spregnut. U datom setu podsistema, problem određivanja spregnutosti stanja njihovih pridruženih stanja je poznat pod nazivom *problem separabilnosti*.

Najjednostavnija stanja unutar razreda separabilnih stanja su produkt stanja, oblika $\rho_{AB} = \rho_A \otimes \rho_B$, ρ_A i ρ_B su, također, redukovani statistički operatori za dva podsistema,

i oni nisu uzajamni. Kada postoji uzajamnost između osobina podsistema opisanih separabilnim stanjima, oni se mogu u potpunosti posmatrati lokalno, jer razdvojena kvantna stanja ρ_A i ρ_B unutar prostorno razdvojenih laboratorija daju zadovoljavajuće opise pridruženih osobina A i B, poput prethodno istaknute. Ishodi lokalnih mjerenja na bilo kojem separabilnom statističkom operatoru se mogu simulirati teorijom lokalno skrivenih varijabli. Kvantna stanja u kojima se mogu uočiti veze između A i B koje krše nejednakost Bellovog tipa se ne mogu objasniti. Međutim, ovo ne vrijedi za miješana spregnuta stanja.

Nedostatak kršenja Bellove nejednakosti, kao potrebnog uslova za spregnutost, ogleda se u tome što je nepoznato postoje li kršenja Bellove nejednakosti za mnoga neseparabilna miješana stanja. Moguće je podesiti da neka stanja krše Bellovu nejednakost. Za stanja koja ne krše Bellovu nejednakost, kažemo da su *vezana stanja.* Spregnutost stanja je invarijantna prema lokalnim operacijama, pa se lokalne operacije i kvantna komunikacija ne bi trebale povećavati. To su centralne pretpostavke pri kvantifikovanju spregnutosti.

4.3 Schmidt-ova dekompozicija

Postoje posebne dekompozicije stanja, kroz koje se jasno manifestuju korelacije vezane za spregnutost. Jedna od njih je Schmidt-ova[1] dekompozicija (u slučaju čistih biparitetnih stanja). Bilo koje biparitetno čisto stanje

$$|\Psi\rangle \in \mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B},$$

može biti napisano u obliku sume. Postoji barem jedna ortonormalna baza za $\mathcal{H}$, $\{|u_i\rangle \otimes |v_i\rangle\}$, gdje je $\{|u_i\rangle\} \in \mathcal{H}_\mathcal{A}$ i $\{|v_i\rangle\} \in \mathcal{H}_\mathcal{B}$, tako da je

$$|\Psi\rangle = \sum_i a_i \, |u_i\rangle \otimes |v_i\rangle \, ,$$

gdje $a_i \in \mathbb{C}$, predstavlja Schmidt-ovu bazu. Ova reprezentacija predstavlja Schmidt-ovu dekompoziciju $|\Psi\rangle$. Indeks sume ide samo do manje od odgovarajuće dvije dimenzije Hilbertovog prostora (dim $\mathcal{H}_\mathcal{A}$ i dim $\mathcal{H}_\mathcal{B}$). Zgodno je uzeti da su amplitude a_i realni brojevi, apsorbujući bilo koje faze u definicije $\{|u_i\rangle\}$ i $\{|v_i\rangle\}$. Međutim, dostupnost ove dekompozicije u multiparitetnim sistemima je ograničena. Sa sigurnošću je dostupna samo u biparitetnim stanjima. Za bilo koje spregnuto biparitetno čisto stanje, moguće je naći parove mjerljivih veličina, koje narušavaju Bell-ovu nejednakost. Tačnije, Schmidt-ove opservable

$$U = \sum_i u_i \, |u_i\rangle \langle u_i| \, , \qquad V = \sum_i v_i \, |v_i\rangle \langle v_i| \, ,$$

[1] Erhard Schmidt (13. 1. 1876.-6. 12. 1959.), baltičko-njemački matematičar. Značajan je njegov uticaj na tok razvoja matematike 20. vijeka.

su potpuno uzajamne, kada je sistem u stanju $|\Psi\rangle$, pri čemu su ovakva narušavanja moguća. Broj amplituda a_i, čija je vrijednost različita od nule u Schmidt-ovoj dekompoziciji kvantnog stanja, naziva se Schmidt-ov broj, ili Schmidt-ov rang. Koristan je pri uočavanju spregnutih stanja, veći je od 1, ako i samo ako se radi o spregnutom stanju. Također je koristan pri gruboj procjeni količine spregnutosti u sistemu (*kriterijum za spregnutost*). Definiše se kao

$$Sch\left(|\Psi\rangle\right) \equiv dim\ supp(\rho_A) = dim\ supp(\rho_B),$$

gdje su ρ_A i ρ_B redukovani statistički operatori za dva podsistema:

$$\rho_A = \sum_i |a_i|^2 |u_i\rangle \langle u_i|$$

$$\rho_B = \sum_i |a_i|^2 |v_i\rangle \langle v_i| ,$$

koji su dijagonalni, istog spektra vlastitih vrijednosti, te stoga i jednakih von Neumannovih entropija. Vrijedi očuvanje Schmidt-ovog broja pri lokalnim unitarnim transformacijama stanja. Koristeći Schmidt-ovu dekompoziciju, Schmidtova mjera spregnutosti čistog stanja će biti

$$E_s\left(|\Psi\rangle\right) \equiv \log_2\left(Sch\left(|\Psi\rangle\right)\right),$$

pa se spregnutost dobije u jedinicama *e-biti* (Schumacher)[2], gdje Bell-ova stanja odgovaraju jednom e-bitu spregnutosti. Kvadrati koeficijenata a_i (vjerovatnoće) su upravo veličine nepromijenjene unitarnim operacijama, izvedenim lokalno na pojedinačnim podsistemima (LUT- *Local Unitary Transformation*). Stoga se očekuje da je moguće izračunavati bilo koje preciznije numeričko mjerenje spregnutosti čistog stanja pomoću $|a_i|^2$. Ne postoji jedinstvena Schmidt-ova baza, jer je moguće da ρ ima degenerisane vlastite vrijednosti. Ako se posmatra sistem sa tri podsistema, pri Schmidt-ovoj dekompoziciji, mjerenja jednog podsistema bi odredila i stanja preostala dva. Međutim, ako su ova dva podsistema spregnuta, onda pojedinačna stanja moraju biti neodređena, iz čega slijedi da ova dekompozicija nije uvijek dostupna van slučaja biparitetnih sistema.

[2]Benjamin "Ben" Schumacher, američki teorijski fizičar. Značajan je njegov doprinos razvoju teorje kvantne informacije. Otkrio je način na koji se kvantna stanja interpretiraju kao informacija.

4.4 Stokesovi parametri

Posmatra se uopšteno stanje para qubita. Stokesovi[3] parametri za dvije čestice, koji predstavljaju poopštenje Stokesovih tradicionalnih parametara,

$$S_{\mu\nu} \equiv tr\left(\rho\sigma_\mu \otimes \sigma_\nu\right),$$

gdje su $\mu, \nu = 0, 1, 2, 3$, potrebni su za opisivanje spregnutih stanja u realnoj reprezentaciji, zbog povećavanja kompleksnosti kvantnih stanja porastom broja qubita. Stokesovi parametri za dva qubita se također mogu koristiti i za nalaženje dvo-qubitnog statističkog operatora,

$$\rho = \frac{1}{4}\sum_{\mu,\nu=0}^{3} S_{\mu\nu}\sigma_\mu \otimes \sigma_\nu,$$

gdje su $\sigma_\mu \otimes \sigma_\nu$ tenzorski produkti Paulijevih matrica. Ako je μ (ili ν) nula, ponovo se dobijaju Stokesovi parametri za jedan qubit, te je odgovarajući faktor matrica identiteta.

