Robustesa de correlacions quàntiques febles a sistemes de tres qubits

Román Orús[†]

[†]*Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, 08028. Barcelona, Espanya.*

Agraïments

Aquest treball no hauria estat possible sense en Rolf Tarrach, a qui li agraeixo haver accedit a dirigir-me un dels meus treballs per a la obtenció del DEA i dedicar-me part del seu (molt valuós) temps. Per a mi ha estat un veritable plaer discutir amb ell sobre les “perversions” de la mecànica quàntica així com treballar junts en l'elaboració de l'article a que ha donat peu aquest treball. També li he d'agrair a en José Ignacio Latorre el seu suport com a director de la meva tesi i les seves opinions sobre el contingut del present estudi. Tanmateix agraeixo a Antonio Acín, Philipp Hyllus, Maciej Lewenstein i Anna Sanpera el donar-nos els seus punts de vista respetce als problemes que en Rolf i jo ens plantejàvem. Gràcies especialment a Juan Ignacio Cirac, per certes puntualitzacions respecte al Teorema 3 del capítol 3. No puc oblidar-me tampoc de la resta dels meus companys de doctorat, sense els quals la meva vida diària al departament seria molt més avorrida, ni de la resta dels meus amics així com de la meva família.

Prefaci

Al llarg de l'últim segle, la mecànica quàntica ha esdevingut un dels punts de més gran interès per a la comunitat de físics, degut principalment a dos motius que començaren a manifestar-se ja des del seu naixement: d'una banda, es tracta d'una teoria d'altíssim poder predictiu; d'altra banda, el fet que involucri un nou paradigma en la manera d'entendre la natura fa que aquesta sigui vista com intrínsecament "estranya". En l'actualitat, hi ha qui encara ens meravellem amb aquesta teoria revolucionària.

Passats aproximadament cent anys des de la seva primera formulació (descobriment?), ens trobem ara en l'adveniment d'una nova revolució quàntica, l'encapçalada pel camp anomenat *computació e informació quàntiques*. Els postulats fonamentals de la mecànica quàntica han passat de ser discutits a ser acceptats pràcticament sense cap dubte, protegits per innombrables corroboracions experimentals (algunes d'elles molt espectaculars, com la superconductivitat [1], la condensació de Bose-Einstein [2] o la difracció de macromolècules [3], entre d'altres). Ara el nou repte consisteix a utilitzar les regles de la mecànica quàntica per a extreure'n profit útil, com per exemple, fer ordinadors amb una capacitat operativa més enllà de tota capacitat possible amb els ordinadors actuals (computació quàntica), fer criptografia incondicionalment segura (criptografia quàntica), o "teleportar" la informació d'un sistema físic entre diferents posicions de l'espai (teleportació quàntica) [4]. No és que fins ara no hàgim fet us de la mecànica quàntica dins del marc de la nostra tecnologia (els semiconductors, els quals juguen un paper fonamental en l'electrònica moderna, en són un exemple), sinó que ara el que pretenem és aprofitar les subtileses que la mecànica quàntica ens ofereix *per principi*, com la superposició d'estats o l'embrollament quàntic[1].

Una de les aportacions més rellevants dins d'aquest camp en els darrers anys ha estat el fet d'arribar a entendre i explotar les correlacions quàntiques com si d'una magnitud fonamental és tractés (com ara l'energia), donant lloc a les aplicacions ja esmentades, entre d'altres. És un fet, doncs, que l'estudi matemàtic de les correlacions quàntiques *per se* és d'indubtable interès. Una caracterització complerta de l'embrollament present als diferents estats de la natura ens pot permetre entendre i conèixer més a fons la mecànica quàntica, i a la vegada atorgar-nos noves sorpreses en els camps de la computació i de la teoria de la informació, tant en l'àmbit clàssic com en el quàntic.

[1] *Quantum entanglement*, en la terminologia anglesa.

En el nostre estudi analitzem un cas molt particular d'embrollament quàntic: l'embrollament entre tres partícules d'espai de Hilbert bidimensional (embrollament entre tres sistemes de dos nivells, o tres *qubits*). El nostre estudi vindrà motivat per la definició actual d'embrollament i es concentrarà en una família d'estats molt particular en la que les correlacions quàntiques són *genuïnament* tripartites[2], tot i demostrant la robustesa d'aquest tipus d'embrollament contra pertorbacions externes. Veurem que aquest resultat implica la rellevància d'aquest tipus d'estat quàntic, de manera que seria plausible -almenys en principi- la preparació d'aquests sistemes a un laboratori, per lo que la seva importància aniria més enllà del merament matemàtic.

El present treball s'ha dividit en quatre capítols i un apèndix. Al primer capítol fem una introducció a alguns dels conceptes bàsics en informació quàntica dels que se'n parlarà al llarg del treball. Al segon capítol introduïm el concepte de Base Producte No-Extensible (BPNE[3]) i les seves implicacions per a la teoria de l'embrollament. En el capítol tres fem una anàlisi detallada de l'entorn al voltant de certs estats embrollats de tres partícules induïts per BPNEs. Al quart capítol recollim les nostres conclusions sobre el nostre estudi i, finalment, en l'apèndix A incloem l'article d'investigació a que ha donat lloc el present treball, i que ha estat enviat a la revista *Physical Review Letters*.

[2]El significat d'aquesta expressió serà més clar a partir del capítol 2.
[3]En la terminologia anglesa, UPB, de *Unextendible Product Basis*.

Índex

Capítol 1

Alguns conceptes bàsics

En aquest capítol fem una petita introducció als conceptes bàsics com ara la descripció d'un sistema físic mitjançant estats quàntics, l'embrollament, la destil·labilitat, l'embrollament lligat[1] i els operadors testimoni[2], els quals seran útils en posteriors capítols. Adrecem al lector interessat en aprofundir en aquests conceptes a la literatura específica en el tema [4].

1.1 Estats purs i estats mescla

En mecànica quàntica, un sistema físic aïllat es descriu mitjançant un vector normalitzat pertanyent a un espai vectorial de Hilbert $|\psi\rangle \in \mathcal{H}$. Un exemple simple però important és aquell d'un sistema físic de dos nivells, com per exemple una partícula d'espí $\frac{1}{2}$, un àtom en un pou de potencial amb dos estats accessibles -com el nitrogen de la molècula d'amoni- o un corrent superconductor que pot circular en dos sentits oposats. En aquest cas particular l'espai de Hilbert és $\mathbb{C}(2)$, i al sistema se li diu *qubit*[3]. Si el sistema té d nivells, l'espai de Hilbert és llavors $\mathbb{C}(d)$ i aquest s'anomena *qudit*.

Als estats $|\psi\rangle$ corresponents a sistemes aïllats hom els anomena *estats purs*. Així, donada una base ortonormal $\{|0\rangle, |1\rangle\}$ per a l'espai de Hilbert d'un qubit, l'estat pur més general que es pot descriure amb aquest sistema és $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$, essent a_0 i a_1 números complexes tals que $\langle\psi|\psi\rangle = |a_0|^2 + |a_1|^2 = 1$. De fet, podem precisar encara més les nostres afirmacions.

[1] *Bound entanglement*, en la terminologia anglesa.
[2] *Witness operators*, en la terminologia anglesa.
[3] Prové de la terminologia anglesa *quantum bit*.

La mecànica quàntica postula que la probabilitat d'observar un cert estat $|a\rangle$ si el sistema es troba en l'estat $|\psi\rangle$ ve donada per l'expressió $|\langle a|\psi\rangle|^2$. Degut a això, els estats $|\psi\rangle$ i $e^{i\phi}|\psi\rangle$ representen de fet al mateix sistema físic, essent $e^{i\phi}$ una certa fase global. Es diu doncs que els sistemes físics aïllats venen representats per "raigs unitaris" de l'espai de Hilbert.

