Introducción a la computación cuántica con autómatas finitos

TRABAJO DE FIN DE GRADO
Curso 2020/2021

UNIVERSIDAD
COMPLUTENSE
MADRID

FACULTAD DE CIENCIAS MATEMÁTICAS
DOBLE GRADO EN MATEMÁTICAS E INGENIERÍA INFORMÁTICA

Director: Manuel Núñez García

Javier Gallego Gutiérrez

Resumen

A lo largo de este trabajo se busca realizar una introducción a la computación cuántica. En primer lugar, presentaremos los formalismos matemáticos necesarios en esta disciplina y comentaremos las nociones más básicas de la misma. En segundo lugar, y partiendo de las nociones introducidas sobre computación cuántica, estudiaremos un marco general de computación: los autómatas finitos cuánticos. Dentro de los autómatas existentes, veremos fundamentalmente dos modelos: los MOQFA y los MMQFA. Presentaremos las definiciones de ambos modelos en su versión unidireccional y la del segundo de ellos en su versión bidireccional. Para la versión unidireccional, estudiaremos su poder a la hora de reconocer lenguajes de dos formas distintas: con error acotado y con error no acotado. Podremos ver que, para la primera forma de aceptación, estos modelos son menos poderosos que sus análogos clásicos. Sin embargo, en el caso del reconocimiento con error no acotado, sucede lo contrario y son más poderosos. Por último, de la versión bidireccional veremos algunos ejemplos que muestran el mayor poder de reconocimiento de lenguajes con error acotado de los modelos cuánticos frente a los clásicos.

Palabras clave. Autómatas finitos cuánticos, reconocimiento con error acotado, reconocimiento con error no acotado

Abstract

Along this document we would like to introduce the main concepts underlying quantum computing. First, we will briefly present the mathematical formalism needed and all the basic concepts of this field. Secondly, we will use the concepts introduced before to study one generic framework of quantum computing: quantum finite automata. Among all existing automata models, we will focus on two of them: MOQFA and MMQFA. We will give their definitions for one-way versions and the definition of the two-way MMQFA. In the one-way case, we will study two ways of language recognition: recognition with bounded error and recognition with unbounded error. For the former way, these models are less powerful than classical automata. Nevertheless, for the latter way of recognition they are more powerful. Finally, we will show some examples of two-way quantum finite automata which confirm two-way quantum versions recognize more languages with bounded error than classical ones.

Keywords. Quantum finite automata, bounded error recognition, unbounded error recognition

Índice general

Capítulo 1

Introducción

1.1 Antecedentes

La computación cuántica es un paradigma de computación distinto al clásico que comenzó a desarrollarse a principios de los años ochenta del siglo XX. A partir de ese momento, se intentó empezar a emplear las leyes de la mecánica cuántica en el mundo de la computación. Fue Benioff el primero en plantear esta posibilidad [5]. Tras él, Richard Feynmann [13] argumentó que un computador cuántico podría realizar algunos cálculos con mayor velocidad que un computador clásico. Poco después, David Deutsch propuso la noción de computador cuántico universal [11]. A partir de estas nociones, en los años noventa, distintos autores ofrecieron ejemplos en que el paradigma cuántico mejoraba en rendimiento al clásico. Algunos de los más conocidos son el algoritmo de Deutsch-Josza [12], el algoritmo de Grover [14] o el algoritmo de Shor para la factorización de enteros [21].

En cuanto a los autómatas finitos cuánticos, se trata de un campo cuyo desarrollo comenzó a finales del siglo XX. Debido al auge de la computación cuántica, se deseaba construir modelos de computación análogos a los modelos clásicos existentes. Es por ello que se desarrollaron modelos correspondientes a los de los autómatas finitos clásicos. El primer modelo de autómata finito cuántico fue presentado por Kondacs y Watrous [17]. Con el tiempo, este modelo ha acabado siendo conocido como MMQFA (*measure many quantum finite automata*). De manera independiente, Moore y Crutchfield [18] presentaron otro modelo, el de los autómatas MOQFA (*measure once quantum finite automata*). Estos dos modelos, que presentan diferencias entre sí, han sido posteriormente estudiados en profundidad. Además, con el tiempo han ido apareciendo otros modelos como el LaQFA (*Latvian Quantum Finite Automata*) [1], NaQFA (*Nayak Quantum Finite Automata*) [19] o generalizaciones de todos ellos como es el caso de los 1QFA (*one-way quantum finite automata*). Este último modelo ha sido definido de muchas maneras equivalentes diferentes (QFA-A, CiQFA, QFA-CL o 1QCFA) por distintos autores.

1.2 Objetivos y plan de trabajo

El objetivo principal de este trabajo es el de adentrarse en el mundo de la computación cuántica. Para ello, se hará uso de los autómatas finitos cuánticos, de los que se presentarán dos modelos distintos. Nos centraremos en el estudio de las versiones unidireccionales, aunque también veremos brevemente la versión bidireccional de uno de los dos modelos.

En primer lugar, en esta memoria encontramos una introducción a la computación cuántica desarrollada a partir del estudio de dos libros introductorios sobre computación cuántica [15, 20]. En ella se recogen las nociones básicas de la computación cuántica que utilizaremos después para estudiar los autómatas. Tras esto, presentamos las dos definiciones de autómatas cuánticos unidireccionales que se emplean a lo largo del trabajo. También recordamos las definiciones de algunos autómatas clásicos que servirán de ayuda para el estudio posterior. A continuación, nos centramos en estudiar la capacidad de reconocimiento de lenguajes por parte de los dos autómatas cuánticos mencionados. Esta capacidad de reconocimiento se estudiará de dos formas distintas: con error acotado y con error no acotado. Podremos comprobar las diferencias de estos modelos con respecto a los modelos clásicos. Por último, presentamos la definición de autómata finito cuántico bidireccional y comprobamos cómo se trata de un modelo capaz de reconocer lenguajes que su análogo clásico no es capaz de reconocer.

Capítulo 2

Breve introducción a la computación cuántica

Este capítulo está dedicado a realizar un resumen sobre los conceptos fundamentales de la computación cuántica. A lo largo de ella, destacamos los cuatro postulados principales de esta disciplina.

2.1 Espacio de Hilbert

En esta sección plantearemos la definición de *espacio de Hilbert* y daremos dos ejemplos de espacios de Hilbert que nos serán de utilidad más adelante.

Definición 2.1.1. Un *espacio con producto interior* H sobre un cuerpo $\mathbb{K}$ (que puede ser $\mathbb{C}$ o $\mathbb{R}$) es un espacio vectorial equipado con un producto interior (o producto escalar), que es una función $\langle \cdot, \cdot \rangle : H \times H \to \mathbb{K}$ que satisface:

1. $\langle x, x \rangle \geq 0$. $\langle x, x \rangle = 0 \Leftrightarrow x = 0$
2. $\langle x, y \rangle = \langle y, x \rangle^*$
3. $\langle x, ay + bz \rangle = a \langle x, y \rangle + b \langle x, z \rangle$ para $a, b \in \mathbb{K}$

Este producto interior induce la norma $\|\cdot\| : H \to \mathbb{R}$ dada por

$$\|x\| = \sqrt{\langle x, x \rangle}$$

A su vez, la norma induce la distancia entre dos vectores $d : H \times H \to \mathbb{R}$ dada por

$$d(x, y) = \|x - y\|$$

Definición 2.1.2. Un *espacio de Hilbert* H es un espacio con producto interior que es completo con respecto a la distancia inducida por su norma.
Un espacio con producto interior H es completo si toda sucesión de Cauchy en H es convergente.

Para definir la noción de espacio de Hilbert hemos empleado la notación habitual. Sin embargo, en la mayoría del trabajo utilizaremos la notación de Dirac, donde un vector de un espacio de Hilbert H se escribirá como $|\psi\rangle$. Este representa un vector columna denominado *ket*. El vector conjugado traspuesto de $|\psi\rangle$, $|\psi\rangle^\dagger$, es el vector fila $\langle\psi|$ y recibe

el nombre de *bra*. Cabe destacar que a lo largo del trabajo emplearemos el símbolo † para representar el conjugado traspuesto de un vector o una matriz y el símbolo $*$ para representar el conjugado de cualquier elemento (ya sea una matriz, un vector o un escalar). Por último, el producto interior de dos vectores $|\psi\rangle, |\phi\rangle$ se expresa como $\langle\psi|\phi\rangle$ y el producto exterior como $|\psi\rangle\langle\phi|$.

El ejemplo más importante de espacio de Hilbert con el que trataremos es el de $\mathbb{C}^n$. Para este espacio consideraremos el producto interior usual de dos vectores $|\psi_1\rangle = (\alpha_1, \ldots, \alpha_n)^T$ y $|\psi_2\rangle = (\beta_1, \ldots, \beta_n)^T \in H$ dado por

$$\langle\psi_1|\psi_2\rangle = \sum_{i=1}^{n} \alpha_i^* \beta_i$$

Además, el producto exterior es

$$|\psi_1\rangle\langle\psi_2| = \begin{pmatrix} \alpha_1\beta_1^* & \alpha_1\beta_2^* & \ldots & \alpha_1\beta_n^* \\ \alpha_2\beta_1^* & \alpha_2\beta_2^* & \ldots & \alpha_2\beta_n^* \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_n\beta_1^* & \alpha_n\beta_2^* & \ldots & \alpha_n\beta_n^* \end{pmatrix}$$

Otro ejemplo de espacio de Hilbert en el que estamos interesados es el siguiente.

