

Algoritmes basats en teoria quàntica de la informació

Artur Garcia Saez

Director: Antonio Acín Dal Maschio

Ponent: Rossend Rey i Oriol

Prefaci

Aquest projecte presenta en primer lloc una introducció als camps de la computació i la informació quàntica. Es desenvolupen després algunes de les eines d'aquestes disciplines per formular algoritmes que permeten el càlcul eficient de propietats de sistemes físics formats per moltes partícules.

El capítol 1 exposa els fonaments de la computació i la informació quàntica, analitza alguns resultats i els compara amb resultats clàssics. La presentació d'aquests conceptes s'orienta als resultats dels capítols posteriors, on es desenvolupen els principals resultats del projecte.

El capítol 2 presenta el problema físic a solucionar: el càlcul dels valors dels nivells d'energia d'una cadena de partícules. Se n'exposen la motivació i algunes realitzacions experimentals.

Al capítol 3 veurem una primera aproximació a la solució del problema presentat al capítol 2 resolent-lo numèricament de manera exacta, sense realitzar cap aproximació. Es mostren els resultats obtinguts amb aquest sistema i les seves limitacions computacionals.

El capítol 4 mostra els resultats per al primer dels algoritmes aproximats

que es presentaran: el “*density matrix renormalization group*” (DMRG), i s’exposen els principals resultats obtinguts aplicant-lo al mateix problema físic. Es realitza també una introducció als algoritmes de renormalització.

El capítol 5 exposa una aplicació directa de les idees de la computació i la informació quàntica al mateix problema físic dels capítol anteriors. A més d’obtenir una explicació física molt clara en la nova representació matemàtica del sistema, els resultats obtinguts amb aquest mètode són clarament una millora respecte als mètodes anteriors.

L’últim capítol tracta les principals consideracions del projecte des del punt de vista de l’enginyeria, explicant els recursos emprats, la planificació i les principals conclusions.

Degut al gran contingut de conceptes físics que apareixen al llarg del projecte s’hi ha afegit un ampli apèndix sobre Mecànica Quàntica. Un segon apèndix inclou el codi de l’algorisme exposat al capítol 5.

Aquest projecte s’ha realitzar a l’Institut de Ciències Fotòniques (ICFO) sota la direcció d’Antonio Acín, i amb la ponència a la UPC de Rossend Rey. Gràcies a la seva paciència, el seu interès i la seva col·laboració aquest projecte va néixer i ha estat possible. També vull donar les gràcies a l’ICFO per proporcionar els recursos necessaris per realitzar el projecte, i per col·locar-me al despatx 116 on l’ambient de treball ha estat immillorable, i on s’ha parlat de quàntica i d’altres coses no tan quàntiques.

Índex

1	Introducció	13
1.1	Introducció	13
1.2	Computació quàntica	15
1.2.1	Introducció	15
1.3	El <i>qubit</i>	17
1.3.1	Algoritme de Deutsch-Jozsa	21
1.3.2	Algoritme de Grover	23
1.3.3	Algoritme de Shor	28
1.3.4	Complexitat	28
1.4	Teoria quàntica de la informació	29
1.4.1	Entrellaçament	30
1.4.2	El protocol BB84	31
1.4.3	Criptografia quàntica i empresa	33
2	Problema físic	35
2.1	Introducció	35
2.2	Models Físics	36
2.2.1	Model d'Ising	36
2.2.2	Model de Heisenberg	41
2.3	Aplicacions i experiments	42
3	Resultats exactes	45
3.1	Introducció	45
3.2	Diagonalització	46
3.2.1	Matrius disperses	46
3.3	El mètode de Lanczos	47
3.3.1	Implementació	48
3.4	Resultats	50

4	DMRG	55
4.1	Introducció	55
4.2	Renormalització	57
4.3	Estructura del problema	57
4.4	DMRG	61
4.5	Resultats	63
5	Algoritmes basats en teoria quàntica de la informació	67
5.1	Introducció	67
5.2	Formulació	69
5.3	Algoritme	72
5.3.1	Càlcul de N_M i H_M	77
5.3.2	Memòria dinàmica	82
5.4	Resultats	88
5.4.1	Valor d' E_0	88
5.4.2	Periodicitat	91
5.4.3	Evolució numèrica	93
5.5	Discussió	98
6	Consideracions finals sobre el projecte	99
6.1	Planificació del projecte	100
6.1.1	Diagrames de Gantt	101
6.2	Valoració econòmica	102
6.3	Ampliació bibliogràfica	105
6.4	Conclusions	106
A	Mecànica quàntica	109
A.1	Quantització	111
A.2	La doble esletxa	113
A.3	El gat de Schrödinger	116
A.4	Spin $\frac{1}{2}$	117
A.5	Notació	119
A.5.1	Mesura	120
A.5.2	Matriu densitat	120
B	Codi C de l'algoritme del capítol 5 pel model d'Ising	123
	Bibliografia	132

Índex de figures

1.1	La llei de Moore.	18
1.2	Esfera de Bloch.	20
1.3	Dues bases per enviar fotons, basades en la seva polarització.	32
1.4	Alice i Bob acorden els bits de la clau privada.	32
1.5	<i>Clavis</i> , el sistema de idQuantique basat en BB84 per distribuir claus privades.	33
2.1	Esquema del model físic de N partícules a estudiar amb condicions de contorn obertes (a) i condicions de contorn periòdiques (b).	37
2.2	Esquema de la trampa lineal d'ions de la universitat de Innsbruck.	43
2.3	Àtoms atrapats en el potencial d'una trampa òptica. Les seves interaccions es poden modelitzar amb el model de Heisenberg.	44
3.1	Valors de E_0 per a condicions de contorn obertes.	51
3.2	Valors de E_0 per a condicions de contorn periòdiques.	52
3.3	Temps d'execució en segons pel cas de condicions de contorn obertes. El comportament és clarament exponencial.	53
3.4	Temps d'execució en segons pel cas de condicions periòdiques.	54
4.1	Pas de renormalització de l'algoritme clàssic (a) i de DMRG (b). El blocs indicats (A' i A'') són el punt de partida del següent pas de renormalització.	62
4.2	Error del càlcul de E_0 respecte als resultats exactes ($E_0 = -\ln(2) + \frac{1}{4}$), en funció del tamany de la descripció aproximada.	64

5.1	Nova formulació del problema fent servir teoria quàntica de la informació. Cada posició s'ha substituït per 2 sistemes (a_k i b_k) de dimensió D . El conjunt de matrius A transformen la nova representació en el model físic.	69
5.2	Relació entre el tamany real dels paràmetres necessaris per descriure el sistema i el tamany de la descripció aproximada (determinada pel valor del paràmetre D), en funció del tamany de la cadena N	72
5.3	El problema original definit amb condicions periòdiques (a). Els estats dels extrems de la nova representació (b) estan connectats. La cadena es transforma en un anell (c).	73
5.4	Després d'actualitzar les matrius A de la posició k (a), passem a la posició $k + 1$ circulant en sentit horari (b). Si circulem en sentit antihorari passem a la posició $k - 1$	74
5.5	Precisió obtinguda per a una cadena de longitud $N = 8$ partícules. Amb valors del paràmetre D moderats s'aconsegueix ja una bona aproximació al valor de E_0	88
5.6	Precisió obtinguda per a una cadena de longitud $N = 12$ partícules.	89
5.7	Precisió obtinguda per a una cadena de longitud $N = 28$ partícules.	90
5.8	Valor de $\langle S_i, S_{i+1} \rangle$ al llarg de tota la cadena, per $N = 14$ i $D = 10$. L'estabilitat d'aquest valor indica la invariància translacional de la solució obtinguda.	91
5.9	Valor de $\langle S_i, S_{i+1} \rangle$ al llarg de tota la cadena, per $N = 14$ i $D = 14$	92
5.10	Evolució del valor de E_0 per a una cadena $N = 10$. La ràpida convergència de les primeres iteracions s'estabilitza a mesura que el valor s'apropa al resultat exacte.	93
5.11	Evolució del valor de E_0 per a una cadena $N = 12$	94
5.12	Evolució del valor de E_0 per a una cadena $N = 16$	95
5.13	Evolució per a $N = 16$. L'aproximació inicial millora a l'augmentar el paràmetre D . La velocitat de convergència es mostra però independent d'aquest valor D	96
5.14	Evolució per a $N = 16$. Els salts indicats senyalen un canvi en la precisió parcial en els diferents estadis d'evolució de l'algoritme.	97

ÍNDEX DE FIGURES

6.1	Diagrames de Gantt de la planificació inicial(a) i final (b) de les diferents tasques del projecte.	108
A.1	Espectre de radiació del cos negre.	112
A.2	Resultat de l'experiment realitzat amb bales	114
A.3	Resultat de l'experiment realitzat amb ones	115
A.4	L'experiment de Stern-Gerlach.	118
A.5	122

Índex de taules

1.1	Operació XOR. Considerant com a sortida només el valor $x \oplus y$ l'operació és irreversible. Afegint el valor de x a la sortida l'operació esdevé reversible.	22
1.2	Càlcul de $q_{\text{random}}(4,0)$ per $N = 4$	26
3.1	Representació dispersa d'una matriu.	47
4.1	Esquema de l'algoritme de renormalització	60
4.2	Esquema de l'algoritme DMRG pel cas infinit	63
5.1	Esquema de l'algoritme de renormalització per a condicions de contorn periòdiques	76

Capítol 1

Introducció

*“Science is what we understand well enough to explain to a computer.
Art is everything else we do.”*

Donald E. Knuth

1.1 Introducció

Al llarg de l'evolució dels computadors i de la teoria de la computació alguns conceptes bàsics han restat intocables. Tot i la modernització dels components, l'augment en capacitat i en velocitat i la creixent complexitat de les arquitectures, els elements fonamentals de computació són els mateixos ara que fa 50 anys. El *bit* segueix sent la unitat fonamental d'informació. També és remarcable que els coneixements que sobre Física (i especialment sobre la branca de la física coneguda com a Mecànica Quàntica) tenien alguns del

pioners de la Teoria de la Computació no es veiessin reflectits fins als anys 80: p.ex. John Von Neumann va ser una de les principals figures en la formulació matemàtica d'aquesta teoria.

Des del punt de vista teòric, la formulació als anys 30 del concepte de màquina de Turing (en resposta a un problema proposat per Hilbert a principis de segle) resta també intocable. Si bé s'han proposat algunes variants (com ara la màquina de Turing indeterminista, amb una component d'aleatorietat), aquestes segueixen bàsicament l'esquema original, i la seva capacitat computacional és similar.

Als últims anys s'ha produït una revisió de tots els conceptes fonamentals del procés de computació i comunicació, basats en la teoria de la Mecànica Quàntica. Aquesta teoria, nascuda també al tombant de segle, sorgeix per explicar les propietats de la matèria i la radiació a escales atòmiques. Tot i que els moderns processadors en fan ús (per descriure el comportament dels semiconductors que els formen) el comportament quàntic no es manifesta en el procés computacional. El *procés* de càlcul és el mateix independentment de si es realitza amb una calculadora de vàlvules de buit o amb un processador modern.

Per altra banda, la successiva miniaturització a que estan sotmesos els components d'un computador pot acabar trobant un límit físic. Si els components fonamentals arriben a l'escala atòmica, el seu comportament es veurà descrit per la Mecànica Quàntica, donant lloc a "estranyos" fenòmens que poden distorsionar els resultats dels càlculs. En principi doncs aquests fenòmens

1.2. COMPUTACIÓ QUÀNTICA

quàntics haurien de ser d'alguna manera controlats per poder mantenir la robustesa computacional dels dispositius actuals.

La disciplina de la Computació Quàntica neix quan aquestes suposades dificultats de la limitació quàntica dels actuals dispositius comencen a ser considerades com un avantatge. Els treballs de Feynman [Fey, Fey82], Deutsch, Ekert . . . reformulen els conceptes de *bit* i de màquina de Turing, demostrant a més que el computador quàntic pot realitzar les mateixes tasques que una computadora clàssica, i també realitzar càlculs impensables per a aquest últim. Veurem un exemple amb els resultats dels algoritmes de Grover i Shor.

A un procés similar de revisió s'ha sotmès la Teoria de la Informació. La Criptografia i la Comunicació s'han vist reformulades gràcies a la possibilitat de transmetre informació fent servir les propietats d'alguns estats quàntics. La realització experimental d'algunes d'aquestes teories és ja una realitat, demostrant tant la seva utilitat com la seva viabilitat. Avui ja és possible comprar un sistema de criptografia quàntica.

1.2 Computació quàntica

1.2.1 Introducció

Suposem que tenim un sistema capaç d'assolir N estats diferents. Fent servir un conjunt de bits volem emmagatzemar informació sobre aquest estat. Amb un únic bit només podem distingir entre 2 estats, amb 2 bits entre 4 estats, . . .

En general per poder representat els N estats necessitem $\log_2 N$ bits. Des del punt de vista físic aquest bit pot ser representat p.ex. per un valor del voltatge, la posició d'un interruptor, o qualsevol magnitud física que pugui assolir 2 valors clarament distingibles.

En aquest punt hem d'establir una distinció que a partir d'ara serà crucial. Els elements habituals amb els que la teoria de la computació ha treballat des dels seus orígens als anys 30 i 40 seran classificats com a *clàssics*, en contraposició als corresponents termes revisats per la teoria quàntica. Així parlarem del bit clàssic (representació d'un 0 o un 1) i del bit quàntic o *qubit*.

Fent servir el bit clàssic com l'element d'informació fonamental, podem construir una màquina de càlcul amb un conjunt d'operacions que es realitzen sobre una configuració inicial de bits, que emmagatzemen un valor corresponent al valor d'entrada. El procés de càlcul el podem representar, fent servir el formalisme de Turing, com el conjunt d'operacions que una màquina realitza sobre les dades: li estan permeses les accions d'escriure i llegir símbols en una cinta, de desplaçar-ne el capçal de lectura, i de situar-se a cada pas en un estat determinat. En el moment de finalitzar les seves operacions, el resultat del procés computacional es troba escrit en la cinta.

En cap cas es va plantejar, en el disseny de la màquina de Turing, quins serien els processos físics que suportarien tot el càlcul: com es construiria la màquina. De fet, el propi Turing havia donat una resposta mecanicista a un problema matemàtic plantejat per Hilbert a principis de segle (conegut com *Entscheidungsproblem*, o problema de la decibilitat). La construcció de les

computadores modernes s'ha fonamentat en aquests principis, i les diferents realitzacions físiques sempre han emulat aquest comportament.

1.3 El qubit

Suposem per començar una extensió del nostre concepte clàssic de bit, suggerida per la teoria quàntica. Fins ara un del principis bàsics del bit clàssic es la seva exclusivitat: només podia estar en l'estat 0 o en l'estat 1. Suposem ara que, seguint l'evolució tecnològica de les últimes dècades, intentem imaginar com pot ser una unitat d'emmagatzemament d'aquí a uns anys. Cada cop els components són més petits, els àtoms necessaris per representar un bit en són cada cop menys ... l'exemple més conegut d'aquesta evolució és la coneguda llei de Moore [Moo65].

Seguint així podem acabar representant un bit mitjançant l'estat d'un sol àtom? Com veurem, a més de ser possible (amb algunes condicions), la possibilitat de realitzar-ho obre un nou ventall de possibilitats computacionals inassequibles als bits clàssics.

Si hem d'explicar el comportament d'un únic àtom hem de recórrer a la Mecànica Quàntica. Tot i que a l'apèndix A d'aquesta memòria s'inclou un resum, introduïrem aquí els principals elements que ens calen. Si considerem el conjunt d'estats en que es pot trobar un sistema (els identificarem amb la notació $|n\rangle$, on n pren tants valors com estats li estan permesos al sistema), fent servir les lleis clàssiques de la Física el nostre sistema només es pot trobar

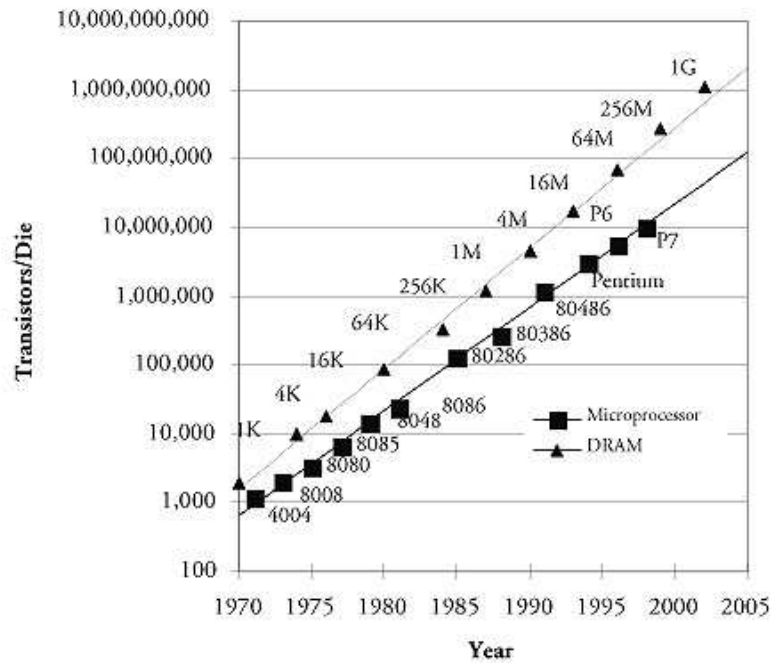


Figura 1.1: La llei de Moore.

en un d'aquest estats: $|1\rangle$ o $|2\rangle \dots$ o $|n\rangle$. A escales atòmiques el comportament no pot ser descrit d'aquesta manera. La física a escales petites permet també estats compostats per la *superposició* del estats base del sistema (els diferents $|n\rangle$) de la manera

$$|\psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \dots + \alpha_n|n\rangle. \quad (1.1)$$

1.3. EL QUBIT

Els coeficients α_n són nombres complexos, que verifiquen la relació

$$\sum_{i=1}^n |\alpha_i|^2 = 1. \quad (1.2)$$

Per completar la imatge quàntica només ens cal, de moment, introduir el concepte de mesura. Tot i que la teoria quàntica permet als sistemes físics trobar-se en una superposició d'estats, en el moment de realitzar una mesura d'una magnitud aquesta superposició *col·lapsa* en un únic estat. A l'apèndix A s'indica la motivació d'aquesta explicació, i les principals conseqüències que implica. Ara només ens interessa saber que després de la mesura podem trobar el nostre sistema en un únic estat $|i\rangle$, amb probabilitat $|\alpha_i|^2$.

Així podem definir un bit quàntic, o *qubit*, com la superposició dels 2 estats $|0\rangle$ i $|1\rangle$

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle. \quad (1.3)$$

Degut a la relació 1.2 entre els coeficients α_0 i α_1 , podem rescriure l'estat $|\psi\rangle$ com

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\varphi} |1\rangle, \quad (1.4)$$

que permet una representació gràfica del *qubit* coneguda com esfera de Bloch, segons la qual podem imaginar el qubit com un vector unitari en l'espai de tres dimensions.

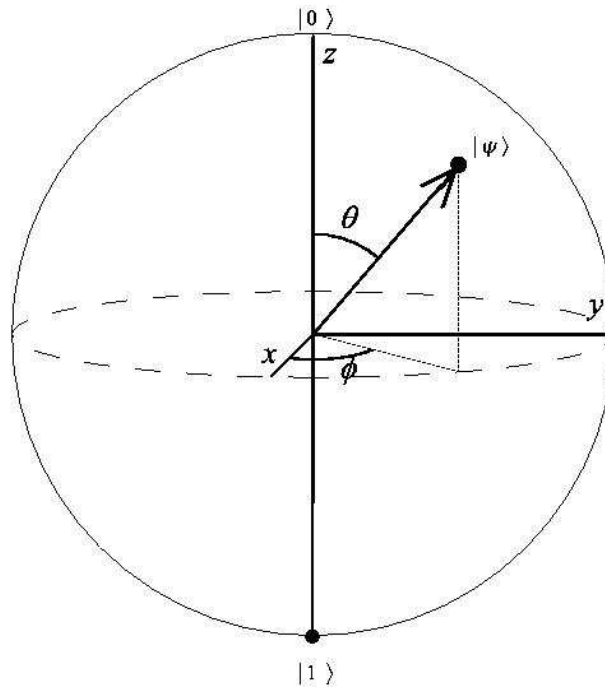


Figura 1.2: Esfera de Bloch.

Aquest element fonamental, el *qubit*, serà la peça bàsica de les computacions quàntiques. L'esquema d'una computació quàntica el podem assimilar fàcilment a l'anàleg clàssic: s'inicia amb la preparació de l'estat d'entrada (ara hem vist que aquest pot ser una superposició d'estats), un procés d'evolució al llarg del temps, i una mesura final (subjecte al principi de col·lapse que hem vist abans) que proporciona el resultat.

Ens trobem, però, amb la dificultat de treballar en un entorn on desapareix la comoditat del determinisme clàssic, ja que les probabilitats associades al procés de mesura en principi semblen un obstacle a qualsevol procés fiable de càlcul. A continuació veurem com el que en principi semblava un

límit físic a l'evolució tecnològica ofereix noves possibilitats computacionals: la paral·lelització quàntica permet l'execució d'un algoritme sobre una superposició d'estats inicials, tot i que el procés de mesura que finalitza el càlcul proporciona una única solució. La relació entre l'entrada (superposició) i la sortida (un únic valor) és la part més crítica en el disseny d'un algoritme quàntic.

En aquest context hem de considerar també la relació entre reversibilitat i dissipació d'energia durant un procés de càlcul. Aquesta relació és coneguda per la termodinàmica [Lan61]. Les equacions que determinen l'evolució quàntica d'un sistema són reversibles en el temps, per tant tot sistema de càlcul basat en aquestes lleis ha de ser reversible (les portes lògiques tradicionals no ho són; no podem determinar l'entrada únicament coneixent la sortida). Una idea suggerida per Paul Benioff l'any 1982 [Ben82] indicava la possibilitat de codificar la configuració de la màquina en un sistema quàntic que no dissipava energia.

1.3.1 Algoritme de Deutsch-Jozsa

Presentarem aquí un exemple senzill de com la superposició d'estats al llarg de la computació pot oferir grans avantatges.

Suposem una funció $f(x)$ amb $x \in \{0, 1\}$ i amb $f(x) \in \{0, 1\}$. Volem determinar si $f(0) = f(1)$ o bé $f(0) \neq f(1)$. Clàssicament hem d'avaluar per una banda $f(0)$ i per una altra $f(1)$ i comparar-ne els resultats, per tant la funció $f(x)$ ha d'ésser avaluada 2 vegades.

Suposem que operem ara amb una entrada que permet la superposició d'estats. Seguint a Deutsch i Jozsa, i triant adequadament l'entrada, veurem com el resultat es pot obtenir amb una *única* avaluació de $f(x)$. Comencem recordant el comportament de l'operació XOR (taula 1.1). Podem veure com

x	y	x	$x \oplus y$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Taula 1.1: Operació XOR. Considerant com a sortida només el valor $x \oplus y$ l'operació és irreversible. Afegint el valor de x a la sortida l'operació esdevé reversible.

el bit x actua de control del resultat: $x = 1$ equival a invertir el valor del bit y com a resultat. Quan $x = 0$ el resultat és igual al valor del bit y a l'entrada.

Escollim com a entrada un estat com

$$|00\rangle + |10\rangle - |01\rangle - |11\rangle,$$

on $|x, y\rangle$ o $|xy\rangle$ representa els estats dels dos paràmetres. Construïm una porta tal que $|x\rangle|x\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ per avaluar la funció f . Podem veure que la redundància del valor x a la sortida permet la reversibilitat de l'operació. Operant amb l'entrada que hem preparat, i tenint present que les lleis de la Mecànica Quàntica són lineals (per tant les nostres operacions també ho

seran), tenim com a sortida

$$|0f(0)\rangle + |1f(1)\rangle - |0f'(0)\rangle - |1f'(1)\rangle,$$

on f correspon a la funció sobre x sense modificar (ja que $y = 0$), i f' correspon a $1 - f$. Pel cas en que es compleix $f(0) = f(1)$ tenim que aquesta sortida es pot factoritzar com

$$(|0\rangle + |1\rangle)(|f(0)\rangle - |f'(0)\rangle),$$

mentre que pel cas $f(0) \neq f(1)$ tenim

$$(|0\rangle - |1\rangle)(|f(0)\rangle - |f'(0)\rangle)$$

Els estats corresponents a x ($|0\rangle + |1\rangle$, $|0\rangle - |1\rangle$) són ortogonals: en realitzar una mesura sobre el bit x només podem obtenir un d'aquests valors. Podem fer doncs una mesura del primer bit i determinar amb una única avaluació de la funció f (sobre una superposició d'estats d'entrada) la solució del problema.

