UNIVERSITAT DE BARCELONA
Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

ATAC QUÀNTIC A LA CRIPTOGRAFIA AMB CORBES EL·LÍPTIQUES

Autor: Laia Canal Guitart

Director: Sr. Eloi Sans Gispert
Realitzat a: Departament de matemàtiques i informàtica

Barcelona, 21 de juny de 2020

Abstract

Generally, the majority of classical cryptography methods that use elliptical curves are based on the difficulty of classical computers to solve the discrete logarithm problem in polynomial time. Here we will study Peter Shor's quantum attack derived from the algorithm for the discrete logarithm problem, published in 1994 [14]. We start with an introduction to elliptical curves and their use in criptography. Then we understand the mathematical foundations of the corresponding quantum computation to understand Shor's algorithm, from which we will study how to reach it and why it works.

Resum

En general, la criptografia clàssica que usa corbes el·líptiques basa el seu procés en la dificultat que té un ordinador clàssic per resoldre el problema del logaritme discret en temps polinòmic. En aquest treball estudiem l'atac quàntic derivat de l'algoritme pel problema del logaritme discret de Peter Shor, publicat l'any 1994 [14]. Comencem amb una introducció a les corbes el·líptiques i el seu ús en l'encriptació. Tot seguit entenem la base matemàtica de la computació quàntica necessària per entendre l'algoritme de Shor, del qual estudiem com s'hi arriba i perquè funciona.

2010 Mathematics Subject Classification. 94A60 , 81P94 , 11T71

Agraïments

En primer lloc m'agradaria agrair al meu tutor Eloi Sans haver acceptat ser el meu tutor i agafar el treball amb tant entusiasme i motivació. Vull agrair-li totes les hores que m'ha dedicat, la seva paciència i la seva bona disposició, sobretot en aquest context tan excepcional.
Voldria dedicar un càlid gràcies als meus pares, per tota la seva confiança i suport i sobretot, les ganes i esforç per voler entendre tot allò que els hi he compartit.
Moltes gràcies també, a totes les meves amigues i amics, per la seva ajuda constant, el seu recolzament, la seva cura i acompanyament, no només ara, sinó en tota l'etapa universitària.
I finalment, i no per això menys important, dedicar un agraïment molt especial a l'Adriana, qui de manera desinteressada ha estat allà en tot moment. Gràcies per les seves idees, consells i ajuda al llarg de tot el treball.

Índex

1 Introducció

Les corbes el·líptiques constitueixen actualment una àrea de recerca molt important, sobretot en els camps de la teoria de nombres i la criptografia. Sense anar més enllà, Andrew Wiles les va utilitzar per resoldre el darrer teorema de Fermat a finals del segle XX.
L'ús de les corbes el·líptiques per encriptar va ser proposat per Neal I.Koblitz i Victor Saul Miller als voltants dels anys vuitanta, però no va ser fins a començaments del 2000 quan es van començar a implementar els primers algoritmes.
La seva popularització es deu al fet que proporcionen una seguretat equivalent als models clàssics, com el model RSA, però usant menys espai de memòria. Tot i que existeix l'anàleg al cas RSA per corbes el·líptiques, la majoria de la criptografia clàssica que usa corbes el·líptiques, basa el seu procés en la dificultat que té un ordinador clàssic per resoldre el problema del logaritme discret en temps polinòmic.
En l'actualitat, la criptografia en corbes el·líptiques es fa servir per al xifrat d'informació, la firma digital o l'intercanvi de claus, i la podem trobar en camps tan diversos com el vot electrònic o la recent popular tecnologia blockchain.
Paral·lelament, a principis dels vuitanta també es despertava l'interès per la computació quàntica. Es considera que el físic Richard Feynman va ser dels primers en suggerir que un ordinador quàntic podia proporcionar més eficàcia algorísmica. Aquesta idea va agafar més força, arran de l'article publicat l'any 1982 per Paul Benioff on es demostrava que una màquina de Turing podia ser simulada a partir d'un procés quàntic [2]. L'any 1993 Dan Simon publicava per primera vegada en el seu paper, un algoritme que permetia resoldre en temps polinòmic, un problema que fins llavors requeria temps exponencial en un ordinador clàssic [17]. Aquest resultat va inspirar la publicació probablement més rellevant fins el moment. Peter Shor publicava l'any 1994 un algoritme que era capaç de resoldre el problema de factorització d'enters i el problema del logaritme discret [14]. Dos anys més tard en feia una correcció i millora [15]. Havia aparegut la possibilitat de trencar la seguretat de pràcticament tota la criptografia existent. Tot i així, encara que s'hagin fet alguns experiments, l'ordinador quàntic amb més potència creat fins el moment, ha estat de 53 qubits (54, de fet, però un va fallar durant l'experiment) [1].
Com a concepte bàsic, la computació quàntica suposa un canvi de paradigma respecte a la computació clàssica. Es treballa amb bits quàntics, normalment denominats qubits, en comptes de bits clàssics que prenen valors 0 o 1. Un qubit és un sistema quàntic amb dues possibles configuracions (com poden ser, per exemple, els espins d'un electró) que es troba en un estat que representa la probabilitat de trobar-se en cada una d'elles. És per això, que moltes vegades es parla de superposició quàntica.
Aquest treball vol seguir aquest mateix recorregut històric. Començarem per entendre diferents sistemes criptogràfics, així com la base teòrica de les corbes el·líptiques sobre la qual treballen. Continuarem per presentar i entendre la base matemàtica de la computació quàntica, veure la transformada de Fourier en la seva corresponent versió quàntica, i entendre la seva importància en la resolució dels algoritmes que porten a trencar el problema del logaritme discret. Veurem doncs, l'algoritme de Simon, una versió de l'algoritme de cerca de període i la seva relació amb l'algoritme de cerca d'ordre d'un grup, un breu incís sobre la seva relació amb l'algoritme de factorització d'enters de Shor, i per últim, una versió de l'algoritme del problema del logaritme discret de Shor. Acabarem amb un exemple aplicat a una corba el·líptica. Entendrem amb més detall perquè la computació quàntica aporta tants avantatges i veurem com, efectivament, arribat el dia en què les lleis de la física quàntica ho permetin, tota la criptografia que ara creiem segura, deixarà de ser-ho.

2 Corbes el·líptiques i criptografia

2.1 Definició i equació de Weierstrass

Denotarem per $\mathbb{P}^2_{\mathbb{K}}$ el pla projectiu sobre el cos $\mathbb{K}$. Cada classe d'equivalència de (x, y, z) es denota per $(x : y : z)$. Els punts $(x : y : z)$ amb $z \neq 0$ són els anomenats punts finits de $\mathbb{P}^2_{\mathbb{K}}$ o punts afins, fent referència a la inclusió de l'espai afí $\mathbb{A}^2_{\mathbb{K}}$ dins $\mathbb{P}^2_{\mathbb{K}}$. Així doncs, podem identificar els punts afins (x, y) amb els punts projectius $(x : y : 1)$. D'altra banda els punts de l'infinit són aquells de la forma $(x : y : 0)$, és a dir, amb tercera coordenada nul·la.

Definició 2.1. Una equació de Weierstrass generalitzada és una equació cúbica sobre $\mathbb{P}^2_{\mathbb{K}}$ de la forma

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{2.1}$$

on $a_1, ..., a_6$ constants pertanyents al cos $\mathbb{K}$.

Observació 2.2. Si el cos té característica diferent de 2 i 3 podem fer servir el canvi de variable:

$$(x : y : z) \to \left(\frac{x - 3a_1^2 - 12a_2}{36} : \frac{y - 3a_1x}{216} - \frac{a_1^3 - 4a_1a_2 - 12a_3}{240} : z \right) \tag{2.2}$$

Obtenim aleshores l'equació reduïda de Weierstrass

$$y^2z = x^3 + axz^2 + bz^3 \tag{2.3}$$

on $a, b \in \mathbb{K}$ constants.

Definició 2.3. Definim el discriminant de l'equació 2.3 com,

$$\Delta := -(4a^3 + 27b^2) \tag{2.4}$$

Considerarem a partir d'ara $\mathbb{K}$ un cos amb característica diferent de 2 i 3.

Definició 2.4. Una corba el·líptica E sobre $\mathbb{K}$ és una corba projectiva que té per equació projectiva l'equació reduïda de Weierstrass

$$y^2z = x^3 + axz^2 + bz^3 \tag{2.5}$$

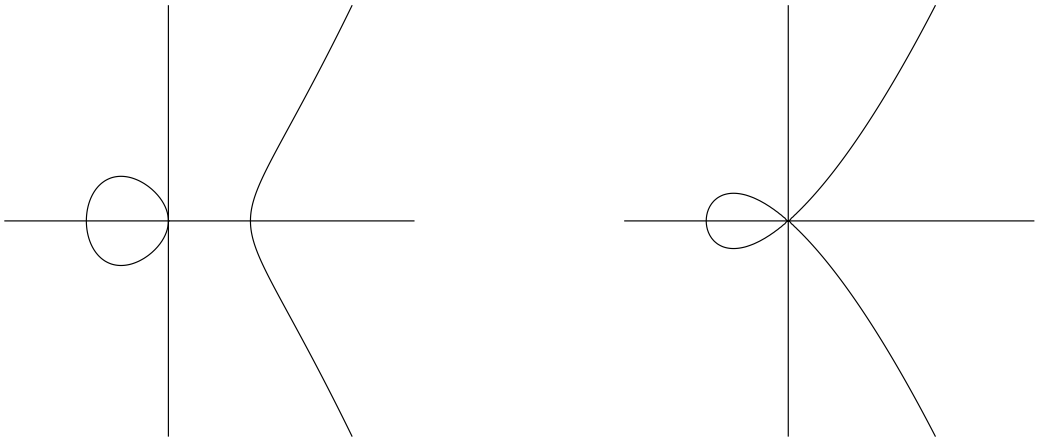
on $a, b \in \mathbb{K}$ constants i discriminant $\Delta \neq 0$.

Observació 2.5. Imposar que el discriminant sigui diferent de 0 equival a que la corba no tingui punts singulars.

Seguint l'argumentació inicial, veiem que si imposem $z = 0$, tenim $x^3 = 0$, i com que no podem tenir les tres coordenades nul·les arribem a que $O := (0 : y : 0) = (0 : 1 : 0)$ es correspon a l'únic punt de la corba que pertany al conjunt de punts de l'infinit de $\mathbb{P}^2_{\mathbb{K}}$. Aleshores podem agafar coordenades afins $X = x/z$ i $Y = y/z$ i mirar-nos doncs, la corba E, com a conjunt de punts $E(\mathbb{K})$ tals que:

$$E(\mathbb{K}) = \{O\} \cup \{(X, Y) \in \mathbb{A}^2_{\mathbb{K}} \ , \ Y^2 = X^3 + AX + B\} \tag{2.6}$$

Fixem-nos doncs que $E(\mathbb{K})$ denotarà la corba el·líptica E sobre el cos $\mathbb{K}$.



(a) $y^2 = x^3 - x$ (b) $y^2 = x^3 + x^2$

Figura 1: Comparació entre una corba el·líptica i una corba amb un punt singular

2.2 Llei de grup

Podem dotar $E(\mathbb{K})$ d'una operació binària $(+)$. La seva definició es deu a una construcció geomètrica. Anem a veure-la amb més detall per entendre-la.
Sigui $E(\mathbb{K})$ una corba el·líptica sobre $\mathbb{K}$. Siguin $P_1, P_2 \in E$ dos punts qualssevols. Tracem la recta L que uneix els punts P_1 i P_2 i considerem el punt d'intersecció R entre L i E. Sigui M la recta que passa per R i O. Aleshores es defineix la suma de $P_1 + P_2$ com el tercer punt d'intersecció entre M i E.
En cas que $P_1 = P_2 + O$, $L \cap E = \{O\}$, i $M \cap E = \{O\}$. Per tant tenim $O + O = O$. Per altra banda si $P_1 = O$, però $P_2 \neq O$, llavors $L = M$ i per tant $M \cap E = \{O, R, P_2\}$ i tenim $O + P_2 = P_2$.

Siguin $P_1 = (x_1, y_1)$ i $P_2 = (x_2, y_2)$. Calculem les expressions del procés anterior per trobar les coordenades exactes de $P_1 + P_2$. Comencem suposant que $x_1 \neq x_2$. Aleshores la recta L és de la forma,

$$y = m(x - x_1) + y_1$$

on m és el pendent, $m = \frac{y_2 - y_1}{x_2 - x_1}$.
Per trobar el punt d'intersecció amb E substituim a l'equació de Weierstrass que defineix E i tenim,

$$\begin{aligned}(m(x - x_1) + y_1)^2 &= x^3 + ax + b \\ 0 &= x^3 - m^2x^2 + \cdots\end{aligned}$$

Com x_1 i x_2 són arrels per construcció, tenim que amb la tercera arrel x_3 se satisfà,

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + \cdots$$

Per tant,

$$-(x_1 + x_2 + x_3) = -m^2 \Rightarrow x_3 = m^2 - x_1 - x_2$$

El tercer punt d'intersecció és doncs, $(m^2 - x_1 - x_2, m(x_3 - x_1) + y_1)$. Per trobar $P + Q$ només cal reflectir respecte l'eix d'abcisses ja que recordem que M té direcció $(1, 0)$. Per

tant $P_3 = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1)$.

Si $x_1 = x_2$, però $y_1 \neq y_2$, aleshores la recta L és vertical i per tant el tercer punt d'intersecció és O de manera que $M \cap E = \{O\}$ i $P_1 + P_2 = O$.

Finalment, si $P_1 = P_2$, L és la recta tangent a P_1, el pendent de la qual serà si derivem implícitament,

$$2y\frac{dy}{dx} = 3x^2 + a \;\Rightarrow\; m = \frac{dy}{dx} = \frac{3x^2 + a}{2y}$$

Els càlculs són idèntics als del principi, per tant, $P_3 = (m^2 - 2x_1, m(x_1 - x_3) - y_1)$, sempre i quan $y \neq 0$. Si $y = 0$, llavors la recta tangent és vertical i per tant passa per O. En aquest cas $P_1 + P_2 = P_1 + P_1 = O$.

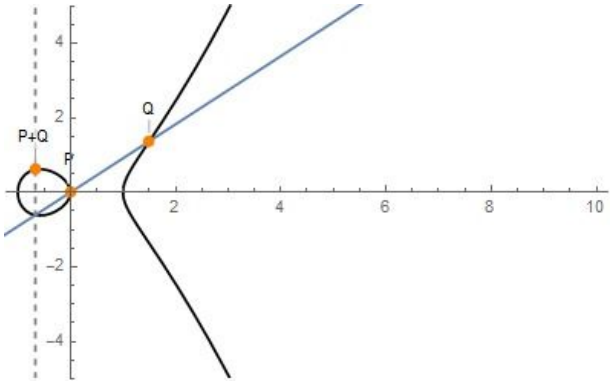


Figura 2: Suma de $P = (0, 0)$ i $Q = (3/2, \sqrt{15/8})$ en la corba el·líptica $y^2 = x^3 - x$

Definició 2.6. Sigui E una corba el·líptica amb equació afí $y^2 = x^3 + Ax + B$. Siguin $P_1 = (x_1, y_1)$ i $P_2 = (x_2, y_2)$ punts de E amb $P_1, P_2 \neq O$. Es defineix $P_1 + P_2 := P_3$ de la manera següent:

1. Si $x_1 \neq x_2$, aleshores

$$x_3 := m^2 - x_1 - x_2, \quad y_3 := m(x_1 - x_3) - y_1, \quad \text{on} \quad m = \frac{y_2 - y_1}{x_2 - x_1}$$

   Aleshores $P_3 := (x_3, y_3)$.

2. Si $x_1 = x_2$, però $y_1 \neq y_2$, aleshores $P_1 + P_2 = O$

3. si $P_1 = P_2$ i $y_1 \neq 0$, aleshores

$$x_3 := m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{on} \quad m = \frac{3x_1^2 + A}{2y_1}$$

   Aleshores $P_3 := (x_3, y_3)$

4. Si $P_1 = P_2$ i $y_1 = 0$, aleshores $P_1 + P_2 = O$.

5. Definim com a element neture el punt O, és a dir,

$$P + O = P \quad \text{per a tots els punts P de E.}$$

Observació 2.7. Sigui P un punt de la corba. Denotarem per conveniència $-P$, com l'element invers de P, és a dir aquell punt tal que, si existeix, $P + (-P) = O$.

Lema 2.8. *Sigui $E(\mathbb{K})$ el conjunt de corbes el·líptiques sobre el cos K. Aleshores $E(\mathbb{K})$ és tancat respecte la suma (+).*

Demostració. La demostració ve donada directament per la construcció de la suma. □

Teorema 2.9. *$(E(\mathbb{K}), (+))$ és un grup abelià.*

Demostració. La demostració es pot trobar a [16]. □

Sigui $\lambda \in \mathbb{Z}^+$. Denotarem per λP la suma de $P + \cdots + P$ punts de la corba. Fer la suma repetidament no resulta molt eficient, sobretot si λ pren valors molt grans. Existeixen algoritmes que optimitzen el càlcul de k vegades P, per exemple un d'ells és el següent:

Sigui λ un enter positiu i P un punt de E, aleshores,

1. Imposem les condicions inicials $a = \lambda$, $B = O$, $C = P$
2. Des de $a = \lambda$ fins a $a = 0$ actualitzem les variables de la manera següent:
   - Si a parell, fem $a = \frac{a}{2}$, $B = B$, $C = C + C$
   - Si a senar, fem $a = a - 1$, $B = B + C$, $C = C$

La solució és $B = \lambda P$

Definició 2.10. Direm que un punt $P \in E(\mathbb{K})$ és de torsió si l'ordre del subrup generat per P és finit.