Definición 2.1.3. Dado un conjunto numerable Q, $\ell_2(Q)$ es el espacio de todas las funciones complejas $x : Q \to \mathbb{C}$ tales que $\left(\sum_{i\in Q} x^*(i)x(i)\right)^{1/2} < \infty$. Nótese que $\ell_2(Q)$ es un espacio de Hilbert respecto del producto interior

$$\begin{aligned} \ell_2(Q) \times \ell_2(Q) &\to \mathbb{C} \\ (x_1, x_2) &\mapsto \langle x_1 \mid x_2\rangle = \sum_{i\in Q} x_1^*(i)x_2(i) \end{aligned}$$

Esta definición vale para cualquier conjunto Q numerable. En el caso finito, se tiene que $\ell_2(Q)$ es isomorfo al espacio $\mathbb{C}^n$. Es fácil de ver, pues si $Q = \{q_1, \ldots, q_n\}$ y tenemos una función $x : Q \to \mathbb{C}$, esta puede identificarse con el vector $|\psi\rangle = (x(q_1), \ldots, x(q_n))^T$ y, para dos vectores $|\psi_1\rangle = (\alpha_1, \ldots, \alpha_n)^T$ y $|\psi_2\rangle = (\beta_1, \ldots, \beta_n)^T$, se tiene

$$\langle\psi_1|\psi_2\rangle = \sum_{i=1}^{n} \alpha_i^*\beta_i = \sum_{q_i\in Q} x_1^*(q_i)x_2(q_i) = \langle x_1|x_2\rangle$$

donde x_1 y x_2 son las funciones con imágenes $x_1(q_i) = \alpha_i$, $x_2(q_i) = \beta_i$ para $1 \le i \le n$.

2.2 Estado cuántico

El primer postulado de la computación cuántica tiene que ver con el espacio en que se mueve un sistema cuántico.

Postulado 1. Todo sistema cuántico tiene asociado un espacio vectorial complejo con producto interior, es decir, un espacio de Hilbert conocido como *espacio de estados* del sistema. El sistema viene descrito por un vector de estado, que es un vector unitario del espacio de estados del sistema.

En este trabajo estamos interesados exclusivamente en el caso de un espacio de Hilbert finito. De esta forma, según el postulado anterior un estado de un sistema cuántico será un vector unitario de coeficientes complejos (llamados *amplitudes*) de la forma:

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Como el vector ha de ser unitario, es necesario que se verifique la siguiente condición:

$$\||\psi\rangle\|^2 = \langle\psi|\psi\rangle = |\alpha_1|^2 + |\alpha_2|^2 + \ldots + |\alpha_n|^2 = 1$$

De cualquier espacio de Hilbert H podemos considerar una base ortonormal $B = \{|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_n\rangle\}$. Es posible trabajar en esta base y escribir un estado como

$$|\psi\rangle = \alpha_1 |\phi_1\rangle + \alpha_2 |\phi_2\rangle + \ldots + \alpha_n |\phi_n\rangle$$

Los vectores $|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_n\rangle$ reciben el nombre de *estados básicos* y la base B, el de *base computacional*. Suele decirse que el sistema se encuentra en una *superposición* de los estados $|\phi_1\rangle, \ldots, |\phi_n\rangle$.

El ejemplo más sencillo de sistema cuántico es el del *qubit*.

Definición 2.2.1. Un *qubit* es un sistema cuántico que tiene asociado un espacio de Hilbert H bidimensional. Una base ortonormal de este estado suele escribirse como $\{|0\rangle, |1\rangle\}$ y un estado cualquiera del espacio de estados se expresa en esta base como

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$$

donde $\alpha, \beta \in \mathbb{C}$ verifican $|\alpha|^2 + |\beta|^2 = 1$.

2.3 Transformaciones unitarias

El segundo postulado de la computación cuántica tiene que ver con la evolución de un sistema cuántico. Hace uso del concepto de *transformación unitaria*, que introducimos antes de plantear el postulado.

Definición 2.3.1. Una *transformación unitaria* es un isomorfismo lineal entre dos espacios de Hilbert H_1 y H_2, $T : H_1 \to H_2$, que verifica la condición $\langle Tx, Ty\rangle_{H_2} = \langle x, y\rangle_{H_1}$.

Una transformación unitaria tiene asociada una matriz U que recibe el nombre de *matriz unitaria*. En el caso complejo se define de la siguiente forma.

Definición 2.3.2. Una *matriz unitaria* es una matriz cuadrada $U \in \mathfrak{M}_n(\mathbb{C})$ que verifica

$$UU^\dagger = I$$

Una condición equivalente a la de la definición anterior para que una matriz sea unitaria es que las columnas de la matriz U formen una base ortonormal de $\mathbb{C}^n$.

Una vez presentados estos conceptos preliminares, ya es posible introducir el segundo postulado de la computación cuántica.

Postulado 2. La evolución de un sistema cuántico cerrado viene descrita por una transformación unitaria. Esto es, el estado $|\psi\rangle$ de un sistema cuántico en un tiempo t_1 está relacionado con el estado $|\psi'\rangle$ en un tiempo t_2 por un operador unitario U que depende únicamente de los tiempos t_1 y t_2,

$$|\psi'\rangle = U\,|\psi\rangle$$

Por la definición de transformación unitaria sabemos que la condición de que el vector sea unitario se cumplirá en todo momento pues

$$\langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle = 1$$

2.3.1 Transformada cuántica de Fourier

Un ejemplo de transformación unitaria es el de la *transformada cuántica de Fourier*, que es la transformación cuántica análoga a la transformada de Fourier discreta. En la transformada discreta de Fourier, un vector $(x_0, x_1, \ldots, x_{N-1})$ es transformado en el vector $(y_0, y_1, \ldots, y_{N-1})$ donde

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{\frac{2\pi i}{N} jk} \tag{2.1}$$

La transformada cuántica de Fourier toma una base ortonormal $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$ y asocia a cada vector $|j\rangle$ el valor dado por la siguiente expresión:

$$QFT_N : |j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=1}^{N} e^{\frac{2\pi i}{N} jk}$$

Así, la transformación sobre un vector cualquiera es

$$\sum_{j=0}^{N-1} x_j\,|j\rangle \mapsto \sum_{k=0}^{N-1} y_k\,|k\rangle$$

donde la amplitud y_k es como en la ecuación (2.1).

Ahora, si consideramos $\omega = e^{\frac{2\pi i}{N}}$ (que es una de las raíces N-ésimas de la unidad), podemos escribir la matriz unitaria F_N asociada a esta transformación de la siguiente manera

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)^2} \end{pmatrix}$$

Se trata de una matriz unitaria. Considerando los vectores $|\psi_{j_1}\rangle = (\alpha_0, \alpha_1, \ldots, \alpha_{N-1})^T$ y $|\psi_{j_2}\rangle = (\beta_1, \beta_2, \ldots, \beta_{N-1})^T$ correspondientes a dos columnas distintas de la matriz $j_1, j_2 \in \{0, 1, \ldots, N-1\}$, el producto escalar de ambas será

$$\langle\psi_{j_1}|\psi_{j_2}\rangle = \sum_{k=0}^{N-1} \alpha_k^* \beta_k = \sum_{k=0}^{N-1} \frac{1}{\sqrt{N}} \omega^{-j_1 k} \frac{1}{\sqrt{N}} \omega^{j_2 k} = \sum_{k=0}^{N-1} \frac{1}{N} \omega^{-j_1 k + j_2 k} = \frac{1}{N} \sum_{k=0}^{N-1} (\omega^{(j_2 - j_1)})^k$$

Como $j_2 \neq j_1$, entonces $\sum_{k=0}^{N-1}(\omega^{(j_2-j_1)})^k$ es la suma parcial de una serie geométrica de razón $\omega^{(j_2-j_1)}$, por lo que es igual a

$$\frac{1-(\omega^{(j_2-j_1)})^N}{1-\omega^{(j_2-j_1)}} = \frac{1-\omega^{N(j_2-j_1)}}{1-\omega^{(j_2-j_1)}} = \frac{1-1^{(j_2-j_1)}}{1-\omega^{(j_2-j_1)}} = 0$$

Además, estos vectores son claramente unitarios, pues

$$\langle\psi_j|\psi_j\rangle = \frac{1}{N}\sum_{k=0}^{N-1}(\omega^{(j-j)})^k = \frac{1}{N}\sum_{k=0}^{N-1}1^k = 1$$

2.4 Medición de un estado

El tercer postulado de la computación cuántica tiene que ver con la interacción con el sistema por parte de un agente externo interesado en obtener información acerca del mismo.