L'únic problema que té la definició anterior d'estat pur $|\psi\rangle$ és que, a la pràctica, és del tot impossible aïllar completament un sistema físic del seu entorn. Podem fer un apantallament quasi perfecte de totes les interaccions amb la resta de l'univers, però tot i així sempre hi haurà un soroll degut a les correlacions residuals entre el nostre sistema i l'exterior que no podrem eliminar completament de cap manera. Els estats purs són, doncs, una idealització matemàtica -molt útil- del que passa a la realitat, i encara ens cal una representació dels estats físics reals que ens proporciona la natura. És un fet notable que aquest tipus d'estats es puguin expressar en termes dels ja presentats estats purs. A aquests estats físicament realitzables hom els anomena *matrius densitat* o *estats mescla*[4].

Mostrem la manera en que apareixen els estats mescla amb un exemple senzill e il·lustratiu: suposem un estat pur de dos qubits $|\psi^+\rangle \in \mathbb{C}(2) \otimes \mathbb{C}(2)$ donat per l'expressió $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$. Considerem que el sistema de dos qubits és tot el nostre univers, i que per tant es tracta d'un sistema aïllat. Anomenem als dos qubits A i B respectivament, e imaginem ara que només volem descriure l'estat quàntic en que es troba el qubit A. La manera matemàticament correcta de realitzar la descripció d'aquest estat és mitjançant la traça parcial del subsistema B al projector $\rho_{AB} = |\psi^+\rangle\langle\psi^+|$, al qual anomenem "matriu densitat del sistema AB". Així, obtenim el que anomenem "matriu densitat reduïda del subsistema A", $\rho_A = \mathrm{tr}_B(\rho_{AB})$, que en el nostre cas ve donada per $\rho_A = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{\mathbb{I}_A}{2}$, i que descriu l'estat quàntic del qubit A. És important notar que aquesta ρ_A no es pot escriure com $|\alpha\rangle\langle\alpha|$, éssent $|\alpha\rangle$ algun cert estat pur d'un qubit, però si que es pot escriure com una suma probabilística de projectors corresponents a estats purs d'un qubit $\rho_A = \sum_i p_i |\phi_i\rangle\langle\phi_i|$, essent $\{p_i\}$ les probabilitats i $\{|\phi_i\rangle\}$ els mencionats estats purs.

Formalitzant les idees anteriors, la mecànica quàntica diu que qualsevol sistema físic ve sempre descrit per una matriu densitat ρ la qual satisfà $\rho = \rho^\dagger$, $\rho \geq 0$ i $\mathrm{tr}(\rho) = 1$. Tots els postulats usuals es poden reformular

[4]Dins d'un àmbit més genèric, aquests estats apareixen sempre que l'observador *ignora* una part del total del sistema.

en termes d'estats mescla, i corresponen a la forma moderna de presentar la teoria [4]. En general, un estat mescla ρ sempre es pot expressar en termes d'una col·lectivitat $\{p_i, |\phi_i\rangle\}$, on p_i són probabilitats i $|\phi_i\rangle$ són estats purs, de manera que $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$. Hi ha una col·lectivitat especial, la col·lectivitat pròpia $\{\lambda_i, |\lambda_i\rangle\}$, on λ_i i $|\lambda_i\rangle$ són respectivament els autovalors i autovectors de ρ. És important destacar que els estats purs són un cas particular dels estats mescla, com era d'esperar.

Les propietats particulars dels estats purs i dels estats mescla són, en general, diferents. Genèricament hi ha molts problemes de caracterització de correlacions quàntiques que han estat resolts per a estats purs, però no per a estats mescla. El fet que aquest tipus d'estat quàntic es pugui expressar com una suma probabilística d'estats purs fa que els problemes que hom es planteja siguin encara més complexes, tot i que més atractius, donat que els estats mescla representen les situacions veritablement realistes. En el que segueix exposem alguns conceptes fonamentals, com ara l'embrollament quàntic, relacionats amb aquests sistemes.

1.2 Embrollament

Cal distingir entre l'embrollament per a estats purs i l'embrollament per a estats mescla. En el que segueix separem les dues definicions, tot i començant per la corresponent als estats purs [4]:

Definició (estat pur separable): un estat pur $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ és *separable* sí i només sí es pot escriure com

$$|\psi\rangle = |\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \cdots \otimes |\alpha_n\rangle \ , \tag{1.1}$$

on $|\alpha_j\rangle \in \mathcal{H}_j, \ j = 1, \ldots n$.

Quan un estat pur no és separable hom diu que l'estat està *embrollat*, o que hi ha embrollament entre les diferents parts del sistema. L'embrollament és una manifestació de les correlacions quàntiques entre els subsistemes, i és el responsable dels éxits més rellevants en computació e informació quàntiques. Val a dir que molts cops se sobreentén el símbol de producte tensorial $\otimes$ quan hom escriu un estat quàntic, de forma que $|a\rangle|b\rangle \equiv |a\rangle \otimes |b\rangle$. Al llarg del nostre treball alternarem entre aquestes dues notacions, quedant sempre clar el significat a partir del contexte.

Tot seguit definim el que entenem per un estat pur bipartit on l'embrollament és màxim:

Definició (estat pur bipartit màximament embrollat): donats dos subsistemes A i B d'espais de Hilbert $\mathcal{H}_A$ i $\mathcal{H}_B$, amb $\dim(\mathcal{H}_A) = d_A$ i $\dim(\mathcal{H}_B) = d_B$, un *estat pur amb embrollament màxim* entre els dos subsistemes ve donat per

$$|\psi^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i_A\rangle |i_B\rangle \ , \tag{1.2}$$

on $d \equiv \min(d_A, d_B)$, i $\{|i_\alpha\rangle\}_{i=1}^{d_\alpha}$ és una base ortonormal local per al subsistema $\alpha = A, B$.

Definim tot seguit la separabilitat per a estats mescla [5]:

Definició (estat mescla separable): un estat mescla ρ que representa a un sistema amb espai de Hilbert $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ és *separable* sí i només sí es pot escriure com

$$\rho = \sum_i p_i \rho_1^i \otimes \rho_2^i \otimes \cdots \otimes \rho_n^i \ , \tag{1.3}$$

on p_i són probabilitats i ρ_j^i són estats mescla del subsistema j $\forall i$, $j = 1, \dots n$.

Al igual que en el cas dels estats purs, si un estat mescla no és separable es diu que està embrollat o que té correlacions quàntiques. Aquesta definició de separabilitat per a estats mescla va ser proposada inicialment per Werner [5] i té una raó de ser molt clara: els estats quàntics de la forma donada en la equació (1.3) es poden crear mitjançant operacions locals en cadascun dels subsistemes $j = 1, \dots n$ i comunicació clàssica entre aquestos (OLCC[5]). Per tant, no poden existir correlacions quàntiques no locals entre els diferents subsistemes (tot i que sí clàssiques), donat que no s'han creat a partir d'operacions quàntiques conjuntes que involucrin diversos subsistemes.

Una idea complementària i diferent a la d'embrollament quàntic és la de destil·labilitat quàntica. Tot seguit presentem aquest concepte i mostrem la seva relació intrínseca amb l'embrollament.

[5]En anglés, LOCC, de *local operations and classical communication.*

1.3 Destil·labilitat

El concepte de destil·labilitat va ser introduït per Bennett *et al.* [6], i es defineix com segueix:

Definició (estat destil·lable): donades M còpies d'un estat bipartit ρ que representa als subsistemes A i B, diem que aquest és *destil·lable* sí i només sí podem obtenir N còpies d'un estat pur màximament embrollat dels dos subsistemes, mitjançant només operacions locals als subsistemes i comunicació clàssica entre ells (OLCC).

