



Universitat Autònoma de Barcelona

Departament de Física

Grup de Física Teòrica

**Codificació d'informació en
sistemes de N espins $\frac{1}{2}$**

Antoni Brey

Setembre 2001

Índex

1 Informació en sistemes quàntics

- 1.1 Què és un sistema quàntic?
- 1.2 Què és un estat quàntic
- 1.3 Introducció
- 1.4 Superposició d'estats
- 1.5 Entrellaçat quàntic
- 1.6 Mesura quàntica
- 1.7 Entropia de Shannon
- 1.8 Entropia de Von Neumann

2 Codificació d'informació en l'espí

- 2.1 Antecedents
- 2.2 Codificació d'informació utilitzant rotacions espacials
 - 2.2.1 Espins paral·lels
 - 2.2.2 Espins entrellaçats
- 2.3 Generalització de la codificació
- 2.4 Conclusions

Referències i bibliografia

Capítol 1

Informació en sistemes quàntics

1.1 Introducció

El desenvolupament, durant els anys quaranta, de les tecnologies que feien possible el tractament automàtic de dades feu evident la necessitat de crear una teoria que donés fonament matemàtic al concepte d'informació i que permetés modelar i estudiar els processos de magatzematge i transmissió d'informació. L'any 1948 C.E.Shannon publicà l'article "A Mathematical Theory of Communication" on establí els trets bàsic d'una Teoria de la Informació, centrant el seu estudi en l'aspecte fonamental de la transmissió d'un missatge entre un emissor i un receptor. Els principals problemes estudiats per Shannon foren dos:

El primer, fins a on es possible a comprimir un missatge? És a dir, quant de redundància és la informació? Per resoldre aquesta qüestió calia establir la forma de quantificar i mesurar la redundància d'un conjunt de dades i aquest punt Shannon encertà plenament en relacionar la informació amb el concepte ja existent d'entropia.

El segon problema estudiat consistia en saber a quina velocitat podem comunicar-nos utilitzant un canal amb soroll, dit d'altra manera, quina quantitat de redundància cal introduir en un missatge per protegir-lo contra els errors. La resolució d'aquesta qüestió constituïa una extensió dels treballs de Nyquist i Harley sobre la Teoria del Senyal utilitzada en comunicacions, i era d'importància pràctica en un moment on estaven apareixent noves tècniques de modulació que calia comparar i estudiar en el cas realista de canals de transmissió amb presència de soroll.

En relacionar-se amb l'entropia, la informació es va manifestar com una magnitud mesurable dels sistemes físics, els quals, des del punt de vista

d'aplicació de la Teoria de la Informació, han estat gairebé sempre tractats com a sistemes clàssics. Però existeix una part del món que únicament pot ser descrita utilitzant les lleis de la Mecànica Quàntica, amb les seves particularitats i fenòmens específics no presents en una visió clàssica de la realitat. En un món així, cal preguntar-se com hi encaixa el concepte d'informació i de quina manera es veuen afectats els processos esmentats de magatzematge i transmissió de dades. Aquest nou camp de la física, format per la convergència de la Teoria Quàntica i la Teoria de la Informació, és el que s'ha anomenat "Informació Quàntica". Cal ser curiosos amb aquest nom perquè pot portar certa confusió: no es tracta d'una teoria quàntica de la informació, sinó d'una teoria de la informació en sistemes quàntics.

L'interès creixent per aquest nou camp ve donat per dos motius: en primer lloc, la millora tecnològica ha fet possible realitzar experiments en sistemes purament quàntics on s'ha posat de manifest l'existència d'aquells efectes que obliguen a afrontar aspectes relacionats amb els fonaments de la Teoria Quàntica, els quals durant molt de temps eren defugits ja que ens aboquen a problemes conceptuals poc estudiats. De fet, bona part del desenvolupament teòric del nou camp es podria haver realitzat fa molts anys, però la impossibilitat de realitzar experiments deixava els resultats en una posició gairebé especulativa. El segon motiu és, precisament, l'interès tecnològic dels avenços. La indústria de la microelectrònica es troba a l'actualitat voltant la frontera on els circuits es comporten com a sistemes quàntics i conèixer amb detall el funcionament i les possibilitats dels nous dispositius pot ser d'importància real per l'evolució del sector en un futur no massa llunyà.