4.5 Svjedoci spregnutosti

Svjedoci spregnutosti omogućavaju raspoznavanje spregnutih stanja. Svjedoče da postoji spregnutost. Svjedok spregnutosti je definisan kao hermitski operator takav da je njegova očekivana vrijednost pozitivna za svako separabilno stanje, ali negativna za neka spregnuta stanja. Dakle, spregnutost se može detektovati preko očekivane vrijednosti svjedoka spregnutosti. Negativna vrijednost ukazuje na spregnutost sistema. Preciznije, statistički operator ρ na složenom sistemu prostora $\mathcal{H}_\mathcal{A}\otimes\mathcal{H}_\mathcal{B}$ je spregnut, ako i samo ako postoji svjedok spregnutosti, hermitska matrica W, takva da je $tr(\rho W) < 0$, ali $tr(\rho^{(S)}W) \geq 0$ za sva separabilna stanja $\rho^{(S)}$. Ovakav operator će imati barem jednu negativnu vlastitu vrijednost. Najpoznatiji ovakav operator je Bell-ov operator $\mathcal{B}$. Mjerenjem vrijednosti svjedoka spregnutosti za stanje datog sistema, može se odrediti da li je stanje spregnuto. Ukoliko je očekivana vrijednost negativna, ne može biti riječ o separabilnom stanju.

4.6 Spregnutost kao izvor

U kvantnoj komunikaciji, kao izvor služe skupine qubita, na primjer, za slanje kopija čistih stanja od odašiljača do prijemnika za distribuciju kvantnog ključa. Osim toga,

[3]Sir George Gabriel Stokes, prvi Baronet (13. 8. 1819.-1. 2. 1903.), anglo-irski fizičar i matematičar. Cijelu karijeru je proveo na Cambridge Univerzitetu. Značajan je njegov doprinos u dinamici fluida i optici.

skupine zajedničkih spregnutih qubita omogućavaju izvedbu zadataka vezanih za obradu kvantne informacije, kao i implementaciju jedinstvenih oblika kvantne komunikacije (poput teleportacije i kvantnog kodiranja). Prenosivi qubiti čine usmjeren izvor, a spregnutost nije usmjerena.

Spregnutost se može posmatrati kao fizički izvor sličan energiji, koji može postojati u nekoliko oblika (koji mogu prelaziti jedan u drugi) i koji se može prenositi između različitih tipova kvantnih sistema. Da bi se našlo koliko tačno dijele ovog izvora (spregnutosti biparitetnih sistema), dvije strane mogu "držati" Bell-ova singlet stanja između sebe. Tačnije, mogu *prečistiti* najveći mogući broj singlet stanja $k < n$ od n kopija početnog biparitetnog čistog spregnutog stanja $|\Phi\rangle_{AB}$, pomoću kolektivne LOCC (Collective Local Operation and Classical Communication):

$$|\Phi\rangle_{AB}^{\otimes n} \to \left|\Psi^{-}\right\rangle_{AB}^{\otimes k}.$$

Prečišćavanje se može provesti sa efikasnošću datom von Neumann-ovom entropijom $S(\rho)$, gdje je ρ redukovani statistički operator podsistema od AB. Postoji asimptotska šema u kojoj se inverzno pretvaranje

$$\left|\Psi^{-}\right\rangle_{AB}^{\otimes k} \to |\Phi\rangle_{AB}^{\otimes n},$$

može izvesti pomoću CLOCC, sa jednakom efikasnošću, što znači da je ovo reverzibilan proces. Ovo je najefikasnija šema prečišćavanja spregnutosti (uslov monotonosti). Baš poput toplotne energije, spregnutost se ne može povećati lokalnim operacijama na međusobno udaljenim podsistemima.

5 Primjena kvantne spregnutosti: Kvantna komunikacija

Saopštavanje informacija između dva prostorno udaljena objekta zahtjeva usmjeren izvor, poput bita ili qubita, koji je po prirodi ograničen brzinom svjetlosti, i u slučaju kvantne informacije podliježe ograničenjima. Uprkos značaju spregnutosti u komunikaciji, klasična komunikacija se ne može simulirati samo pomoću izvora zajedničke kvantne spregnutosti, u cilju da se zaobiđe ograničenje brzine svjetlosti, zbog neusmjerene prirode spregnutosti.

U direktnom prenosu kvantnog sistema, zahtjevi izvora komunikacije su zadovoljeni putem jednog kanala. U kvantnoj teleportaciji, zahtjevi izvora su zadovoljeni putem dva udaljena sistema, jednog koji prolazi kroz klasični kanal, kao klasična informacija i drugog, koji prolazi kroz kvantni kanal, da bi prenio kvantnu informaciju. Kvantno kodiranje koristi prethodno podijeljenu spregnutost i klasičnu komunikaciju, s ciljem udvostručavanja sposobnosti kvantnog kanala da prenosi klasičnu informaciju. Zamjena spregnutosti i pročišćavanje spregnutosti su zadaci koji se odnose na raspodjelu kvantnog izvora. Kvantna kriptografija koristi i klasični, i kvantni kanal, za sigurnu raspodjelu uzajamnih ključeva.

5.1 Kvantni kanali

Kvantni kanal je sredstvo prenosa kvantne informacije. Poput optičkog vlakna, kvantni kanal predstavlja medijum prenosa informacije, zajedno sa ansamblom kvantnih sistema, poput fotona, kojeg priprema odašiljač u kvantnim stanjima ρ_i, $i = 1, 2, ..., n$. Kvantni kanali koji prenose informaciju bez grešaka su *bešumni* kvantni kanali, a kvantni kanali koji unose greške u prenos informacija su *bučni* kvantni kanali. Međutim, klasični i kvantni kanali se značajno razlikuju. Zbog neizbježne i, u opštem slučaju ireverzibilne interakcije prenesenih kvantnih sistema sa okolinom stvarnog kvantnog kanala, ulazno kvantno stanje, kao takvo, neće se moći ponovo dobiti iz samih izlaznih stanja samo unitarnim transformacijama. U teoriji kvantnog signala je dopušteno korištenje kodiranja-dekodiranja u svrhu poboljšanja vjernosti signala. Korisno je ponovo razmotriti vjernost

$$F\left(|\psi\rangle, \rho'\right) = \langle\psi| \rho' |\psi\rangle,$$

da bi se shvatio koncept kvantnog kanala, kroz koji se može poslati čisto kvantno stanje $|\psi\rangle$. Ovdje je ρ' stanje sistema poslije prenosa, kao mjera vjernosti kanala. Kvantni kanal je vjeran, ako ova očekivana vrijednost ide u jedinicu u odgovarajućoj granici obrade informacija.