El procés de destil·lació ve representat per la Figura (1.1), i la seva extensió al cas de n subsistemes és immediata: només cal separar els n subsistemes en dos conjunts diferents, i aplicar de nou la mateixa definició. D'una manera natural es defineix l'embrollament que es pot destil·lar d'un cert estat ρ en el límit d'un nombre infinit de còpies: $E_D = N/M$ en el límit $M \to \infty$. La definició de E_D en termes d'un límit assimptòtic el fa difícil de calcular de manera explícita d'una forma genèrica. Tot i això, un resultat molt notable és que per a estats purs bipartits $|\psi_{AB}\rangle$ aquesta mesura coincideix amb l'entropia de Von Neumann de qualsevol de les dues matrius densitat reduïdes, $E_D = S(\rho_A) = S(\rho_B)$, amb $S(\sigma) = -\mathrm{tr}(\sigma \log_2(\sigma))$.

$$(\rho)^{\otimes M} \xrightarrow{\quad\text{OLCC}\quad} (|\psi^+><\psi^+|)^{\otimes N}$$

Figura 1.1: destil·lació de N estats purs màximament embrollats $|\psi^+\rangle$ a partir de M còpies de l'estat mescla ρ.

1.4 Embrollament lligat

A partir de les definicions d'embrollament i destil·labilitat donades a les seccions anteriors, és ben clar que existeix una relació entre aquests dos conceptes. Tots els estats ρ dels quals hom pot destil·lar estats màximament embrollats tenen embrollament. Aparentment, sembla que el contrari també hauria de ser cert: per qualsevol estat embrollat ρ hom hauria de poder destil·lar estats màximament embrollats.

Va ser una troballa sorprenent l'existència d'estats embrollats dels quals no es pot destil·lar cap estat màximament embrollat. La demostració d'aquest fet és deguda a Horodecki *et al.* [7], i hom els hi atribueix a aquests estats el nom d'estats amb "embrollament lligat". La raó del nom és ben simple: són estats amb un embrollament que no es pot concentrar en estats màximament embrollats ni tan sols quan hom disposa d'un nombre infinit de còpies d'aquestos. És un embrollament que no es pot extreure, i per tant és aparentment inútil a l'hora de realitzar tasques d'informació quàntica, on típicament calen estats amb embrollament màxim.

Per tal d'entendre millor com són aquests estats, introduïm el concepte de transposició parcial:

Definició (transposició parcial): donat un estat bipartit ρ representant dos subsistemes A i B d'espais de Hilbert $\mathcal{H}_A$ i $\mathcal{H}_B$ de dimensions d_A i d_B respectivament, i donada una base local per a cada subespai $\{|i_\alpha\rangle\}_{i=1}^{d_\alpha}$, $\alpha = A,\ B$, la *transposició parcial* de la matriu ρ respecte al subsistema A ve donada per

$$(\rho^{T_A})_{i_A j_A i_B j_B} = (\rho)_{j_A i_A i_B j_B}\ . \tag{1.4}$$

La transposició parcial simplement transposa respecte a un dels dos subsistemes, un cop donada una base, i és un concepte molt important en la teoria de l'embrollament degut a teoremes com el següent, que no demostrarem:

Teorema: qualsevol estat bipartit ρ representant dos subsistemes A i B tal que $\rho^{T_A} \geq 0$ (un cop definida una base local a cada subsistema) no és destil·lable.

Als estats ρ com els del teorema anterior tals que la seva matriu transposada parcial és positiva hom els anomena "estats TPP", de "transposada parcial positiva"[6]. Se segueix que qualsevol estat embrollat que sigui TPP té embrollament lligat. L'exemple original donat per Horodecki *et al.* correspón a una família d'estats en un espai de Hilbert $\mathbb{C}(3) \otimes \mathbb{C}(3)$ (dos qutrits). Utilitzant la notació estàndard per a les bases locals en aquest cas ($|1\rangle|1\rangle$, $|1\rangle|2\rangle$,

[6]En la terminologia anglesa, són els estats PPT, de *positive partial transposition*.

$|1\rangle|3\rangle$, $|2\rangle|1\rangle$, $|2\rangle|2\rangle$, etc), aquestes matrius venen donades per l'expressió

$$\rho(a) = \frac{1}{8a+1}\begin{pmatrix} a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & a & 0 & 0 & 0 & 0 & 0 \\ a & 0 & 0 & 0 & a & 0 & 0 & 0 & a \\ 0 & 0 & 0 & 0 & 0 & a & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1+a}{2} & 0 & \frac{\sqrt{1-a^2}}{2} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & a & 0 \\ a & 0 & 0 & 0 & a & 0 & \frac{\sqrt{1-a^2}}{2} & 0 & \frac{1+a}{2} \end{pmatrix}, \tag{1.5}$$

on $0 < a < 1$. Aquest és un exemple de família d'estats amb embrollament lligat, i adrecem al lector interessat a [7] per a la demostració explícita de que l'estat donat a l'equació (1.5) és embrollat i TPP.

1.5 Operadors testimoni

Introduïm en aquesta secció el concepte d'operador testimoni, de la manera en que segueix: suposem que tenim dos conjunts convexes S_1 i S_2 dins de l'espai de tots els operadors que actuen sobre un cert espai de Hilbert (espai al qual pertanyen les matrius densitat), tals que S_1 és inclòs a S_2. Recordem aquí que un conjunt S és convex sí i només sí donats dos membres del conjunt ρ, $\sigma \in S$, la combinació

$$\gamma(p) \equiv p\rho + (1-p)\sigma \tag{1.6}$$

és tal que $\gamma(p) \in S$, amb $p \in [0,1]$. Un operador hermític W és un *operador testimoni* sí i només sí verifica que:

- $\forall \sigma \in S_1,\ \mathrm{tr}(W\sigma) \geq 0$.
- Hi ha al menys un $\rho \in S_2$ tal que $\mathrm{tr}(W\rho) < 0$.
- $\mathrm{tr}(W) = 1$ (normalització).

Un cas particularment interessant és aquell en el que S_1 és el conjunt d'estats separables, S_2 és el conjunt de tots els estats quàntics i W és un observable que té valor esperat ≥ 0 per a tots els estats separables i < 0 per

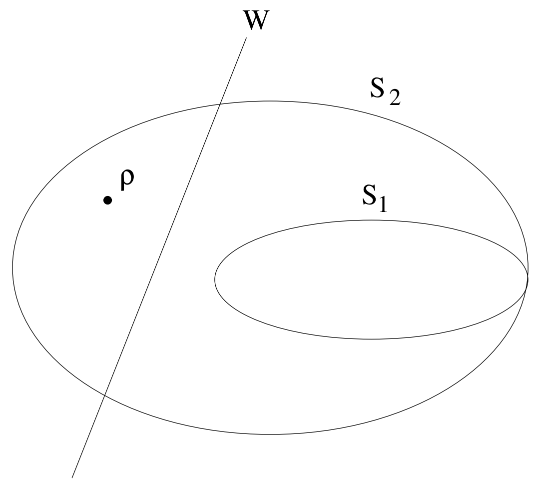

Figura 1.2: respresentació pictòrica d'un operador testimoni W distingint un estat ρ dins de S_2 i fora de S_1. Per exemple, S_1 podria ser el conjunt d'estats separables, S_2 el conjunt de tots els estats quàntics, i ρ un estat embrollat.

algun estat embrollat. Un altre exemple podria ser aquell en el que, donat un espai de Hilbert de tres qubits, S_1 és el conjunt d'estats biseparables respecte de les tres possibles biparticions del sistema i S_2 és el conjunt d'estats biseparables respecte a només dues biparticions particulars.

La importància dels operadors testimoni radica en que ens proporcionen una condició necessària i suficient per a saber si un determinat estat és embrollat o no [8, 9, 10] (l'anomenat "problema de la separabilitat"). Això queda de manifest pel teorema següent, que no demostrarem:

Teorema: un estat ρ és embrollat sí i només sí existeix un operador testimoni W que "detecta" ρ, és a dir, $\mathrm{tr}(W\rho) < 0$ i $\mathrm{tr}(W\sigma) \geq 0\ \forall\sigma$ separable.