1.2 Què és un sistema quàntic?

Un sistema quàntic és una part del món físic que pot ser conceptualment separada de la resta per ésser estudiada i modelada segons les lleis de la Teoria Quàntica. No és necessari que es tracti d'una part microscòpica de la realitat ni que estigui completament aïllada del seu entorn, ben al contrari, habitualment estarà interaccionant amb l'ambient que l'envolta.

1.3 Què és un estat quàntic?

La Mecànica Quàntica postula que tota la informació disponible d'un sistema quàntic es troba en un "artefacte" anomenat estat quàntic. Matemàticament, un estat quàntic és qualsevol operador densitat ρ en un espai de Hilbert de dimensió D . Els operadors densitat són hermitics, amb autovalors no negatius i de traça unitat. Els operadors densitat de rang unitat, és a dir, projectors del tipus

$$\rho = |\varphi\rangle\langle\varphi| \quad (1.1)$$

s'anomenen estats purs i satisfan la relació

$$\rho^2 = \rho \quad (1.2)$$

En oposició, els operadors de rang superior s'anomenen estats mixtos.

Els estats purs són aquells dels quals es disposa de la màxima informació des del punt de vista de la Mecànica Quàntica, tal i com es veurà a l'apartat 1.8.

1.4 Superposició d'estats

Una característica dels sistemes quàntics, sense equivalència en els clàssics, és l'existència d'estats superposició, és a dir, estats que poden ser expressats com a combinació lineal d'altres estats. De forma similar al bit clàssic, un estat quàntic de dos nivells representa la unitat bàsica d'informació en sistemes quàntics i se l'anomena qubit. Matemàticament es tracta d'un vector en un espai vectorial complex de dimensió dos. Els dos valors lògics del qubit seran els dos elements de la base ortonormal de l'espai vectorial,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (1.3)$$

però, a diferència del bit, el qubit també es pot trobar en qualsevol estat superposició resultant d'una combinació lineal dels elements de la base,

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (1.4)$$

on α i β són números complexos que satisfan

$$|\alpha|^2 + |\beta|^2 = 1 \quad (1.5)$$

Per tant, els valors que pot prendre un qubit són infinits, de forma ben diferent a allò que succeïa amb el bit clàssic. A primer cop d'ull pot fer la impressió que disposem d'un objecte en el qual seria possible emmagatzemar una gran quantitat d'informació. Ara bé, és important tenir en compte que no tota la informació de l'estat superposició és accessible, i el resultat no determinista del procés de mesura quàntica s'encarrega de fer-ho evident.

1.5 Entrellaçat quàntic

L'entrellaçat quàntic (*entanglement*) és l'altre fenomen que, juntament a la superposició d'estats, apareix en Informació Quàntica sense tenir anàleg en la Teoria Clàssica de la Informació. El fenomen es produeix en sistemes formats per varis subsistemes entre els quals poden existir correlacions que no admeten explicació utilitzats models locals. El sistema sencer té certes propietats que no es poden assignar als elements individuals. Si es troba en un estat pur, l'estat queda màximament descrit per una matriu densitat. En canvi, la matriu densitat de cadascun dels subsistemes no correspon a un estat pur.

La possibilitat de manipular aquestes correlacions pot obrir portes a dispositius impossibles de realitzar en sistemes clàssics. De fet, bona part de les aplicacions més atractives suggerides per diferents autors (teleportació, criptografia quàntica, algorismes quàntics [4,5,6,7]) es basen en l'existència de l'entrellaçat quàntic, tot i ser un fenomen encara no plenament entès.

1.6 Mesura quàntica

Una mesura quàntica és qualsevol procés físic dut a terme sobre un sistema quàntic i que genera una distribució de probabilitat en un conjunt de “sortides”. La Mecànica Quàntica ens facilita les eines per tractar matemàticament el procés de mesura, el qual es pot interpretar en diverses etapes tal i com es descriu tot seguit.

