UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

Treball final del grau de matemàtiques

El problema del subgrup amagat per a grups no abelians

Yaiza Aguilar Carós

Director: Dr. Artur Travesa i Grau
Barcelona, gener 2025

Abstract

The hidden subgroup problem is a theoretical formalism that encompasses several highly relevant problems, such as factorization, discrete logarithm, and graph isomorphism. While this problem can be solved for abelian groups using quantum computation in polynomial time, a general resolution for non-abelian groups has not yet been found. This work explores some results related to the potential resolution of the problem for finite non-abelian groups, as well as its limitations. We will begin by introducing the foundations of quantum mechanics, which are necessary to describe the quantum computation model. Next, we will present the basic concepts of finite group representation theory that help us construct the quantum Fourier transform, a key component in most quantum algorithms. Subsequently, we will discuss a general result on the possibility of solving the problem for arbitrary finite groups with a polynomial number of queries, although possibly requiring exponential time. Furthermore, we will analyze which non-abelian groups allow the construction of a more efficient algorithm, as well as some theorems that demonstrate the impossibility of implementing an efficient algorithm in the cases of the dihedral group and the symmetric group. Finally, we will address some potential limitations of solving the problem and reflect on its possible extension to infinite groups.

Resum

El problema del subgrup amagat és un formalisme teòric que engloba alguns problemes de gran rellevància, com el de factorització, el del logaritme discret i el d'isomorfisme de grafs. Tot i que per a grups abelians es pot resoldre aquest problema amb l'ús de computació quàntica en temps polinòmic, encara no s'ha trobat una resolució general per a grups no abelians. Aquest treball explora alguns resultats relacionats amb la possible resolució del problema per a grups finits no abelians, així com també les seves limitacions. Començarem introduint els fonaments de la mecànica quàntica, necessaris per a descriure el model de computació quàntica. A continuació, presentarem els conceptes bàsics de la teoria de representació de grups finits que ens ajuden a construir la transformada de Fourier, una peça clau en la majoria d'algoritmes quàntics. Posteriorment, exposarem un resultat general sobre la possibilitat de resoldre el problema per a grups finits qualssevol en un nombre de peticions polinòmic, malgrat poder requerir temps exponencial. A més, analitzarem quins grups no abelians permeten la construcció d'un algoritme més eficient, així com alguns teoremes que demostren la impossibilitat d'implementar un algoritme eficaç en els casos del grup diedral i del grup simètric. Finalment, abordarem algunes possibles limitacions de la resolució del problema i reflexionarem sobre la seva possible extensió als grups no finits.

2020 Mathematics Subject Classification: 11Y16, 68Q12, 20C35.

Agraïments

En primer lloc, vull donar les gràcies al Dr. Artur Travesa. Gràcies no només per haver dirigit aquest treball, sinó també per tota la seva dedicació durant tot aquest temps, per les reunions tan enriquidores en diversos aspectes i per no voler únicament que desenvolupés un bon treball de final de grau, sinó que també aprengués les eines essencials per fer una bona recerca.

En segon lloc, m'agradaria agrair als meus pares, que han fet tot el possible perquè jo pogués tenir una bona educació, tant en l'àmbit personal com acadèmic. Gràcies al meu pare, qui sempre ha intentat que desenvolupés un pensament crític sense imposar res i que m'ha ensenyat a afrontar la vida de la millor manera possible. Gràcies també a la meva mare per escoltar-me sempre i per estar-hi en tot moment. Gràcies al meu germà, pel seu suport incondicional.

També, gràcies a en Joel, la meva parella, per estar al meu costat durant aquests anys i regalar-me tants bons moments. Gràcies també a la seva família, que m'ha acollit com una més i m'ha ajudat en tot el que ha pogut.

Gràcies a tots els professors que he tingut durant la secundària, i que avui dia encara tinc presents, per tot el que em van ensenyar.

Finalment, agrair a tots els meus amics, en especial a la Lídia i l'Elena, que m'han ajudat en tot moment i han fet que aquests anys fossin una millor experiència.

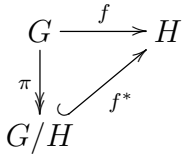
Índex

Introducció

El problema del subgrup amagat és un problema fonamental en matemàtiques i ciències computacionals. Aquest problema engloba altres problemes diversos, com el problema de factorització, el del logaritme discret, el d'isomorfisme de grafs i el de cerca del vector més proper a un vector donat en una xarxa (cf. [S-R22]). Aquests problemes no sols tenen un gran interès teòric, sinó també nombroses aplicacions en criptografia, anàlisi de dades i altres àmbits relacionats amb la ciència i la tecnologia. En alguns casos, hi ha hagut un avenç en la resolució del problema del subgrup amagat gràcies al nou paradigma de la computació quàntica.

En tot el treball, llevat de l'últim capítol, pressuposarem que el grup donat és finit i que treballem amb l'operació donada per aquest grup. Denotem l'element neutre com 1_G.

Siguin G un grup, $H \subseteq G$ un subgrup i X un conjunt; es diu que una aplicació $f : G \to X$ *separa les classes laterals* (per la dreta) de G mòdul H si $\forall g, g' \in G,\ f(g) = f(g') \iff gH = g'H$; és a dir, si f factoritza injectivament a través de la projecció en el conjunt quocient $G/H = \{gH : g \in G\}$:



Una condició equivalent a que f separi classes laterals és que $\forall g, h \in G,\ f(gh) = f(g) \iff h \in H$.

Problema (Problema del subgrup amagat)**.** Siguin G un grup, $H \subseteq G$ un subgrup, X un conjunt finit i $f : G \to X$ una aplicació que separa les classes laterals de G mòdul H. El problema del subgrup amagat consisteix a determinar un conjunt de generadors de H a partir d'avaluacions de f.

El problema del subgrup amagat es pot resoldre en alguns casos mitjançant algoritmes clàssics. Tanmateix, la complexitat de la seva resolució depèn de la naturalesa del grup i, en la majoria de casos, la solució requereix una quantitat exponencial d'avaluacions i, consegüentement, una quantitat exponencial de temps.

En canvi, en el cas quàntic, el problema es pot resoldre en temps polinòmic per a un conjunt més ampli de grups. En particular, quan el grup és abelià, la resolució es pot trobar en temps polinòmic. Aquest fet explica per què problemes com la

factorització de nombres enters o el logaritme discret podrien ser resolts mitjançant algoritmes quàntics, ja que aquests dos problemes són casos particulars del problema del subgrup amagat quan el grup G és abelià (cf. [S-R22]). Tot i això, quan G és no abelià, només s'han descobert algoritmes polinòmics en casos específics. La resolució d'aquest problema per al grup diedral, D_{2n}, permetria resoldre el problema del vector més proper en una xarxa, mentre que per al grup simètric, S_n, es podria resoldre el problema d'isomorfisme de grafs.

En aquest treball, introduirem la teoria de representació de grups finits. Aquesta teoria estudia com els elements d'un grup poden ser representats per mitjà de matrius o transformacions lineals d'un espai vectorial, mantenint la seva estructura algebraica. Els orígens de la teoria es remunten al segle XIX amb el treball de matemàtics com Évariste Galois i Arthur Cayley, els quals van estudiar les simetries i permutacions de les arrels de les equacions. El desenvolupament va continuar amb Sophus Lie, qui va introduir els grups de Lie. Va experimentar un gran avenç a principis del segle XX amb Felix Klein, Emil Artin i John von Neumann, els quals van aplicar la teoria a la física i altres camps. Durant el segle XX, matemàtics com Hermann Weyl i Jean-Pierre Serre van formalitzar i expandir la teoria, establint les bases per a la classificació de representacions irreductibles i l'anàlisi de grups finits i de Lie. La teoria de representació de grups finits ens serà útil per a definir una de les parts clau dels diversos algoritmes que resolen el problema del subgrup amagat: la transformada de Fourier.

També presentarem les bases de la mecànica quàntica, necessàries per a entendre el funcionament dels ordinadors quàntics. Alguns dels seus principis fonamentals són la superposició, que estableix que l'estat d'un sistema quàntic és una combinació lineal dels possibles estats, i l'entrellaçament, que implica que l'estat de cada partícula del grup no pot ser descrit de manera independent de les altres. Els ordinadors quàntics utilitzen aquests principis per a manipular qubits, els equivalents quàntics dels bits clàssics. Aquests ordinadors representen un nou model computacional que permet abordar problemes, com el del subgrup amagat, que requereixen més temps i recursos per als ordinadors clàssics.

L'objectiu d'aquest treball és donar una visió global del problema del subgrup amagat per a grups finits no abelians. Per tal d'abastar tota la profunditat del problema i tenint en compte la limitació d'espai, donarem només les proves dels resultats que considerem més rellevants; a les referències que anirem citant, hi ha totes les demostracions i informació addicional. Donarem un resultat general que afirma que es pot resoldre el problema del subgrup amagat per a qualsevol grup amb una quantitat de peticions polinòmica, malgrat que això no suposi que el temps també ho sigui. Demostrarem que aquesta fita es pot acurar per a alguns grups en particular i, fins i tot, per a alguns grups podem resoldre el problema en temps polinòmic. Més endavant, parlarem del cas del grup diedral i del grup simètric i donarem alguns teoremes d'impossibilitat. Per últim, plantejarem algunes reflexions i qüestions sobre la possible resolució del problema. Reflexionarem sobre alguns conceptes que poden dificultar-ne la resolució i també explorarem el cas de grups no abelians no finits.

Capítol 1

Fonaments matemàtics de la mecànica quàntica

1.1 Axiomes de la mecànica quàntica

Per a descriure com es pot arribar a resoldre el problema del subgrup amagat amb computació quàntica, primerament, cal exposar les bases de la mecànica quàntica. Es pot veure aquesta secció com un seguit de lleis que permetran, amb eines matemàtiques, modelitzar sistemes quàntics.

Recordem que *producte escalar* sobre H en un espai vectorial complex és una aplicació $\langle \cdot, \cdot \rangle : H \times H \to \mathbb{C}$ tal que per a tot $x, y, z \in H$ i tot $\lambda \in \mathbb{C}$ compleix:

i. $\langle x, y \rangle = \overline{\langle y, x \rangle}$;

ii. $\langle x, x \rangle \geq 0$, i $\langle x, x \rangle = 0$ si, i només si, $x = 0$;

iii. $\langle \alpha x + \beta z, y \rangle = \overline{\alpha} \langle x, y \rangle + \overline{\beta} \langle z, y \rangle$ i $\langle x, \alpha y + \beta z \rangle = \alpha \langle x, y \rangle + \beta \langle x, z \rangle$.

Un espai vectorial H amb un producte escalar $\langle \cdot, \cdot \rangle$ s'anomena *espai prehilbertià*. Un espai prehilbertià és un *espai de Hilbert* si és un espai normat i complet amb la norma induïda pel producte escalar (cf. [SHO09]).

A continuació, s'exposen els cinc postulats que descriuen les lleis que regeixen la modelització dels sistemes quàntics (cf. [Hall23]).

Axioma 1. L'estat d'un sistema és representat per un vector unitari ψ en un espai de Hilbert $\mathcal{H}$ apropiat. Si ψ_1 i ψ_2 són dos vectors unitaris a l'espai de Hilbert $\mathcal{H}$ amb $\psi_1 = c\psi_2$ per a alguna constant $c \in C$ aleshores, ψ_1 i ψ_2 representen el mateix estat físic. La funció ψ que defineix el sistema quàntic s'anomena *funció d'ona*.

Axioma 2. Per a cada funció f definida en l'espai de fases clàssic, la imatge de la qual pren valors o vectors reals, hi ha un operador autoadjunt $\hat{f}$ associat en l'espai quàntic de Hilbert.

Sigui X un operador. Recordem que X és un *operador hermitià* si X és autoadjunt. Anomenarem *observable* un operador hermitià associat a una magnitud que es pot mesurar en un sistema quàntic.

Notem la diferència entre f i $\hat{f}$. Per una banda, f representa el valor observat experimentalment. Aquest valor s'associa amb una magnitud física, com ara el moment o l'energia. Per altra banda, $\hat{f}$ és l'operador autoadjunt (observable) associat a la magnitud física representada per f. Aquest operador l'utilitzem per a descriure formalment el comportament quàntic d'aquesta magnitud en termes d'estats i probabilitats. De fet, més endavant, veurem que els valors propis de $\hat{f}$ són els possibles valors de f que podem observar experimentalment.

Axioma 3. Si un sistema quàntic està en un estat descrit pel vector unitari $\psi \in \mathcal{H}$, la distribució de probabilitat de la mesura de f satisfà, per a la seva esperança matemàtica, que

$$E(f^m) = \langle \psi, (\hat{f})^m \psi \rangle.$$

En particular, el valor esperat de la mesura de f ve donat per $\langle \psi, \hat{f}\psi \rangle$.

Si un sistema quàntic es troba en un estat descrit per un vector unitari $\psi \in \mathcal{H}$ i per a algun observable $\hat{f}$ tenim que $\hat{f}\psi = \lambda\psi$, per a $\lambda \in \mathbb{R}$, diem que el sistema quàntic es troba en un *estat propi*.

Proposició 1.1.1 (Valors propis)**.** *Si un sistema quàntic es troba en un estat propi aleshores,*

$$E(f^m) = \langle (\hat{f})^m \rangle_\psi = \lambda^m,$$

per a tots els valors enters possibles de m. L'única mesura de probabilitat consistent amb aquesta condició és en la qual f té el valor definit λ, amb probabilitat 1.

Demostració. El resultat de la proposició es segueix de l'axioma 3 i del fet que el sistema es troba en un estat propi, és a dir, $\hat{f}\psi = \lambda\psi$ i $\langle \psi | \psi \rangle = 1$. □

És a dir, tots els moments $E(f^m)$ coincideixen amb λ^m i, per tant, $P(f = \lambda) = 1$. Consegüentment, en mesurar un sistema quàntic en un estat propi ψ, on ψ és un vector propi de l'observable $\hat{f}$, el resultat serà sempre el mateix i correspondrà al valor propi de l'observable. Aquest fet implica que algunes propietats físiques, com l'energia d'una partícula confinada, només poden prendre valors discrets, fenomen conegut com a *quantització*.

El següent teorema afirma que tot operador hermitià té per valors propis nombres reals; en particular, els valors propis d'observables són nombres reals. Aquest fet és coherent amb que les mesures que realitzem d'estats físics sempre són reals. A la vegada, tenim que els vectors propis corresponents a valors propis diferents són ortogonals ([Sak93]).

Teorema 1.1.2. *El valor propi d'un operador hermitià A és sempre un nombre real; els vectors propis corresponents a valors propis diferents són ortogonals.*

Considerarem només observables que tinguin tots els valors propis diferents. Sota aquesta condició, tot observable diagonalitza i es pot trobar una base de vectors ortogonals, pel teorema anterior. En particular, podem trobar una base de vectors ortonormal. Quan la funció d'ona s'expressa com a combinació lineal de dos o més vectors, diem que tenim una *superposició de la funció d'ona*.

Exemple 1.1.3 (Càlcul de probabilitats de mesura)**.** Suposem que $\hat{f}$ té una base ortonormal $\{e_j\}$ de vectors propis amb valors propis, $\{\lambda_j\}$, diferents. Suposem que ψ és un vector unitari de l'espai de Hilbert corresponent tal que

$$\psi = \sum_{j=1}^{n} a_j e_j.$$

Aleshores, una mesura d'una magnitud f del sistema descrit per la funció d'ona ψ sempre serà un dels valors $\{\lambda_j\}$. La probabilitat d'observar λ_j ve donada per

$$P(f = \lambda_j) = |a_j|^2.$$

Cal destacar que la mecànica quàntica substitueix el paradigma determinista de la física clàssica per un escenari probabilístic, en què les probabilitats d'obtenir un valor determinat d'un observable depenen de l'estat del sistema, descrit pel vector unitari $\psi \in \mathcal{H}$.

Axioma 4. Suposem que un sistema quàntic es troba inicialment en l'estat ψ i que mesurem f. Si el resultat de la mesura és $\lambda \in \mathbb{R}$ aleshores, immediatament després de la mesura, el sistema estarà en l'estat ψ' per al qual se satisfà que

$$\hat{f}\psi' = \lambda\psi'.$$

El pas de ψ a ψ' s'anomena *col·lapse de la funció d'ona*.

Si s'observa el valor λ_j en mesurar $\hat{f}$ aleshores, $\psi' = e_j$, on e_j és el vector propi de l'observable $\hat{f}$ associat a λ_j. És a dir, l'acte de mesurar col·lapsa la funció d'ona només en la direcció e_j.

Podem interpretar que la funció d'ona ψ no és, de fet, l'estat del sistema (malgrat que s'utilitzi el terme físic "estat") sinó allò que descriu la probabilitat de l'estat del sistema. El col·lapse de la funció d'ona és, doncs, similar a la probabilitat condicionada.

Axioma 5. L'evolució temporal de la funció d'ona ψ en un sistema quàntic ve donada per l'equació de Schrödinger

$$\frac{d\psi}{dt} = \frac{1}{i\hbar}\hat{H}\psi,$$

on $\hat{H} := \frac{\hbar}{2m}\frac{\partial^2}{\partial x^2} + V(x)$ és l'operador hamiltonià, $V(x)$ és el potencial i $\hbar$ és la constant de Planck.

Abans d'entrar en detall amb la computació quàntica, exposarem la notació de Dirac (cf. [Sak93]).

Notació 1. Un vector $\psi \in \mathcal{H}$ s'anomena *ket* i es denota $|\psi\rangle$. Aquest vector conté tota la informació sobre l'estat físic.

Els observables, com $\hat{f}$, actuen sobre els kets per l'esquerre:

$$\hat{f} \cdot (|\alpha\rangle) := \hat{f}|\alpha\rangle.$$

El resultat d'aquesta operació és un altre ket.

Els vectors propis d'un observable $\hat{f}$ formen una base ortogonal. Cadascun d'aquests vectors, $\{e_j\}_j$, es pot escriure com $|\lambda_j\rangle$, on λ_j és el valor propi associat al vector e_j. En particular, tenim que $\hat{f}|\lambda_j\rangle = \lambda_j|\lambda_j\rangle$.