Postulado 3. Una medición de un sistema cuántico viene dada por un conjunto de *operadores de medición* $\{M_m\}$ que actúan sobre el espacio de estados que quiere ser medido. El índice m se corresponde con el posible resultado que puede obtenerse en el experimento. Si el estado del sistema es $|\psi\rangle$ antes de la medición, entonces la probabilidad de que el resultado m ocurra viene dada por

$$\langle\psi|M_m^\dagger M_m|\psi\rangle$$

y el siguiente estado del sistema en ese caso es

$$\frac{M_m\,|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

Los operadores de medición satisfacen la *condición de completitud*

$$\sum_m M_m^\dagger M_m = I$$

De ese modo, la suma de las probabilidades anteriores es igual a 1, pues

$$\sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|I|\psi\rangle = 1$$

2.4.1 Medición proyectiva

En esta sección nos centraremos en un caso particular de medición: las mediciones proyectivas. Estas son las que usaremos a lo largo del resto del trabajo. Nótese que en la literatura existen otros tipos de mediciones como pueden ser las mediciones POVM.

En el caso de las mediciones proyectivas, los operadores $\{M_m\}$ son proyecciones ortogonales $\{P_m\}$ sobre subespacios. Estos operador son idempotentes y hermíticos, es decir, verifican $P_m^2 = P_m$ y $P_m = P_m^\dagger$. Estos subespacios llevan a la definición de *observable*.

Definición 2.4.1. Un *observable* es un conjunto de subespacios de H disjuntos y ortogonales entre sí $\mathcal{O} = \{E_1, E_2, \ldots, E_k\}$ de modo que $H = E_1 \oplus E_2 \oplus \ldots \oplus E_k$.

Al realizar una medición respecto al observable $\mathcal{O}$, se obtendrá el subespacio E_i con probabilidad

$$\langle\psi|P_i|\psi\rangle = \|P_i|\psi\rangle\|^2$$

donde P_i es la proyección ortogonal sobre el subespacio E_i. Si el resultado de la medición es haber observado el subespacio E_i, el siguiente estado en que se encontrará el sistema es

$$\frac{P_i|\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}}$$

Si tenemos un subespacio E_i del espacio de Hilbert H anterior, podemos considerar una base del mismo $B_i = \{|\phi_1\rangle, \ldots, |\phi_m\rangle\}$ donde $m \leq n = \dim(H)$. Podemos entonces considerar una base de H

$$B = \cup_{i=1}^{k} B_i$$

El operador proyección P_i sobre el subespacio E_i será

$$P_i = \sum_{j=1}^{m} |\phi_j\rangle\langle\phi_j|$$

Un caso particular de medición proyectiva es el de la *medición en la base computacional*. Si tenemos un espacio de dimensión n con base $B = \{|\phi_1\rangle, \ldots, |\phi_n\rangle\}$ y un estado del sistema $|\psi\rangle = \alpha_1|\phi_1\rangle + \ldots + \alpha_n|\phi_n\rangle$, no será posible observar la superposición de estados de la base. Si consideramos como operadores de medición las proyecciones sobre cada estado cada estado de la base, tenemos que un estado $|\phi_i\rangle$ será observado con probabilidad $|\alpha_i|^2$. Tras la medición, el sistema colapsará en el estado $|\phi_i\rangle$.

2.5 Sistemas compuestos

En primer lugar, planteamos la definición de producto tensorial de dos vectores.

Definición 2.5.1. Dados dos vectores de dos espacios de Hilbert cualesquiera $|\psi\rangle = (\alpha_1, \alpha_2, \ldots, \alpha_m)^T \in H_1, |\phi\rangle = (\beta_1, \beta_2, \ldots, \beta_n)^T \in H_2$, definimos el *producto tensorial de los dos vectores* como el vector

$$|\psi\rangle \otimes |\phi\rangle = (\alpha_1\beta_1, \ldots, \alpha_1\beta_n, \alpha_2\beta_1, \ldots, \alpha_2\beta_n, \ldots, \alpha_m\beta_1, \ldots, \alpha_m\beta_n)^T$$

A partir de esta definición, podemos definir la noción de producto tensorial de dos espacios de Hilbert.

Definición 2.5.2. Dados dos espacios de Hilbert H_1 y H_2 de dimensiones m y n, respectivamente, el *producto tensorial de ambos espacios* es el espacio

$$H = H_1 \otimes H_2$$

de dimensión $m \cdot n$, donde un vector $|\psi\rangle \in H$ es el producto tensorial de dos vectores $|\psi\rangle \in H_1$ y $|\phi\rangle \in H_2$. En particular, si tenemos dos bases $B_1 = \{|\phi_1\rangle, \ldots, |\phi_m\rangle\}, B_2 = \{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ de H_1 y H_2, respectivamente, puede obtenerse la base de H

$$B = \{|\phi_i\rangle \otimes |\psi_j\rangle \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$$

Además, el producto interior en este espacio es

$$\langle\psi_1 \otimes \psi_2|\phi_1 \otimes \phi_2\rangle = \langle\psi_1|\phi_1\rangle_{H_1}\langle\psi_2|\phi_2\rangle_{H_2}$$

donde $\psi_1, \phi_1 \in H_1$ y $\psi_2, \phi_2 \in H_2$.

A su vez, el producto tensorial también está definido en el caso de las matrices.

Definición 2.5.3. Dadas dos matrices $A \in \mathfrak{M}_{m,n}$ y $B \in \mathfrak{M}_{p,q}$, el *producto tensorial de ambas matrices* es la matriz $A \otimes B \in \mathfrak{M}_{m\cdot p,n\cdot q}$ dada por

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}$$

A partir de la noción de producto tensorial podemos plantear el cuarto postulado de la computación cuántica. Este postulado tiene que ver con la formación de sistemas compuestos por varios sistemas cuánticos.

Postulado 4. El espacio de estados de un sistema compuesto es el producto tensorial del espacio de estados de los sistemas que lo componen. Además, si tenemos n sistemas y cada sistema i se encuentra en el estado $|\psi_i\rangle$, entonces el estado del sistema compuesto es $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

2.5.1 Registro cuántico de varios qubits

Un ejemplo de sistema compuesto es el de un *registro cuántico*, que es un sistema de varios qubits: si tenemos dos sistemas de un qubit y se considera la base ortonormal $\{|0\rangle, |1\rangle\}$ en ambos casos, tomaremos como base del registro cuántico $B = \{|0\rangle, |1\rangle\} \otimes \{|0\rangle, |1\rangle\}$. Esta base se suele escribir como $B = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, donde $|ij\rangle = |i\rangle \otimes |j\rangle$. Entonces, a partir dos qubits $|\psi_1\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ y $|\psi_2\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$, el producto tensorial de ambos qubits será

$$\begin{aligned} |\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle &= (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \\ &= (\alpha_0, \alpha_1) \otimes (\beta_0, \beta_1) = \alpha_0\beta_0 |00\rangle, \alpha_0\beta_1 |01\rangle, \alpha_1\beta_0 |10\rangle, \alpha_1\beta_1 |11\rangle \end{aligned}$$

Esta noción puede generalizarse para considerar registros de n qubits. En ese caso, tendremos el espacio de Hilbert 2^n-dimensional con la base $B = \{|i\rangle \mid \ i \in \{0,1\}^n\}$. Por tanto, la dimensión del espacio de Hilbert crece exponencialmente en función del número de qubits.

Sin embargo, no todos los estados cuánticos pueden ser representados mediante el producto tensorial de estados de dimensión inferior. Un ejemplo de ello es el conocido como *estado de Bell*

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Intentemos expresar este estado como el producto tensorial de dos qubits

$$\begin{aligned} \frac{|00\rangle + |11\rangle}{\sqrt{2}} &= (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \\ &= \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle \end{aligned}$$

Ha de verificarse $\alpha_0\beta_1 = \alpha_1\beta_0 = 0$, pero para eso es necesario que α_0 o β_1 sean 0 y que α_1 o β_0 también. Esto haría 0 la amplitud de $|00\rangle$ o la de $|11\rangle$. Por tanto, es imposible expresar el estado de Bell como producto tensorial de dos qubits. Un estado como este,

que no puede ser expresado mediante un producto tensorial recibe el nombre de *estado entrelazado*.

Una propiedad de este tipo de estados tiene que ver con los resultados de algunas mediciones. Por ejemplo, sea el *estado de Bell* y consideremos el observable $\mathcal{O}_1 = \{\text{span}(|00\rangle, |01\rangle), \text{span}(|10\rangle, |11\rangle)\}$ donde $\text{span}(|\psi_1\rangle, \ldots, |\psi_k\rangle)$ representa el subespacio generado por los vectores $|\psi_1\rangle, \ldots, |\psi_k\rangle$. Obtendremos el primer subespacio (asociado a que el primer qubit sea 0) con probabilidad $\frac{1}{2}$. En ese caso, el estado colapsará en $|00\rangle$. Si ahora queremos volver a medir, en esta ocasión haciendo uso del observable $\mathcal{O}_2 = \{\text{span}(|00\rangle, |10\rangle), \text{span}(|01\rangle, |11\rangle)\}$, obtendremos el valor 0 con probabilidad 1. Al hacer la primera medición, también se obtiene el valor 1 con probabilidad $\frac{1}{2}$. En ese caso, el estado siguiente es $|11\rangle$. Al medir con respecto a $\mathcal{O}_2$, obtendríamos el valor 1 con probabilidad 1. Queda entonces claro que el resultado de la segunda observación viene siempre determinado por el resultado obtenido en la primera.