La Teoria afirma que un sistema quàntic envoltat d'un entorn, ambdós completament especificats, on no s'hi duen a terme mesures, evoluciona segons l'acció d'un operador unitari U ,

$$\rho \rightarrow U\rho U^\dagger \quad (1.6)$$

Una mesura de Von Newman correspon a una interpel·lació al sistema utilitzant un conjunt complet de projectors P_b ortogonals en l'espai de Hilbert del sistema quàntic. La probabilitat de cadascun dels resultats de la mesura es pot calcular com a

$$p(b) = \text{tr}(\rho P_b) \quad (1.7)$$

Per tant, si es disposa d'un sistema quàntic, ρ_s , on es vol realitzar una mesura, en primer lloc s'ha de posar en contacte el sistema a mesurar amb un altre sistema auxiliar, descrit per l'operador densitat ρ_a , preparat en un estat conegut. La unió dels dos estats quedarà descrita per l'operador densitat

$$\rho_{sa} = \rho_s \otimes \rho_a \quad (1.8)$$

Seguidament els dos sistemes evolucionen conjuntament, segons un operador unitari U , fins a quedar entrelaçats

$$\rho_{sa} \rightarrow U\rho_{sa}U^\dagger \quad (1.9)$$

Per finalitzar, es realitza la mesura sobre el sistema auxiliar que serveix d'indicador, descrita per un conjunt ortogonal de projectors, associats a cadascun dels valors de sortida b ,

$$\{I \otimes P_b\} \quad (1.10)$$

on I és l'operador identitat, i que actuen sobre l'espai de Hilbert del sistema auxiliar. La probabilitat d'obtenir una determinada sortida b serà

$$p(b) = \text{tr}(U(\rho_s \otimes \rho_a)U^\dagger(I \otimes P_b)) \quad (1.11)$$

Aquesta expressió per obtenir la probabilitat de les sortides pot ser re-escrita usant només dels operadors que operen sobre l'espai de Hilbert del sistema a mesurar. Per fer-ho utilitzem les bases ortonormals $|s_\alpha\rangle$ i $|a_c\rangle$, una del sistema a mesurar i l'altra del sistema auxiliar. La base del sistema complet serà $|s_\alpha\rangle|a_c\rangle$. Això ens permet refer l'expressió de la probabilitat de les sortides com

$$\begin{aligned} p(b) &= \sum_{\alpha} \langle s_\alpha | \langle a_c | \left((\rho_s \otimes \rho_a) U^\dagger (I \otimes P_b) U \right) | s_\alpha \rangle | a_c \rangle \\ &= \sum_{\alpha} \langle s_\alpha | \rho_s \left(\sum_c \langle a_c | \left((I \otimes \rho_a) U^\dagger (I \otimes P_b) U \right) | a_c \rangle \right) | s_\alpha \rangle \end{aligned} \quad (1.12)$$

i finalment escriure-la com

$$p(b) = \text{tr}(\rho E_b) \quad (1.13)$$

on

$$E_b = \text{tr}_a \left((I \otimes \rho_a) U (I \otimes P_b) U^\dagger \right) \quad (1.14)$$

és un operador que actua només en l'espai de Hilbert del sistema original que es volia mesurar (les traces amb subíndex indiquen traça parcial sobre el subespai indicat).

Els operadors E_b són hermítics definits positius, és a dir, amb valors propis no negatius

$$E_b \geq 0, \quad (1.15)$$

ja que han estat creats a partir de la traça parcial de dos operadors definits positius. A més, satisfan la següent relació

$$\sum_b E_b = I \quad (1.16)$$

Aquestes dues propietats constitueixen la definició de POVM (*Positive Operator-Valued Measure*). Un conjunt d'operadors que satisfan la relació anterior formen una generalització del concepte de mesura introduït per Von Neuman que es coneix com mesura generalitzada, però a diferència d'un conjunt complet i ortogonal d'operadors, els elements del POVM no comunquen entre ells. El teorema de Neumark [2] afirma que tots els POVM es poden escriure en la forma expressada a (1.14) o, dit d'altra manera, que qualsevol POVM pot ser realitzat o convertit en una mesura amb operadors ortogonals, expandint l'espai de Hilbert en un espai de dimensió superior.