Notació 2. Denotarem per $\langle\psi|$ al dual del ket $|\psi\rangle$. Anomenarem a aquest element *bra*.

Com que els diferents kets formen un espai vectorial, els elements del dual són formes lineals. Per tant, els bras són les formes lineals corresponents a cadascun dels kets. En particular, al aplicar un bra a un ket obtenim el producte escalar definit sobre l'espai de Hilbert. Al producte del bra $\langle\beta|$ pel ket $|\alpha\rangle$, $(\langle\beta|) \cdot (|\alpha\rangle)$, el denotarem com $\langle\beta|\alpha\rangle$.

Sigui X un operador també podem considerar el producte d'un bra per un operador, que denotarem per $\langle\alpha|X$; el resultat és un altre bra.

Notació 3. Sigui X un operador, denotarem per $X^\dagger$ l'operador autoadjunt de X.

Tenim la relació següent donada per la dualitat:

$$X|\alpha\rangle \iff \langle\alpha|X^\dagger.$$

Anomenem *producte exterior* al producte de $|\beta\rangle$ i $\langle\alpha|$. El producte exterior el denotem com $|\beta\rangle\langle\alpha|$ i tenim que

$$(|\alpha\rangle\langle\beta|)(|\gamma\rangle) = |\beta\rangle(\langle\alpha|\gamma\rangle).$$

Per tant, podem considerar el producte exterior com un operador. Per últim, denotarem per $\langle\beta|X|\alpha\rangle$ al producte $(\langle\beta|) \cdot (X|\alpha\rangle)$ o, el que és el mateix, al producte $(\langle\beta|X) \cdot (|\alpha\rangle)$.

1.2 Computació quàntica

En aquesta secció donarem alguns conceptes bàsics per a entendre la computació quàntica (cf. [S-R22]). Això passarà per adjudicar a cada entitat d'un ordinador quàntic una funció d'ona que resultarà de la superposició de dos estats que es poden identificar amb els estats 0 i 1 dels ordinadors clàssics.

Treballarem sobre un espai de Hilbert $\mathcal{H} \cong \mathbb{C}^2$ amb norma euclidiana. Per tant, podem prendre com a base la canònica. A aquesta base l'anomenarem *base computacional*:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{i} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Aquests dos vectors són els vectors propis de l'observable que descriu l'energia de l'ordinador quàntic i tenen com a valors propis 0 i 1, respectivament.

Definició 1.2.1 (qubit)**.** Un bit quàntic o *qubit* és un estat quàntic, descrit per una funció d'ona ϕ, que es correspon a un component de l'espai de Hilbert $\mathcal{H} \cong \mathbb{C}^2$ i té la forma:

$$|\phi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad \text{on} \quad |\alpha|^2 + |\beta|^2 = 1,\ \alpha, \beta \in \mathbb{C}.$$

Donada la base computacional $\{|0\rangle, |1\rangle\}$, també podem expressar un qubit com

$$|\phi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle.$$

Observació 1.2.2. D'acord amb l'exemple 1.1.3, la probabilitat que, quan mesurem el qubit descrit per la funció d'ona ϕ, el seu estat col·lapsi a 1 és $|\beta|^2$, mentre que la probabilitat que col·lapsi a 0 és $|\alpha|^2$.

També es poden crear sistemes de n qubits si apliquem el producte tensorial a n qubits. En aquest cas, treballarem sobre l'espai $\mathcal{H}_n \cong \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \cong (\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$ amb norma euclidiana. Aquest espai té com a base ortonormal la induïda pel producte tensorial de n vectors de la base computacional, que coincideix amb la $\mathbb{C}$-base canònica de $\mathbb{C}^{2^n}$. Per exemple, si $n = 3$, ens trobem a l'espai $\mathbb{C}^{2^3} = \mathbb{C}^8$ i tenim un sistema de tres qubits. Aleshores, un element d'aquesta base ortonormal ve donat per les possibles combinacions de tres elements de la base computacional. Per exemple, podem prendre $|1\rangle$, $|0\rangle$ i $|1\rangle$:

$$|101\rangle := |1\rangle \otimes |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \begin{pmatrix} 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} \\ 1 \begin{pmatrix} 1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

La definició de l'espai d'estats d'un sistema de n qubits amb el producte tensorial (i no amb una suma directa) permet modelitzar el fenomen de l'entrellaçament quàntic. Els estats de $\mathbb{C}^{2^n}$ que es poden escriure com a producte tensorial de vectors de $\mathbb{C}^{2^n}$ s'anomenen estats purs. Els estats que no són purs s'anomenen *estats entrellaçats*. Un exemple d'estat entrellaçat és l'estat de Bell descrit per $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Notació 4. Denotarem per $|\phi\rangle_n \in \mathbb{C}^{2^n}$ l'estat d'un sistema de n qubits. Siguin dos registres $|\phi\rangle_n$ i $|\psi\rangle_m$ de n i m qubits, respectivament. Escriurem $|\phi\rangle_n|\psi\rangle_m$ per denotar el producte tensorial de $|\phi\rangle_n$ i $|\psi\rangle_m$.

Les operacions possibles en un ordinador quàntic, és a dir, les que manipulen l'estat dels qubits, estan definides per operadors unitaris aplicats a l'espai de Hilbert associat al sistema considerat. El fet que siguin unitaris és essencial per a preservar la norma dels estats quàntics, garantint així la conservació de probabilitat durant l'evolució del sistema. Un exemple d'operador unitari és l'operador *oracle*. En el cas del problema del subgrup amagat, aquest operador està associat a la funció f i el podem definir com $\mathcal{O}_f|g\rangle_n|0\rangle_m = |g\rangle_n|f(g)\rangle_m$, per a $g \in G$. Gràcies a la superposició, podem fer consultes a múltiples valors de x simultàniament, el que permet explorar moltes classes laterals alhora. Les transformacions unitàries de $\mathbb{C}^{2^n}$, que actuen sobre n qubits, s'anomenen *portes quàntiques*.

Exemple 1.2.3. Un exemple de porta quàntica és la *porta de Hadamard*. Aquesta porta es defineix com

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Quan mesurem l'estat d'un circuit quàntic, el sistema col·lapsa en un dels estats propis de l'observable associat a la mesura. En el cas d'un sistema de n qubits, aquest col·lapse correspon a un dels vectors de la base canònica de $\mathbb{C}^{2^n}$, formada pels estats $\{|0\rangle, |1\rangle\}^{\otimes n}$ que representen els estats base del sistema de n qubits. La probabilitat que el sistema col·lapsi a un estat en concret vindrà donada pel mòdul al quadrat de l'amplitud corresponent a aquest estat. Cal destacar que les variables aleatòries associades a la mesura de cada qubit no són, en general, independents. Quan es mesura un qubit, el seu estat col·lapsa i aquest procés pot afectar l'estat global de tot el registre quàntic a causa de les possibles correlacions o entrellaçament entre qubits. En conseqüència, els coeficients dels vectors de la base computacional s'actualitzen segons les probabilitats condicionades pel resultat de la mesura realitzada.

Per últim, cal remarcar el paral·lelisme amb el cas clàssic. Mentre que, en el cas clàssic, un bit només pot prendre els valors 0 o 1, en el cas quàntic, cada qubit pot estar en una superposició d'aquests dos estats. Per tant, en un ordinador quàntic amb n qubits, es poden realitzar simultàniament fins a 2^n càlculs, mentre que un ordinador clàssic amb n bits només podria gestionar n operacions. Així, amb un ordinador quàntic s'obtindria una millora exponencial en temps de càlcul per a determinats tipus de problemes. Per exemple, algoritmes quàntics poden resoldre una determinada classe de problemes matemàtics considerats difícils en el cas clàssic, com la factorització d'enters.

Capítol 2

Teoria de representació de grups finits

A continuació, donarem alguns conceptes i resultats bàsics de teoria de representació de grups finits que seran útils per a la construcció de la transformada de Fourier. Tot aquest capítol es basa en la referència [Serre12]; ens abstindrem de citar-la cada vegada.

Com que l'objectiu és implementar possibles resolucions del problema del subgrup amagat en un ordinador quàntic, considerem que treballem sobre $K = \mathbb{C}$. Tot i això, alguns dels resultats que donarem a continuació són vàlids si el cardinal de G i la característica del cos K són coprimers.

2.1 Conceptes bàsics

Siguin V un espai vectorial de dimensió n sobre el cos dels nombres complexos i $\mathbf{GL}(V)$ el grup dels isomorfismes de $V \to V$.

Definició 2.1.1. Un homomorfisme

$$\begin{array}{rccc} \rho\colon & G & \longrightarrow & \mathbf{GL}(V) \\ & s & \mapsto & \rho(s) \end{array}$$

s'anomena *representació lineal de G en V*. Si la dimensió de V és n aleshores, la dimensió o el *grau de la representació* és també n.

Quan tinguem ρ, anomenarem a V *l'espai de representació de G* o, per abús de notació, direm que V és una representació de G.

Per tant, si fixem una base de V, podem considerar la matriu R_s de ρ_s en aquesta base.

Definició 2.1.2. Dues representacions de G, ρ en l'espai vectorial V i ρ' en l'espai vectorial V', són isomorfes si existeix un isomorfisme $\tau : V \to V'$ tal que $\tau \circ \rho(s) = \rho'(s) \circ \tau,\ \forall s \in G$. És a dir, dues representacions ρ *i* ρ' *són isomorfes* si existeix una matriu T invertible tal que $T \cdot R_s = R'_s \cdot T,\ \forall s \in G$.

Un exemple de representació d'un grup G qualsevol és la *representació regular* que podem construir de la manera següent. Siguin g l'ordre de G i V un espai vectorial de dimensió g amb base $(e_t)_{t\in G}$, és a dir, amb base indexada pels elements de G. Per a cada $s \in G$, definim ρ_s l'aplicació lineal de V a V que envia $e_t \mapsto e_{st}$.

Definició 2.1.3. Si (ρ, W) i (ρ^0, W^0) venen donades per les matrius R_s i R_s^0. Aleshores, la suma directa de les dues representacions, $W \oplus W^0$ ve donada per la matriu

$$\begin{pmatrix} R_s & 0 \\ 0 & R_s^0 \end{pmatrix}.$$

A continuació, definirem les representacions irreductibles, que tindran un paper clau per a la definició de la transformada de Fourier per a grups no abelians.

Definició 2.1.4. Sigui $\rho : G \to \mathbf{GL}(V)$ una representació lineal de G. La representació ρ és *irreductible* si V no es pot escriure com a suma directa de subespais invariants no trivials.

Teorema 2.1.5 (Teorema de Mashke)**.** *Tota representació és suma directa de representacions irreductibles.*

Observació 2.1.6. Tot grup no abelià té almenys una representació irreductible de grau més gran o igual que 2. En canvi, si un grup és abelià, totes les representacions irreductibles tenen grau 1. També tenim que tota representació de grau 1 és irreductible.

A continuació, donarem com a exemple les diferents representacions irreductibles del grup diedral, que ens seran útils a la secció 5.1 (cf. [ChS24]).

Exemple 2.1.7 (Representacions irreductibles del grup diedral)**.** En primer lloc, definim el grup diedral D_{2n} com el grup format per les rotacions i reflexions en el pla que preserven un polígon regular de n vèrtexs. El grup té ordre $2n$. Si denotem per x la rotació d'angle $2\pi/n$ i y una de les reflexions, tenim que

$$D_{2n} = \langle\ x,\ y\ ;\ x^n,\ y^2,\ (xy)^2\ \rangle.$$

Les representacions del grup diedral depenen de la paritat de n.

Sigui n parell. Hi ha 4 representacions de dimensió 1 doandes per

$$\phi_{u,v} : x \mapsto (-1)^u, \quad y \mapsto (-1)^v,$$

on $u, v \in \mathbb{Z}/2\mathbb{Z}$. Aquestes representacions són retraccions de les dues representacions 1-dimensionals de $D_{2n}/\langle x^2\rangle \cong C_2 \times C_2$ sota l'homomorfisme $D_{2n} \to D_{2n}/\langle x^2\rangle$.

Sigui n senar. Tenim dues representacions 1-dimensionals donades per $\phi_{0,v},\ v \in \mathbb{Z}/2\mathbb{Z}$. Aquestes representacions són retraccions de les representacions 1-dimensionals de $D_{2n}/\langle x\rangle \cong C_2$ sota l'homomorfisme quocient $D_{2n} \to D_{2n}/\langle x\rangle$. Denotem per w les arrels n-èsimes de la unitat, $w = e^{2\pi i/n}$. Hi ha $\lfloor \frac{n-1}{2} \rfloor$ representacions irreductibles de dimensió 2 donades per $\rho_k : D_{2n} \longrightarrow \mathbf{GL}(2, \mathbb{C})$ tal que

$$x \mapsto \begin{pmatrix} w^k & 0 \\ 0 & w^{-k} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

per a $0 < k < \frac{n}{2}$. Aquestes són les representacions induïdes per la representació $\psi_k : C_n \to \mathbb{C}^\times$, donada per $\psi_k(x) = \omega^k$ de C_n a D_{2n}.

Les representacions $\phi_{u,v}$ i ρ_k són totes les representacions irreductibles de D_{2n} llevat d'isomorfisme.

Ara, definirem el caràcter d'una representació i en donarem algunes propietats. Aquest és important ja que permet obtenir informació sobre la irreductibilitat d'una representació o saber si dues representacions són isomorfes.

Definició 2.1.8. Sigui $\rho : G \to \mathbf{GL}(V)$ una representació lineal del grup G, per a cada $s \in G$ definim el *caràcter de la representació* ρ com $\chi(s) := \mathrm{Tr}(\rho_s)$.

Proposició 2.1.9. *Sigui χ el caràcter de la representació ρ de grau n. Tenim les següents igualtats $\forall s \in G$: $\chi(1) = n$; $\chi(s^{-1}) = \chi(s)^*$ i $\chi(tst^{-1}) = \chi(s)$, per a $t \in G$.*

2.2 Lemma de Shur i relacions d'ortogonalitat dels caràcters

Presentarem el lema de Schur, un resultat fonamental en la teoria de representacions de grups, i definirem un producte escalar específic per als caràcters.

Lema 2.2.1 (Lema de Shur)**.** *Siguin $\rho^1 : G \to \mathbf{GL}(V_1)$ i $\rho^2 : G \to \mathbf{GL}(V_2)$ representacions irreductibles del grup G i f una aplicació lineal de $V_1 \to V_2$ tal que $\rho^2_s \circ f = f \circ \rho^1_s$, $\forall s \in G$. Aleshores, si $\rho^1 \ncong \rho^2$ tenim que $f = 0$ i si $V_1 = V_2$ i $\rho^1 = \rho^2$ tenim que f és una homotècia.*

Definició 2.2.2. Siguin ϕ i ψ dues funcions que van de G a $\mathbb{C}$, podem definir el *producte escalar* com

$$(\phi|\psi) = \frac{1}{g} \sum_{t \in G} \phi(t)\psi(t)^*,$$

on g és l'ordre del grup G.

Observació 2.2.3. Siguin ϕ i ψ funcions de G i g l'ordre de G; podem definir $\langle \phi|\psi \rangle = \frac{1}{g} \sum_{t \in G} \phi(t)\psi(t^{-1})$. Si χ és un caràcter d'una representació irreductible de G, tenim que $(\phi|\chi) = \langle \phi|\chi \rangle$ per a qualsevol funció ϕ de G.

A partir d'aquesta definició podem deduir si dues representacions són o no isomorfes o si una representació és irreductible. Si ϕ és el caràcter de la representació (ρ, V), $(\phi|\phi) = 1$ si, i només si, la representació és irreductible. També tenim que si χ i χ' són els caràcters de dues representacions no isomorfes i irreductibles aleshores, $(\chi|\chi') = 0$. El resultat següent ens dóna el nombre de representacions irreductibles d'un grup.

Teorema 2.2.4. *Sigui V una representació lineal de G, amb caràcter ϕ i suposem que V descompon en suma directa de representacions irreductibles: $V = W_1 \oplus \cdots \oplus W_k$. Aleshores, si W és una representació irreductible amb caràcter χ, el nombre de $W_i \cong W$ és igual al producte escalar $(\phi|\chi) = \langle\phi|\chi\rangle$.*

Corol·lari 2.2.5. *Dues representacions irreductibles amb el mateix caràcter són isomorfes.*

Recordem que t *i* t' *són conjugats* si $\exists s \in G$ tal que $t' = sts^{-1}$. Aquesta relació és d'equivalència i parteix G en classes de conjugació.

Definició 2.2.6. Una funció $f \in G$ s'anomena *funció de classe* si $f(tst^{-1}) = f(s),\ \forall s, t \in G$.

Teorema 2.2.7. *Els caràcters $\chi_1, ..., \chi_n$ formen una base ortonormal de l'espai generat per les funcions de classe.*

En el cas de grups abelians, com que totes les representacions irreductibles són unidimensionals, tenim que aquestes són els caràcters que, a la vegada, constitueixen una base ortogonal de l'espai generat per les funcions de classe.

Teorema 2.2.8. *El nombre de representacions irreductibles de G (llevat d'isomorfisme) és igual al nombre de classes de conjugació de G.*

Proposició 2.2.9. *Siguin $s \in G$ i $c(s)$ el nombre d'elements en la classe de conjugació de s. Tenim que*

i. $\sum_{i=1}^{i=n} \chi_i(s)^* \chi_i(s) = \dfrac{g}{c(s)}$;

ii. per a $t \in G$ no conjugat amb s: $\sum_{i=1}^{i=n} \chi_i(s)^* \chi_i(s) = 0$.

2.3 Representacions induïdes

Les representacions induïdes són una eina fonamental en la teoria de representacions de grups ja que permeten construir noves representacions a partir d'altres, generalment a partir de representacions d'un subgrup.

Siguin H un subgrup de G; anomenem *sistema de representació de G/H*, $\mathcal{R}$, a l'elecció d'un element de cada classe per la dreta de H. Aleshores, cada $s \in G$ es pot escriure de manera única com $s = rt$, per a $r \in \mathcal{R}$ i per a $t \in H$.

Siguin $\rho : G \to \mathbf{GL}(V)$ una representació lineal de G i ρ_H la seva restricció a H. Sigui W una subrepresentació de ρ_H, és a dir, un subespai estable sota ρ_t, per a $t \in H$. Denotarem per θ la representació de H en W, $\theta : H \to \mathbf{GL}(W)$.