2.6 Estados mixtos y el operador densidad

Los estados que hemos definido anteriormente suelen denominarse estados cuánticos puros. También existen los llamados *estados mixtos*.

Definición 2.6.1. Un *estado mixto* es una combinación probabilista de estados cuánticos puros $\{(p_i, |\psi_i\rangle) \mid 1 \geq i \geq k\}$ donde cada $|\psi_i\rangle$ es un estado cuántico y para todo i, $p_i \geq 0$ representa la probabilidad de estar en el estado $|\psi_i\rangle$. Además, se verifica la siguiente propiedad:

$$p_1 + p_2 + \ldots + p_k = 1$$

A partir de la noción de estado mixto se define el *operador densidad*. Es posible describir un sistema cuántico mediante este operador en lugar de mediante un vector.

Definición 2.6.2. Dado un estado mixto $\{(p_i, |\psi_i\rangle) \mid 1 \geq i \geq k\}$, se define el *operador densidad* ρ asociado a él como

$$\rho = \sum_{i=1}^{k} p_i |\psi_i\rangle \langle\psi_i|$$

La evolución del sistema que viene dada por una transformación unitaria modificará el operador densidad de la siguiente manera

$$\rho \to \sum_{i=1}^{k} p_i U |\psi\rangle \langle\psi| U^\dagger = U\rho U^\dagger$$

Además, si se realiza una medición con el conjunto de operadores de medición $\{M_m\}$, la probabilidad de obtener el valor m viene dada por la expresión

$$\sum_{i=1}^{n} p_i \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \sum_{i=1}^{n} p_i \sum_j \langle j|M_m^\dagger M_m |\psi_i\rangle \langle\psi_i| j\rangle = \sum_{i=1}^{n} p_i tr(M_m^\dagger M_m |\psi_i\rangle \langle\psi_i|)$$

$$= \sum_{i=1}^{n} tr(p_i M_m^\dagger M_m |\psi_i\rangle \langle\psi_i|) = tr(M_m^\dagger M_m \sum_{i=1}^{n} p_i |\psi_i\rangle \langle\psi_i|) = tr(M_m^\dagger M_m \rho)$$

y el nuevo operador densidad será

$$\frac{M_m \rho M_m^\dagger}{tr(M_m^\dagger M_m \rho)}$$

Capítulo 3

Autómatas finitos cuánticos unidireccionales

A lo largo de este capítulo, y haciendo uso de las nociones presentadas en el capítulo anterior, estudiaremos los principales modelos de autómatas finitos cuánticos y su capacidad de aceptación de lenguajes según dos definiciones distintas de aceptación. Antes de introducir estos autómatas, veremos las definiciones de algunos autómatas clásicos que utilizaremos más adelante para estudiar las propiedades de los autómatas cuánticos.

3.1 Autómatas finitos deterministas

Los autómatas finitos clásicos representan un modelo de computación ampliamente conocido. Existen diversos modelos de autómatas finitos: deterministas, no deterministas y no deterministas con transiciones ϵ. Sin embargo, todos ellos tienen el mismo poder de reconocimiento: son capaces de reconocer cualquier lenguaje regular.

Definición 3.1.1. Un *autómata finito determinista* (AFD) es una 5-tupla

$$(\Sigma, S, s_0, \delta, F)$$

donde

- Σ es un alfabeto de entrada.
- S es un conjunto finito de estados.
- $s_0 \in S$ es el estado inicial del autómata.
- $\delta : S \times \Sigma \to S$ es una función de transición.
- $F \subseteq S$ es un conjunto de estados de aceptación.

Un AFD comienza a leer una cadena $w \in \Sigma^*$ partiendo del estado inicial s_0. Lee el primer símbolo σ de w y pasa al estado $\delta(s_0, \sigma)$. Este proceso se repite hasta leer la palabra completa. En ese momento, si el autómata se encuentra en un estado $s \in F$, la palabra es aceptada. Si $s \notin F$, la palabra es rechazada.

Dado un AFD, se define el lenguaje reconocido por el autómata como el conjunto $L = \{w \in \Sigma^* \mid \hat{\delta}(w, s_0) \in F\}$ donde si $w = \sigma_1\sigma_2 \cdots \sigma_n$, $\hat{\delta}(w, s_0) = \delta(\sigma_n, \delta(\ldots(\delta(\sigma_1, s_0))))$.

Dentro de los autómatas finitos deterministas existe un tipo que nos será útil más adelante.

Definición 3.1.2. Un *group finite automata* (GFA) es un autómata finito determinista que cumple que para todo estado $s \in S$ y todo símbolo $\sigma \in \Sigma$ hay exactamente un estado s' tal que $\delta(s', \sigma) = s$.

Los lenguajes reconocidos por un *group finite automata* se denominan *group languages*.

3.2 Autómatas finitos probabilísticos

Una generalización de los autómatas finitos clásicos es la de los autómatas probabilísticos. En este tipo de autómata, en lugar de estar el autómata en un estado concreto, se dispone de una distribución de probabilidad sobre los estados en que puede estar el autómata. En este caso, las transformaciones vienen dadas por matrices.

Definición 3.2.1. Un *autómata finito probabilístico* (PFA) es una 5-tupla

$$(\Sigma, S, \{A_\sigma \mid \sigma \in \Sigma\}, v_0, F)$$

donde

- Σ es un alfabeto de entrada.
- $S = \{s_0, s_1, \ldots, s_{n-1}\}$ es un conjunto de estados.
- A_σ es una *matriz estocástica*. Una matriz estocástica A_σ verifica que para todo elemento a_{ij} de A_σ, $0 \leq a_{ij} \leq 1$, y para cada columna j, $\sum_{i=1}^{n} a_{ij} = 1$. En particular, el elemento a_{ij} representa la probabilidad de pasar del estado s_j al estado s_i tras leer el símbolo σ.
- v_0 es un vector columna de dimensión n que representa la distribución inicial de estados. La componente i-ésima v_{0i} representa la probabilidad de que el estado inicial sea s_i. Así, para cada componente de v_0 se verifica $0 \leq v_{0i} \leq 1$. Además, todas ellas cumplen $\sum_{i=0}^{n-1} v_{0i} = 1$.
- $F \subseteq S$ es el conjunto de estados de aceptación.

Un autómata probabilístico lee una cadena $w = \sigma_1\sigma_2 \cdots \sigma_n \in \Sigma^*$ y la acepta si el estado final está en F. Este cómputo puede ser descrito de la siguiente manera: el estado inicial v_0 es transformado mediante la matriz A_{σ_1} y se obtiene el vector $v_1 = A_{\sigma_1} v_0$, que describe la probabilidad de que el autómata esté en cada uno de los estados de S tras la lectura de σ_1. Este proceso se repite para el resto de símbolos de w. De este modo, la distribución de estados final vendrá dada por el vector

$$v_n = A_{\sigma_n} \cdots A_{\sigma_2} A_{\sigma_1} v_0 \tag{3.1}$$

Una cadena es aceptada por el autómata si el estado final está en F. Como el vector v_n anterior representa la distribución de estados tras leer la cadena w, la probabilidad de aceptación de w será igual a

$$f(w) = \sum_{s_i \in F} v_{ni}$$

Como en un autómata probabilístico no se acepta o se rechaza una cadena en todos los casos sino que se hace con una cierta probabilidad, es necesaria una definición que determine qué lenguaje se considera que reconoce el autómata.

Definición 3.2.2. Se llama lenguaje reconocido con *punto de corte estricto* $\lambda \in \mathbb{R}$ al conjunto de palabras

$$L = \{w \in \Sigma^* \mid f(w) > \lambda\}$$

En caso de que la condición sea $f(w) \geq \lambda$, se dice que el lenguaje es reconocido por un autómata con *punto de corte no estricto*. Los lenguajes reconocidos por un autómata probabilístico con punto de corte estricto reciben el nombre de *lenguajes estocásticos*. Además, para cualquier lenguaje estocástico L y para cualquier $\lambda \in (0, 1)$ es posible construir un PFA que reconozca L con punto de corte estricto λ [23].

Por otra parte, la definición de autómata probabilístico anterior puede generalizarse de la siguiente manera.

Definición 3.2.3. Un *autómata probabilístico generalizado* (GPFA) es un PFA en el que v_0 y las matrices A_σ son reales, pero no necesariamente estocásticas. Además, en lugar de tener un conjunto de estados finales F, se tiene un vector fila real v_{acc}, tal que la imagen de la función de aceptación para una cadena $w \in \Sigma^*$ es igual a

$$f(w) = v_{acc} v_n$$

donde v_n es un vector calculado como en la ecuación 3.1.

Es conocido que los GPFAs reconocen con punto de corte no estricto exactamente el conjunto de los lenguajes estocásticos [23].

3.3 MOQFA

Estamos en disposición de presentar el primer modelo de autómata cuántico: los autómatas finitos cuánticos *measure once* (MOQFA) propuestos por Moore y Crutchfield [18].