Per tant, per estudiar els aspectes de la mesura que formen part d'aquest treball serà suficient treballar amb conjunts d'operadors que compleixin les condicions (1.15) i (1.16), és a dir, amb POVM's.

1.7 Entropia de Shannon

Dins la Teoria Clàssica de la Informació s'estudia la preparació de missatges a partir d'un conjunt de símbols o alfabet $X=\{x, p(x)\}$, on cadascun dels símbols "x" es dona amb una determinada probabilitat $p(x)$. La distribució de probabilitats reflecteix el desconeixement de l'observador, el "grau de sorpresa" que li produirà l'aparició d'un nou símbol en el missatge. Com més sorpresa, més informació. Per quantificar aquesta sorpresa és raonable cercar una funció que s'ajusti als següents requeriments:

- en primer lloc, donats dos successos, aquell més probable ha d'aportar menys informació que aquell altre menys probable
- en segon lloc, en el cas de produir-se dos successos independents, és a dir, la probabilitat conjunta dels quals sigui el producte de probabilitats individuals, el guany d'informació ha de ser la suma del guany d'informació aportat per cada succés
- finalment, ha de ser una funció no negativa.

L'única funció que satisfà els requeriments anteriors és el logaritme. L'entropia de Shannon del conjunt X es defineix com

$$H(X) = \sum_x -p(x) \log_2 p(x) \quad (1.17)$$

i constitueix una mesura de la quantitat d'informació que cada lletra afegida aporta al missatge. Com a exemple, si es disposa d'un alfabet de dos símbols equiprobables, cada lletra del missatge aporta 1 bit d'informació. Si l'alfabet és de 4 símbols equiprobables, cada lletra aporta 2 bits.

També és possible interpretar l'entropia de Shannon com una quantificació de la ignorància d'un observador sobre un sistema físic. Així, el guany d'informació correspon a la diferència d'entropies entre una situació final i una situació inicial de l'observador: abans d'extraure un símbol, l'entropia s'obté utilitzant l'expressió (1.17) i prové de la incertesa de l'observador a l'hora de predir el resultat, però una vegada és coneix el símbol, l'entropia és 0.

1.8 Entropia de Von Neumann

La generalització del concepte d'entropia de Shannon per sistemes quàntics implica algunes modificacions. Ara, l'alfabet de símbols està format per un conjunt d'estats quàntics ρ_x cadascun d'ells amb una probabilitat d'aparició p_x . Si un observador no disposa de cap informació addicional, la descripció completa de qualsevol mesura que vulgui realitzar es troba en la matriu densitat

$$\rho = \sum_x p_x \rho_x \quad (1.18)$$

i per un POVM concret $\{F_a\}$ obtenim les probabilitats associades a cada sortida de la mesura

$$\text{Prob}(a) = \text{tr}(F_a \rho). \quad (1.19)$$

Per una matriu densitat es defineix l'entropia de Von Neumann com

$$S(\rho) = -\text{tr}(\rho \log_2 \rho) \quad (1.20)$$

Si es treballa amb una base ortonormal en la qual ρ és diagonal

$$\rho = \sum_a \lambda_a |a\rangle\langle a| \quad (1.21)$$

llavors

$$S(\rho) = H(A) \quad (1.22)$$

on $H(A)$ és l'entropia de Shannon del conjunt de símbols $A = \{a, \lambda_a\}$. Per tant, en el cas que l'alfabet de símbols estigui format tan sols per estats purs i ortogonals que són totalment distingibles, la font de missatges quàntics es comportaria com el cas clàssic. Les diferències apareixen quan els estats que formen ρ no commuten entre ells i els símbols que formen el missatge no poden ser distingits clarament.

Si es calcula l'entropia de von Neumann d'un estat pur sempre trobarem que val zero. És la confirmació que un estat pur correspon a una situació on es disposa de tota la informació possible sobre un sistema quàntic, una situació on aquest està completament definit. Si es té la certesa que un estat és pur i conegut és evident que podem realitzar una mesura on el resultat serà totalment determinista. De fet, en aquesta situació no té gaire sentit realitzar una mesura perquè no obtindrem cap informació addicional sobre l'estat. No s'ha de confondre aquest cas amb aquell altre on sabem, per exemple, que l'estat a mesurar és pur però desconegut. Llavors la matriu densitat de l'estat a mesurar reflectirà aquest desconegut en forma d'una entropia de Von Neumann diferent de zero i, mitjançant una mesura adequada, podem incrementar el nostre coneixement sobre l'estat quàntic observat.