Sigui $s \in G$; l'espai vectorial $\rho_s W$ depèn únicament de la classe per la dreta sH de s. Si substituïm s per st, per a $t \in H$, tenim que $\rho_{st}W = \rho_s\rho_t W = \rho_s W$.

Si σ és una classe per la dreta de H, podem definir el subespai W_σ de V com $\rho_s W,\ \forall s \in \sigma$. Tenim que W_σ es permuta entre les classes laterals mitjançant ρ_s, per a $s \in G$. La seva suma $\sum_{\sigma \in G/H} W_\sigma$ és, doncs, una subrepresentació de V.

Definició 2.3.1. Diem que *la representació ρ de G en V està induïda per representacions θ de H en W* si, seguint la notació anterior,

$$V = \bigoplus_{\sigma \in G/H} W_\sigma.$$

Equivalentment,

i. cada $x \in V$ pot ser escrit de manera única com $x = \sum_{\sigma \in G/H} X_\sigma$, $X_\sigma \in W_\sigma$, per a cada σ;

ii. si $\mathcal{R}$ és un sistema de representacions de G/H, V és la suma directa de $\rho_r W$, per a $r \in \mathcal{R}$.

Teorema 2.3.2. *Sigui (W, θ) una representació lineal de H. Aleshores, existeix una representació (V, σ) de G induïda per (W, θ) i és única llevat d'isomorfisme.*

2.4 Mètode estàndard del mostreig de Fourier

Per tal de resoldre el problema del subgrup amagat podem utilitzar el que s'anomena mètode estàndard del mostreig de Fourier (cf. [MRRS04]). Un dels passos d'aquest mètode és aplicar la transformada de Fourier al registre de qubits.

Definició 2.4.1. Per a una funció $f : G \to \mathbb{C}$ i una representació irreductible ρ, la *transformada de Fourier de f a ρ* es defineix com

$$\widehat{f}(\rho) = \sqrt{\frac{d_\rho}{|G|}} \sum_g f(g)\rho(g).$$

És a dir, la transformada de Fourier associa a cada representació irreductible ρ una matriu de dimensió $d_\rho \times d_\rho$ (o, més generalment, un operador lineal) que reflecteix com la funció f es descompon segons aquesta representació. Així, doncs, la transformada de Fourier és una aplicació que va de l'espai de funcions $\mathcal{F} = \{f \mid f : G \to \mathbb{C}\}$ a l'espai de matrius $\mathbf{M}(d_\rho, \mathbb{C})$. El resultat de la transformada de Fourier depèn de la representació ρ que triem. El factor $\sqrt{\frac{d_\rho}{|G|}}$ serveix per a normalitzar la transformada de Fourier i garantir-ne bones propietats.

Prosseguim a descriure els passos del mètode ([cf. [GSVV04]]). En primer lloc, es forma una superposició uniforme de classes per la dreta gH aleatòries del subgrup amagat H, és a dir, es forma una distribució uniforme dels vectors $|gH\rangle$,

$$|gH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |gh\rangle.$$

Si coneixem g (o gH) aleshores, tenim la superposició $|gH\rangle$. Per formar aquesta superposició, primer formem la superposició $\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g, 0\rangle$. Després, calculem f

i obtenim $\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g, f(g)\rangle$. Aleshores, mesurem $f(g)$, el que determina la classe lateral gH. Suposem que escollim g uniformement, el resultat d'aquest procés és la superposició $\frac{1}{\sqrt{|H|}}\sum_{h\in H}|gh\rangle$, on g és aleatori. Utilitzem aquesta superposició perquè la informació de H està codificada en classes laterals i gH conté informació de H dins del grup G.

Després, apliquem la transformada de Fourier a aquesta superposició i obtenim el vector

$$\frac{1}{\sqrt{|G||H|}}\sum_{\rho,i,j}\sqrt{d_\rho}\sum_{h\in H}\rho_{i,j}(gh)|\rho,i,j\rangle,$$

on $\rho_{i,j}(gh)$ és l'entrada i,j de la matriu de la representació de gh.

Quan mesurem l'estat, la probabilitat d'obtenir el resultat $|\rho,i,j\rangle$ quan seleccionem l'element gH és

$$P_{gH}(|\rho,i,j\rangle) = \frac{d_\rho}{|G||H|}\left|\sum_{h\in H}\rho_{i,j}(gh)\right|^2 = \frac{d_\rho}{|G|}|\rho(gH)_{i,j}|^2.$$

La probabilitat anterior està condicionada al g escollit per a definir la classe lateral. Tot i això, si seleccionem g de manera uniforme, la probabilitat global és

$$P_H(|\rho,i,j\rangle) = \frac{1}{|G|}\sum_{g\in G}P_{gH}(|\rho,i,j\rangle).$$

La capacitat d'encert d'aquest mètode depèn de la quantitat d'informació estadística sobre H que hi ha a la distribució. Una gran quantitat d'informació de H es dóna només mostrejant ρ i ignorant els índexs de la matriu. Aquest mètode l'anomenem *mètode estàndard feble*. Si mostregem els índexs de la matriu ho anomenarem *mètode estàndard fort*.

Lema 2.4.2. *$\rho(H) = \frac{1}{\sqrt{|H|}}\sum_{h\in H}\rho(h)$ és $\sqrt{H}$ vegades una matriu de projecció i $rank(\rho(H)) = \frac{1}{|H|}\sum_{h\in H}\chi_\rho(h)$, on $\chi_\rho(h)$ és el caràcter de la representació ρ aplicada a h.*

Demostració. Si ens restringim a H, ρ descompon en suma directa de representacions irreductibles $\sigma_1, ..., \sigma_k$. Tenim que $\rho(H)$ és la suma directa de $\sigma_i(H)$. Com que $\sigma_i(H)$ és $\sqrt{|H|}$ si σ_i és la representació trivial i zero altrament es dedueix el primer resultat. La fórmula per a $\text{rank}(\rho(H))$ es dedueix del fet que $\text{rank}(\rho(H))$ és la dimensió de l'espai on $\rho(H)$ no actua trivialment, i que la traça és la suma dels valors propis. □

Lema 2.4.3. *La probabilitat de mesurar ρ és la mateixa per a la superposició uniforme de les classes laterals gH (o Hg), així com per la superposició de H.*

Demostració. El resultat es dedueix de què $\rho(gH) = \rho(g)\rho(H)$ i $\rho(g)$ és unitari. □

Corol·lari 2.4.4. $P_{gH}(|\rho\rangle) = P_H(|\rho\rangle) = \frac{d_\rho}{|G|}\sum_{h\in H}\chi_\rho(h) = \frac{|H|d_\rho}{|G|}rank(\rho(H))$.

Corol·lari 2.4.5. *La probabilitat de mesurar ρ és la mateixa per al subgrup H que per al seu subgrup conjugat $g^{-1}Hg$.*

Capítol 3

Resultat general sobre la complexitat de peticions

Ettinger, Høyer i Knill van demostrar que per a qualsevol grup finit, tant abelià com no abelià, existeix una seqüència de peticions polinòmiques a l'oracle amb les quals es pot obtenir informació suficient per trobar un conjunt de generadors del subgrup amagat (cf. [EHK04]). Tot i això, l'execució de l'algoritme pot requerir una quantitat de temps exponencial. Aquest resultat representa un avenç important ja que redueix el nombre de consultes necessàries, encara que el processament posterior pot seguir sent costós en determinats casos.

3.1 Resultat principal

Definició 3.1.1. Una funció f sobre G s'anomena *$H-$periòdica* si f és constant en les classes laterals per la dreta del subgrup H de G. Si a més a més, f pren valors diferents en les diferents classes laterals, f s'anomena *$H-$periòdica estricta*.

Observem que definir f com a estrictament $H-$periòdica és equivalent a que f separi les classes laterals.

Sigui r el nombre de diferents subgrups de G; podem ordenar els subgrups de G, que denotarem per K_μ, de manera que $|K_\mu| \geq |K_{\mu+1}|$ per a tot $1 \leq \mu \leq r$. Ara, sigui i $n = \lceil \log_2 |G| \rceil$. Si escrivim com $r(G)$ el nombre de generadors del grup G, on $|G| = p_1^{e_1} \cdots p_s^{e_s}$, per a p_i primers diferents i $e_i \in \mathbb{N}$ aleshores, tenim que $r(G) \leq \sum_{i=1}^{s} e_i$ (cf. [New67]). En particular, com que $|G| \leq 2^n$, tenim que $r(G) \leq n$ i, per tant, per a tots els subgrups H de G tindrem que $r(H) \leq n$. És a dir, qualsevol subgrup de G és generat com a màxim per n elements de G. El nombre de subconjunts possibles de G amb cardinalitat menor o igual a n és $\sum_{k=0}^{n} \binom{|G|}{k} \leq \sum_{k=0}^{n} \binom{2^n}{k} \leq n2^{n^2}$. Tenint en compte que no tots els subconjunts generen un subgrup, podem refinar l'acotació i fitar r superiorment per $2^{\mathcal{O}(n^2)}$.

Podem assumir que l'algoritme que enunciarem per al problema del subgrup amagat sempre retorna un subconjunt del subgrup amagat H. Altrament, si retorna

$X \not\subseteq H$ aleshores, podem trobar la intersecció de X i H en avaluar f en cada element $x \in X$ i emmagatzemant aquells valors de x per als quals $f(x) = f(1_G)$. Aquest procés requereix com a màxim $|X| + 1$ avaluacions de f.

Un algoritme que té una *complexitat superpolinòmica* és un algoritme en què el temps d'execució o el nombre de peticions, segons el cas, creix més ràpidament que qualsevol funció polinòmica en la mida de l'entrada. Això vol dir que no es pot expressar un d'aquests valors com una funció polinòmica, sinó que creix de manera més ràpida (per exemple, 2^n). En el cas del problema del subgrup amagat, considerem que la mida de l'entrada és $\log |G|$ i, per tant, considerem que un algoritme és de *temps polinòmic* o té *complexitat polinòmica* si el temps o el nombre de crides a l'oracle, respectivament, es pot expressar com un polinomi en $\log |G|$.

El teorema següent és el resultat principal d'aquest capítol. Aquest mostra que per a tot grup finit G existeix un algoritme que determina el subgrup amagat, H, en un nombre polinòmic de peticions a l'oracle i amb un error exponencialment petit. Notem que només assegurem que la quantitat de crides a l'oracle és polinòmica.

Teorema 3.1.2. *Existeix un algoritme quàntic que, donat un grup finit G i un oracle f en G estrictament $H-$periòdic per a algun subgrup $H \subseteq G$, cridant l'oracle $\mathcal{O}(\log^4 |G|)$ vegades, retorna un conjunt de generadors de H. L'algoritme falla amb probabilitat exponencialment petita en $\log |G|$. L'algoritme es pot fer exacte en qualsevol model que permeti operadors unitaris que actuen sobre un qubit.*

La demostració d'aquest teorema és el contingut d'aquest capítol. Una conseqüència d'aquest resultat és que no es poden obtenir fites inferiors superpolinòmiques de la complexitat de peticions total dels algoritmes per a resoldre el problema del subgrup amagat.

Tot i que per executar l'algoritme es necessita un nombre polinòmic de consultes a l'oracle, el processament posterior d'aquestes dades per determinar amb precisió el subgrup amagat requereix operacions que escalen exponencialment amb la mida de l'entrada. Això inclou tasques com analitzar els estats quàntics resultants de les consultes a l'oracle, realitzar transformades de Fourier quàntiques, construir les transformacions unitàries que es defineixen (implícitament) a través del resultat d'un càlcul clàssic, preparar estats quàntics, executar tècniques d'amplificació d'amplitud... Per tant, el temps per a resoldre el problema del subgrup amagat, en alguns casos, pot ser exponencial.

3.2 Algoritme

Per implementar l'algoritme es necessiten $2 + 2s$ registres, on s és un enter positiu que s'ajusta per a reduir la probabilitat d'error. El primer registre és el de sortida i conté un enter ν entre 0 i r, que indica l'índex del subgrup. El segon registre actua com a comptador i emmagatzema un enter l entre 0 i r. Els $2s$ registres restants s'organitzen en s blocs de dos registres cadascun. El primer registre de cada bloc, anomenat registre del subgrup, conté un element de G, mentre que el segon, anomenat registre de la funció, emmagatzema un valor dins el rang de f.

L'estat inicial que hem de preparar és

$$|\psi_{init}\rangle = |0\rangle|0\rangle \otimes \left(\frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle|f(g)\rangle\right)^{\otimes s}.$$

Per definició, aquest estat el podem crear de manera eficient utilitzant s aplicacions de l'operador $\mathcal{O}_f$. Aleshores, apliquem l'operador Test, que definirem més endavant, obtenint així l'estat $|\psi_{final}\rangle = \text{Test}|\psi_{init}\rangle$. Quan mesurem el primer registre de $|\psi_{final}\rangle$ obtenim l'enter ν. Si $1 \leq \nu \leq r$, obtenim un conjunt de generadors per a K_ν; altrament, obtenim 1_G, que pot ser una resposta errònia. És a dir, $\{1_G\}$ pot no ser el subgrup amagat. L'objectiu d'aquest apartat és demostrar el teorema següent que garanteix que aquest algoritme té una probabilitat d'error exponencialment petita.

Teorema 3.2.1. *Sigui $Prob[K_\nu|H]$ la probabilitat que el resultat de mesurar el primer registre de $|\psi_{final}\rangle$ sigui ν si el subgrup amagat és H. Aleshores $Prob[H|H] \geq 1 - 4r/2^{s/2}$ per a tots els subgrups $H \subseteq G$, on r és el nombre de subgrups de G i s és el nombre de peticions. En particular, per a $s \in \mathcal{O}(n^2 + \log(1/\epsilon))$, l'algoritme retorna el subgrup correcte amb probabilitat com a mínim $1 - 1/\epsilon$, on $\epsilon = \frac{4r}{2^{s/2}}$.*

Algoritme amb probabilitat d'error exponencialment petita

Definició 3.2.2. Un *traslladat* (per l'esquerre) d'un subgrup K de G és un subconjunt $T \subseteq G$ tal que qualsevol element $g \in G$ pot ser escrit de manera única com $g = tk$ per a alguna $t \in T$ i $k \in K$.

Fixem un traslladat T_μ per a cada un dels r subgrups, K_μ, de G.

L'operador Test actua en cadascun dels r subgrups amagats possibles, un per un. Per tant, el podem factoritzar com $\text{Test} = \text{Test}_r \cdot \cdots \cdot \text{Test}_2 \cdot \text{Test}_1$, on cada Test_μ és un operador unitari que comprova si f és K_μ-periòdica. Si una funció és K-periòdica, és $K'-$periòdica per a qualsevol subgrup propi K' de K. Per tant, ho comprovarem primer per a subgrups més grans demanant que $|K_{\mu+1}| \leq |K_\mu|$, per a tot $1 \leq \mu < r$. Si trobem que f és K_μ-periòdica per a algun subgrup K_μ, enregistrem aquesta informació en el primer registre i iniciem el comptador del segon registre. Per tal de definir explícitament l'operador Test, hem de definir dos altres operadors, que denotarem per Q_μ i $P_{s,\mu}$.

Per a qualsevol subgrup $K_\mu \subseteq G$, anomenem Q_μ l'operador unitari que actua en els dos primers registres tal que

$$\begin{cases} Q_\mu|0\rangle|0\rangle = |\mu\rangle|1\rangle, & \text{si } l = 0, \\ Q_\mu|\nu\rangle|l\rangle = |\nu\rangle|l+1\rangle, & \text{si } l > 0. \end{cases}$$

Un cop el comptador l incrementa de 0 a 1, el contingut del primer registre no canvia. L'objectiu del primer registre és assegurar que els operadors utilitzats siguin unitaris i, si alguna comprovació té èxit, que cap comprovació afecti el contingut del primer registre. Així, el primer registre contindrà el valor μ més gran per al qual la

funció f és K_μ-periòdica, mentre que el segon registre indicarà el nombre total de subgrups K_μ tal que la funció f és K_μ-periòdica.

Per tal de comprovar si f és $K_\mu-$periòdica és necessari definir un altre operador que actuara sobre els $2s$ registres restants. Denotem per $\mathrm{P}_{s,\mu}$ la projecció dels s parells de registres definida per

$$\mathrm{P}_{s,\mu} = \left(\sum_{t \in T_\mu} |tK_\mu\rangle\langle tK_\mu| \otimes I \right)^{\otimes s},$$

on I és l'operador identitat. L'operador $|tK_\mu\rangle\langle tK_\mu|$ extreu de l'estat quàntic la part que correspon a la classe tK_μ, mentre que I actua sobre els registres que no tenen informació relativa a les classes laterals. El sumatori sobre les diferents $t \in T_\mu$ cobreix totes les classes laterals, assegurant que l'operador projecta l'estat quàntic al subespai associat al subgrup K_μ. Finalment, el producte tensorial per s indica que actuem de manera independent i en paral·lel sobre els s blocs de dos registres cadascun. Denotem per $\mathrm{P}^{\perp}_{s,\mu}$ al complement de l'operador anterior, que projecta sobre el subespai ortogonal el generat per les classes laterals de K_μ.

Ara, ja podem definir l'operador Test_μ: $\mathrm{Test}_\mu := Q_\mu \otimes \mathrm{P}_{s,\mu} + I \otimes \mathrm{P}^{\perp}_{s,\mu}$, que és unitari per construcció. L'operador Test_μ aplica Q_μ als dos primers registres, condicionat al fet que els s registres del subgrup es trobin en estats corresponents a una classe lateral de K_μ. Per comprovar aquesta condició, s'utilitzen els operadors unitaris U_μ i V_μ. L'operador U_μ transforma l'estat $|1_G\rangle$ en una superposició uniforme dels elements del subgrup K_μ, $U_\mu|1_G\rangle = \frac{1}{\sqrt{|K_\mu|}} \sum_{k \in K_\mu} |k\rangle$. Per altra banda, V_μ transforma $|t\rangle|k\rangle$ en $|1_G\rangle|tk\rangle$ per a tot $t \in T_\mu$ i $k \in K_\mu$. El procediment és el següent. Primer, s'adjunta un registre auxiliar a cada registre del subgrup i s'aplica $V_\mu^\dagger$ a aquests s parells de registres, de manera que aquesta operació reconstrueix l'estat $|t\rangle|k\rangle$ a partir de $|tk\rangle$. A continuació, s'aplica $U_\mu^\dagger$ als registres del subgrup, el que projecta els estats dels subgrups a $|1_G\rangle$ si la funció f és K_μ-periòdica. Si tots els registres del subgrup es troben en l'estat $|1_G\rangle$, s'aplica Q_μ. Aquest pas és el que comprova que els s parells de registres es trobin en una classe lateral de K_μ ja que, en cas contrari, no s'aplica Q_μ. Finalment, es reverteixen els passos anteriors per assegurar que l'operació global sigui unitària. Per definició dels diferents operadors unitaris que utilitzem, és possible realitzar tots aquests passos amb una xarxa d'operacions de complexitat polinòmica en $|G|$ i s.