L'anterior teorema és, de fet, molt més general, i es pot estendre a conjunts convexes en general (l'anomenat teorema d'Hahn-Banach). Pictòricament hom representa aquesta situació de la manera en que apareix a la Figura 1.2. És un fet important que aquest teorema ens dona un criteri matemàtic per a determinar si un determinat estat ρ és embrollat o no: simplement cal cercar un operador testimoni adequat que el detecti. Malauradament, aquest no és un criteri pràctic, donat que trobar l'operador testimoni que detecta un determinat estat embrollat és en general un problema *molt* difícil. Només per a casos molt particulars s'han aconseguit construir de manera sistemàtica operadors testimoni, per lo que en general, respecte al problema de la separabilitat o no d'un determinat estat quàntic, els operadors testimoni proporcionen un criteri matemàtic però complicat a la pràctica.

La teoria dels operadors testimoni dins del camp de la teoria de l'embrollament ha donat lloc a resultats molt notables, que no esmentarem en aquest treball (veure, per exemple, [8, 9, 10], i de manera més general, els treballs del grup teòric de Hannover dirigit pel professor Maciej Lewenstein). Val a dir que són una eina molt útil en l'estudi de l'embrollament, com constatarem més endavant en aquest mateix treball en fer ús d'ells per a un dels nostres resultats.

Capítol 2

Bases Producte No-Extensibles (BPNEs)

En aquest capítol introduïm el concepte de Base Producte No-Extensible (BPNE) i la seva important relació amb l'embrollament lligat. Veurem com un cas particular de BPNE ens porta cap a un estat de tres qubits perfectament biseparable, però amb embrollament lligat, el que ens conduirà cap a una discussió al voltant de l'actual definició d'embrollament, i motivarà la resta del treball que aquí s'exposa.

2.1 BPNEs i embrollament lligat

La definició matemàtica precisa de BPNE és la següent [11]:

Definició (BPNE): considerem un sistema quàntic format de m subsistemes $\mathcal{H} = \bigotimes_{i=1}^{m} \mathcal{H}_i$, on la dimensió de l'espai de Hilbert de cada subsistema es $d_i = \dim(\mathcal{H}_i)$. Una (incompleta i ortogonal) base producte (BP) és un conjunt S d'estats purs producte ortogonals entre ells, que expandeixen un subespai $\mathcal{H}_S$ de $\mathcal{H}$. Una *Base Producte No-Extensible (BPNE)* és una BP tal que el seu subsespai complementari $\mathcal{H} - \mathcal{H}_S$ no conté cap estat producte.

Un exemple de BPNE és el següent conjunt d'estats a $\mathbb{C}(3) \otimes \mathbb{C}(3)$, anomenat **Tiles** [11]:

$$\begin{aligned}
|\psi_0\rangle &= \frac{1}{\sqrt{2}}|0\rangle(|0\rangle-|1\rangle),\ |\psi_1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)|2\rangle,\\
|\psi_2\rangle &= \frac{1}{\sqrt{2}}|2\rangle(|1\rangle-|2\rangle),\ |\psi_3\rangle=\frac{1}{\sqrt{2}}(|1\rangle-|2\rangle)|0\rangle,\\
|\psi_4\rangle &= \frac{1}{3}(|0\rangle+|1\rangle+|2\rangle)(|0\rangle+|1\rangle+|2\rangle)\ .
\end{aligned} \tag{2.1}$$

La forma de veure que **Tiles** forma una BPNE és adonar-se de que qualsevol subconjunt de tres vectors restringits a un dels dos subsistemes expandeix tot l'espai tridimensional del subsistema, lo que impedeix que qualsevol altre nou vector producte sigui ortogonal a tots els existents.

Un concepte important associat a les BPNEs és el d'estat associat a una BPNE, o "estat BPNE", que tot seguit definim:

Definició (estat BPNE): donada una BPNE de m vectors $\{|\psi_i\rangle\}_{i=1}^m$ dins d'un espai de Hilbert de dimensió total D, l'estat associat a la BPNE (estat BPNE) ve donat per l'expressió

$$\rho(\mathrm{BPNE})=\frac{1}{D-m}\left(\mathbb{I}-\sum_{i=1}^{m}|\psi_i\rangle\langle\psi_i|\right)\ . \tag{2.2}$$

En poques paraules, l'estat associat a una certa BPNE és simplement la identitat del subespai ortogonal a la BPNE. Aquests estats són importants, degut al teorema que tot seguit demostrem:

Teorema: els estats associats a qualsevol BPNE són estats amb embrollament lligat.

Demostració: l'estat donat a l'equació (2.2) és la identitat en el subespai ortogonal a la BPNE. Degut a la definició de BPNE, aquest és un subespai que no conté cap estat producte, i per tant l'estat $\rho(\mathrm{BPNE})$ és un estat embrollat. Per veure que aquest embrollament és un embrollament lligat, cal provar que aquest estat no és destil·lable respecte de qualsevol possible bipartició. Per tal de demostrar aquest fet, ens adonem que, un cop escollida una bipartició del sistema, els estats $|\psi_i\rangle$ de la BPNE sempre es podem escriure com $|\psi_i\rangle=|a_i\rangle|b_i\rangle$, on $|a_i\rangle$ pertany a un dels subsistemes $\forall i$, e idènticament per $|b_i\rangle$ respecte de l'altre subsistema. La transposició parcial deixa la identitat inalterada, mentre que és fàcil veure que transforma $|a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|$ en $|a_i'\rangle\langle a_i'| \otimes |b_i\rangle\langle b_i|$, on $|a_i'\rangle \equiv (|a_i\rangle)^* \; \forall i$ (hem suposat, sense pèrdua de generalitat, que la transposició parcial es fa respecte del primer subsistema). L'estat així obtingut es pot interpretar també com una matriu densitat, i és doncs un operador ≥ 0, el que implica que $\rho(\text{BPNE})$ és un estat TPP. Com que aquest també era un estat embrollat, $\rho(\text{BPNE})$ té embrollament lligat, per qualsevol BPNE. □

El teorema anterior és important, donat que ens proporciona una manera sistemàtica de construir estats amb embrollament lligat a partir de la construcció de BPNEs. Els estats BPNE són estats embrollats, tot i que de manera molt feble, donat que hom no pot destil·lar absolutament res a partir d'ells. Són, doncs, en principi poc útils de cara a realitzar tasques pràctiques en informació quàntica. Tot seguit veurem que alguns d'aquests estats, a més a més de tenir embrollament lligat, tenen d'altres propietats que els fan particularment interessants des del punt de vista de la teoria de l'embrollament.

2.2 Estats BPNE perfectament biseparables

Considerem a continuació la següent BPNE per tres qubits ($\mathcal{H} = \mathbb{C}(2) \otimes \mathbb{C}(2) \otimes \mathbb{C}(2)$) anomenada **Shifts** [11]:

$$\textbf{Shifts} \equiv \{|0,0,0\rangle,\ |1,-,+\rangle,\ |+,1,-\rangle,\ |-,+,1\rangle\} \ , \tag{2.3}$$

on $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Podem veure que **Shifts** és una BPNE pels mateixos arguments de l'apartat anterior: qualsevol subconjunt de dos estats, quan ens restringim a un dels tres qubits, expandeix tot l'espai de Hilbert d'aquest qubit, lo que impedeix que qualsevol altre estat producte pugui ser ortogonal a tots els vectors de la BPNE.