Capítol 2

Codificació d'informació en l'espí

2.1 Antecedents

En la etapa inicial de qualsevol processament d'informació utilitzant sistemes quàntics les dades s'han de codificar en estats. Una vegada processada o transmesa, al final del procés, la informació s'ha de recuperar, és a dir, s'ha de dur a terme algun tipus de mesura quàntica. Plantejar-se quina és la forma òptima de codificar les dades en els estats quàntics i quina és la millor manera de realitzar la mesura per recuperar-ne la informació, constitueixen doncs qüestions d'importància fonamental.

Per conèixer amb tota certesa un estat a través de mesures quàntiques caldria disposar d'un conjunt infinit de mostres idèntiques a l'hora de realitzar l'experiment. En la pràctica, però, només es podrà disposar d'un conjunt finit de mostres. Peres i Wootters [8] van proposar la interessant qüestió de si és possible obtenir més informació realitzant mesures col·lectives de les mostres en lloc d'un conjunt de mesures individuals, aprofitant així l'existència del fenomen de l'entrellaçat quàntic.

L'objectiu d'aquest treball consisteix en estudiar les qüestions esmentades per un cas concret de sistemes quàntics, aquells on es vol codificar una direcció espacial utilitzant l'espí. La resolució d'aquest tipus de problemes és d'interès per dues bandes: en primer lloc ens ajuda a aprofundir el nostre coneixement en el camp de la Teoria de la Informació Quàntica i en segon lloc poden ser d'utilitat en aspectes pràctics d'aplicació de la teoria.

La primera aproximació al problema la van fer Massar i Popescu [9] a través d'un "joc quàntic" molt senzill: uns jugadors reben un conjunt de N partícules d'espí $\frac{1}{2}$, totes polaritzades en la mateixa direcció. El jugador sap que les N partícules tenen l'espí paral·lel i que cada partida rebrà les N partícules

polaritzades en una nova direcció aleatòria i uniformement distribuïda a l'espai. El jugador pot fer qualsevol tipus de mesura i guanyarà qui millor pronostica la direcció de les N partícules. La puntuació de cada partida es quantifica amb la fórmula

$$p = \cos^2(\alpha/2) \quad (2.1)$$

on α és l'angle entre la direcció real i la direcció pronosticada. La puntuació total del joc s'obté fent la mitjana de puntuacions aconseguides en cada partida i guanya el jugador que assoleix la puntuació més elevada. Massar i Popescu demostren que la puntuació màxima teòrica és $(N+1)/(N+2)$, i s'aconsegueix amb mesures col·lectives del grup de N partícules. L'entrellaçat quàntic és el responsable d'aquest resultat, tot i ser poc evident en aquesta ocasió ja que els estats que reben els jugadors són estats producte.

Poc temps després Gisin i Popescu [10] troben un resultat ben sorprenent. És possible codificar més informació en un sistema de dos espins antiparal·lels que en un sistema de dos espins paral·lels, en contra d'allò que una falsa intuïció ens podria dur a pensar i fent notar novament la subtilitat dels aspectes fonamentals de la Mecànica Quàntica.

Es planteja llavors, de forma natural, la qüestió de quina és l'estratègia òptima de codificar la informació d'una direcció espacial en l'espai d'un sistema quàntic.