Definición 3.3.1. Un *autómata finito cuántico measure once (MOQFA)* es una 5-tupla

$$(\Sigma, H, \{U_\sigma \mid \sigma \in \Sigma\}, |s_{init}\rangle, H_{acc})$$

donde:

- Σ es el alfabeto de entrada.
- H es un espacio de Hilbert de dimensión finita. Este espacio suele venir dado por un conjunto de estados clásicos $Q = \{|q_0\rangle, |q_1\rangle, \ldots, |q_n\rangle\}$, es decir, $H = \ell_2(Q)$.
- U_σ es la matriz unitaria que determina la transición correspondiente al símbolo $\sigma \in \Sigma$.
- $|s_{init}\rangle \in H$ es el estado inicial (que ha de cumplir $\||s_{init}\rangle\|^2 = 1$).
- H_{acc} es un subespacio del espacio de Hilbert H llamado subespacio de aceptación y P_{acc} una proyección sobre él.

El autómata lee una palabra $w = \sigma_1\sigma_2\cdots\sigma_n \in \Sigma^*$, símbolo a símbolo, aplicando la transformación U_σ correspondiente en cada caso sobre el estado $|\psi\rangle$ del autómata, que empieza siendo $|s_{init}\rangle$. Tras leer entera la palabra, se observa y se acepta si se obtiene un elemento que pertenece al subespacio de aceptación H_{acc}. La probabilidad de obtener un elemento de H_{acc} será igual a

$$\|P_{acc} U_{\sigma_n} \cdots U_{\sigma_1} |s_{init}\rangle\|^2$$

3.3.1 Definiciones alternativas

La definición anterior es exactamente la que plantearon Moore y Crutchfield. Sin embargo, en ocasiones es posible encontrar una definición equivalente en la que se considera el alfabeto $\tilde{\Sigma} = \Sigma \cup \{\#, \$\}$ donde # y \$ son los símbolos que marcan el principio y el final de la palabra. Además, se considera como estado inicial un estado clásico $|q_0\rangle \in Q$ y la transformación $U_\#$ es la que permite que el autómata comience en cualquier estado $|\psi\rangle$ de norma uno. Para pasar de una definición a otra basta con modificar las matrices unitarias y seleccionar el estado inicial de forma apropiada.

Esta nueva definición todavía puede ser simplificada, pues en realidad no es necesario el símbolo #. Si tenemos un autómata MOQFA M que satisface la definición anterior, podemos construir un MOQFA M' equivalente sin la necesidad de #. Veámoslo:

Si las transformaciones unitarias de M vienen dadas por las matrices U_σ para $\sigma \in \tilde{\Sigma}$, consideramos las transformaciones unitarias $U'_\sigma = U_\#^{-1} U_\sigma U_\#$ para $\sigma \in \Sigma$ y $U'_\$ = U_\$ U_\#$. Así, para $w = \sigma_1 \cdots \sigma_n \in \Sigma^*$, tendremos

$$\begin{aligned} U'_w |q_0\rangle = U'_\# U'_{\sigma_n} \cdots U'_{\sigma_1} w &= U_\$ U_\# U_\#^{-1} U_{\sigma_n} U_\# \cdots U_\#^{-1} U_{\sigma_1} U_\# |q_0\rangle \\ &= U_\$ U_{\sigma_n} \cdots U_{\sigma_1} U_\# |q_0\rangle = U_w |q_0\rangle \end{aligned}$$

El motivo de introducir estas definiciones alternativas se debe a su mayor parecido con la definición del otro modelo que nos interesa y que introduciremos a continuación.

3.4 MMQFA

Los autómatas finitos cuánticos *measure many* (MMQFA) fueron propuestos por Kondacs y Watrous [17] y su principal diferencia con respecto a los MOQFA está en que se realiza una medición tras la lectura de cada símbolo, no solo al final.

Definición 3.4.1. Un *autómata finito cuántico measure many (MMQFA)* es una 7-tupla

$$(\Sigma, H, \{U_\sigma \mid \sigma \in \tilde{\Sigma}\}, |q_0\rangle, H_{acc}, H_{rej}, H_{non})$$

que presenta las siguientes diferencias respecto a la definición 3.3.1:

- Se tiene en cuenta el alfabeto $\tilde{\Sigma} = \Sigma \cup \{\#, \$\}$.
- El estado inicial $|s_{init}\rangle$ es un estado clásico, por lo que se suele expresar como $|q_0\rangle \in Q$.
- La regla de aceptación es diferente a la de los MOQFA. Se divide H en tres subespacios H_{acc}, H_{rej} y H_{non} de modo que $H = H_{acc} \oplus H_{rej} \oplus H_{non}$. Tras la lectura de un símbolo $\sigma \in \Sigma$, se realiza una observación. Si se obtiene H_{acc}, la ejecución termina y se acepta la cadena. Si es H_{rej}, la ejecución también termina pero no se acepta la cadena. Por último, si obtenemos H_{non}, la ejecución continúa salvo si se ha leído ya la palabra completa (incluído \$), en cuyo caso se rechaza. Además, si tras medir la ejecución continúa, el siguiente estado en que nos encontraremos será $\dfrac{P_{non} U_\sigma |\psi\rangle}{\|P_{non} U_\sigma |\psi\rangle\|}$.

  De este modo, tras la lectura de un símbolo σ, el autómata aceptará con probabilidad $\|P_{acc} U_\sigma |\psi\rangle\|^2$, rechazará con probabilidad $\|P_{rej} U_\sigma |\psi\rangle\|^2$ y continuará con probabilidad $\|P_{non} U_\sigma |\psi\rangle\|^2$.

3.4.1 Eliminación del símbolo

Igual que antes, en este caso también es posible prescindir del símbolo #. Si tenemos un MMQFA $M = (\Sigma, H, \{U_\sigma \mid \sigma \in \tilde{\Sigma}\}, |q_0\rangle, H_{acc}, H_{rej}, H_{non})$ donde $H = \ell_2(Q)$ con $Q = Q_{non} \cup Q_{acc} \cup Q_{rej}$, podemos construir un autómata equivalente

$$M' = (\Sigma, H', \{U'_\sigma \mid \sigma \in \Sigma \cup \{\$\}\}, |q'_0\rangle, H'_{acc}, H'_{rej}, H'_{non})$$

que no haga uso de #. Consideremos sin pérdida de generalidad que

$$Q = \{|q_{non_1}\rangle, \ldots, |q_{non_j}\rangle, |q_{acc_1}\rangle, \ldots, |q_{acc_k}\rangle, |q_{rej_1}\rangle, \ldots, |q_{rej_l}\rangle\}$$

con $Q_{non} = \{|q_{non_1}\rangle, \ldots, |q_{non_j}\rangle\}$, $Q_{acc} = \{|q_{acc_1}\rangle, \ldots, |q_{acc_k}\rangle\}$ y $Q_{rej} = \{|q_{rej_1}\rangle, \ldots, |q_{rej_l}\rangle\}$ determinan H_{non}, H_{acc} y H_{rej}, respectivamente. A partir de estos estados, construimos el conjunto

$$Q' = \{|q_{non_1}\rangle, \ldots, |q_{non_j}\rangle, |q_{acc_1}\rangle, \ldots, |q_{acc_k}\rangle, |q_{rej_1}\rangle, \ldots, |q_{rej_l}\rangle, |q'_{acc_1}\rangle, \ldots, |q'_{acc_k}\rangle, |q'_{rej_1}\rangle, \ldots, |q'_{rej_l}\rangle\}$$

Consideramos $H' = \ell_2(Q')$. Los nuevos estados $|q'_{acc_1}\rangle, \ldots, |q'_{acc_k}\rangle$ serán de aceptación y $|q'_{rej_1}\rangle, \ldots, |q'_{rej_l}\rangle$ serán estados de rechazo. Por su parte, pasarán a ser de no parada los estados $|q_{acc_1}\rangle, \ldots, |q_{acc_k}\rangle, |q_{rej_1}\rangle, \ldots, |q_{rej_l}\rangle$. Tenemos así los espacios $Q'_{acc} = \{|q'_{acc_1}\rangle, \ldots, |q'_{acc_k}\rangle\}$, $Q'_{rej} = \{|q'_{rej_1}\rangle, \ldots, |q'_{rej_l}\rangle\}$ y Q'_{non}, que está formado por el resto de vectores de Q'.

Las transiciones vendrán determinadas por las matrices

$$U'_\sigma = \begin{pmatrix} U_\#^{-1} & \\ & I_m \end{pmatrix} \begin{pmatrix} I_n & \\ & I_m \end{pmatrix} \begin{pmatrix} U_\sigma & \\ & I_m \end{pmatrix} \begin{pmatrix} U_\# & \\ & I_m \end{pmatrix}$$

$$U'_\$ = \begin{pmatrix} I_n & \\ & I_m \end{pmatrix} \begin{pmatrix} U_\$ & \\ & I_m \end{pmatrix} \begin{pmatrix} U_\# & \\ & I_m \end{pmatrix}$$

donde $n = \dim(H_{non})$, $m = \dim(H_{acc}) + \dim(H_{rej})$ e I_m, I_n son las matrices identidad de dimensiones $m \times m$ y $n \times n$, respectivamente.