Definició 2.11. Sigui $E(\mathbb{K})$ una corba el·líptica sobre $\mathbb{K}$ i n un enter. Aleshores definim el conjunt $E[n]$ com,

$$E[n] := \{P \in E(\overline{\mathbb{K}}) \mid nP = O\} \tag{2.7}$$

on $\overline{K}$ denota la clausura algebraica de $\mathbb{K}$.

Teorema 2.12. *Sigui $E(\mathbb{K})$ una corba el·líptica sobre $\mathbb{K}$ i $E[n]$ el conjunt definit com a 2.7. Aleshores,*

(i) Si la característica de $\mathbb{K}$ és 0 o no divideix n,

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \tag{2.8}$$

(ii) Si la característica de $\mathbb{K}$ és p on p divideix n, escrivim n de la forma $n = p^r n'$ on p no divideix l'enter n'. Aleshores,

$$E[n] \cong \mathbb{Z}/n'\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \quad o\ bé \quad \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \tag{2.9}$$

Demostració. La demostració es pot trobar a [16]. □

2.3 Corbes el·líptiques sobre cossos finits

Denotarem per $\mathbb{F}_q$ el cos finit d'ordre q, on q és potència d'un primer.

En criptografia s'utilitzen les corbes sobre cossos finits per la dificultat que suposa resoldre el problema del logaritme discret sobre ells. En general treballar amb cossos finits d'ordre q no és fàcil, per això moltes vegades s'agafen els cossos on q és primer o una potència de 2.

Exemple 2.13. Sigui $\mathbb{K} = \mathbb{F}_7$. Sigui $y^2 = x^3 + 2$ l'equació de Weierstrass definida sobre $\mathbb{F}_7$. Tenim que $\Delta = -(4 \cdot 1 + 27 \cdot 2^2) = -112 \neq 0$, per tant l'equació defineix una corba el·líptica sobre $\mathbb{F}_7$. Aleshores,

$$E(\mathbb{F}_7) = \{O, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}$$

Resulta interessant estudiar l'estructura del grup de punts sobre la corba, ja que ens dóna una idea general de com és.

Veiem dos dels resultats més clàssics en aquest camp que ens seran útils més endavant.

Teorema 2.14. *Sigui E una corba el·líptica sobre $\mathbb{F}_q$. Aleshores*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \quad o \quad E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \tag{2.10}$$

per un cert enter $n \geq 1$ o enters $n_1, n_2 \geq 1$ tals que $n_1 | n_2$.

Demostració. Podem aplicar el teorema de l'estructura de grups abelians finitament generats vist a estructures algebraiques. $E(\mathbb{F}_q)$ és un grup abelià finit, per tant existeixen un nombre natural r i enters positius $n_1, \ldots, n_s$ amb n_i dividint n_{i+1} per a $1 \leq j < s$ tals que

$$E(\mathbb{F}_q) = \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_s\mathbb{Z}$$

En particular, l'ordre de $E(\mathbb{F}_q)$ és igual al producte $n_1 \cdots n_s$.
Com $\mathbb{Z}/n_i\mathbb{Z}$ té n_1 elements d'ordre un divisor de n_1, tenim que $E(\mathbb{F}_q)$ té n_1^s elements d'ordre un divisor de n_1.
Pel teorema 2.12, $E(\mathbb{F}_q)$ en té com a màxim n_1^2 (seria el cas $E[n_1] \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_1\mathbb{Z}$), per tant, $r \leq 2$. □

Observació 2.15. Fixem-nos que tots els punts d'una corba el·líptica sobre un cos finit, són de torsió.

Teorema 2.16. *(Hasse) Sigui E una corba el·líptica sobre el cos finit $\mathbb{F}_q$. Aleshores l'ordre de $E(\mathbb{F}_q)$ satisfà,*

$$\left|q + 1 - \#E(\mathbb{F}_q)\right| \leq 2\sqrt{q} \tag{2.11}$$

A [18] o [16] podem trobar una discussió més detallada sobre com trobar o aproximar l'ordre de $E(\mathbb{F}_q)$, així com les demostracions dels teoremes clàssics anteriors, però com veurem més endavant, existeix un algortime quàntic que troba l'ordre d'un grup així que no hi entrarem amb més profunditat.

2.4 El problema del logaritme discret

Anem a veure en què consisteix i com es fa servir per encriptar.

Definició 2.17. Sigui $(G, \cdot)$ un grup cíclic d'ordre n. Sigui b un generador de G. Aleshores per cada element $g \in G$ tenim que $g = b^k$ per una certa $k \in \mathbb{Z}$. Definim el logaritme discret en base b com l'aplicació

$$\begin{aligned} Log_b : G &\to (\mathbb{Z}/n\mathbb{Z}) \\ g &\to \overline{k} \end{aligned} \tag{2.12}$$

on $(\mathbb{Z}/n\mathbb{Z})$ denota l'anell dels nombres enters mòdul n i $\overline{k}$ la classe d'equivalència de l'enter k a $(\mathbb{Z}/n\mathbb{Z})$.

Observació 2.18. En el cas de les corbes el·líptiques el problema es tradueix en trobar el valor k tal que $g = bk$ on g és el generador del grup cíclic $(G, +)$ i $b \in G$ un element del grup.

Proposició 2.19. *El logaritme discret és un isomorfisme de grups.*

Demostració. Fixem-nos que l'aplicació està ben definida.
Ara, prenem $\overline{k_1}$, $\overline{k_2}$ dues classes d'equivalència de $\mathbb{Z}/n\mathbb{Z}$ tals que $Log_b(g) = \overline{k_1}$ i $Log_b(g) = \overline{k_2}$. Tenim doncs $b^{k_1} = b^{k2} \pmod{n}$. Forçosament $k_1 \equiv k_2 \pmod{n}$, per tant l'aplicació és injectiva.
L'exhaustivitat ve donada pel propi fet que b sigui generador de G, ja que per tota classe d'equivalència $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ existeix un element s del grup G tal que $s = b^{\overline{k}}$. □

El problema del logaritme discret o DLP *(discrete logarithm problem)* té com a objectiu trobar el valor de k donat un element g del grup G. Existeixen diferents maneres d'usar el problema en criptografia. Segons les propietats del grup tindrem més o menys dificultats.

2.4.1 Atacs clàssics al DLP

Una manera d'atacar el problema és amb el mètode del Baby Step, Giant Step. Aquest algoritme creat per Daniel Shanks és força senzill i funciona sempre i quan l'ordre del grup sigui petit.

Algoritme 1. Donat un grup cíclic G d'ordre n, el seu generador P i un element Q, el següent algoritme troba l'enter k tal que $kP = G$.

1. Fixem un enter $m \geq \sqrt{n}$ i calculem mP. En cas que no coneguem n podem aprofitar el teorema de Hasse i agafar un m tal que $m^2 \geq (q + 1 + 2\sqrt{q})$.
2. (Baby step) Fem una llista de tots els iP per a $0 \leq i \leq m - 1$.
3. (Giant step) Calculem els punts $Q - jmP$ per a $0 \leq j \leq m-1$ fins que un coincideixi amb un element de la llista creada al pas anterior.
4. Sigui i l'índex tal que $iP = Q - jmP$. Tenim que k satisfà $0 \leq k < m^2$ Aleshores definint $k := k_0 + mk_1$ on $k = k_0 \pmod{m}$ tindrem $0 \leq k_0 < m$ i $k_1 = (k - k_0)/m$. Aleshores
$$Q - k_1 mP = kP - k_1 mP = k_0 P$$
Per tant $Q = kP$ amb $k \equiv i + jm \pmod{n}$.

En el cas particular de corbes el·líptiques podem aprofitar el fet que un punt de la corba P i el seu oposat $-P$ tenen la mateixa coordenada x. Aleshores només cal emmagatzemar els punts iP del pas 2 per $i = 0, \cdots, m/2$ i conseqüentment avaluar si $Q - jmP = \pm iP$. Necessitem doncs la meitat d'espai i menys càlculs.

Altres atacs són una mica més complicats i no els veurem amb exactitud, però si resulta interessant veure la seva complexitat per entendre la necessitat de la cerca d'un algoritme més eficient, que acabarem veient al final del treball.
Sigui n l'ordre del grup sobre el qual tractem el problema. Alguns dels atacs existents i que funcionen en el cas específic de corbes el·líptiques són,

- Cerca exhaustiva, amb una complexitat de $\mathcal{O}(n)$.
- Baby step, Giant step, amb una complexitat de $\mathcal{O}(\sqrt{n})$.
- Mètode de la Rho de Pollard i mètode de la Lambda de Pollard amb una complexitat de $\mathcal{O}(\sqrt{n})$.La diferència respecte l'anterior és que aquests són mètodes probabilístics i no determinístics.
- Mètode de Pohlig-Hellman. Sigui $\prod_i p_i^{e_i}$ la descomposició en factors primers de n, aleshores l'algoritme té una complexitat de $\mathcal{O}(\sum_i e_i(log(n) + \sqrt{p_i}))$.

2.5 Criptografia clàssica

Distingim dos tipus d'encriptació: la de clau secreta i la de clau pública, també conegudes per criptografia simètrica i asimètrica. En el primer cas, la clau per encriptar i desencriptar és la mateixa, d'aquí la referència a simètric. Alguns dels exemples més populars són el DES o l'AES, més popularment conegut com Rijndael.
La criptografia simètrica pot semblar-nos poc segura a primera vista, però amb una bona tria de clau, pot arribar a ser-ho tant com alguns mètodes d'encriptació amb clau pública.

2.5.1 Intercanvi de claus Diffie Hellman

Un procés molt utilitzat en el qual dos usuaris A i B extreuen una clau per xifrar és l'intercanvi de claus Diffie Hellman.

Algoritme 2.

1. A i B trien conjuntament una corba el·líptica E definida sobre $\mathbb{F}_q$. També trien un punt $P \in E(\mathbb{F}_q)$ tal que el subgrup generat per P tingui un ordre considerablement gran (preferiblement un primer).
2. A escull en privat un enter a, calcula $P_a := aP$ i l'envia B.
3. B escull en privat un enter b, calcula $P_b := bP$ i l'envia a A.
4. A calcula $aP_b = abP$.
5. B calcula $bP_a = abP$.
6. Els dos trien de forma pública quin mètode d'encriptació simètric volen utilitzar a partir de la clau abP.

Un observador només veu aP i bP, per tant només pot desencriptar si aconsegueix resoldre el problema del logaritme discret per trobar a o b i així obtenir la clau abP.

2.5.2 El Gamal

Vegem ara un ús del logaritme discret en un sistema d'encriptació de clau pública. Aquest algoritme es pot definir per qualsevol grup finit G. Per l'enfoc del treball, agafarem el cas en què $G = E(\mathbb{F}_q)$.
Suposem que A vol enviar un missatge a B.

Definició 2.20. La clau pública ElGamal consisteix en $(E(\mathbb{F}_q), P, B)$ on P és un punt de la corba $E(\mathbb{F}_q)$ i $B := sP$ on s és un enter que forma part de la clau privada que crea l'usuari emissor B.

Definició 2.21. La clau privada ElGamal és l'enter s que tria B.

Algoritme 3.

1. B construeix la clau pública $(E(\mathbb{F}_q), P, B)$ (implícitament queda construïda la clau privada s).
2. B publica la clau pública que A es descarrega per encriptar el seu missatge.
3. A codifica el seu missatge com un punt $M \in E(\mathbb{F}_q)$.
4. A tria un enter aleatori k i calcula $B' := kP$
5. A encripta el seu missatge com
$$M_1 := kP$$
$$M_2 := M + B'$$
6. A envia el missatge xifrat (M_1, M_2) a B.
7. B desencripta el missatge usant $M_2 - sM_1$. Això funciona ja que
$$M = M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M$$

Un observador només podrà llegir el missatge si és capaç de calcular el logaritme discret de sP o kP.

2.5.3 ECIES

Un altre sistema d'encriptació de clau pública és l'*ECIES (Elliptic Curve Integrated Encryption Scheme)*. Fa servir un tipus de funció molt utilitzada en criptografia, les funcions hash.

Definició 2.22. Una funció Hash és una funció que té com a entrada una sèrie de dades amb una llargada arbitrària i com a sortida una cadena de valors d'una llargada determinada. És per això que en català se la coneix també com a funció resum.

Suposem que A vol enviar un missatge a B.

Definició 2.23. La clau pública del sistema *ECIES* consisteix en $(E(\mathbb{F}_q), N, P, B)$ on P és un punt de la corba $E(\mathbb{F}_q)$ d'ordre N, i $B := sA$ on s és un enter que forma part de la clau privada que crea l'usuari emissor B.

Definició 2.24. La clau privada del sistema *ECIES* és l'enter s que tria B.

Algoritme 4.

1. B construeix la clau pública $(E(\mathbb{F}_q), N, P, Q)$. Implícitament queda construïda la clau privada s.
2. A i B decideixen conjuntament dues funcions d'encriptació hash H_1, H_2 i una funció d'encriptació simètrica E_k que depèn d'una certa k que triarà A en privat.
3. B publica la clau pública que A es descarrega per encriptar el seu missatge.
4. A tria un enter aleatori k tal que $1 \leq k \leq N-1$ i calcula $R : kP$ i $Z := kQ = k(sP)$.
5. A calcula $H_1(R, Z)$ a partir de $k_1||k_2$, on k és la mesura del nombre concatenat (és a dir, $||$ serveix per denotar la concatenació de dos nombres, per exemple $123456 = 123||456$ i la mesura és 6).
6. Sigui m el missatge codificat. A calcula $C = E_{k_1}(m)$ i $t = H_2(C, k_2)$ i envia el misssatge encriptat (R, C, t) a B.
7. B calcula $Z := sR$ gràcies al coneixement de la clau privada s. Després l'utilitza per calcular $H_1(R, Z)$ i escriu el resultat $k_1||k_2$.
8. B calcula $H_2(C, k_2)$. Si no coincideix amb t, atura el procés. En cas contrari, segueix al pas següent,
9. B desencripta el missatge a partir de la funció de desencriptació D_k corresponent a E_k.
$$m = D_{k_1}(C)$$

Fixem-nos que el pas 8 aporta més seguretat al procés, ja que en molts sistemes criptogràfics un atacant pot forçar a B a desencriptar i deduir la clau privada. Un altre avantatge d'aquest sistema és que no es necessita codificar el missatge com un punt de la corba, cosa que redueix dificultat en el procés.

2.5.4 Signatura digital ElGamal

Suposem que A vol firmar un document que ha enviat a B telemàticament. El mètode tradicional de la signatura escrita no resulta molt útil si el que es busca és assegurar l'autenticitat de l'autoria d'un document digital.
Una signatura digital és un mecanisme de xifrat que dóna solució a aquesta necessitat.

Igual que abans, aquest mètode és un sistema d'encriptació amb clau pública i és vàlid per a qualsevol grup cíclic, però agafarem el cas en què $G = E(\mathbb{F}_q)$.

Definició 2.25. La clau pública de la Sigantura el Gamal consisteix en el conjunt d'elements $(E, \mathbb{F}_q, f, P, Q)$ on E és una corba el·líptica sobre F_q, $P \in E(\mathbb{F}_q)$ un punt de la

corba d'ordre N, $Q := aP$ on a és un enter que forma part de la clau privada i f una funció

$$f : E(\mathbb{F}_q) \to \mathbb{Z} \tag{2.13}$$

Definició 2.26. La clau privada de la Signatura el Gamal és l'enter a que tria l'usuari que signa el document.

Suposem que A vol signar un document que ha enviat a B.

Algoritme 5.

1. A construeix i publica la clau pública $(E, \mathbb{F}_q, f, P, Q)$ que es descarrega el receptor B.
2. A codifica el seu document com un enter m. En cas que A vulgui encriptar també el document en si, pot fer servir qualsevol dels mètodes esmentats anteriorement, entre d'altres.
3. A tria de manera aleatòria un enter k tal que $mcd(k, N) = 1$ i calcula $R := kP$.
4. A calcula $s \equiv k^{-1}(m - af(R)) \pmod{N}$.
5. A envia el document signat (m, R, s). Fixem-nos que (R, s) són el que constitueix la signatura digital.
6. B calcula $V_1 := f(R)B + sR$ i $V_2 := mP$.
7. Si $V_1 = V_2$ dóna la signatura per vàlida. Ho pot assegurar ja que,

$$skA = (m - af(R))P + zNP = (m - af(R))P + O = (m - af(R))A$$

on hem utilitzat que $sk = m - af(R) + zN$. Per tant,

$$V_1 = f(R)B + sR = f(R)aP + skP = f(R)aP + (m - af(R))P = mP = V_2$$

3 Computacio quàntica

3.1 Conceptes previs

3.1.1 Espai de Hilbert

Definició 3.1. Un espai prehilbertià és un espai vectorial E sobre un cos $\mathbb{K}$ amb un cert producte hermític $\langle\ ,\ \rangle$. És a dir, una aplicació

$$\begin{aligned} \langle\ ,\ \rangle :& E \times E \longrightarrow \mathbb{R} \\ & (u,v) \longrightarrow \langle u,v\rangle \end{aligned} \tag{3.1}$$

tal que

1. $\langle u,v\rangle = \langle v,u\rangle^* \quad \forall u,v \in \mathbb{K}$.
2. $\langle \lambda u + \mu v, w\rangle = \lambda \langle u,w\rangle + \mu \langle v,w\rangle \quad \forall u,v,w \in E,\ \lambda,\mu \in \mathbb{K}$.
3. $\langle u,u\rangle \geq 0 \quad \forall u \in E - \{0\}$ i $\langle u,u\rangle = 0$ si, i només si, $u = 0$.