1.3.2 Algoritme de Grover

Suposem que volem realitzar una cerca en una base de dades (BD) definida per una clau. Si les claus que fem servir per indexar la cerca estan ordenades el cost d'aquesta cerca es logarítmic respecte el nombre d'instàncies (N) que

conté la BD. Suposem l'operació inversa: tenim uns valors de la base de dades i volem saber quina és la clau que els indexa (p.ex. tenim un número de telèfon i volem saber a qui pertany, fent consultes a una guia de telèfons). En el cas millor, cerquem un element de la BD i coincideix amb l'element que estem cercant. En aquest cas tenim que l'operació té un cost constant, independent del tamany de la BD. En el cas pitjor anem triant elements de la BD (de tamany N), però no trobem el registre que ens interessa fins a haver recorregut tota la BD. En aquest cas el cost és N . En promig podem suposar que trobarem l'element desitjat després de realitzar $\frac{N}{2}$ consultes. Podem representar l'algoritme així:

```
inrandom();
int f();
main()
{
    int i, r, answer = -1 ;
    r = random(N);
    for(i = 0; i < N; i++)
    {
        si (f(r) == 1) answer = r ;
        r = random(N) ;
    }
    print(answer);
}
```

Anem a veure com de nou el paral·lelisme quàntic pot millorar l'algoritme clàssic fent servir un estat superposició com a entrada. El següent algoritme fou proposat per Grover l'any 1996 [Gro96], arribant al límit teòric demostrat abans [BBBV96]. La versió en codi és molt similar a la seva variant clàssica:


```
int qrandom();
int f();
quantum_main()
{
    int i, r;
    r = qrandom(N, 0);
    for(i = 0; i < eta; i++)
    {
        si (f(r) == 1) invert_phase();
        r = qrandom(N, r);
        si (r == 0) invert_phase();
        r = qrandom(N, r);
    }
    print(r);
}
```

Les funcions *qrandom()* i *invert_phase()* són inherentment quàntiques. *qrandom()* genera un nombre aleatori que és la superposició dels nombres entre 0 i $(N - 1)$ amb alguns canvis de signe. La funció *invert_phase()* deixa invariant el valor de les amplituds, però n'inverteix la fase de l'element cercat. Amb un exemple veurem com funciona tot plegat:

Suposem un tamany de BD $N = 4$: Analíticament es calcula el valor de *eta*, que varia entre $0.5\sqrt{N}$ i $0.8\sqrt{N}$, i tenim $eta = 1$. Així, en el cas clàssic teníem (en cas pitjor) 4 iteracions. En el cas quàntic en tenim només 1. La funció $q = qrandom(N, r)$ funciona així: suposem la representació binària dels nombres q i r . Si el nombre de 1 en la mateixa posició en les dues representacions és parell, s'associa un signe +, i - si és imparell. Així per al valor $q = 01$ i $r = 01$ tenim un nombre senar de 1 en la mateixa posició (en tenim només 1), i el signe associat és negatiu (veure taula 1.2).

	0	1	2	3
0	0.5	0.5	0.5	0.5
1	0.5	-0.5	0.5	-0.5
2	0.5	0.5	-0.5	-0.5
3	0.5	-0.5	-0.5	0.5

Taula 1.2: Càlcul de $qrandom(4,0)$ per $N = 4$.

- Primer es genera $qrandom(4,0)$. Es crea un estat superposició de tots els valors de r amb probabilitat $\frac{1}{2}$,

$$\frac{1}{2} \cdot (|0\rangle + |1\rangle + |2\rangle + |3\rangle).$$

- Si suposem que el valor que cerquem és el tercer, aplicar la inversió de fase retorna

$$\frac{1}{2} \cdot (|0\rangle + |1\rangle - |2\rangle + |3\rangle).$$

- Ara el valor de r per a les 4 components és calculat a partir de la suma de les probabilitats d'assolir un estat r després d'aplicar l'operació $qrandom(4,r)$. P.ex. pel cas de $r = 0$ hem de sumar les probabilitat d'assolir l'estat $r = 0$ a partir dels estats (superposició) $r = 0, 1, 2, 3$. Del càlcul obtenim el valor $\frac{1}{2}$, resultat de la suma dels coeficients de la columna 0 de la taula 1.2 multiplicats per les respectives amplituts de cada component al pas anterior. Similarment s'opera amb els altres

1.3. EL QUBIT

valors de r i obtenim

$$\frac{1}{2} \cdot (|0\rangle - |1\rangle + |2\rangle + |3\rangle).$$

- Ara treballem només amb l'estat 0, invertint la seva fase per obtenir l'estat

$$\frac{1}{2} \cdot (-|0\rangle - |1\rangle + |2\rangle + |3\rangle).$$

- Operant com abans s'aplica l'operació $qrandom(4,r)$ a partir dels 4 valors de r per a cada probabilitat. Obtenim

$$0|0\rangle + 0|1\rangle - |2\rangle + 0|3\rangle.$$

Després d'aquest últim pas realitzem una mesura al registre. Com la probabilitat és igual al quadrat del coeficient obtenim la resposta $r = 3$, com volíem.

Tot i la millora en eficiència de l'algoritme, passant d'un cost respecte els elements de la base de dades a cercar $O(N)$ a un cost $O(\sqrt{N})$, ens estem mantenint en la mateixa classe de complexitat que en el cas clàssic. La versió quàntica que acabem de trobar, tot i ser més ràpida en un factor quadràtic, pertany doncs a la mateixa classe de complexitat.

1.3.3 Algoritme de Shor

Els moderns sistemes de criptografia com el RSA es basen en la dificultat actual de factoritzar un nombre enter. Per desxifrar una clau d'aquest sistema cal trobar els factors primers d'un nombre molt gran, tasca que amb el millor algoritme conegut actualment (l'algoritme de Lenstra) té un cost $O\left(\exp\left[(\log N)^{\frac{1}{3}}(\log \log N)^{\frac{2}{3}}\right]\right)$.

L'any 1995 P. Shor [Sho97] presenta el que és potser el resultat més important de la computació quàntica: un algoritme capaç de factoritzar un nombre en $O((\log N)^2(\log \log N)(\log \log \log N))$, això és, en temps polinòmic respecte al nombre de dígit ($O(\log N)$) de N . Així, si l'algoritme clàssic es demostrés que pertany a la classe de complexitat NP aleshores la solució del computador quàntic suposaria un canvi de classe de complexitat, i una millora exponencial respecte la versió clàssica. La seguretat dels sistemes actuals d'enciptació estaria doncs compromesa. Veurem més endavant com la Informació Quàntica permet la distribució segura d'una clau privada.

1.3.4 Complexitat

De manera clàssica les classes de complexitat es classifiquen de la següent manera [Pap94]:

- La classe P es defineix com la classe de problemes decidibles en temps polinòmic respecte el tamany de l'entrada.
- Similarment, la classe EXP defineix la classe de problemes decidibles

1.4. TEORIA QUÀNTICA DE LA INFORMACIÓ

en temps exponencial.

- La classe NP es defineix com la classe de problemes que permeten verificar en temps polinòmic si una solució satisfà la condició del problema. També es defineix com la classe de problemes que són resolts per una màquina de Turing indeterminista en temps polinòmic [Kar72].

Aquestes classes de complexitat verifiquen la relació $P \subsetneq EXP$ i $P \subseteq NP \subseteq EXP$. No se sap si la classe NP coincideix amb la classe P o amb la classe EXP , o amb cap de les dues.

Amb els resultats dels apartats anteriors podem afegir, a partir de les operacions realitzables amb un computador quàntic, la classe de complexitat QP que defineix els problemes decidibles en temps polinòmic per un computador quàntic. Com hem vist en els exemples anteriors es dedueix que $P \subset QP$ (el computador quàntic pot solucionar actualment més problemes en temps polinòmic que el computador clàssic).

1.4 Teoria quàntica de la informació

Estenent les idees dels apartats anteriors, també podem sotmetre a revisió els conceptes clàssics de transmissió d'informació. La disciplina de la Teoria de la Informació s'ha encarregat de l'estudi de tots els fenòmens associats al procés de codificació i transmissió d'informació a través d'un canal. A partir d'aquí podem establir algunes condicions de seguretat en la transmissió, parlant de criptografia. Hem vist abans com l'aparició del computador quàntic,

gràcies a l'algoritme de factorització, comprometia els esquemes clàssics de criptografia. L'aparició de la teoria de la informació quàntica utilitza un conjunt de nous fenòmens, alguns d'ells sense la corresponent analogia clàssica, que permeten nous esquemes de transmissió i de codificació, així com noves solucions a problemes clàssics.

La teoria clàssica de la informació (de la mateixa manera que la majoria de teories físiques clàssiques) es recolza en fenòmens que els nostres sentits i la nostra experiència diària verifiquen contínuament. Si tenim un sistema d' n estats (clàssics) i volem transmetre el seu estat a algú a través d'un canal de comunicació, el màxim nombre de missatges que podem compondre per transmetre l'estat complet és n .

1.4.1 Entrellaçament

Parlarem en aquest capítol de l'*entrellaçament*, que serà la pedra angular de l'algoritme del capítol 4, i que constitueix el principal tema d'estudi d'aquest projecte.

Seguint l'argument de mesura que hem vist abans, suposem que tenim l'estat conjunt de dos sistemes especificat com

$$|\psi\rangle = \alpha_0|0, 0\rangle + \alpha_1|1, 1\rangle,$$

i realitzem una mesura en una de les meitats del sistema. En realitzar la mesura podem obtenir l'estat $|0\rangle$ o $|1\rangle$. Sigui quin sigui el resultat, una de

1.4. TEORIA QUÀNTICA DE LA INFORMACIÓ

les dues components que definien el sistema global desapareix, de manera que l'estat de l'altre meitat del sistema queda definit després de la mesura que hem fet. Aquest col·lapse conjunt es pot produir en sistemes separats una gran distància, i es realitza de manera immediata després de la mesura en el primer sistema. No obstant això, en tot el procés no es produeix cap transmissió d'informació entre les dues meitats del sistema, de manera que els principis de la teoria de la relativitat que impedeixen comunicacions més ràpides que la velocitat de la llum no es veuen contradits.

En aquest resultat es basa la famosa crítica d'Einstein, Podolsky i Rosen [EPR35] a la teoria quàntica. L'aparició però d'un fenomen inherentment quàntic ens permet cercar mètodes que millorin els resultats clàssics o, en el pitjor dels casos, en siguin equivalents.

1.4.2 El protocol BB84

Presentat per Bennett i Bassard l'any 1984 [BB84], aquest protocol permet una manera segura de distribuir una clau privada entre un emissor **A** (Alice) i un receptor **B** (Bob). El procés de comunicació es basa en la polarització dels fotons enviats entre els dos participants.

Per tot el procés de comunicació són necessaris dos canals: un quàntic, pel qual s'enviaran els fotons, i un canal clàssic. Alice tria de manera aleatòria per a cada fotó que envia a Bob una base de polarització (figura 1.3) i un valor 0 o 1 per a enviar. A l'altra banda, Bob tria també de manera aleatòria una base per mesurar el valor 0 o 1 dels fotons que li arriben d'Alice. Finalitzada



Figura 1.3: Dues bases per enviar fotons, basades en la seva polarització.

la transmissió quàntica Bob comunica a Alice pel canal clàssic (p.ex. una línia telefònica) i li indica la base triada per a mesurar cada fotó. En els casos en que la seva base coincideix amb la utilitzada per Alice tots dos guarden el valor enviat/mesurat (figura 1.4). El conjunt d'aquests valors guardats formen la clau privada.

• Alice	x + x + + x x +
	0 0 1 0 1 1 1 0
• Bob	+ x x + + + x x
	0 1 1 0 1 1 1 0
• Clau	1 0 1 1

Figura 1.4: Alice i Bob acorden els bits de la clau privada.

A diferència del cas clàssic, Alice i Bob poden detectar la presència d'un espia en la transmissió. Per determinar la clau, aquest espia ha de mesurar també els fotons enviats i per tant triar també una base de polarització. En la meitat dels casos triarà la base equivocada (com li passava a Bob) i com a resultat de les seves mesures (que col·lapsen la funció d'ona del fotó) l'estat dels fotons que arriben a Bob, encara que aquest triï la base correcta (la

1.4. TEORIA QUÀNTICA DE LA INFORMACIÓ

mateixa triada per Alice) no correspondrà a l'enviat per Alice. Així, encara que Alice i Bob hagin enviat i mesurat un fotó determinat en la mateixa base els seus resultats no coincidirán. Per verificar la presència de l'espia només han de comparar alguna seqüència de la clau transmesa per comprovar la seva correcció, garantint així la privacitat de la clau.

1.4.3 Criptografia quàntica i empresa

Actualment ja existeixen empreses que comercialitzen sistemes de criptografia quàntica. L'empresa suïssa **idQuantique** (<http://www.idquantique.com>) i als Estats Units **MagiQtechnologies** (<http://www.magiqtech.com>) produeixen sistemes de criptografia basats en el protocol BB84. És el millor exemple de l'aplicació a la vida quotidiana dels resultats teòrics que fins ara hem vist.



Figura 1.5: *Clavis*, el sistema de **idQuantique** basat en BB84 per distribuir claus privades.

Capítol 2

Problema físic

“The most direct, and in a sense the most important, problem which our conscious knowledge of Nature should enable us to solve is the anticipation of future events.”

Heinrich Hertz

2.1 Introducció

Presentarem a continuació el model físic que estudiarem al llarg del projecte. Es tracta d'un model general, amb algunes variants, que permet simular sistemes unidimensionals de partícules.

La varietat de fenomenologia que presenta fa que es tracti d'un model àmpliament estudiat, i molt adequat per a l'estudi de propietats físiques com la superconductivitat. Tot i semblar un model relativament senzill, la

dificultat de trobar solucions analítiques ha forçat la utilització de tècniques d'aproximació per obtenir resultats.

Les recents propostes experimentals del computador quàntic inclouen sistemes amb trampes d'ions. La interacció dels elements d'aquests dispositius és pot modelitzar també amb aquesta família de models, permetent així un millor coneixement dels processos que s'hi produeixen.

2.2 Models Físics

Tenim una cadena de N posicions, on a cada posició hi posem una partícula. Definint el tipus de partícula que situem a cada posició, el tipus d'interaccions que es produeixen entre aquestes partícules i l'abast d'aquesta interacció tenim definit el problema físic que volem estudiar.

A continuació es presenten les dues variants que s'estudien en aquest projecte: el model d'Ising i el model de Heisenberg. Aquests models són generalitzables a d'altres amb presència de camps magnètics, assimetries en les interaccions entre partícules, interaccions a veïns més llunyans o amb la introducció d'impureses en el sistema.

2.2.1 Model d'Ising

En aquest model les partícules que formen el sistema només interactuen amb els seus veïns més propers. Així, si tenim una cadena com la de la figura 2.1, cada partícula interactua únicament amb les partícules situades imme-

2.2. MODELS FÍSICS

diatament a la seva dreta i a la seva esquerra. Pel cas de la figura 2.1(a) existeixen 2 partícules (situades als extrems de la cadena) que només interactuen amb una altra partícula. Pel cas de la figura 2.1(b) totes les partícules tenen 2 veïns. La diferència entre les dues disposicions serà important quan comencem a fer servir descripcions del problema més sofisticades, com veurem en els següents capítols. Suposarem a cada posició una partícula quàntica de

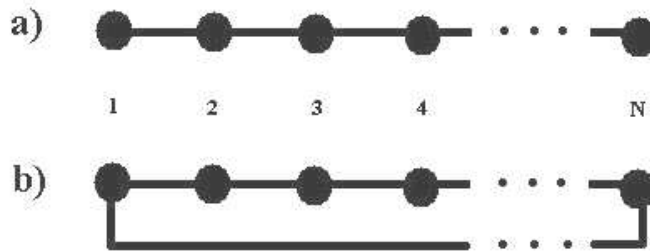


Figura 2.1: Esquema del model físic de N partícules a estudiar amb condicions de contorn obertes (a) i condicions de contorn periòdiques (b).

2 estats (o partícula de $spin = \frac{1}{2}$), com els *qubits* que hem descrit anteriorment.

Per definir les interaccions hem d'establir únicament la matriu d'energia H del sistema. Amb aquesta matriu, que ara veurem com construir, podem trobar els valors d'energia permesos segons la Mecànica Quàntica

(veure l'Apèndix A) resolent l'equació

$$H \cdot x = \lambda \cdot x, \quad (2.1)$$

on λ són els *autovalors* (*eigenvalues*) de la matriu i x són els *autovectors* (*eigenvectors*). Els valors λ corresponen als valors d'energia que pot assolir el sistema. En aquest projecte ens centrarem en l'obtenció d'uns pocs d'aquests valors, els corresponents als nivells d'energia més petits. Seran per tant les solucions de l'equació 2.1 amb els valors de λ més petits.

Per determinar la matriu H del sistema hem de definir el tipus d'interaccions entre les partícules. Ja hem vist que tractarem només amb sistemes on les interaccions es produeixen entre veïns més propers. El tipus d'interaccions venen definides per la fórmula en el model d'Ising venen definides per la fórmula

$$H^{Ising} = \sum_{n=1}^{N-1} \mathbb{I}_2^{[1]} \dots \sigma_z^{[n]} \otimes \sigma_z^{[n+1]} \dots \mathbb{I}_2^{[N]}, \quad (2.2)$$

on N és el tamany de la cadena de partícules, i

$$\sigma_z = \frac{1}{2} \times \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

2.2. MODELS FÍSICS

$$\sigma_z \otimes \sigma_z = \frac{1}{4} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Així, de l'operació \otimes (producte tensorial) de dues matrius de tamany $m \times m$ en resulta una matriu de tamany $m^2 \times m^2$. Podem veure aleshores que a mesura que considerem instàncies de problemes més grans (augmentem el nombre de partícules del nostre sistema) hem de treballar amb matrius que creixen exponencialment, ja que hem de considerar interaccions entre més partícules. Aquesta és una de les principals dificultats a l'hora de treballar amb aquest tipus de problemes, i que ens forçarà a cercar altres formes de solucionar-los.

A tall d'exemple veurem com construir la matriu H per a una cadena de 3 partícules amb condicions de contorn obertes. Segons la fórmula 2.2

$$H_3^{Ising} = \sigma_z^{[1]} \otimes \sigma_z^{[2]} \otimes \mathbb{I}_2^{[3]} + \mathbb{I}_2^{[1]} \otimes \sigma_z^{[2]} \otimes \sigma_z^{[3]}, \quad (2.3)$$

i per a condicions periòdiques

$$H_3^{Ising} = \sigma_z^{[1]} \otimes \sigma_z^{[2]} \otimes \mathbb{I}_2^{[3]} + \mathbb{I}_2^{[1]} \otimes \sigma_z^{[2]} \otimes \sigma_z^{[3]} + \sigma_z^{[1]} \otimes \mathbb{I}_2^{[2]} \otimes \sigma_z^{[3]}, \quad (2.4)$$

on \mathbb{I}_2 és la matriu identitat de tamany 2×2 .

La matriu d'energia H per a condicions obertes és

$$H_3^{Ising} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -\frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{pmatrix} \quad (2.5)$$

Com veiem aquest model té la propietat que les seves interaccions sempre es poden definir com una matriu diagonal. L'absència d'elements fora de la diagonal mostra el caràcter clàssic d'aquest model.

Així, aquesta matriu pot ser emmagatzemada com un vector (passem de tenir un cost $O(m^2)$ a tenir-lo de només $O(m)$, tant en espai com en la diagonalització), i a més els seus autovalors més petits es poden determinar ordenant el vector format amb els elements de la diagonal. El procés de diagonalització és aquí innecessari, però com veurem a continuació -amb el model de Heisenberg- aquesta propietat no és habitual, i no es presenta en el principal model que volem estudiar, el model de Heisenberg.

2.2.2 Model de Heisenberg

Hem considerat un tipus d'interacció molt específica en l'apartat anterior, aquella limitada únicament a l'eix z . És immediat estendre'l als eixos x i y , donant lloc al model de Heisenberg que podem escriure

$$H^{Heisenberg} = \sum_{n=1}^{N-1} \mathbb{I}_2^{[1]} \dots \vec{\sigma}^{[n]} \otimes \vec{\sigma}^{[n+1]} \dots \mathbb{I}_2^{[M]}, \quad (2.6)$$

on $\vec{\sigma} = \{\mathbb{I}, \sigma_x, \sigma_y, \sigma_z\}$, i

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}.$$

És habitual utilitzar la parametrització

$$\sigma_+ = \frac{1}{2}(\sigma_x + i\sigma_y) \quad (2.7)$$

$$\sigma_- = \frac{1}{2}(\sigma_x - i\sigma_y) \quad (2.8)$$

$$\sigma_+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \sigma_- = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Tornant a l'exemple d'una cadena de 3 partícules. Construïm H per a aquest tipus d'interacció amb condicions de contorn obertes

$$\begin{aligned}
 H_3^{Heisenberg} &= \sigma_z^{[1]} \otimes \sigma_z^{[2]} \otimes \mathbb{I}_2^{[3]} + \mathbb{I}_2^{[1]} \otimes \sigma_z^{[2]} \otimes \sigma_z^{[3]} + \\
 &\quad \sigma_+^{[1]} \otimes \sigma_-^{[2]} \otimes \mathbb{I}_2^{[3]} + \mathbb{I}_2^{[1]} \otimes \sigma_+^{[2]} \otimes \sigma_-^{[3]} + \\
 &\quad \sigma_-^{[1]} \otimes \sigma_+^{[2]} \otimes \mathbb{I}_2^{[3]} + \mathbb{I}_2^{[1]} \otimes \sigma_-^{[2]} \otimes \sigma_+^{[3]}
 \end{aligned} \tag{2.9}$$

La matriu corresponent resulta

$$H_3^{Heisenberg} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -\frac{1}{2} & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -\frac{1}{2} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{pmatrix} \tag{2.10}$$

2.3 Aplicacions i experiments

L'estudi d'un sistema físic d'aquestes característiques bé motivat per la gran quantitat de fenomenologia que ofereix. Es tracta d'un sistema proposat inicialment l'any 1925 per Lenz per al seu estudiant, Ising. Més tard l'ampliació de Heisenberg l'any 1928 li va permetre, juntament amb Dirac, formular una teoria del magnetisme basada en propietats quàntiques. Des de aleshores el

2.3. APLICACIONES I EXPERIMENTS

model s'ha ampliat a variants en presència de camps magnètics, a problemes de dues dimensions, a temperatura finita ... Fenòmens com la superconductivitat a temperatures finites poden estudiar-se amb models similars. La dificultat de trobar solucions analítiques ha motivat al llarg dels anys diferents mètodes d'aproximació.

Recentment, la proposta de J.I.Cirac i P.Zoller [CZ95] de construir un computador quàntic amb sistemes d'ions exigeix un estudi detallat del comportament entre els components d'aquests sistemes.

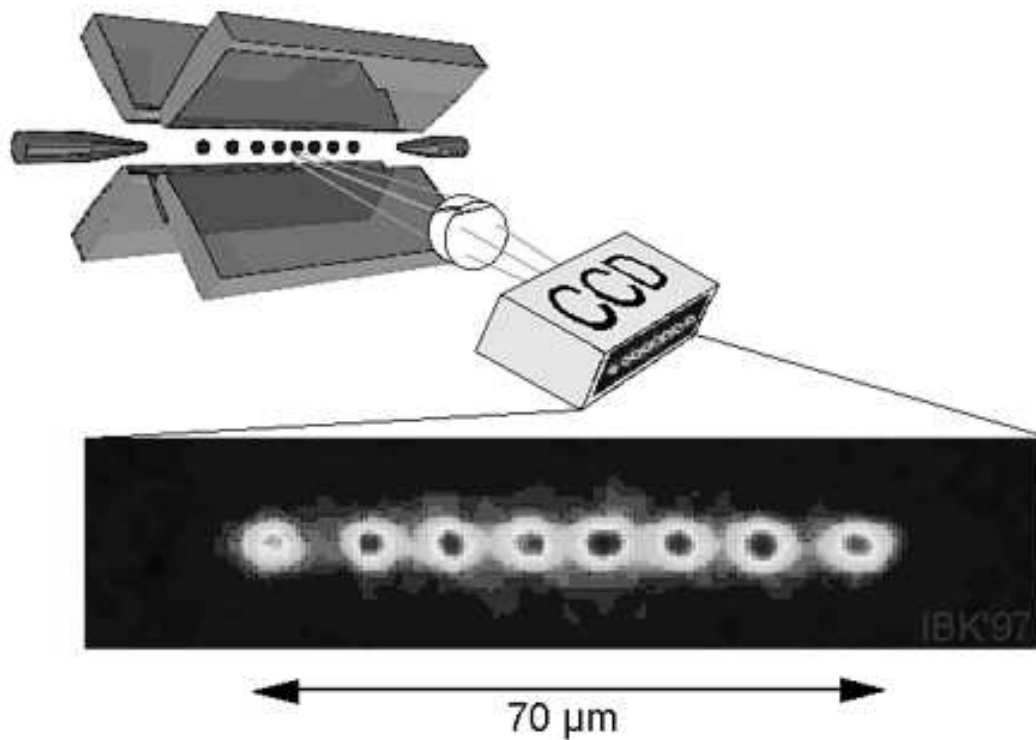


Figura 2.2: Esquema de la trampa lineal d'ions de la universitat de Innsbruck.

Les interaccions efectives entre les partícules a cada posició és pot simular amb el model original d'Ising o Heisenberg. La realització experimental d'algunes portes lògiques seguint aquest esquema indica [SKHR⁺03] la viabilitat de construir un computador quàntic segons la proposta de Cirac i Zoller. Altres realitzacions experimentals proposades com la resonància nuclear magnètica o les trampes òptiques també són candidates com a dispositius possibles.

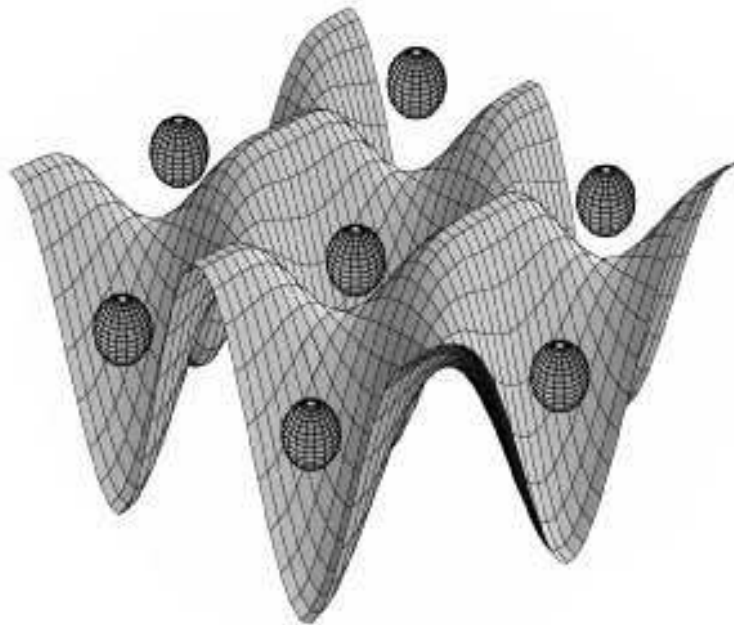


Figura 2.3: Àtoms atrapats en el potencial d'una trampa òptica. Les seves interaccions es poden modelitzar amb el model de Heisenberg.