Za većinu kvantnih kanala se uzima da su stacionarni i da *nemaju pamćenje*, da bi imali isti efekat na svaki blok qubita kojeg bi mogli prenositi. Kvantni kanal koji je bešuman i bez izobličenja, opisan je operatorom identiteta $\mathbb{I}$ i u potpunosti će očuvati kvantnu koherentnost ulaznog stanja. Drugo ekstremno stanje je dekoherentni kanal, koji uništava sve vandijagonalne elemente statističkog operatora, tako da

$$\rho \to \rho' = \sum \rho_{ii} P\left(|\psi_i\rangle\right).$$

Potpuno dekoherentni kanal može savršeno prenositi klasičnu informaciju, ali će uništiti sve koherentne osobine ključne za vjerno prenošenje kvantne informacije. Zanimljivo je da se odnos klasičnog kapaciteta potpomognutog spregnutošću i klasičnog kapaciteta bez pomoći spregnutosti, u opštem slučaju, povećava sa vrijednošću šuma u kvantnom kanalu, čak i kad kvantni kapaciteti idu u nulu.

5.2 Sposobnost razlikovanja kvantnih stanja

Korištenje kvantnih kanala za slanje informacija ima određene prednosti u odnosu na korištenje klasičnih kanala. Na primjer, korištenje qubita za šifriranje bita dopušta distribuciju kvantnog ključa bez povjerljivog glasnika, tako da je obezbijeđena kriptografska sigurnost zasnovana na osnovnim principima fizike, što se nije postiglo klasičnim putem. Sposobnost razlikovanja mogućih signala u komunikaciji je ključna za bilo koju vrstu prenosa informacije (kvantne ili klasične). Problem razlikovanja kvantnih stanja je esencijalan za distribuciju kvantnog ključa, kao i za mnoge probleme osnova kvantne teorije.

Za uspješnu kvantnu komunikaciju, moraju se *razlikovati* različita stanja, u kojima se kvantni sistem može pripremiti. Osim u slučaju da mjerena grupa sistema čini ansambl ortogonalnih podansambala, dato stanje se ne može savršeno razlikovati od ostalih mogućih stanja, te se mora naći optimalan pristup za razlikovanje ovih mogućnosti. Mogućnost savšenog razlikovanja svih članova seta neortogonalnih stanja bi protivrječio teoremu o nerazlikovanju. Ova činjenica je osnova protokola distribucije kvantnog ključa (QKD- Quantum Key Distribution), koji su zasnovani na korištenju stanja iz srodne neortogonalne baze. Problem određivanja stanja pojedinačnih qubita u jednom od dva ne nužno ortogonalna stanja $|p\rangle$ i $|q\rangle$ se eksplicitno razmatrao osamdesetih godina.

Ovom problemu se pristupilo na nekoliko načina. Jedan od pristupa razmatra problem sada poznat kao problem testiranja hipoteze ili razlikovanje dvoznačnih stanja.

Potrebno je pronaći postupak koji prosječno daje maksimalan broj tačnih klasifikacija stanja u ansamblu ovakvih slučajeva, sa pretpostavkom da je za svaki član ansambla napravljena konačna klasifikacija.

U drugom pristupu se posmatra problem razlikovanja jednoznačnih stanja. Ovaj pristup će biti opisan u nastavku. Potrebno je naći postupak koji, u maksimalnom broju slučajeva, omogućava da se može sa sigurnošću zaključiti da li je sistem pripremljen u $|p\rangle$ ili $|q\rangle$, ostavljajući tako minimalan broj neklasifikovanih slučajeva.

Rješenje problema razlikovanja jednoznačnih stanja u jednostavnom slučaju, u kojem se pretpostavlja da je pola ansambla pripremljeno u stanju $|p\rangle$, a drugo pola u stanju $|q\rangle$ (idealan slučaj u BB84 protokolu), pronađeno je kroz evaluaciju maksimalne vjerovatnoće tačne klasifikacije i minimalne vjerovatnoće da nema odluka:

$$P = 1 - |\langle p|\, q\rangle|\,,$$

što predstavlja vjerovatnoću ispravne klasifikacije. Izraz

$$1 - P = |\langle p|\, q\rangle|\,,$$

predstavlja vjerovatnoću da ne postoji klasifikacija. $|\langle p|\, q\rangle|$ je mjera stepena nerazlikovanja ova dva stanja. Da bi se bolje shvatio ovaj rezultat, uzima se u obzir priprema pomoćnog sistema unutar početnog stanja $|s_0\rangle$, kao dodatak datom qubitu, te izazivanje razvoja unitarnog stanja na rezultujućem složenom sistemu:

$$|p\rangle\,|s_0\rangle \to a\,|p_1\rangle\,|s_1\rangle + b\,|p_2\rangle\,|s_2\rangle\,,$$

$$|q\rangle\,|s_0\rangle \to c\,|q_1\rangle\,|s_1\rangle + d\,|q_2\rangle\,|s_2\rangle\,.$$

Vektori stanja su ortogonalni, tako da je

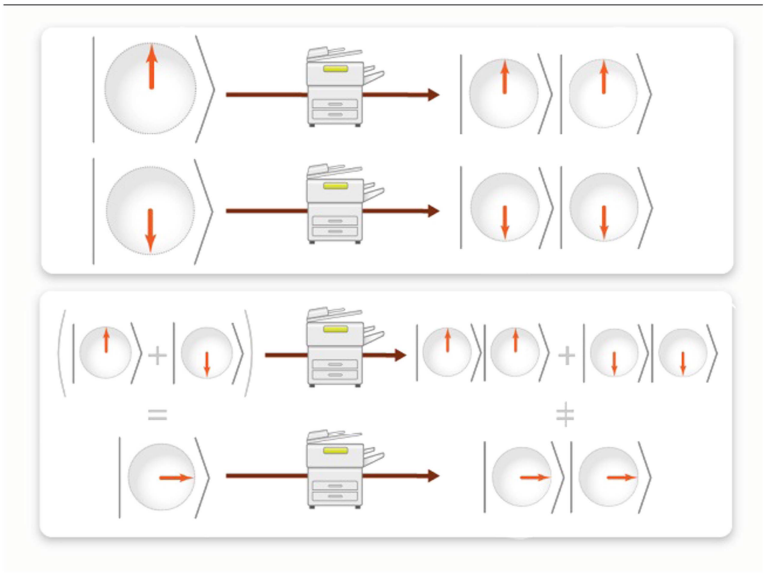
$$\langle p_1|\, q_1\rangle = 0,$$

$$\langle s_1|\, s_2\rangle = 0.$$

Ovaj proces pruža mogućnost mjerenja pomoćnog sistema koji razlikuje $|s_1\rangle$ i $|s_2\rangle$ (što se inače obavlja pomoću "prisluškivača" distribucije kvantnog ključa). U stanju $|s_1\rangle$, rezultati mjerenja p_1 i q_1 određuju da li je qubit u stanju $|p\rangle$ ili $|q\rangle$. U stanju $|s_2\rangle$, qubit mora biti u stanju $|p_2\rangle$ ili $|q_2\rangle$.

No-cloning teorem

No-cloning teorem je izravna matematička demonstracija nemogućnosti kloniranja nepoznatog kvantnog stanja unitarnim operacijama.