D'acord amb lo vist a l'apartat anterior, l'estat associat a aquesta BPNE

$$\rho(\textbf{Shifts}) = \frac{1}{4}\left(\mathbb{I} - \sum_{i=1}^{4} |\psi_i\rangle\langle\psi_i|\right) \ , \tag{2.4}$$

amb $|\psi_i\rangle \in$ **Shifts**, és un estat amb embrollament lligat, ja que es TPP respecte a qualsevol bipartició del sistema. De fet, l'estat de l'equació (2.4) té una propietat encara més sorprenent: és perfectament biseparable respecte a qualsevol bipartició, tot i ser un estat embrollat. Si anomenen als qubits A, B i C, això vol dir que per a l'estat $\rho(\mathbf{Shifts})$ existeixen descomposicions probabilístiques tals que

$$\rho(\mathbf{Shifts}) = \sum_i p_i \rho_A^i \otimes \rho_{BC}^i = \sum_i p_i' \rho_B'^i \otimes \rho_{AC}'^i = \sum_i p_i'' \rho_C''^i \otimes \rho_{AB}''^i \ , \qquad (2.5)$$

però no existeix *cap* descomposició probabilística de l'estat de la forma

$$\rho(\mathbf{Shifts}) \neq \sum_i \tilde{p}_i \tilde{\rho}_A^i \otimes \tilde{\rho}_B^i \otimes \tilde{\rho}_C^i \ , \qquad (2.6)$$

donat que l'estat és embrollat. Per demostrar aquesta propietat, ens basta amb trobar les descomposicions particulars de l'equació (2.5), per a cada possible bipartició del sistema. Centrem-nos en la bipartició A *vs* BC per ara. Definim el conjunt de vectors S_A com

$$\begin{aligned} S_A \;=\; \{ & \frac{1}{\sqrt{2}}|-\rangle(|-\rangle|1\rangle + |1\rangle|0\rangle), \\ & \frac{1}{\sqrt{2}}|-\rangle(|-\rangle|1\rangle - |1\rangle|0\rangle), \\ & \frac{1}{\sqrt{2}}|1\rangle(|0\rangle|-\rangle - |+\rangle|+\rangle), \\ & \frac{1}{\sqrt{2}}|1\rangle(|0\rangle|-\rangle + |+\rangle|+\rangle)\} \ . \end{aligned} \qquad (2.7)$$

És fàcil observar que tots els vectors de S_A són biseparables respecte a la bipartició que estem considerant (A *vs* BC). També es pot comprovar que tots aquest estats són ortogonals entre ells, i també que són ortogonals a tots els estats $|\psi_i\rangle \in \mathbf{Shifts}\ \forall i$. Degut a això, la suma dels projectors associats a aquests quatre estats purs forma una resolució de la identitat dins del subespai ortogonal a **Shifts**, lo que no és res més que la definició (amb el factor de normalització corresponent) de l'estat $\rho(\mathbf{Shifts})$. Hem demostrat doncs que aquest estat es pot obtenir com una suma probabilística d'estats biseparables respecte a la bipartició A *vs* BC, i és per tant un estat mescla biseparable respecte a aquesta bipartició. El mateix argument es pot repetir per a les altres dues biparticions B *vs* AC i C *vs* AB, degut a la simetria de l'estat $\rho(\mathbf{Shifts})$. Això demostra la perfecta biseparabilitat de l'estat en

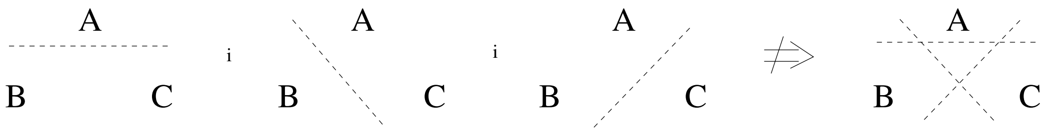

Figura 2.1: biseparabilitat perfecta no implica triseparabilitat per a estats mescla. Les línies puntejades representen que l'estat es pot crear mitjançant només OLCC entre els subsistemes que aquestes delimiten.

consideració, tot i ser embrollat. Representem la situació al dibuix de la Figura 2.1.

Aquest tipus d'estat de característiques tant especials no és únic. A [12] es demostra que, de fet, *qualsevol* estat BPNE de tres qubits és embrollat i perfectament biseparable. Més concretament, es demostra que totes les BPNEs per a tres qubits venen donades pel conjunt de vectors

$$\begin{aligned} |\psi_1\rangle &= |0\rangle|0\rangle|0\rangle \\ |\psi_2\rangle &= |1\rangle|B\rangle|C\rangle \\ |\psi_3\rangle &= |A\rangle|1\rangle|\bar{C}\rangle \\ |\psi_4\rangle &= |\bar{A}\rangle|\bar{B}\rangle|1\rangle \ , \end{aligned} \tag{2.8}$$

amb $\langle A|\bar{A}\rangle = 0$ (igualment per $|B\rangle$ i $|C\rangle$), on $|A\rangle$, $|B\rangle$ i $|C\rangle$ depenen només d'un paràmetre real cadascun, el que sempre es pot aconseguir per mitjà d'operacions unitàries locals a cada un dels subsistemes. Específicament,

$$\begin{aligned} |A\rangle\langle A| &= \frac{1}{2}\left(\mathbb{I} + \cos(\theta_A)\sigma^z + \sin(\theta_A)\sigma^x\right) \\ |B\rangle\langle B| &= \frac{1}{2}\left(\mathbb{I} + \cos(\theta_B)\sigma^z + \sin(\theta_B)\sigma^x\right) \\ |C\rangle\langle C| &= \frac{1}{2}\left(\mathbb{I} + \cos(\theta_C)\sigma^z + \sin(\theta_C)\sigma^x\right) \ , \end{aligned} \tag{2.9}$$

on $\theta_A \in (0, \pi)$ (i similarment per θ_B i θ_C). Als estats associats a aquestes BPNEs generals per a tres qubits els anomenarem $\rho(A, B, C)$ d'ara endavant. Aquestes matrius densitat tenen embrollament lligat, d'acord amb lo presentat en la secció anterior. Per tal de veure que són perfectament biseparables, el procediment és similar a com ja vàrem fer per a $\rho(\mathbf{Shifts})$. Ens centrem en una bipartició particular, A *vs* BC, i definim ara el conjunt S_A de vectors biseparables respecte a aquesta bipartició com segueix:

$$
\begin{aligned}
S_A = \; & \{|\bar{A}\rangle(c_1^*|1\rangle|0\rangle - b_1^*c_0^*|B\rangle|1\rangle), \\
& |0\rangle(b_1c_0|1\rangle|0\rangle + c_1|B\rangle|1\rangle), \\
& |1\rangle(c_1|0\rangle|\bar{C}\rangle + b_1c_0^*|\bar{B}\rangle|C\rangle), \\
& |A\rangle(c_1^*|\bar{B}\rangle|C\rangle - b_1^*c_0|0\rangle|\bar{C}\rangle)\} \;, \qquad (2.10)
\end{aligned}
$$

on $|A\rangle = a_0|0\rangle + a_1|1\rangle$, $|\bar{A}\rangle = a_1^*|0\rangle - a_0^*|1\rangle$, i similarment per a $|B\rangle$ i $|C\rangle$. És fàcil verificar que tots els vectors del conjunt S_A són ortogonals entre ells i també que són ortogonals als vectors de la BPNE definida a l'equació (2.8). Per tant, la suma dels projectors corresponents als estats de S_A és una resolució de la identitat al subespai ortogonal a la BPNE, el que no és res més que la definició de l'estat BPNE $\rho(A, B, C)$, amb el convenient factor de normalització. Això demostra la biseparabilitat de $\rho(A, B, C)$ respecte de la bipartició A *vs* BC. Per a la resta de biparticions es procedeix de manera similar, tot i aprofitant la simetria del problema en permutar els diferents subsistemes. Per tant, $\rho(A, B, C)$ és una família d'estats amb embrollament lligat i perfectament biseparable, de la qual $\rho(\mathbf{Shifts})$ n'és un cas particular.