Lema 3.2.3. *Si f és K_μ-periòdica aleshores,*

$$\mathit{Test}_\mu|\psi_{\mathit{init}}\rangle = |\mu\rangle|1\rangle \otimes \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle \right)^{\otimes s}.$$

Per inducció sobre s, obtenim el resultat següent.

Lema 3.2.4. *Si f no és K_μ-periòdica aleshores, la distància $|(\mathit{Test}_\mu|\psi_{\mathit{init}}\rangle - |\psi_{\mathit{init}}\rangle)|$ és com a màxim $\frac{2}{2^{s/2}}$.*

Per a cada $1 \leq j \leq r$, denotem per $|\psi_j\rangle = \mathrm{Test}_j \cdots \mathrm{Test}_1|\psi_{\mathrm{init}}\rangle$ l'estat del sistema després d'aplicar j tests. Pel lema anterior, és possible iterar els operadors Test sense que la distància creixi exponencialment.

Lema 3.2.5. *Si f no és K_μ-periòdica per a tot $1 \leq \mu \leq j$ aleshores, la distància $||\psi_j\rangle - |\psi_{init}\rangle|$ és com a màxim $\frac{2j}{2^{s/2}}$.*

Suposem que f és una funció estrictament K_ν- periòdica, on ν denota l'índex del grup que guardem en el primer registre. Recordem que $0 \leq \nu \leq r$. Pel lema 3.2.5, l'estat $|\psi_{\nu-1}\rangle$, anterior a l'aplicació de Test_ν, és com a màxim a una distància $\epsilon = \frac{2r}{2^{s/2}}$ de l'estat inicial. Aleshores, la probabilitat que el test Test_ν no doni la resposta correcta $|\nu\rangle$ és, pel lema 3.2.3, com a màxim $2\epsilon = \frac{4r}{2^{s/2}}$.

La probabilitat de mesurar el resultat μ depèn de quin subgrup amagat H tenim, però és independent dels valors que f pren en les diferents classes laterals de H. És a dir, per a dues funcions f i f' que tinguin el mateix subgrup amagat, H, la probabilitat de mesurar μ és la mateixa. Per tant, podem denotar per $\text{Prob}[K_\mu|H]$ la probabilitat que μ sigui el resultat de mesurar el primer registre, ν, de l'estat $|\psi_{\text{final}}\rangle$, condicionat al fet que el subgrup amagat sigui H. Això demostra el teorema 3.2.1, ja que la probabilitat que el test Test_ν doni la resposta correcta $|\nu\rangle$ en el primer registre és 1-2$\epsilon = 1 - \frac{4r}{2^{s/2}}$. En conseqüència, per $s \in \mathcal{O}(\log^2 |G| + 1/\epsilon)$ l'algoritme falla amb probabilitat exponencialment petita en $\log |G|$.

Notem que hem fet un nombre total de crides a l'oracle de l'ordre de $\log^4 |G|$. En primer lloc, per preparar l'estat inicial de superposició per $s \in \mathcal{O}(\log^2 |G| + 1/\epsilon)$ necessitem $\mathcal{O}(\log^2 |G|)$ crides a l'oracle. En segon lloc, s'ha de preparar l'estat inicial per a tots els Test, en particular, $r = \log^2 |G|$ vegades. Aleshores, tenim que el nombre total de crides és de $\mathcal{O}(\log^4 |G|)$.

Per tant, queda demostrada la primera part del teorema 3.1.2.

Millora de l'exactitud de l'algoritme

Per tal de fer l'algoritme exacte, necessitem de calcular amb precisió, sense utilitzar l'oracle, les probabilitats condicionades $\text{Prob}[K_\mu|H]$. Una manera de fer-ho és escollir una funció f qualsevol que sigui estrictament H-periòdica i simular el càlcul quàntic de l'operador Test sobre l'oracle f utilitzant un ordinador clàssic. En la demostració del resultat següent veurem que aquest càlcul es necessari per a tot K_μ, $1 \leq \mu \leq r$. Per a demostrar la baixa complexitat de consultes només necessitem saber que existeixen les transformacions unitàries adequades. Aquest model, tot i que no és realista, perquè involucra un preprocessament clàssic costós, és suficient per descartar límits simples inferiors en la complexitat de consultes.

Sigui $Y_{\frac{1}{4}} \cup Y_{\frac{3}{4}}$ qualsevol partició del conjunt $\{K_1, ..., K_r\}$, on els subíndexs es relacionaran amb les probabilitats que el subgrup amagat es trobi en un dels dos conjunts en particular. Prosseguim a descriure l'algortime ExactTest que distingeix en quin dels dos conjunts donats es troba el subgrup amagat.

Lema 3.2.6. *La probabilitat que el resultat de la mesura del qubit auxiliar de l'estat $ExactTest(|\psi_{init}\rangle \otimes |0\rangle)$ sigui 1 és $\frac{3}{4}$ si el subgrup amagat H està en $Y_{\frac{3}{4}}$ i és $\frac{1}{4}$ si H està en $Y_{\frac{1}{4}}$.*

Demostració. En primer lloc, construïm la matriu M, matriu $r \times r$ sobre $[0, 1]$, on

cadascuna de les seves files i columnes està indexada per un subgrup. L'entrada (H, K_μ) de la matriu M ve donada per la probabilitat condicionada $\text{Prob}[K_\mu|H]$, és a dir, la probabilitat que el mesurament del primer registre de $|\psi_{\text{final}}\rangle$ sigui μ condicionat al fet que f sigui estrictament $H-$periòdica. Sigui $s = \lceil 2\log(4r^3)\rceil \in \mathcal{O}(\log^2|G|)$. Pel teorema 3.2.1 qualsevol entrada de la diagonal de la matriu M és com a mínim $1-\frac{1}{r^2}$. Com que les entrades de qualsevol fila de la matriu M sumen 1, qualsevol element fora de la diagonal es troba entre 0 i $\frac{1}{r^2}$. Aleshores, podem escriure $M = I - \Delta$, on el valor absolut de cada entrada de la matriu Δ està acotat per $1/r^2$. Es segueix que $M^{-1} = I + \Delta + \Delta^2 + \Delta^3 + \cdots$, subjecte a la convergència del sumatori $\Gamma = \Delta + \Delta^2 + \Delta^3 + \cdots$ que es demostra utilitzant la fórmula geomètrica tenint en compte que cada entrada de Δ^i està acotat per $\frac{1}{r^{i+1}}$.

Sigui y un vector columna de dimensió r amb valors entre $\frac{1}{4}$ i $\frac{3}{4}$ i cada fila indexada per un subgrup. Denotem per x al vector resultant de l'operació $M^{-1}y$. Aleshores, com que $M^{-1}y = y + \Gamma y$, cada entrada de x divergeix com a màxim un factor de $\frac{3}{4(r-1)}$ de la corresponent entrada de y ja que $\Gamma y \leq \frac{1}{r(r+1)}\frac{3}{4}$, per la fórmula de la suma geomètrica. Per tant, cada entrada de x es troba en l'interval [0,1], per a $r \geq 3$.

L'algoritme ExactTest actua sobre el registre inicial $|\psi_{init}\rangle \otimes |0\rangle$, on l'últim registre és un qubit auxiliar. Aquest algoritme es pot definir com

$$\text{ExactTest} := \text{R} \cdot (\text{Test} \otimes \text{I}).$$

És a dir, primer s'aplica l'operador Test a la primera part del sistema i després s'aplica R que, condicionat al fet que el registre de sortida contingui l'índex del subgrup μ, rota el qubit auxiliar de $|0\rangle$ a $\sqrt{1-x_\mu}|0\rangle + \sqrt{x_\mu}|1\rangle$. Aquesta rotació garanteix que es retorni la probabilitat desitjada per a cada subconjunt, $Y_{\frac{1}{4}}$ i $Y_{\frac{3}{4}}$. Com que $\text{R} = \sum_\mu \text{P}_\mu \otimes \text{R}_\mu$ per a projeccions $\text{P}_\mu = |\mu\rangle\langle\mu|$ i certes rotacions de qubits R_μ, es pot implementar de manera unitària. La probabilitat que el mesurament del qubit auxiliar del resultat $\text{ExactTest}(|\psi_{\text{init}}\rangle \otimes |0\rangle)$ sigui 1 és $\sum_\mu x_\mu \text{Prob}[K_\mu|H_\nu]$. Per definició del vector x, és igual a y_ν, on H_ν és el subgrup amagat. És a dir, la probabilitat de mesurar 1 depèn únicament de l'índex del subgrup amagat. Posem $y_\nu = \frac{3}{4}$ si $K_\nu \in Y_{\frac{3}{4}}$ i posem $y_\nu = \frac{1}{4}$ si $K_\nu \in Y_{\frac{1}{4}}$ aleshores, obtenim el resultat desitjat. □

Podem utilitzar l'amplificació de l'amplitud (cf. [BHMT02]) per alterar les probabilitats a 0 i 1 i, per tant, distingir amb probabilitat 1 en quin dels dos conjunts es troba el subgrup amagat H. Mitjançant la partició recursiva del conjunt de subgrups en meitats i l'aplicació del mètode anterior a cada partició, l'algorisme acota progressivament el subgrup amagat exacte, provant així la segona part del teorema 3.1.2.

Capítol 4

Grups resolts

En aquest capítol presentarem alguns resultats que garanteixen que el problema del subgrup amagat es pot resoldre en temps polinòmic o amb un nombre acotat de consultes a l'oracle. Com veurem, els grups per als quals s'ha aconseguit resoldre aquest problema no difereixen gaire dels grups abelians. Malgrat això, aquest fet representa un avenç significatiu gràcies a l'ús d'eines diferents respecte al cas abelià.

4.1 Grups hamiltonians

Veurem que és possible identificar en temps polinòmic un subgrup amagat si aquest és un subgrup normal de G (cf. [GSVV04]).

Lema 4.1.1. *Si H és un subgrup normal de G i ρ és una representació irreductible de G aleshores, $\rho(H)$ és un múltiple escalar no negatiu de la matriu identitat. És diferent de zero si, i només si, $H \subseteq \ker(\rho)$.*

Demostració. Sigui $\sigma_1, ..., \sigma_k$ la descomposició de ρ restringida a H. Volem veure que si σ_1 és la representació trivial aleshores, totes les altres representacions també són trivials.
Sigui W l'espai on actua ρ. Sigui V el subespai 1-dimensional de W on actua σ_1. Com ρ és irreductible sobre G, els elements $g \in G$ porten V a un conjunt de subespais que recobreixen W. Com que $H = gHg^{-1}$, $\forall g \in G$, cada una de les imatges gV és invariant per a H. □

Ara, tenim que

$$\cap_\rho \ker(\rho) = \cap_\rho \{g \in G \mid \rho(g) = \mathrm{Id}_V\}$$

i a aquest conjunt el denotarem per N.

Teorema 4.1.2. *La intersecció de $\ker(\rho)$ amb $\mathcal{O}(\log |G|)$ repeticions del mostreig de Fourier és, amb alta probabilitat, igual al subgrup normal més gran del subgrup amagat.*

Demostració. Sigui H el subgrup amagat. Per a demostrar el teorema serà suficient veure que si $N \not\subseteq H$ aleshores, amb probabilitat com a molt $1/2$, el pròxim mostreig de Fourier donarà una representació irreductible ρ tal que $N \subseteq \ker(\rho)$. La probabilitat de què això succeeixi ve donada per

$$\sum_{\rho:N\subseteq\ker(\rho)} \frac{d_\rho |H| \text{rank}(\rho(H))}{|G|},$$

com afirma el resultat 2.4.4.

Com que N és normal en G, el mostreig de Fourier de la superposició $|NH\rangle$, on NH és el conjunt de productes ordenats d'elements de N i H, dóna com a resultat només representacions irreductibles amb nuclis que contenen N. A la vegada, com que $N \triangleleft G$, tenim que NH és un grup i

$$1 = \sum_{\rho:N\subseteq\ker(\rho)} \frac{d_\rho |NH| \text{rank}(\rho(NH))}{|G|}.$$

Notem que $\rho(NH) = \rho(N)\rho(H)$ és una matriu no nul·la múltiple de $\rho(H)$ per a qualsevol ρ tal que $H \subseteq \ker(\rho)$, pel lema anterior. Aleshores, quan realitzem el mostreig de Fourier per a la superposició $|H\rangle$, la probabilitat d'obtenir ρ tal que el seu nucli contingui N és

$$\sum_{\rho:N\subseteq\ker(\rho)} \frac{d_\rho |H| \text{rank}(\rho(H))}{|G|} = \sum_{\rho:N\subseteq\ker(\rho)} \frac{d_\rho |H| \text{rank}(\rho(NH))}{|G|} \leq$$

$$\leq \frac{1}{2} \sum_{\rho:N\subseteq\ker(\rho)} \frac{d_\rho |NH| \text{rank}(\rho(NH))}{|G|} = \frac{1}{2}.$$

□

Suposem que el subgrup amagat és un subgrup normal de G aleshores, el subgrup normal més gran del subgrup amagat serà ell mateix i, per tant, el mètode estàndard feble ens retornarà el resultat correcte. Per tant, serà possible resoldre el problema del subgrup amagat per a aquells grups que tinguin tots els subgrups normals.

Notem que l'algoritme es basa en repetir el mostreig de Fourier $\mathcal{O}(\log |G|)$ vegades i calcular la intersecció amb $ker(\rho)$. En conseqüència, podem executar l'algoritme en temps polinòmic.

Definició 4.1.3. Direm que un grup G és *hamiltonià* si tots els seus subgrups són normals.

Un exemple de grup hamiltonià no abelià és el grup dels quaternions, Q_8. Aquest grup ve generat pels elements $\{1, -1, i, -i, j, -j, k, -k\}$ i les relacions

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ ji = -k,\ jk = i,\ kj = -i,\ ki = j,\ ik = -j.$$

Els subgrups de Q_8 són: els subgrups trivials $\langle 1\rangle$ i Q_8, els grups cíclics d'ordre quatre $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$ i, per últim, $\langle 1, -1\rangle$. Tots els subgrups de Q_8 són normals.

4.2 Grups quasi-abelians

S'ha demostrat que el problema del subgrup amagat també es pot resoldre en temps polinòmic per al que anomenarem grups quasi-abelians si utilitzem el que hem vist a la secció anterior (cf. [GSVV04]). Sigui G un grup no abelià finit i H un subgrup amagat.

Definició 4.2.1. Denotem per $\kappa(G)$ la intersecció dels normalitzadors de tots els subgrups de G. Sigui G pertany a una família de grups G_n d'ordre n. Diem que G és *quasi abelià* si l'índex de $\kappa(G)$ en G és d'ordre igual o menor que $\exp(\mathcal{O}(\log^{1/2} n))$.

El motiu que s'imposi $[G : \kappa(G)] \leq \exp(\mathcal{O}(log^{1/2}n))$ és garantir que l'algoritme corri en temps polinòmic. Si es dóna aquesta condició, heurísticament podem dir que $\kappa(G)$ està a prop de ser tot G i, per tant, que quasi tots els elements de G commuten. Observem que $\kappa(G) = \cap_V N(V) \subseteq N(H) \subseteq G$, on V és un subgrup qualsevol. Tenim que $\kappa(G)$ és normal en G. El subgrup $N(H)$ no és conegut però sabem que $N(H)/\kappa(G) \subseteq G/\kappa(G)$ i podem examinar totes les possibilitats.

Considerem el següent algoritme per a trobar H. Per a cada subgrup J de G que contingui $\kappa(G)$, correm l'algoritme descrit a la secció anterior per a J i detectem amb alta probabilitat el subgrup normal del subgrup amagat de J, H_J, tal que H_J és el subgrup normal més gran del subgrup amagat H en cada J. Un cop executat l'algoritme anterior per a tots els subgrups de G que continguin $\kappa(G)$, calculem la unió de tots els H_J. El següent resultat afirma que si G és un grup quasi abelià, podem trobar el subgrup amagat H utilitzant aquest algoritme en temps polinòmic.

Teorema 4.2.2. *Amb alta probabilitat $H = \bigcup_J H_J$. A més a més, si $[G : \kappa(G)] \in \exp(O(\log^{1/2} n))$, l'algoritme s'executa en temps polinòmic.*

Demostració. Tot i que $N(H)$ és desconegut, $N(H)/\kappa(G)$ és un subgrup de $G/\kappa(G)$, i l'algoritme examina totes les possibilitats. Notem també que $\kappa(G) \subseteq N(H)$ i $H \subseteq N(H)$. Un grup d'ordre a té com a màxim $2^{\log_2 a}$ subgrups, com hem vist al capítol anterior. Per tant, la cota de $[G : \kappa(G)] \leq \exp(O(\log^{1/2} n))$ garanteix que només cal considerar un nombre polinòmic de subgrups.

Tots els subgrups ocults dels diferents J són subgrups (normals) de H. Com que executem l'algoritme per a tots els subgrups que contenen $\kappa(G)$, $\kappa(G) \subseteq N(H)$ i $H \triangleleft N(H)$, almenys un dels subgrups amagats trobats és igual a H. Pels resultats donats en la secció anterior per a subgrups amagats normals, només hi ha una petita probabilitat que qualsevol H_J produït per l'algoritme sigui diferent del subgrup ocult de J. □

Notem que l'algoritme per a detectar el subgrup normal més gran del subgrup amagat s'executa en temps polinòmic i per al cas de grups quasi-abelians només considerem un nombre polinòmic de subgrups, gràcies a l'acotació de $[G : \kappa(G)]$. Aleshores, com que només executem l'algoritme per a detectar el subgrup normal del subgrup amagat un nombre polinòmic de vegades, l'algoritme per a grups quasi-abelians que hem donat es pot executar en temps polinòmic.