El estado inicial lo escribimos como $|s'_{init}\rangle = |s_{init}, 0\rangle$. Será el mismo que el de M, pero con todas las componentes correspondientes a los nuevos estados clásicos iguales a 0. Además, podemos considerar sin pérdida de generalidad que $U_\# |s_{init}\rangle$ es un estado de no parada. Relajamos la notación para mostrar cómo sería la lectura de un símbolo σ si estamos en un estado $|\psi'\rangle = |\psi, 0\rangle$:

$$\begin{pmatrix} |\psi\rangle \\ 0 \\ 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} U_\# |\psi\rangle \\ 0 \\ 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} U_\sigma U_\# |\psi\rangle \\ 0 \\ 0 \end{pmatrix}$$

$$= \begin{pmatrix} P_{non} U_\sigma U_\# |\psi\rangle \\ P_{acc} U_\sigma U_\# |\psi\rangle \\ P_{rej} U_\sigma U_\# |\psi\rangle \\ 0 \\ 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} P_{non} U_\sigma U_\# |\psi\rangle \\ 0 \\ 0 \\ P_{acc} U_\sigma U_\# |\psi\rangle \\ P_{rej} U_\sigma U_\# |\psi\rangle \end{pmatrix} \rightsquigarrow \begin{pmatrix} U_\#^{-1} P_{non} U_\sigma U_\# |\psi\rangle \\ P_{acc} U_\sigma U_\# |\psi\rangle \\ P_{rej} U_\sigma U_\# |\psi\rangle \end{pmatrix}$$

Tras esto, se aceptará con probabilidad $\|P_{acc}U_\sigma U_\# |\psi\rangle\|^2$ y rechazará con probabilidad $\|P_{rej}U_\sigma U_\# |\psi\rangle\|^2$, igual que en M. En caso de no parar, el autómata colapsará en el nuevo estado

$$|\psi'\rangle = \begin{pmatrix} \frac{U_\#^{-1}P_{non}U_\sigma U_\# |\psi\rangle}{\left\|U_\#^{-1}P_{non}U_\sigma U_\# |\psi\rangle\right\|} \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{U_\#^{-1}P_{non}U_\sigma U_\# |\psi\rangle}{\left\|P_{non}U_\sigma U_\# |\psi\rangle\right\|} \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} U_\#^{-1} |\phi\rangle \\ 0 \\ 0 \end{pmatrix}$$

donde $|\phi\rangle = \frac{P_{non}U_\sigma U_\# |\psi\rangle}{\left\|P_{non}U_\sigma U_\# |\psi\rangle\right\|}$. Es claro que la transformación $U_\# |s_{init}\rangle$ se realizará igual que en M. Para el resto de símbolos, todos los estados serán iguales que en M aunque multiplicados por $U_\#^{-1}$, ya que sucesivas transformaciones mediante un símbolo $\sigma \in \Sigma$ cancelarán la aplicación de $U_\#^{-1}$ en el estado anterior, pero la volverán a añadir al comienzo. Al llegar a la lectura del símbolo \$, las transiciones desde un estado $|\psi, 0\rangle$ son:

$$\begin{pmatrix} |\psi\rangle \\ 0 \\ 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} U_\# |\psi\rangle \\ 0 \\ 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} U_\sigma U_\# |\psi\rangle \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} P_{non}U_\$ U_\# |\psi\rangle \\ P_{acc}U_\$ U_\# |\psi\rangle \\ P_{rej}U_\$ U_\# |\psi\rangle \\ 0 \\ 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} P_{non}U_\$ U_\# |\psi\rangle \\ 0 \\ 0 \\ P_{acc}U_\$ U_\# |\psi\rangle \\ P_{rej}U_\$ U_\# |\psi\rangle \end{pmatrix}$$

Tanto si se ha llegado a la lectura de \$ en el estado $|\psi\rangle = |s_{init}\rangle$ como si se ha llegado en otro estado $|\psi\rangle = \begin{pmatrix} U_\#^{-1} |\phi\rangle \\ 0 \\ 0 \end{pmatrix}$, donde $|\phi\rangle$ es el estado en el que se encuentra M tras leer toda la cadena menos el símbolo \$, obtenemos el mismo resultado que en M.

Además, también es posible que el estado inicial sea un vector unitario cualquiera $|s_{init}\rangle \in H$. Claramente, todo MMQFA sin símbolo # y estado inicial clásico entra dentro de esta nueva definición. A su vez, todo MMQFA M sin símbolo # y estado inicial unitario cualquiera puede ser simulado por un MMQFA M' con símbolo # y estado inicial clásico $|q_0\rangle$. Basta con ampliar la dimensión de H como en el caso anterior y tomar las transformaciones para M'

$$U'_\# |q_0\rangle = |s_{init}\rangle$$

$$U'_\sigma = \begin{pmatrix} I_n & & \\ & & I_m \\ & I_m & \end{pmatrix} \begin{pmatrix} U_\sigma & & \\ & I_m & \\ & & I_m \end{pmatrix}, \ \forall \sigma \in \Sigma \cup \{\$\}$$

3.4.2 Función de evolución

Una forma de expresar la evolución de un autómata MMQFA tras la lectura de un símbolo es mediante la siguiente definición.

Definición 3.4.2. Dado un autómata MMQFA M, se define la *función de evolución* asociada al símbolo $\sigma \in \Sigma$

$$T_\sigma : H \times \mathbb{C} \times \mathbb{C} \to H \times \mathbb{C} \times \mathbb{C}$$
$$(|\psi\rangle, p_{acc}, p_{rej}) \mapsto (P_{non}U_\sigma |\psi\rangle, p_{acc} + \|P_{acc}U_\sigma |\psi\rangle\|^2, p_{rej} + \|P_{rej}U_\sigma |\psi\rangle\|^2)$$

En la definición anterior, una configuración $(|\psi\rangle, p_{acc}, p_{rej})$ representa la situación del autómata hasta un momento concreto: habrá aceptado con probabilidad p_{acc}, rechazado con probabilidad p_{rej} y no parado con probabilidad $\||\psi\rangle\|^2$. Como configuración inicial tomamos $(|s_{init}\rangle, 0, 0)$. Además, dada una palabra $w \in \Sigma^*$, escribimos $T_w = T_{w_{|w|}} \cdots T_{w_1}$. Así, tras la lectura de w, la configuración del autómata será $T_w(|s_{init}\rangle, 0, 0) = (|\psi\rangle, p_{acc}, p_{rej})$. Es importante ver que, salvo en la configuración inicial, $|\psi\rangle$ no representa el estado del autómata en ese momento, ya que al aplicar T_σ la primera componente de la nueva configuración es $P_{non}U_\sigma |\psi\rangle$ sin normalizar.

3.5 1QFA

A partir de estas definiciones, se puede generalizar la noción de autómata finito cuántico de la siguiente manera:

Definición 3.5.1. Un *autómata finito cuántico unidireccional* (1QFA) es una 5-tupla

$$(\Sigma, H, \{T_\sigma \mid \sigma \in \tilde{\Sigma}\}, |s_{init}\rangle, R)$$

que se diferencia de las definiciones anteriores en lo siguiente:

- H es un espacio de Hilbert de dimensión finita.
- T_σ es la transformación correspondiente al símbolo $\sigma \in \tilde{\Sigma}$. Puede ser una transformación unitaria, como en los casos anteriores, pero puede ser también una secuencia de transformaciones unitarias y mediciones. Es más, estas transformaciones pueden incluso depender del resultado de mediciones anteriores.
- R es una regla que determina la forma en que el autómata acepta una cadena. Habitualmente suele emplearse alguno de los dos casos anteriores.

Existen otros autómatas que se adaptan a esta definición distintos de los dos en que nos hemos centrado. Dos de los principales ejemplos de ello son:

- El autómata finito cuántico *Latvian* (LaQFA) [1], que presenta la misma regla de aceptación que el MOQFA, pero difiere de él en que las transformaciones son una combinación de transformaciones unitarias y mediciones.
- El autómata finito cuántico *Nayak* (NaQFA) [19], cuyas transformaciones son del mismo tipo que las del LaQFA, pero su regla de aceptación es como la del MMQFA.

3.6 Simulación de un MOQFA por un MMQFA

Veremos más adelante cómo los autómatas MMQFA son más poderosos que los MOQFA. Antes de eso, vamos a probar que para todo autómata MOQFA es posible construir un MMQFA equivalente.