Definició 3.2. Un espai de Hilbert és un espai prehilbertià complet respecte la norma induïda pel producte hermitià.

Observem que si $\mathbb{K} = \mathbb{R}$, el producte hermitià es correspondria amb el ja conegut producte escalar, amb les propietats de simetria, bilinealitat i la qualitat de ser una aplicació definida positiva habituals. D'ara en endavant considerarem sempre $\mathbb{K} = \mathbb{C}$.

Exemple 3.3. $\mathbb{C}^n$ és un espai de Hilbert finit de dimensió n amb el corresponent producte hermitià,

$$\langle (a_1,\cdots,a_n),(b_1,\cdots b_n)\rangle = \sum_{k=0}^{n-1} a_k^* b_k \tag{3.2}$$

Proposició 3.4. *Siguin* $(X,\|\ \|_1)$ *i* $(Y,\|\ \|_2)$ *dos espais normats sobre* $\mathbb{K}$ *i* $T : X \to Y$ *una aplicació lineal. Aleshores són equivalents,*

(i) T *és contínua.*

(ii) T *és contínua en 0.*

(iii) Existeix una constant $C \geq 0$ *tal que* $\big\|T(x)\big\| \leq C\|x\|$ *per* $x \in X$, $C \in \mathbb{K}$.

Definició 3.5. Sigui T un operador lineal i continu entre espais normats X i Y. Aleshores definim la norma de T com

$$\|T\| := \sup_{\|x\|\leq 1} \big\|T(x)\big\| \tag{3.3}$$

Teorema 3.6. *(Riesz) Sigui* H *un espai de Hilbert i* $f \in H'$. *Aleshores existeix un únic* $u \in H$ *tal que* $f(x) = \langle u,x\rangle$ *per a tot* $x \in H$. *Tenim a més, que* $\|f\| = \|u\|$ *i l'aplicació* $H' \ni f \mapsto u \in H$ *és una bijecció isomètrica antilinear.*

Proposició 3.7. *Siguin* H_1 *i* H_2 *dos espais de Hilbert, i* $T \in \mathcal{L}(H_1,H_2)$ *una aplicació lineal de* H_1 *en* H_2, *llavors,*

$$\|T\| = sup\left\{\big|\langle T(x),y\rangle\big|\ ;\ \|x\|,\|y\| \leq 1\right\} = sup\left\{\langle T(x),y\rangle\ ;\ \|x\| = \|y\| = 1\right\} \tag{3.4}$$

Teorema 3.8. *(Existència de l'operador adjunt). Siguin H_1 i H_2 espais de Hilbert i $T : H_1 \to H_2$ una operador lineal i continu. Aleshores existeix un únic operador lineal i continu $T^\dagger : H_2 \to H_1$ tal que*

$$\langle T(x), y\rangle = \langle x, T^\dagger(y)\rangle \tag{3.5}$$

per a tot $x \in H_1$ i $x \in H_2$. A més a més, $\|T\| = \left\|T^\dagger\right\|$.

Demostració 3.9. Fixat un $y \in H_2$ definim l'aplicació lineal $f_y : H_2 \to \mathbb{K}$ com $f_y(w) := \langle w, y\rangle$ per a tot $w \in H_2$. Per la desigualtat de Cauchy-Schwarz tenim que

$$\left|\langle y, T(x)\rangle\right| \leq \|y\|\|T\|\|x\| \tag{3.6}$$

prenent $C = \|y\|\|T\|$ tenim f_y contínua.
Considerem l'aplicació $f_y \circ T : H_1 \to \mathbb{K}$. Tenim que és lineal i contínua per construcció. Pel teorema de Riesz, existeix $z \in H_1$ tal que

$$\langle T(x), y\rangle = f_y(T(x)) = \langle x, z\rangle \tag{3.7}$$

Si definim $T^\dagger(y) := z$, aleshores $T^\dagger : H_2 \to H_1$ és lineal i a més,

$$sup\left\{\left|\langle T(x), y\rangle\right| ; \|x\| ,\|y\| \leq 1\right\} = sup\left\{\left|\langle x, T^\dagger(y)\rangle\right| ; \|x\| ,\|y\| \leq 1\right\}, \tag{3.8}$$

per tant apliquem la proposició 3.7 i tenim $\left\|T^\dagger\right\| = \|T\|$.

Definició 3.10. Sigui H un espai de Hilbert i $T \in \mathcal{L}(H)$. A l'operador $T^\dagger$ l'anomenarem operador adjunt. A més,

(i) T es diu auto-adjunt si $T^\dagger = T$

(ii) T es diu unitari si és invertible i $T^\dagger = T^{-1}$

Observació 3.11. Suposem $H = \mathbb{C}^n$. Sigui $T \in \mathcal{L}(\mathbb{C}^n)$ l'operador lineal amb forma matricial una matriu $M^{\mathbb{C}}_{n\times n}$ expressada en una certa base. Aleshores la matriu associada a l'operador adjunt serà la transposada de la matriu conjugada, és a dir, $M^\dagger = (M^*)^T$. Se l'anomena matriu hermítica.

3.1.2 Producte tensorial

El producte tensorial és un dels conceptes més importants de l'àlgebra multilineal.
Recordem que $E* = \mathcal{L}(E, \mathbb{K}) = \{f : E \to \mathbb{K} \mid \text{f lineal }\}$ denota l'espai dual de E. Per parlar del producte tensorial hem d'introduir l'espai vectorial dels tensors. Considerem E un espai vectorial de dimensió n sobre un cos $\mathbb{K}$ i $\{e_1, \cdots, e_n\}$ la base canònica de E.

Definició 3.12. Un tensor p-covariant de E és una aplicació p-lineal (és a dir, lineal en les p components)

$$f : E \times \cdots \times E \to \mathbb{K} \tag{3.9}$$

Un tensor q-contravariant de E és una aplicació q-lineal

$$f : E^* \times \cdots \times E^* \to \mathbb{K} \tag{3.10}$$

Anomenem $T_p(E) := \mathcal{L}_p(E^p, \mathbb{K})$ al conjunt de tensors p-covariants i $T^q(E) := \mathcal{L}_q(E^{*q}, \mathbb{K})$ al conjunt de tensors q-contravariants.

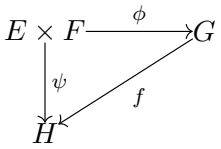
Observació 3.13. 1. $T_1(E) = \mathcal{L}_1(E, \mathbb{K}) = E^*$ és l'espai dual de E.

2. $T_2(E) = \mathcal{L}_2(E^2, \mathbb{K}) = \{f : E \times E \mid \text{f bilineal } \}$. Fixem-nos doncs, que el producte escalar en E és un tensor 2-covariant.

3. $T^1(E) = \mathcal{L}_1(E^*, \mathbb{K}) = \{f : E^* \to \mathbb{K} \mid \text{f lineal } \} = E^{**}$ és el bidual de E. Recordem que si dim $E \leq \infty$, aleshores el monomorfisme canònic $i : E \to E^{**}$ definit per $i(x) = \hat{x}$ on $\hat{x}$ és l'aplicació $\hat{x} : E \to \mathbb{K}$ on $\hat{x}(w) = w(x)$ és un isomorfisme. Així, de forma natural, considerarem $T^1(E) = E^{**} = E$

Considerem dos espais vectorials E, F sobre un cos $\mathbb{K}$ tals que $dimE = n$ i $dimF = m$. Siguin $\{u_1, \cdots, u_n\}$ i $\{v_1, \cdots, v_m$ les seves respectives bases.

Notació. *Anomenarem un parell a (G, ϕ) on G és un espai vectorial sobre $\mathbb{K}$ i $\phi : E \times F \to G$ és una aplicació bilineal. Un morfisme de parells $f : (G, \phi) \to (H, \psi)$ de (G, ϕ) a (H, ψ) és una aplicació lineal $f : G \to H$ tal que $f \circ \phi = \psi$, és a dir, que fa commutatiu el diagrama*



Definició 3.14. Sigui $x \in E$ que s'identifica amb $\hat{x} \in E^{**}$ i $y \in F$ que s'identifica amb $\hat{y} \in F^{**}$. Aleshores definim el producte tensorial de x i y com,

$$\begin{aligned} x \otimes y : E^* \times F^* &\to \mathbb{K} \\ (w, \rho) &\to (x \otimes y)(w, \rho) = (\hat{x} \otimes \hat{y})(w, \rho) = \hat{x}(w)\hat{y}(\rho) = w(x)\rho(y) \end{aligned} \tag{3.11}$$

on $w \in E^*$ i $\rho \in F^*$. Dit d'una altra manera, $x \otimes y$ és un element de $\mathcal{L}_2(E^* \times F^*, \mathbb{K})$.

Proposició 3.15. *Sigui $\tau : E \times F \to \mathcal{L}_2(E^* \times F^*, \mathbb{K})$ definida com $\tau(x, y) := x \otimes y$ per a tota $x \in E$ i $y \in F$. Aleshores $(\mathcal{L}_2(E^* \times F^*, \mathbb{K}), \tau)$ és un parell.*

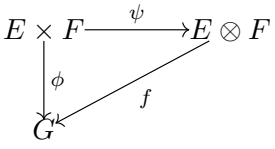
Es pot comprovar, a més a més que $\{\tau(u_i, v_j)\}_{i,j} = \{u_i \otimes v_j\}_{i,j}$ és una base de $\mathcal{L}_2(E^* \times F^*, \mathbb{K})$. En particular, $dim\mathcal{L}_2(E^* \times F^*, \mathbb{K}) = nm$. Denotarem doncs $\mathcal{L}_2(E^* \times F^*, \mathbb{K}) = E \otimes F$.

Definició 3.16. Un producte tensorial de E i F és un parell (G, ϕ) que compleix la propietat següent: per a cada parell (H, ψ) existeix un únic morfisme de parells

$$f : (G, \phi) \to (H, \psi) \tag{3.12}$$

Aquesta propietat s'anomena la propietat universal del producte tensorial.

Observació 3.17. El producte tensorial fa commutatiu el diagrama :



Teorema 3.18. *El producte tensorial és únic llevat d'isomorfisme. A més a més són equivalents,*

1. *(G, ψ) és el producte tensorial de E i F.*
2. *Existeixen una base u de E i una base v de F amb $\{\psi(u_i, v_j)\}_{i,j}$ base de G.*
3. *Per a qualsevol base u de E i base v de F, $\{\psi(u_i, v_j)\}_{i,j}$ és base de G.*

Corol·lari 3.19. *El parell $(E \otimes F, \tau) = (\mathcal{L}_2(E^* \times F^*, \mathbb{K}), \tau)$ amb*

$$\tau : E \times F \to \mathcal{L}_2(E^* \times F^*, \mathbb{K}) \tag{3.13}$$

definida per $\tau(x, y) = x \otimes y$ és el producte tensorial de E i F.

Per a més detalls i demostracions es pot consultar [11].
Acabem aquest apartat amb unes últimes observacions que seran d'especial importància quan entrem a la secció de computació quàntica.

Exemple 3.20. Siguin $E = F = \mathbb{C}^2$. Siguin $\{v_1, v_2\}$ i $\{w_1, w_2\}$ les respectives bases de cada un. Aleshores

$$\{v_1 \otimes w_1, v_1 \otimes w_2, v_2 \otimes w_1, v_2 \otimes w_2\} \tag{3.14}$$

serà una base de $\mathbb{C} \otimes \mathbb{C}$. A més a més $dim(\mathbb{C}^2 \otimes \mathbb{C}^2) = 4$ i pel teorema 3.18 sabem que l'espai és únic llevat d'isomorfisme, per tant al ser els dos sobre $\mathbb{C}$ tenim $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$.

Exemple 3.21. Siguin $A = \mathcal{M}_{n\times m}(\mathbb{C})$ i $B = \mathcal{M}_{s\times r}(\mathbb{C})$ dues matrius sobre $\mathbb{C}$ tals que

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \quad \text{i} \quad B = \begin{pmatrix} b_{11} & \cdots & b_{1r} \\ \vdots & \ddots & \vdots \\ b_{s1} & \cdots & b_{sr} \end{pmatrix}$$

Aleshores,

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \cdots & a_{nm}B \end{pmatrix} \in \mathcal{M}_{ns\times mr}(\mathbb{C})$$

El producte tensorial en el cas de les matrius també s'anomena producte de Kronecker.

Definició 3.22. Siguin V, W dos espais de Hilbert tals que $dimV = n$ i $dimW = m$. Definim de manera natural el producte hermitià en $V \otimes W$ com

$$\langle \sum_{i=0}^{nm-1} \lambda_i a_i \otimes b_i, \sum_{j=0}^{nm-1} \mu_i a'_i \otimes b'_i \rangle := \sum_{i,j} \lambda_i^* \mu_j \langle a_i, a'_i \rangle \langle b_i, b'_i \rangle \tag{3.15}$$

A partir d'aquí ja tenim intrínsicament totes les propietats enunciades anteriorment d'espais de Hilbert.

3.2 Qubit i postulats de la física quàntica

Definició 3.23. Un qubit és un espai de Hilbert H de dimensió 2 amb el corresponent producte hermitià

$$\langle (a_0, a_1), (b_0, b_1) \rangle = (a_0^* b_0, a_1^* b_1) \tag{3.16}$$

Denotarem la base canònica ortonormal seguint la notació de Dirac:

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \ , \ |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{3.17}$$

Utilitzarem aquesta mateixa notació per denotar tota la resta de vectors. Podem doncs, expressar un vector arbitrari del sistema com:

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle \text{ on } a_0, a_1 \in \mathbb{C}. \tag{3.18}$$

Més generalment, podem considerar un sistema de n qubits de la següent manera,

Definició 3.24. Un sistema de n qubits és un espai de hilbert H isomorf al producte tensorial de n qubits,

$$\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \cong \mathbb{C}^{2^n}$$

amb el corresponent producte hermitià

$$\langle (a_0, \cdots, a_{2^n-1}), (b_0, \cdots, b_{2^n-1}) \rangle = \sum_{i=0}^{2^n-1} a_i^* b_i. \tag{3.19}$$

Igual que abans, denotarem els elements de la base canònica com l'expressió binària dels nombres de 0 a 2^n-1. És una bona manera de veure que els vectors de la base canònica d'un sistema de n qubits són el producte tensorial dels vectors de la base canònica de n qubits. Fixem-nos que un element de la base serà aleshores un estat $|x_{n-1} \cdot \cdots \cdot x_0\rangle$ on $x_i \in \{0, 1\} \ \forall \ i \in \{0, \ldots, n-1\}$.
Pel que fa a la notació, són equivalents:

$$|a\rangle \otimes |b\rangle = |a\rangle |b\rangle = |ab\rangle$$

Definició 3.25. Sigui H un sistema de n qubits. Un estat és un vector unitari del sistema.

Definició 3.26. Sigui H un sistema de n qubits i B_H una base ortonormal de H. Anomenarem estats ben definits als vectors de B_H. A vegades els elements la base canònica $\{|0\rangle, \cdots, |2^n - 1\rangle\}$ també s'anomenen estats purs. Qualsevol altre vector que sigui combinació d'elements de la base es dirà que està en un estat de superposició.

Exemple 3.27. Sigui $|\psi\rangle$ un estat d'un sistema de n qubits que es troba en superposició.

$$|\psi\rangle = \sum_{j=0}^{2^n-1} c_j |j\rangle \text{ on } c_j \in \mathbb{C} \quad \text{i} \quad \sum_{j=0}^{2^n-1} |c_j| = 1$$

Aleshores parlarem de c_j com l'amplitud de $|\psi\rangle$. La podem escriure com $c_j = a_j e^{i\theta_j}$ on $a_j \in \mathbb{R}$ i $0 \leq \theta_j < 2\pi$, on θ_j es defineix com la fase.

Observació 3.28. Aquestes definicions resulten naturals si tenim en compte els postulats de la física quàntica. Físicament, sabem que en fer una observació d'un qubit en estat de superposció, aquesta anirà a parar sempre a un dels estats base. Prenem com exemple $|\Psi\rangle$ un estat arbitrari de dimensió 2 definit com a 3.17. Podem concebre $|a_0|^2$,$|a_1|^2$ com les probabilitats on el qubit es troba en un dels estats ben definits en el moment de l'observació. Veiem que aquesta interpretació és consistent amb el fet que les diferents probabilitats sumin 1, ja que el vector és unitari.
Sigui doncs H un sistema de n qubits, $B_H = \{\omega_0, \cdots, \omega_{2^n-1}\}$ una base ortonormal del sistema. Sigui $|\psi\rangle = a_0 |\omega_0\rangle, \cdots, a_{2^n-1} |\omega_{2^n-1}\rangle$. Definim per χ_{B_H} la variable aleatòria associada a H i B_H com la variable aleatòria amb espai mostral els diferents estats de B_H i distribució multinomial, és a dir,

$$\begin{aligned} P : \Omega &\longrightarrow [0,1] \\ P(\chi_{B_h} = |j\rangle) &= |a_j|^2 \end{aligned} \tag{3.20}$$

Fer una observació és doncs, fer un experiment aleatori i obtenir un valor experimental χ_{B_H}, diem-li $|j\rangle$. Després de l'observació, el sistema passa a estar a l'estat $|j\rangle$.