Slika 5.2.1: Ilustracija *no-cloning* teorema: Kopirni aparat, koji bi mogao uspješno klonirati stanja $|\psi\rangle$ i $|\phi\rangle$, davao bi netačan rezultat superpozicije datih stanja. Savršena kvantna mašina za kloniranje ne može postojati. [4]

Problem povezan sa rezultatima vezanim za prethodni dio (sposobnost razlikovanja kvantnih stanja) jeste problem kopiranja kvantnih stanja. Nije moguće napraviti savršene kopije nepoznatog stanja kvantnog sistema unitarnim transformacijama. Ovakvom operacijom bi se dozvolilo istovremeno mjerenje dvije osobine, koje predstavljaju operatori koji ne komutiraju, što osnovni principi kvantne mehanike ne dozvoljavaju. Da bi se provjerila ova tvrdnja, posmatra se unitarna operacija U, koja može na dva različita neortogonalna vektora, $|\psi\rangle$ i $|\phi\rangle$, izvesti obje transformacije:

$$|a\rangle\,|\psi\rangle \rightarrow |\psi\rangle\,|\psi\rangle\,,$$

$$|a\rangle\,|\phi\rangle \rightarrow |\phi\rangle\,|\phi\rangle\,.$$

Rezultat ovih transformacija su savršene kopije dva nepoznata vektora $|\psi\rangle$ i $|\phi\rangle$, načinjena od datog kvantnog stanja $|a\rangle$. Ova transformacija bi, u tom slučaju, dala

$$\langle\psi|\,\phi\rangle = \langle\psi|\,\langle a|\,a\rangle\,|\phi\rangle = c \Rightarrow \langle\psi|\,\langle\psi|\,\phi\rangle\,|\phi\rangle = \langle\psi|\,\phi\rangle\,\langle\phi|\,\psi\rangle = (\langle\psi|\,\phi\rangle)^2 = c^2,$$

što je moguće samo ako je $c = 0$ ili $c = 1$, a to bi značilo da su ovi vektori ortogonalni, što je suprotno pretpostavci. Dakle, ne postoji unitarna operacija, koja bi mogla stvoriti identične kopije nepoznatog kvantnog stanja, putem ovakvog procesa. Istovremeno, ovaj račun je kompatibilan sa važnim zadatkom kopiranja stanja iz poznate ortogonalne baze.

Nemogućnost postojanja univerzalnog postupka kloniranja predstavlja snažnu razliku između klasične i kvantne informacije, te ima široke praktične mogućnosti, poput pružanja sigurnosti pri distribuciji kvantnog ključa. Praktični problem od interesa je postizanje optimalnog univerzalnog kopiranja.

5.3 Kvantna teleportacija

Alternativni način postizanja prenosa kvantne informacije jeste putem teleportacije. Spregnuto stanje, poput

$$\left|\phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle\right),$$

koristi se kao izvor. Naziv *teleportacija* vrlo vjerovatno podsjeća na naučnu fantastiku, na primjer, na beamovanje u Star Treku. Teleportacija je fizički izvodiva, te je već eksperimentalno demonstrirana.

Kvantna spregnutost između dvije *strane*, Alice i Boba, koristi se za prenos nepoznatog stanja dodatnog kvantnog sistema. Za razliku od beamovanja, prenosi se samo kvantna informacija, a ne i materija. Spregnutost mora postojati unaprijed, i *in-coupling* mjerenje na Aliceinoj strani napušta sistem na Bobovom kraju, u stanju koje je (do na rotaciju) jednako početnom stanju

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle,$$

koje se teleportira od Alice do Boba. U ovom slučaju, stanje $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ na Aliceinom kraju je uništeno, zbog *no-cloning* teorema. Dakle, dva bita klasične informacije, koja su rezultat mjerenja u bazi maksimalno spregnutih stanja, moraju biti prenesena, inače bi stanje na Bobovoj strani bilo potpuno nasumično i ne bi sadržavalo nikakvu informaciju. Zbog ovoga je sigurno da se nijedna informacija ne može prenositi brzinom većom od brzine svjetlosti (kvantna mehanika poštuje osnovne principe relativiteta, iako relativitet nije eksplicitno uključen u kvantnomehaničke aksiome).

Da bi se bolje razumjela teleportacija, posmatra se sljedeće: $|\psi\rangle_{\tilde{A}}$ je početno stanje, koje će se teleportirati od Alice do Boba, a $|\phi^{+}\rangle_{AB}$ je spregnuto stanje, koje obezbjeđuje kvantna mreža, za postizanje ovog cilja. Pomoću Bell-ove baze

$$\left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right),$$

$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

u sistemu $\tilde{A}A$, početno stanje se može drugačije zapisati, koristeći

$$|00\rangle = \frac{1}{\sqrt{2}}\left(\left|\phi^{+}\right\rangle + \left|\phi^{-}\right\rangle\right),$$

$$|11\rangle = \frac{1}{\sqrt{2}}\left(\left|\phi^{+}\right\rangle - \left|\phi^{-}\right\rangle\right),$$

$$|01\rangle = \frac{1}{\sqrt{2}}\left(\left|\psi^{+}\right\rangle + \left|\psi^{-}\right\rangle\right),$$

$$|10\rangle = \frac{1}{\sqrt{2}} \left(\left|\psi^+\right\rangle - \left|\psi^-\right\rangle \right).$$

Tada je

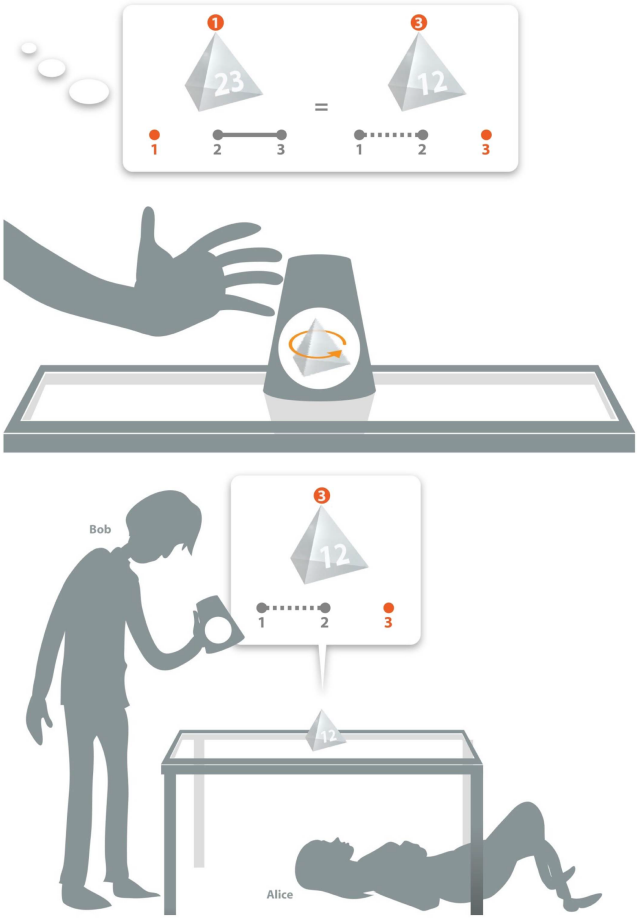
$$\begin{aligned} |\psi\rangle_{\tilde{A}} |\phi\rangle_{AB} &= \alpha |000\rangle + \alpha |011\rangle + \beta |100\rangle + \beta |111\rangle = \\ &= \frac{1}{2} \left[\left|\phi^+\right\rangle_{\tilde{A}A} (\alpha |0\rangle + \beta |1\rangle)_B + \left|\phi^-\right\rangle_{\tilde{A}A} (\alpha |0\rangle - \beta |1\rangle)_B \right. \\ &\quad \left. + \left|\psi^+\right\rangle_{\tilde{A}A} (\alpha |1\rangle + \beta |0\rangle)_B + \left|\psi^-\right\rangle_{\tilde{A}A} (\alpha |1\rangle - \beta |0\rangle)_B \right]. \end{aligned}$$