Exemple 4.2.3. Alguns grups que podem considerar quasi abelians són els grups generats per extensió d'un grup abelià A per un grup B; és a dir, qualsevol grup G tal que $A \triangleleft G$ i $G/A \cong B$. Tot i que alguns grups d'aquest tipus són quasi abelians no tots satisfan que $[\kappa(G) : G]$ sigui de l'ordre de $\exp(\mathcal{O}(log^{1/2}n))$.

Per tal de generar grups per extensions podem utilitzar el producte semidirecte que denotarem per $A \rtimes B$. Sigui $G = A \rtimes B$, tenim que $A \triangleleft G$, B és isomorf a un subgrup de G, $AB = G$ i $A \cap B = \{1\}$. Per a definir l'estructura necessitem l'homomorfisme $\theta : B \to \mathrm{Aut}(A)$, que descriu com els elements de B actuen sobre els elements de A. Aleshores, l'operació de $A \triangleleft G$ per a qualssevol elements $(a_1, b_1), (a_2, b_2) \in A \rtimes B$ es defineix com:

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot (\theta(b_1))(a_2, b_1 \cdot b_2).$$

Alternativament, l'estructura del grup $G = AB$, ve donada per la igualtat $bab^{-1} = (\theta(b))(a)$. En el cas que tant A com B siguin subgrups de G, no cal especificar l'homomorfisme θ ja que els elements de B actuen sobre els elements de A per l'operació de G.

Per tal que el grup $G = A \rtimes B$ sigui quasi abelià és convenient que $\ker(\theta)$ sigui gran ja que, com que $\ker(\theta) \subseteq Z(G) \subseteq \kappa(G)$, tindrem que $\kappa(G)$ serà gran i, per tant, $[G : \kappa(G)]$ serà petit.

Un exemple de grup generat a partir del producte semidirecte de dos grups és el grup diedral: $D_{2n} = C_n \rtimes C_2$. Tot i això, el grup diedral no és un grup quasi abelià ja que si n és senar tenim que $|\kappa(D_{2n})| = |\{1\}| = 1$ i si n és parell tenim que $|\kappa(D_{2n})| = |\{1, r^{n/2}\}| = 2$. Per tant, $[D_{2n} : \kappa(G)] \geq n \geq \exp(\mathcal{O}(log^{1/2}2n))$.

Alguns grups generats a partir del producte semidirecte que sí són quasi abelians són grups amb l'estructura $G = C_3 \rtimes C_m$, on $m = 2^n$, per a algun $n \in \mathbb{N}$. L'homomorfisme θ per a $(a, b) \in C_2 \rtimes C_m$ ve donat per la igualtat $(\theta(b))(a) = a^2 = a^{-1}$. Ara, els subgrups no trivials de G són $\langle(a, 0)\rangle$ i $\langle(0, b)\rangle$, per a $a \in C_3$ tal que $a^3 = 1$ i $a \neq 1$ i $b \in C_m$ tal que $b^m = 1$ i $b \neq 1$. El normalitzador de $\langle(a, 0)\rangle$ és tot G, ja que $bab^{-1} \in \langle(a, 0)\rangle$, i el normalitzador de $\langle(0, b)\rangle$ és C_m. Per tant, $|\kappa(G)| = |\kappa(C_3 \rtimes C_m)| = |C_m| = m$ i tenim que $[C_3 \rtimes C_m : \kappa(C_3 \rtimes C_m)] = \frac{3m}{m} = 3 \leq \exp(\mathcal{O}(log^{1/2}3m)) = \exp(\mathcal{O}(log^{1/2}3 \cdot 2^n)) \simeq exp(\mathcal{O}(c\sqrt{n}))$, per a alguna constant $c > 0$; que demostra que $C_3 \rtimes C_m$ és quasi abelià per a $n \geq 2$.

4.3 Grups afins

En aquesta secció veurem que és possible resoldre el problema del subgrup amagat per a grups afins amb un circuit quàntic de mida polinòmica (cf. [MRRS04]). Tot i que en el capítol 3 ja hem vist que es pot resoldre el problema per a qualsevol grup utilitzant una quantitat de peticions polinòmica amb baixa probabilitat d'error, en aquesta secció explicitarem un algoritme per a aquest tipus de grup. També donarem un cas més general per a grups generats per extensions.

Definició 4.3.1. Anomenem grup afí A_p al grup format pels parells ordenats $(a.b) \in (\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}/p\mathbb{Z}$, on p és primer, amb l'operació $(a_1, b_1) \cdot (a_2, b_2) = (a_1a_2, b_1 + a_1b_2)$.

El grup afí es pot interpretar com el conjunt de funcions afins $f_{(a,b)} : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ que envien $x \in \mathbb{Z}/p\mathbb{Z}$ a $ax + b \in \mathbb{Z}/p\mathbb{Z}$ i tenen com a operació la composició de funcions. A nivell estructural, A_p és el producte semidirecte $(\mathbb{Z}/p\mathbb{Z})^* \ltimes \mathbb{Z}/p\mathbb{Z}$. També podem veure el grup afí com el grup format per les matrius

$$\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix} \subseteq \mathbf{GL}(2, \mathbb{Z}/p\mathbb{Z}),$$

per a p primer, amb l'operació donada per la multiplicació de matrius.

El grup afí té subgrups normals i subgrups no normals. Sigui $a \in (\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $q < p$; aleshores els subgrups normals del grup afí són de la forma $\mathbb{Z}/q\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$. Aquests subgrups els anomenarem N_a i els seus elements són de la forma (a^t, b) per a $1 \leq t \leq q$. Per altra banda, els subgrups no normals del grup afí els podem expressar com $H_a = \langle (a, 0) \rangle$. Tenim que $|H_a| = q$. El conjugat de H_a el denotarem com H_a^b i consisteix en els elements de la forma $(a^t, (1 - a^t)b)$.

Per tal de construir una representació del grup afí, cal fixar un generador γ de $(\mathbb{Z}/p\mathbb{Z})^*$. Sigui $\phi : (\mathbb{Z}/p\mathbb{Z})^* \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z}$ l'isomorfisme $\phi(\gamma^t) = t$ i sigui ω_p l'arrel p-ésima de la unitat, $e^{2\pi i/p}$. Aleshores, $A_p \cong (\mathbb{Z}/p\mathbb{Z})^* \ltimes \mathbb{Z}/p\mathbb{Z}$ i té $p - 1$ representacions unidimensionals que anomenarem σ_s i que vénen donades per $\sigma_t((a, b)) = \omega_{p-1}^{t\phi(a)}$. També tenim una representació $p - 1$-dimensional donada per

$$\rho((a, b))_{j,k} = \begin{cases} \omega_p^{bj}, & k = aj \mod p, \\ 0, & \text{altrament}, \end{cases}$$

per a $1 \leq j$ i $k < p$.

A continuació, exposarem un seguit de teoremes que garanteixen que és possible resoldre el problema del subgrup amagat per a grups afins. Abans donarem algunes definicions (cf. [MRS05]). Denotarem per polylog(p) a qualsevol funció que creixi com un polinomi en logaritme de p.

Definició 4.3.2. Anomenem *POVM* (de l'anglès *Positive Operator-Valued Measure*) a un tipus de mesurament quàntic generalitzat. Un *POVM* amb un conjunt de possibles resultats J és un conjunt d'operadors positius $\{M_j \mid j \in J\}$ que satisfan la condició de completitud $\sum_{j \in J} M_j = \mathbb{1}$, on $\mathbb{1}$ és l'operador identitat. El resultat d'aplicar aquesta mesura a un estat quàntic $|\psi\rangle$ és una variable aleatòria que pren valors en J. La probabilitat d'obtenir el resultat $j \in J$ ve donada per $P_j = \langle \psi | M_j | \psi \rangle$.

Definició 4.3.3. Direm que els subgrups de la família $G = \{G_i\}$ són *reconstructibles des del punt de vista de la teoria de la informació quàntica* si el problema del subgrup amagat pels G_i ve determinat pel resultat d'un circuit quàntic de mida polinòmica en $\log |G_i|$. És a dir, existeix un POVM que dóna el subgrup H amb una probabilitat constant. Notem que no es garanteix que el POVM es pugui implementar amb un circuit de baixa complexitat.

Teorema 4.3.4. *Sigui p primer i $q|p-1$. Els conjugats en $\mathbb{Z}/q\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$, H_a^b, són reconstructibles des del punt de vista de la teoria de la informació quàntica.*

Demostració. Les representacions de $\mathbb{Z}/q\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$ inclouen les q representacions unidimensionals de $\mathbb{Z}/q\mathbb{Z}$, donades per $\sigma_\ell((a^t, b)) = \omega_q^{\ell t}, \quad \ell \in \mathbb{Z}/q\mathbb{Z}$, i $(p-1)/q$ representacions q-dimensionals ρ_k, definides com

$$\rho_k((a^u, b))_{s,t} = \begin{cases} \omega_p^{ka^s b}, & \text{si } t = s + u \mod q, \\ 0, & \text{altrament,} \end{cases}$$

per a cada $0 \leq s, t < q$. Aquí k recorre els elements de $(\mathbb{Z}/p\mathbb{Z})^*/(\mathbb{Z}/q\mathbb{Z})$, o equivalentment, k pren valors en $(\mathbb{Z}/p\mathbb{Z})^*$ però ρ_k i $\rho_{k'}$ són equivalents si k i k' pertanyen a la mateixa classe lateral de $\langle a \rangle$. Aquestes ρ_k són els $(p-1)/q$ blocs diagonals de les representacions $p-1$-dimensionals de A_p.

Notem que tots els conjugats de H_a es troben en l'únic subgrup isomorf a $(\mathbb{Z}/q'\mathbb{Z}) \ltimes (\mathbb{Z}/p\mathbb{Z})$, on q' és l'ordre de a; per tant, sense pèrdua de generalitat, podem assumir que estem treballant amb el màxim subgrup no normal, H_a, on a és un generador de $\mathbb{Z}/q\mathbb{Z}$.

Sumant ρ_k sobre els elements $(a^t, (1-a^t)b)$, obtenim l'operador de projecció associat

$$(\pi_{H_a^b}(\rho_k))_{s,t} = \frac{1}{q}\omega_p^{k(a^s - a^t)b},$$

per a $0 \leq s, t < q$. Aquest és una matriu de rang 1, on cada columna és alguna arrel de la unitat multiplicada pel vector $u_k = \frac{1}{q}\omega_p^{ka^s b}$. Notem que el grau de ρ, n_ρ, és igual a q/p.

Ara volem demostrar que hi ha una mesura els resultats de la qual, donats dos valors diferents de b, tenen una gran distància total de variació (almenys $1/\text{poly}(n)$). Primer, mesurem el nom de la representació. Després, mesurem la columna de la representació. Per últim, realitzem una mesura POVM amb q possibles resultats, on cada resultat determina si s és u o $u+1 \mod q$ per a algun $u \in \mathbb{Z}/q\mathbb{Z}$.

La probabilitat total d'observar una de les representacions q-dimensionals és $n_\rho(p-1)/q = 1 - 1/p$, ja que n'hi ha $(p-1)/q$. Aquestes passos que hem descrit determinen k, eliminen l'efecte de la classe lateral i determinen si s té el valor u o $u+1$. Podem escriure això com el vector $\frac{1}{\sqrt{2}}\begin{pmatrix} \omega_p^{ka^u b} \\ \omega_p^{ka^{u+1} b} \end{pmatrix}$. Apliquem la porta de Hadamard, donada a l'exemple 1.2.3, a l'estat anterior i mesurem s.

La probabilitat de mesurar u és $\cos^2\theta$ i la probabilitat de mesurar $u+1$ és $\sin^2\theta$, on $\theta = (\pi k a^u (a-1)b)/p$. Ara, quan observem una representació de dimensió q, el valor k que observem està distribuït uniformement sobre $(\mathbb{Z}/p\mathbb{Z})^*/(\mathbb{Z}/q\mathbb{Z})$, i quan realitzem el POVM, el u que observem està distribuït uniformement sobre $\mathbb{Z}/q\mathbb{Z}$. Deduïm que el coeficient $m = ka^u(u-1)$ està distribuït uniformement sobre $(\mathbb{Z}/p\mathbb{Z})^*$. Per a dos valors diferents b i b', la distància total de variació entre les distribucions de probabilitats és

$$\frac{1}{2(p-1)} \sum_{m \in (\mathbb{Z}/p\mathbb{Z})^*} \left| \cos^2 \frac{\pi m b}{p} - \cos^2 \frac{\pi m b'}{p} \right| + \left| \sin^2 \frac{\pi m b}{p} - \sin^2 \frac{\pi m b'}{p} \right|.$$

Utilitzant identitats trigonomètriques i sumant sobre m, podem demostrar que aquesta distància és més gran que $\frac{1}{4}$. Per tant, la variació total de la distància entre

dos conjugats diferents qualssevol està acotada inferiorment per una constant. Aleshores, podem distingir entre els p conjugats diferents H_a^b amb un nombre polinòmic de mostres. Això demostra el teorema. □

Aquest teorema no diu que el subgrup H es pugui trobar de forma eficient, però sí que la informació per a determinar-lo està present en l'estat quàntic generat pel circuit.

Teorema 4.3.5. *Sigui p primer i $q|p-1$. Els subgrups dels grups q-hedral, $\mathbb{Z}/q\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$, són reconstructibles des del punt de vista de la teoria de la informació quàntica. En particular, els subgrups del grup afí $A_p = (\mathbb{Z}/p\mathbb{Z})^* \ltimes \mathbb{Z}/p\mathbb{Z}$ són reconstructibles des del punt de vista de la teoria de la informació quàntica.*

Demostració. Si apliquem l'algoritme per a grups hamiltonians podem reconstruir (totalment) H si H és un subgrup normal no trivial. Això es deu a que aquest tipus de grups generats usant el producte semidirecte tenen la propietat que si A és un subgrup normal no trivial i $A \subset B$ aleshores, B també és normal; i el cor normal

$$\cap_{\gamma \in G} \gamma C \gamma^{-1}$$

de qualsevol subgrup C no normal és la identitat.

En el cas que H no sigui un subgrup normal de $\mathbb{Z}/q\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$, tenim que $H = \langle (a,b) \rangle$ i és cíclic. Tenim que $|H|$ és l'ordre de a. Ara, per a cada $i \in [k]$ i per a $1 \leq \alpha \leq \alpha_i$, sigui $\Upsilon_i^\alpha : \mathbb{Z}/q\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/(q/p_i^\alpha)\mathbb{Z}$ l'homomorfisme donat per

$$\Upsilon_i^\alpha : (a,b) \mapsto a^{p_i^\alpha}.$$

Aleshores, tenim que

$$A_i^{\alpha_i} = \ker \Upsilon_i^\alpha = \{\gamma \in \mathbb{Z}/q\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z} | \gamma^{p_i^{\alpha_i}} = 1\}.$$

És a dir, $A_i^{\alpha_i}$ és el subgrup de $\mathbb{Z}/q\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$ format per aquells elements l'ordre dels quals és múltiple de p_i^α.

Considerem ara la funció

$$\begin{array}{rccc} (f, \Upsilon_i^\alpha): & \mathbb{Z}/q\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z} & \longrightarrow & S \times \mathbb{Z}/(q/p_i^\alpha)\mathbb{Z} \\ & \gamma & \mapsto & (f(\gamma), \Upsilon_i^\alpha(\gamma)). \end{array}$$

Notem que (f, Υ_i^α) separa classes de $H \cap A_i^\alpha$. Tenim que el subgrup $H \cap A_i^\alpha$ té ordre p^α si, i només si, p^α divideix l'ordre de a. Aleshores, podem determinar si $H \cap A_i^\alpha$ té ordre p^α assumint que té aquest ordre, aplicant el teorema anterior i comprovant el resultat comparant amb l'oracle original, f. Això ens permet determinar la factorització de $|H|$, com volíem. Per tant, tots els subgrups dels grups $q-$hedral $\mathbb{Z}/q\mathbb{Z} \ltimes \mathbb{Z}/p\mathbb{Z}$ són reconstructibles des del punt de vista de la informació quàntica. □

Aquest resultat es pot generalitzar per a grups generats per extensions.

Teorema 4.3.6. *Sigui H un grup els subgrups amagats del qual es poden trobar amb una quantitat de peticions polinòmica i K un grup de mida polinòmica en* $\log|H|$. *Aleshores, es pot resoldre el problema del subgrup amagat per a qualsevol extensió de K per H, és a dir, qualsevol grup G tal que $K \triangleleft G$ i $G/K \cong H$, utilitzant una quantitat de peticions polinòmica*

Demostració. Podem assumir que la multiplicació de G i K es poden dur a terme en temps polinòmic clàssic. Denotem per $t(h)$ un conjunt de representats de les classes per l'esquerre de K. En primer lloc, notem que qualsevol subgrup $L \subseteq G$ pot ser descrit en termes de la intersecció $L \cap K$, la projecció $L_H = L/(L \cap K) \subseteq H$ i un representant $\eta(h) \in L \cap (t(h) \cdot K)$ per a cada $h \in L_H$.

Aleshores, cada element de L_H està associat a alguna classe lateral per l'esquerre de $L \cap K$, és a dir, $L = \cup_{h \in L_H} \eta(h) \cdot (L \cap K)$. És més, si S és un conjunt de generadors de $L \cap K$ i T és un conjunt de generadors per a L_H aleshores, $S \cup \eta(T)$ és un conjunt de generadors de L.

Podem reconstruir S en temps polinòmic clàssic consultant la funció f, del problema del subgrup amagat, en tots els elements de K. Aleshores, $L \cap K$ és el conjunt de tots els elements k tals que $f(k) = f(1)$. El conjunt de generadors S es construeix afegint elements de $L \cap K$ un a un fins que generem tot $L \cap K$.