Si tenemos el MOQFA M con un espacio de Hilbert H de dimensión n y base $\{|q_1\rangle, \ldots, |q_n\rangle\}$, subespacio de aceptación H_{acc} (con la respectiva proyección P_{acc}), estado inicial $|s_{init}\rangle$ y transformaciones unitarias determinadas por las matrices unitarias U_σ con

$\sigma \in \Sigma$, podemos considerar el MMQFA M' (sin símbolo # y estado inicial no necesariamente clásico) con espacio de Hilbert H' de dimensión $3n$, estado inicial $|s'_{init}\rangle = |s_{init}, 0, 0\rangle$ y transformaciones unitarias dadas por las matrices

$$U'_\sigma = \begin{pmatrix} U_\sigma & & \\ & I_n & \\ & & I_n \end{pmatrix}$$

Tenemos los tres subespacios $H'_{non} = \text{span}(|q_1\rangle, \ldots, |q_n\rangle)$, $H'_{acc} = \text{span}(|q_{n+1}\rangle, \ldots, |q_{2n}\rangle)$ y $H'_{rej} = \text{span}(|q_{2n+1}\rangle, \ldots, |q_{3n}\rangle)$ y la transformación unitaria correspondiente al símbolo \$

$$U'_\$ = \begin{pmatrix} & P_{acc} & I_n - P_{acc} \\ P_{acc} & I_n - P_{acc} & \\ I_n - P_{acc} & & P_{acc} \end{pmatrix}$$

Es claro que el vector obtenido tras aplicar un operador U'_σ sobre el estado $|s'_{init}\rangle$ se encuentra en el subespacio H'_{non}. Así, tras la aplicación de $U'_{\sigma_1}, \ldots, U'_{\sigma_n}$, obtendremos el estado $|\psi, 0, 0\rangle$ donde $|\psi\rangle = U_{\sigma_n} \cdots U_{\sigma_1} |s_{init}\rangle$. Tras la lectura de \$, llegaremos al estado

$$U'_\$ |\psi, 0, 0\rangle = \begin{pmatrix} & P_{acc} & I_n - P_{acc} \\ P_{acc} & I_n - P_{acc} & \\ I_n - P_{acc} & & P_{acc} \end{pmatrix} \begin{pmatrix} |\psi\rangle \\ 0 \\ 0 \end{pmatrix} = |0, P_{acc}\psi, (I_n - P_{acc})\psi\rangle$$

De este modo, la probabilidad de aceptación será $\|P_{acc} |\psi\rangle\|^2$, igual que en M. Falta comprobar que $U'_\$$ es, efectivamente, una matriz unitaria y verifica

$$I_{3n} = U'_\$ U'^\dagger_\$ = \begin{pmatrix} & P_{acc} & I_n - P_{acc} \\ P_{acc} & I_n - P_{acc} & \\ I_n - P_{acc} & & P_{acc} \end{pmatrix} \begin{pmatrix} & P^\dagger_{acc} & (I_n - P_{acc})^\dagger \\ P^\dagger_{acc} & (I_n - P_{acc})^\dagger & \\ (I_n - P_{acc})^\dagger & & P^\dagger_{acc} \end{pmatrix}$$

Recordamos que todo operador proyección P verificaba $P = P^2 = P^\dagger$. Al ser P_{acc} una proyección ortogonal, $I_n - P_{acc}$ también lo es. Concretamente, es la proyección sobre el subespacio $H^\perp_{acc}$. Todo esto, junto con $P_{acc}(I_n - P_{acc}) = P_{acc} - P^2_{acc} = P_{acc} - P_{acc} = 0$, permite comprobar fácilmente que el anterior producto de matrices tiene por resultado la matriz identidad I_{3n}.

3.7 Aceptación de un lenguaje

Igual que en los autómatas probabilísticos, es necesario dar una definición para el reconocimiento de lenguajes por parte de un autómata finito cuántico. Usaremos también la noción de reconocimiento con punto de corte, pero plantearemos también otras alternativas. En primer lugar, para todo autómata, consideraremos una función de aceptación análoga a la que considerábamos en el caso probabilístico

$$\begin{aligned} f\colon \Sigma^* &\to [0, 1] \\ w &\mapsto f(w) \end{aligned}$$

que asigna a cada cadena w la probabilidad de que sea aceptada por el autómata. En el caso de los autómatas MOQFA, en que sólo se mide una vez tras leer toda la cadena w, se tiene la función $f(w) = \|P_{acc} U_w |s_{init}\rangle\|^2$. En el caso de los autómatas MMQFA, si $T_w(|s_{init}\rangle, 0, 0) = (|\psi\rangle, p_{acc}, p_{rej})$, $f(w) = p_{acc}$. A partir de esta función, encontramos distintas formas de aceptación de un lenguaje $L \subseteq \Sigma^*$.

Definición 3.7.1. Un lenguaje L es reconocido con *error no acotado* si existe un punto de corte λ tal que L es reconocido con punto de corte (estricto o no) λ. En particular, se denomina lenguaje reconocido con *error no acotado parcial positivo* al conjunto $L = \{w \in \Sigma^* \mid f(w) > 0\}$ y lenguaje reconocido con *error no acotado parcial negativo* al conjunto $L = \{w \in \Sigma^* \mid f(w) = 1\}$.

A continuación veremos otras dos definiciones de reconocimiento más restrictivas que la anterior.

Definición 3.7.2. Se dice que un conjunto L es un lenguaje reconocido con *punto de corte aislado* λ si existe $\epsilon > 0$ tal que:

- $f(w) \geq \lambda + \epsilon$ cuando $w \in L$
- $f(w) \leq \lambda - \epsilon$ cuando $w \notin L$

Definición 3.7.3. Se denomina lenguaje reconocido con *error acotado* (o *cota de error* $\epsilon \in \left[0, \frac{1}{2}\right)$) al conjunto $L \subseteq \Sigma^*$ tal que:

- $f(w) \geq 1 - \epsilon$ cuando $w \in L$
- $f(w) \leq \epsilon$ cuando $w \notin L$

Las formas de aceptación con error acotado y con error no acotado son las dos con las que trataremos a lo largo del trabajo.

3.8 Ejemplos

Veamos ahora algunos ejemplos sencillos de cada uno de los dos modelos de autómatas presentados.

MOQFA

Mostraremos dos ejemplos de autómata MOQFA. Uno será capaz de reconocer un lenguaje regular con error acotado y el otro reconocerá un lenguaje no regular con error no acotado.

Ejemplo 3.8.1. Sea p un número impar mayor que 2. Consideramos el lenguaje $MOD_p = \{a^k \mid p|k\}$. Sea M el siguiente autómata MOQFA: tomamos el alfabeto $\Sigma = \{a\}$, un registro de un qubit (es decir, un espacio de Hilbert con base $Q = \{|q_0\rangle, |q_1\rangle\}$), un estado inicial $|s_{init}\rangle = |q_0\rangle$ y unas transformaciones unitarias dadas por la matriz

$$U_a = \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix}$$

con $\theta = \frac{2\pi}{p}$. El subespacio de aceptación es $H_{acc} = \operatorname{span}(|q_0\rangle)$ y, por tanto, $P_{acc} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

La transformación determinada por la matriz U_a aplica una rotación de ángulo θ sobre el estado $|s_{init}\rangle$, transformándolo en $\cos\theta\,|q_0\rangle + \operatorname{sen}\theta\,|q_1\rangle$. Es fácil ver que la aplicación k veces de U_a supone una rotación de ángulo $k\theta$. Lo probamos por inducción, viendo que se verifica

$$U_a^k = \begin{pmatrix} \cos k\theta & -\operatorname{sen} k\theta \\ \operatorname{sen} k\theta & \cos k\theta \end{pmatrix} \tag{3.2}$$

Claramente se cumple para $k = 1$. Si lo suponemos cierto para $k-1$, tenemos que

$$U_a^k = U_a^{k-1}U_a = \begin{pmatrix} \cos(k-1)\theta & -\operatorname{sen}(k-1)\theta \\ \operatorname{sen}(k-1)\theta & \cos(k-1)\theta \end{pmatrix} \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{pmatrix}$$
$$= \begin{pmatrix} \cos(k-1)\theta\cos\theta - \operatorname{sen}(k-1)\theta\operatorname{sen}\theta & -(\cos(k-1)\theta\operatorname{sen}\theta + \operatorname{sen}(k-1)\theta\cos\theta) \\ \cos(k-1)\theta\operatorname{sen}\theta + \operatorname{sen}(k-1)\theta\cos\theta & \cos(k-1)\theta\cos\theta - \operatorname{sen}(k-1)\theta\operatorname{sen}\theta \end{pmatrix}$$

Haciendo uso de las identidades $\cos(\alpha+\beta) = \cos\alpha\cos\beta - \operatorname{sen}\alpha\operatorname{sen}\beta$ y $\operatorname{sen}(\alpha+\beta) = \operatorname{sen}\alpha\cos\beta + \cos\alpha\operatorname{sen}\beta$, obtenemos la matriz de la expresión (3.2).

Por tanto, tras leer k símbolos, el autómata estará en el estado $|\psi\rangle = U_a^k|s_{init}\rangle = \cos k\theta\,|q_0\rangle + \operatorname{sen} k\theta\,|q_1\rangle$ y

$$f(a^k) = \|P_{acc}(\cos k\theta\,|q_0\rangle + \operatorname{sen} k\theta\,|q_1\rangle)\|^2 = \cos^2(k\theta) = \cos^2\left(\frac{2\pi k}{p}\right)$$

Como $\cos^2\left(\frac{2\pi k}{p}\right) = 1$ sólo en caso de que p divida a k (hemos tomado p impar mayor que 2), se tiene que este autómata reconoce el lenguaje MOD_p con punto de corte aislado:

- $f(w) = 1$ si $w \in MOD_p$.
- $f(w) \leq \cos^2\left(\frac{\pi}{p}\right)$ si $w \notin MOD_p$, ya que el valor máximo que puede tener una cadena que no está en MOD_p es $\cos^2\left(\frac{\pi}{p}\right)$. Este valor se corresponde con $k = \frac{p+1}{2}$ y $k = \frac{p-1}{2}$.