Koeficijenti α i β, pa stoga i Aliceino početno stanje $|\psi\rangle$, pojavljuju se na Bobovoj strani. To ne znači da Bob već posjeduje stanje $|\psi\rangle$, čak što više, Bobovo stanje je potpuno miješano, $\rho_B = \frac{1}{2}\mathbb{I}$, i ne sadrži nikakvu informaciju. Bilo koje mjerenje daje nasumičan ishod, što se može vidjeti korištenjem početnog načina zapisivanja stanja u kojem je Bob dio maksimalno spregnutog para. Alice može izvesti mjerenje na njenom dijelu sistema, projektujući jednačinu superponiranog stanja nasumično u jednu od četiri mogućnosti. Slijedi da Bob mora primijeniti jednu od četiri moguće operacije ispravljanja na svoj qubit (vidjeti referencu [4]), da bi dobio željeno stanje. Međutim, za ovo mora znati rezultat Bell-ovog mjerenja, koji mora biti saopšten klasičnim putem.
Na primjer, ako Alice dobije rezultat $|\psi^+\rangle$, rezultujuće stanje nakon mjerenja je dato sa

$$\left|\psi^+\right\rangle_{\tilde{A}A} (\alpha |1\rangle + \beta |0\rangle)_B ,$$

pa je na Bobovoj strani potrebna ispravka σ_x, koja zamjenjuje $|0\rangle \leftrightarrow |1\rangle$, da bi se dobilo stanje $|\psi\rangle$ (slično i za ostale tri mogućnosti). Proces teleportacije se vidi na Slici 5.3.1. Stanje se odmah redukuje. Mjerenje se može shvatiti kao promjena onoga što se zna o situaciji, gdje se jedna od četiri mogućnosti nasumično ostvaruje. Međutim, bez klasične informacije na potrebnoj operaciji ispravke, nije postojao prenos kvantne informacije. Također, moguće da je Bobova lokacija nepoznata. On jednostavno treba da primi klasičnu informaciju o rezultatima mjerenja, što ne daje nikakve informacije o teleportiranom kvantnom stanju, pa se ne mora prenositi tajno. Prenosnici informacija za ulaz i izlaz se ne moraju podudarati. Dalje, qubit na Bobovoj strani u potpunosti preuzima ulogu teleportiranog qubita. Važno je da sve informacije o teleportiranom stanju na Aliceinoj strani nestanu (zbog *no-cloning* teorema).

Da je na početku ovaj qubit bio spregnut sa trećim sistemom, C, Bobov qubit bi, konačno, bio spregnut sa njim. Ovaj proces se naziva *zamjena spregnutosti* (*entanglement swapping*) i igra važnu ulogu u generaciji spregnutih parova na daljinu. Teleportacijom pojedinačnih qubita složenog sistema, može se postići teleportacija kompleksnog objekta. Problem kvantne komunikacije je tada redukovan na problem stvaranja maksimalno spregnutih parova qubita u kvantnoj mreži.



Slika 5.3.1: Teleportacija: Prije mjerenja, postoji superpozicija stanja tri qubita, figura u obliku tetrahedrona još nije pala. *Bell* mjerenje na qubitima $\tilde{A}A$ na Aliceinoj strani odgovara popravljanju stanja ovih qubita, *kocka* je bačena, i pala je na jednu svoju stranu. Ovo popravlja stanje qubita B na jedno od suprotnih tjemena tetrahedrona. Nakon prenosa klasične informacije o ishodu mjerenja, Bob može rotirati svoj qubit i vratiti početno stanje qubita $\tilde{A}$, qubiti $\tilde{A}AB$ su obilježeni sa 1, 2, 3. [4]

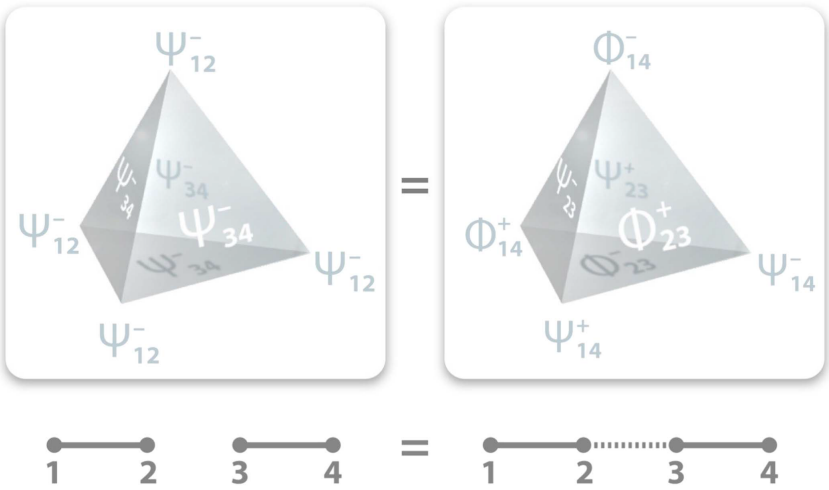
Zamjena spregnutosti

Još jedan zadatak u obradi kvantne informacije je preraspodjela spregnutosti. Na primjer, ako su na početku dvije čestice spregnute sa svojim česticama *partnerima*, ali ne i jedna sa drugom, to mogu postati ako se izvrši odgovarajuće mjerenje na dva qubita (na jednom iz svakog para). Ovo se postiže *zamjenom* spregnutosti.

Ovaj se proces može razmotriti u kontekstu optike. Posmatraju se dva para fotona, koja istovremeno nastaju u Bell singlet stanjima iz dva izvora. Oba para su nastala u SPDC (Spontaneous Parametric Down-Conversion) procesu, u odvojenim nelinearnim kristalima. Fotoni iz prvog para su označeni sa 1 i 2, a fotoni iz drugog para su označeni sa 3 i 4. Izvodeći Bell-ovo mjerenje na dva fotona (na po jednom iz svakog izvora), dobija se projekcija stanja preostala dva fotona, također iz različitih izvora, na Bell-ovo stanje. Dolazi do zamjene *uparenosti* spregnutih fotona. U tom smislu, dolazi do premještanja spregnutosti. Početno stanje para fotonskih parova, napisano na sljedeći način, pokazuje važne korelacije:

$$\begin{aligned}|\Xi\rangle &= \frac{1}{2}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)_{12}\left(|0\rangle|1\rangle - |1\rangle|0\rangle\right)_{34} \\ &= \frac{1}{2}\left(|\psi^+\rangle_{14}|\psi^+\rangle_{23} + |\psi^-\rangle_{14}|\psi^-\rangle_{23} + |\phi^+\rangle_{14}|\phi^+\rangle_{23} + |\phi^-\rangle_{14}|\phi^-\rangle_{23}\right).\end{aligned}$$

Bellovo mjerenje pridruženog stanja fotona 2 i 3, na primjer, dat će za rezultat da su fotoni 1 i 4 u istom Bell-stanju, kao i fotoni 2 i 3. Na ovaj način je postignuta preraspodjela spregnutosti između fotona.



Slika 5.3.2: *Zamjena* spregnutosti. [4]

Nedavni eksperimenti

Ubrzo nakon prvog objavljenog članka 1993. godine, koji uvodi i objašnjava ideju o kvantnoj teleportaciji, (vidjeti referencu [5]), došlo je i do prvih eksperimentalnih testiranja. U nastavku su navedeni neki od tih eksperimenata.