2.2 Codificació d'informació utilitzant rotacions espacials

És més entenedor plantejar el problema en uns termes diferents als de Massar i Popescu: suposem l'existència de dues persones que, d'acord amb la tradició en Informació Quàntica, anomenarem Alice i Bob i que es troben físicament separades. Alice vol comunicar a Bob una direcció espacial, és a dir, un vector unitari \vec{h} , i ho fa aplicant una operació unitària $U(\vec{h})$, una rotació, sobre un estat de referència $|A\rangle$ format per N partícules de espí $\frac{1}{2}$. L'operació unitària $U(\vec{h})$ es genera utilitzant els operadors d'espí S^{μ} i l'estat de referència $|A\rangle$ és un estat propi de S_z

$$S_z |A\rangle = m |A\rangle \quad (2.2)$$

D'aquesta manera,

$$S \cdot \hat{h} |A(\hat{h})\rangle = m |A(\hat{h})\rangle \quad (2.3)$$

on

$$|A(\hat{h})\rangle = U(\hat{h}) |A\rangle \quad (2.4)$$

Aquest estat quàntic és enviat a en Bob, el qual realitza una mesura quàntica per recuperar la informació continguda en l'estat. Suposem que en Bob realitza constantment mesures i que els estats enviats provenen d'una font isotròpica, és a dir, que el vector unitari \hat{h} de cada sistema enviat apunta en una direcció aleatòria i uniformement distribuïda sobre una esfera. El resultat de les mesures d'en Bob es concreta en la predicció d'una direcció \hat{h}_r a partir d'un POVM $\{O_r\}$. Es pretén maximitzar l'exactitud amb que Bob pot conèixer \hat{h} en funció de la preparació de l'estat quàntic enviat i la mesura realitzada.

Per quantificar el procés cal utilitzar una figura de mèrit que mesuri l'incert d'en Bob, i una bona opció per simplificar les matemàtiques del problema consisteix en valer-se de la fidelitat mitjana

$$F = \sum_r \int dn \frac{(1 + \hat{h} \cdot \hat{h}_r)}{2} P_r(\hat{h}) \quad (2.5)$$

on dn és la mesura invariant de la 2-esfera unitària i $P_r(\hat{h})$ és la probabilitat d'obtenir la sortida \hat{h}_r si la direcció enviada per Alice és \hat{h} , en el nostre cas

$$F = \sum_r \int dn \frac{(1 + \hat{h} \cdot \hat{h}_r)}{2} \langle A(\hat{h}) | O_r | A(\hat{h}) \rangle \quad (2.6)$$

Per treballar amb més comoditat és convenient convertir el sumatori de la expressió (2.6) en una integral utilitzant un POVM continu d'infinites sortides on cada projector $O(\hat{h})$ és generat a partir de rotacions d'un estat combinació d'estats propis de S_z . La condició de resolució de la identitat del POVM fixa les components d'aquesta combinació.

$$O(\vec{h}) = U(\vec{h})[|B\rangle\langle B| + |B'\rangle\langle B'| + \dots] \quad (2.7)$$

Això junt amb la invariança rotacional del problema permet d'escriure la fidelitat mitjana com

$$F = \int d\vec{n} \frac{1 + \vec{h} \cdot \vec{n}}{2} \langle A | O(\vec{n}) | A \rangle. \quad (2.8)$$

La fidelitat mitjana és una quantitat que pren valors entre 0 i 1. Si les prediccions fossin completament aleatòries valdria $\frac{1}{2}$, i qualsevol desviació per sota o per sobre de $\frac{1}{2}$ representa un guany d'informació. La fidelitat màxima, que correspondria a un encert constant per part d'en Bob de la direcció enviada per Alice, és 1. Una fidelitat 0 seria també un encert constant però sistemàticament en la direcció contrària.

Existeixen altres figures de mèrit en teoria d'estimacions [3] pensades per mesurar la distància entre distribucions de probabilitat però solen ser més incòmodes de tractar, com ara del guany d'informació

$$\Delta I = \sum_r \int d\vec{n} P_r(\vec{h}) \text{Log}_2(P_r(\vec{h})) \quad (2.9)$$

on la presència de logaritmes complica el desenvolupament matemàtic. Malgrat això, si el problema presenta suficient simetria, com és el nostre cas, també és possible obtenir resultats que ajuden a confirmar els estudis duts a terme utilitzant la fidelitat.

Un cop en aquest punt es possible optar per diferents estratègies a l'hora de triar l'estat on es codificarà la informació, en funció de l'habilitat tècnica d'Alice i Bob per manipular estats quàntics.