Exemple 3.29. Sigui $\{|+\rangle, |-\rangle\}$ la base ortonormal definida per: $|\pm\rangle := \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$. Sigui l'estat $|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle = \frac{a_0+a1}{\sqrt{2}} |+\rangle + \frac{a_0-a_1}{\sqrt{2}} |-\rangle$. Si fem una observació d'aquest estat respecte aquesta base obtindrem l'estat $|+\rangle$ amb probabilitat $\frac{|a_0+a_1|^2}{2}$ i l'estat $|-\rangle$ amb probabilitat $\frac{|a_0-a_1|^2}{2}$

Tot i que es poden fer observacions en diverses bases ortonormals, la dificultat de dur-les a terme fa que normalment s'utilitzi la base canònica.

3.3 Portes i circuits quàntics

Els ordinadors clàssics consisteixen en una sèrie de diferents circuits elèctrics basats en la composició de diverses portes lògiques. Tenint en compte que els elements d'un ordinador clàssic són els bits, elements de $(\mathbb{Z}/2\mathbb{Z})$, podem modelitzar les portes lògiques com aplicacions

$$f : (\mathbb{Z}/2\mathbb{Z})^r \to (\mathbb{Z}/2\mathbb{Z})^s \tag{3.21}$$

Exemple 3.30. Vegem algunes de les portes lògiques més conegudes,

- La porta *AND*

$$\begin{aligned} (\mathbb{Z}/2\mathbb{Z})^2 &\to (\mathbb{Z}/2\mathbb{Z}) \\ (x,y) &\mapsto xy \ = \ \min\{x,y\} \end{aligned} \tag{3.22}$$

- La porta *XOR*

$$\begin{aligned} (\mathbb{Z}/2\mathbb{Z})^2 &\to (\mathbb{Z}/2\mathbb{Z}) \\ (x,y) &\mapsto x+y \end{aligned} \tag{3.23}$$

- La porta *NOT*

$$\begin{aligned} (\mathbb{Z}/2\mathbb{Z}) &\to (\mathbb{Z}/2\mathbb{Z}) \\ (x,y) &\mapsto x+1 \end{aligned} \tag{3.24}$$

- La porta *OR*

$$\begin{aligned}(\mathbb{Z}/2\mathbb{Z})^2 &\to (\mathbb{Z}/2\mathbb{Z}) \\ (x,y) &\mapsto \max\{x,y\}\end{aligned} \tag{3.25}$$

El conjunt de portes $\{NOT, AND\}$ o el conjunt $\{NOT, OR\}$ formen el que s'anomena un conjunt universal. És a dir, a partir d'elles es pot construir qualsevol altra porta lògica.
Moltes vegades es parla directament dels conjunts de portes *NAND* i *NOR* La porta *NAND* és aquella que aplica *AND* i despres la nega aplicant *NOT*, i la porta *NOR* que anàlogament fa la negació de la porta *OR*.

De la mateixa manera, un ordinador quàntic es basa en circuits quàntics, constituïts per portes quàntiques. Resulta natural intentar adaptar el model anterior, però les lleis físiques imposen algunes restriccions.

1. $U : \mathbb{C}^n \to \mathbb{C}^n$ ha de transformar un estat quàntic en un altre estat quàntic.
2. U ha de ser una transformació lineal (i.e $U(|x_1\rangle + |x_2\rangle) = U|x_1\rangle + U|x_2\rangle$. En altres paraules, U és una matriu.

Sigui $|\psi\rangle$ un estat de partida. Fixem-nos què passa si es compleixen aquestes dues premisses:

$$\langle\psi|\psi\rangle = 1, (U|\psi\rangle)^\dagger U|\psi\rangle = 1$$

i

$$\begin{aligned}&(U|\psi\rangle)^\dagger U|\psi\rangle = 1 \\ &\Rightarrow |\psi\rangle^\dagger U^\dagger U|\psi\rangle = 1 \\ &\Rightarrow \langle\psi|U^\dagger U|\psi\rangle = 1 \\ &\Rightarrow U^\dagger U = I\end{aligned}$$

En definitiva U ha de ser una transformació unitària. Ara ja podem entendre el perquè de la següent definició.

Definició 3.31. Una porta quàntica de n qubits o universal és l'aplicació d'una transformació unitària U als estats dels n qubits, és a dir,

$$U : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n} \tag{3.26}$$

Observació 3.32. Fer una observació no es correspon amb cap transformació unitària.

3.3.1 Portes simples o transormacions d'un qubit

Definició 3.33. Una porta quàntica simple és l'apliació d'una transformació unitària a un qubit, és a dir,

$$U : \mathbb{C}^2 \to \mathbb{C}^2 \tag{3.27}$$

Exemple 3.34. Vegem algunes de les portes quàntiques més conegudes. Assumim que prenem com a base ortonormal la base canònica $\{|0\rangle, |1\rangle\}$ per expressar les seves formes matricials.

- La porta *NOT*,
$$NOT := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

- La porta Z,
$$Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- La porta *Hadamard* H,
$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$
Una altra manera de visualitzar H que pot resultar útil és la següent. Sigui $|j\rangle \in \{|0\rangle, |1\rangle\}$
$$|j\rangle \mapsto \frac{(|0\rangle + e^{2\pi i 0.j} |1\rangle)}{\sqrt{2}}$$
on $0.j$ denota l'expressió de la fracció binària $j \cdot \frac{1}{2}$ La porta *Hadamard* és una de les portes més utilitzades per la seva qualitat de crear superposició. Observem a més, que la porta *Hadamard* transforma $|0\rangle \to |+\rangle$ i $|1\rangle \to |-\rangle$.

- La porta de desplaçament de fase R_θ, on $\theta \in [0, 2\pi)$
$$R_\theta := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

- La porta $\pi/8$, també denotada per T,
$$T := \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}.$$
que no deixa de ser un cas particular de R_θ molt usat a vegades.

Notació. *Normalment es fa servir el següent diagrama per representar les diferents portes quàntiques on a vegades, vindran respresentats els estats anteriors i posteriors a la transformació.*

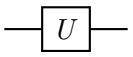


Figura 3: Diagrama corresponent a la transformació unitària U

Figura 4: Diagrama corresponent a la transformació unitària *NOT*

3.3.2 Portes de dos qubits

Definició 3.35. Una porta quàntica de dos qubits és l'apliació d'una transformació unitària

$$U : \mathbb{C}^4 \to \mathbb{C}^4 \tag{3.28}$$

Com podríem intuir, podem crear portes de dos qubits fent el producte tensorial entre dues portes simples. Siguin V i W dues portes quàntiques simples i $H \cong \mathbb{C}^4$ un sistema de dos qubits. Siguin $|v\rangle$ i $|w\rangle$ dos qubits, aleshores pel que hem vist anteriorment del producte tensorial,

$$V \otimes W(|v\rangle \otimes |w\rangle) = V(|v\rangle) \otimes W(|w\rangle) \tag{3.29}$$

Observació 3.36. No hem de confondre les portes de més d'un qubit amb un circuit quàntic. Un circuit es basa en la composició seqüencial de diverses portes quàntiques, mentre que una porta quàntica de dos o més qubits no deixa de ser l'aplicació, a la vegada, de diferents portes simples. És per això que molt sovint es parla de paral·lelisme quàntic. Aquest és el fet que ens permet poder avaluar una funció en diferents valors a la vegada.

Exemple 3.37. Sigui H la porta *Hadamard* simple. Prenem com a base del sistema la base canònica. Tenim doncs,

$$H^{\otimes 2} := H \otimes H(|00\rangle) = |+\rangle \otimes |+\rangle = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} \tag{3.30}$$

Altres vegades ens interessarà tenir portes que ens permetin implementar la condició "Si A és cert, llavors B". Aquest tipus de transformacions són dutes a terme per portes que s'anomenen controlades.

Sigui U una porta simple amb forma matricial $M_U = \begin{pmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{pmatrix}$.

Una porta controlada $C_U^{i,j}$ és una porta que opera sobre dos qubits de manera que i actua com a qubit de control i j com a objectiu, en el qual s'hi aplica la transformació U. Normalment s'agafa $i, j = 1, 2$.

$$C_U^{1,2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x_{00} & x_{01} \\ 0 & 0 & x_{10} & x_{11} \end{pmatrix} \tag{3.31}$$

Exemple 3.38. La més important dins del grup de portes controlades és la porta $C_{NOT}^{1,2}$ per la seva propietat d'universalitat que veurem més endavant.

$$C_{NOT}^{1,2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{3.32}$$

Per raons de practicitat moltes vegades es denota $C_{NOT}^{1,2} = C_{NOT}$.

Vegem un últim exemple que també resultarà útil

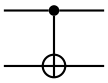


Figura 5: Porta controlada *CNOT*. El cercle negre indica el qubit de control i el blanc el qubit objectiu

Exemple 3.39. La porta *SWAP* o porta S. Aqueta porta intercanvia el valor de dos qubits. Suposem que $|j\rangle$ i $|k\rangle$ són dos estats ben definits. Aleshores $S(|jk\rangle) = |kj\rangle$. La seva forma matricial en la base canònica és

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

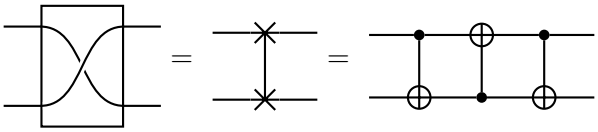


Figura 6: Tres representacions equivalents de la porta *SWAP*

3.3.3 Portes de n qubits

Definició 3.40. Una porta quàntica de n qubits és l'apliació d'una transformació unitària

$$U : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n} \tag{3.33}$$

Igual que abans, podem considerar el producte tensorial de n portes simples. En els exemples utilitzarem la base canònica $\{|0\rangle, \ldots, |2^n - 1\rangle\}$.

Exemple 3.41. Sigui x un estat pur del sistema ($x \in \{|0\rangle, \cdots, |2^n - 1\rangle\} \forall i \in 0, \cdots, n-1$). Denotem per H_{x_k} la porta *Hadamard* aplicada al qubit x_k. Tenim que,

$$H^{\otimes n} := H_{x_0} \otimes H_{x_1} \otimes \cdots H_{x_{n-1}} = \bigotimes \frac{(|0\rangle + (-1)^{x_i} |1\rangle)}{\sqrt{2}} = \frac{1}{2^{\frac{n}{2}}} \sum_{s \in \{0,1\}} (-1)^{\sum_{i=0}^{n-1} s_i x_i} |s\rangle \tag{3.34}$$

De la mateixa manera podrem generalitzar les portes controlades sobre n qubits amb k qubits de control on evidentment $k < n$. Dos exemples d'aquest cas seran els següents:

Exemple 3.42. (Porta *Toffoli*) La porta *Toffoli* és una porta quàntica que actua sobre 3 qubits on els 2 primers fan de control. Sobre els estats ben definits aplica la porta NOT al tercer qubit si els dos primers es troben en l'estat $|1\rangle$.
La seva forma matricial ve donada per

$$\textit{Toffoli} := \begin{pmatrix} I_{6\times 6} & 0 \\ 0 & NOT \end{pmatrix} \tag{3.35}$$

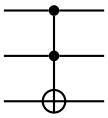


Figura 7: Diagrama de la porta *Toffoli*

Exemple 3.43. (Porta *Fredkin*) La porta *Fredkin* és un altre exemple de porta controlada de 3 qubits que, sobre els estats ben definits, aplica la porta $SWAP$ al segon i tercer qubit en cas que el primer estigui en l'estat $|1\rangle$.
La seva forma matricial ve donada per

$$Fredkin := \begin{pmatrix} I_{4\times 4} & 0 \\ 0 & SWAP \end{pmatrix} \tag{3.36}$$

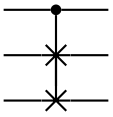


Figura 8: Diagrama de la porta *Fredkin*

3.4 Lògica reversible

És interessant preguntar-se si podem adaptar qualsevol algoritme clàssic en un algoritme quàntic. A causa de la reversabilitat de la computació quàntica, implementar un algoritme clàssic en un ordinador quàntic és possible només si aquest és reversible.
Afortunadament s'ha estudiat molt sobre la computació reversible i s'ha vist que tot procés determinista es pot fer de manera reversible (es pot trobar l'explicació amb més detall a [7]). No només això, sinó que coneixem portes o conjunts universals de portes dins la computació reversible. Dues d'elles són la porta *Toffoli* i la porta *Fredkin* introduïdes abans.

Vegem com actua la porta *Toffoli* sobre 3 bits:

$$(a, b, c) \to (a, b, ab \oplus c)$$

Si volem recuperar l'estat de partida només cal que tornem a aplicar la porta *Toffoli*.

$$(a, b, ab \oplus c) \to (a, b, ab \oplus ab \oplus c) = (a, b, c)$$

Fixem-nos que quan $c = 1$, el tercer bit de sortida equival a la imatge de la porta $NAND$ aplicada als 2 primers bits. La qualitat d'universalitat de la porta $NAND$ indueix la qualitat d'universalitat a la porta *Toffoli*. Podem doncs, expressar totes les portes clàssiques només amb portes *Toffoli* i alguns bits addicionals.
De forma anàloga podríem veure que les portes AND i NOT poden ser creades per la porta *Fredkin*, demostrant així que també és una porta universal. Observem que el fet que les portes *Toffoli* i *Fredkin* siguin reversibles és el que ens permet tenir-les com a portes quàntiques sense problema.

En resum, hem vist que podem computar un circuit clàssic fent servir un circuit quàntic a partir de portes *Toffoli* o *Fredkin* i alguns qubits addicionals.
En particular això ens diu que podrem aplicar una transformació que apliqui una certa funció $f(x)$, sempre i quan guardem el valor x. Més específicament, tenim el següent teorema:

Teorema 3.44. *Sigui $g : \{0,1\}^n \to \{0,1\}^m$ una funció computable per un circuit clàssic de mida S. Aleshores existeix un circuit quàntica que opera sobre $n + m + \mathcal{O}(S)$ qubits, fet a partir de portes $CNOT$ i alguns qubits addicionals, que computa una transformació unitària U_g tal que per a tot $x \in \{0,1\}^n$,*

$$U_g(|x\rangle\,|0,\ldots,0\rangle\,|0,\ldots,0\rangle) = |x\rangle\,|g(x)\rangle\,|0,\ldots,0\rangle$$

on el primer registre és de longitud n, el segon de longitud m i el tercer $\mathcal{O}(s)$.

Demostració. La demostració es pot trobar a [13] □

4 Algoritme de Shor

4.1 Transformada de Fourier quàntica

Definició 4.1. Donat un vector $x \in \mathbb{C}^n$ es defineix la transformada de fourier discreta com la transformació de x a un vector y tal que,

$$y_k := \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} w^{kj} x_j \tag{4.1}$$

on $w = e^{\frac{2\pi i}{n}}$

De manera pràcticament anàloga trobem la transformada de Fourier en el cas quàntic.

Definició 4.2. Sigui H un sistema de n qubits. Es defineix la transformada de fourier quàntica QFT *(Quantum Fourier Transform)* d'ordre N sobre els estats de la base canònica $\{|0\rangle, \cdots, |2^n - 1\rangle\}$ com la transformació d'estats següent,

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} w^{jk} |k\rangle \tag{4.2}$$

on $N = 2^n$ i $w = e^{\frac{2\pi i}{N}}$

Veiem doncs, que per un estat arbitrari tindrem,

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{2^n-1} y_k |k\rangle \tag{4.3}$$

on $y_k := \frac{1}{\sqrt{N}} \sum_{k=0}^{2^n-1} w^{jk} x_j$

Proposició 4.3. *La transformada de Fourier quàntica és una transformació unitària.*

Demostració. Sigui H un sistema de n qubits. En el fons, aplicar la transformada de Fourier és en realitat fer un canvi de base. Veure que és una transformació unitària equival doncs, a veure que la nova base és ortonormal. Considerem dos estats de la base canònica als quals se'ls ha aplicat la QFT

$$|i\rangle \to |s\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} w^{il} |l\rangle \qquad |j\rangle \to |t\rangle = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} w^{jm} |m\rangle \tag{1}$$

Tenim que

$$\langle s|t\rangle = \frac{1}{N} \sum_{l=0}^{N-1} \sum_{m=0}^{N-1} w^{il-jm} \langle l|m\rangle = \frac{1}{N} \sum_{l=0}^{N-1} \sum_{m=0}^{N-1} w^{l(i-j)} \tag{2}$$

a causa de l'ortonormalitat de bases.

- Si $i = j$ és obvi que $\langle s|t\rangle = 1$
- Si $i \neq j$, $\langle s|t\rangle$ es tracta d'una suma geomètrica $\langle s|t\rangle = \frac{1}{N}\left(\frac{1-w^{(i-j)N}}{1-w^{i-j}}\right)$ que és nul·la per ser w una arrel N-èssima de la unitat.

□

Un cop sabem que la QFT és una transformació unitària, ens proposem a trobar el seu corresponent circuit quàntic.