- 1997. godine, dva tima naučnika, jedan iz Italije (vidjeti referencu [6]), i jedan iz Austrije (vidjeti referencu [7]), pokazali su da je moguća teleportacija kvantnog stanja fotona, od pošiljaoca, do udaljenog primaoca. Ovaj proces je obuhvatao par spregnutih fotona. Jedan od tih fotona je, prije procesa teleportacije, dodijeljen primaocu. Pošiljalac, zatim, priprema foton u nepoznatom kvantnom stanju, nakon čega uparuje ovaj foton sa drugim spregnutim fotonom, u uređaju koji se naziva *Bell-state analyser*. Ovaj uređaj vrši pridruženo mjerenje kvantnih stanja dva fotona, te šalje rezultat primaocu, u obliku klasičnog signala. Konačno, primalac koristi ovu informaciju za transformaciju svog fotona, ponovo stvarajući kvantno stanje fotona pošiljaoca.

- 2003. godine, jedan od najistaknutijih eksperimenata u ovoj oblasti je demonstrirao teleportaciju na velikim udaljenostima (do 140 km), između dva Kanarska ostrva (vidjeti referencu [10]). U ovom procesu su, također, korišteni fotoni.

- 2017. godine, naučnici iz Kine, na čelu sa Jian-Wei Pan-om (vidjeti referencu [11]), uspješno su izvršili teleportaciju kvantnog stanja fotona sa postaja na Zemlji, do satelita Micius (udaljenosti do 1400 km).

5.4 Kvantna kriptografija

Kriptografija (grčki: kryptos-skriveno, graphia-pisanje) predstavlja metodu pružanja bezbjednosti informacija, onemogućujući neželjenim primaocima pristup privatnim informacijama putem enkripcije. Kriptoanaliza je metodologija za dešifrovanje informacija kodiranih na ovaj način. Za uspješno sprovođenje kriptografije, prvo se koristi algoritam pod nazivom kriptosistem, koji transformiše (dekodira) informaciju tako da ostane tajna, što zahtjeva korištenje dodatnih informacija (*key*), te se za rezultat dobija kriptogram. U idealnom slučaju, algoritmi enkripcije i dekripcije biraju se na način da, za neželjenog primaoca, dešifrovanje bez ključa bude ekvivalentno dešifrovanju iscrpnom pretragom svih mogućih kriptografskih ključeva.

Kriptosistemi mogu biti simetrični (koriste isti ključ za enkripciju i dekripciju) i asimetrični (koriste različite ključeve za enkripciju i dekripciju).

Public key (*javni ključ*) kriptosistemi su asimetrični. Oni funkcionišu na sljedeći način. Primalac privatne poruke, Bob, stvori ili dobije *privatni ključ*, koji čuva u tajnosti. Bob zatim stvori odgovarajući javni ključ, koristeći privatni ključ, i pruži ga eventualnom pošiljaocu, Alice. Alice koristi Bobov javni ključ za enkripciju njene poruke i prenosi je Bobu. Konačno, Bob dešifruje kriptogram koji je proizvela Alice, koristeći njegov javni ključ. Sigurnost ovog kriptosistema se temelji na računarskoj kompleksnosti dekripcije poruka.

Jedini dokazano siguran kriptosistem jeste simetrični Vernam kriptosistem. Pošiljalac Alice kodira svoju poruku, M, u formi niza *plaintext* bita, m_i, korištenjem nasumičnog niza (*keystream* K) bita, k_i, sumiranjem preko binarnog sabiranja svakog bita poruke sa odgovarajućim bitom ključa, što za rezultat daje enkriptovani niz bita

$$c_1 c_2 ... c_n = (m_1 \oplus k_1)\,(m_2 \oplus k_2)\,...\,(m_n \oplus k_n)\,,$$

što čini kriptogram C. Nakon prenosa, primalac Bob dešifruje poruku korištenjem istog ključa, inverznom operacijom binarnog oduzimanja, vraćajući

$$m_i = c_i \otimes k_i.$$

U ovom kriptosistemu vrijedi

$$H\,(M \mid C) = H\,(M)\,,$$

i

$$I(M:C) = 0,$$

tako da kriptogram ne daje nikakve informacije o *plain text* poruci. Ova metoda je bezuslovno bezbjedna, bez obzira na statističke osobine *plain text* poruke. Poteškoću ove metode, pored osobine da ključ mora biti jednako dug kao *plain text* poruka, predstavlja problem dijeljenja ključa između Alice i Boba (problem distribucije ključa). Tajni ključ se mora prenijeti povjerljivim sredstvom, poput glasnika kojeg nije moguće kompromitovati.

Distribucija kvantnog ključa

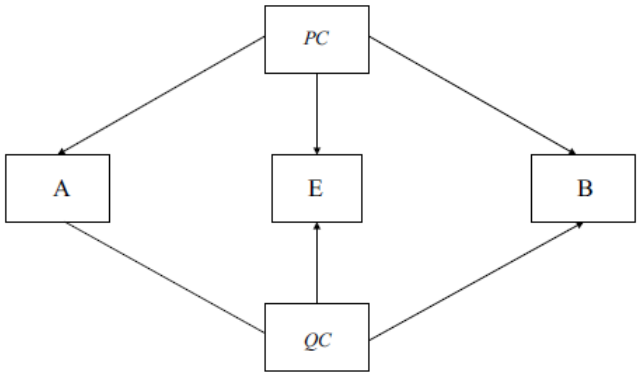
Najzastupljenija netrivijalna primjena kvantne informacije jeste distribucija kvantnog ključa (*Quantum Key Distribution - QKD*), koja predstavlja metodu bezbjedne distribucije materijala za kasniju kriptografsku upotrebu. Tačnije, to je podjela nasumičnih nizova bita, korištenjem kvantnih stanja. Kvantno kodiranje kriptografskih ključeva za distribuciju je vrijedno, jer *no-cloning* teorem i princip superpozicije daju jedinstveno snažan oblik sigurnosti informacija pri prenosu *key* bita.

QKD nudi rješenje problema kriptografske raspodjele ključa preko kvantnog kodiranja binarnih informacija, *koje zakoni fizike čine bezbjednim* (tačnije, principi kvantne mehanike). U kombinaciji sa Vernam kriptosistemom, distribucija kvantnog ključa nudi jedinstven nivo kriptografske sigurnosti, ukidanjem potrebe za povjerljivim ljudskim glasnikom. Iz tog razloga se QKD sistemi ponekad nazivaju *nepovjerljivim* (pored odgovarajuće fizičke operacije, nema potrebe za povjerljivošću sistema).

QKD funkcioniše na sljedeći način. Pošiljalac nasumičnog kriptografskog *key* materijala, Alice, kodira nasumične bite informacija u setu kvantnih stanja, koja nisu sva međusobno ortogonalna, na primjer, pojedinačnih fotona, koja se direktno ili indirektno dostavljaju primaocu Bobu kroz kvantni kanal, ili preko dijeljenja spregnutosti. Ako Bob primi ovu informaciju u nepromijenjenom stanju, stanja prenesenog fotona se mogu smatrati nepoznatima bilo kojem mogućem prisluškivaču. U ovom slučaju, nijedan prisluškivač neće dobiti željene informacije o *bit-coding* podprostorima stanja fotona, zbog fizičkih ograničenja, koja nameću Heisenbergove relacije neodređenosti i *no-cloning* teorem, koji proizilaze iz principa superpozicije. U praksi, komunikacijom putem klasičnog kanala, Alice i Bob mogu provjeriti da li je neko pokušao dobiti materijal iz njihovog zajedničkog kvantnog kanala, poređenjem nasumično izabranog podseta njihovog (sada zajedničkog) bit materijala. U slučaju bilo kakve perturbacije, dati materijal se smatra ugroženim, pa se, stoga, zanemaruje.