Capítol 3

Resultats exactes

“No, no, you’re not thinking; you’re just being logical.”

Niels Bohr

3.1 Introducció

Davant un problema físic com el que ens proposem estudiar podem, amb l’ajuda de l’àlgebra lineal, determinar una solució numèrica exacta. No es tracta d’una solució analítica, que al llarg de tot el projecte trobarem rarament. Les equacions que es plantegen poden ser resoltes amb diferents mètodes numèrics, que triarem segons el grau de precisió que vulguem pels resultats.

La complexitat del problema fa que tot i que inicialment l’obtenció de resultats exactes sigui factible, al augmentar el tamany del sistema aquest esdevingui intractable. Més endavant farem servir els resultats exactes

d'aquest capítol per verificar la correcció dels mètodes aproximats que es desenvolupen als següents capítols.

3.2 Diagonalització

Tenim una matriu H de la que en volem obtenir alguns dels autovalors més petits, els autovectors no cal calcular-los. A més, degut a les característiques de les interaccions que estem considerant, aquesta matriu està formada per pocs valors que siguin $\neq 0$. Veurem ara com treure profit d'aquesta propietat.

3.2.1 Matrius disperses

En matrius formades majoritàriament per elements $= 0$ podem triar representacions que permetin una millora en l'eficiència (tant en temps com en espai d'emmagatzemament) de les operacions on intervinguin. Veurem amb un exemple com disminuir l'espai necessari per guardar una d'aquestes matrius *disperses*.

Suposem una matriu com [PRL96]

$$\begin{pmatrix} 1 & 2 & 0 & 0 & 3 \\ 4 & 5 & 6 & 0 & 0 \\ 0 & 7 & 8 & 0 & 9 \\ 0 & 0 & 0 & 10 & 0 \\ 11 & 0 & 0 & 0 & 12 \end{pmatrix},$$

3.3. EL MÈTODE DE LANCZOS

considerant només les posicions $\neq 0$ podem guardar aquesta informació com a la taula 3.1. Aquesta nova disposició converteix el cost d'emmagatzema-

valor	1	2	3	4	5	6	7	8	9	10	11	12
fila	0	0	0	1	1	1	2	2	2	3	4	4
columna	0	1	4	0	1	2	1	2	4	3	0	4

Taula 3.1: Representació dispersa d'una matriu.

ment en proporcional al nombre d'elements $\neq 0$ que tenim, millorant el cost quadràtic de la representació completa. A més, el producte matriu-matriu o matriu-vector és ara també proporcional al número d'elements $\neq 0$. En algorismes que fan ús d'aquestes operacions (com el de Lanczos que veurem a continuació) aquesta representació suposa una gran millora.

3.3 El mètode de Lanczos

Suposem una matriu $A \in \mathbb{R}^{n \times n}$, de tamany gran, dispersa i simètrica. Amb el mètode de Lanczos, proposat l'any 1950, podem trobar de manera eficient un subconjunt dels seus autovalors. El mètode genera una seqüència de matrius tridiagonals T_k (matrius que només tenen elements diferents de zero a la diagonal principal, i a les situades immediatament per sobre i per sota d'aquesta). Amb aquestes matrius podem trobar els autovalors de A fent servir:

- Els autovalors extrems (més grans i més petits) de les matrius T_k s'aproximen molt als autovalors extrems de A .

- Trobar els autovalors d'una matriu tridiagonal és un procés computacionalment menys costós que diagonalitzar una matriu completa.

Així el mètode es divideix en dues parts: una primera de construcció de la matriu tridiagonal i una segona de diagonalització d'aquesta matriu.

3.3.1 Implementació

Per la conversió de la matriu A en una matriu tridiagonal hem de trobar la transformació que ho fa possible. Volem trobar una matriu S tal que la matriu A esdevingui tridiagonal a l'aplicar la transformació

$$T = S^{-1}AS.$$

Per fer-ho es calcula una successió de vectors x_1, x_2, \dots, x_n (vectors columna de S) biortogonals a una altra successió y_1, y_2, \dots, y_n ($y_j^T \cdot x_i = 0$, si $i \neq j$), on aquestes successions venen definides recursivament

$$\begin{aligned} x_{k+1} &= Ax_k - b_k x_k - c_{k-1} x_{k-1}, \\ y_{k+1} &= A^T y_k - b_k y_k - c_{k-1} y_{k-1}, \end{aligned}$$

amb $x_0 = y_0$, x_1 i y_1 arbitraris, $c_0 = 0$ i

$$\begin{aligned} b_k &= \frac{y_k^T Ax_k}{y_k^T x_k}, \\ c_{k-1} &= \frac{y_{k-1}^T Ax_k}{y_{k-1}^T x_{k-1}} = \frac{y_k^T x_k}{y_{k-1}^T x_{k-1}}. \end{aligned}$$

3.3. EL MÈTODE DE LANCZOS

Amb aquestes definicions tenim

$$\begin{aligned}Ax_1 &= x_2 + b_1x_1 \\Ax_k &= x_{k+1} + b_kx_k + c_{k-1}x_{k-1} \\Ax_n &= b_n + c_{n-1}x_{n-1},\end{aligned}$$

i per tant

$$AS = S \begin{pmatrix} b_1 & c_1 & & & 0 \\ 1 & b_2 & c_2 & & \\ & \ddots & \ddots & \ddots & \\ & & & 1 & b_{n-1} & c_{n-1} \\ 0 & & & & 1 & b_n \end{pmatrix} = ST.$$

Si volem aconseguir que la matriu T sigui simètrica (això facilitarà encara més el procés de diagonalització) podem fer servir la relació

$$Ax_k = c_kx_{k+1} + b_kx_k + c_{k-1}x_{k-1}.$$

Aquesta transformació la podem obtenir amb el següent procés iteratiu [GvL96, Par80]:

```

 $r_o = x_1; c_0 = 1; x_0 = 0; k = 0;$ 
while ( $c_k = 0$ )
     $x_{k+1} = \frac{r_k}{c_k}; k = k + 1; b_k = x_k^T A x_k;$ 
     $r_k = (A - b_k \mathbb{I})x_k - c_{k-1}x_{k-1}; c_k = \|r_k\|^2$ 
end

```

A partir d'aquesta matriu tridiagonal podem trobar els autovalors que cerquem amb qualsevol dels mètodes existents, com el de la bisectriu o per partició [GvL96]. A més, existeixen versions paral·lelitzables d'aquests mètodes.

3.4 Resultats

Un cop decidit el mètode de diagonalització podem veure el cost associat executant l'algoritme per a instàncies de tamanys diferents. Disposem dels resultats exactes [MC91] a la bibliografia, però només amb una precisió de 10^{-5} . Els càlculs aquí realitzats s'han efectuat amb una precisió de 10^{-13} , necaessària per utilitzar-los després com a referència dels mètodes aproximats, que poden arribar a aquest nivell d'exactitud.

S'han executat els algorismes en 2 entorns diferents. En un s'ha emprat una implementació ineficient basada en la llibreria LAPACK (un conjunt de rutines escrites en FORTRAN i optimitzades progressivament al llarg dels anys). Es tracta d'una llibreria que pot ser utilitzada des de una plataforma com Matlab, en codi escrit en FORTRAN o, mitjançant una interfície, util-

3.4. RESULTATS

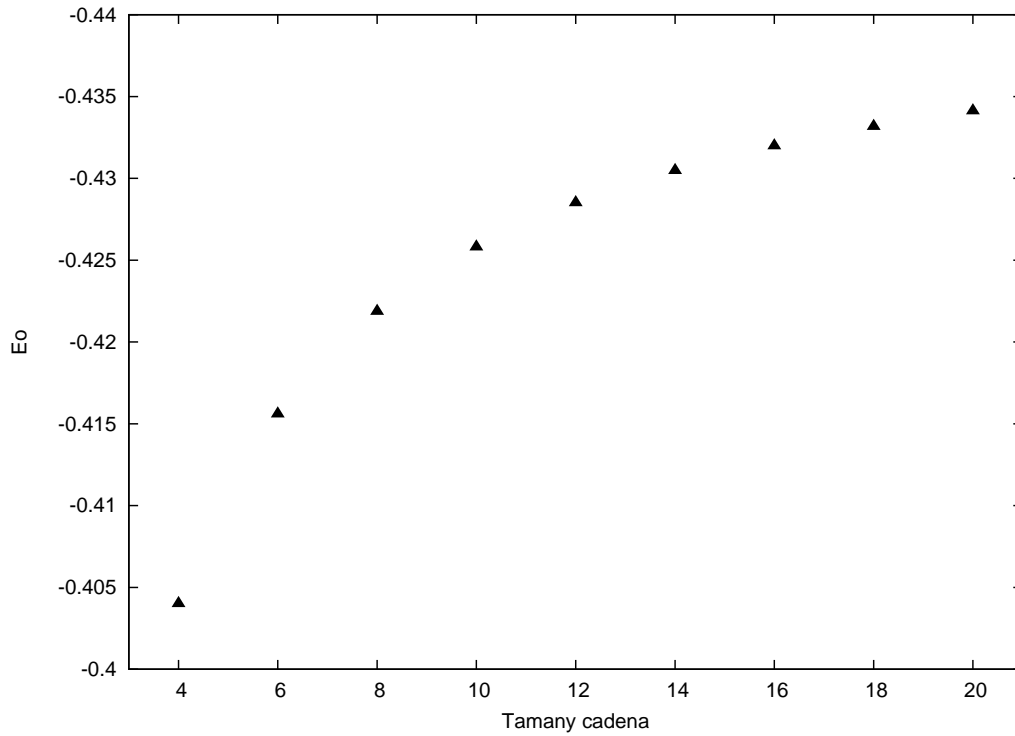


Figura 3.1: Valors de E_0 per a condicions de contorn obertes.

itzades des de codi escrit en C , com s'ha fet aquí. L'altra alternativa és, seguint a G.Golub i Q. YE [GY00], utilitzar una implementació eficient de l'algoritme de Lanczos amb matrius disperses.

El principal paràmetre que ens interessa estudiar és, com hem vist, l'energia del nivell fonamental. Farem servir l'energia *per posició* $E_0 = \frac{E}{N}$, obtinguda a partir de l'energia de tota la cadena (E) i del nombre de partícules que la formen (N).

Podem controlar el grau de precisió dels nostres resultats a partir de la condició d'aturada de l'algoritme de Lanczos. Quan per sota d'un determinar

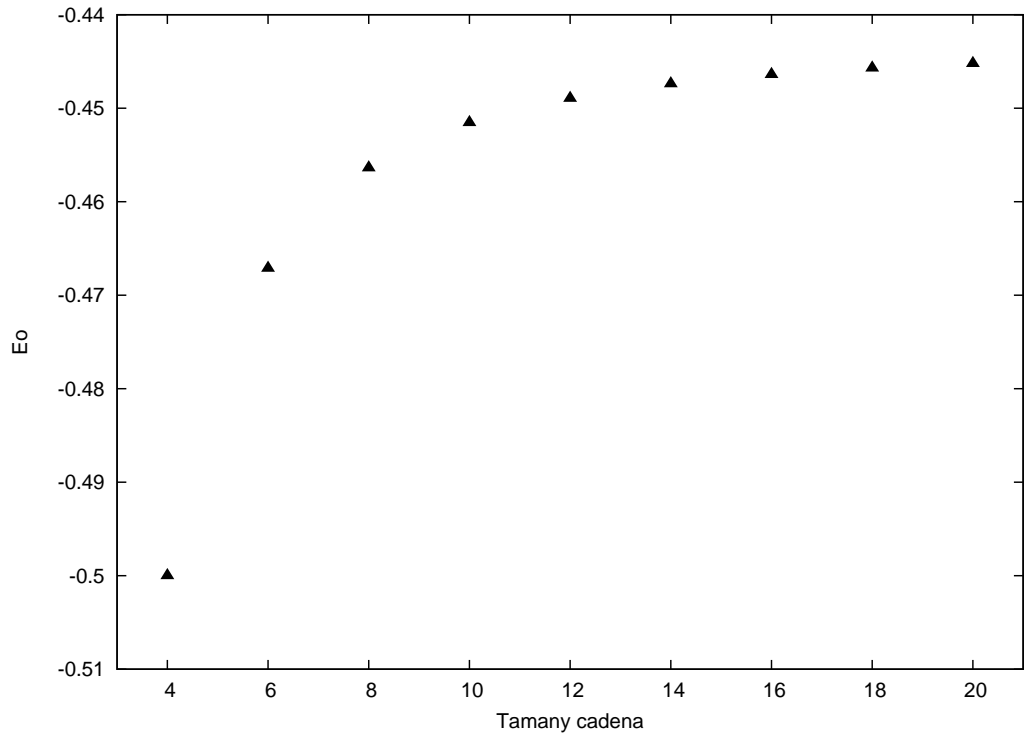


Figura 3.2: Valors de E_0 per a condicions de contorn periòdiques.

llindar no podem millorar el resultat que obtenim ampliant el tamany de la matriu T_k , l'algoritme s'atura proporcionant aquest resultat. S'ha establert aquí un límit de 10^{-13} per garantir una bona referència per als resultats aproximats que obtindrem als següents capítols.

Comencem veient l'evolució del valor de E_0 per a diferents longituds de la cadena, tant en condicions de contorn obertes (figura 3.1) o periòdiques (figura 3.2). Podem veure el comportament asimptòtic del E_0 , i pel cas de les condicions obertes com aquest valor tendeix cap al valor analític obtingut per Bethe per a la cadena infinita, $E_0 = -\ln(2) + \frac{1}{4} = -0.443147$.

3.4. RESULTATS

Per veure les dificultats computacionals d'aquest procediment per resoldre el problema podem analitzar el temps d'execució del procés de diagonalització per a cadenes de longitud diferent. Podem veure clarament (figures 3.3 i 3.4) el comportament exponencial en temps d'execució emprat. En espai de memòria l'algoritme també consumeix recursos de manera exponencial, limitant el tamany màxim de la cadena que podem estudiar.

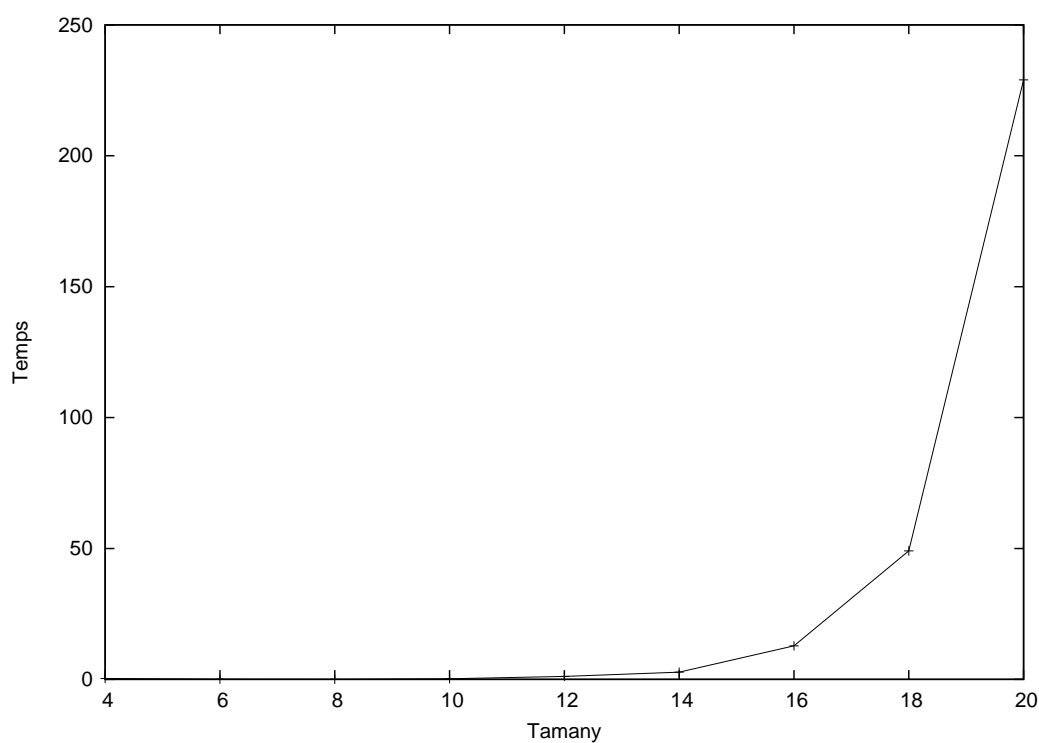


Figura 3.3: Temps d'execució en segons pel cas de condicions de contorn obertes. El comportament és clarament exponencial.

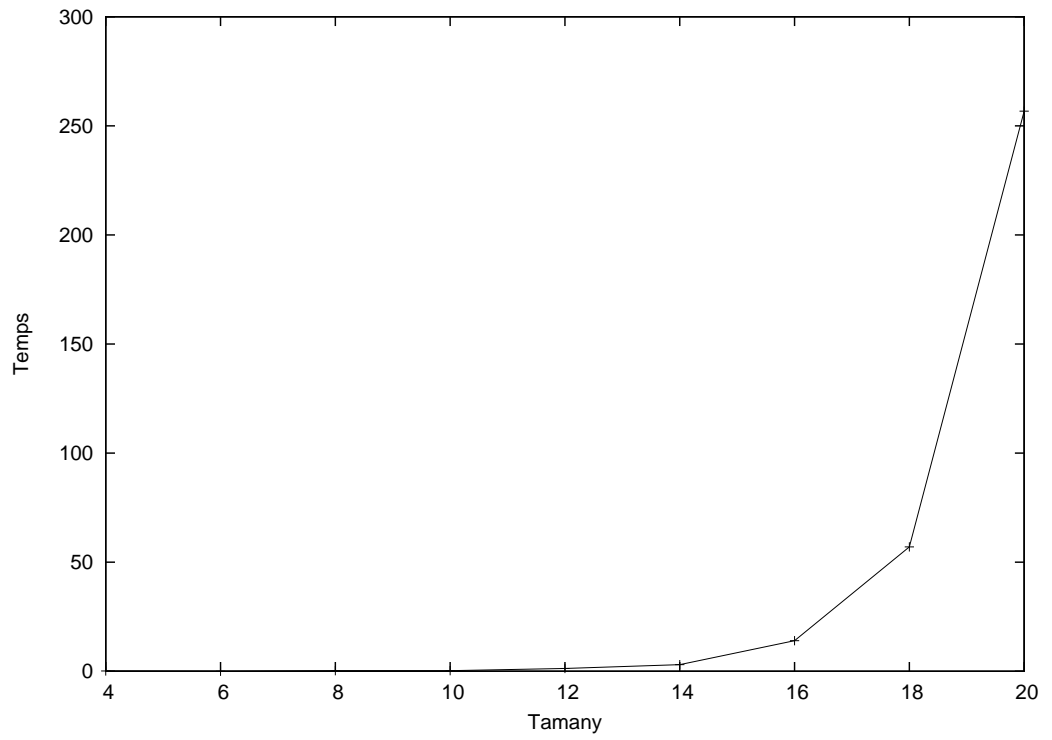


Figura 3.4: Temps d'execució en segons pel cas de condicions periòdiques.

Capítol 4

DMRG

*“It doesn’t matter how beautiful your theory is,
it doesn’t matter how smart you are.
If it doesn’t agree with experiment, it’s wrong.”*

Richard P. Feynman

4.1 Introducció

Hem vist al capítol anterior que la utilització de mètodes numèrics exactes pot resultar computacionalment inabordable. La mateixa natura exponencial del problema a resoldre fa que, a partir d’un tamany del sistema raonablement moderat (unes desenes de partícules), trobar aquestes solucions amb mitjans estàndards sigui impracticable.

En aquest punt es on hem de fer servir el coneixement que tenim de la natura dels elements que formen el nostre sistema, i el tipus d’interaccions

que existeixen entre aquests elements. Un millor coneixement de les lleis físiques implicades en el problema a resoldre ens pot permetre enfocar la resolució de manera més adequada a la informació que volem calcular.

Els esquemes de renormalització permeten la descripció de les propietats del sistema a partir de la descripció d'un sistema de tamany menor. Es defineixen unes regles d'“augment”, o com construir instàncies més grans a partir de les més petites. La clau d'aquests esquemes és que el tamany de la informació que emprem per descriure el sistema és constant. Per tant, fem servir el mateix tamany de la descripció per a problemes amb quantitats diferents de partícules, fet que permet tractar instàncies de problemes més grans.

El preu que hem de pagar per aquesta reducció d'informació és la pèrdua de precisió: deixem de proporcionar resultats exactes per oferir resultats aproximats. El grau de precisió ve directament determinat pel tamany de la descripció que emprem, de manera que l'error es pot fer arbitràriament petit.

A continuació es presenten les idees fonamentals dels esquemes de renormalització, i s'acaba per explicar i implementar el “density matrix renormalization group” (DMRG), que és un dels esquemes de renormalització que millors resultats ha proporcionat.

4.2 Renormalització

Suposem que volem descriure un sistema de partícules (p.ex. una cadena com en l'apartat anterior) d'una mida determinada. Per fer-ho comencem escrivint una descripció vàlida per a un sistema més petit, i definim una manera per anar fent augmentar el seu tamany. D'aquesta manera iterativa podem acabar assolint un sistema que tingui la mida que volem. La clau d'aquest mètode està en que a cada pas, a mesura que anem augmentant el tamany del sistema inicial, la descripció que fem servir no augmenta de tamany (en el nostre cas hauria de fer-ho exponencialment!).

Per tant per definir un esquema iteratiu de renormalització necessitem dos mètodes: un que ens permeti definir el creixement del nostre sistema (com construir una cadena de longitud l , tenint un sistema de longitud n , on $l > n$). L'altre ens ha de definir una manera de “retallar” la descripció del sistema de manera que al llarg de tot el procés la quantitat d'informació utilitzada sigui constant.

4.3 Estructura del problema

Suposem que tenim una cadena de partícules de longitud l , definida per una matriu H_l que ens defineix les seves propietats d'energia. Volem trobar la descripció per al sistema de p.ex. $2 \cdot l$ partícules. Si treballem en un sistema com en l'apartat anterior, on les partícules de la cadena unidimensional interactuaven només amb els seus veïns més propers (les partícules situades

immediatament a la seva dreta i a la seva esquerra) les regles que ens permeten construir $H_{2,l}$ són

$$\begin{aligned}
 [H_{BB}]_{i_1 i_2; i'_1 i'_2} &= [H_B]_{i_1 i'_1} \delta_{i_2 i'_2} + [H_B]_{i_2 i'_2} \delta_{i_1 i'_1} \\
 &+ [S_r^z]_{i_1 i'_1} [S_l^z]_{i_2 i'_2} + \frac{1}{2} [S_r^+]_{i_1 i'_1} [S_l^-]_{i_2 i'_2} \\
 &+ \frac{1}{2} [S_r^-]_{i_1 i'_1} [S_l^+]_{i_2 i'_2},
 \end{aligned} \tag{4.1}$$

on $\delta_{ii'}$ és la matriu identitat, i l'operació entre matrius és el producte tensorial que ja hem vist abans. Per les propietats del producte tensorial aquesta matriu $H_{2,l}$ és més gran que la matriu H_l , de manera que aplicant iterativament aquest procediment per tal de descriure cadenes més llargues arribem a un creixement exponencial.

Els termes que formen l'equació 4.1 són:

$[H_B]_{i_1 i'_1}$ La matriu H_B conté la descripció del bloc bàsic a partir del qual farem el creixement del tamany de la cadena. El seu tamany és $D \times D$, constant al llarg de tot el procés. Així mantenim fitat el tamany de tota la representació. La relació entre aquest paràmetre D i la precisió dels resultats serà l'element principal d'estudi al llarg del projecte.

$[S_r^z]_{i_1 i'_1} [S_l^z]_{i_2 i'_2}$ Interacció entre la partícula situada en la posició més a la dreta del bloc esquerre i la partícula situada més a l'esquerra del bloc dret. Com la interacció que estem considerant només es realitza entre veïns més propers, aquesta és la única interacció que es produeix entre

4.3. ESTRUCTURA DEL PROBLEMA

tots els elements dels dos blocs (apart de les interaccions que es produeixen dins de cada bloc). Aquest terme considera només la interacció en l'eix z .

$\frac{1}{2} [S_r^+]_{i_1 i'_1} [S_l^-]_{i_2 i'_2} + \frac{1}{2} [S_r^-]_{i_1 i'_1} [S_l^+]_{i_2 i'_2}$ Aquests termes, com l'anterior, només consideren la interacció entre les partícules dels extrems de cada bloc. En aquest cas es consideren conjuntament les interaccions en els eixos x i y .