Arribem doncs a la conclusió de que existeixen estats quàntics mescla que tenen correlacions quàntiques (doncs estan embrollats), però de tal manera que aquestes correlacions no estan amagades dins de les correlacions entre les diferents biparticions del sistema. En el cas que hem analitzat, es tracta d'un cas d'embrollament *genuí per a tres qubits*, ja que l'estat no es pot crear mitjançant OLCC entre els tres subsistemes per separat, però sí que es pot crear pel mateix procediment un cop s'han juntat dos *qualsevol* dels subsistemes. Aquest és un fet únic i exclusiu per als estats mescla: és fàcil comprovar que qualsevol estat pur de tres qubits que sigui perfectament biseparable és també triseparable. Veiem doncs que, tal i com ja havíem avançat en el capítol anterior, la teoria de l'embrollament per a estats mescla (que, recordem-ho, són els estats que ens proporciona la natura) és profundament diferent de la dels estats purs, aportant-nos situacions tant i tant estranyes com la que acabem de presentar. És precisament aquest resultat sorprenent el que ens motiva a fer una petita discussió sobre la definició actual del concepte d'embrollament, que tot seguit presentem.

2.3 És satisfactòria la definició d'embrollament?

La definició actual de separabilitat donada a l'equació (1.3) per a estats mescla va ser inicialment introduïda per Werner [5] i està basada en un criteri essencialment operacional: els estats "separables" (no embrollats) són aquells que no es poden crear mitjançant OLCC entre els diferents subsistemes, i corresponen a aquells que no es poden escriure de la forma donada en l'expressió (1.3). Aquesta definició pretén separar el que són les correlacions completament clàssiques de les quàntiques. Així, hom diu que un estat no embrollat (d'acord amb aquesta definició) és un estat correlacionat quànticament.

Ja hem vist com aquesta definició d'embrollament ha portat a l'existència de l'embrollament lligat: un tipus d'embrollament que no es pot destil·lar, o dit d'una altra manera, que probablement no serveix per a cap tasca útil d'informació quàntica (com ara la teleportació). De fet, no és cert que tots els estats amb embrollament lligat no siguin útils: alguns d'ells s'han emprat a algunes aplicacions molt particulars [13, 14, 15], però sempre dins de situacions molt concretes i característiques. En canvi, la gran majoria d'estats amb embrollament lligat que es coneixen en la actualitat no han trobat cap aplicació encara, com és el cas dels estats perfectament biseparables però embrollats $\rho(A, B, C)$ que discutíem a l'apartat anterior.

Ens veiem doncs enfrentats a una situació en la que la nostra definició d'embrollament implica una sèrie d'estats "poc útils", o el que és el mateix, tant feblement correlacionats quànticament que no semblen pràctics. Les correlacions quàntiques hi són (d'acord amb la definició estàndard), però per a tots els propòsits pràctics, és com si no hi fossin[1]

Aquesta situació ens porta a pensar que, potser, la nostra definició d'embrollament és excessivament matemàtica -tot i estar basada en un criteri operacional-, i que una definició *més física* del que és un estat correlacionat quànticament podria ser d'interès. La importància d'aquest problema, de la "inutilitat" d'alguns estats quàntics amb embrollament lligat, es centra en la possibilitat real de reproduir aquest estats al laboratori. En el nostre cas, considerem la possibilitat de realitzar físicament els estats embrollats i perfectament biseparables que centren la nostra discussió. Si en tot l'espai de Hilbert de tres qubits només hi ha un únic estat amb aquestes caracterís-

[1] De fet, els estats $\rho(A, B, C)$ tampoc violen *cap* desigualtat de Bell que involucri correladors a dos cossos [16].

tiques, aleshores aquest estat és del tot irrellevant des del punt de vista físic, ja que a la pràctica qualsevol sistema està sotmès a petites pertorbacions e imprecisions que el porten fora del seu estat ideal. En aquesta situació, l'estat no seria mai realitzable al laboratori, i per tant es tractaria d'un estat "fantasma", no observable, que no afectaria a la definició d'embrollament des del punt de vista pràctic. Així doncs, una condició necessària per a que aquest tipus d'estat sigui rellevant és que siguin robusts sota l'acció de soroll, és a dir, que les propietats fonamentals de l'estat no es vegin alterades per petites pertorbacions externes. Si, per exemple, una propietat interessant determinada només fos certa per als estats purs, mancaria aquesta de tot interès físic, ja que els estats purs són idealitzacions matemàtiques dels estats que són físicament realitzables. Les condicions experimentalment interessants han de ser considerades per als estats mescla en general.

Motivats per la possible rellevància dels estats embrollats i perfectament biseparables de cara a una possible redefinició més pràctica del que és l'embrollament, emprenem una anàlisi de les propietats de l'entorn matemàtic en l'espai de Hilbert d'aquest tipus d'estat. Aquest és l'objectiu del capítol que segueix, el qual conté els resultats principals als quals hem arribat respecte a la qüestió aquí presentada.

Capítol 3

L'entorn matemàtic dels estats $\rho(\mathrm{A}, \mathrm{B}, \mathrm{C})$

En aquest capítol analitzem com varien les propietats essencials dels estats $\rho(\mathrm{A}, \mathrm{B}, \mathrm{C})$ (embrollament, biseparabilitat i no destil·labilitat) en el seu entorn matemàtic a l'espai de Hilbert. La nostra anàlisi no queda restringida únicament a aquest tipus particular d'estats, doncs es fonamenta en assumpcions molt genèriques, obtenint així una sèrie de teoremes que són perfectament aplicables a una gran varietat de casos diferents, i dels que els estats $\rho(\mathrm{A}, \mathrm{B}, \mathrm{C})$ no són més que un cas particular. Més concretament, demostrem que els estats mescla que són embrollats però biseparables respecte d'alguna bipartició del sistema formen un conjunt de mesura no nul·la en l'espai de Hilbert, lo que implica que els estats $\rho(\mathrm{A}, \mathrm{B}, \mathrm{C})$ tenen un significat físic real. Realitzem també un estudi general de l'embrollament entorn a qualsevol estat embrollat mitjançant l'ús dels operadors testimoni, i duem a terme una anàlisi de les propietats de destil·labilitat en l'entorn dels estats quàntics associats a BPNEs.

3.1 Anàlisi de biseparabilitat i embrollament

El nostre estudi s'inicia amb el següent teorema:

Teorema 1: les matrius densitat ρ de n qubits que són separables respecte d'alguna bipartició particular del sistema formen un conjunt de mesura no nul·la en l'espai de Hilbert (és un conjunt *dens*).

Demostració: considerem una matriu densitat ρ de n qubits, la qual és separable respecte d'alguna bipartició particular. Volem introduir pertorbacions independents en l'espai de paràmetres de les matrius densitat de n qubits de tal forma que l'operador pertorbat sigui encara separable respecte d'aquella bipartició. Amb aquest propòsit, considerem el següent conjunt de $2^n \times 2^n$ projectors independents i completament separables:

$$E(j_1 \dots j_n) \equiv |j_1 \dots j_n\rangle\langle j_1 \dots j_n| \quad j_\alpha = \{0, 1, \phi_1, \phi_2\}\ , \tag{3.1}$$

per $\alpha = 1, \dots n$, $|\phi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ i $|\phi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$. Podem ara escriure qualsevol pertorbació utilitzant aquest conjunt de projectors com $\rho(\epsilon_\mu) = \frac{1}{C}\left(\rho + \sum_\mu \epsilon_\mu E(\mu)\right)$, éssent ϵ_μ un conjunt de paràmetres reals, $\mu \equiv (j_1 \dots j_n)$ i C la constant de normalització. Per a que la matriu densitat pertorbada tingui sentit físic, el conjunt de paràmetres ϵ_μ ha de ser tal que la condició $\rho(\epsilon_\mu) \geq 0$ sigui vàlida. Donat que els projectors $E(\mu)$, els quals formen una base de les matriu densitat de dimensió $2^n \times 2^n$, corresponen a estats purs separables, si ens restringim a la regió $\epsilon_\mu \geq 0\ \forall\mu$ (la qual correspon físicament a un soroll extern local), aquests estats comparteixen al menys les mateixes propietats de separabilitat que la matriu densitat sense pertorbar ρ. Queda doncs demostrat que aquests estats formen un conjunt de mesura no nul·la en l'espai de Hilbert, donat que el número de paràmetres pertorbatius independents és màxim, i la propietat de separabilitat és robusta contra el soroll local. □

El següent resultat diu que donat un estat ρ, el seu embrollament es preserva en un entorn infinitesimal. Això es demostra al nostre segon teorema:

Teorema 2: si l'estat ρ de n qubits és embrollat i ϵ_μ són infinitesimals, aleshores l'estat $\rho(\epsilon_\mu) = \frac{1}{C}\left(\rho + \sum_\mu \epsilon_\mu E(\mu)\right)$ és embrollat (en particular, l'embrollament és una propietat *robusta*).