BB84 protokol

Postoji nekoliko protokola za distribuciju kvantnog ključa, čija je sigurnost utemeljena na fizičkim principima kvantne mehanike. Jedan od njih je i BB84 protokol, nastao 1984. godine, nazvan po svojim izumiteljima (Charles Bennet[1] i Gilles Brassard[2]). Sigurnost ovog protokola se temelji na činjenici da bilo koji pokušaj otkrivanja informacija o prenesenom kvantnom sistemu uključuje mjerenje, pa stoga i promjenu prenesenog stanja (sve dok se pravac mjerenja ne poklapa sa pravcem qubita). Ovu promjenu stanja je moguće detektovati i pomoću nje otkriti prisutnost prisluškivača. Nemoguće je klonirati stanje pojedinačnog qubita, kao i odrediti njegovo nepoznato stanje, kada je dostupna samo jedna kopija, što se može iskoristiti u svrhu kreiranja protokola u kojem je sigurnost zagarantovana zakonima prirode (odnosno, ponašanjem kvantnih sistema na kojima se vrše mjerenja). To se potpuno razlikuje od klasičnih kriptografskih šema, čija se sigurnost temelji na nedokazanim pretpostavkama složenosti, odnosno, poteškoće računanja određenih funkcija, ili izvođenja određenih zadataka. Ovaj problem se može riješiti pomoću kvantnog kompjutera (čim ga bude moguće izgraditi).



Slika 5.4.1: Šematski prikaz kvantnog kriptografskog sistema, koji uključuje pošiljaoca A i primaoca B. Kvantni kanal, QC, predstavlja privatni, jednosmjerni kanal. Klasični kanal, PC, predstavlja javni, dvosmjerni kanal. E predstavlja prisluškivača. [1]

U BB84 protokolu, pojedinačni qubiti se prenose od Alice do Boba, pa se onda mjere. Alice nasumično bira vrijednost bita $j \in \{0, 1\}$ i bazu $\alpha \in \{x, z\}$. Ona priprema qubit

[1] Charles Henry Bennet (rođen 1943. godine, u SAD), fizičar, teoretičar informacije i IBM Fellow.
[2] Gilles Brassard (rođen 1955. godine, u Kanadi), poznat po istraživanju u polju kvantne komunikacije (kvantna kriptografija, kvantna teleportacija, ...

u stanju $\{j_\alpha\}$, odnosno, u jednom od četiri stanja $\{|0\rangle, |1\rangle, |0_x\rangle, |1_x\rangle\}$. Bob nasumično bira bazu mjerenja $\beta \in \{x, z\}$ i vrši mjerenje u njoj (opservabla σ_x) na primljenom qubitu. U slučaju da je $\alpha = \beta$ (baza mjerenja se podudara sa bazom pripreme), Bob dobija konačan (deterministički) ishod, $|j_\beta\rangle$, iz kojeg može odrediti vrijednost bita, j. Kada ove baze nisu jednake, odnosno, kada je $\alpha \neq \beta$, rezultat mjerenja je nasumičan.

Primjer: Za $\alpha = x$ i $j = 0$, stanje $|0_x\rangle$ je preneseno, a za z-mjerenje, odnosno, $\beta = z$, dobiju se rezultati $|0\rangle$ i $|1\rangle$, sa vjerovatnoćom $p_0 = p_1 = \frac{1}{2}$.

Ukupno N nasumičnih qubita je preneseno do Boba, koji mjeri svaki qubit. U svakom krugu, vrijednost bita j i bazu pripreme α bira Alice nasumično. Također, Bob nasumično odabire bazu mjerenja β u svakom krugu. Nakon toga se kroz javni kanal otkrivaju korištene baze, α i β. Informacija je dostupna prisluškivaču (samo otkrivene baze, a ne i pripremljena i izmjerenja vrijednost bita). Ako je $\alpha = \beta$ u određenom krugu, onda se zna da se rezultati Bobovog mjerenja podudaraju sa pripremljenim stanjem, to jest, Alice i Bob dijele nasumičan bit j. Dakle, nakon N krugova, Alice i Bob dijele niz od $\tilde{N} \approx \frac{N}{2}$ nasumičnih bita. Za konačnu provjeru, Alice i Bob nasumično biraju M ovih bita i porede vrijednosti bita kroz javni kanal. Ako se svih M bita podudara, Alice i Bob mogu zaključiti da je prisluškivač mogao dobiti samo eksponencijalno malu količinu informacija o njihovom nizu nasumičnih bita. Preostalih $\tilde{N} - M$ bita se mogu koristiti kao niz nasumičnih bita, to jest, kao kriptografski ključ, i stoga, za bezbjedno prenošenje tajnih informacija. Ukoliko se većina odabranih bita ne podudara, onda se mora pretpostaviti da je prisluškivač ometao prenos, i da postoji mogućnost da je dobio informacije o cijelom nizu bita. U ovom se slučaju protokol obustavlja- nema prenosa informacija. Gubi se samo stvaranje ključa, ali prisluškivač se nije domogao nijednog dijela poruke.

Postoji nekoliko različitih strategija prisluškivanja. Prva strategija podrazumijeva da prisluškivač jednostavno pogodi vrijednost bita. Za svaki bit je moguće pogoditi tačnu vrijednost sa vjerovatnoćom $\frac{1}{2}$, bez da Alice i Bob nešto detektuju. Međutim, vjerovatnoća da se pogodi tačna vrijednost cijelog niza bita je $\left(\frac{1}{2}\right)^{\tilde{N}}$, dakle- eksponencijalno mala.

Druga strategija bi podrazumijevala da prisluškivač pohranjuje sve prenesene qubite do trenutka kada Alice i Bob otkriju korištenu bazu pripreme, i jednostavno pošalju različite qubite Bobu, u nasumično odabranom stanju. U ovom slučaju, prisluškivač sazna vrijednost bita za svaki qubit, pa i cijelog niza bita. Međutim, kad Bob izvrši mjerenje na primljenom qubitu, vrijednost bita koju on dobije će odgovarati vrijednosti koju je Alice prenijela samo sa vjerovatnoćom $\frac{1}{2}$- u kontrolnom koraku, veliki dio provjerenih bita se neće podudarati. Vjerovatnoća da se svi podudaraju je data sa $\left(\frac{1}{2}\right)^M$, pa je vjerovatnoća da se detektuje prisluškivač data sa $1 - \left(\frac{1}{2}\right)^M$.