Per construir les matrius $[S]$ fem servir a cada pas les definicions

$$\left[\tilde{S}_l^z \right]_{i_1 i_2; i'_1 i'_2} = [S_l^z]_{i_1 i'_1} \delta_{i_2 i'_2}, \quad (4.2)$$

$$\left[\tilde{S}_l^+ \right]_{i_1 i_2; i'_1 i'_2} = [S_l^+]_{i_1 i'_1} \delta_{i_2 i'_2}, \quad (4.3)$$

$$\left[\tilde{S}_l^- \right]_{i_1 i_2; i'_1 i'_2} = [S_l^-]_{i_1 i'_1} \delta_{i_2 i'_2}, \quad (4.4)$$

$$\left[\tilde{S}_r^z \right]_{i_1 i_2; i'_1 i'_2} = [S_r^z]_{i_2 i'_2} \delta_{i_1 i'_1}, \quad (4.5)$$

$$\left[\tilde{S}_r^+ \right]_{i_1 i_2; i'_1 i'_2} = [S_r^+]_{i_2 i'_2} \delta_{i_1 i'_1}, \quad (4.6)$$

$$\left[\tilde{S}_r^- \right]_{i_1 i_2; i'_1 i'_2} = [S_r^-]_{i_2 i'_2} \delta_{i_1 i'_1} \quad (4.7)$$

Així tenim que al llarg del procés iteratiu tant les matrius H_B com les matrius $[S]$ van creixent en tamany exponencialment. Si volem mantenir constant aquest tamany (i poder arribar a calcular propietats de sistemes més grans) necessitem un procés de “retallat”. Matemàticament el podem

expressar com

$$S_l^z = O\tilde{S}_l^z O^\dagger, \quad (4.8)$$

$$S_r^z = O\tilde{S}_r^z O^\dagger, \quad (4.9)$$

$$S_l^+ = O\tilde{S}_l^+ O^\dagger, \quad (4.10)$$

$$S_r^+ = O\tilde{S}_r^+ O^\dagger, \quad (4.11)$$

$$S_l^- = O\tilde{S}_l^- O^\dagger, \quad (4.12)$$

$$S_r^- = O\tilde{S}_r^- O^\dagger, \quad (4.13)$$

on la matriu O és rectangular i de tamany $D \times D^2$, on D és el tamany que volem mantenir per a la representació de les matrius H_B i S al llarg de tot el procés. Després de les operacions amb matrius del tipus 4.8-4.13 passem de tenir una matriu $D^2 \times D^2$ a tenir-ne una de tamany $D \times D$. D'aquesta manera el tamany de les nostres matrius es manté constant al llarg de tot l'algoritme.

Algoritme de renormalització

1. Formar H_{BB} a partir de H_B fent servir l'equació 4.1
 2. Formar representacions dels operadors pel nou sistema
 3. Formar la matriu O
 4. Aplicar l'operació amb la matriu O a tots els operadors
 5. Substituir H_B per H_{BB}
 6. Tornar a 1
-

Taula 4.1: Esquema de l'algoritme de renormalització

L'estructura dels algorismes de renormalització, proposats per K. Wilson

[Wil75] l'any 1971, s'exposa a la taula 4.1. El punt determinant es produeix quan descartem part de la descripció del nostre sistema per mantenir constant el tamany de la matriu H_B , fent servir la matriu O .

4.4 DMRG

Per completar l'esquema de renormalització cal un mecanisme per construir la matriu O que s'encarrega de mantenir estable el tamany del problema, independent del tamany real de la cadena que estem estudiant. Seguint les idees de Steven White [S.R92a, S.R92b], un possible mecanisme es pot construir basant-se en els estats més probables del sistema. Per fer-ho fem servir la matriu densitat del sistema que volem “retallar” i conservem els estats més probables. La matriu densitat (apèndix A) és un operador que expressa l'estat d'un sistema que es troba en l'estat $|a_1\rangle$ amb probabilitat p_1 , en l'estat $|a_2\rangle$ amb probabilitat $p_2 \dots$

$$\rho = \sum_i p_i |a_i\rangle\langle a_i|, \quad (4.14)$$

de manera que per conservar els estats més probables cal diagonalitzar la matriu ρ i conservar els estats corresponents als autovalors més grans. Un cop determinats aquests, la matriu O es forma amb els autovectors corresponents a aquests autovalors més grans.

Per definir el procés de creixement suposem que a cada pas afegim dues

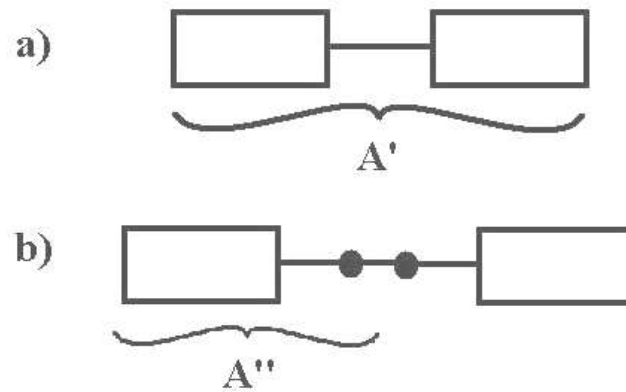


Figura 4.1: Pas de renormalització de l'algoritme clàssic (a) i de DMRG (b). El blocs indicats (A' i A'') són el punt de partida del següent pas de renormalització.

partícules al centre de la cadena que tenim formada fins al moment. Aquest sistema ve justificat per estudis sobre l'efecte que les condicions de contorn tenen sobre l'algoritme. A més, així l'estructura dispersa de les matrius implicades en els càlculs és va mantenint, amb la millora d'eficiència que ja hem vist que això suposa.

A cada pas afegim 2 noves partícules al centre de la cadena (figura 4.1), calculem els valors d'energia, i per començar el següent pas només mantenim informació de la meitat del sistema amb el que acabem de treballar. D'aquesta manera es controla el creixement i els resultats s'ajusten millor als valors exactes. Així al final de cada iteració el tamany de la cadena que hem descrit augmenta en una posició. Tot el procés complet es mostra a la taula 4.2. L'execució s'atura quan l'ampliació del tamany de la cadena produeix canvis

4.5. RESULTATS

en el valor del nivell d'energia. La precisió d'aquest valor d'estabilització depèn del paràmetre D , obtenint millors resultats a mesura que augmenta D ja que es manté més informació sobre l'estat real del sistema.

Algoritme DMRG per la cadena infinita

1. Formar bloc H_B a partir d'unes quantes partícules
 2. Formar H_{BB}
 3. Diagonalitzar H_{BB}
 4. Formar la matriu densitat ρ d'una meitat del sistema
 5. Diagonalitzar ρ per trobar les estats més probables del sistema
 6. Construir representacions dels operadors per a la meitat del sistema que considerem
 7. Aplicar la matriu de transformació O als operadors
 8. Substituir el bloc de longitud k de la dreta pel de $k + 1$
 9. Substituir el bloc de longitud k de l'esquerra pel de $k + 1$
 10. Tornar al pas 2
-

Taula 4.2: Esquema de l'algoritme DMRG pel cas infinit

4.5 Resultats

Basarem l'estudi dels resultats que obtinguem amb els mètodes d'aproximació en la comparació amb els resultats numèrics exactes que hem obtingut en l'apartat anterior. Ens centrarem en el valor de E_0 , tot i que altres magnituds també poden ser avaluades amb aquests mètodes.

Pel cas del model de Heisenberg unidimensional disposem del resultat analític trobat per H. Bethe [Bet31] l'any 1931, enunciat amb condicions de contorn obertes. Aquest valor és $E_0 = -\ln(2) + \frac{1}{4} = -0.443147$. Podem veure

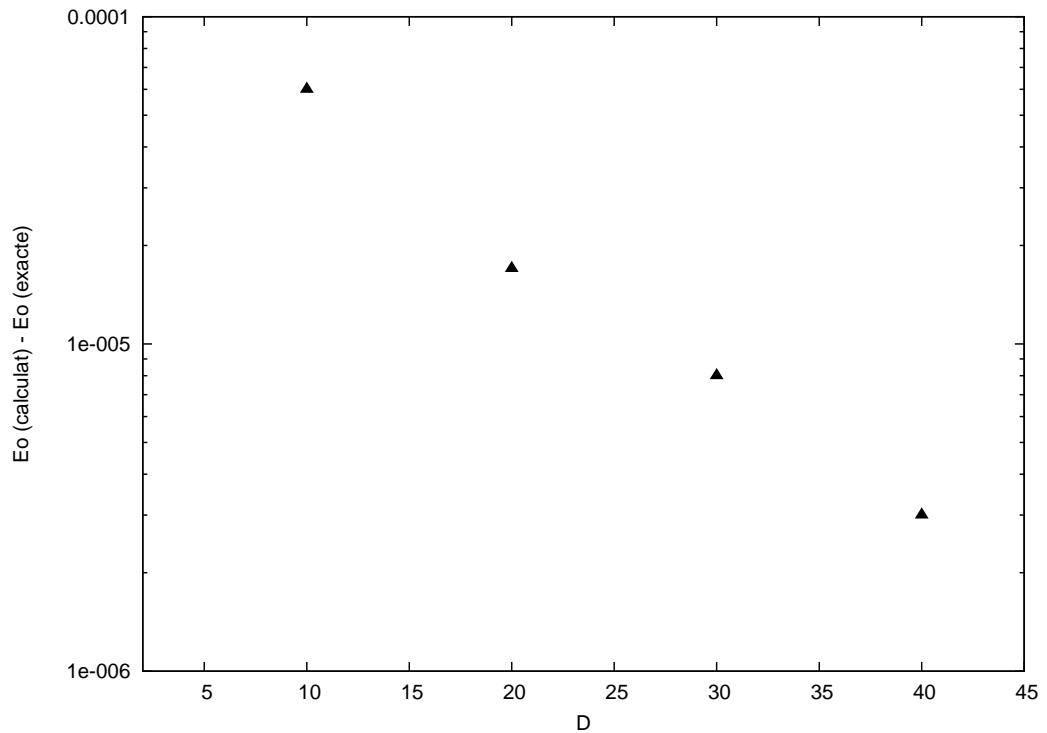


Figura 4.2: Error del càlcul de E_0 respecte als resultats exactes ($E_0 = -\ln(2) + \frac{1}{4}$), en funció del tamany de la descripció aproximada.

a la figura 4.2 que la precisió del resultat que obtenim depèn del tamany que triem per realitzar la descripció del sistema infinit de manera aproximada, tal com esperàvem. La capacitat de millora dels resultats de l'algoritme no és constant; presenta un comportament asimptòtic, de manera que a partir d'un determinat valor de D (relativament petit) la millora és negligible.

L'extensió d'aquest mètode per al cas de problemes finits on es defineixen condicions de contorn obertes també resulta molt acurada. El mètode DMRG no proporciona resultats tan acurats però en les solucions al problema finit

4.5. RESULTATS

format en condicions de contorn periòdiques. Per al mateix valor D la precisió es molt més baixa. És principalment degut al fet que en aquest model cal descriure també la interacció entre els extrems de la cadena. Al següent capítol veurem com una nova formulació matemàtica basada en teoria quàntica de la informació millora els resultats de DMRG en aquest cas.

Capítol 5

Algoritmes basats en teoria quàntica de la informació

*“Every mathematical discipline goes through three periods of development:
the naive, the formal, and the critical.”*

David Hilbert

5.1 Introducció

Fins ara hem vist com els esquemes de renormalització podien produir una solució iterativa per tipus de problemes com el de la cadena de partícules que hem estat estudiant. Amb una quantitat molt reduïda de paràmetres s’aconsegueix una descripció molt acurada dels valors numèrics d’algunes de les magnituds físiques a estudiar. Aquesta validesa, que sembla justificada

pel principi físic que es fa servir en la seva formulació (mantenir la descripció més probable del sistema a cada pas), pot ser formulada amb més precisió matemàtica.

Amb l'aparició del mètode DMRG van aparèixer també a la bibliografia els treballs de Affleck, Kennedy, Lieb, Tasaki, Rommer i Östlund [OR95, RO97, AKLT87] que proposen una descripció matemàtica per un sistema de partícules unidimensional. Aquestes noves formulacions justificaven el principi matemàtic sobre el que el DMRG es basa (tot i haver sigut formulat en un context diferent), i a més en mostraven les seves limitacions. Aquestes limitacions, ja detectades en els primers articles que presentaven el mètode DMRG, corresponen sobretot als sistemes on s'estableixen unes condicions de contorn periòdiques. En aquestes condicions, aconseguir la mateixa precisió que en els altres casos requeria una descripció del sistema molt més gran.

Partint d'aquesta nova formulació matemàtica, que ara introduïrem, i reinterpretant els components matemàtics **fent servir eines de la teoria de la informació** quàntica [VPC04] tenim un nou algorisme iteratiu que ofereix uns millors resultats. Pel cas de condicions de contorn obertes aquest nou mètode és equivalent al DMRG. Per al cas de condicions de contorn periòdiques, millora clarament els resultats del DMRG.

Començarem presentant la formulació matemàtica de l'algorisme per acabar implementant-lo fent servir algunes millores que ens permet la pròpia estructura del sistema, i que n'augmenten clarament la seva eficiència.

5.2 Formulació

Podem reformular el problema que hem estudiat fins, seguint les idees publicades per Verstraete, Porras i Cirac [VPC04], ara de forma que cada partícula del nostre sistema és substituïda per 2 subsistemes a_k i b_k per a cada posició k (figura 5.1). Aquests subsistemes són de dimensió D , que serà el paràmetre

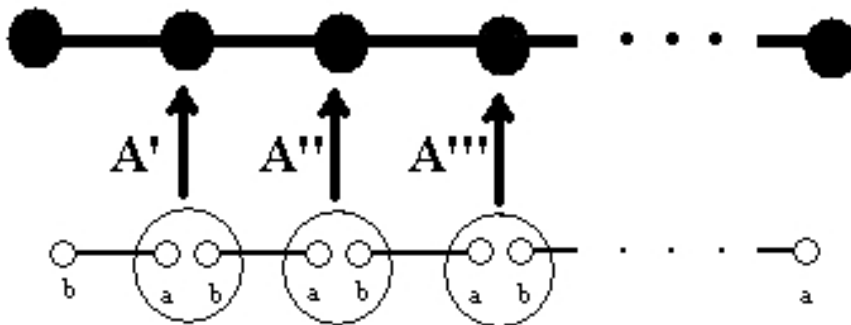


Figura 5.1: Nova formulació del problema fent servir teoria quàntica de la informació. Cada posició s'ha substituït per 2 sistemes (a_k i b_k) de dimensió D . El conjunt de matrius A transformen la nova representació en el model físic.

més important que definirà el nostre algoritme i que determinarà la precisió dels resultats. Aquest paràmetre D es correspon en significat i funció al paràmetre D que caracteritzava l'algoritme DMRG del capítol anterior. El tamany total de la descripció del sistema serà proporcional a aquest valor D , i a N (recordem que en el capítol 3, cercant la solució exacta, el tamany

creixia exponencialment amb el tamany N de la cadena).

El sistema b_k de cada posició es troba *entrellaçat* amb el corresponent a_{k+1} , com a la figura 5.1. La descripció del sistema la fem ara a partir de l'estat d'entrellaçament entre els estats b_k i a_{k+1} , com vam veure al capítol 1 per al sistema de dues partícules

$$|\phi\rangle := \sum_{\alpha=1}^D |\alpha_{b_k}\rangle \otimes |\alpha_{a_k}\rangle, \quad (5.1)$$

per a cada parell de sistemes b_k i a_{k+1} (en total en tenim N parells), amb les respectives bases $|\alpha_{b_k}\rangle$ i $|\alpha_{a_k}\rangle$.

Podem passar d'aquesta nova manera de descriure el nostre sistema a la corresponent al model físic que hem estat fent servir fins ara mitjançant un conjunt de matrius definides per a cada posició, A^s , de tamany $D \times D$. Per a la descripció d'un sistema de N partícules hem de considerar el conjunt de coeficients $c^{i_1 \dots i_N}$ que defineixen el nostre estat

$$|\psi\rangle := \sum_{i_1 \dots i_N=0}^1 c^{i_1 \dots i_N} |i_1 \dots i_N\rangle. \quad (5.2)$$

Podem obtenir els valors dels 2^N coeficients $c^{i_1 \dots i_N}$ a partir de les matrius A^s , de manera que aquestes defineixen completament un estat determinat. Per determinar un valor concret d'un dels paràmetres $c^{i_1 \dots i_N}$ només hem de calcular

$$c^{i_1 \dots i_N} = \text{Tr}(A^{[1],i_1} \dots A^{[N],i_N}). \quad (5.3)$$

5.2. FORMULACIÓ

Les matrius A^s projecten la descripció “artificial” del sistema que hem fet amb els subsistemes a_k i b_k , a l'estat físic de d estats. Fins ara, com les nostres cadenes estaven formades per *qubits*, teniem $d = 2$. Així, per a cada posició k tenim definides dues matrius, $A^{[k],0}$ i $A^{[k],1}$. D'aquesta manera estem emmagatzemant els 2^N paràmetres que ens caldrien habitualment per descriure el nostre sistema en una sèrie de matrius A^s de tamany total $N \times D^2$. A la figura 5.2 podem veure com evoluciona aquest tamany per a alguns dels valors de D que s'han emprat, comparant-lo amb el tamany de la descripció exacta.

D'aquesta descripció, el que hem de fer a cada pas de l'algoritme és actualitzar les matrius A^s de la posició en que ens trobem, subjectes a que l'estat que descriuen correspon al de mínima energia.

Com hem definit ara el problema amb condicions de contorn periòdiques, l'última posició de la cadena (posició $k = N$) té com a veïns més propers a les partícules de les posicions $k = N - 1$ i $k = 1$, on N és el nombre de partícules que formen la nostra cadena. Amb aquesta disposició tenim que la topologia del sistema és la d'un anell: totes les partícules de la cadena tenen 2 veïns més propers, un a la dreta i un altre a l'esquerra, úniques partícules amb les que interactúa. Les partícules dels extrems de la cadena “tanquen” l'anell (figura 5.3) convertint-se en veïns més propers.

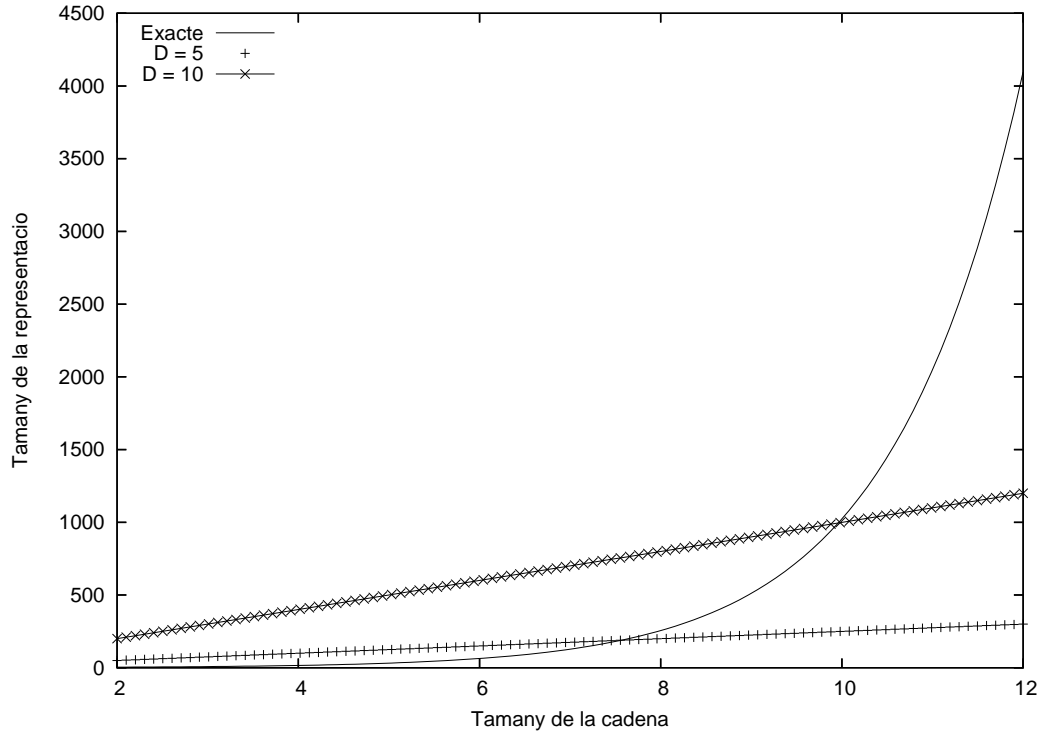


Figura 5.2: Relació entre el tamany real dels paràmetres necessaris per descriure el sistema i el tamany de la descripció aproximada (determinada pel valor del paràmetre D), en funció del tamany de la cadena N .

5.3 Algoritme

A partir de la formulació anterior podem establir un algoritme iteratiu per estimar el nivell fonamental d'energia de la cadena de *qubits*, on la descripció del sistema està continguda en el conjunt de valors de les matrius $A^{[k],s}$. Podem formular un algoritme tal i com es descriu a continuació.

A cada pas ens situem en una posició k del sistema, i cerquem les matrius $A^{[k]}$ d'aquesta posició que minimitzen el valor d'energia per a tota la cadena.

5.3. ALGORITME

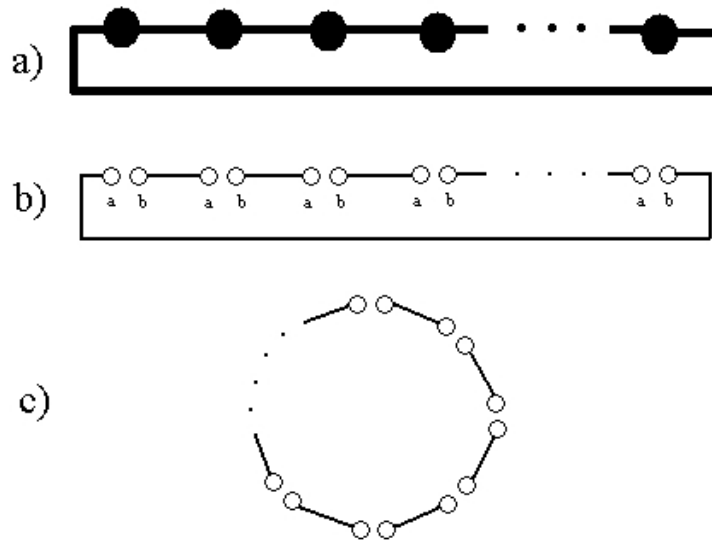


Figura 5.3: El problema original definit amb condicions periòdiques (a). Els estats dels extrems de la nova representació (b) estan connectats. La cadena es transforma en un anell (c).

Actualitzem aquestes matrius i ens desplaçem a una nova posició. Així, anem iterant per a totes les posicions de la cadena fins que trobem un valor estable de l'energia (canvis en les matrius d'aquesta posició no canvien el valor total de l'energia). D'aquesta manera hem convertit el problema de trobar el mínim d'energia global de tota la cadena en un problema de trobar les matrius a cada posició (sense modificar la resta de matrius $A^{[k],s}$ per a les altres posicions) que minimitzen aquesta energia.

Per anar recorrent totes les posicions del sistema ens situem inicialment p.ex. en la posició $k = 1$. Determinem les matrius $A^{[1],s}$ d'aquesta posició que

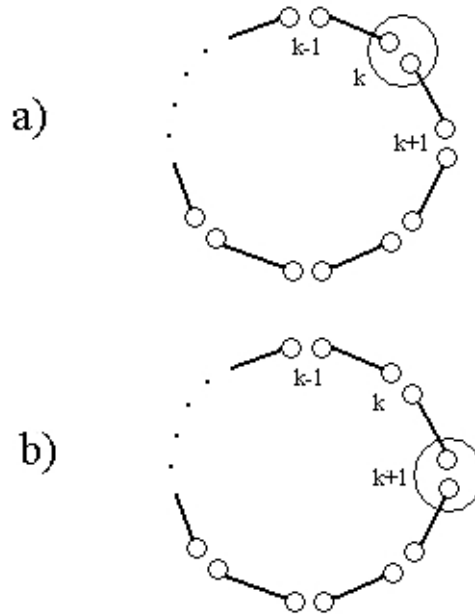


Figura 5.4: Després d'actualitzar les matrius A de la posició k (a), passem a la posició $k + 1$ circulant en sentit horari (b). Si circulem en sentit antihorari passem a la posició $k - 1$.

minimitzen l'energia de tota la cadena. Un cop determinades aquestes noves matrius, ens desplaçem a la següent posició ($k = 2$), i calculem les noves $A^{[2],s}$ d'aquesta posició fent servir les matrius $A^{[1],s}$ de la iteració anterior. Operem així fins arribar a la posició $k = N$, a partir de la qual seguim recorrent la cadena però ara en sentit contrari (dirigint-nos des de la posició $k = N$ fins a $k = 1$). Seguim operant així fins trobar un valor mínim en el que s'estabilitzi el valor de E_0 . Com a cada pas cerquem les matrius A^0 i A^1 que minimitzen l'energia total, aquesta no pot augmentar mai (en cas pitjor es

5.3. ALGORITME

manté igual). Quan assolim el valor mínim els valors de A^s no s'actualitzen, ja que la nova descripció és equivalent a l'anterior i els seus nivell d'energia són iguals. Aquest valor mínim d' E_0 correspon al valor d'energia del nivell fonamental, que es el que volem calcular.