Proposició 4.4. *Sigui H un sistema de n qubits, $|j\rangle$ un element de la base canònica amb la corresponent expressió binària $|j\rangle = |j_{n-1}, \cdots, j_0\rangle$. La transformada de Fourier definida anteriorment és equivalent a la següent transformació*

$$|j\rangle = |j_{n-1} \cdot \cdots \cdot j_0\rangle \longrightarrow \frac{(|0\rangle + e^{2\pi i 0.j_0}|1\rangle)(|0\rangle + e^{2\pi i 0.j_1 j_0}|1\rangle)\cdots(|0\rangle + e^{2\pi i 0.j_{n-1}j_{n-2}\cdots j_0}|1\rangle)}{\sqrt{2^n}} \tag{4.4}$$

Demostració. Agafem la transformada de Fourier definida com a 4.2. Tenim llavors que

$$\begin{aligned}
|j\rangle &\longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i j k}{2^n}} |k\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_{n-1}=0}^{1} \cdots \sum_{k_0=0}^{1} e^{2\pi i j \sum_{l=0}^{n-1} k_l 2^{(l-n)}} |k_{n-1} \cdots k_0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_{n-1}=0}^{1} \cdots \sum_{k_0=0}^{1} \bigotimes_{l=0}^{n-1} e^{2\pi i j k_l 2^{(l-n)}} |k_l\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{l=0}^{n-1} \left(\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{(l-n)}} |k_l\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{l=0}^{n-1} \left(|0\rangle + e^{2\pi i j 2^{(l-n)}} |1\rangle \right) \\
&= \frac{(|0\rangle + e^{2\pi i 0.j_0}|1\rangle)(|0\rangle + e^{2\pi i 0.j_1 j_0}|1\rangle)\cdots(|0\rangle + e^{2\pi i 0.j_{n-1}j_{n-2}\cdots j_0}|1\rangle)}{\sqrt{2^n}}
\end{aligned} \tag{1}$$

On hem jugat bàsicament amb l'expressió binària dels nombres i les propietats del producte tensorial. □

Teorema 4.5. *Podem aplicar la transformada de Fourier en un sistema de n qubits a través de portes Hadamard i de desplaçament de fase controlades.*

Demostració. Considerem la transformada de Fourier definida com a la proposició (afegir etiqueta prop).
Considerem la porta de desplaçament de fase controlada de dos qubits següent:

$$C_R^{s,t} := C_{R_{\theta_{s,t}}}^{s,t} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta_{s,t}} \end{pmatrix}$$

on $\theta_{s,t} = \pi/2^{t-s}$. Recordem també que H_i denota l'aplicació de la porta Hadamard al qubit i. Prenem ara el qubit $|j\rangle$ que estem intentant transformar. Fixem-nos què passa

quan apliquem la seqüència de portes $H_{n-1}C_{R_{n-2}}$ a $|j\rangle$. A efectes pràctics, només estem canviant el primer qubit, j_{n-1}.

$$|j_{n-1}\cdots j_0\rangle \xrightarrow{H_{n-1}} \frac{|0\rangle + e^{2\pi i 0.j_{n-1}}|1\rangle}{\sqrt{2}}|j_{n-2}\cdots j_0\rangle \xrightarrow{C_R^{n-2,n-1}} \frac{|0\rangle + e^{2\pi i 0.j_{n-2}j_{n-1}}|1\rangle}{\sqrt{2}}|j_{n-2}\cdots j_0\rangle$$

Seguim aplicant R_k per a $k = \{n-2,\ldots,0\}$. És a dir,

$$\begin{aligned}|j_{n-1}\cdots j_0\rangle &\xrightarrow{H_{n-1}} \frac{|0\rangle + e^{2\pi i 0.j_{n-1}}|1\rangle}{\sqrt{2}}|j_{n-2}\cdots j_0\rangle \\ &\xrightarrow{C_R^{n-2,n-1}C_R^{n-3,n-1}\cdots C^{0,n-1}} \frac{|0\rangle + e^{2\pi i 0.j_0\cdots j_{n-2}j_{n-1}}|1\rangle}{\sqrt{2}}|j_{n-2}\cdots j_0\rangle\end{aligned}$$

Podem aplicar el mateix procediment per cada qubit. Al final tindrem la següent seqüència de portes:

$$\begin{aligned}&H_{n-1}C_R^{n-2,n-1}C_R^{n-3,n-1}\cdots C_R^{0,n-1}H_{n-2}C_R^{n-3,n-2} \\ &\cdots C_R^{0,n-2}H_{n-3}C_R^{n-4,n-3}\cdots C_R^{0,n-3}\cdots H_1C_R^{0,1}H_0.\end{aligned}$$

Vegem que obtenim la transformació de l'equació 4.4, però amb els bits invertits. És per això que l'últim pas és aplicar la porta $SWAP$ per tenir exactament el que volem. □

A partir de la demostració anterior queda clar quin és l'esquema de l'algoritme.

Algoritme 6. *(Transformada de Fourier per un sistema de n qubits.* Partim de l'estat $|j\rangle = |j_{n-1}\cdots j_0\rangle$.

1. Implementem l'estat inicial del circuit.
2. Apliquem la següent seqüència de portes

   $$H_iC_R^{i-1,i}\cdot\cdots\cdot C_R^{0,i}$$

   des de $i = n-1$ fins a $i = 1$
3. Apliquem la porta *Hadamard* al qubit 0.
4. Apliquem la porta swap que intercanvia els qubits i i $n-i-1$ per a i des de $i = 0$ fins a $i = \frac{n-1}{2} - 1$ si n senar i des de $i = 0$ fins a $i = \frac{n}{2} - 1$ si n és parell.

Exemple 4.6. Sigui H un sistema de tres qubits i $|\psi\rangle = |x_2x_1x_0\rangle$ un estat arbitrari. Volem aplicar la transformada de Fourier quàntica a ψ, és a dir, trobar y_0, y_1, y_2 tals que $|\phi\rangle = |y_2y_1y_0\rangle = \mathrm{QFT}_8|x_2x_1x_0\rangle$.

1. Apliquem la porta *Hadamard* a $|x_2\rangle$.

   $$\psi_1 = \frac{1}{\sqrt{2}}\left[|0\rangle + e^{\left(\frac{2\pi i}{2}x_2\right)}|1\rangle\right] \otimes |x_1\rangle \otimes |x_0\rangle$$

2. Apliquem la porta $C_{R_{\pi/2}}$ a $|x_2\rangle$ depenent de x_1.

   $$\psi_2 = \frac{1}{\sqrt{2}}\left[|0\rangle + e^{\left(\frac{2\pi i}{2^2}x_1 + \frac{2\pi i}{2}x_2\right)}|1\rangle\right]|x_1\rangle \otimes |x_0\rangle$$

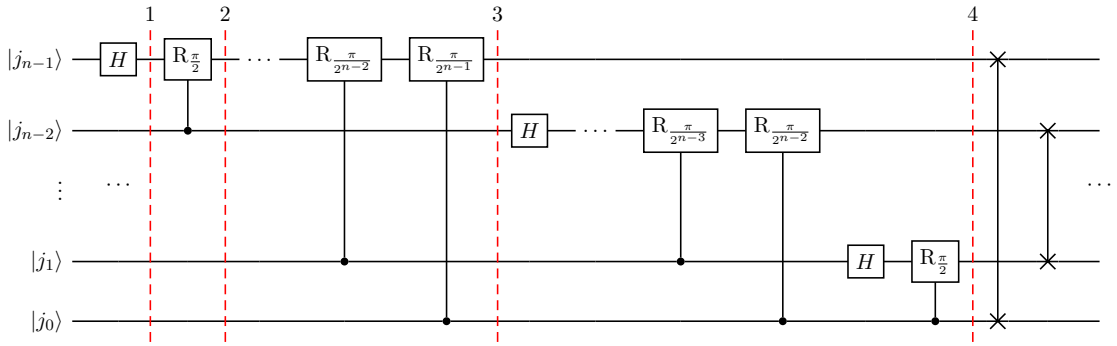


Figura 9: Circuit quàntic corresponent a la transformada de Fourier d'ordre N aplicat a l'estat $|j\rangle = |j_{n-1} \cdots j_0\rangle$

3. Apliquem la porta $C_{R_{\pi/4}}$ a $|x_2\rangle$ depenent de x_0.

$$\psi_3 = \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\left(\frac{2\pi i}{2^3} x_0 + \frac{2\pi i}{2^2} x_1 + \frac{2\pi i}{2} x_2\right)} |1\rangle \right] \otimes |x_1\rangle \otimes |x_0\rangle$$

   Acabem el procés sense tant detall perquè la idea és exactament igual que en els passos anteriors.

4. Apliquem el seguit de portes $H_1 C^{0,1} H_0$ i arribem a

$$\phi' = \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\left(\frac{2\pi i}{2^3} x_0 + \frac{2\pi i}{2^2} x_1 + \frac{2\pi i}{2} x_2\right)} |1\rangle \right] \otimes \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\left(\frac{2\pi i}{2^2} x_0 + \frac{2\pi i}{2} x_1\right)} |1\rangle \right] \otimes \frac{1}{\sqrt{2}} \left[|0\rangle + e^{\left(\frac{2\pi i}{2} x_0\right)} |1\rangle \right]$$

5. Hem de revertir l'ordre del resultat. En aquest cas només caldrà invertir el primer i tercer qubit per arribar a l'estat desitjat $|\phi\rangle$.

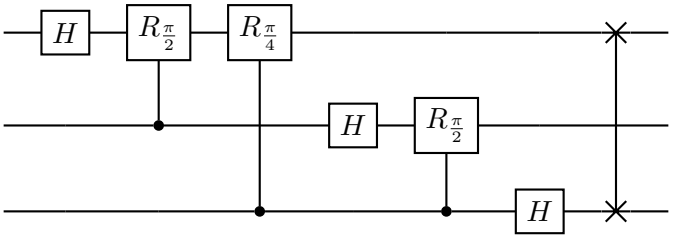


Figura 10: Circuit quàntic correponent a la transformada de Fourier per tres qubits ($N = 8$)

Observació 4.7. La transformada de Hadamard definida a 3.41 es correspon amb la transformada de Fourier pel cas $N = 2$. En el cas de dimensió superior necessitem algunes portes de correció per tal que realitzin la mateixa operació.

La transformada de Fourier quàntica és la base de molts dels algoritmes quàntics existents, i en particular de l'algoritme de Shor pel logaritme discret. Veurem més endavant com l'algoritme pel problema del logaritme discret no deixa de ser una versió en dues dimensions de l'algoritme que troba el període d'una funció. Farem un recorregut similar al que va seguir Shor per arribar-hi, així que començarem amb l'algoritme de Simon, un cas particular de cerca de període per funcions de $\mathbb{Z}/2\mathbb{Z}$.

4.2 Algoritme de Simon

L'algoritme de Simon és molt útil perquè tracta la mateixa qüestió però en el cas de funcions booleanes. L'aritmètica és més senzilla i permet veure l'estructura del procés amb claredat. Ens disposem a trobar la solució al següent problema: Sigui f una funció booleana de període r, és a dir, r és el valor més petit tal que,

$$\begin{aligned} f : \left(\mathbb{Z}/2\mathbb{Z}\right)^n &\to \left(\mathbb{Z}/2\mathbb{Z}\right)^n \\ x &\to f(x) = f(x \oplus r) \end{aligned} \tag{4.5}$$

on $\oplus$ denota la suma mòdul 2. El nostre objectiu és trobar el valor de r.

Algoritme 7. (de Simon). Donada una funció booleana f de període r el següent algoritme troba el valor de r, suposant que podem implementar la funció f en un circuit clàssic de mida $\mathcal{O}(s)$.

1. Implementar l'estat inicial

$$|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} |0\rangle^{\otimes \mathcal{O}(s)}$$

2. Aplicar la porta Hadamard al primer registre i després la transformació U_f al segon registre.

$$\mapsto \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

3. Mesurar els últims n bits de l'estat. Ens queda l'estat residual

$$\frac{1}{\sqrt{2}} |z\rangle |f(z)\rangle + \frac{1}{\sqrt{2}} |z+r\rangle |f(z)\rangle$$

4. Aplicar la transformada de Hadamard als primers n bits

$$\frac{1}{\sqrt{2}} |z\rangle + \frac{1}{\sqrt{2}} |z+r\rangle \mapsto \frac{1}{\sqrt{2^{n+1}}} \sum_{s=0}^{2^n-1} \left((-1)^{\sum_{i=0}^{n-1} s_i z_i} + (-1)^{\sum_{i=0}^{n-1} s_i (z_i + r_i)} \right) |s\rangle$$

   Observem que l'amplitud de $|s\rangle$ és $\frac{1}{\sqrt{2^{n-1}}}$ si:

$$\sum_{i=0}^{n-1} s_i z_i \equiv \sum_{i=0}^{n-1} s_i (z_i + r_i) \pmod 2$$

   que és equivalent a:

$$\sum_{i=0}^{n-1} s_i r_i \equiv 0 \pmod 2$$

   i 0 en cas contrari.

5. Mesurar els primers n bits. Obtenim un estat $|s\rangle$ tal que

$$\sum_{i=0}^{n-1} s_i r_i \pmod 2$$

   Fixem-nos que s no deixa de ser un vector de n coordenades.

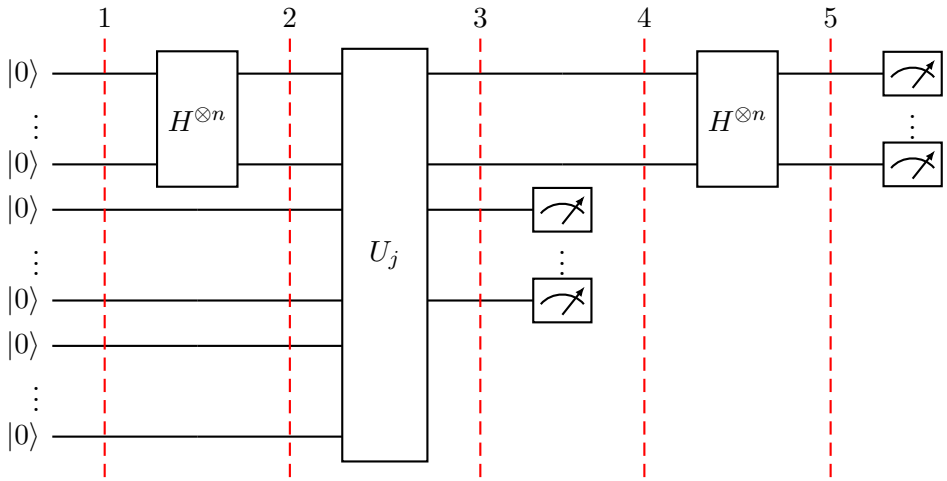


Figura 11: Diagrama corresponent al circuit de l'algoritme de Simon

6. Repetim el procés fins a tenir $(n-1)$ vectors linealment independents.
7. Resolem el sistema i trobem r.

Vegem a continuació si té sentit descriure l'algoritme d'aquesta manera, és a dir, si arribarem a trobar dins un temps raonable $n-1$ vectors linealment independents per crear el sistema.

Proposició 4.8. *Sigui $A_{(n-1)\times k} \in M(\mathbb{F}_2)$ una matriu aleatòria, amb $k \geq (n-1)$. És a dir, els coeficients de la matriu $a_{i,j}$ són variables aleatòries de Bernoulli sobre el conjunt $\{0,1\}$ independents i distribuïdes idènticament per a tot $1 \leq i \leq n$ i $1 \leq j \leq k$. Aleshores $\mathbb{P}(\{Rang(M) = n-1\}) \geq \frac{1}{4}$*

Demostració. Sigui E_j l'esdeveniment corresponent a que les primeres j columnes de A siguin linealment independents.

$$\begin{aligned}\mathbb{P}(E_{j+1}) &= \mathbb{P}(E_{j+1} \mid E_j)\mathbb{P}(E_j) + \mathbb{P}(E_{j+1} \mid E_j^c)\mathbb{P}(E_j^c) \\ &= \mathbb{P}(E_{j+1} \mid E_j)\mathbb{P}(E_j) \\ &= \left(1 - \frac{1}{2^{n-1-j}}\right)\mathbb{P}(E_j)\end{aligned}$$

Tenim que E_1 es complirà sempre i quan la primera columna no sigui nul·la, per tant

$$\mathbb{P}(E_1) = \frac{2^{n-1}-1}{2^{n-1}} = 1 - \frac{1}{2^{n-1}};$$

i per tant,

$$\mathbb{P}(E_k) = \mathbb{P}(E_1)\prod_{j=2}^{k}\mathbb{P}(E_j \mid E_{j-1}) = \prod_{j=1}^{k}\frac{2^{n-1}-2^{j-1}}{2^{n-1}} = \prod_{j=n-k}^{n-1}\left(1-\frac{1}{2^j}\right)$$

Aleshores si volem mirar la probabilitat que el rang sigui màxim tindrem,

$$\mathbb{P}(E_{n-1}) = \prod_{j=1}^{n-1}\left(1-\frac{1}{2^j}\right) \geq \left(1-\left(\frac{1}{2^{n-1}}+\frac{1}{2^{n-2}}+\cdots+\frac{1}{2^2}\right)\right)\cdot\frac{1}{2} \geq \frac{1}{4}$$

on hem utilitzat que si $a, b \in [0,1]$, $(1-a)(1-b) \geq 1-(a+b)$ i el resultat de la suma geomètrica.
□

D'ara en endavant, a part d'utilitzar la notació ja vista a aritmètica, introduïm el següent. Sigui $u \in \mathbb{R}$, aleshores

- $\lfloor u \rfloor = \max\{m \in \mathbb{Z} \mid m \leq u\}$ i $\lceil u \rceil = \min\{n \in \mathbb{Z} \mid n \geq u\}$.
- $\lfloor u \rceil$ denota l'enter més proper a u (serà doncs $\lfloor u \rfloor$, o bé, $\lceil u \rceil$).
- $\{u\}_n$ denota $u \pmod n$ restringit a l'interval:

$$-\frac{n}{2} \leq \{u\}_n < \frac{n}{2}$$

- $u \bmod 1 = u - \lfloor u \rceil$ denota la part decimal de u.