Demostració: la demostració es fonamenta en el concepte d'operador testimoni (veure el capítol 1). Recordem a continuació la seva definició: donats dos conjunts convexes S_1 i S_2 tals que S_1 és inclòs a S_2, un operador hermític W és un operador testimoni sí i només sí (i) $\forall\sigma \in S_1$, $\mathrm{tr}(W\sigma) \geq 0$, (ii) hi ha al menys un $\rho \in S_2$ tal que $\mathrm{tr}(W\rho) < 0$ i (iii) $\mathrm{tr}(W) = 1$. En el que ens interessa, S_1 és el conjunt d'estats separables, S_2 és el conjunt del tots els estats quàntics i W és un observable que té valor esperat ≥ 0 per a tots els estats separables i < 0 per algun estat embrollat. És un fet ben conegut [8, 9, 10] que un estat ρ és embrollat sí i només sí existeix un operador testimoni W que "detecta" ρ, és a dir, $\mathrm{tr}(W\rho) < 0$ i $\mathrm{tr}(W\sigma) \geq 0$ $\forall\sigma$ separable (això és una conseqüència del teorema d'Hahn-Banach per a conjunts convexes). Donat un estat pertorbat $\rho(\epsilon_\mu)$, aquest serà embrollat sí i només sí existeix un operador testimoni W tal que $\mathrm{tr}(W\rho(\epsilon_\mu)) < 0$. Assumint que ρ és embrollat, escollim treballar amb l'operador testimoni particular W_ρ que el "detecta" (és a dir, $\mathrm{tr}(W_\rho\rho) < 0$). Per a que $\rho(\epsilon_\mu)$ sigui detectat per W_ρ imposem que

$$\mathrm{tr}(W_\rho\rho(\epsilon_\mu)) = \frac{1}{C}\left(\mathrm{tr}(W_\rho\rho) + \sum_\mu \epsilon_\mu \mathrm{tr}(W_\rho E(\mu))\right) < 0 \ . \tag{3.2}$$

Donat que $\mathrm{tr}(W_\rho\rho) < 0$ i $\mathrm{tr}(W_\rho E(\mu)) \geq 0$ (ja que $E(\mu)$ són projectors que corresponen a estats purs completament separables), la condició anterior s'escriu com $\sum_\mu \epsilon_\mu \mathrm{tr}(W_\rho E(\mu)) < |\mathrm{tr}(W_\rho\rho)|$, el que sempre es pot aconseguir per valors dels paràmetres ϵ_μ suficientment propers a zero. L'estat pertorbat és detectat per algun operador testimoni, i pertant és embrollat. $\square$

Dels dos teoremes anteriors inferim que existeix un entorn parcial de mesura no nul·la al voltant d'aquells estats de n qubits que són embrollats però separables respecte d'alguna bipartició que comparteix també les mateixes propietats que l'estat original, per lo que aquestes són propietats robustes. En particular, aquest resultat és vàlid per als estats de tres qubits estudiats a [17], i específicament per als estats amb embrollament lligat que són perfectament biseparables, com ara $\rho(\mathrm{A},\mathrm{B},\mathrm{C})$ [12] (veure capítol 2).

Recordant les BPNEs genèriques per a tres qubits (veure equació (2.8)), els nostres teoremes impliquen també que, a més a més d'aquests estats associats a BPNEs, hi ha també matrius densitat embrollades i perfectament biseparables que no es poden associar a cap BPNE de tres qubits, ja que els estats $\rho(\epsilon_\mu)$ que s'obtenen de pertorbar algun dels estats BPNE no estan en general relacionats a cap BPNE. Aquests tipus d'estats tampoc es poden escriure sempre com a una combinació convexa d'estats associats a BPNEs, ja que hom pot comprovar fàcilment que una combinació convexa de dos estats BPNE diferents per tres qubits té al menys rang 6, al temps que és possible aconseguir estats de rang 5 barrejant simplement un estat BPNE amb algun dels estats purs separables que constitueixen la BPNE.

3.2 Anàlisi de la no destil·labilitat

Volem ara analitzar les propietats de destil·labilitat de l'entorn d'aquests estats de tres qubits associats a BPNEs d'una forma més detallada. El Teorema 1 ja implica un cert tipus de robustesa (òbvia) per a la no destil·labilitat d'aquests estats, restringida a la regió $\epsilon_\mu \geq 0\ \forall \mu$. Tot seguit veurem que, de fet, aquesta robustesa és més forta degut a algunes peculiaritats dels estats BPNE, ja que es pot estendre també a alguns casos amb valors negatius petits dels paràmetres ϵ_μ. La nostra anàlisi es fonamenta només en propietats generals de les BPNEs, independentment del tipus particular de sistema, i per tant el seu rang d'aplicació no queda restringit només al cas de tres qubits.

Primer presentem un lema previ del qual farem ús per a demostrar el nostre tercer teorema:

Lema: si ρ és un estat BPNE a $\mathcal{H}_A \otimes \mathcal{H}_B$, aleshores el nucli (autoespai nul) de ρ^{T_A} té una base de vectors separables.

Demostració: sigui $\{|a_i\rangle|b_i\rangle\}_{i=1}^m$ una BPNE amb m vectors producte en l'espai de Hilbert $\mathcal{H}_A \otimes \mathcal{H}_B$ de dimensió D. L'estat BPNE és

$$\rho = \frac{1}{D-m}\left(I - \sum_{i=1}^{m} |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|\right) , \tag{3.3}$$

essent expandit el seu nucli pel conjunt de vectors de la BPNE. Fent la transposició parcial respecte del subsistema A obtenim

$$\rho^{T_A} = \frac{1}{D-m}\left(I - \sum_{i=1}^{m} (|a_i\rangle\langle a_i|)^{T_A} \otimes |b_i\rangle\langle b_i|\right) . \tag{3.4}$$

Donat que $|a_i\rangle\langle a_i|$ és un operador hermític, es verifica que $(|a_i\rangle\langle a_i|)^{T_A} = (|a_i\rangle\langle a_i|)^* = |a_i'\rangle\langle a_i'|$, essent $|a_i'\rangle = (|a_i\rangle)^*$ el vector conjugat complex del vector $|a_i\rangle$. Per tant, el nucli de ρ^{T_A} s'expandeix a partir de la base separable $\{|a_i'\rangle|b_i\rangle\}_{i=1}^m$. $\square$

En aquest punt estem en condicions de presentar el nostre tercer teorema:

Teorema 3: qualsevol estat BPNE ρ pertorbat per una quantitat suficientment petita de soroll ρ_1, tal que $\rho_1^{T_A} > 0$ en el nucli de ρ^{T_A}, es manté no destil·lable (la no destil·labilitat és una propietat condicionalment *robusta*).

Prèviament a la demostració del Teorema 3, volem recordar que qualsevol soroll físic sempre es pot representar en termes d'una barreja (amb pesos positius) en l'espai de les matrius densitat, és a dir, com a una combinació probabilística de l'operador original (no pertorbat) i l'operador induït pel soroll.