A cada pas hem de resoldre un sistema d'equacions que ens determini els coeficients de les matrius $A^{[k],s}$ que minimitzen l'energia. Aquest sistema d'equacions, resultat de la condició de minimització d' E_0 , és equivalent a un sistema d'autovalors similar als que hem vist al capítol 2 (de fet l'algoritme que farem servir per resoldre'l serà el de Lanczos, tal com havíem fet abans, ara però amb alguna modificació). Es pot demostrar que el problema de diagonalització que hem de resoldre és [VPC04]

$$E = \frac{\langle \Psi | H | \Psi \rangle}{\langle \Psi | \Psi \rangle} = \frac{\langle \psi^{[M]} | H_M | \psi^{[M]} \rangle}{\langle \psi^{[M]} | N_M | \psi^{[M]} \rangle}, \quad (5.4)$$

on N_M i H_M són matrius quadrades de tamany $d \times D^2$, determinades a partir de les matrius $A^{[M],s}$ de les posicions $k \neq M$. El vector $|\psi^{[M]}\rangle$ es forma directament a partir dels paràmetres de les matrius $A^{[M],s}$. La relació entre tots aquests elements la podem expressar com

$$H_M \begin{pmatrix} a^0 \\ a^1 \end{pmatrix} = E_0 \cdot N_M \begin{pmatrix} a^0 \\ a^1 \end{pmatrix},$$

on a^0 i a^1 són les representacions en forma de vector dels coeficients de les matrius $A^{[M],0}$ i $A^{[M],1}$ respectivament. Així els coeficients de les matrius $A^{[M],s}$

es converteixen en les incognites d'unes equacions que condicionen els seus valors a l'estat de mínima energia (es tracta d'un problema de minimització), i els paràmetres que defineixen el problema corresponen als coeficients de les matrius A^s de la resta de posicions $\neq M$.

A cada pas doncs hem de determinar les matrius N_M i H_M , resoldre el sistema d'autovalors (5.4), i amb els autovectors resultants ($|\psi^{[M]}\rangle$) construir les noves matrius $A^{[M],s}$ per a la posició on ens trobem, i desplaçar-nos a la següent posició. Així anirem modificant successivament les matrius A^s per a les posicions que anem recorrent fins a trobar un valor estable de E_0 .

Algoritme de renormalització per a condicions periòdiques

1. Establir les matrius A inicials
 2. $M = 1$
 3. Circular en sentit horari per la cadena
(si $M = N$ circular en sentit antihorari)
 4. Formar H_M i N_M a partir de les matrius $A^{[k],s}$ de les posicions $k \neq M$
 5. Resoldre el problema d'autovalors. Obtenim E_0 per aquest pas.
 6. Composar $A^{[M],s}$ amb els autovectors corresponents a E_0
 7. Si E_0 no convergeix, tornar a 3
-

Taula 5.1: Esquema de l'algoritme de renormalització per a condicions de contorn periòdiques

Aquest problema d'autovalors és similar al que calia resoldre en el capítol 1, quan volíem resoldre el mateix problema de manera exacta. En aquell cas no es tractava del problema d'autovalors generalitzat que tenim ara

$$A \cdot x = \lambda \cdot B \cdot x. \tag{5.5}$$

5.3. ALGORITME

L'autovalor x es farà servir per determinar les matrius A^s de la posició actual. A més a cada pas d'iteració obtenim el valor mínim actual d'energia (valor λ), que és el resultat del nostre nivell fonamental del sistema

$$H_M \cdot |\psi^{[M]}\rangle = E_0 \cdot N_M \cdot |\psi^{[M]}\rangle. \quad (5.6)$$

5.3.1 Càlcul de N_M i H_M

Per completar l'algoritme només ens cal determinar les matrius H_M i N_M a partir de les matrius A^s que tenim definides per a cada posició. En la formulació que estem fent servir podem recórrer a les expressions

$$\langle \Psi | O_1 \dots O_N | \Psi \rangle = \text{Tr} \left(E_{O_1}^{[1]} \dots E_{O_N}^{[N]} \right), \quad (5.7)$$

on

$$E_O^{[k]} = \sum_{s,s'=1}^d \langle s | O | s' \rangle A^{[k],s} \otimes (A^{[k],s})^*. \quad (5.8)$$

P.ex. si volem calcular $E_{\mathbf{1}}^{[k]}$ per a la posició k tenim

$$\begin{aligned} E_{\mathbf{1}}^{[k]} &= \langle 1|1 \rangle A^{[k],1} \otimes (A^{[k],1})^* \\ &\quad + \langle 1|0 \rangle A^{[k],1} \otimes (A^{[k],0})^* \\ &\quad + \langle 0|1 \rangle A^{[k],0} \otimes (A^{[k],1})^* \end{aligned}$$

$$\begin{aligned}
 & +\langle 0|0\rangle A^{[k],0} \otimes (A^{[k],0})^* \\
 = & A^{[k],0} \otimes (A^{[k],0})^* + A^{[k],1} \otimes (A^{[k],1})^*
 \end{aligned}$$

Per al cas $E_{\sigma_z}^{[k]}$ tenim

$$\begin{aligned}
 E_{\sigma_z}^{[k]} & = \langle 1|\sigma_z|1\rangle A^{[k],1} \otimes (A^{[k],1})^* \\
 & + \langle 1|\sigma_z|0\rangle A^{[k],1} \otimes (A^{[k],0})^* \\
 & + \langle 0|\sigma_z|1\rangle A^{[k],0} \otimes (A^{[k],1})^* \\
 & + \langle 0|\sigma_z|0\rangle A^{[k],0} \otimes (A^{[k],0})^* \\
 = & A^{[k],0} \otimes (A^{[k],0})^* - A^{[k],1} \otimes (A^{[k],1})^*
 \end{aligned}$$

Aquestes expressions, deduïdes a partir del formalisme exposat abans permeten escriure les matrius H_M i N_M com a un producte de matrius. P.ex, a partir de l'equació 5.9 trobem

$$\langle \Psi|\Psi \rangle = \text{Tr} \left(E_1^{[1]} \dots E_1^{[N]} \right). \quad (5.9)$$

Com hem expressat el problema d'autovalors en la base formada pels estats $|\psi^{[M]}\rangle$, hem de fer algunes transformacions per escriure la matriu N_M a partir d'aquest producte. La matriu N_M és de la forma

$$\left(\begin{array}{c|c} \tilde{N}_0 & 0 \\ \hline 0 & \tilde{N}_0 \end{array} \right),$$

5.3. ALGORITME

on

$$N_0 = E_1^{[k+1]} \dots E_1^{[N]} E_1^{[1]} \dots E_1^{[k-1]}, \quad (5.10)$$

i on k és la posició actual de càlcul de l'algoritme. Així per a determinar N_M només fem els coeficients de les matrius de posicions $\neq k$. Per obtenir \tilde{N}_0 a partir de N_0 cal realitzar l'operació $(\tilde{N}_0)_{(\alpha,\alpha'),(\beta,\beta')} = (N_0)_{(\alpha,\beta),(\alpha',\beta')}$. Es tracta d'una operació de transposició generalitzada. P.ex. si tenim una matriu

$$C = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{pmatrix}$$

i li apliquem l'operació anterior obtenim

$$\tilde{C} = \begin{pmatrix} 1 & 5 & 2 & 6 \\ 9 & 13 & 10 & 14 \\ 3 & 7 & 4 & 8 \\ 11 & 15 & 12 & 16 \end{pmatrix}.$$

La construcció de la matriu H_M depèn del tipus de model físic que representa el nostre sistema. A continuació veurem com construir-lo pels diferents models que hem estudiat amb els mètodes anteriors.

Per determinar completament el problema físic no cal únicament establir

el tipus de partícules que formen el sistema que volem estudiar. També cal especificar la naturalesa de les interaccions entre els seus elements. En sistemes d'aquestes característiques podem triar entre gran varietat de models, diferenciats típicament pels eixos que defineixen les interaccions, l'abast d'aquestes interaccions i la presència o no de camps externs com p.ex. camps magnètics.

En el nostre cas ens centrarem únicament en 2 tipus diferents de sistemes, tot i que aquest algoritme és fàcilment extensible als altres models, així com també és extensible a problemes amb altres geometries. Aquests models són el model d'Ising i el model de Heisenberg, tal i com hem fet als capítols anteriors.

Amb aquestes interaccions definides i de manera similar a com hem operat abans per calcular N_M , podem ja donar una expressió per al càlcul de la matriu H_M . Si considerem el model d'Ising (capítol 2) les interaccions entre veïns més propers estaven definides sobre l'eix z . La matriu H_M corresponent a aquesta interacció resulta

$$\left(\begin{array}{c|c} \tilde{H}_1 + \tilde{H}_2 & 0 \\ \hline 0 & \tilde{H}_1 - \tilde{H}_2 \end{array} \right),$$

on

$$H_1 := \sum_{n=1}^{N-1} E_1^{[k+1]} \dots E_{\sigma_z}^{[n]} E_{\sigma_z}^{[n+1]} \dots E_1^{[k-2]} E_1^{[k-1]} \quad (5.11)$$

$$H_2 := E_1^{[k+1]} \dots E_{\sigma_z}^{[k-1]} + E_{\sigma_z}^{[k+1]} \dots E_1^{[k-1]}. \quad (5.12)$$

5.3. ALGORITME

La transformació \tilde{H} és la mateixa que la transformació \tilde{N}_0 , similar com hem vist a una operació de transposició sobre una matriu.

Podem considerar el model de Heisenberg que hem estudiat abans com l'extensió als eixos x i y del model anterior. Hem de completar doncs la forma de la matriu H_M amb aquestes interaccions (la matriu N_M és de la mateixa forma en els dos models).

En el model de Heisenberg la matriu H_M que farem servir és de la forma

$$\left(\begin{array}{c|c} \tilde{H}_1 + \tilde{H}_2 & \tilde{H}_3 \\ \hline \tilde{H}_4 & \tilde{H}_1 - \tilde{H}_2 \end{array} \right),$$

on

$$H_3 := E_1^{[k+1]} \dots E_{\sigma_+}^{[k-1]} + E_{\sigma_+}^{[k+1]} \dots E_1^{[k-1]} \quad (5.13)$$

$$H_4 := E_1^{[k+1]} \dots E_{\sigma_-}^{[k-1]} + E_{\sigma_-}^{[k+1]} \dots E_1^{[k-1]}. \quad (5.14)$$

A cada pas doncs, després de realitzar els productes adequats, es construeixen aquestes matrius i es resol el problema d'autovalors que defineixen. Aquesta sèrie de productes és costosa computacionalment, però degut al caràcter successiu del recorregut que es realitza sobre la cadena podem definir unes relacions que permeten accelerar aquest procés.

5.3.2 Memòria dinàmica

L'eficiència de l'algoritme es pot veure dramàticament millorada si fem servir un esquema de memòria dinàmica al llarg del recorregut per totes les posicions de la cadena.

En les formulacions típiques de memòria dinàmica s'identifiquen parts dels càlculs que al llarg de l'algoritme s'aniran repetint. S'adapta l'algoritme per tal que aquestes operacions tan repetides es realitzin només un cop i, després de ser emmagatzemades convenientment, els seus resultats puguin ser fàcilment accessibles. Considerem que el producte de dues matrius de tamany $D^2 \times D^2$ té un cost $\sim D^4$. A cada pas hem de fer $\sim N^2$ operacions (productes principalment) amb les matrius. Veurem ara que unes definicions apropiades permetran mantenir el número de productes de matrius es pot mantenir independent de la longitud de la cadena.

Model d'Ising

Podem definir per a cada posició $k < M$ (M és la nostra posició actual) les matrius

$$r_k := E_1^{[1]} E_1^{[2]} \dots E_1^{[k-2]} E_1^{[k-1]}, \quad (5.15)$$

$$s_k := E_{\sigma_z}^{[1]} E_1^{[2]} \dots E_1^{[k-2]} E_1^{[k-1]}, \quad (5.16)$$

$$t_k := E_1^{[1]} E_1^{[2]} \dots E_1^{[k-2]} E_{\sigma_z}^{[k-1]}, \quad (5.17)$$

$$h_k := \sum_{n=1}^{k-2} E_1^{[1]} E_1^{[2]} \dots E_{\sigma_z}^{[n]} E_{\sigma_z}^{[n+1]} \dots E_1^{[k-2]} E_1^{[k-1]}. \quad (5.18)$$

5.3. ALGORITME

Per a les posicions $k \geq M$ definim

$$r_k := E_1^{[k]} E_1^{[k+1]} \dots E_1^{[N-1]} E_1^{[N]}, \quad (5.19)$$

$$s_k := E_{\sigma_z}^{[k]} E_1^{[k+1]} \dots E_1^{[N-1]} E_1^{[N]}, \quad (5.20)$$

$$t_k := E_1^{[k]} E_1^{[k+1]} \dots E_1^{[N-1]} E_{\sigma_z}^{[N]}, \quad (5.21)$$

$$h_k := \sum_{n=k}^{N-1} E_1^{[k]} E_1^{[k+1]} \dots E_{\sigma_z}^{[n]} E_{\sigma_z}^{[n+1]} \dots E_1^{[N-1]} E_1^{[N]}. \quad (5.22)$$

Hem d'establir ara les operacions de recurrència per construir les matrius r_{k+1} , s_{k+1} , t_{k+1} i h_{k+1} en el cas en que avancem en sentit horari a partir de r_k , s_k , t_k i h_k definides en el pas d'iteració anterior. Pel cas en sentit antihorari, a cada pas redefinim els valors de r_k , s_k , t_k i h_k amb els calculats anteriorment per a les matrius r_{k+1} , s_{k+1} , t_{k+1} i h_{k+1} .

Anem a veure com funciona la recurrència en el cas horari. Si escrivim l'expressió de r_k i r_{k+1}

$$\begin{aligned} r_k &:= E_1^{[1]} E_1^{[2]} \dots E_1^{[k-2]} E_1^{[k-1]}, \\ r_{k+1} &:= E_1^{[1]} E_1^{[2]} \dots E_1^{[k-2]} E_1^{[k-1]} E_1^{[k]}, \end{aligned}$$

veiem que es verifica la relació

$$r_{k+1} := r_k \cdot E_1^{[k]} \quad (5.23)$$

Operant de forma similar per a la resta de matrius trobem

$$s_{k+1} := s_k \cdot E_{\mathbf{1}}^{[k]}, \quad (5.24)$$

$$t_{k+1} := r_k \cdot E_{\sigma_z}^{[k]}, \quad (5.25)$$

$$h_{k+1} := h_k \cdot E_{\mathbf{1}}^{[k]} + t_k \cdot E_{\sigma_z}^{[k]}. \quad (5.26)$$

Ara definim les mateixes lleis de recurrència però per al cas en que “circulem” en sentit antihorari. Comencem igualment estudiant el cas de r_k i r_{k+1} . Ara tenim

$$\begin{aligned} r_k &:= E_{\mathbf{1}}^{[k]} E_{\mathbf{1}}^{[k+1]} \dots E_{\mathbf{1}}^{[N-1]} E_{\mathbf{1}}^{[N]} \\ r_{k+1} &:= E_{\mathbf{1}}^{[k+1]} \dots E_{\mathbf{1}}^{[N-1]} E_{\mathbf{1}}^{[N]}, \end{aligned}$$

de manera que podem establir la relació

$$r_k := E_{\mathbf{1}}^{[k]} \cdot r_{k+1}. \quad (5.27)$$

Similarment, per a la resta de matrius,

$$s_k := E_{\sigma_z}^{[k]} \cdot r_{k+1} \quad (5.28)$$

$$t_k := E_{\mathbf{1}}^{[k]} \cdot t_{k+1} \quad (5.29)$$

$$h_k := E_{\mathbf{1}}^{[k]} \cdot h_{k+1} + E_{\sigma_z}^{[k]} \cdot s_{k+1}. \quad (5.30)$$

Ara podem veure clarament la funció de les matrius anteriors. r i h s'u-

5.3. ALGORITME

tilitzaran directament per construir les matrius H_M i N_M . s i t són matrius auxiliars que ens permeten redefinir de manera iterativa les matrius de cada posició a partir de les que hem determinat en els passos anteriors, independentment de si recorrem la cadena en sentit horari o antihorari.

Amb aquestes definicions podem veure que el problema es redueix a realitzar a cada pas un nombre determinat de productes de matrius per preparar-les per a la següent iteració. Aquest nombre de productes és independent del nombre de partícules del nostre sistema, fet que fa desaparèixer la dependència del nou algoritme respecte el paràmetre N (número de partícules del sistema), per dependre únicament del paràmetre D (tamany de les matrius que es multipliquen a cada pas).

Model de Heisenberg

Proposem ara, de manera similar al cas anterior, un conjunt de matrius que ens permetin rescriure les matrius H_M i N_M amb unes poques multiplicacions de matrius. Definim per l'eix z

$$r_k := E_{\mathbf{1}}^{[1]} E_{\mathbf{1}}^{[2]} \dots E_{\mathbf{1}}^{[k-2]} E_{\mathbf{1}}^{[k-1]} \quad (5.31)$$

$$s_k^z := E_{\sigma_z}^{[1]} E_{\mathbf{1}}^{[2]} \dots E_{\mathbf{1}}^{[k-2]} E_{\mathbf{1}}^{[k-1]} \quad (5.32)$$

$$t_k^z := E_{\mathbf{1}}^{[1]} E_{\mathbf{1}}^{[2]} \dots E_{\mathbf{1}}^{[k-2]} E_{\sigma_z}^{[k-1]} \quad (5.33)$$

$$h_k^z := \sum_{n=1}^{k-2} E_{\mathbf{1}}^{[1]} E_{\mathbf{1}}^{[2]} \dots E_{\sigma_z}^{[n]} E_{\sigma_z}^{[n+1]} \dots E_{\mathbf{1}}^{[k-2]} E_{\mathbf{1}}^{[k-1]}. \quad (5.34)$$

Per als eixos x i y , fent servir relacions similars, podem escriure

$$s_k^+ := E_{\sigma_+}^{[1]} E_1^{[2]} \dots E_1^{[k-2]} E_1^{[k-1]} \quad (5.35)$$

$$s_k^- := E_{\sigma_-}^{[1]} E_1^{[2]} \dots E_1^{[k-2]} E_1^{[k-1]} \quad (5.36)$$

$$t_k^+ := E_1^{[1]} E_1^{[2]} \dots E_1^{[k-2]} E_{\sigma_+}^{[k-1]} \quad (5.37)$$

$$t_k^- := E_1^{[1]} E_1^{[2]} \dots E_1^{[k-2]} E_{\sigma_-}^{[k-1]} \quad (5.38)$$

$$h_k^{+-} := \sum_{n=1}^{k-2} E_1^{[1]} E_1^{[2]} \dots E_{\sigma_+}^{[n]} E_{\sigma_-}^{[n+1]} \dots E_1^{[k-2]} E_1^{[k-1]} \quad (5.39)$$

$$h_k^{-+} := \sum_{n=1}^{k-2} E_1^{[1]} E_1^{[2]} \dots E_{\sigma_-}^{[n]} E_{\sigma_+}^{[n+1]} \dots E_1^{[k-2]} E_1^{[k-1]} \quad (5.40)$$

per a les posicions $k < M$ (M és la nostra posició actual). Per a la resta de posicions ($k \geq M$) tenim

$$s_k^+ := E_{\sigma_+}^{[k]} E_1^{[k+1]} \dots E_1^{[N-1]} E_1^{[N]} \quad (5.41)$$

$$s_k^- := E_{\sigma_-}^{[k]} E_1^{[k+1]} \dots E_1^{[N-1]} E_1^{[N]} \quad (5.42)$$

$$t_k^+ := E_1^{[k]} E_1^{[k+1]} \dots E_1^{[N-1]} E_{\sigma_+}^{[N]} \quad (5.43)$$

$$t_k^- := E_1^{[k]} E_1^{[k+1]} \dots E_1^{[N-1]} E_{\sigma_-}^{[N]} \quad (5.44)$$

$$h_k^{+-} := \sum_{n=k}^{N-1} E_1^{[1]} E_1^{[2]} \dots E_{\sigma_+}^{[n]} E_{\sigma_-}^{[n+1]} \dots E_1^{[N-1]} E_1^{[N]} \quad (5.45)$$

$$h_k^{-+} := \sum_{n=k}^{N-1} E_1^{[k]} E_1^{[k+1]} \dots E_{\sigma_-}^{[n]} E_{\sigma_+}^{[n+1]} \dots E_1^{[N-1]} E_1^{[N]}. \quad (5.46)$$

Novament hem de rescriure les relacions de recurrència, exteses ara per als 3 eixos, per a incloure les noves interaccions. Comencem per la circulació en

5.3. ALGORITME

sentit horari

$$s_{k+1}^z := s_k^z \cdot E_1^{[k]} \quad (5.47)$$

$$s_{k+1}^+ := s_k^+ \cdot E_1^{[k]} \quad (5.48)$$

$$s_{k+1}^- := s_k^- \cdot E_1^{[k]} \quad (5.49)$$

$$t_{k+1}^z := r_k \cdot E_{\sigma_z}^{[k]} \quad (5.50)$$

$$t_{k+1}^+ := r_k \cdot E_{\sigma_+}^{[k]} \quad (5.51)$$

$$t_{k+1}^- := r_k \cdot E_{\sigma_-}^{[k]} \quad (5.52)$$

$$h_{k+1}^z := h_k^z \cdot E_1^{[k]} + t_k^z \cdot E_{\sigma_z}^{[k]} \quad (5.53)$$

$$h_{k+1}^+ := h_k^+ \cdot E_1^{[k]} + t_k^+ \cdot E_{\sigma_-}^{[k]} \quad (5.54)$$

$$h_{k+1}^- := h_k^- \cdot E_1^{[k]} + t_k^- \cdot E_{\sigma_+}^{[k]}. \quad (5.55)$$

Similarment, pel cas circulant en sentit antihorari

$$s_k^z := E_{\sigma_z}^{[k]} \cdot r_{k+1} \quad (5.56)$$

$$s_k^+ := E_{\sigma_+}^{[k]} \cdot r_{k+1} \quad (5.57)$$

$$s_k^- := E_{\sigma_-}^{[k]} \cdot r_{k+1} \quad (5.58)$$

$$t_k^z := E_1^{[k]} \cdot t_{k+1}^z \quad (5.59)$$

$$t_k^+ := E_1^{[k]} \cdot t_{k+1}^+ \quad (5.60)$$

$$t_k^- := E_1^{[k]} \cdot t_{k+1}^- \quad (5.61)$$

$$h_k^z := E_1^{[k]} \cdot h_{k+1}^z + E_{\sigma_z}^{[k]} \cdot s_{k+1}^z \quad (5.62)$$

$$h_k^+ := E_1^{[k]} \cdot h_{k+1}^+ + E_{\sigma_+}^{[k]} \cdot s_{k+1}^- \quad (5.63)$$

$$h_k^- := E_1^{[k]} \cdot h_{k+1}^- + E_{\sigma_-}^{[k]} \cdot s_{k+1}^+. \quad (5.64)$$

5.4 Resultats

5.4.1 Valor d' E_0

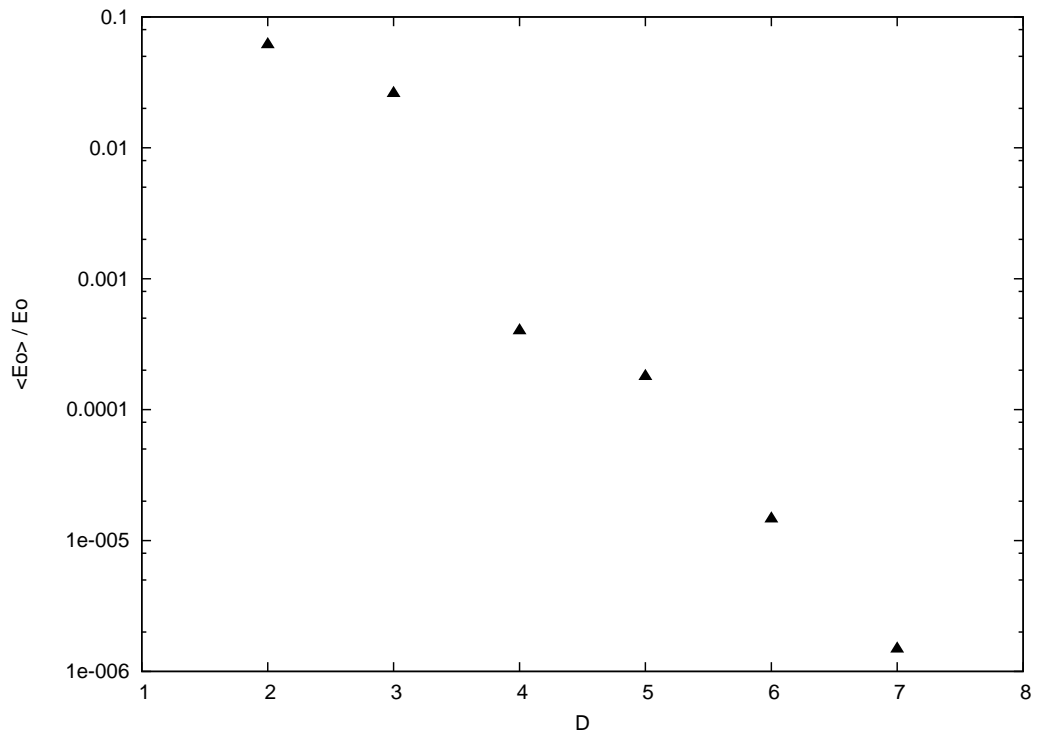


Figura 5.5: Precisió obtinguda per a una cadena de longitud $N = 8$ partícules. Amb valors del paràmetre D moderats s'aconsegueix ja una bona aproximació al valor de E_0 .