4.3 Algoritme de cerca de període

Anem a veure la versió en general de la cerca de període. Sigui f una funció periòdica de període r sobre el conjunt $S := \{0, 1, \cdots, M-1\}$, és a dir,

$$\begin{aligned} f : \{0,1,\cdots,M-1\} &\to \{0,1,\cdots,M-1\} \\ x &\to f(x) = f(x+r) \end{aligned} \tag{4.6}$$

per a tot $x \in S$, $r \in S - \{0\}$.
El nostre objectiu és, com abans, trobar r.

Algoritme 8. *(de cerca de període).* Donada una funció f de període r sobre el conjunt $\{0, \cdots, M\}$ on $M = 2^m$ per algun enter m i $r \leq \frac{\sqrt{M}}{2}$. El següent algoritme troba el valor de r. Suposem a més, que som capaços d'aplicar la funció f en un circuit clàssic de mida s.

1. Implementem l'estat inicial de $l = n + n + \mathcal{O}(s)$ qubits següent,

$$|0\rangle^n \otimes |0\rangle^n \otimes |0\rangle^{\mathcal{O}(s)}$$

2. Apliquem la porta *Hadamard* als primers n qubits i després la transformació U_f per arribar a l'estat

$$\mapsto \frac{1}{M} \sum_{x=0}^{M-1} |x\rangle\, |f(x)\rangle$$

   Ignorem a partir d'ara els últims $l - 2n$ qubits.

3. Mesurem els últims n qubits. Obtenim un cert $y = f(\cdot)$. Ens queda l'estat residual

$$\frac{1}{\sqrt{\left\lfloor \frac{M}{r} \right\rceil}} \sum_{t=0}^{\left\lfloor \frac{M}{r} \right\rceil} |x_0 + tr\rangle\, |f(x_0)\rangle$$

   on hem denotat per x_0 l'input més petit tal que $f(x_0) = y$.

4. Apliquem la transformada de Fourier d'ordre M als primer n qubits

$$\mapsto \frac{1}{\sqrt{M}} \frac{1}{\sqrt{\left\lfloor \frac{M}{r} \right\rfloor}} \sum_{s=0}^{M-1} \sum_{t=0}^{\lfloor \frac{M}{r} \rceil} exp\left(\frac{2\pi i}{2^m} s(x_0 + tr)\right) |s\rangle$$

5. Mesurem els primers n qubits. Obtenim un valor s tal que:

$$\mathbb{P}(s) = \frac{1}{M} \cdot \frac{1}{\left\lfloor \frac{M}{r} \right\rfloor} \underbrace{\left| exp\left(\frac{2\pi i}{2^m}(x_0 s)\right)\right|^2}_{=1} \left| \sum_{t=0}^{\lfloor \frac{M}{r} \rceil} exp\left(\frac{2\pi i}{2^m}(trs)\right)\right|^2 =$$

$$\frac{1}{M} \cdot \frac{1}{\left\lfloor \frac{M}{r} \right\rfloor} \left| \sum_{t=0}^{\lfloor \frac{M}{r} \rceil} exp\left(\frac{2\pi i}{2^m}(trs)\right)\right|^2$$

6. Recuperem el valor de r.

Ens centrem en com extreure r, és a dir, com fer el pas 6. Comencem pel cas fàcil on M és un múltiple de r.

Definició 4.9. Suposem que M és múltiple de r i definim $q := M/r$. Aleshores direm que s és un bon valor si s és múltiple de q.

Fixem-nos que tenim exactament r bons valors s.
Sigui $S = \#\{0, M/r, 2M/r, ...\}$ Per una banda tenim que $\frac{aM}{r} = \frac{(a+r)M}{r} \pmod M$ per a tot a enter. Per tant $S \leq r$. A la vegada, tenim que si $S < r$ aleshores $s \cdot \frac{M}{r} \neq 0 \pmod M$ i prenent $a < b < r$ tindríem $\frac{(b-a)M}{r} = 0 \pmod M$, cosa impossible si tenim en compte que $b - a \leq b < r$. Necessàriament $S = r$.
Observem també que si s és un bon valor aleshores trs és un múltiple de M i per tant $w^{trs} = 1$, per ser w una arrel M-èssima de la unitat. Tenim aleshores $\mathbb{P}(s) = 1/r$.

Unint les dues observacions anteriors, podem assegurar que al pas 6, el valor obtingut s està uniformement distribuit sobre el conjunt $\{0, M, 2M/r, ..., M - r\}$. Si després d'aquest pas considerem el valor s/M tindrem que és de la forma k/r per un enter $k \in \{0, ..., r-1\}$ aleatori. Si simplifiquem la fracció s/M, obtenim dos enters coprimers a, b tals que $\frac{s}{M} = \frac{a}{b}$. Això implica que si k i r són coprimers, llavors $r = b$, i en cas contrari b serà un divisor de r.

Proposició 4.10. *Suposem que M és múltiple de r. Aleshores la probabilitat de trobar el període de la funció, és a dir, el valor correcte de r, és superior a $1/3$.*

Demostració. Suposem que exectuem l'algoritme dues vegades. Obtenim dos valors s_1, s_2 tal que $s_i/M = k_i/r$ on $k_1, k_2 \in \{0, ..., r-1\}$ nombres aleatoris. Calculem les fraccions simplificades, $\frac{a_i}{b_i} = \frac{s_i}{M}$, aleshores $b_i = r$ o b_i divideix r.
Més precisament, tenim $b_i = r/\text{mcd}(k_i, r)$ i per tant si $\text{mcd}(k_1, r)$ i $\text{mcd}(k_2, r)$ són coprimers, $r = \text{mcm}(b_1, b2)$.
Tindrem èxit sempre i quan k_1, k_2, r no comparteixin factors primers. Aquest fet és equivalent a dir que $\text{mcd}(k_1, k_2) > 1$. Notem abans que k_1 i k_2 són dues variables aleatòries

independents i idènticament distribuïdes i que com a màxim $1/p$ dels elements del conjunt $\{1, 2, ..., r-1\}$ són múltiples de p. Llavors,

$$\mathbb{P}(\{\text{mcd}(k_1, k_2) > 1\}) = \sum_{p\ primer} \mathbb{P}(\{p|k_1,\ p|k_2\}) \leq \sum_{p\ primer} \frac{1}{p^2} < \sum_{n\geq 2} \frac{1}{n^2} = \frac{\pi^2}{6} - 1 < 0.65$$

On hem utilitzat el següent resultat de teoria de nombres:

$$\sum_{n\geq 2} \frac{1}{n^2} = \zeta(2) = \frac{\pi^2}{6}$$

On ζ denota la funció zeta de Riemann.
□

Imaginem que repetim l'algoritme a vegades amb l'objectiu de tenir més seguretat a l'hora de trobar la bona solució. Obtindrem una sèrie de valors $r_1, ..., r_a$ on amb alta probabilitat, un d'ells és el valor que busquem. Llavors només cal que comprovem si $f(0) = f(r_i)\ \forall i \in \{1, ..., a\}$ i quedar-nos amb el més petit dels que ho compleixen. La resta o bé estaran malament, o seran múltiples d'aquest.

Anem a veure el cas general, on r no divideix M. La figura 12 mostra que té sentit agafar un camí similar a l'anterior. Veiem que amb alta probabilitat els valors observats de s són pròxims a un múltiple de M/r. Notem que $s = 0$ i $s = 128$, que són els únics enters múltiples de $M/10$ recullen la probabilitat més alta. Els valors $s = 25$ i $= 26$ s'apropen a $M/10$ però no els hi correspon una probabilitat de les més altes, a diferència de $s = 51$ que s'acosta a $2M/10$ amb més probabilitat.
Podríem seguir l'anàlisi per veure com els valors que apareixen amb més probabilitat són molt propers als diferents múltiples de $M/10$.

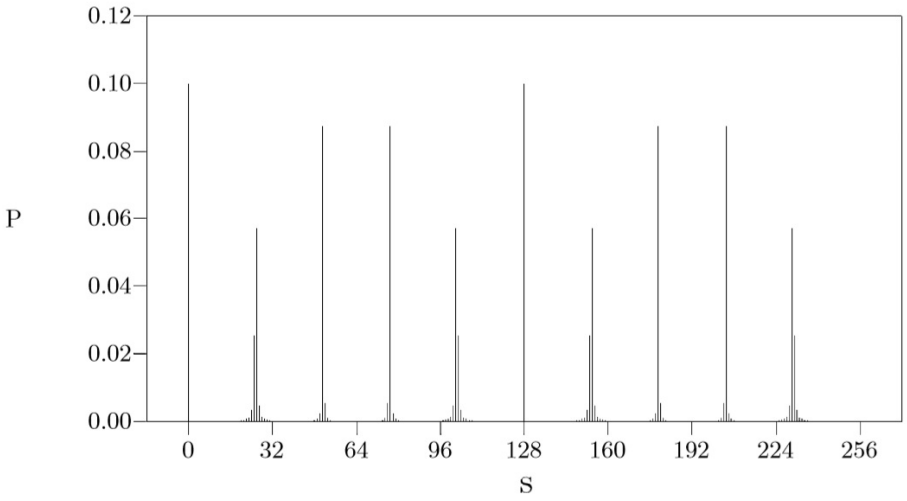


Figura 12: Probabilitat d'observar un cert valor s per a $M = 2^8 = 256$ i $r = 10$. Gràfica extreta de [15].

Podem extreure la conclusió que la probabilitat d'observar un valor s concret depèn de la seva diferència amb el múltiple de M/r més proper. En conseqüència, donem la següent definició.

Definició 4.11. Direm que s és un bon valor si

$$-\frac{r}{2} \leq sr \pmod{M} \leq \frac{r}{2} \tag{4.7}$$

Proposició 4.12. *Cada bon resultat té com a mínim* $\frac{1}{8r} - o(1/r)$ *possibilitats d'aparèixer.*

Demostració. Necessitem aproximar la probabilitat

$$\mathbb{P}(s) = \frac{1}{M} \cdot \frac{1}{\left\lfloor \frac{M}{r} \right\rceil} \left| \sum_{t=0}^{\lfloor \frac{M}{r} \rceil - 1} exp\left(\frac{2\pi i}{2^m}(trs) \right) \right|^2$$

Comencem pel estudiar el cas on $0 \leq sr \pmod{M} \leq \frac{r}{2}$. Definim $g := (sr \bmod M)/M$. Aleshores,

$$\sum_{t=0}^{\lfloor \frac{M}{r} \rceil - 1} e^{2\pi i \frac{1}{M} trs} = \sum_{t=0}^{\lfloor \frac{M}{r} \rceil - 1} e^{2\pi i g t} \tag{1}$$

Fixem-nos que en el fons, 1 és equivalent a sumar $e^{i\theta}$ per a $\left\lfloor \frac{M}{r} \right\rceil$ diferents valors de θ equiespaiats en l'interval $[0, \ldots, 2\pi g \frac{M}{r}]$. Per tant $\theta \leq \pi$ i podem pensar aquest sumatori com el sumatori de diferents vectors unitaris amb angles inferiors a π i equispaiats dins l'interval $[0, \ldots, 2\pi g \frac{M}{r}]$. Llavors és correcte dir que almenys la meitat d'ells tindran un angle inferior a $\frac{\pi}{4}$. Per tant,

$$\left| \sum_{t=0}^{\left(\lfloor \frac{M}{r} \rceil /2\right) - 1} e^{i\theta} \right|^2 = \left| \sum_{t=0}^{\left(\lfloor \frac{M}{r} \rceil /2\right) - 1} (\cos\theta_t + i \sin\theta_t) \right|^2 \geq \left| \sum_{t=0}^{\left(\lfloor \frac{M}{r} \rceil /2\right) - 1} \cos\theta_t \right|^2 \geq \left\lfloor \frac{M}{r} \right\rceil^2 \cdot \frac{1}{2^2} \cdot \frac{1}{2}$$

ja que per t tal que $0 \leq t < \left(\left\lfloor \frac{M}{r} \right\rceil /2 \right)$ tenim $|\theta_t| \geq \frac{\pi}{4}$, que ens dóna,

$$\frac{1}{\sqrt{2}} \leq \cos\theta_t \leq 1$$

i per tant podem concloure si recuperem 1, que,

$$\mathbb{P}(s) \geq \frac{1}{M} \frac{1}{\left\lfloor \frac{M}{r} \right\rceil} \cdot \frac{1}{8} \cdot \left\lfloor \frac{M}{r} \right\rceil^2 \geq \frac{1}{8r} \cdot (1 - o(1))$$

□

Proposició 4.13. *Existeixen almenys* r *bons resultats* s*.*

Demostració. Per cada $k \in \{0, \ldots, r-1\}$ hi ha un enter s_k a l'interval $\left[k\frac{M}{r} - \frac{1}{2}, k\frac{M}{r} + \frac{1}{2} \right]$ tal que se satisfà $-\frac{r}{2} \leq s_k r \leq \frac{r}{2}$. A més a més tots els s_k són diferents ja que pertanyen a intervals disjunts. □

Fins ara hem vist que tenim almenys r bons possibles resultats s amb una probabilitat considerablement bona d'aparèixer. Suposem que hem mesurat un bon s a l'últim pas de l'algoritme. L'objectiu és recuperar r. Observem dos fets abans,

- Mesurar un bon s equival a que per una certa variable aleatòria $|sr - kM| \leq \frac{r}{2}$, és a dir,
$$\left|\frac{s}{M} - \frac{k}{s}\right| \leq \frac{1}{2M}$$
- Si $\frac{a}{b}$ i $\frac{a'}{b'}$ són dos nombres racionals diferents tals que $b, b' \leq D$ per una certa constant $D \in \mathbb{Z}$, aleshores
$$\left|\frac{a}{b} - \frac{a'}{b'}\right| \geq \frac{1}{D^2}$$

L'observació anterior ens fa veure que si tenim $\rho, D \in \mathbb{R}$, aleshores exiteix com a màxim un nombre racional $\frac{a}{b}$ amb $b \leq D$ tal que $\left|\rho - \frac{a}{b}\right| < \frac{1}{2D^2}$. De fet, tenim la manera de trobar ρ:

Teorema 4.14. *Siguin $\rho, \frac{a}{b}$ dos nombres racionals tals que*
$$\left|\frac{a}{b} - \rho\right| \leq \frac{1}{2b^2} \tag{4.8}$$
aleshores $\frac{a}{b}$ és convergent pel mètode de les fraccions continuades de ρ.

Corol·lari 4.15. *Siguin $\rho, \frac{a}{b}$ dos nombres racionals definits com al teorema anterior. Aleshores existeix un algoritme que calcula $\frac{a}{b}$ on $b \leq D$ per una certa cota $D \in \mathbb{R}$ amb una complexitat de $\mathcal{O}((log\ D)^{\mathcal{O}(1)})$. Anomenarem aquest algoritme com l'algoritme de les fraccions continuades.*

Més detalls del dos resultats teòrics anteriors es poden trobar a [8].

En definitiva, l'observació feta al pas 6 proporciona amb una prou bona probabilitat un bon valor s. A partir d'aquest valor, fent servir el fet que $\left|\frac{s}{M} - \frac{k}{r}\right| \leq \frac{1}{2M}$ per una variable aleatòria $k \in \{0, \ldots, r-1\}$ i recordant que $r < \sqrt{M}$ podem fer servir l'algoritme de les fraccions continuades per trobar dos enters coprimers a, b tals que $\frac{a}{b} = \frac{k}{r}$.
Una vegada arribats aquí, veiem que ens trobem en la mateixa situació que havíem vist en el cas on r dividia M. Per tant, repetint l'algoritme dues vegades obtindrem
$$\frac{a_1}{b_1} = \frac{k_1}{r} i \frac{a_2}{b_2} = \frac{k_2}{r} \text{ on } \mathbb{P}(\text{mcd}(k_1, k_2) > 1)$$
D'aquí trobem $r = \text{mcm}(b_1, b_2)$.

Exemple 4.16. Anem a buscar el període de la funció $f(x) = x \pmod 2$. És clar que el període r de f és 2. Per poder fer l'exemple a mà agafem un sistema de 3 qubits. Aleshores $N = 8$.

1. Apliquem la següent transformació d'estats
$$|0\rangle\,|0\rangle \to \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle\,|0\rangle \to \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle\,|x \pmod 2\rangle$$
2. Mesurem $|f\rangle$. Tenim que $|f\rangle$ col·lapsarà en $|0\rangle$ o $|1\rangle$. Suposem que l'experiment aleatori retorna $|f(x)\rangle = |1\rangle$.Veiem que ens quedarà l'estat residual següent:
$$\frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle \otimes |f(x)\rangle \to \frac{1}{2}\left(|1\rangle + |3\rangle + |5\rangle + |7\rangle\right) \otimes |1\rangle$$

3. Apliquem la transformada de Fourier al primer registre

$$\frac{1}{2}\left(|1\rangle + |3\rangle + |5\rangle + |7\rangle\right) \otimes |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |4\rangle)$$

4. Mesurem el primer registre. Ens dona un estat s ben definit.

Fixem-nos que l'últim pas ens sortirà $|0\rangle$ o $|4\rangle$. Sabem pels resultats que hem vist anteriorment que si repetim l'algoritme algunes vegades, la probabilitat que acabin sortint els dos resultats és força alta. Estem davant del cas més fàcil de tots els esmentats anteriorent ja que clarament $r|N$, i 1 i 2 són coprimers, per tant

$$\frac{s}{N} = \frac{1}{2} = \frac{1}{r} \Rightarrow \ r = 2$$

Aquest algoritme, a part de ser interessant en si mateix, és especialment important ja que és el pas clau que Shor va fer servir pel seu algoritme de factorització de nombres enters. No és el tema principal d'aquest treball, però veure l'algoritme de factorització d'enters de Shor proporciona una idea de com l'algoritme de cerca de període i l'algoritme de cerca de l'ordre d'un grup són intercanviables.