Per a identificar L_H, definim una nova funció f' en H que consisteixi en una col·lecció desordenada de valors de f en les classes laterals per l'esquerre corresponents de K. Tenim que

$$f'(h) = \{f(g) | g \in t(h) \cdot K\}.$$

Cada consulta a f' consisteix en $|K| = \text{poly}(n)$ consultes a f. Els conjunts de nivell de f' són les classes laterals de L_H, de manera que reconstruïm L_H resolent el problema del subgrup amagat en H. Això proporciona un conjunt T de generadors per a L_H.

Encara falta trobar un representant $\eta(h)$ en $L \cap (t(h) \cdot K)$, per a cada $h \in T$. Per a trobar un representant, avaluem f en g per a $g \in t(h) \cdot K$ i definim $\eta(h)$ com qualsevol g tal que $f(g) = f(1)$. Com que $|T| = \mathcal{O}(\log|H|) = \text{poly}(n)$, podem trobar $\eta(h)$ en temps polinòmic. □

Tot i això, no podem iterar aquest algoritme més d'un nombre constant de vegades ja que això requerirà un nombre superpolinòmic de peticions de h per a cada petició de h'. En el cas que K tingui mida superpolinòmica, aquest resultat no dóna informació de com obtenir $\eta(h)$, encara que H tingui dos elements. Aquesta és la dificultat que ens trobem amb el grup diedral.

Capítol 5

Grups no resolts

A continuació, presentarem dos exemples de grups no abelians per als quals encara no es coneix cap algoritme de temps polinòmic que resolgui el problema del subgrup amagat: el grup simètric i el grup diedral. Aquests grups són especialment rellevants, ja que la seva resolució està vinculada a problemes de gran importància des d'una perspectiva computacional i pràctica.

5.1 Grup diedral

Malgrat que el grup diedral és un grup no abelià amb una estructura relativament senzilla, encara no s'ha trobat un algoritme, ni tan sols quàntic, que resolgui en temps polinòmic el problema del subgrup amagat per al cas general. En aquesta secció, donarem alguns teoremes d'impossibilitat, importants per a establir límits a la resolució d'aquest problema (cf. [ChS24]).

En primer lloc, prenem $G = D_{2n} = \langle x, y \ ; \ x^n, y^2, (yx)^2 \rangle$ com el grup diedral d'ordre $2n$. Les representacions d'aquest grup (cf. exemple 2.1.7) permetran discutir, a continuació, la possible resolubilitat del problema del subgrup amagat.

Es pot demostrar que el problema del subgrup amagat per al grup diedral es pot reduir al cas on el subgrup amagat és de la forma $H_a = \langle yx^a \rangle$, per a $0 \leq a < n$ (cf. [HoE99]). Aleshores, el problema del subgrup amagat per al cas del diedral es basa en la possibilitat de trobar el paràmetre a.

Expressem en la base complexa el sumatori de les representacions irreductibles dels elements de la forma gh, per a $g \in D_{2n}$ i $h \in H_a$. Tenim els dos casos següents.

Si $\rho = \rho_k$:

$$\sum_{h \in H} \rho(x^\alpha h) = \begin{pmatrix} \omega^{\alpha k} & \omega^{-(a-\alpha)k} \\ \omega^{(a-\alpha)k} & \omega^{-\alpha k} \end{pmatrix}, \tag{5.1.1}$$

$$\sum_{h \in H} \rho(yx^\alpha h) = \begin{pmatrix} \omega^{(a-\alpha)k} & \omega^{-\alpha k} \\ \omega^{\alpha k} & \omega^{-(a-\alpha)k} \end{pmatrix}. \tag{5.1.2}$$

Si $\rho = \phi_{u,v}$:

$$\sum_{h\in H} \rho(x^\alpha h) = (-1)^{\alpha u} + (-1)^{v+(a-\alpha)u} = (-1)^{\alpha u}(-1 + (-1)^{v+au}),$$

$$\sum_{h\in H} \rho(yx^\alpha h) = (-1)^{(a-\alpha)u} + (-1)^{v+\alpha u} = (-1)^{(a-\alpha)u}(-1 + (-1)^{v+au}).$$

Recordem que aquests sumatoris apareixen quan apliquem la transformada de Foruier a l'estat de superposició, com hem vist a la secció 2.4. La transformada de Fourier és un operador unitari i, per tant, necessitem que $\rho_k(gh)$ sigui unitària per a cada k, $g \in D_{2n}$ i $h \in H_a$. En conseqüència, s'ha de satisfer que $|\rho_k(gh)_{i,j}| \leq 1$, per a $1 \leq i, j \leq 2$. Per a cada conjunt de representacions irreductibles 2-dimensionals, ρ_k, tenim que la probabilitat de mesurar $|\rho_k, i, j\rangle$ és

$$\mathbf{P}(\rho_k, i, j) = \frac{1}{n}|(\rho_k(cyx^a)_{i,j} + \rho_k(c))_{i,j}|^2 \leq \frac{1}{2n}(|\rho_k(cyx^a)_{i,j}| + |\rho_k(c)_{i,j}|)^2 \leq \frac{4}{2n},$$

on $c = y^\beta x^\alpha$, per a $0 \leq \beta < 2$ i per a $0 \leq \alpha < n$. Obtenim que, si n és gran, la probabilitat és petita.

Per altra banda, tenim que existeix la mesura òptima de valor d'operador positiu per a determinar a a partir d'una única mostra de la forma

$$\psi_a = \psi_{a;\alpha} = \frac{1}{\sqrt{2}}(|x^\alpha\rangle + |yx^{a-\alpha}\rangle)$$

(cf. [MoR05]) i el resultat obtingut es pot considerar una bona mesura de a. És més, el mesurament òptim té una probabilitat d'èxit donada per

$$\mathbf{P}_{\text{èxit}} = \frac{2}{2n}\left(1 - \frac{1}{4n}\right),$$

que és incompatible amb la probabilitat anterior.

Teorema 5.1.1. *L'algoritme estàndard per al problema del subgrup amagat en el cas de $G = D_{2n}$ no pot implementar una mesura òptima mesurant només una classe lateral.* □

Aquest teorema implica, doncs, que en el cas d'utilitzar l'algoritme estàndard de resolució del problema del subgrup amagat per al grup diedral, la mesura d'una sola classe lateral no dóna prou informació per a reconstruir el subgrup H_a o, el que és el mateix, per a trobar a.

Tot i això, disposem d'un algoritme que permet resoldre el problema del subgrup amagat en el cas de grups diedrals, D_{2n}, on $n = 2^t$. Aquest algoritme utilitza $2^{\mathcal{O}(\sqrt{\log 2n})}$ temps, espai i peticions. Donarem un esquema de l'algoritme. L'algoritme detallat i demostracions es poden consultar en [Kup11].

1. Expressem la primera fila de 5.1.1 com
$$\frac{1}{\sqrt{2(2n)}}\sum_k\left(\omega^{\alpha k}|k\rangle|0\rangle+\omega^{(a-\alpha)k}|k\rangle|1\rangle\right)=\frac{1}{\sqrt{2n}}\sum_k\omega^{\alpha k}\oplus\frac{1}{\sqrt{2}}(|0\rangle+\omega^{ak}|1\rangle).$$

2. Mesurem el primer registre i obtenim una mostra de la forma $|\psi_k\rangle=\frac{1}{\sqrt{2}}(|0\rangle+\omega_N^{ak}|1\rangle)$, que proporciona k.

3. Combinem els estats de la forma donada per $|\psi_k\rangle$ i obtenim que $|\psi_p\rangle|\psi_q\rangle=\frac{1}{\sqrt{2}}(|\psi_{p+q}\rangle|0\rangle+\omega_N^{aq}|\psi_{p-q}\rangle|1\rangle)$. Si p i q tenen el mateixos mj bits no significatius aleshores, $p\pm q$ incrementa estrictament el nombre de bits no significatius que p i q comparteixen.

4. Obtenint prou mostres de la forma ψ_p que tinguin mj bits no significatius en comú i combinant els estats descrits del pas anterior, podem produir prou estats amb $m(j+1)$ bits no significatius en comú.

5. Obtenint prou mostres des del principi, eventualment, produïm estats de la forma $\psi_{2^{t-1}}=|0\rangle+(-1)^a|1\rangle$, que permeten determinar la paritat de a.

També tenim un algoritme concret per a trobar el subgrup amagat H_a i, en conseqüència, resoldre el problema del subgrup amagat per al grup diedral. Aquest algoritme utilitza un nombre polinòmic de peticions i una quantitat exponencial de temps. Tot i així, aquest no suposa un avenç perquè, malgrat donar un algoritme específic per al cas del grup diedral, no millora el resultat que hem demostrat en el capítol 3 (cf. [HoE99]).

Problema de les classes lateral del grup diedral i clonació quàntica

Per tancar aquesta secció, acabarem amb alguns resultats d'impossibilitat i veurem com podem relacionar el problema de classes per al grup diedral amb el problema de clonació quàntica. Totes les demostracions dels resultats auxiliars que es necessiten per a demostrar el teorema principal es poden veure amb més detall a la referència [ChS24]. En primer lloc, donarem algunes definicions.

Problema 5.1.2. Donada una mostra de la forma $\psi_a=\psi_{a;\alpha}=\frac{1}{\sqrt{a}}(|x^\alpha\rangle+|yx^{a-\alpha}\rangle)$, anomenarem *problema de les classes laterals del grup diedral* (o DCP per les seves sigles en anglès) al problema de trobar generadors del subgrup amagat $H=H_a$.

Notem que si produïm la mostra ψ_a amb el mètode estàndard del mostreig de Fourier per al problema del subgrup amagat, obtenim les mateixes mostres que amb el problema de les classes laterals del grup diedral.

Definició 5.1.3. Partim d'un sistema quàntic inicial compost per l'estat quàntic $|\psi\rangle$ que volem clonar, un registre auxiliar $|A\rangle$ i un registre inicial $|0\rangle$ (en blanc). Direm que *copiem un estat quàntic* $|\psi\rangle$ si apliquem una operació quàntica unitària U a aquest sistema per tal d'obtenir com a resultat $U(|A\rangle|\psi\rangle|0\rangle)=|\Sigma(\psi)\rangle|\psi\rangle|\psi\rangle$.

El teorema de no clonació estableix que no hi ha cap operació unitària capaç de copiar un estat quàntic desconegut arbitrari sense alterar-lo (cf. [Wei09]). No obstant això, es poden imposar certes condicions sobre l'estat que es vol clonar per tal que sigui possible realitzar-ne una còpia.

Proposició 5.1.4. *Sigui $|\psi_{a;1}\rangle, ..., |\psi_{a;m}\rangle$ un conjunt d'estats mútuament ortogonals que depenen d'un paràmetre a. Suposem que $|\psi\rangle = |\psi_{a;i}\rangle$ per a algun índex i desconegut. Si coneixem el valor de a aleshores, existeix un operador unitari que copia $|\psi\rangle$.*

Una versió més forta del resultat anterior és la següent.

Proposició 5.1.5. *Sigui $|\psi_{a:1}\rangle, ..., |\psi_{a:m}\rangle$ un conjunt d'estats mútuament ortogonals que depenen d'un paràmetre a i que podem codificar un operador unitari T tal que $T|a\rangle|\psi_{a;i}\rangle = |a\rangle|i\rangle$. Si tenim el valor de a en un registre aleshores, existeix un operador unitari que copia $|\psi\rangle$.*

A continuació, donarem un teorema que relaciona el problema de classes laterals del grup diedral i la capacitat de clonació d'una de les mostres.

Teorema 5.1.6. *Si a és desconegut, no existeix cap operació unitària que, a partir d'una llista de mostres DCP per a a, copiï una mostra DCP addicional per al mateix a i alhora que deixi intacta la llista de mostres.*

Per últim, acabarem amb un teorema d'impossibilitat que demostrarem amb els resultats que hem donat anteriorment sobre la clonació d'estats quàntics.

Teorema 5.1.7. *No existeix cap operació unitària que calculi el valor de a d'un registre a partir d'una llista de mostres DCP per a a.*

Demostració. Suposem que existeix un operador unitari U tal que

$$U|A\rangle|\psi_a^1\rangle \cdots |\psi_a^m\rangle|0\rangle = |\Sigma_a(\psi_a)\rangle|a\rangle.$$

És a dir, a partir d'una llista de mostres del problema de classes laterals per al grup diedral per a una a fixada, però desconeguda, per a un estat en blanc $|0\rangle$ i per a un estat auxiliar $|A\rangle$, U calcula a en el registre en blanc. Utilitzant un registre en blanc addicional i copiant a, existeix un operador unitari U' tal que

$$U'|A\rangle|\psi_a^1\rangle \cdots |\psi_a^m\rangle|0\rangle|0\rangle = |\Sigma_a(\psi_a)\rangle|a\rangle|a\rangle.$$

Podem utilitzar U^{-1} per permutar $|a\rangle$ i $|0\rangle$ i obtenir el registre

$$|A\rangle|\psi_a^1\rangle \cdots |\psi_a^m\rangle|a\rangle|0\rangle.$$

Aleshores, sense pèrdua de generalitat, podem assumir que l'operador U té l'efecte que

$$U|A\rangle|\psi_a^1\rangle \cdots |\psi_a^m\rangle|0\rangle = |A\rangle|\psi_a^1\rangle \cdots |\psi_a^m\rangle|a\rangle.$$

És a dir, a partir d'una llista de mostres del problema de classes laterals per al grup diedral per a una a fixada, però desconeguda, per a un estat en blanc $|0\rangle$ i per a un estat auxiliar $|A\rangle$, U calcula a en el registre en blanc deixant la llista de mostres intacta.

Notem que les mostres del problema de classes laterals per al grup diedral, $\psi_{a;\alpha}$, es poden codificar com

$$\frac{1}{\sqrt{2}}(|0\rangle|\alpha\rangle + |1\rangle|a-\alpha\rangle).$$

L'operador unitari V donat per

$$V|a\rangle|0\rangle|\alpha\rangle = |a\rangle|0\rangle|\alpha\rangle, \quad V|a\rangle|1\rangle|\alpha\rangle = |a\rangle|1\rangle|a-\alpha\rangle,$$

té el l'efecte següent sobre el registre $\psi_{a;\alpha}$:

$$V|a\rangle|\psi_{a;\alpha}\rangle = |a\rangle\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\alpha\rangle.$$

Si utilitzem la porta de Hadamard (cf. exemple 1.2.3), podem codificar un operador unitari U_0 tal que

$$U_0\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\alpha\rangle = |0\rangle|\alpha\rangle, \quad U_0\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)|\alpha\rangle = |1\rangle|\alpha\rangle.$$

Aleshores, si apliquem l'operador $(I \otimes U_0)V$ a $|a\rangle$ i $|\psi_{a;\alpha}\rangle$ tenim que

$$(I \otimes U_0)V|a\rangle|\psi_{a;\alpha}\rangle = |a\rangle|0\rangle|\alpha\rangle.$$

Ara bé, si apliquem la proposició 5.1.5, de la possibilitat de clonació quan tenim el valor de a en un registre i els estats són mútuament ortogonals, podem copiar $|\psi_{a;\alpha}\rangle$ deixant les altres mostres del DCP intactes. Aquest fet contradiu el teorema 5.1.6 que afirma que si a és desconegut no existeix cap operador unitari que pugui copiar una mostra i deixar la resta de la llista intacta. □

Per tant, per molt que apliquem el mètode estàndard per a resoldre el problema del subgrup amagat en el cas del grup diedral no podrem trobar un operador unitari que calculi a a partir d'un conjunt de mostres del DCP i, per tant, que resolgui el problema. Notem que això no implica que el problema sigui irresoluble; de fet, ja hem vist que el problema del subgrup amagat es pot resoldre per a tots els grups, sinó que, per tal de resoldre el problema a partir de les mostres obtingudes amb el mètode estàndard, és necessari utilitzar una seqüència d'operadors unitaris, donada una llista de mostres de DCP, o combinar operadors clàssics i quàntics.

5.2 Grup simètric

A continuació, exposem el problema del subgrup amagat per al cas del subgrup simètric. Veurem que sota condicions generals tant el mètode estàndard feble com el mètode estàndard fort, descrits a la secció 2.4, fallen i no donen cap avantatge sobre el cas clàssic. Veurem també que el problema principal que ens trobem al intentar resoldre el problema per al grup simètric és el que anomenarem problema del subgrup conjugat amagat.

Problema del subgrup conjugat amagat

Problema 5.2.1. Siguin G un grup i H un subgrup no normal de G. Denotem un conjugat de H com $H^g = g^{-1}Hg$. Considerem el problema del subgrup amagat per a G, on el subgrup amagat és H^g per a algun $g \in G$. Aleshores, el *problema del subgrup conjugat* consisteix a identificar quin H^g és el subgrup amagat.

A continuació, veurem més en detall el corol·lari 2.4.5, és a dir, veurem que emprant el mètode estàndard no podem distingir subgrups conjugats (cf. [MRS05]). Suposem que $|H\rangle$ és una superposició sobre un subgrup. Sigui ρ una representació irreductible sobre un espai vectorial V. Anem a veure si podem distingir dos conjugats diferents de H o podem distingir H del grup trivial. Tenim l'estat de superposició

$$|H\rangle = \frac{1}{\sqrt{H}} \sum_{h \in H} |h\rangle.$$

Si apliquem la transformada de Fourier, obtenim el coeficient

$$\hat{H}(\rho) = \sqrt{\frac{d_\rho}{|H||G|}} \sum_{h \in H} \rho(h) = \sqrt{\frac{d_\rho |H|}{|G|}} \Pi_H,$$

on $\Pi_H = (1/|H|) \sum_{h \in H} \rho(h)$ és l'operador projecció al subespai V. La probabilitat que observem ρ és

$$P(\rho) = \|\hat{H}(\rho)\|^2 = \frac{d_\rho |H|}{|G|} rk \Pi_H.$$

Aquesta probabilitat és la mateixa per a tots els conjugats H^g. Això es deu a que per a un subgrup H del grup simètric, H^g tindrà la mateixa distribució d'elements en les classes de conjugació de S_n. És a dir, la informació quàntica obtinguda després de la transformada de Fourier no permet distingir entre un grup i un dels seus conjugats. A més, en el cas del grup simètric tenim que el nombre de conjugats possibles augmenta la complexitat del problema.