2.2.1 Espins paral·lels

L'opció més senzilla i evident consisteix en enviar les N partícules idènticament polaritzades

$$|A\rangle = |\uparrow\uparrow\uparrow\dots\rangle \quad (2.10)$$

és a dir

$$|A\rangle = |N/2, N/2\rangle \quad (2.11)$$

L'estat pertany a la representació d'espí més elevada de l'espai del sistema quàntic, $J=N/2$, i correspon al cas estudiat per Massar i Popescu [9], on la fidelitat mitjana màxima és

$$F_p = \frac{N+1}{N+2} \quad (2.12)$$

que s'aproxima a la unitat en funció de N com

$$F_p \approx 1 - 1/(2N) \quad (2.13)$$

2.2.2 Espins entrelaçats

Gisin i Popescu [10] van trobar que utilitzant un sistema de dos espins antiparal·lels es pot assolir una fidelitat $F=(3+3^{1/2})/6 > 3/4$ i Massar [11] demostra que aquesta és la millor fidelitat per $N=2$. Per estudiar sistemes de $N > 2$ és convenient considerar, d'acord amb Clebsch-Gordan, la descomposició de l'estat en una combinació d'estats que pertanyen a les representacions irreduïbles de l'operador S , on les representacions $S < N/2$ poden aparèixer varies vegades [13]. Es demostra que les representacions repetides no aporten cap millora a la fidelitat, per tant l'espai de Hilbert efectiu on es trobaran els estats enviats és

$$H = \frac{N}{2} \oplus \left(\frac{N}{2} - 1\right) \oplus \left(\frac{N}{2} - 2\right) \oplus \dots \quad (2.14)$$

De forma similar, es possible escriure les rotacions com

$$U(\hat{h}) = \oplus_j U^{(j)}(\hat{h}) \quad (2.15)$$

Amb aquest plantejament és possible maximitzar la fidelitat mitjana deixant lliures els coeficients dels estats on es codifica la direcció. Les expressions exactes dels estats per qualsevol valor de N es poden trobar a [12]. Es tracta

d'estats que presenten entrellaçat quàntic i únicament per $N=2$ corresponen a un estat producte, aquell format pels dos espins antiparal·lels. En el cas de N parell la fidelitat màxima ve donada per l'expressió

$$F_o = \frac{1}{2} \left(1 + \chi_{N/2+1}^{0,0} \right) \quad (2.16)$$

on $\chi_{N/2+1}^{0,0}$ correspon al major zero del polinomi de Legendre $P_{N/2+1}^{0,0}(x) = P_{N/2+1}^{0,0}(x)$, i en el cas de N imparell

$$F_o = \frac{1}{2} \left(1 + \chi_{N/2+1/2}^{0,1} \right) \quad (2.17)$$

on $\chi_{N/2+1/2}^{0,1}$ correspon al major zero del polinomi de Jacobi $P_{N/2+1/2}^{0,1}(x)$. El comportament asimptòtic de la fidelitat en funció de N és

$$F_o \approx 1 - 1/N^2 \quad (2.18)$$

2.3 Generalització de la codificació

Els mètodes presentats fins ara codifiquen la informació de la direcció \vec{h} d'una forma força clara: l'estat $|A(\vec{h})\rangle$ enviat per l'Alice s'assembla a un giroscop clàssic i l'operació unitària $U(\vec{h})$ és una rotació espacial. La codificació de la direcció es pot aconseguir orientant adequadament l'aparell que crea els estats enviats. En Bob disposarà d'un aparell de mesura que projectarà l'estat rebut sobre un POVM, el qual indicarà una sortida com a resultat de la mesura, i l'usuari podrà confiar en el resultat amb una certesa directament relacionada amb la fidelitat mitjana que s'ha calculat. És a dir, la mesura ens ajuda a disminuir la ignorància sobre el sistema en la proporció en què es redueix l'entropia.