Algoritme 9. Sigui $N \in \mathbb{N}$ un nombre natural compost. Sigui m tal que $2^m \leq N^2 < 2^m + 1$. Definim $M := 2^m$. El següent algoritme troba una factorització de N en temps polinòmic i probabilitat constant.

1. Determinem si $N = a^k$ per alguna $k \geq 2$ i $a \geq 3$. En cas positiu retornem a.

2. Triem de manera equiprobable $a \in \{2, \ldots, N-1\}$. Si $\text{mcd}(a, N) \neq 1$, retornem el valor $\text{mcd}(a, N)$.

3. Trobem l'ordre de a a $\mathbb{Z}_N$. Aquí és on utilitzem la cerca de període. Definim la funció $f(x) := a^x \pmod{M}$ amb domini $\{0, \ldots, M-1\}$. Hem vist abans que la podem implementar en temps $\mathcal{O}(m^3)$ i partim de la base que sabem com fer-ho. És evident que el valor r és tal que $f(x+r)$. Podem veure també que $f(0), \ldots, f(r-1)$ són tots diferents ja que en cas contrari tindríem $a^j \equiv a^i \pmod{N}$ i per tant $a^{j-i} \equiv 1 \pmod{N}$ que contradiu el fet que r sigui l'ordre de a. A més a més $r \leq N \leq \sqrt{M}$ per tant podem aplicar sense problema l'algoritme de cerca de període.

4. Si r és senar tornem al pas 2. En cas contrari seguim.

5. Calculem $b := a^r/2 \in \mathbb{Z}_N$. Si $b \equiv -1 \pmod{N}$ tornem al pas 2. En cas contrari retornem $\text{mcd}(b+1, N)$

Observació 4.17. Fixem-nos que queda implícitament demostrat a l'algoritme que podem resoldre el problema de cerca de l'ordre d'un element d'un grup cíclic amb l'algoritme de cerca de període.

4.4 El problema del logaritme discret

Veurem com l'algoritme que va donar Shor per trencar el problema del logaritme discret es pot visualitzar com un algoritme en dues dimensions de l'algoritme de cerca de període.

Sigui $(G, \cdot)$ un grup cíclic finit. Sigui g un generador del grup, és a dir $G = \langle a \rangle = \{1, a, a^2, \ldots, a^{s-1}\}$. Recordem que el problema del logaritme discret es proposa trobar l'element $r \in \{0, 1, \ldots, s-1\}$ tal que

$$a = g^r$$

per un cert element a de G.

Partim de la base que coneixem l'ordre del grup. En cas contrari simplement apliquem l'algorime de cerca d'ordre (cf. observació 4.17).

Ens resultarà útil definir la funció següent. Sigui p un nombre primer, g un generador de $\mathbb{Z}_p^*$ i x un element de $\mathbb{Z}_p^*$ tal que $x = g^r \pmod p$. Definim la funció F com:

$$\begin{aligned} F : \mathbb{Z}^2 &\to \langle g \rangle \\ (a, b) &\mapsto g^a \cdot (x^{-1})^b = g^{a-rb} \end{aligned}$$

Observem que F és periòdica en el sentit que

$$F(a, b) = F(a + \lambda r, b - \lambda)$$

per qualsevol $\lambda \in \mathbb{Z}$.

Algoritme 10. *(de Shor pel problema del logaritme discret).* Donat $(G, \cdot)$ un grup d'ordre primer q, un generador g i un element $x \in G$. Suposem que som capaços de trobar el natural l tal que $2^l < q$. Suposem també que és possible aplicar la funció F en un circuit clàssic de mida s. Aquest algoritme troba el logaritme discret de $x = g^r$ en base x.

1. Implementem l'estat inicial

$$|0\rangle^{\otimes l} \otimes |0\rangle^{\otimes l} \otimes |0\rangle^{\otimes \mathcal{O}(s)}$$

2. Apliquem la porta *Hadamard* als dos primers registres. Ens queda l'estat següent:

$$\mapsto \frac{1}{2^l} \sum_{a=0}^{2^l-1} \sum_{b=0}^{2^l-1} |a\rangle\, |b\rangle\, |0\rangle$$

3. Apliquem la funció F al tercer registre.

$$\begin{aligned} \mapsto & \frac{1}{2^l} \sum_{a=0}^{2^l-1} \sum_{b=0}^{2^l-1} |a\rangle\, |b\rangle\, |g^a x^{-b} \pmod q\rangle \\ = & \frac{1}{2^l} \sum_{a=0}^{2^l-1} \sum_{b=0}^{2^l-1} |a\rangle\, |b\rangle\, |g^{a-rb} \pmod q\rangle \end{aligned}$$

4. Apliquem la transformada de Fourier d'ordre 2^l als dos primers registres.

$$\mapsto \frac{1}{2^{2l}} \sum_{a=0}^{2^l-1} \sum_{b=0}^{2^l-1} \sum_{c=0}^{2^l-1} \sum_{d=0}^{2^l-1} exp\left(\frac{2\pi i(ac+bd)}{2^l}\right) |c\rangle\, |d\rangle\, |g^a x^{-b} \pmod q\rangle$$

5. Sigui $k = a - rb \pmod q$. Fem una observació. La probabilitat d'obtenir l'estat $|c, d, y\rangle$ on $y = g^k \pmod q$ és:

$$\frac{1}{2^{4l}} \left| \sum_{\substack{a,b \\ a-rb\equiv k}} exp\left(\frac{2\pi i(ac+bd)}{2^l}\right) \right|^2$$

6. Recuperem r a partir d'aquest output.

Com abans, aquest algoritme té dues parts. En la primera obtenim un conjunt de valors (c, d, y) on $y = g^k \pmod q$. Podem obviar l'últim valor ja que ha quedat fixat per l'observació i no ens dona cap informació extra. En el segon, si la probabilitat d'obtenir unes bones condicions és prou alta, podrem recuperar la solució que busquem.

Anem a analitzar la distribució de probabilitat del pas 4.

1. Com $k = a - rb \pmod q$ tenim $a = k + rb \pmod q$, per tant,

$$ac + bd = ((k + rb) \pmod q)c + bd = kc + brc - \left\lfloor \frac{k+br}{q} \right\rfloor cq + bd$$

   ja que $u \pmod q = u - \left\lfloor \frac{u}{q} \right\rfloor q$. Aleshores, podem reescriure la probabilitat en la que obtenim l'estat al pas 4 com,

$$\frac{1}{2^{4l}} \left| \sum_b exp\left(\frac{2\pi i}{2^l}\left(kc + b(rc+d) - \left\lfloor \frac{k+br}{q} \right\rfloor cq\right)\right) \right|^2$$

2. Podem extreure el terme $exp(2\pi ikc/2^l)$ ja que no fa variar la probabilitat.

$$\frac{1}{2^{4l}} \underbrace{\left| exp\left(\frac{2\pi i}{2^l} kc\right) \right|^2}_{=1} \left| \sum_b exp\left(\frac{2\pi i}{2^l}\left(b(rc+d) - \left\lfloor \frac{k+br}{q} \right\rfloor cq\right)\right) \right|^2$$

3. Podem centrar b entorn de 0 obtenint:

$$\frac{1}{2^{4l}}\left|\sum_b exp\left(\frac{2\pi i}{2^l}\left((b+2^{l-1}-2^{l-1})(rc+d)-\left\lfloor\frac{k+br}{q}\right\rfloor cq\right)\right)\right|^2 =$$

$$\frac{1}{2^{4l}}\underbrace{\left|exp\left(-\pi i(rc+d)\right)\right|^2}_{=1}\left|\sum_b exp\left(\frac{2\pi i}{2^l}\left((b-2^{l-1})(rc+d)-\left\lfloor\frac{k+br}{q}\right\rfloor cq\right)\right)\right|^2 =$$

$$\frac{1}{2^{4l}}\left|\sum_b exp\left(\frac{2\pi i}{2^l}\left((b-2^{l-1})(rc+d)-\left\lfloor\frac{k+br}{q}\right\rfloor \{cq\}_{2^l}\right)\right)\right|^2$$

ja que un estat quàntic és invariant respecte un canvi de fase global, és a dir, suma o resta de 2π a la fase corresponent.

Seguim la mateixa lògica que en cas de l'algoritme de cerca de període. A partir d'aquesta última mesura amb la seva corresponent probabilitat, anem a la cerca d'uns *outputs* que ens permetin obtenir r.

Definició 4.18. Direm que una parella (c,d) on c és un enter que es troba dins l'interval $0 \leq c \leq 2^l$ és una bona parella si c és tal que,

(i) $\left|\{cq\}_{2^l}\right| \leq 2^{l-4}$

(ii) $\left|\frac{r}{q}\{cq\}_{2^l} - f_c\right| \leq 2^{-3}$ per algun $f_c \in \mathbb{Z}$ tal que $d \equiv f_c - rc \pmod{2^l}$.

Lema 4.19. *Existeixen almenys* $2^{l-8}+1$ *bones parelles* (c,d).

Demostració. Podem reescriure la definició anterior com:

(i) $\left|\{cq\}_{2^l}\right| \leq 2^{l-4}$

(ii) $\left|\alpha\{cq\}_{2^l} - \lfloor\alpha\{cq\}_{2^l}\rceil\right| = \left|\alpha\{cq\}_{2^l} \bmod 1\right| \leq 2^{-3}$ on $\alpha := \frac{r}{q} \in \mathbb{R}$

Considerem per a tot $0 \leq c < 2^l$ el següent conjunt de punts:

$$p_c = (x_c, y_c) = (\{cq\}_{2^l}, \alpha\{cq\}_{2^l}) \bmod 1)$$

Fixem-nos que

$$-\frac{2^l}{2} \leq x_c < \frac{2^l}{2} \quad \text{i} \quad 0 \leq y_c < 1$$

$$p_c \in \mathbb{Z} \cap [-\frac{2^l}{2}, \frac{2^l}{2}] \times [0,1)$$

Fixem-nos que el conjunt de punts anteriors creen un rectangle en l'espai de dues dimensions de mida $2^l \times 1$
Dividim aqust rectangle en rectangles més petits de mida $2^{l-1} \times 2^{-3}$. Aleshores si p_{c_1} i p_{c_2} són dós punts qualssevol

$$\{c_2 q\}_{2^l} - \{c_1 q\}_{2^l} \equiv \{(c_2 - c_1)q\}_{2^l} \pmod{2^l} \tag{1}$$

A més, tenim que si els dos punts p_{c_1} i p_{c_2} van a parar al mateix rectangle llavors per la definició de bona parella,

$$\left|\{c_2 q\}_{2^l} - \{c_1 q\}_{2^l}\right| \leq 2^{l-4}$$

Si tenim en compte que dos nombres que són iguals en mòdul 2^l i estan tots dos acotats per 2^{l-1} aleshores són iguals, podem ajuntar les dues condicions anteriors obtenint:

$$\left|\{c_2 q\}_{2^l} - \{c_1 q\}_{2^l}\right| = \left|\{(c_2 - c_1) q\}_{2^l}\right| \leq 2^{l-4}$$

Anàlogament si p_{c_1} i p_{c_2} són dos punts qualssevol per la coordenada y_c tindrem que

$$\begin{aligned}\left|(\alpha\{c_2 q\}_{2^l} \bmod 1) - (\alpha\{c_1 q\}_{2^l} \bmod 1)\right| = \\ \left|\alpha(\{c_2 q\}_{2^l} - \{c_1 q\}_{2^l} \bmod 1)\right| \leq 2^{-3}\end{aligned}$$

I aplicant 1 podem reduir-ho a

$$\left|\alpha\{(c_2 - c_1) q\}_{2^l} \bmod 1\right| \leq 2^{-3}$$

Suposem que p_{c_1} i p_{c_2} es troben en el mateix rectangle i $c_1 \leq_2$. Llavors si considerem la parella (c', d') on

$$c' = c_2 - c_1 \quad \text{i} \quad d' \equiv (f_{c'} - r c') \pmod{2^l} \text{ on } f_{c'} = \lfloor \alpha\{c' q\}_{2^l} \rceil$$

tenim que (c', d') és una bona parella ja que $0 \leq c' < 2^l$

$$\left|\{c' q\}_{2^l}\right| \leq 2^{l-4} \quad \text{i} \quad \left|\alpha\{c' q\}_{2^l} - \lfloor \alpha\{c' q\}_{2^l} \rceil\right| = \left|\alpha\{c' q\}_{2^l} \bmod 1\right| \leq 2^{-3}$$

El problema que abans consistia en trobar una cota inferior pel nombre de bons parells (c', d') s'ha convertit en la busca d'una cota inferior pel nombre de punts p_{j_1}, p_{j_2} que hi ha dins el rectangle gran descrit anteriorment i a partir dels quals definim (c', d').

Recordem que tenim el rectangle de mida $2^l \times 1$ dividit en rectangles més petits de mida $2^{l-4} \times 2^{-3}$. En total tindrem doncs, $(2^l / 2^{l-4}) \cdot (1/2^{-3}) = 2^7$ rectangles petits.
Sigui R_i el nombre de punts que es troben dins el rectangle i. Aleshores tenim $\frac{R_i(R_i+1)}{2} \left(> \frac{R_i^2}{2} \right)$ combinacions de parelles (p_{c_1}, p_{c_2}) tals que $p_{c_1}, p_{c_2} \in R_i$ i $c_2 \geq c_1$.
Ens proposem acotar:

$$\frac{1}{2} \sum_{i=0}^{2^7-1} R_i^2$$

Veiem que si apliquem la desigualtat de Cauchy-Schwarz obtenim,

$$2^{2l} = \left(\sum_{i=0}^{2^7-1} R_i \right)^2 \leq \left(\sum_{i=0}^{2^7-1} 1^2 \right) \left(\sum_{i=0}^{2^7-1} R_i^2 \right) \Rightarrow \frac{1}{2} \sum_{i=0}^{2^7-1} R_i^2 \geq 2^{2l-8} \tag{2}$$

Hem demostrat que per dos punts p_{c_1}, p_{c_2} que cauen dins el mateix rectangle i tals que $c_2 > c_1$, la parella (c', d') és bona. A més, hem vist que hi ha més de 2^{2l-8} parelles dins a cada rectangle i.
Tenint en compte que si c_1 i $c_2 \geq c_1$ defineixen una bona parella (c', d') aleshores $c_1 + u$ i $c_2 + u$ també per a tot enter u tal que,

$$0 \leq j_1 + u \leq j_2 + u < 2^l$$

veiem que podem reduir la cota de 2, ja que cada bona parella estaria contada amb multiplicitat com a màxim 2^l.
Per tant hi ha (estrictament) més de $2^{2l-8}/2^l = 2^{l-8}$. □

Lema 4.20. *La probabilitat d'obtenir un bon valor (c, d) a partir d'una execució de l'algoritme és, com a mínim*

$$\frac{1}{2q}$$

Demostració. Havíem observat que la probabilitat d'observar un estat $|c, d, g^k\rangle$ era

$$\frac{1}{2^{4l}}\left|\sum_b exp\left(\frac{2\pi i}{2^l}\left((b-2^{l-1})(rc+d)-\lfloor\frac{k+br}{q}\rfloor\{cq\}_{2^l}\right)\right)\right|^2 \tag{1}$$

Definim $\lambda := \left\lfloor\frac{k+br}{q}\right\rfloor$.
Observem que com que $k = a - br \bmod q$ tenim $0 \leq k < q$, que implica,

$$\frac{br}{q} - 1 \leq \lambda \leq \frac{br}{q} + 1 \quad \Rightarrow \quad \left|\lambda - \frac{br}{q}\right| \leq 1$$

Si hem obtingut un bon parell $d = f_c - rc \pmod{2^l}$ podem reescriure l'expressió anterior com:

$$\frac{1}{2^{4l}}\left|\sum_b exp\left(\frac{2\pi i}{2^l}\left((b-2^{l-1})f_c-\lambda\{cq\}_{2^l}\right)\right)\right|^2$$

Afegim una constant addicional a la fase global de l'estat.

$$\frac{1}{2^{4l}}\underbrace{\left|\exp\left(\pi i\{cq\}_{2^l}\frac{r}{q}\right)\right|^2}_{=1}\left|\sum_b exp\left(\frac{2\pi i}{2^l}\left((b-2^{l-1})f_c-\lambda\{cq\}_{2^l}\right)\right)\right|^2 =$$

$$\left|\sum_b exp\left(\frac{2\pi i}{2^l}\left((b-2^{l-1})f_c-\lambda\{cq\}_{2^l}+2^{l-1}\{cq\}_{2^l}\frac{r}{q}\right)\right)\right|^2$$

Aleshores per la desigualtat triangular tenim que

$$\left|\{cq\}_{2^l}\lambda-\frac{br}{q}\{cq\}+\frac{br}{q}\{cq\}-(b-2^{l-1})f_c-2^{l-1}\{cq\}_{2^l}\frac{r}{q}\right| \leq$$
$$\left|\{cq\}_{2^l}\left(\lambda-\frac{br}{q}\right)\right|+\left|(b-2^{l-1})\left(\{cq\}_{2^l}\frac{r}{q}-f_c\right)\right|$$