5.4. RESULTATS

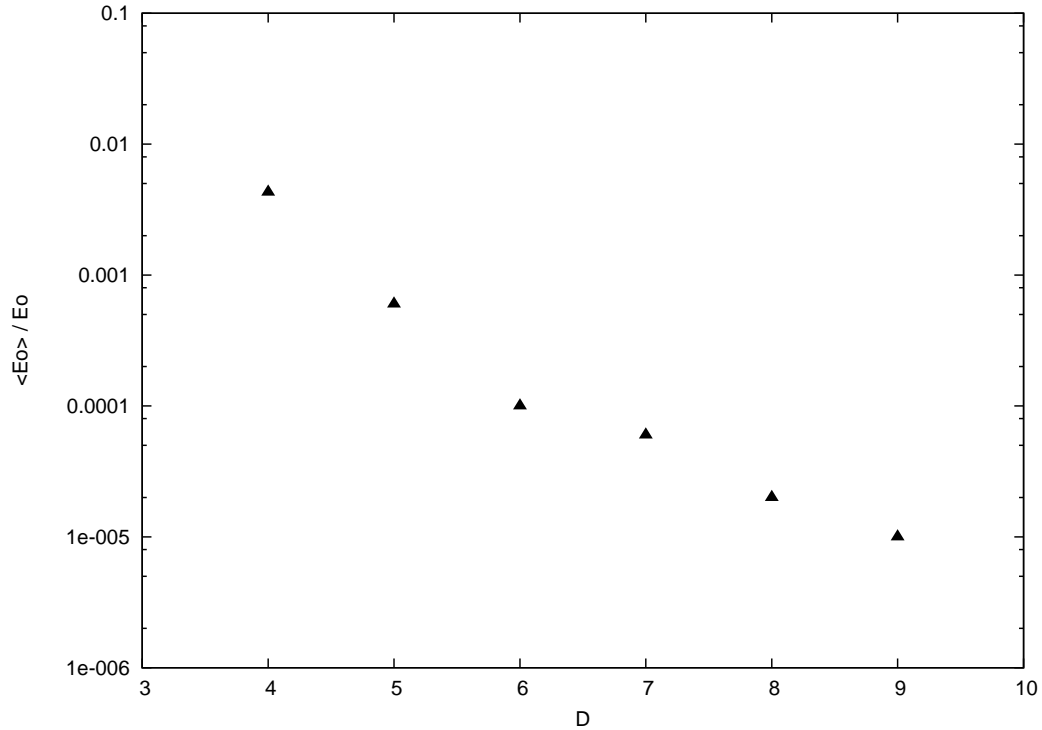


Figura 5.6: Precisió obtinguda per a una cadena de longitud $N = 12$ partícules.

S'ha centrat l'estudi numèric en la relació entre el paràmetre D , que determina el tamany de les matrius que fem servir, i el grau de precisió en comparació amb els resultats exactes. Les figures 5.5, 5.6 i 5.7 mostren aquesta relació per a cadenes de diferents tamanys, fent servir com a referència les dades exactes trobades abans. Podem veure que la tendència al valor exacte és molt similar en tots els casos. La dependència amb el valor D depèn del tamany de la cadena, ja que aquest condiona la relació entre el tamany de les dues representacions.

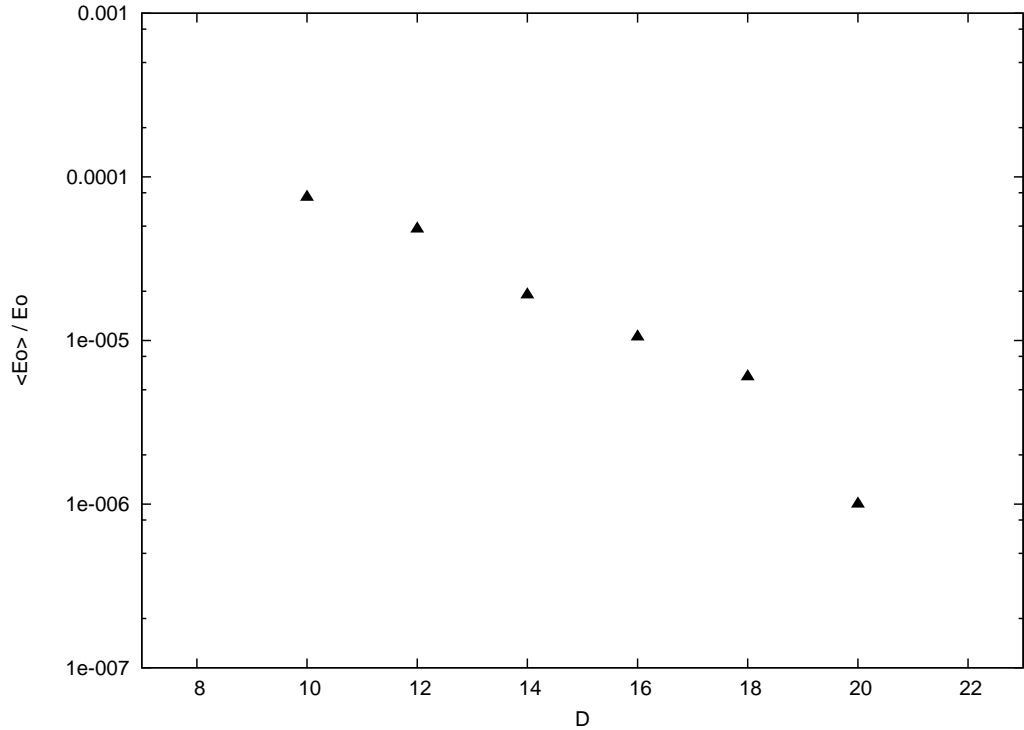


Figura 5.7: Precisió obtinguda per a una cadena de longitud $N = 28$ partícules.

Per a valors relativament de D obtenim bones aproximacions (de fins a 6 xifres significatives) en el valor de E_0 calculat. Per a la cadena $N = 28$ (figura 5.7), amb valor $D = 16$ tenim un sistema definit per $2 \times D^2 \times N = 14.336$ paràmetres enlloc dels $2^{28} = 268.435.456$ que calen per fer la descripció exacta. En aquestes condicions obtenim un valor de E_0 amb una precisió de 10^{-5} . Així podem veure que les característiques d'entrellaçament entre veïns propers permet la nova descripció ja que la informació descartada a cada pas no té una contribució significativa en el nivell fonamental [VJEK03].

5.4. RESULTATS

Cal destacar també el comportament similar de l'algoritme per a cadenes de longitud diferent. Per obtenir resultats més precisos el valor de D ha de tendir al valor del tamany real de la representació del sistema corresponent. Per a cadenes més llargues aquest espai és més gran, com hem vist al capítol 2. El valor necessari per obtenir una descripció exacta és $D = d^{\lfloor \frac{N}{2} \rfloor}$ [VPC04].

5.4.2 Periodicitat

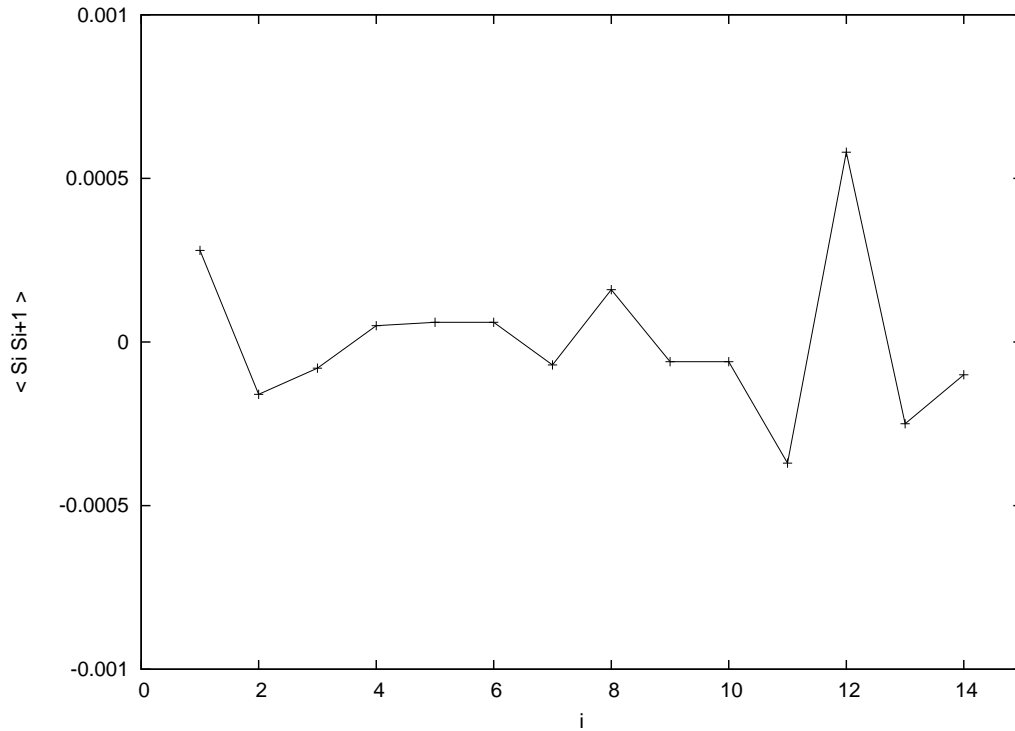


Figura 5.8: Valor de $\langle S_i, S_{i+1} \rangle$ al llarg de tota la cadena, per $N = 14$ i $D = 10$. L'estabilitat d'aquest valor indica la invariància translacional de la solució obtinguda.

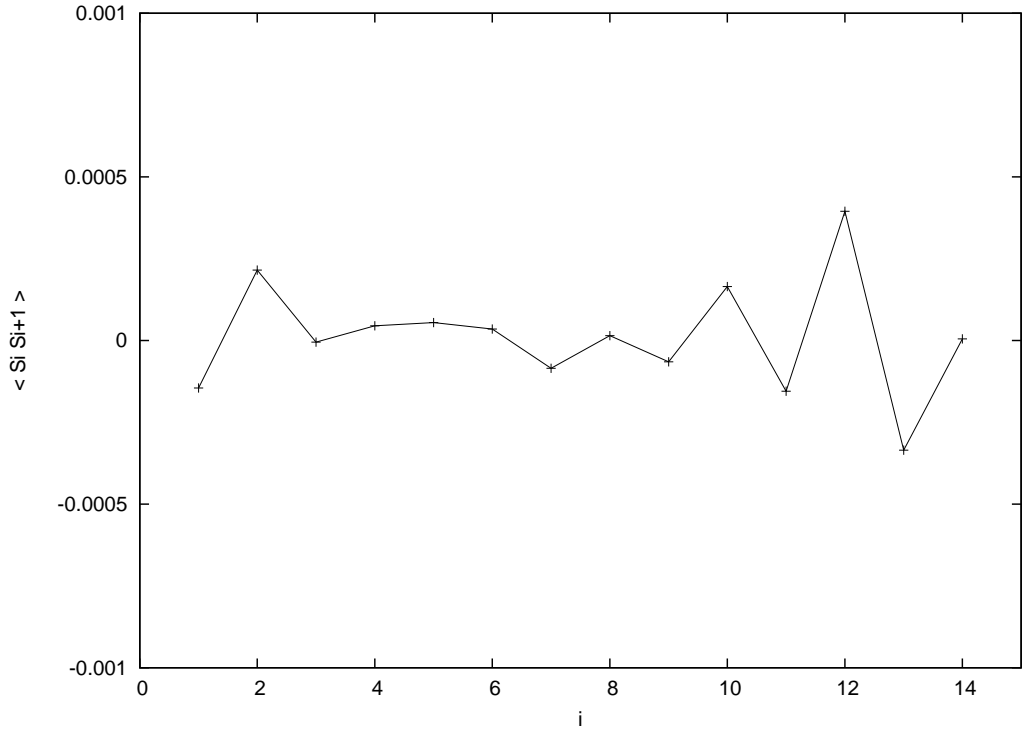


Figura 5.9: Valor de $\langle S_i, S_{i+1} \rangle$ al llarg de tota la cadena, per $N = 14$ i $D = 14$.

Com el nostre estudi de resultats es centra en models amb condicions de contorn periòdiques, podem verificar que les propietats de la cadena són similars a totes les posicions. Per fer-ho fem servir l'indicador $\langle S_i, S_{i+1} \rangle$. Un valor similar (o variacions petites, com és el nostre cas) a totes les posicions de la cadena acredita la simetria del model (figures 5.8 i 5.9), ja que degut a aquesta simetria el comportament ha de ser similar a totes les posicions. Podem veure que igual com passava amb l'energia, augmentant el valor del paràmetre D obtenim millors resultats.

5.4. RESULTATS

A mesura que considerem operadors més complexos, on hi intervenen magnituds que depenen de més d'una posició, el valor de D necessari per assolir una bona aproximació augmenta.

5.4.3 Evolució numèrica

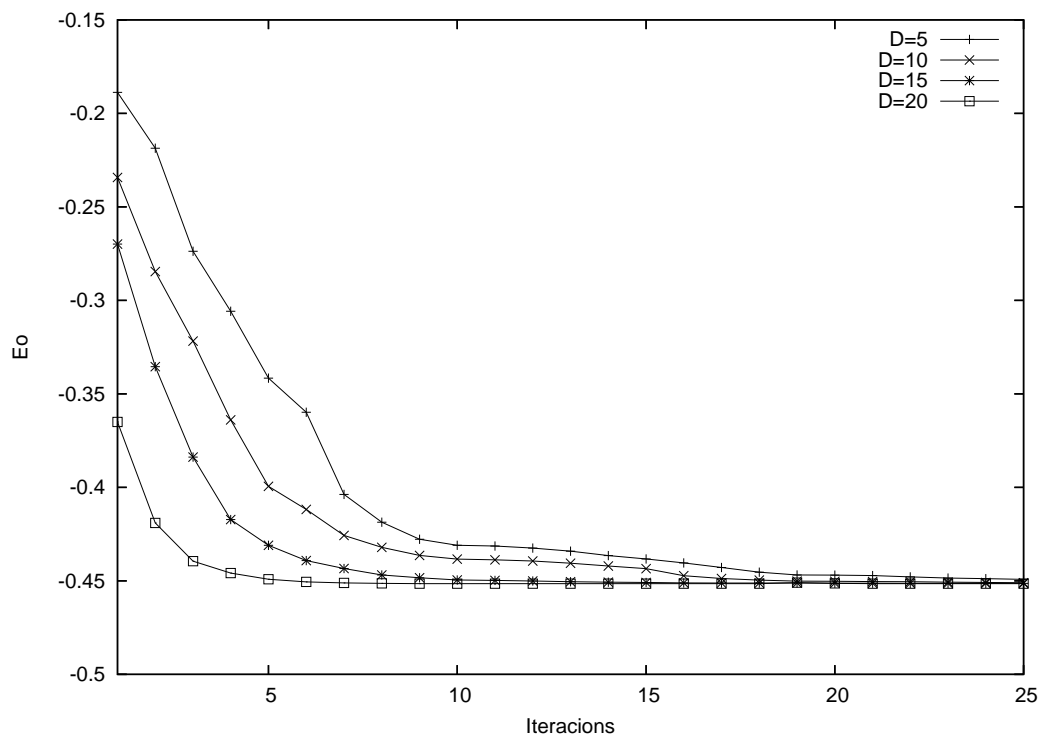


Figura 5.10: Evolució del valor de E_0 per a una cadena $N = 10$. La ràpida convergència de les primeres iteracions s'estabilitza a mesura que el valor s'apropa al resultat exacte.

Per analitzar el comportament del l'algoritme al llarg de tot el procés de càlcul, des de les condicions inicials fins al punt d'estabilització, representem

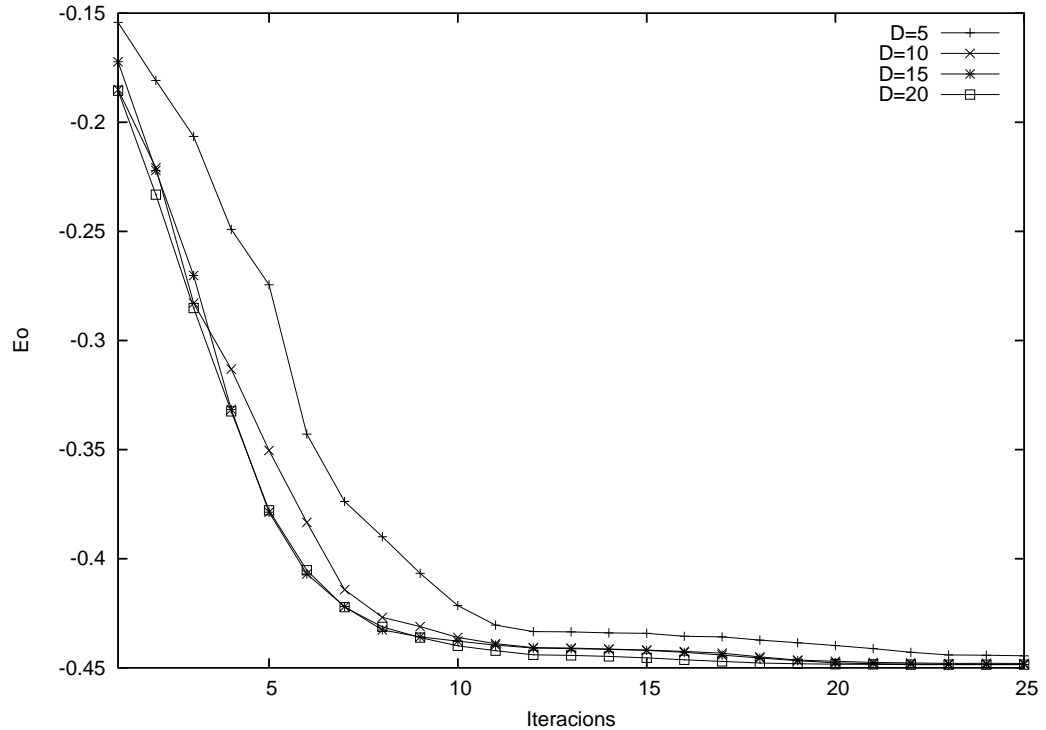


Figura 5.11: Evolució del valor de E_0 per a una cadena $N = 12$.

el valor de E_0 a cada pas. Podem veure (figures 5.10, 5.11, i 5.12) com aquest comportament, independentment de la longitud de la cadena, tendeix més ràpidament a la solució als primers estadis de l'evolució. A mesura que E_0 s'apropa al valor exacte apareix un comportament asimptòtic, que s'estabilitza en un valor amb precisió dependent de D .

Les condicions inicials del nostre sistema es poden establir de diferents maneres. Podem començar a treballar amb resultats parcials de l'algoritme DMRG i millorar els seus resultats, podem triar un estat concret que puguem suposar proper a l'estat fonamental, o en el nostre cas establir unes condicions

5.4. RESULTATS

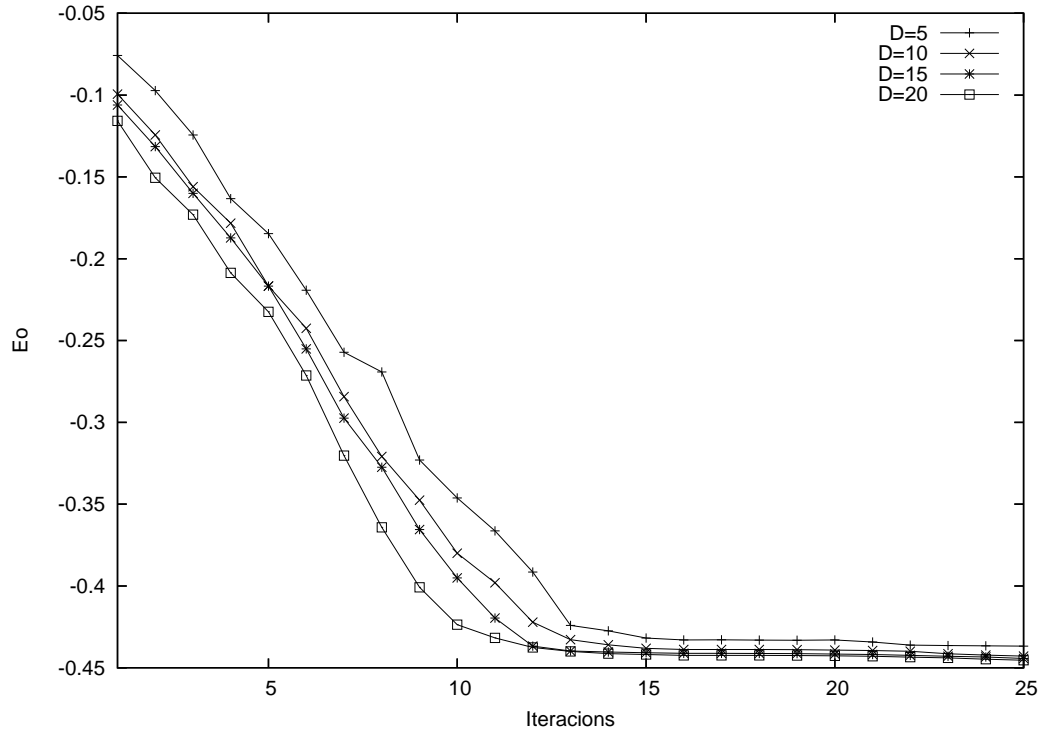


Figura 5.12: Evolució del valor de E_0 per a una cadena $N = 16$.

inicials aleatòries. Ho hem fet així primer per tenir un punt de partida homogeni a totes les execucions de l'algoritme. A més es disminueix el temps de preparació de l'estat a partir del qual començar a fer l'aproximació al valor real. Tot i que la tendència inicial és de convergir ràpidament, l'algoritme requereix així més iteracions. L'anàlisi de l'evolució als primers estadis de l'execució mostra que de seguida obtenir, amb el mateix algoritme, una bona aproximació sense gaire esforç de càlcul.

Per compensar la poca precisió d'aquest estat inicial fem servir, a les primeres iteracions de l'algoritme, menys precisió en l'obtenció de E_0 . Re-

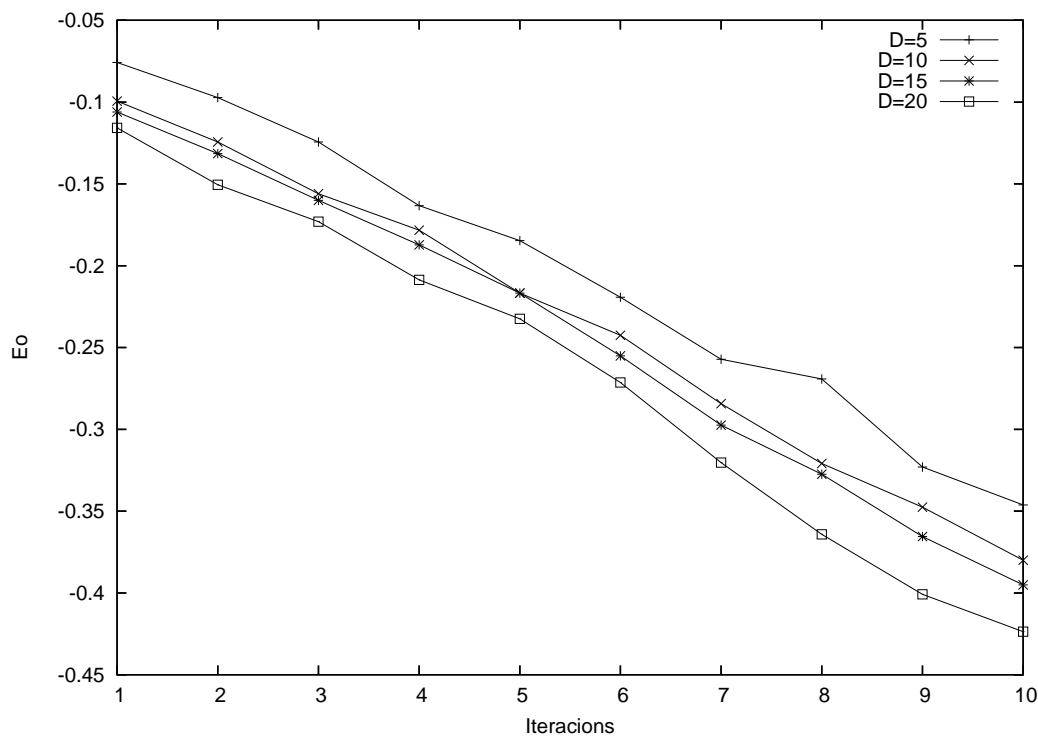


Figura 5.13: Evolució per a $N = 16$. L'aproximació inicial millora a l'augmentar el paràmetre D . La velocitat de convergència es mostra però independent d'aquest valor D .

cuperant les idees de l'algoritme de Lanczos (que aquí utilitzem en la seva versió generalitzada) equival a treballar amb matrius T_k més petites.

Així, en unes poques iteracions al llarg de tota la cadena ens situem en una bona primera aproximació per obtenir millors resultats (figura 5.13). Típicament la precisió inicial s'ha establert a 10^{-3} . Aleshores, un cop assolida aquesta precisió, l'augmentem fins que aconseguim la nova precisió requerida pel valor de E_0 . Repetim aquest procés d'aproximació “a salts”

5.4. RESULTATS

(figura 5.14) fins a no poder obtenir cap millora. Així obtenim un mètode numèricament estable i eficient, ja que establir el problema d'autovalors amb molta precisió en condicions molt allunyades de la solució suposa una gran despesa computacional.