Possibilitat de distingir l'element trivial

Per al cas del grup simètric la forma forta del mètode estàndard no proporciona cap informació addicional no negligible per al grup simètric i els subgrups que considerem (cf. [KeS04]).

Siguin G un grup finit i H un subgrup de G. Per a resoldre el problema del subgrup amagat necessitem determinar H a partir de la distribució resultant del mètode estàndard. Si utilitzem el resultat del corol·lari 2.4.4, la probabilitat de mesurar ρ amb el mètode estàndard feble és $P_H(\rho) = (d_\rho/|G|) \sum_{h \in H} \chi_\rho(h)$. Anomenem D_H a la variació total de la distància entre P_H i $P_{\{1_G\}}$, quan mostregem amb el mètode estàndard feble. Podem distingir l'element trivial, $\{1_G\}$, de l'element d'un altre subgrup de H si, i només si, D_H és més gran que un cert invers

polinòmic en $\log|G|$. Podem expressar D_H com

$$D_H = \frac{1}{|G|}\sum_{\rho} d_\rho \left| \sum_{h\in H, h\neq 1_G} \chi_\rho(h)\right|.$$

Definició 5.2.2. Direm que H és *distingible* (utilitzant el mètode estàndard feble) si $D_H \geq (\log|G|)^{-c}$ per a alguna constant c. Direm que és *indistingible* en cas contrari.

Tenim les següents fites de D_H.

Teorema 5.2.3. *Sigui $C_1, ..., C_k$ les classes de conjugació de G diferents de la identitat. Aleshores,*

$$\sum_{i=1}^{k} |C_i \cap H|^2 |H|^{-1} |C_i|^{-1} < D_H \leq \sum_{i=1}^{k} |C_i \cap H||C_i|^{-\frac{1}{2}}.$$

Demostració. Per a cada representació irreductible ρ de G, tenim que

$$\left| \sum_{h\in H, h\neq e} \chi_\rho(h)\right| \leq \sum_{h\in H, h\neq e} |\chi_\rho(h)| \leq \sum_{h\in H, h\neq e} d_\rho < |H| d_\rho,$$

on d_ρ és la dimensió de la representació ρ. Per tant, $d_\rho > |H|^{-1}|\sum_{h\in H,h\neq e}|\chi_\rho(h)|$. Si substituïm a l'expressió de D_H obtenim que $D_H > \frac{1}{|G||H|}\sum_\rho \left|\sum_{h\in H,h\neq e}\chi_\rho(h)\right|^2$.

Notem que si $h \in H \cap C_i$ aleshores, $\chi_\rho(h) = \chi_\rho(C_i)$. Per tant, tenim que $\sum_{h\in H,h\neq e}\chi_\rho(h) = \sum_{i=1}^{k}|H\cap C_i|\chi_\rho(C_i)$. Això implica que

$$D_H > \frac{1}{|G||H|}\sum_\rho \left|\sum_{i=1}^{k}|H\cap C_i|\chi_\rho(C_i)\right|^2. \tag{5.2.1}$$

Notem que podem desenvolupar el terme $\left|\sum_{i=1}^{k}|H\cap C_i|\chi_\rho(C_i)\right|^2$ de la següent manera:

$$\left|\sum_{i=1}^{k}|H\cap C_i|\chi_\rho(C_i)\right|^2 = \sum_{i=1}^{k}|H\cap C_i|^2|\chi_\rho(C_i)|^2 + \sum_{i\neq j}|H\cap C_i||H\cap C_j|\chi_\rho(C_i)\overline{\chi_\rho}(C_j).$$

Si utilitzem les relacions d'ortogonilitat tenim que $\sum_\rho\sum_{i=1}^{k}|H\cap C_i|^2|\chi_\rho(C_i)|^2 = \sum_{i=1}^{k}|H\cap C_i|^2|G|/|C_i|$ i que $\sum_\rho\sum_{i\neq j}|H\cap C_i||H\cap C_j|\chi_\rho(C_i)\overline{\chi_\rho}(C_j) = 0$. Per tant, si substituïm a 5.2.1 obtenim la cota inferior.

Prosseguim ara demostrar la cota superior. Podem escriure

$$D_H|G| = \sum_\rho d_\rho\left|\sum_{h\in H,h\neq e}\chi_\rho(h)\right| \leq \sum_\rho d_\rho \sum_{h\in H,h\neq e}|\chi_\rho(h)| = \sum_{h\in H,h\neq e}\sum_\rho|\chi_\rho(h)|. \tag{5.2.2}$$

Fixem un $h \in H$ i una i tal que $h \in C_i$. Si utilitzem la desigualtat de Cauchy-Schwarz obtenim que $\sum_\rho d_\rho|\chi_\rho(h)| \leq \left(\sum_\rho d_\rho\right)^{1/2}\left(\sum_\rho |\chi_\rho(h)|^2\right)^{1/2}$. Ara, si apliquem les relacions d'ortogonalitat tenim que $\sum_\rho d_\rho|\chi_\rho(h)| \leq |G|^{1/2}(|G|/|C_i|)^{1/2} = |G||C_i|^{-1/2}$. Sumem per a tots els elements de H diferents de la identitat i notem que la cota superior anterior succeeix $|H \cap C_i|$ vegades. Consegüentment, tenim que $\sum_{h\in H, h\neq e}\sum_\rho d_\rho|\chi_\rho(h)| \leq \sum_{i=1}^k |G \cap C_i||G||C_i|^{-1/2}$. Si combinem aquesta cota amb la cota 5.2.2 obtenim que $D_H \leq \sum_{i=1}^k |H \cap C_i||C_i|^{-1/2}$. □

El següent resultat és una conseqüència immediata del teorema.

Corol·lari 5.2.4. *Sigui C_{min} la classe de conjugació més petita diferent de la identitat que interseca amb H de manera no trivial. Aleshores,*

$$|H|^{-1}|C_{min}|^{-1} < D_H \leq (|H| - 1)|C_{min}|^{-1/2}.$$

□

Amb aquest resultat ja podem identificar subgrups distingibles d'ordre polilogarítmic en un grup arbitrari G. Si $|H|$ és polilogarítimic, pel corol·lari anterior, D_H^{-1} és polilogarítmic si, i només si, $|C_{\min}|$ ho és.

Teorema 5.2.5. *Suposem $|H| \leq (\log|G|)^c$, per a alguna constant c. Aleshores, H és distingible si, i només si, H té un element h diferent de la identitat tal que $|h^G| \leq (\log|G|)^{c'}$, per a alguna constant c'.*

□

Sigui $X = G/H$; denotem per $\mathrm{fix}_X(g)$ el nombre de punts fixos de $g \in G$ per l'acció de G. Denotem per $r = r_X(G)$ el rang de G, és a dir, el nombre d'òrbites del estabilitzador H en X.

De la desigualtat $D_H > r_X(G)/|X| - 1/|H|$ es dedueix el següent teorema.

Teorema 5.2.6. *Suposem que $|H|$ no és polilogarítmic però que el subgrau mitjà de G en G/H és polilogarítmic. Aleshores, H és indistingible. En particular, això es compleix quan $|H : H \cap H^g| \leq (\log|G|)^c,\ \forall g \in G$.*

Del teorema anterior es dedueix que si H és normal en G aleshores H és distingible, fet que recolza la possibilitat de resoldre el problema del subgrup amagat per a grups hamiltonians o grups quasi abelians, tal i com hem vist al capítol anterior. A la vegada, els subgrups de mida $|G|/(\log|G|)^c$ són sempre distingibles.

Considerem ara el cas particular del grup simètric. Sigui $G = S_n$.

Definició 5.2.7. El *grau mínim $m(H)$ d'un grup de permutacions H* es defineix com el nombre mínim de punts que es mouen a un element de H diferent de la identitat. Per a cada $g \in S_n$ denotem per $\mathrm{fix}(g)$ el nombre de punts fixos de g. Anomenem suport de g a $\mathrm{supp}(g) = n - \mathrm{fix}(g)$. Aleshores,

$$m(H) = \min\{\mathrm{supp}(h) \mid 1 \neq h \in H\}.$$

Teorema 5.2.8. *Sigui $H \subseteq S_n$ tal que $|H| \leq n^c$ per a alguna constant c. Aleshores, H és distingible si, i només si, $m(H)$ és constant.*

Demostració. Sigui $g \in S_n$ amb $\text{supp}(g) = k$. Aleshores, es pot verificar que $\binom{n}{k} \leq |g^{S_n}| \leq n^k$. En conseqüència, una classe de conjugació C de S_n té ordre polinòmic si, i només si, consisteix en element de suport constant. Aquesta observació juntament amb el teorema 5.2.5 prova el resultat. □

Un exemple de grup on $m(H)$ és no constant és el grup generat per un cicle de llargada no constant. Notem que aquest teorema assegura que tots els grups distingibles de mida polinòmica han de contenir un element de suport constant.

Definició 5.2.9. Un grup de permutacions s'anomena *primitiu* si és transitiu.

Els grups de permutació primitius només tenen una òrbita. Aquests grups són considerats els grups que construeixen els grups de permutacions finites en general. Sigui $H \subseteq S_n$ un subgrup primitiu diferent de A_n, tenim que $|H| \leq 2n^{\sqrt{n}}$ i, per tant, no es pot aplicar el teorema anterior. El resultat següent demostra que en aquest cas, el subgrup H és indistingible.

Teorema 5.2.10. *Sigui $H \neq A_n$ un subgrup primitiu de S_n. Aleshores, H és indistingible.*

Podríem suposar que si el subgrup H és gran, és fàcil distingir-lo. Tanmateix, el teorema següent prova que encara que H sigui extremadament gran pot no ser possible distingir-lo utilitzant el mètode estàndard.

Teorema 5.2.11. *Sigui $\epsilon(n)$ una seqüència de nombres reals que tendeix a zero quan $n \to \infty$. Aleshores, per a qualsevol n suficientment gran existeix un grup $H \subset S_n$ indistingible de mida $|H| \geq |S_n|^{\epsilon(n)}$.*

La resolució dels dos últims teoremes és complexa i es basa en el resultat següent juntament amb altres resultats de classificació de grups simples i acotacions de $m(H)$. Més detalls es poden consultar a la referència donada a l'inici de l'apartat, [KeS04].

Proposició 5.2.12. *Sigui $H \subseteq S_n$ un subgrup amb un grau mínim no constant. Suposem que per a cada $k \leq n$, H té com a màxim $n^{k/7}$ elements de suport k. Aleshores, H és indistingible.*

Demostració. Podem aplicar l'acotació del teorema 5.2.3 escrita de la forma $D_H \leq \sum_{1 \neq h \in H} |h^G|^{-1/2}$. Per $G = S_n$ i per a $h \in G$ de suport k tenim que $|h^G| > n^{ak}$, per a qualsevol nombre real $a < 1/3$ i per a n suficientment gran. Si denotem per H_k el conjunt $\{h \in H : \text{supp}(h) = h\}$ aleshores, $D_H < \sum_{k \geq m(H)} |H_k| n^{-bk}$ per a qualsevol nombre real $b < 1/6$ i per a n suficientment gran. Fixem b tal que $1/7 < b < 1/6$ i posem $c = b - 1/7, m = m(H)$. Aleshores,

$$D_H < \sum_{k \geq m} n^{k/7} n^{-bk} = \sum_{k \geq m} n^{-ck} \leq 2n^{-cm}.$$

Com que $m = m(H)$ és no constant, tenim que D_H és més petita que qualsevol potència negativa de n i, per tant, H és indistingible. □

Conjectures

Conjectura 5.2.13. Suposem que $H \subseteq S_n$ és distingible. Aleshores el grau minimal de H, $m(H)$, és constant.

Conjectura 5.2.14. Tot subgrup $H \subseteq S_n$ amb grau minimal no constant té com a màxim $n^{k/7}$ elements de suport k.

La proposició 5.2.12 demostra que la segona conjectura implica la primera.

Es pot veure que la segona conjectura es compleix per a grups primitius i grups generats a partir del producte en corona de dos grups $K \wr L$, si K satisfà la conjectura. A la vegada, el conjunt de subgrups que compleixen la segona conjectura és tancat sota productes directes.

Possibilitat de distingir dues involucions

Demostrarem que les distribucions que obtenim per a $H = \{1_{S_n}, m\}$ amb el mètode estàndard, on m és una involució, estan exponencialment properes a la distribució de $H = \{1_{S_n}\}$ i, per tant, no podem distingir els diferents subgrups H_m (cf. [MRS05]). Recordem que una involució m del grup simètric S_n és un element tal que $m^2 = 1_{S_n}$. Les involucions de S_n són permutacions que es descomponen en transposicions disjuntes o bé són la identitat.

Abans de discutir la possibilitat de distingir involucions explicarem els diagrames de Young. Les representacions irreductibles de S_n venen etiquetades per els *diagrames de Young*, o, equivelentment, les particions enteres de n, $\lambda = (\lambda_1, ..., \lambda_t)$, on $t = \sum_i \lambda_i = n$ i $\lambda_i \geq \lambda_{i+1}$ per a tot i. Denotarem per S^λ aquestes representacions irreductibles, per χ^λ els seus caràcters i per d_λ la seva dimensió. El *diagrama de Young conjugat*, $S^{\lambda'}$, s'obté permutant λ sobre la diagonal, $\lambda' = (\lambda'_1, ..., \lambda'_{\lambda_1})$, on $\lambda'_j = |\{i \mid \lambda_i \geq j\}|$. En particular, $\lambda'_1 = t$. Tenim que cada representació S^λ té una base en la qual la matriu té elements reals i, per tant, els seus caràcters són reals. Tot i això, en alguna altra base S^λ pot ser complexa. Denotarem per $(S^\lambda)^*$ la representació conjugada. Més informació sobre diagrames de Young i representacions de S_n es poden trobar a [Sag01].

Considerem que el subgrup amagat és $H = \{1, m\}$, on m és escollida uniformement de la classe de conjugació de involucions $M = M_n = \{\pi^{-1}((12)(34)\cdots(n-1n))\pi | \pi \in S_n\}$, on n és parell. Comencem mesurant el nom de la representació irreductible i obtenim S^λ per al diagrama λ. Sigui V l'espai vectorial associat a les representacions irreductibles. Podem escollir un POVM (cf. definició 4.3.2) amb el conjunt de generadors finit $B = \{\mathbf{b}_j \in S^\lambda | \ \mathbf{im}\ \mu_j \in \rho\}$ de V, on $\mu_j = |\mathbf{b}_j\rangle\langle\mathbf{b}_j| \otimes (\mathbb{1}/d_\rho)$. Escollim els pesos $\{a_j\}$ tal que satisfacin la condició de completesa $\sum_{\mathbf{b}_j \in B} a_j |\mathbf{b}_j\rangle\langle\mathbf{b}_j| = \mathbb{1}$. La probabilitat que observem el vector $\mathbf{b}_j$ si hem observat ρ ve donada per

$$P(\rho, \mathbf{b}_j) = a_j \frac{\|\Pi^\rho_{\mathbf{b}_j} |H\rangle\|^2}{P_\rho} = a_j \frac{\|\hat{H}(\rho)\mathbf{b}_j\|^2}{P_\rho} = a_j \frac{\|\Pi_H \mathbf{b}_j\|^2}{\mathbf{rk}\Pi_H},$$

on $\Pi^{\rho}_{\mathbf{b}_j} = \mu_j$. Recordem que $\Pi_H = (1/|H|)\sum_{h\in H}\rho(h)$ denota l'operador projecció en l'espai vectorial V.

Demostrarem que amb alta probabilitat la distribució condicionada induïda en els vectors de B és exponencialment a prop del que anomenarem *distribució natural en* B, $P(\rho, \mathbf{b}_j) = \frac{a_j}{d_\rho}$. La distribució natural en B correspon al cas on el subgrup amagat H és el subgrup trivial. D'aquí se segueix que necessitem un nombre exponencial d'experiments d'un únic registre per distingir 2 involucions i, de fet, per distingir-les de la identitat. Equivalentment, podem anomenar $B = \{\mathbf{b}\}$ i redefinir a_j com $a_{\mathbf{b}}$. Aleshores, la condició de completesa resulta com $\sum_{\mathbf{b}} a_{\mathbf{b}}|\mathbf{b}\rangle\langle\mathbf{b}| = \mathbb{1}$.

Sigui una constant c tal que $0 < c < 1/4$. Denotem per $\Lambda = \Lambda_c$ el conjunt de diagrames de Young, μ, tal que $\mu_1 \geq (1-c)n$ o $\mu'_1 \geq (1-c)n$. Denotem per E_0 l'esdeveniment que $d^\lambda \geq n^{dn}$. Tenim els següents resultats.

Lema 5.2.15. *Suposem que estem en el cas descrit per E_0. Per a $c < 1/4 < d < 1/2$ tenim que $\lambda \notin \Lambda$. També tenim que*

$$\frac{d^\lambda}{2}(1 - e^{-\alpha n}) \leq \mathbf{rk}\ \Pi_m \leq \frac{d^\lambda}{2}(1 + e^{-\alpha n}),$$

on $\Pi_m \boldsymbol{v} = \frac{\boldsymbol{v}+m\boldsymbol{v}}{2}$.

Lema 5.2.16. *Sigui L un subespai de $S^\lambda \otimes (S^\lambda)^*$ i Π_L l'operador projecció en L. Aleshores,*

$$\sum_{\mathbf{b}\in B} a_{\mathbf{b}} \|\Pi_L(\mathbf{b}\otimes\mathbf{b}^*)\|^2 \leq dim L.$$

Demostració. Primer, observem que un vector $e \in S^\lambda \otimes (S^\lambda)^*$ té components $e_{j,k}$ per a $1 \leq j,k \leq d^\lambda$. Existeix un operador lineal únic E en S^λ els elements de matriu del qual són $E_{j,k} = e_{j,k}$, i el producte escalar $\langle \mathbf{b}\otimes\mathbf{b}^*, e\rangle$ en $S^\lambda \otimes (S^\lambda)^*$ es pot escriure com la forma bilineal $\langle \mathbf{b}, E\mathbf{b}\rangle$ en S^λ. La norma de Frobenius de E és $\|E\|^2 = \mathrm{tr}(E^\dagger E) = \|e\|^2$.