Per un bon parell es compleix, per definició, $\{cq\}_{2^l} \leq 2^{l-4}$ i

$$\left|\{cq\}_{2^l}\frac{r}{q}-f_c\right| \leq 2^{-3} \quad \Rightarrow \quad \left|(b-2^{l-1})\left(\{cq\}_{2^l}\frac{r}{q}-f_c\right)\right| \leq 2^{l-4}$$

on hem fet servir que $0 \leq b < 2^l$. Combinant els resultats anteriors arribem a

$$\left|\{cq\}_{2^l}\lambda-(b-2^{l-1})f_c-2^{l-1}\{cq\}_{2^l}\frac{r}{q}\right| \leq \left|\{cq\}_{2^l}\right|+2^{l-4} \leq 2^{l-3}$$

Acotar l'anterior expressió pot resultar una mica aparatós. Introduïm el següent:
Denotarem per S_k el nombre de parells (a, b) tals que

$$k \equiv a - rb \pmod{q}$$

on $a, b \in \mathbb{Z}$ i $0 \leq a, b < 2^l$.
Fixem-nos en que :

$$\sum_{k=0}^{q-1} S_k = 2^{2l}$$

i si apliquem la desigualtat de Cauchy-Schwarz,

$$2^{4l} = \left(\sum_{k=0}^{q-1} S_k\right)^2 \leq \left(\sum_{k=0}^{q-1} 1^2\right)\left(\sum_{k=0}^{q-1} S_k^2\right) \Rightarrow \sum_{k=0}^{q-1} S_k^2 \geq \frac{2^{4l}}{q}$$

Aleshores recuperant la probabilitat de l'output de sortida,

$$\frac{1}{2^{4l}}\left|\sum_b exp\left(\frac{2\pi i}{2^l}\left((b-2^{l-1})(rc+d) - \left\lfloor \frac{k+br}{q} \right\rfloor \{cq\}_{2^l}\right)\right)\right|^2 = \frac{1}{2^{4l}}\left|\sum_b e^{i\theta_b}\right|^2 \geq \frac{S_k^2}{2\cdot 2^{4l}}$$

ja que $|\theta_b| \leq \frac{2\pi}{8} = \frac{\pi}{4}$ per tots els valors de b dins S_k.
Per últim sumem sobre tots els possibles valors k i arribem a:

$$\sum_{k=0}^{q-1} \frac{S_k^2}{2\cdot 2^{4l}} \geq \frac{2^{4l}}{q}\cdot\frac{1}{2\cdot 2\cdot 2^{4l}} = \frac{1}{2q}$$

□

Lema 4.21. *Sigui (c, d) un bon valor tal que $c \neq 0$. Aleshores*

$$r \equiv \left\lfloor \frac{dq}{2^l} \right\rceil t^{-1} \pmod q \quad on \quad t = \frac{\{cq\}_{2^l} - cq}{2^l} \in \mathbb{Z}$$

Demostració. Per la definició de bon valor tenim que

$$\left|\frac{r}{q}\{cq\}_{2^l} - f_c\right| \leq 2^{-3} \quad \Rightarrow \quad \frac{r}{q}\{cq\}_{2^l} - f_c = \delta$$

on $|\delta| \leq 2^{-3}$. Podem interpretar δ com el terme d'error respecte la cota. A més recordem que

$$d \equiv f_c - rc \pmod{2^l}$$

Per tant, per algun $n \in \mathbb{N}$,

$$\{cq\}_{2^l}\frac{r}{q} - d - rc + n2^l = \delta$$
$$\{cq\}_{2^l} r - dq - rcq + nq2^l = \delta q$$
$$r\underbrace{\frac{\{cq\}_{2^l} - cq}{2^l}}_{t\in\mathbb{Z}} - \frac{dq}{2^l} + nq = \frac{\delta q}{2^l}$$

Aproximant els dos costats a l'enter més proper obtenim,

$$rt + \left\lfloor -\frac{dq}{2^l} \right\rceil + nq = \left\lfloor rt - \frac{dq}{2^l} + nq \right\rceil = \left\lfloor \frac{\delta q}{2^l} \right\rceil = 0$$

Per tant,

$$rt + \left\lfloor -\frac{dq}{2^l} \right\rceil \equiv 0 \pmod{q} \tag{1}$$

Fixem-nos que per una banda el fet que $c > 0$ fa que tinguem $cq > 2^l$ i per tant $\left|\{cq\}_{2^l}\right| \leq \frac{2^l}{2}$, que implica que $0 < |t|$. Per altra banda,

$$|t| = \left|\frac{\{cq\}_{2^l} - cq}{2^l}\right| \leq \frac{1}{2} + \frac{cq}{2^l} \leq \frac{1}{2} + \frac{(2^l-1)q}{2^l} \leq \frac{1}{2} + q - \underbrace{\frac{q}{2^l}}_{>1} < q$$

Podem assegurar doncs, que $0 < |t| < q$ que implica $t \not\equiv 0 \pmod{q}$ i podem concloure reescrivint sense problema 1 com

$$r \equiv \left\lfloor \frac{dq}{2^l} \right\rceil t^{-1} \pmod{q}$$

□

Quan observem una parella (c, d) com a *output*, no sabem el resultat r, per tant a priori no podem saber si hem obtingut un bon valor o no. El següent teorema resumeix els resultats anteriors amb l'objectiu de saber amb quina probabilitat aconseguirem trobar r executant l'algoritme una vegada.

Teorema 4.22. *Suposem que hem executat l'algoritme de Shor pel cas del logaritme discret en un ordinador quàntic per trobar el valor r tal que $x = g^r$ i hem obtingut un output (c, d). Aleshores obtindrem la solució que busquem amb una probabilitat de com a mínim 2^{-10}.*

Demostració. Pel lema 4.20 tenim que la probabilitat d'obtenir un bon valor concret (c, d) executant una sola vegada l'algoritme està acotada inferiorment per $\frac{1}{2q}$.
D'altra banda, el lema 4.19 ens diu que existeixen com a mínim $2^{l-8} + 1$ bons valors. Per definició tenim que j és diferent per cada bon valor. Per tant, unint els dos lemes tenim que la probabilitat d'obtenir un bon parell (c, d) tal que $c \neq 0$ és,

$$2^{l-8} \cdot \frac{1}{2q} \geq 2^{-10}$$

Ja que en tot l'algoritme havíem triat l tal que $2^l < q$ per tant $\frac{2^l}{q} \geq \frac{1}{2}$.
Per últim només cal observar que amb una parella (c, d) on $c \neq 0$, podem aplicar el lema 4.21 i per tant, obtenir r. □

Observació 4.23. Si al lema 4.21 no imposéssim la condició $c \neq 0$, podria passar que t i q compartissin algun factor primer. En aquest cas seguiria sent cert que,

$$\left\lfloor \frac{dq}{2^l} \right\rceil \equiv rt \bmod \left(\frac{q}{\operatorname{mcd}(q, t)}\right)$$

Per tant podem invertir t i a partir de dues observacions, aplicar el teorema xinès dels residus per recuperar r.

4.5 Algoritme de Shor per corbes el·líptiques

Per últim intentem veure com podem aplicar l'algoritme de Shor pel problema del logaritme discret en el cas específic d'una corba el·líptica. Com ja hem vist a la primera secció les corbes més utilitzades en criptografia són les que estan definides sobre $\mathbb{F}_p$. El problema del logaritme discret en aquest cas ve donat pel subgrup generat per un punt $P \in E(\mathbb{F}_q)$ que s'ha triat en cada sistema d'encriptació d'una certa manera. Moltes vegades s'assumeix directament que l'ordre d'aquest subgrup és un altre primer q considerablement gran i que coneixem el seu valor (en cas contrari coneixem un algoritme per trobar-lo). Aquesta assumpció és certa per la majoria de sistemes criptogràfics.

Observació 4.24. De fet, si no fos així i l'ordre del subgrup no fos primer,es coneix una manera estàndard de descompondre el problema del logaritme en una sèrie de logaritmes discrets d'ordre els diferents factors primers de N (cf. [9]). Això va molt bé tenint en compte l'existent algoritme quàntic de Shor per factoritzar enters. Per tant, aquesta assumpció no suposa en realitat, cap pèrdua de generalitat.

Els següents càlculs s'han fet amb l'ajuda del programa *Mathematica*.

Exemple 4.25. Sigui $E(\mathbb{F}_{23})$ la corba definida per l'equació $y^2 = x^3 + 5x + 1$. Notem que $-(4 \cdot 5^3 + 27 \cdot 1^3) = -527 \neq 0$, per tant $E(\mathbb{F}_{23})$ és una corba el·líptica. La corba E té 31 punts.

Triem el punt $P = (0, 1)$ i considerem $Q := 28P = (13, 20)$. Planegem trobar la solució al següent logaritme discret:

$$Q = rP$$

. Veiem que P té ordre 31, per tant $q = 31$. La potència de 2 més propera a 31 és $2^l = 16$, que implica $l = 4$. . Vegem a continuació l'algoritme del logaritme discret aplicat en aquest cas.

Algoritme 11. Donada la corba el·líptica $E(\mathbb{F}_{23})$ definida per $y^2 = x^3 + 5x + 1$, el punt $P = (0, 1)$. El següent algoritme vol trobar el valor r tal que $Q := (13, 20) = rP$.

1. Implementem l'estat incial
$$|0\rangle^{\otimes 4} |0\rangle^{\otimes 4} |0\rangle^{\otimes 4}$$

2. Apliquem la porta Hadamard als dos primers registres i posteriorment la transformació U_F al tercer.
$$\mapsto \frac{1}{16} \sum_{a=0}^{15} \sum_{b=0}^{15} |a\rangle |b\rangle |0\rangle \mapsto \frac{1}{16} \sum_{a=0}^{15} \sum_{b=0}^{15} |a\rangle |b\rangle |aP - bQ\rangle$$

3. Apliquem la transformada de Fourier quàntica d'ordre 16 als dos primers registres.
$$\mapsto \frac{1}{16^2} \sum_{a=0}^{15} \sum_{b=0}^{15} \sum_{c=0}^{15} \sum_{d=0}^{15} \exp\left(\frac{2\pi i(ac + bd)}{16}\right) |c\rangle |d\rangle |aP - bQ\rangle$$

4. Fem una observació. Obtenim una parella (c, d).

Vegem quines seran les bones parelles (c, d) en aquest cas (seguint la definició 4.18).

(i) $\left|\{cq\}_{16}\right| \leq 2^{4-4} = 1$

(ii) $\left|\{cq\}_{16} - f_c\right| \leq 2^{-3}$

De la primera condició n'extraiem $c = 15$ i de la segona $f_c = 1$, per tant

$$d \equiv 1 - 15 \cdot 28 \equiv 13 \pmod{16}$$

Podem comprovar fàcilment com és cert que, a partir d'aquesta bona parella, podem recuperar r. Tenim que,

$$t = \frac{\{cq\}_{16} - cq}{16} = \frac{1 - 15 \cdot 31}{16} = -29$$
$$t^{-1} \equiv 16 \pmod{31}$$
$$\left\lfloor \frac{dq}{2^l} \right\rceil = \left\lfloor \frac{13 \cdot 31}{16} \right\rceil = \left\lfloor \frac{403}{16} \right\rceil = 25$$

I ara aplicant el lema 4.21:

$$r \equiv 25 \cdot 16 \equiv 28 \pmod{31}$$

que és efectivament el valor que buscàvem.
Imaginem que ens hagués sortit una parella que no compleix les condicions de bona parella, per exemple $(c, d) = (2, 8)$. Efectivament,

$$\left|\{2 \cdot 31\}_{16}\right| = 14 > 1$$

Observem que per tant, no obtenim la r correcta quan fem

$$t = \frac{\{2 \cdot 31\}_{16} - 2 \cdot 31}{16} = -3$$
$$t^{-1} \equiv 10 \pmod{31}$$
$$\left\lfloor \frac{dq}{2^l} \right\rceil = \left\lfloor \frac{8 \cdot 31}{16} \right\rceil = 16$$

I clarament no podríem trobar la bona r, ja que aplicaríem el lema 4.21 i ens sortiria:

$$r \equiv 16 \cdot 10 \equiv 5 \not\equiv 28 \pmod{31}.$$

5 Conclusions

Podem extreure diverses conclusions d'aquest treball.
Primer hem vist les bones propietats de les corbes el·líptiques en cossos finits i la seva aplicació en sistemes criptogràfics, com l'intercanvi de claus Diffie Helmann o el sistema ECIES. Entendre com funcionen ens ha fet veure quin hauria de ser el mecanisme per trencar el sistema de xifrat: atacar el problema del logaritme discret.
D'altra banda, introduir-nos en el món de la computació quàntica ens ha permès veure com la superposició d'estats i el paral·lelisme quàntic juguen un paper clau en l'eficiència dels diversos algoritmes estudiats. Hem comprovat com la transformada de Fourier quàntica desenvolupa el rol essencial en tots ells. Això és degut a la seva propietat de transformar una funció de període r sobre un conjunt d'ordre M en un estat on, en fer una observació, s'obté, amb alta probabilitat, un valor que difereix d'un múltiple de M/r, $1/2$ en el pitjor dels casos.
Hem treballat més específicament quins valors es consideren bons per extreure el període r a partir de l'observació, i com la versió en dues dimensions d'aquest procés es correspon a l'algoritme pel problema del logaritme discret de Shor.
El treball intenta cenyir-se al màxim al procés que Peter Shor va seguir per treure els resultats publicats en els seus dos papers [14],[15]. En el llibre de Michael A.Nielsen i Isaac L.Chuang [8] es pot trobar una aproximació a les mateixes qüestions plantejades, a partir de l'algoritme de cerca de fase i l'aplicació de l'inversa de la transformada de Fourier. Aquesta és l'aproximació que actualment es fa servir en la majoria de casos.
Com hem mencionat anteriorment, el treball s'ha centrat en entendre la procedència i funcionalitat de l'algoritme pel problema del logaritme discret. És per això, que dóna peu a la recerca de millors cotes de les que s'han exposat. Shor mateix, en els seus dos papers, en dona aproximacions més fines.
De la mateixa manera que s'obren portes a l'hora de buscar com optimitzar l'algoritme de Shor, se'n poden obrir per estudiar el cas particular de les corbes el·líptiques. Christof Zalka i John Proos donen a [10] algunes idees per corbes el·líptiques sobre $\mathbb{F}_q$ on q és primer, i a [6] Christof Zalka, aquesta vegada amb Phillip Kaye, fan el mateix per corbes el·líptiques sobre $\mathbb{F}_{2^m}$.
Em sembla interessant fer una menció al fet que tots els algoritmes presentats en el treball no deixen de ser un cas particular del problema del subgrup amagat. Donem la versió simplificada, en el cas d'un grup abelià finit, ja és el que ens hem trobat en el nostre estudi.

Donat un grup abelià G, un subgrup $H \subseteq G$ i un conjunt finit X, diem que una funció $f : G \to X$ amaga el subgrup H si per a tot $g_1, g_2 \in G$, $f(g_1) = f(g_2)$ si, i només si $g_1 H = g_2 H$

El problema del subgrup amagat abarca des de qüestions de teoria de nombres fins al problema dels graphs isomorfs.
Finalment, dir que tot i haver vist el potencial que conté la computació quàntica, i la seva visible amenaça per a la majoria de sistemes de xifrat actuals, com ja hem mencionat al principi, estem lluny encara de poder treballar amb un ordinador quàntic prou potent per poder aplicar els algoritmes de Shor a aquestes claus de mida tan gran. A més, en els últims anys s'han iniciat estudis en el camp de la criptografia post-quàntica, com el del sistema SIDH o el sistema CSIDH pel cas de corbes el·líptiques, que busquen nous formes d'encriptar, resistents als atacs quàntics.

Referències

[1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[2] P. Benioff. Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics*, 29(3):515–546, 1982.

[3] M. Ekerå. Modifying shor's algorithm to compute short discrete logarithms. *IACR Cryptology ePrint Archive*, 2016:1128, 2016.

[4] M. Hayward. Quantum computing and shor's algorithm. *Sydney: Macquarie University Mathematics Department.*, 2008.

[5] A. T. i Grau. *Aritmètica*, volume 25. Edicions Universitat Barcelona, 1998.

[6] P. Kaye and C. Zalka. Optimized quantum implementation of elliptic curve arithmetic over binary fields. *arXiv preprint quant-ph/0407095*, 2004.

[7] K.-J. Lange, P. McKenzie, and A. Tapp. Reversible space equals deterministic space. *Journal of Computer and System Sciences*, 60(2):354–367, 2000.

[8] M. A. Nielsen and I. Chuang. Quantum computation and quantum information, 2002.

[9] S. Pohlig and M. Hellman. An improved algorithm for computing logarithms over gf (p) and its cryptographic significance (corresp.). *IEEE Transactions on information Theory*, 24(1):106–110, 1978.

[10] J. Proos and C. Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. *arXiv preprint quant-ph/0301141*, 2003.

[11] F. Puerta Sales. *Algebra lineal*. Number 512.64 PUE. 1976.

[12] M. Roetteler, M. Naehrig, K. M. Svore, and K. Lauter. Quantum resource estimates for computing elliptic curve discrete logarithms. In *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2017.

[13] S. Rudich and A. Wigderson. *Computational complexity theory*, volume 10. American Mathematical Soc., 2004.

[14] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994.

[15] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2), 1999.

[16] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[17] D. R. Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997.

[18] L. C. Washington. *Elliptic curves: number theory and cryptography*. CRC press, 2008.