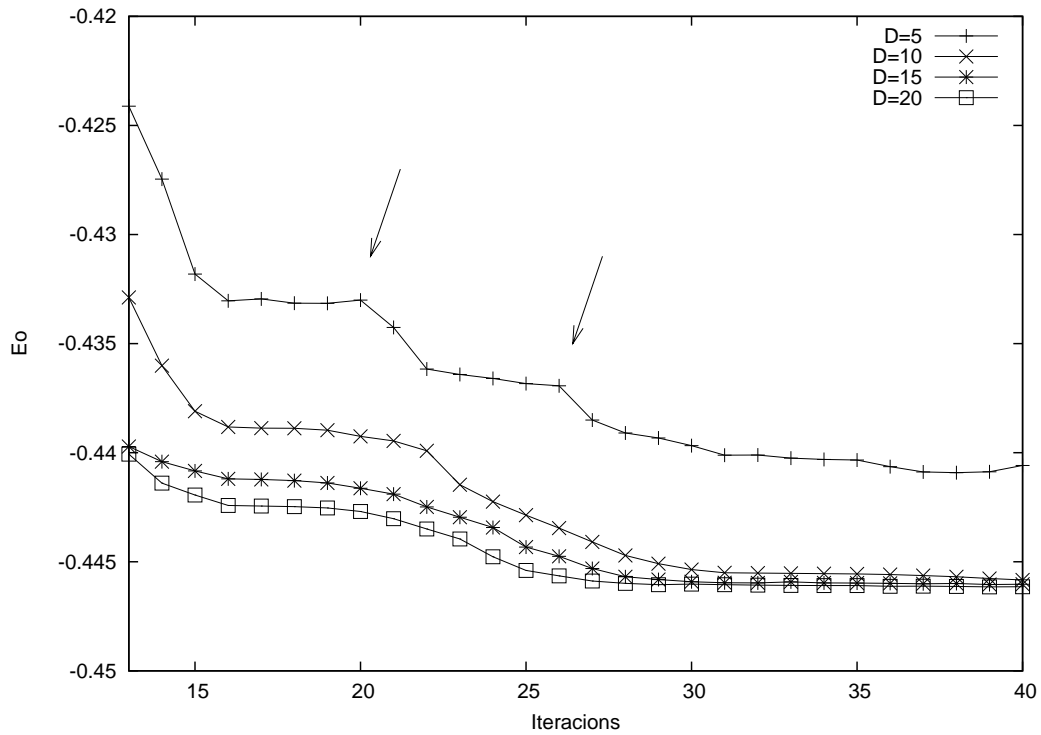


Figura 5.14: Evolució per a $N = 16$. Els salts indicats senyalen un canvi en la precisió parcial en els diferents estadis d'evolució de l'algoritme.

Aquests resultats mostren complet acord amb les dades originals de [VPC04], tant en els valors obtinguts per a E_0 com per a $\langle S_i, S_{i+1} \rangle$. Obtenim així la confirmació de tots els passos que hem realitzat en el disseny, implementació i execució d'aquest algoritme.

5.5 Discussió

Tant aquests darrers resultats com els corresponents a DMRG demostren l'èxit dels algoritmes de renormalització en sistemes físics com els que hem estudiat. Malgrat la seva precisió, no existeix una justificació clara de per què aquesta descripció tan reduïda d'un sistema físic permet un grau de precisió tan alt. A més, l'absència de mínims locals al llarg del procés de convergència numèrica tampoc està justificada teòricament.

Si bé hem vist com aquest darrer algoritme permetia calcular el nivell d'energia amb precisió arbitràriament petita (només cal augmentar el valor del paràmetre D), i millorar també els resultats de DMRG per a condicions de contorn periòdiques, existeixen algunes limitacions corresponents als seus límits d'aplicació. Aquest tipus d'algoritmes mostren una eficiència considerablement menor en funció del *grau de criticalitat* dels sistemes als que s'aplica, produïda per les condicions d'asimetria del sistema i la presència de camps magnètics. En aquest règim la descripció parcial (en blocs) que proposen aquests algoritmes deixa de ser vàlida, ja que els fenòmens que dominen el comportament de tota la cadena s'han de descriure globalment.

Capítol 6

Consideracions finals sobre el projecte

“We start off confused and end up confused on a higher level.”

Alan F. Chalmers

El desenvolupament d'un projecte de final de carrera requereix, a part del treball explícit de disseny, implementació i documentació, un treball de planificació i d'avaluació. Com es tracta d'un treball a desenvolupar durant un període relativament llarg de temps (la planificació inicial corresponia a 5 mesos), cal una bona planificació per organitzar les diferents parts de tot el procés i poder reflectir les possibilitats del projecte en unes condicions reals de temps i mitjans.

6.1 Planificació del projecte

Aquest projecte va començar a ser considerat després de xerrades amb membres del departament FEN de la UPC i de l'Institut de Ciències Fotòniques (ICFO), on es van comentar varies propostes i alternatives de projectes diferents. Un cop triat el tema, i sota credencial de pràctiques amb l'ICFO VUN0505, es va iniciar el projecte el mes de març del 2005, planificant-lo per ser finalitzat el juliol del mateix any. Tot i que s'havia de compaginar amb altres tasques, el temps de dedicació diari podia arribar a ser d'unes 7 hores, per poder cobrir així els corresponents 37'5 crèdits establerts per la normativa de PFC.

L'objectiu inicial era implementar l'algoritme de Verstraete, Porras i Cirac [VPC04], tenint en compte que no hi havia cap informació a l'article respecte als detalls de la implementació. Degut a les característiques d'aquest nou algoritme respecte als anteriors, i a la diversitat de possibilitats per obtenir resultats similars (mètode exacte, DMRG ...) es va decidir implementar també aquests altres mètodes per poder fer una avaluació comparativa.

El treball de les primeres setmanes del projecte va ser dedicat a la consulta de les fonts bibliogràfiques. Per una part a les relacionades directament amb el problema físic, i per l'altra a les solucions algorísmiques per resoldre algunes etapes, com la diagonalització. A més, es va decidir simultanejar aquestes consultes amb la implementació del mètode exacte. Per fer-ho, va caldre

6.1. PLANIFICACIÓ DEL PROJECTE

també realitzar consultes tant a la bibliografia estrictament matemàtica, com a les referències de les llibreries que haurien de ser utilitzades. Posteriorment es va començar la implementació dels mètodes aproximats.

La part final del projecte s'ha dedicat a la preparació de la documentació. No només ha consistit en la redacció explícita de la memòria del projecte, sinó també en la utilització dels algoritmes implementats per oferir els resultats d'un joc de proves complet i exhaustiu.

6.1.1 Diagrames de Gantt

Podem expressar la planificació del projecte fent servir diagrames de Gantt (figura 6.1). Hi podem veure la dedicació inicial a la consulta d'informació, que després seria utilitzada per construir els algoritmes. El temps de durada del projecte estava clarament delimitat, així que la durada no podia ser modificada. Tot i que inicialment semblava que les tasques relacionades amb els 2 algoritmes aproximats ocuparien la major part del projecte, la utilització d'una eina com MATLAB ha accelerat molt el seu disseny. Aquest factor ha causat els principals canvis respecte de la planificació inicial, tot i l'augment de treball associat a afegir feina addicional al tema inicial del projecte.

La principal dificultat ha estat l'adquisició inicial de suficients coneixements per entendre el model amb el que s'ha treballat, i l'elecció de les millors alternatives per aconseguir una implementació eficient.

A més, les consultes bibliogràfiques s'han anat allargant al llarg de tot el projecte. Això és degut a la riquesa de fenomenologia d'aquest camp, tot i

que amb les referències consultades inicialment es podria haver realitzat el projecte completament.

Malhauradament les tasques de documentació s'han acumulat al final, abandonant així la saludable pràctica de treballar-hi durant tot el desenvolupament del projecte.

6.2 Valoració econòmica

El projecte realitzat té una clara orientació acadèmica. És aleshores una mica més complicat fer una avaluació econòmica clara del cost i rendiment, ja que p.ex. el concepte de producte no hi és present. Es tracta d'un treball d'investigació on els elements produïts no tenen una aplicació concreta de la qual una empresa en pogués treure beneficis.

De totes maneres, la utilització de recursos i el temps emprat poden ser avaluats fàcilment. El caràcter teòric d'aquest projecte fa que la gran majoria dels recursos utilitzats siguin de *software*. La implementació s'ha realitzat en un PC de taula.

Les principals eines que s'han fet servir pel desenvolupament del projecte són:

1. *Software*

- MATLAB.
- Compilador *Intel* per a les aplicacions programades en *C*,

6.2. VALORACIÓ ECONÒMICA

- Intel math kernel library.

2. *Hardware*

- Processador Intel P4 per al desenvolupament dels algoritmes en MATLAB i en *C*.

Per al software *Intel* s'han fet servir llicències de desenvolupament de software no comercial. Aquestes llicències es distribueixen de manera gratuïta a programadors sobre plataforma Linux. Per fer l'estimació econòmica real es pot fer servir el preu del mateix producte pel cas de desenvolupament de software comercial. El cost de la llicència (tant pel cas de Linux com Windows) per al compilador de *C* es de \$399. El cost de la llibreria matemàtica és també de \$399.

Pel desenvolupament inicial dels algoritmes s'ha fet servir la plataforma MATLAB. Aquest software es distribueix amb llicència per estudiants al preu de \$99, tant en la versió per Windows com en la versió per Linux.

Respecte a la resta d'utilitats, les eines i llibreries emprades són de lliure distribució:

- TAUCS i SparseLib, per a la implementació de l'algoritme de diagonalització exacta fent servir matrius disperses.
- Entorn de desenvolupament \LaTeX per redactar la documentació.

Per tenir una estimació del preu del temps dedicat al projecte, tenint en consideració les condicions acadèmiques del mateix, podem fer servir dues

CAPÍTOL 6. CONSIDERACIONS FINALS SOBRE EL PROJECTE

aproximacions. La primera es basa en la quantitat d'hores dedicades i el preu aproximat que es pot pagar a un analista-programador. L'altra, que sembla més ajustada, correspon a assimilar aquesta feina a un projecte, i tenir en compte el cost que pot tenir per a un grup d'investigació tenir una persona dedicada a aquesta feina. En aquestes condicions els sous s'ajusten a l'estàndard d'investigador. Suposant que el sou mensual assignat a un investigador (en qualitat de becari) pot ser aproximadament 1000 euros, considerant el temps de desenvolupament del projecte, tenim un cost de 5000 euros corresponent a la persona contractada.

Finalment també hem de considerar el preu de la principal matèria prima d'aquest projecte: els articles científics. En algunes institucions com la UPC es disposa de subscripcions a revistes científiques especialitzades, però per estimar el cost aproximat podem fer servir el preu de cada article referenciat. La principal revista consultada en aquest projecte és el *Physical Review Letters* de la *American Physical Society*. El preu de cada article és de \$23. Mirant la bibliografia d'aquest projecte veiem que s'han realitzat consultes a un total d'uns 20 articles d'aquesta publicació. El caràcter especialitzat d'aquesta revista fa que el seu accés sigui complicat per altres mitjans, a diferència de la resta de material bibliogràfic del projecte que degut a ser d'interés més general pot trobar-se amb facilitat a moltes biblioteques.

Amb aquesta informació podem estimar el cost total del projecte

6.3. AMPLIACIÓ BIBLIOGRÀFICA

Concepte	Preu(euros)
Matlab	81,57
Intel C compiler	328,77
Intel MKL	328,77
Ordinador Intel P4	700
Programador	5000
Articles	460
	6899,12

6.3 Ampliació bibliogràfica

Per a la part corresponent als mètodes numèrics fets servir el “Matrix Computations” de Golub i van Loan [GvL96] és el més complet. La documentació de la llibreria LAPACK és també un referent per conèixer les rutines que ofereix.

Per la part més física del projecte és molt recomanable el vol.3 del curs de Física d’en Richard Feynman [FLS71]. Una introducció històrica a l’evolució de la teoria es pot trobar a la “Biografia de la física” de G. Gamow [Gam71]. A més, d’aquest mateix autor tenim “El breviario del señor Tompkins” [Gam85] que, tot i estar allunyat de l’entorn més acadèmic, ofereix una bona il·lustració de moltes d’aquestes noves idees.

Malauradament existeixen poques referències sobre el tema de la computació i la informació quàntica. Un bon començament pot ser “Ultimate zero and one”, de Colin P. Williams i Scott H. Clearwater [WC00], que presenta amb claredat els principals conceptes i resultats de la computació quàntica. El text de referència d’aquest camp és “Quantum Computation and

Quantum Information”, de Michael A. Nielsen i Isaac L. Chuang [NC00].

La majoria d’articles científics utilitzats en aquest projecte es troben publicats en repositoris científics de la xarxa, com l’*Arxiv* (<http://arxiv.org>). La millor introducció als algorismes d’aproximació com el DMRG pot ser l’article de U.Schöllwock [Sch05], on es presenta amb detall juntament amb algunes variants.

6.4 Conclusions

Per acabar podrien resultar útils algunes reflexions sobre el desenvolupament d’aquest projecte. Es tracta d’un tipus de projecte que inclou coneixements de camps diversos. S’hi fan servir coneixements de Física, Matemàtiques (especialment d’Àlgebra) i d’Informàtica. D’aquesta última s’hi utilitzen conceptes d’algorísmia i de mètodes numèrics. Cal dir que tot i que inicialment la gran quantitat de material necessari per desenvolupar el projecte podria semblar conceptualment dispersa, al llarg del treball s’ha vist que està profundament relacionada, i que els mateixos conceptes anaven apareixent un i altre cop en contextos diferents.

L’elecció d’un projecte d’aquestes característiques obliga a revisar alguns conceptes que tot i que durant tota la carrera d’Enginyeria Informàtica són contínuament presents, sempre són tractats des de un mateix punt de vista. P.ex. el concepte de màquina de Turing: qüestions tan immediates com *com es construeix?* porten a respostes tan sorprenents com les apun-

6.4. CONCLUSIONS

tades al llarg del projecte. Altres idees sobre la difusió de la calor al llarg del procés computacional també porten a conclusions sorprenents, sovint omeses.

Tot i que el camp de la Computació Quàntica és relativament jove (es pot considerar iniciat als anys 80) existeixen gran quantitat de treballs sobre les aplicacions teòriques (aquí n'hem vist només unes quantes) així com sobre la factibilitat de la realització experimental. Ja hem vist que existeixen realitzacions experimentals d'algunes portes lògiques quàntiques [SKHR⁺03], així mateix la transmissió a llarga distància fent servir principis d'informació quàntica és ja una realitat comercial. Es tracta per tant d'un camp viu, del que els enginyers informàtics n'haurien de ser conscients. Tot i que la informàtica convencional segueix sent una increïble font de resultats, la nova perspectiva quàntica ha de ser per força un referent.

Finalment, ha estat molt estimulant treballar en un tema de vanguardia científica. Durant la realització del projecte han aparegut nous articles continuant els treballs que aquí s'han desenvolupat. A més, ha existit la possibilitat de mantenir converses amb els principals impulsors d'aquests algorismes, com J.I.Cirac, D.Porrás o J.J.Garcia Ripoll. En un entorn així es fàcil sentir-se estimulat per ampliar els coneixements i seguir amb interès qualsevol novetat que hi estigui relacionada.

CAPÍTOL 6. CONSIDERACIONS FINALS SOBRE EL PROJECTE

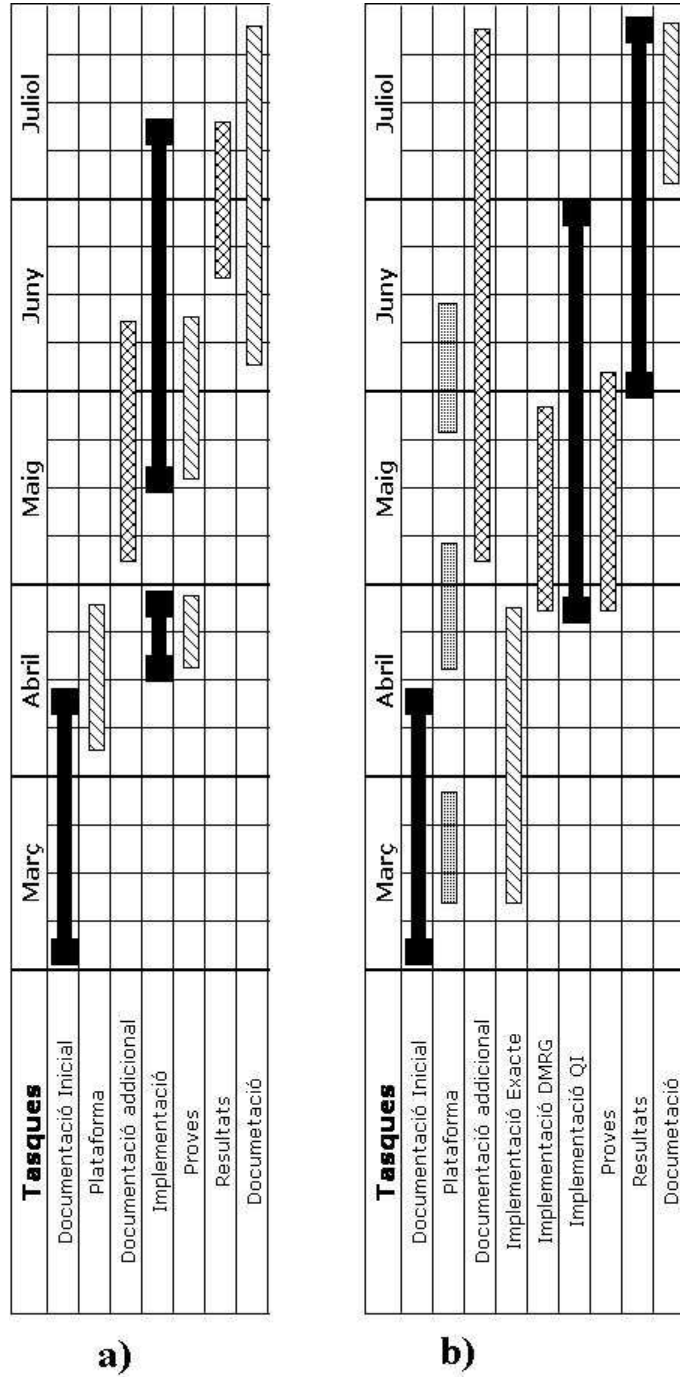


Figura 6.1: Diagrames de Gantt de la planificació inicial(a) i final (b) de les diferents tasques del projecte.

Apèndix A

Mecànica quàntica

“A new scientific truth does not triumph by convincing its opponents, but rather because its opponents die, and a new generation grows up that is familiar with it.”

Max Planck

A finals del segle XIX un conjunt d'experiments, inicialment sense cap relació, van mostrar nous fenòmens físics per als que la Física d'aquell moment no tenia cap explicació. La radioactivitat, l'aparició de càrrega elèctrica als materials atravesats per la llum, o l'aparició de llum en tubs de gas on s'aplicava un voltatge són alguns d'aquests fenòmens.

La descripció que aleshores es feia de la matèria es basava en principis fonamentals establerts al llarg del segle XIX on p.ex. l'àtom de Dalton era la unitat indivisible de matèria, i la taula periòdica de Mendelejev no tenia una base teòrica.

La culminació de tots aquests descobriments és potser la descoberta de l'electró, feta per Thompson del laboratori Cavendish de Cambridge. Combinats amb altres experiments, els seus resultats demostren la reduïda massa de la nova partícula descoberta. A més, aquesta partícula posseeix càrrega elèctrica. Immediatament es proposa un model d'àtom on aquest és format per partícules amb càrrega negativa (els nous electrons) envoltades per una gran càrrega positiva. Els intents de fer servir aquest model primigeni d'àtom (ara ja compost de partícules més fonamentals) per explicar fenòmens com les línies espectrals d'alguns gasos no donen bons resultats.

Posteriorment els experiments de Rutherford de bombardeig amb partícules demostren que de fet la càrrega positiva de l'àtom es troba concentrada al nucli i està envoltada pels electrons que hi orbiten al voltant. Apareix doncs el model actual (conceptual) de l'àtom. A mesura que els resultats experimentals donen forma a l'estructura de l'àtom, des del punt de vista teòric comencen a aparèixer greus dificultats per acceptar com a vàlid aquest model. La inestabilitat energètica d'aquest model n'és la principal, ja que segons la teoria electromagnètica els electrons anirien perdent l'energia que els fa orbitar fins a caure al nucli.

Paral·lelament al desenvolupament de la teoria de l'àtom, i per un camí molt diferent i purament teòric, apareixen algunes contradiccions sobre la descripció del comportament energètic de sistemes en equilibri entre matèria i energia. S'estudia amb profunditat el problema del cos negre, on un cos absorbeix tota la radiació que li arriba, i l'emet després en un espectre dependent

A.1. QUANTITZACIÓ

de la seva temperatura. L'anomenada crisi de l'ultraviolat, segons la qual el cos negre hauria d'emetre una gran quantitat de radiació d'aquest tipus és resolta amb una solució que obriria les portes a la nova teoria quàntica.

El terme Física Clàssica es refereix al conjunt de teories anteriors a l'aparició de la teoria de la Relativitat i la Mecànica Quàntica, les dues grans teories del segle XX. A partir d'ara aquesta distinció serà important per la gran diferència en els conceptes i en els resultats entre la física anterior a aquestes dues teories i a les seves conseqüències.

A.1 Quantització

La Física del segle XIX representa la culminació dels treballs teòrics en branques tan distants com l'Electromagnetisme o la Termodinàmica. Malgrat això alguns problemes es mostren intractables per aquestes dues potents teories. Un està relacionat amb la velocitat constant de la llum en tots els sistemes de referència: la seva solució, proposada per Albert Einstein l'any 1905 dóna lloc a la teoria de la Relativitat. L'altre problema és l'explicació teòrica de l'espectre del cos negre.

El cos negre és el model físic d'un cos que absorbeix tota la radiació que li arriba. Com aquest cos es va escalfant, comença a emetre radiació. Aquesta radiació té un espectre (figura A.1) que ni la teoria estadística de Boltzmann, ni la mecànica de Newton, ni les distribucions de Maxwell, que havien donat bons resultats per problemes similars amb gasos, podien explicar. De fet, els

resultats teòrics predeien una majoria de radiació d'alta energia (amb longitud d'ona curta). L'any 1900, a la reunió de Nadal de la societat Germànica

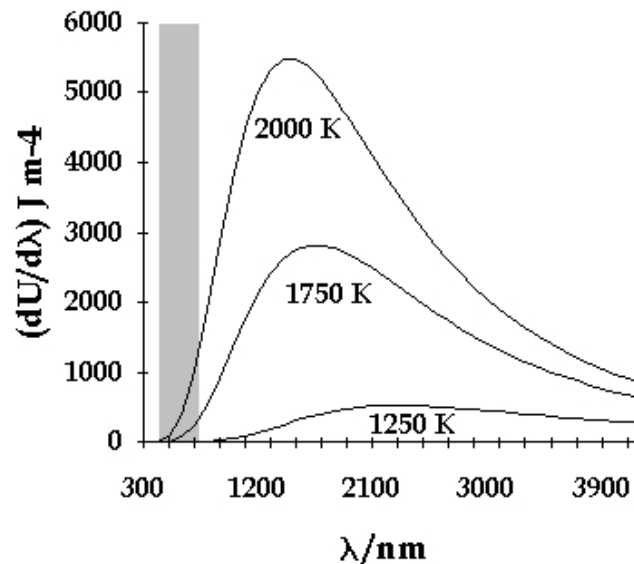


Figura A.1: Espectre de radiació del cos negre.

de física, el físic alemany Max Planck va proposar una nova teoria que resol·lia el problema de la radiació del cos negre. El punt més important era la quantització dels paquets de radiació (*quanta*). Apareixia en el seu argument una constant d'acció anomenada h , des de aleshores anomenada constant de Planck, que dominarà tota la teoria quàntica.

Com a solució al problema de les òrbites dels electrons (la seva pèrdua d'energia al llarg de l'òrbita al voltant del nucli, en dramàtica contradicció amb la realitat!), es proposa un sistema atòmic on les òrbites dels electrons estan quantitzades a través del seu moment angular. Niels Bohr, el pare

A.2. LA DOBLE ESCLETXA

d'aquesta nova visió de l'àtom, aconseguim per fi una explicació de l'espectre dels elements a més de resoldre l'estabilitat energètica de l'àtom. La quantització de les òrbites dels electrons, a través del seu moment angular, és postulada com

$$L = h \cdot \frac{n}{2\pi},$$

on h torna a ser la constant de Planck.

A.2 La doble escletxa

Potser l'experiment que il·lustra més clarament les estranyes característiques de la nova Mecànica Quàntica és el conegut com de la doble escletxa. Es disparen bales contra una pantalla separada de la font per una paret amb dues escletxes (figura A.2). Tal i com es representa, el resultat a la pantalla és la distribució que resulta de suposar que la bala passa per una de les escletxes o per l'altra. Si es tapa una de les escletxes, la distribució a la pantalla correspon a la distribució d'una única escletxa, una de les components de la distribució total.

Si repetim el mateix experiment però “disparant” ones (p.ex. ones en la superfície de l'aigua) obtenim un resultat característic de la descripció ondulatòria: apareixen fenòmens d'interferència entre els fronts d'ona provinents de les dues obertures a la paret (figura A.3).

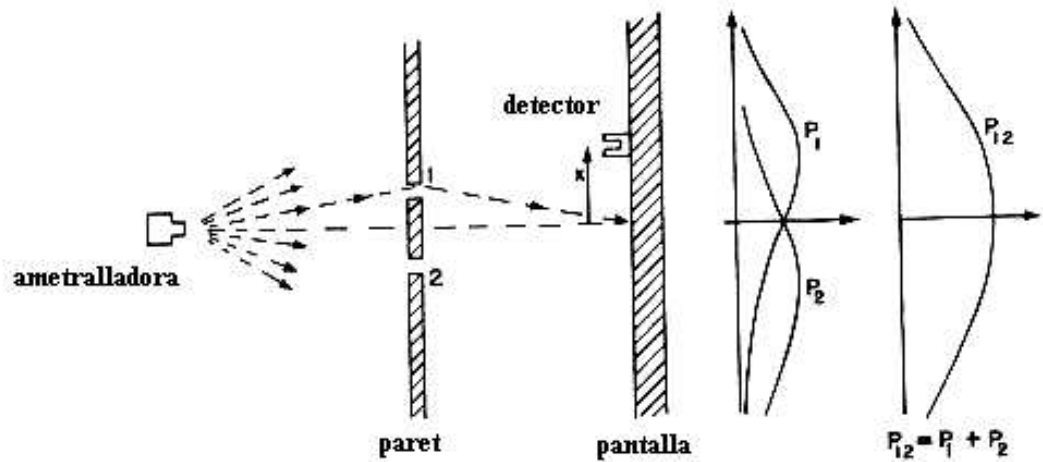


Figura A.2: Resultat de l'experiment realitzat amb bales

Que passa si enlloc de realitzar l'experiment amb bales o amb ones el realitzem amb electrons? En aquestes condicions es manifesta una propietat de la matèria, purament quàntica, que per ser explicada requereix d'una imatge ondulatoria del seu comportament. Els electrons, en arribar a la pantalla (en ser mesurats) es comporten com una partícula. En el seu recorregut fins a la pantalla es comporten com una ona. Aquest comportament ondulatori s'associa a la probabilitat de trobar a un electró a un punt de la pantalla. La funció de probabilitat descriu un patró similar al de les interferències de les ones en arribar-hi: apareixen interferències que produeixen una probabilitat $= 0$ de trobar l'electró en alguns punts, en oposició a la imatge corpuscular on en cap punt s'hi produïa aquest fenomen.