Sigui $\{e_i\}$ una base ortonormal per L i sigui E_i l'operador corresponent a e_i. Aleshores,

$$\sum_{\mathbf{b}\in B} a_{\mathbf{b}}|\langle \mathbf{b}\otimes\mathbf{b}^*, e_i\rangle|^2 = \sum_{\mathbf{b}\in B} a_{\mathbf{b}}|\langle \mathbf{b}, E_i\mathbf{b}\rangle|^2 \leq \sum_{\mathbf{b}\in B} a_{\mathbf{b}}\|\mathbf{b}\|^2\|E_i\mathbf{b}\|^2 = \sum_{\mathbf{b}\in B} a_{\mathbf{b}}\|E_i\mathbf{b}\|^2.$$

Utilitzant la desigualtat de Cauchy-Schwarz i la condició de completitud, obtenim el resultat del lema. □

Passem ara a veure que no podem distingir el subgrup H_m del trivial.

Teorema 5.2.17. *Sigui $B = \{\mathbf{b}\}$ un conjunt de generadors finit amb pesos $\{a_{\mathbf{b}}\}$ que satisfà la condició de completesa per a les representacions irreductibles de S^λ. Considerem com a subgrup amagat $H = \{1, m\}$, on $m \in M$ és escollit uniformement. Sigui $P_m(\boldsymbol{b})$ la probabilitat d'observar el vector $\mathbf{b}$ condicionada a haver observat la representació anomenada S^λ. Sigui N la distribució natural en B. Aleshores, existeix una constant $\delta > 0$ tal que, per algun n suficientment gran i probabilitat com a mínim $1 - e^{-\delta n}$ en m i λ, tenim que*

$$\|P_m - N\|_1 < e^{-\delta n}.$$

Demostració. Recordem que la distribució condicional en B està donada per

$$P_m(\mathbf{b}) = \frac{a_{\mathbf{b}}\|\Pi_m \mathbf{b}\|^2}{\text{rk } \Pi_m},$$

on $\Pi_m := \Pi_{H_m}$. La distribució natural està donada per $N(\mathbf{b}) = \frac{a_{\mathbf{b}}}{d^\lambda}$.

Donat un subconjunt $A \subseteq B$, definim la mida ponderada d'A com $|A| = \sum_{\mathbf{b}\in A} a_{\mathbf{b}}$. Amb aquesta definició, la probabilitat total d'observar A sota la distribució natural és $N(A) = \frac{|A|}{d^\lambda}$.

Sigui $L \subset S^\lambda \otimes (S^\lambda)^*$ el subespai que consisteix en còpies de representacions S^μ amb $\mu \in \Lambda$. Sigui $B_L \subset B$ el conjunt de $\mathbf{b}$ amb la propietat que $\|\Pi_L(b \otimes b^*)\|^2 \geq e^{-\alpha n}$. Aleshores, el lema anterior implica que $|B_L| \leq e^{\alpha n} \dim L$. Denotem per B_{bad} el conjunt de $\mathbf{b} \in B \setminus B_L$ tal que

$$\left| \|\Pi_m \mathbf{b}\|^2 - \|\mathbf{b}\|^2 \frac{\mathbf{rk}\Pi_m}{\dim S^\lambda} \|\Pi_m \mathbf{b}\|^2 \right| \geq e^{-\alpha n/3}.$$

Aplicant les desigualtats de Chebyshev i Markov, l'esdeveniment E_1, definit com $|B_{\text{bad}}| < e^{-\alpha n/6} d^\lambda$, succeeix amb probabilitat almenys $1 - e^{-\alpha n/6}$.

Ara, tenim que

$$\|P_m - N\|_1 = \sum_{\mathbf{b}\notin B_L \cup B_{\text{bad}}} |P_m(\mathbf{b}) - N(\mathbf{b})| + \sum_{\mathbf{b}\in B_L \cup B_{\text{bad}}} |P_m(\mathbf{b}) - N(\mathbf{b})|.$$

Com que $\left| \|\Pi_m \mathbf{b}\|^2 - \|\mathbf{b}\|^2 \frac{\mathbf{rk}\Pi_m}{\dim S^\lambda} \|\Pi_m \mathbf{b}\| \right| < e^{-\alpha n/3}$, per a tot $\mathbf{b} \notin B_L \cup B_{\text{bad}}$, i $\sum_{\mathbf{b}} a_{\mathbf{b}} = d^\lambda$, si condicionem a l'esdeveniment E_0 obtenim que

$$\sum_{\mathbf{b}\notin B_L \cup B_{\text{bad}}} |P_m(\mathbf{b}) - N(\mathbf{b})| \leq \frac{e^{-\alpha n/3}}{\mathbf{rk}\ \Pi_m} d_\lambda \leq 4e^{-\alpha n/3},$$

aplicant el lema 5.2.15. D'aquí se segueix que $P_m(B_L \cup B_{bad})$ és com a màxim $|B_L \cup B_{bad}|/d^\lambda + 4e^{-\alpha n/3}$. Si suposem que estem en els casos E_1 i E_0, tenim que $|B_L \cup B_{bad}| \leq (n^{-\Omega(n)+e^{-\alpha n/6}})d^\lambda < 2e^{-\alpha n/6} d^\lambda$. Aleshores,

$$\sum_{\mathbf{b}\in B_L \cup B_{\text{bad}}} |P_m(\mathbf{b}) - N(\mathbf{b})| \leq P_m(B_L \cup B_{\text{bad}}) + N(B_L \cup B_{\text{bad}}) < 4e^{-\alpha n/6} + 4e^{-\alpha n/3} < 5e^{-\alpha n/6}.$$

Finalment, combinant aquestes desigualtats:

$$\|P_m - N\|_1 < 2e^{-\alpha n/3} + 5e^{-\alpha n/6} < 6e^{-\alpha n/6},$$

com a mínim, amb probabilitat $\Pr[E_0 \wedge E_1] \geq 1 - n^{-\gamma n} - e^{-\alpha n/6} \geq 1 - 2e^{-\alpha n/6}$. Si posem $\delta < \alpha/6$, queda provat el teorema. □

Qüestions obertes

Hi ha moltes preguntes encara sense resposta sobre el problema del subgrup amagat per a grups no abelians. En discutirem algunes de les més importants i plantejarem la possibilitat de resoldre el problema del subgrup amagat per a alguns grups no finits. El contingut d'aquestes pàgines és merament descriptiu i es podrien veure com nous temes per a una possible continuació d'aquest treball.

Per tal de resoldre el problema del subgrup amagat sembla necessari utilitzar la transformada quàntica de Fourier, que està definida en termes de representacions irreductibles de grups. Per al cas abelià totes les representacions irreductibles són de grau 1 i, per tant, queda unívocament definida ja que només podem agafar com a base aquestes representacions irreductibles, que coincideixen amb els caràcters. En canvi, per al cas de grups no abelians tenim com a mínim una representació irreductible de grau més gran que 1. Aleshores, la transformada de Fourier queda definida llevat de canvi de base. Aquest fet té implicacions directes en la resolució del problema ja que la quantitat d'informació addicional que podem obtenir en mesurar els índexs de la matriu, amb el mètode estàndard fort, pot dependre de l'elecció de la base (cf. [MRRS04]). També destacar la importància de poder distingir subgrups conjugats de manera eficient, fins i tot usant potser un altre mètode, ja que hem vist que aquest fet és un dels impediments per a la resolució del cas simètric. Un dels mètodes a considerar podria ser el de cerca binària, per a una partició que separi els subgrups conjugats.

Per a resoldre el problema del subgrup amagat per a grups abelians l'algoritme de Shor selecciona un morfisme exhaustiu $\nu : G \to Q$ que aproximi f. És a dir, selecciona una aplicació injectiva correcte $\tau : Q \to G$, tal que $\nu \circ \tau = \mathrm{Id}_Q$. Un cop definides aquestes aplicacions, podem definir una funció $\tilde{f}$ que aproxima f com $\tilde{f} = f \circ \tau$. Aleshores, podem utilitzar la transformada de Fourier de $\tilde{f}$ associada al grup Q per a trobar el subgrup amagat de $\tilde{f}$. Això ens donarà un conjunt de caràcters de Q que aproximen els caràcters de H. Una bona elecció de τ genera un algoritme eficient. En el cas de grups no abelians, però, no és clar com seleccionar τ correctament (cf. [LSK04]).

Pel que fa al problema per a grups infinits, caldria definir què vol dir un algoritme de temps polinòmic en aquest context. Per a grups infinits, no és possible comparar el temps d'execució amb $\log |G|$, ja que aquest valor no està definit per a grups amb cardinalitat infinita. En el cas de les representacions d'un grup G infinit, generalment hi ha infinites representacions irreductibles. Aquestes poden ser totes de dimensió finita, com és el cas dels grups abelians, o poden existir al-

gunes representacions irreductibles de dimensió infinita. Per exemple, en el cas de grups de Lie compactes com $SU(2)$, sabem que per a cada enter $m \geq 0$ existeix una representació irreductible de dimensió $m+1$ (cf. [Hal03]). Aquest fet té implicacions directes en el càlcul de la transformada de Fourier. Per exemple, anem a veure com seria la transformada de Fourier per al grup localment compacte de Heisenberg $2n+1-$dimensional (cf. [Tha04]). Aquest grup és un exemple de grup de Lie nilpotent. El grup de Heisenberg, H^n, és $\mathbb{C}^n \times \mathbb{R}^n$ amb el producte definit com

$$(z,t)(w,s) = \left(z+w, t+s+\frac{1}{2}\mathrm{Im}(z\cdot\overline{w})\right).$$

Hi ha dues famílies de representacions irreductibles i unitàries de grups de Heisenberg. Per una banda, totes les que tenen dimensió infinita i venen parametritzades per $\lambda \in \mathbb{R}\setminus\{0\}$. Per altra banda, tenim les representacions de dimensió finita que estan parametritzades per a $w \in \mathbb{C}^n$. Per a cada, $\lambda \in \mathbb{C}^n$ i per a cada $w \in \mathbb{R}\setminus\{0\}$, considerem l'operador $\pi_\lambda(z,t)$ que actua en $L^2(\mathbb{R}^2)$ per

$$\pi_\lambda(z,t)=\varphi(\theta)=e^{i\lambda t}e^{i\lambda(x\cdot\theta+\frac{1}{2}x\cdot y)\varphi(\theta+y)}, \quad z=x+iy,\ \varphi\in L^2(\mathbb{R}^n).$$

Com que el grup és no finit, tenim la següent transformada de Fourier per a $f \in L^2(SU(2))$ es defineix com la integral

$$\hat{f}(\lambda)=\int_{H^n} f(z,t)\pi_\lambda(z,t)\ dz\ dt.$$

Per realitzar aquesta integral sobre el grup de Heisenberg en un ordinador quàntic, seria necessari discretitzar l'espai d'integració. Això es deu al fet que els ordinadors quàntics operen amb estats quàntics en espais de dimensió finita, la qual cosa impedeix representar directament espais continus. Per tant, hauríem de construir dues xarxes: una per a cobrir $\mathbb{C}^n$ i l'altra per a cobrir $\mathbb{R}$. No obstant això, aquestes serien xarxes infinites, i hauríem de fer una altra aproximació; concretament, hauríem de truncar el domini i construir una bola al voltant de l'origen per a $\mathbb{C}^n$ i un interval per a $\mathbb{R}$, prou grans per incloure una part representativa de la funció. Aquesta aproximació permetria realitzar càlculs numèrics fins a un cert nivell de precisió, tenint en compte les limitacions derivades de les discretitzacions. En conseqüència, això comporta múltiples reptes, tant d'aproximació com d'implementació.

Cal destacar que s'han aconseguit avenços en els resultats sobre la possibilitat d'implementar la transformada de Fourier de grups de Lie sobre cossos finits (cf. [MRR03]). Considerem els grups $\mathbf{GL}(n,q)$, $\mathbf{SL}(n,q)$, $\mathbf{PGL}(n,q)$ i $\mathbf{PSL}(n,q)$, que són els grups corresponents sobre $\mathbb{F}_q$. En el cas de $\mathbf{GL}(n,q)$, tenim la següent seqüència d'inclusions:

$$\left(\begin{array}{c|c} A & v \\ \hline 0\ldots0 & c \end{array}\right)$$

Figura 5.1: P_k

$$\{1\} \subseteq \mathbf{GL}(n-1,q) \subseteq \mathbf{GL}(n-1,q)\times\mathbf{GL}(1,q) \subseteq P_n(q) \subseteq \mathbf{GL}(n,q).$$

on P_n és el subgrup parabòlic maximal definit per la matriu de la figura 5.1. El Teorema 1 de la referència citada implica que existeix un circuit quàntic de mida $q^{O(n)}$ per a la transformada quàntica de Fourier sobre aquests grups. Atès que $|G| = O(q^{n^2})$, podem escriure-ho com $|G|^{O(1/n)}$, que és $\exp(O(\sqrt{\log|G|}))$, si q és fix. Aquest resultat millora el cas clàssic. Tot i això, aquest fet no assegura que el temps d'execució sigui subexponencial.

Bibliografia

[BHMT02] Brassard G.; Høyer, P.; Mosca, M.; Tapp, A.: *Quantum amplitude amplification and estimation*. Quantum Computation and Information, American Mathematical Society, (2002), 53–74. url: http://dx.doi.org/10.1090/conm/305/05215, DOI: 10.1090/conm/305/05215.

[ChS24] Chen I.; Sun D.: *The dihedral hidden subgroup problem*. Journal of Mathematical Cryptology, **18**, 1, (2024). url: http://dx.doi.org/10.1515/jmc-2022-0029. DOI: 10.1515/jmc-2022-0029.

[EHK04] Ettinger, M.; Høyer P.; Knill, E.: *The Quantum Query Complexity of the Hidden Subgroup Problem Is Polynomial*. Information Processing Letters, **91**, 1, (2004), 43–48. url: https://doi.org/10.1016/j.ipl.2004.01.024. DOI: 10.1016/j.ipl.2004.01.024.

[GSVV04] Grigni, M.; Schulman, L.; Vazirani, M, Vazirani, U.: *Quantum Mechanical Algorithms for Nonabelian Hidden Subgroup Problem*. Combinatorica, **24**, (2004), 137–154. url: https://doi.org/10.1007/s00493-004-0009-8. DOI: 10.1016/j.ipl.2004.01.024.

[Hal03] Hall, B.: *Lie groups, Lie algebras and representations*. Graduate Texts in Mathematics, Springer, (2003). ISBN: 978-3-319-13466-6.

[Hall23] Hall, B.C: *Quantum Theory for Mathematicians*. Graduate Texts in Mathematics, Springer (2013). ISBN: 978-1-4614-7115-8.

[HoE99] Høyer P.; Ettinger M.: *On Quantum Algorithms for Noncommutative Hidden Subgroups*. STACS 99, Springer Berlin Heidelberg, (1999), 478–487. url: http://dx.doi.org/10.1007/3-540-49116-3_45. DOI: 10.1007/3-540-49116-3_45.

[KeS04] Kempe, J.; Shalev, A.: *The hidden subgroup problem and permutation group theory*. (2004). url: https://arxiv.org/abs/quant-ph/0406046.

[Kup11] Kuperberg, G: *Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem*. (2011). url: https://arxiv.org/abs/1112.3333.

[LSK04] Lomonaco, J.; Samuel J.; Kauffman, L.: *Quantum hidden subgroup algorithms: The devil is in the details*. Quantum Information and Computation II,

5436, SPIE(publisher), (2004), 137. url: http://dx.doi.org/10.1117/12.543921. DOI: 10.1117/12.543921.

[MRS05] Moore, C.; Russell, A.; Schulman, J.: *The Symmetric Group Defies Strong Fourier Sampling: Part I*, (2005). url: https://arxiv.org/abs/quant-ph/0501056.

[MRR03] Moore, C.; Russell, A.; Rockmore, D.; *Generic Quantum Fourier Transforms* (2003). url: https://arxiv.org/abs/quant-ph/0304064.

[MRRS04] Moore, C.; Rockmore, D.; Russel, A.; Schulman L.: *The power of basis selection in fourier sampling: hidden subgroup problems in affine groups*. Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms, (2004), 1113 -1122. url: https://arxiv.org/abs/quant-ph/0211124. DOI: 10.1145/982792.982957.

[MoR05] Moore, C.; Russell, A.: *For Distinguishing Conjugate Hidden Subgroups, the Pretty Good Measurement is as Good as it Gets*. Quantum Information and Computation, **7**, (2005). url: https://arxiv.org/abs/quant-ph/0501177. DOI: 10.26421/QIC7.8-5.

[New67] Newman, M: *Bounds for the number of generators of a finite group*. Journal of Research of the National Bureau of Standards Section B Mathematics and Mathematical Physics, **71**, (1967), 247. url: https://nvlpubs.nist.gov/nistpubs/jres/71B/jresv71Bn4p247_A1b.pdf.

[S-R22] Serrallonga Rosell, Guillem: *El problema del subgrup amagat*. Universitat de Barcelona, (2022). url: https://hdl.handle.net/2445/186863.

[Sag01] Sagan, B.: *The Symmetric Group. Representations, Combinatorial Algorithms, and Symmetric Functions.*. Graduate Texts in Mathematics, Springer, (2001). ISBN: 0-387-95067-2.

[Sak93] Sakurai, J.J.: *Modern Quantum Mechanics, Revised Edition*, Addison Wesley, (1993). ISBN: 978-0201539295.

[Serre12] Serre, Jean-Pierre: *Linear Representations of Finite Groups*. Graduate Texts in Mathematics, Springer, (2012). ISBN: 0-387-90190-6.

[SHO09] Scholz, E.: *Hilbert space*. Compendium of Quantum Physics, Springer Berlin Heidelberg, (2009), 404-405. url: https://doi.org/10.1007/978-3-540-70626-7_90. DOI: 10.1007/978-3-540-70626-7_90.

[Tha04] Thangavelu, S.: *An introduction to the uncertainty principle: Hardy's theorem on Lie groups*. Progress in mathematics, **217**, (2004). ISBN: 0817643303.

[Wei09] Weigert, S.: *No-Cloning Theorem*. Compendium of Quantum Physics, Springer Berlin Heidelberg, (2009), 404-405. url: https://doi.org/10.1007/978-3-540-70626-7_124. DOI: 10.1007/978-3-540-70626-7_124.