Postoji i strategija prema kojoj se mjerenje vrši u nasumično izabranoj bazi $\gamma \in \{x, z\}$, na svakom qubitu, koji je prenesen. Ovo se naziva *individualni napad*. Ukoliko

onaj ko pokušava otkriti ključ tačno pogodi, to jest, ako je $\gamma = \alpha$, onda će se saznati vrijednost bita, i mjerenje neće promijeniti preneseno stanje. Međutim, ako prisluškivač vrši mjerenje u pogrešnoj bazi, odnosno, ako je $\gamma \neq \alpha$ (što se može desiti sa vjerovatnoćom $\frac{1}{2}$), preneseno stanje će biti promijenjeno. Na primjer, ako je preneseno stanje $|0_x\rangle$, i vrši se mjerenje u z-bazi, stanje nakon mjerenja će biti $|0\rangle$ ili $|1\rangle$. U oba slučaja, Bob će dobiti nasumičan ishod, ukoliko izvede x-mjerenja. Dakle, on će dobiti tačnu vrijednost bita sa vjerovatnoćom $\frac{1}{2}$, odnosno, sa istom vjerovatnoćom će dobiti pogrešnu vrijednost, što će biti naknadno detektovano u kontrolnom koraku. Zauzvrat, s obzirom na to da je rezultat mjerenja nasumičan, dobit će se tačna vrijednost bita sa vjerovatnoćom $\frac{1}{2}$. Ako prisluškivač bude koristio ovu strategiju, vjerovatnoća da dobije tačnu vrijednost bita je $p = \frac{3}{4}$, dok je vjerovatnoća da Bob dobije pogrešnu vrijednost data sa $p_{error} = \frac{1}{4}$. Stoga, za prisluškivača će biti poznat niz bita sa vjerovatnoćom $\left(\frac{3}{4}\right)^{\tilde{N}}$, dok je vjerovatnoća detektovanja greške u kontrolnom koraku data sa $1 - (1 - p_{error})^M = 1 - \left(\frac{3}{4}\right)^M$. Ako je M dovoljno veliko, pokušaj prisluškivanja će biti detektovan skoro sigurno. Dakle, bezbjedan prenos poruke je moguć. Ukoliko prisluškivač dobije bilo kakvu informaciju, doći će do promjene prenesenog stanja, to jest, do greške u vrijednosti bita, koju je dobio Bob. Ova greška se može eksponencijalno pojačati, te stoga i detektovati u kontrolnom koraku, provjeravajući dovoljno veliki broj bita M. Ukoliko je broj grešaka dovoljno mali, može se zaključiti da prisluškivač neće doći ni do kakve informacije o cjelokupnom nizu bita.

6 Zaključak

Ne znamo šta je, ali znamo šta čini. Na ovaj način neki od naučnika opisuju fenomen kvantne spregnutosti. Na ovom mjestu bi bilo razumljivo teoriju kvantne spregnutosti shvatiti kao alegoriju neobjašnjive, ali jake povezanosti između ljudi, ili nekih drugih bića (ili nekih drugih bića i ljudi). Uostalom, ima li smisla pomisliti da, na određen način, nije spregnut cijeli Svemir? No, ovdje stavljam tačku na tu alegoriju, iz jasnih razloga. Nastankom ideje o spregnutosti (prepletenosti, upetljanosti), nastala je, odnosno, došla je do izražaja sumnja u razumijevanje pojma *priroda*. Nema sigurnog oslonca. I dobro je da nema. Možda su Einstein i njegovi istomišljenici samo jako željeli s vremena na vrijeme osjetiti čvrsto tlo. Kao što stoji u uvodnom dijelu, EPR argument se zauzima za lokalnost (da se nikakva informacija ne može prenositi brzinom većom od brzine svjetlosti) i realnost (da su stvari takve kakve jesu, i prije nego što ih mjerimo), sugerišući da je kvantnoj mehanici potrebno dodati neke skrivene varijable, koje bi *opravdale* neobične fenomene, poput spregnutosti, i tako učinile kvantnu mehaniku kompletnom.

Međutim, zahvaljujući Bell-ovom teoremu, odnosno, testiranju Bell-ove nejednakosti, došlo se do zaključka da je, u ovom slučaju, lokalnost narušena. Neko bi mogao postaviti pitanje, zašto se uopšte ulaže toliko u nešto, u šta većina naučnika svakako "vjeruje". Stoga je važno naglasiti da postoje takozvani *loopholes*, odnosno, propusti u teoriji, tačnije, njih tri:

1. moguće je da detektori, dok mjere spregnute čestice, često propuste neke od parova, pa se u eksperimentu vrši statistička analiza samo male frakcije čestica, što stvara vjerovatnoću da bi nedetektovane čestice mogle promijeniti cjelokupnu sliku.

2. moguće je da dvije čestice na neki način mogu *iskomunicirati* svoje stanje jedna drugoj prije detekcije.

3. moguće je da nasumičan izbor spregnutog stanja nije uopšte nasumičan, nego je na taj izbor uticao neki faktor, nerazumljiv za ljudsku svijest.

Do danas je izvedeno nekoliko eksperimenata, koji su potvrdili kvantnu spregnutost, pa je ostvarena i praktična primjena ovog fenomena (kvantna teleportacija, kvantna kriptografija,...). Neki od njih su uspjeli "ukinuti" te propuste.

Eksperiment u kojem su se koristili fotoni iz svijetlih predjela blizu galaktičkih centara, kvazara, udaljenih toliko da svjetlost od njih do Zemlje putuje 11-12 milijardi

godina, došao je jako blizu zatvaranja trećeg propusta. Pored ovog eksperimenta, neizbježno je pomenuti *The BIG Bell Test*, koji je imao za cilj zatvoriti *loophole* pitanja slobodne volje. Naime, kada se koriste određeni vidovi generatora nasumičnih stanja, postavlja se pitanje koliko je to, ustvari, nasumično. Ali, ukoliko se koriste ljudi kao *generatori*, moguće je eliminisati ovu mogućnost. Upravo to je i urađeno u BIG Bell Testu.

Pojava kvantne spregnutosti jarkim bojama naglašava mnogo pitanja, vezanih za sve što smo posmatrali kao intuitivno. Obećava da će uvijek zazvoniti, ako se na trenutak uspavamo u svojoj ideji o tome šta priroda predstavlja. Koliko je priroda *prirodna*? Šta, uopšte, znači *prirodno*?

No, zar *konačno* nije isto što i *tragično*?

Literatura

[1] Jaeger, G., *Quantum Information, An Overview*, Springer Science+Business Media, LLC (2007).

[2] Bell, J. S., *Speakable and unspeakable things in quantum mechanics*, Cambridge University Press (1987).

[3] Dür, W., Heusler, S., *What we can learn about quantum physics from a single qubit*, arXiv:1312.1463v1 [physics.ed-ph] (2013).

[4] Dür, W., Lamprecht, R., Heusler, S., *Towards a quantum internet*, Eur. J. Phys. 38 043001 (2017).

[5] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W. K., *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,* Phys Rev Lett. 70 (13):1895-1899 (1993).

[6] Boschi, D., Branca, S., De Martini, F., Hardy, L., Popescu, *S., Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels*, Phys. Rev. Lett. 80, 1121, (1998).

[7] Bouwmeester, D., Pan, J-W, Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, *A., Experimental quantum teleportation,* Nature, 390, 575–579 (1997).

[8] Pospiech, G., *Teaching the EPR paradox at high school?*, Phys. Educ. 34 311 (1999).

[9] Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K., *Quantum entanglement*, arXiv:quant-ph/0702225v2 (2007).

[10] Ma, X-S, Herbst, T., Scheidl, T., Wang, D., Kropatschek, S., Naylor, W., Wittmann, B., Mech, A., Kofler, J., Anisimova, E., Makarov, V., Jennewein, T., Ursin, R., Zeilinger, A., *Quantum teleportation over 143 km using active feed-forward,* Nature 489 269–73 (2012).

[11] Ren, J-G, Xu, P., Yong, H-L, Zhang, L., Liao, S-K, Yin, J., Liu, W-Y, Cai, W-Q, Yang, M., *Ground-to-satellite quantum teleportation,* Nature, 549, 70–73 (2017).