Aquest comportament dual de les partícules es coneix com *dualitat ona-*

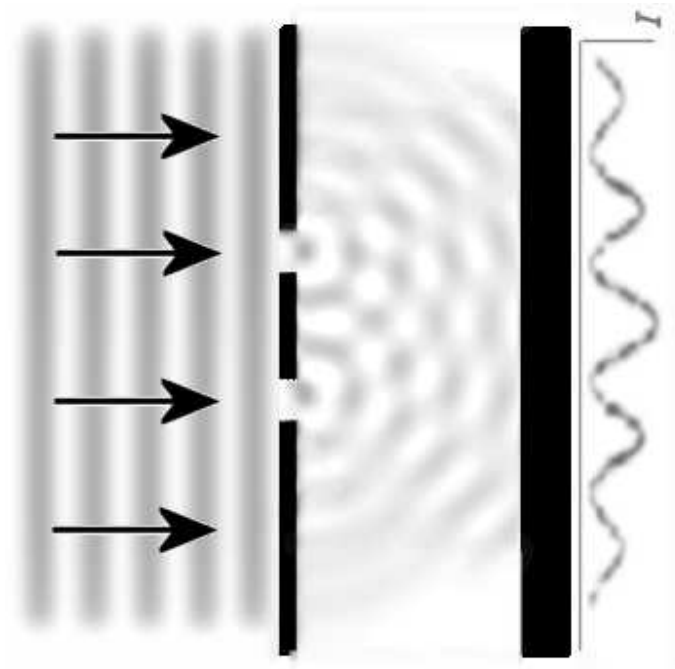


Figura A.3: Resultat de l'experiment realitzat amb ones

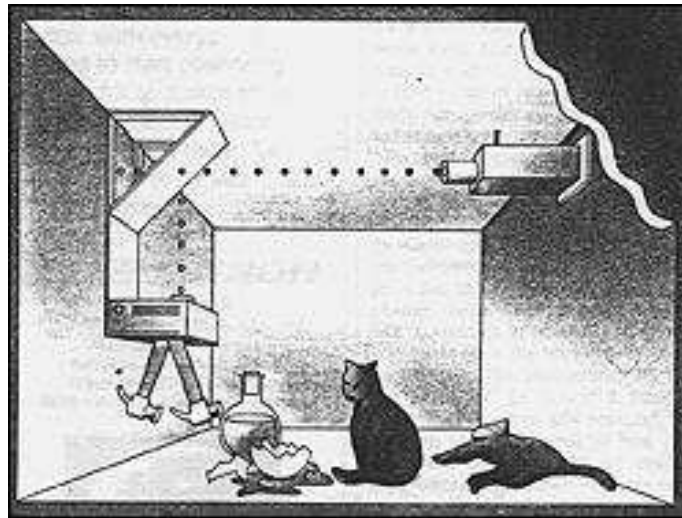
corpúscle, postulat per Louis DeBroglie.

Així, podem explicar el comportament dels electrons en l'experiment amb una descripció ondulatoria. Hem d'admetre doncs que per que apareguin les interferències l'ona associada a l'electró *passi pels dos forats alhora*. Qualsevol intent de determinar (mesurar) per quin forat passa l'electró, o si durant l'experiment tapem una de les dues escletxes, resulta en que les franges d'interferència desapareixen a la pantalla. La interacció entre els electrons i qualsevol dispositiu de mesura fa manifestar la seva propietat corpuscular, no ondulatoria.

Així els electrons evolucionen com a ones, amb fenòmens associats d'in-

terferència i difracció, fins a que es realitza una mesura (p.ex. de la seva posició o moment) on es passen a comportar com a partícules.

A.3 El gat de Schrödinger



La paradoxa proposada per Erwin Schrödinger l'any 1935 s'utilitza per explicar l'extranya relació entre el món microscòpic descrit per la mecànica quàntica i el món macroscòpic que percebem.

Suposem un mostra radioactiva connectada a un detector. Si es produeix una emissió de radiació de la mostra el detector activa un dispositiu que mou un martell. Aquest, un cop activat, trenca una ampolla plena de verí. Tots aquests elements, juntament amb un gat, es tanquen dins d'una caixa. Així, si la mostra activa el martell el gat mor enverinat.

Deixant tots els elements tancats, sense interactuar amb l'exterior, comencem

A.4. SPIN $\frac{1}{2}$

un experiment: la mostra de l'isòtop radioactiu té una probabilitat d'emetre en la següent hora igual a 0.5. Així, tancat a la caixa, el gat té una probabilitat de viure al cap d'una hora equivalent a 0.5. Ara bé, com no realitzem cap mesura sobre la mostra radioactiva durant una hora, tenim un estat superposició de l'estat en que l'isòtop emet i l'estat en que no ho fa. Després d'una hora, abans d'obrir la caixa tenim un estat superposició de dos estats macroscòpics: en un el gat és viu; en l'altre és enverinat i mor!

Aquesta manifestació quàntica a gran escala s'ha intentat reproduir en dispositius anomenats SQUIDS [Leg92], on s'intenten crear estats superposició de corrents en sentits inversos. Tot i que els resultats no semblen clars, la dificultat de mantenir aïllat un sistema de l'exterior (al cap i a la fi els elements de la caixa interaccionen amb les seves parets) sembla impedir la realització d'un experiment com aquest. Aquesta és també la principal dificultat associada amb la realització d'un computador quàntic ja que qualsevol interacció del sistema amb l'entorn pot crear distorsions (decoherencia) en els càlculs.

A.4 Spin $\frac{1}{2}$

En analitzar experimentalment el pas d'un feix d'àtoms de plata per un camp magnètic, els físics esperaven ja algun comportament quantitzat seguint els experiments dels anys anteriors. Era d'esperar que si els àtoms tenien algun moment magnètic aquest seria quantitzat i per tant, en interactuar

amb un camp extern es trobessin només alguns valors acceptats per a les desviacions de les trajectòries del electrons. Clàssicament, com el moment de cada àtom estaria orientat a l'atzar no caldria esperar cap pauta en la mesura. L'experiment de Stern-Gerlach mostrava però només dos possibles valors del

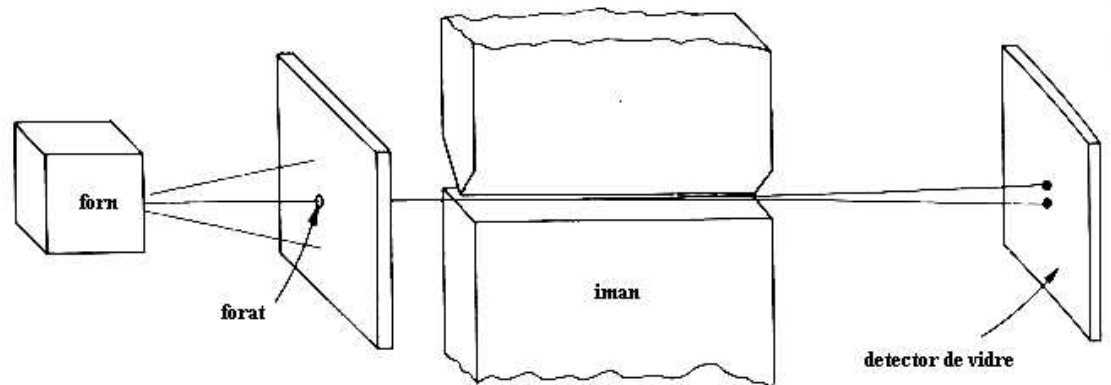


Figura A.4: L'experiment de Stern-Gerlach.

moment magnètic dels electrons en mesurar el seu moment magnètic. A les partícules amb el moment orientat cap amunt l'imant les desviava en sentit contrari a les que el tenien orientat cap avall.

Aquest comportament s'associa amb un moment angular intrínsec de les partícules desviades. Se'ls hi associa un moment angular intrínsec (*spin*) igual a $\frac{1}{2}$. Partícules amb aquest comportament són les que hem emprat al llarg del projecte per formar les cadenes de partícules, i que es poden fer servir -degut a la seva descripció amb una base de dos estats discrets- per codificar un *qubit*.

A.5 Notació

La notació utilitzada actualment correspon a la desenvolupada pel físic P.A.M.Dirac.

Els elements principals d'aquesta notació són:

- Els estats d'un sistema quàntic es descriuen com vectors d'un espai de Hilbert. Aquests vectors $|n\rangle$ i les seves combinacions lineals són estats permesos al sistema.
- Si tenim un sistema descrit per

$$|\psi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \dots + \alpha_n|n\rangle, \quad (\text{A.1})$$

es verifica

$$\sum_{i=1}^n |\alpha_i|^2 = 1, \quad (\text{A.2})$$

on els α_i són nombres complexos.

- A tota magnitud mesurable li correspon un operador autoadjunt A .

Aquesta notació s'extèn fàcilment al cas de conjunt de més d'un partícula.

Per exemple per l'estat format per dues partícules escrivim

$$|\psi\rangle = \alpha_{00}|0, 0\rangle + \alpha_{11}|1, 1\rangle + \alpha_{01}|0, 1\rangle + \alpha_{10}|1, 0\rangle.$$

A.5.1 Mesura

Segons els postulats que defineixen el comportament quàntic, en mesurar una magnitud sobre un sistema només podem trobar com a resultats alguns valors. Aquests valors permesos en realitzar la mesura corresponen als autovalors de l'operador que volem mesurar. Per això és tan important disposar de bons mètodes de diagonalització en treballar amb sistemes on aquests operadors, descrits per matrius, són molt grans com en el cas de sistemes formats per moltes partícules que hem estudiat en aquest projecte.

Si suposem una magnitud observable, podem expressar un estat en la base d'estats propis d'aquest operador

$$|\psi\rangle = \sum_i \alpha_i |a_i\rangle,$$

on $|a_i\rangle$ és la base de l'operador A . El resultat de la mesura de l'operador A és un dels autovalors de A , amb una probabilitat

$$P_{A,|\psi\rangle}(a_i) = |\langle a_i|\psi\rangle|^2,$$

on $\langle x|y\rangle$ és el producte escalar dels vectors de l'espai de Hilbert $|x\rangle$ i $|y\rangle$.

A.5.2 Matriu densitat

En la descripció d'alguns sistemes quàntics ens pot ser d'utilitat utilitzar l'operador matriu densitat. Suposem un sistema que està format amb proba-

A.5. NOTACIÓ

bilitat P_1 per l'estat $|\psi_1\rangle$, amb probabilitat P_2 per l'estat $|\psi_2\rangle$... de manera que es verifica

$$\sum_i P_i = 1,$$

aleshores definim la matriu densitat com

$$\rho = \sum_i P_i |\psi_i\rangle\langle\psi_i|.$$

Suposem un sistema pur de 2 estats (un *qubit*). Si l'estat és pur, només tenim $P_1 = 1$. Amb l'estat

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

obtenim la matriu densitat

$$\rho = |\psi_1\rangle\langle\psi_1| = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Si disposem de la matriu densitat d'un sistema podem obtenir informació de la seva composició a partir de la descomposició espectral d'aquesta matriu. Els autovectors obtinguts corresponen als estats que el formen amb probabilitat igual a l'autovalor corresponent. Així, els autovectors amb autovalors més grans corresponen als estats amb més probabilitat.

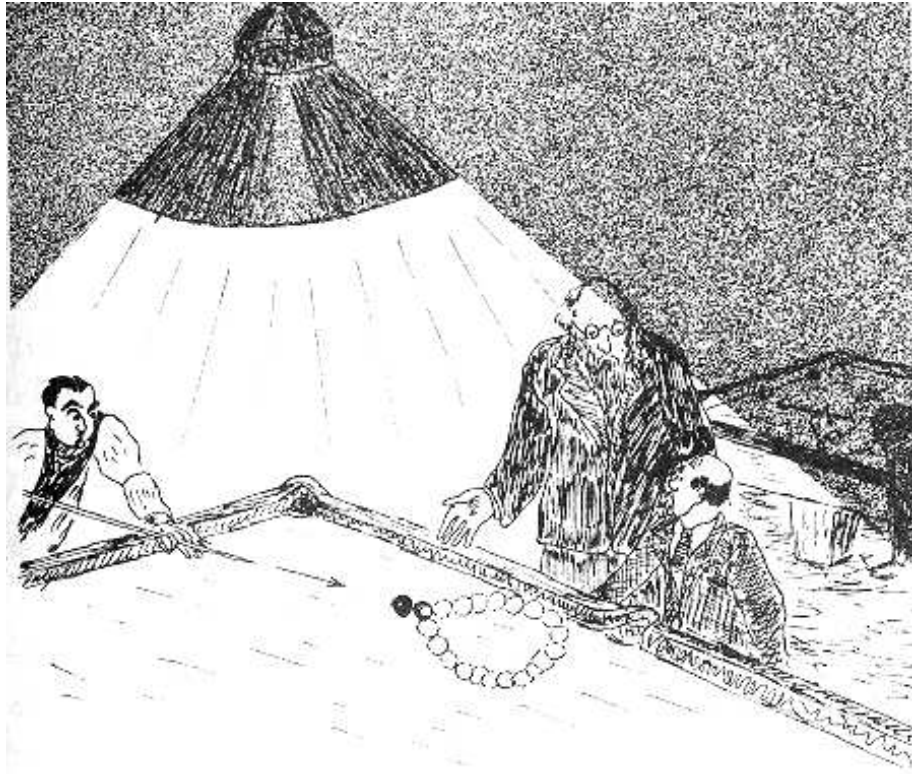


Figura A.5: “(...)había en el fondo una sala de billar, llena de hombres en mangas de camisa que jugaban en la mesa central. Se acercó a la mesa y empezó a mirar la partida. ¡Pero sucedía algo muy extraño! Un jugador puso una bola en la mesa y le dió con el taco. Al mirarla rodar, el señor Tompkins advirtió con gran sorpresa que la bola empezaba a “desplazarse”. No podía describir con otra palabra el extraño comportamiento de la bola, la cual, mientras recorría el tapete verde, se veía cada vez más desleída y perdía sus límites claros.” [Gam85]

Apèndix B

Codi C de l'algoritme del capítol 5 pel model d'Ising

*“Should array indices start at 0 or 1?
My compromise of 0.5 was rejected without, I thought,
proper consideration.”*

Stan Kelly-Bootle

S'inclou aquí una part del codi desenvolupat al llarg del projecte, corresponent a l'algoritme del capítol 5 per al model d'Ising.

```
#include "Ising1D.hpp"  
  
void fill(double* mat, int s){  
    for(int i = 0; i < s*s; i++)  
        mat[i] = 0;  
}  
  
void loadI(double* mat, int s){
```

```

    fill(mat, s);
    for(int i = 0; i < s; i++)
        mat[i*s+i] = 1;
}

void initValues(){
    srand(time(NULL));
    pos = 0;
    clw = true;
    conv = LIMIT_CONV-1;
}

void init(){
    double tmp;
    for(int i = 0; i < S; i++){
        b[i] = (double*) malloc(D*D*sizeof(double));
    }
    normB();
    for(int i = 0; i < N; i++){
        u[i] = (double*) malloc(D*D*D*sizeof(double));
        v[i] = (double*) malloc(D*D*D*sizeof(double));
    }
    for(int i = 0; i < N; i++){
        consE1(u[i]);
        consEz(v[i]);
    }
}

//general transposition operation
void transpose(double* in, double* out){
    double tmp;
    for(int i = 0; i < D; i++)
        for(int j = 0; j < D; j++)
            for(int k = 0; k < D; k++)
                for(int l = 0; l < D; l++)
                    out[(l*D+j)*D*D+k*D+i] = in[(i*D+j)*D*D+k*D+l];
}

void consE1(double* out){

```

```

fill(out,D*D);
double* c = (double*) malloc(D*D*D*D*sizeof(double));
for(int i = 0; i < S; i++){
    BxB(b[i], b[i], c, D);
    for(int j = 0; j < D*D*D*D; j++)
        out[j] += c[j];
    }
}

```

```

void consEz(double* out){
    fill(out,D*D);
    BxB(b[1], b[1], out, D);
    double* c = (double*) malloc(D*D*D*D*sizeof(double));
    for(int i = 0; i < 1; i++){
        BxB(b[i], b[i], c, D);
        for(int j = 0; j < D*D*D*D; j++)
            out[j] -= c[j];
        }
    }
}

```

```

void BxI(double* in, double* out, int s){
    fill(out,S*s);
    for(int i = 0; i < S; i++)
        for(int l = 0; l < s; l++)
            for(int k = 0; k < s; k++)
                out[i*S*s*s+i*s+k*s*S+l]=in[k*s+l];
    }
}

```

```

void Bx_I(double* in, double* out, int s){
    fill(out,S*s);
    for(int l = 0; l < s; l++)
        for(int k = 0; k < s; k++)
            out[k*s*S+l]=-in[k*s+l];
    for(int l = 0; l < s; l++)
        for(int k = 0; k < s; k++)
            out[S*s*s+s+k*s*S+l]=in[k*s+l];
    }
}

```

```

void BxB(double* in1, double* in2, double* out, int s){
    for(int j = 0; j < s; j++)
        for(int i = 0; i < s; i++)
            for(int l = 0; l < s; l++)
                for(int k = 0; k < s; k++)
                    out[i*s*s*s+j*s+k*s*s+l]=in1[l*s+k]*in2[i*s+j];
}

void eigen(){
    consH();
    consN();
    char JOBVL = 'N';
    char JOBVR = 'V';
    long NN = S*D*D;
    double* alphas = (double*) malloc(NN*sizeof(double));
    double* alphas_i = (double*) malloc(NN*sizeof(double));
    double* beta = (double*) malloc(NN*sizeof(double));
    long LDVL=NN;
    double* vl;
    long LDVR=NN;
    double* vr = (double*) malloc(S*NN*NN*sizeof(double));
    long LWORK = 20*NN;
    double* work = (double*) malloc(LWORK*sizeof(double));
    long INFO;
    dggev_(&JOBVL,&JOBVR,&NN,Hm,&NN,Nm,&NN, alphas , alphas_i , beta ,
        vl ,&LDVL, vr ,&LDVL, work ,&LWORK,&INFO);
    if (INFO!=0)
        cerr<<"Eigenproblem fails!"<<endl;
    double min = alphas[0]/beta[0];
    double curr;
    int sel = 0;
    for(int i = 1; i < NN; i++){
        curr = alphas[i]/beta[i];
        if (curr<min) {
            sel = i;
            min = curr;
        }
    }
    cout<<"Eo: " << alphas[sel]/beta[sel] << " " << alphas[sel]

```

```

    <<'_'<<alpha[ sel]<<'_'<<beta[ sel]<<endl;
    for (int i = 0; i < S; i++){
        for (int j = 0; j < D*D; j++){
            b[i][j] = vr[ sel*S*D*D+j+i*D*D];
        }
    }
    normB();
    consE1(u[pos]);
    consEz(v[pos]);
    updConv( alphas[ sel]/beta[ sel]);
}

void joinB(){
    for(int i = 0; i < D; i++){
        for(int j = 0; j < D; j++){
            BX[j+i*D*S] = b[0][j+i*D];
            BX[j+i*D*S+D] = b[1][j+i*D];
        }
    }
}

void sepB(){
    for(int i = 0; i < D; i++){
        for(int j = 0; j < D; j++){
            b[0][j+i*D] = BX[i*S*D+j];
            for(int j = 0; j < D; j++){
                b[1][j+i*D] = BX[i*S*D+j+D];
            }
        }
    }
}

double updConv(double nw){
    conv = sEigValue - nw;
    sEigValue = nw;
}

int main(){

    initValues();
    init();
    while(conv < TOL){
        if(cw){

```

```
eigen ();  
actC ();  
pos++;  
if (pos == N-1) clw = false;  
}  
else {  
    eigen ();  
    actCounter ();  
    pos--;  
    if (pos == 0) clw = true;  
}  
}
```

```
free (r);  
free (s);  
free (t);  
free (h);  
free (e1);  
free (ez);  
free (b);  
free (Nm);  
free (No);  
free (Hm);  
free (Ho);  
exit (0);  
}
```


Bibliografia

- [AKLT87] Ian Affleck, Tom Kennedy, Elliot H. Lieb, and Hal Tasaki. Thermodynamic limit of density matrix renormalization. *Phys. Rev. Lett.*, 59:799, 1987.
- [BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.
- [BBBV96] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 1996.
- [Ben82] Paul Benioff. Quantum mechanical models of Turing machines that dissipate no energy. *Phys. Rev. Lett.*, 48:1581, 1982.
- [Bet31] Hans Bethe. Zur theorie der metalle. Eigenwerte und Eigenfunktionen der linearen Atomkette. *Z. Phys.*, 71:205, 1931.
- [CZ95] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, 74:4091–4094, 1995.
- [EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev. Lett.*, 47:777, 1935.
- [Fey] R. P. Feynman. There’s plenty of room at the bottom. December 29th 1959 at the annual meeting of the American Physical Society at the California Institute of Technology (Caltech).
- [Fey82] R. P. Feynman. Simulating physics with computers. *Int. Journal of theoretical physics*, 21:467, 1982.

-
- [FLS71] Richard P. Feynman, Robert B. Leighton, and Matthew Sands. *The Feynman lectures on physics*. Addison-Wesley, 1971.
- [Gam71] George Gamow. *Biografía de la Física*. Salvat, 1971.
- [Gam85] George Gamow. *El breviario del señor Tompkins*. Fondo de cultura económica, 1985.
- [Gro96] Lev Grover. A fast quantum mechanical algorithm for database search. *Proceedings, 28th Annual ACM Symposium on the Theory of Computing*, pages 212–219, 1996.
- [GvL96] Gene H. Golub and Charles F. van Loan. *Matrix Computations*. Johns Hopkins University Press, 1996.
- [GY00] Gene H. Golub and Qiang Ye. *An inverse free preconditioned Krylov subspace method for symmetric generalized eigenvalue problems*. 2000.
- [Kar72] R. M. Karp. *Reducibility among combinatorial problems*. Plenum Press, 1972.
- [Lan61] R. Landauer. Irreversibility and heat generation in the computing process. *IBM journal of research and development*, 5(3), 1961.
- [Leg92] A.J. Leggett. *Quantum Tunneling in Condensed Media*. Elsevier Science, 1992.
- [MC91] D. Medeiros and G.G. Cabrera. Lanczos calculation for the $s = \frac{1}{2}$ antiferromagnetic Heisenberg chain up to $n = 28$ spins. *Phys. Rev. B*, 43:3703, 1991.
- [Moo65] Gordon E. Moore. Cramming more components onto integrated circuits. *Electronics*, 38(8), 1965.
- [NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [OR95] Stellan Ostlund and Stefan Rommer. Thermodynamic limit of density matrix renormalization. *Phys. Rev. Lett.*, 75:3537, 1995.

BIBLIOGRAFIA

- [Pap94] C. H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.
- [Par80] Beresford N. Parlett. *The symmetric eigenvalue problem*. Prentice-Hall, 1980.
- [PRL96] Roldan Pozo, Karin A. Remington, and Andrew Lumsdaine. *SparseLib++ v.1.5*. 1996.
- [RO97] Stefan Rommer and Stellan Ostlund. Class of ansatz wave functions for one-dimensional spin systems and their relation to the density matrix renormalization group. *Phys. Rev. B*, 55:2164, 1997.
- [Sch05] U. Schollwöck. The density-matrix renormalization group. *Rev. Mod. Phys.*, 77:259, 2005.
- [Sho97] Peter W. Shor. Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. on Computing*, 26:1484 – 1509, 1997.
- [SKHR⁺03] F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G. P. T. Lancaster, T. Deuschle, C. Becher, C. F. Roos, J. Eschner, and R. Blatt. Realization of the Cirac - Zoller controlled-NOT quantum gate. *Nature*, 422:408–411, 2003.
- [S.R92a] S.R.White. Density-matrix algorithms for quantum renormalization groups. *Phys. Rev. B*, 48:10345, 1992.
- [S.R92b] S.R.White. Density matrix formulation for quantum renormalization groups. *Phys. Rev. Lett.*, 69:2863, 1992.
- [VJEK03] G. Vidal, J.I.Latorre, E.Rico, and A. Kitaev. Entanglement in quantum critical phenomena. *Phys. Rev. Lett.*, 90:227902, 2003.
- [VPC04] F. Verstraete, D. Porras, and J. I. Cirac. Density matrix renormalization group and periodic boundary conditions: a quantum information perspective. *Phys. Rev. Lett.*, 93:227205, 2004.
- [WC00] Colin P. Williams and Scott H. Clearwater. *Ultimate zero and one*. Copernicus, 2000.

- [Wil75] K. G. Wilson. The renormalization group: critical phenomena and the Kondo problem. *Rev. Mod. Phys.*, 47:773, 1975.