Demostració: la demostració es basa en la teoria de pertorbacions degenerada. Considerem un estat BPNE $\{|a_i\rangle|b_i\rangle\}_{i=1}^m$ a $\mathcal{H}_A \otimes \mathcal{H}_B$ i anomenem ρ el corresponent estat BPNE. Volem remarcar aquí que qualsevol estat BPNE es pot escriure sempre d'aquesta manera, ajuntant els diferents subsistemes en dos conjunts diferents A i B. Considerem també ρ_1 qualsevol altre possible estat amb suport en el mateix espai de Hilbert. Escrivim una petita pertorbació de ρ amb ρ_1 com $\rho(\epsilon) = \frac{1}{1+\epsilon}\left(\rho + \epsilon\rho_1\right)$, essent $\epsilon > 0$ un paràmetre de soroll infinitesimal. Fent la transposició parcial respecte d'un dels subsistemes obtenim $\rho(\epsilon)^{T_A} = \frac{1}{1+\epsilon}\left(\rho^{T_A} + \epsilon\rho_1^{T_A}\right)$. Els autovectors nuls de ρ es poden escollir de forma que siguin els estats de la BPNE $\{|a_i\rangle|b_i\rangle\}_{i=1}^m$, al temps que els estats del subespai de dimensió $(D-m)$ ortogonal a aquest conjunt tenen autovalor $\frac{1}{D-m}$. D'acord amb el Lema previ, el nucli de ρ^{T_A} s'expandeix per mitjà del conjunt de vectors $\{|a_i'\rangle|b_i\rangle\}_{i=1}^m$, al temps que els vectors del seu subsepai ortogonal tenen autovalor $\frac{1}{D-m}$. Utilitzant la teoria de pertorbacions per al cas degenerat, per ϵ suficientment petit els autovalors més baixos de $\rho(\epsilon)^{T_A}$ venen donats per $\epsilon\lambda_r + O(\epsilon^2)$, essent $\{\lambda_r\}_{r=1}^m$ els autovalors de la matriu Q de dimensions $m \times m$ definida per $Q_{ij} \equiv \langle a_i'|\langle b_i|\rho_1^{T_A}|b_j\rangle|a_j'\rangle$. Si $\lambda_r < 0$ per algun r, això implica autovalors negatius en l'espectre de $\rho(\epsilon)^{T_A}$, i per tant transforma $\rho(\epsilon)$ en un estat amb transposició parcial negativa. El cas en el que $\lambda_r = 0$ per algun r necessita d'un estudi en segon ordre en teoria de pertorbacions, a partir del qual es pot veure fàcilment que de nou sorgeixen autovalors negatius en l'espectre de $\rho(\epsilon)^{T_A}$, i per tant aporta conclusions similars al cas anterior. En conseqüència, per tal que l'operador pertorbat es mantingui TPP (transposició parcial positiva), hem d'exigir la condició $Q > 0$, la qual vol dir que $\rho_1^{T_A} > 0$ al nucli de ρ^{T_A}. $\square$

Desitgem ressaltar que, en termes dels projectors $E(\mu)$ del Teorema 1, qualsevol ρ_1 es pot sempre descompondre com $\rho_1 = \sum_\mu c_\mu E(\mu)$, éssent c_μ certs paràmetres reals. Definint $\epsilon_\mu \equiv \epsilon c_\mu$, observem que la hipòtesi del Teorema 3 no restringeix ϵ_μ a ser no negativa. També val la pena destacar el cas en el que la BPNE és només formada per vectors reals. En aquesta situació, el nucli de l'estat ρ^{T_A} coincideix amb el subespai espai generat pels vectors de la BPNE, i per tant la condició imposada sobre el soroll al Teorema 3 és més simple. És un fet remarcable que aquesta simplificació s'aplica a una gran varietat de BPNEs, com ara totes les BPNEs de tres qubits i moltes de dos qutrits. [11, 18, 12].

Capítol 4

Conclusions

En el capítol anterior hem demostrat tres teoremes molt generals, els quals ens donen idea de la robustesa de les propietats de separabilitat, embrollament i no destil·labilitat per a certs tipus d'estats. En particular, els teoremes demostren que aquells estats de tres qubits amb embrollament lligat però perfectament biseparables, com ara els estats $\rho(A, B, C)$, són robusts més enllà del soroll merament local, en el sentit de que el seu embrollament, la seva perfecta biseparabilitat i la seva no destil·labilitat no es veuen alterats per petites pertorbacions locals i algunes de no locals associades a soroll. En conseqüència, les característiques rellevants d'aquest tipus d'estat tenen un significat físic real, i no són només una creació matemàtica sense sentit experimental.

Arribats a aquest punt volem recordar que el nostre estudi venia motivat inicialment per la nostra definició de separabilitat quàntica. Veiem ara que aquesta definició implica l'existència d'uns estats amb correlacions quàntiques extraordinàriament febles, els quals ocupen un *volum* en l'espai de Hilbert (són de mesura no nul·la), lo que implica que no són casos aïllats ni punts "singulars" de l'espai d'estats físics. En tant que això és cert, hem de tenir doncs en compte que la forma en que definim actualment les correlacions quàntiques dóna lloc *per se* a un conjunt rellevant d'estats que són tant feblement embrollats que, a tots els efectes pràctics, sembla que no ho siguin. Aquest podria ser un motiu de cara a possibles futures revisions del concepte d'"embrollament" des d'un punt de vista potser més pràctic.

Tanmateix desitgem ressaltar que l'existència d'aquest tipus d'estats embrollats i perfectament biseparables per a tres qubits està fonamentada en el concepte de BPNE, el qual s'associa a certs espais de Hilbert de dimensió 4 que no tenen cap estat producte. Una possible generalització d'aquest concepte seria l'existència de subespais de dimensió 5 amb menys de 5 vectors producte independents, tot emmarcat dins d'un espai de Hilbert global de tres qubits. L'autor del present treball no ha tingut éxit en trobar aquest tipus de subespai, per lo que sospita de la seva no existència, tot i que tampoc ha pogut demostrar això últim -quedi, doncs, com a una conjectura-. En el cas d'existir, aquests subespais serien probablement d'interès per a la teoria de l'embrollament, de la mateixa manera en que el concepte de BPNE és important, i podrien aportar més coneixement e intuïció sobre les propietats d'embrollament, separabilitat i destil·labilitat a sistemes de tres cossos.

Bibliografia

[1] H. K. Onnes, *Commun. Phys. Lab.* **12**, 120 (1911); J. Bardeen, L.N. Cooper, J.R. Schrieffer, Phys. Rev. **108**, 1175 (1957).

[2] M. H. Anderson, J. R. Ensher, M. R. Matthews, C. E. Wieman, E. A. Cornell, *Science* **269**, 198 (1995).

[3] L. Hackermueller, S. Uttenthaler, K. Homberger, E. Reiger, B. Brezger, A. Zeilinger, M. Amdt, *Phys. Rev. Lett.* **91**, 090408 (2003).

[4] M. A. Nielsen, I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[5] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[6] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996); quant-ph/9511027.

[7] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998); quant-ph/9801069.

[8] M. Horodecki, P. Horodecki, R. Horodecki, Phys. Rev. A **223**, 1 (1996).

[9] B. M. Terhal, Phys. Lett. A **271**, 319 (2000).

[10] D. Bruß, J. I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, A. Sanpera, J. Mod. Opt. **49**, 1399 (2002); quant-ph/0110081.

[11] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, B. M. Terhal, Phys. Rev. Lett. **82**, 5385 (1999); quant-ph/9808030.

[12] S. Bravyi; quant-ph/0310172.

[13] K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim; quant-ph/0309110.

[14] T. S. Cubitt, F. Verstraete, W. Dür, J. I. Cirac, Phys. Rev. Lett. **91**, 037902 (2003); quant-ph/0302168.

[15] A. Acín, J. I. Cirac, Ll. Masanes; quant-ph/0311064.

[16] R. F. Werner, M. M. Wolf; quant-ph/0102024.

[17] W. Dür, J. I. Cirac, R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999); quant-ph/9903018.

[18] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, B. M. Terhal, Comm. Math. Phys. **238**, 379 (2003); quant-ph/9908070.

Apèndix A

quant-ph/0404100