La millora de la fidelitat hem vist que depèn de la dimensió de l'espai de Hilbert del sistema quàntic enviat i això ens porta a cercar alguna estratègia de codificació que exhaurixi els recursos de l'espai complet. El cas més senzill per estudiar aquesta possibilitat es presenta amb $N=2$, un sistema quàntic format per dues partícules d'espí $1/2$. La dimensió de l'espai de Hilbert és $d=4$, la mateixa que

tindria l'espai d'una partícula d'espí $3/2$ o bé un estat de 3 espins $1/2$ paral·lels $|A\rangle = |\uparrow\uparrow\uparrow\rangle$. L'operador S d'aquest sistema de dimensió $d=4$ es pot escriure com una operació unitaria sobre un espai suma directa d'espí 1 i espí 0, però aquests generadors no corresponen a rotacions del sistema de dos espins $1/2$. La fidelitat que s'aconsegueix en aquesta situació és $4/5$. Aquest resultat és pot generalitzar i a partir de la interpretació de l'espai de Hilbert de dimensió d com una única partícula d'espí $(d-1)/2$ s'arriba a una fidelitat òptima

$$F_G = \frac{d}{d+1} \quad (2.19)$$

En el nostre cas, l'espai de Hilbert del sistema quàntic format per N partícules de espí $1/2$ (el producte tensorial de N espais de dimensió 2) té una dimensió $d=2^N$ i la fidelitat en funció de N és

$$F_G = \frac{2^N}{2^N + 1} \quad (2.20)$$

que presenta una tendència exponencial cap a la unitat en termes del nombre de espins $1/2$ utilitzats

$$F_G \approx 1 - 2^{-N} \quad (2.21)$$

El resultat és l'autèntic òptim assolible però presenta el problema que les operacions unitàries de codificació no són rotacions espacials. Aquestes operacions s'haurien de dur a terme sobre estats entrelaçats i finalment caldria realitzar mesures no locals. Tot plegat, sembla força complicat.

2.4 Conclusions

S'han estudiat, doncs, diferents formes d'utilitzar conjunts de N partícules d'espí $\frac{1}{2}$ per enviar o emmagatzemar informació codificant-la en l'orientació de l'espí. La taula 1 recull la fidelitat mitjana màxima assolible en funció de N i de l'estratègia de codificació usada:

N	2	3	4	5	6	7
F_P	0.75	0.8	0.8333	0.8571	0.875	0.8889
F_O	0.7887	0.8449	0.8873	0.9114	0.9306	0.9492
F_G	0.8	0.8889	0.9412	0.9697	0.9846	0.9922

Taula 1: fidelitat mitjana màxima (F) utilitzant espins paral·lels (P), espins entrelaçats i rotacions espacials (O) i codificació generalitzada (G)

S'han trobat les estratègies òptimes de codificació tant pel cas en què es volen utilitzar només rotacions espacials com aquell més general on es possible realitzar qualsevol tipus d'operació unitària sobre el conjunt de N partícules.

La possibilitat d'implementar manipulacions complexes d'estats quàntics entrelaçats i sobre ells realitzar mesures no locals es troba en l'actualitat fora de l'abast de la tecnologia experimental. Bona part dels experiments més interessants que es duen a terme en aquest camp es realitzen usant fotons. Així doncs, plantejar el problema objecte d'aquest treball utilitzant fotons en lloc de partícules de espí $\frac{1}{2}$ sembla una via lògica i interessant de continuació.

Referències i bibliografia

- [1] A.Peres, *Quantum Theory: Concepts and Methods*, Kluwer, Dordrecht 1995.
- [2] J.Preskill, *Quantum Computation*,
<http://www.theory.caltech.edu/people/preskill/ph229>
- [3] C.A.Fuchs, quant-ph/9601020
- [4] C.H.Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).
- [5] A.K.Ekert, Phys. Rev. Lett. **70**, 661 (1991)
- [6] P.W.Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, S.Goldwasser (IEEE Computer Society Press, Los Alamitos, C.A.) 1994.
- [7] L.K.Grover, *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, Philadelphia, 1996
- [8] A.Peres and W.K.Wooters, Phys. Rev. Lett. **66**, 1119 (1991).
- [9] S.Massar and S.Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
- [10] N.Gisin and S.Popescu, Phys. Rev. Lett. **83**, 432 (1999).
- [11] S.Massar, Phys. Rev. **A62**, (2000) 040101(R).
- [12] E.Bagan *et al.*, quant-ph/0012045.
- [13] A.R.Edmonds, *Angular Momentum in Quantum Mechanics*, Princeton University Press, 1960