Ejemplo 3.8.2. En este segundo ejemplo vamos a ver un caso de un lenguaje no regular que es reconocido por un MOQFA con error no acotado. Consideremos el lenguaje $NEQ = \{w \in \{a,b\}^* \mid |w|_a \neq |w|_b\}$ y sea el autómata MOQFA con dos estados clásicos $|q_0\rangle$ (estado inicial) y $|q_1\rangle$ (estado de aceptación) y transformaciones unitarias dadas por las matrices

$$U_a = \begin{pmatrix} \cos\sqrt{2}\pi & -\operatorname{sen}\sqrt{2}\pi \\ \operatorname{sen}\sqrt{2}\pi & \cos\sqrt{2}\pi \end{pmatrix},\ U_b = \begin{pmatrix} \cos(-\sqrt{2}\pi) & -\operatorname{sen}(-\sqrt{2}\pi) \\ \operatorname{sen}(-\sqrt{2}\pi) & \cos(-\sqrt{2}\pi) \end{pmatrix}$$

Este autómata aplica una rotación de ángulo $\sqrt{2}\pi$ tras leer una a y otra rotación de ángulo $-\sqrt{2}\pi$ tras leer una b. Claramente, tras leer una cadena que verifique $|w|_a = |w|_b$, el autómata habrá hecho las mismas rotaciones de ángulo $\sqrt{2}\pi$ que de ángulo $-\sqrt{2}\pi$ y estará en el estado $|q_0\rangle$, por lo que aceptará con probabilidad 0. Por contra, tras leer una cadena $w \in NEQ$, el autómata no podrá estar nunca en el estado $|q_0\rangle$ (o $-|q_0\rangle$) ya que la rotación es de un múltiplo irracional de π. Por tanto,

- $f(w) > 0$ si $w \in NEQ$.
- $f(w) = 0$ si $w \notin NEQ$.

El autómata reconoce el lenguaje NEQ con error no acotado parcial positivo. Esta forma de aceptación también se llama *no determinista*.

MMQFA

En el caso de los MMQFA, vamos a ver un ejemplo de un autómata que reconoce un lenguaje regular con error acotado.

Ejemplo 3.8.3. Consideremos el lenguaje $L = a^*b^*$. Ambainis y Freivalds [2] probaron que este lenguaje puede ser reconocido con probabilidad $p \simeq 0{,}68$, donde p es la raíz del polinomio $p^3 + p = 1$.

Consideremos el autómata MMQFA (sin símbolo #) M en el que se tiene que $Q = \{|q_0\rangle, |q_1\rangle, |q_{acc}\rangle, |q_{rej}\rangle\}$, $H = \ell_2(Q)$, $|s_{init}\rangle = (\sqrt{1-p})\,|q_0\rangle + \sqrt{p}\,|q_1\rangle$ y las transformaciones vienen dadas por:

$$\begin{aligned}
U_a\,|q_0\rangle &= (1-p)\,|q_0\rangle + \sqrt{p(1-p)}\,|q_1\rangle + \sqrt{p}\,|q_{rej}\rangle \\
U_a\,|q_1\rangle &= \sqrt{p(1-p)}\,|q_0\rangle + p\,|q_1\rangle - \sqrt{1-p}\,|q_{rej}\rangle \\
U_b\,|q_0\rangle &= |q_{rej}\rangle,\ U_b\,|q_1\rangle = |q_1\rangle \\
U_\$\,|q_0\rangle &= |q_{rej}\rangle,\ U_\$\,|q_1\rangle = |q_{acc}\rangle
\end{aligned}$$

Las matrices U_a, U_b y $U_\$$ han de ser completadas de modo que sean unitarias. Para conseguir esta propiedad, es suficiente con que las columnas que no hemos especificado formen, junto con las que sí hemos especificado, una base ortonormal.

El espacio de Hilbert H queda dividido en tres subespacios $H_{acc} = \text{span}(|q_{acc}\rangle)$, $H_{rej} = \text{span}(|q_{rej}\rangle)$ y $H_{non} = \text{span}(|q_0\rangle, |q_1\rangle)$.

De cara a la lectura de una cadena w por parte del autómata, diferenciamos tres posibles casos:

1. $w = a^*$. La lectura de varias as deja al autómata en el mismo estado $|s_{init}\rangle$:

$$\begin{aligned}
U_a\,|s_{init}\rangle &= U_a((\sqrt{1-p})\,|q_0\rangle + \sqrt{p}\,|q_1\rangle) \\
&= \sqrt{1-p}((1-p)\,|q_0\rangle + \sqrt{p(1-p)}\,|q_1\rangle + \sqrt{p}\,|q_{rej}\rangle) \\
&\quad + \sqrt{p}(\sqrt{p(1-p)}\,|q_0\rangle + p\,|q_1\rangle - \sqrt{1-p}\,|q_{rej}\rangle) \\
&= (\sqrt{1-p})\,|q_0\rangle + \sqrt{p}\,|q_1\rangle = |s_{init}\rangle
\end{aligned}$$

   Por tanto, al leer la cadena entera, y tras aplicar $U_\$$, la probabilidad de aceptación será p.

2. $w = a^*bb^*$. El estado permanece inalterado hasta la lectura de la primera b, que deja al autómata en el estado

$$U_b((\sqrt{1-p})\,|q_0\rangle + \sqrt{p}\,|q_1\rangle) = (\sqrt{1-p})\,|q_{rej}\rangle + \sqrt{p}\,|q_1\rangle$$

   A partir de aquí, la lectura de las siguientes bs deja inalterada la segunda componente del vector, por lo que la probabilidad de aceptación vuelve a ser p.

3. $w \notin L$. Necesariamente, w ha de contener alguna b seguida de una a. Así, tras la lectura de la primera b, el estado pasará a ser el mismo que en el caso anterior, $(\sqrt{1-p})\,|q_{rej}\rangle + \sqrt{p}\,|q_1\rangle$. Llegado a este punto, el autómata ya rechaza con probabilidad $1-p$. Si después de esta b se leen más, la parte que no para $(\sqrt{p}\,|q_1\rangle)$ permanece intacta. Al llegar la siguiente a, $\sqrt{p}\,|q_1\rangle$ se convierte en

$$\begin{aligned}
U_a(\sqrt{p}\,|q_1\rangle) &= \sqrt{p}(\sqrt{p(1-p)}\,|q_0\rangle + p\,|q_1\rangle - \sqrt{1-p}\,|q_{rej}\rangle) \\
&= p\sqrt{(1-p)}\,|q_0\rangle + p\sqrt{p}\,|q_1\rangle + \sqrt{p(1-p)}\,|q_{rej}\rangle
\end{aligned}$$

   En este momento, el autómata ya rechaza w con probabilidad $(1-p) + p(1-p)$. Ahora, la parte que no ha parado se corresponde con $\sqrt{p}\,|s_{init}\rangle$. Así, si llega una a,

permanece inalterado. Si llega una b o el símbolo \$, se rechaza con probabilidad $p^2(1-p)$, ya que $U_b |q_0\rangle = U_\$ |q_0\rangle = |q_{rej}\rangle$.

Tenemos, por tanto, que el autómata rechazará w con una probabilidad de al menos

$$(1-p) + p(1-p) + p^2(1-p) = (1-p)(p^2+p+1) = (1-p)\frac{1-p^3}{1-p} = 1-p^3 = p$$

Recapitulando, hemos obtenido lo siguiente:

- Si $w \in L \Rightarrow f(w) = p$, es decir, $f(w) \geq 1-(1-p)$.
- Si $w \notin L \Rightarrow f(w) \leq 1-p$.

Por tanto, el autómata M reconoce $L = a^*b^*$ con cota de error $1-p$.

3.9 Reconocimiento con error acotado

En esta sección estamos interesados en el reconocimiento de un lenguaje con error acotado. Veremos que los autómatas finitos cuánticos son menos poderosos que los clásicos y, en las versiones en que nos centramos (MOQFA y MMQFA), sólo pueden reconocer un subconjunto de los lenguajes regulares.

3.9.1 Todo lenguaje reconocido por un MMQFA es regular

En primer lugar, veremos cómo cualquier lenguaje que pueda ser reconocido por un MMQFA es necesariamente un lenguaje regular. Para ello, comenzaremos recogiendo el Teorema de Myhill-Nerode [16], que nos permite caracterizar los lenguajes regulares.

Teorema 3.9.1 (Teorema de Myhill-Nerode)**.** *Sea $\sim_L$ una relación de equivalencia de modo que $w \sim_L w'$ si $\forall y \in \Sigma^*$ se verifica $wy \in L \Leftrightarrow w'y \in L$. Un lenguaje L es regular si y sólo si $\sim_L$ tiene un número finito de clases de equivalencia.*

Demostración. Para demostrar la *implicación de izquierda a derecha*, consideremos un AFD $M = (\Sigma, S, s_0, \delta, F)$ que reconoce L. Sean w y w' dos palabras que alcanzan el mismo estado, es decir, $\hat{\delta}(s_0, w) = \hat{\delta}(s_0, w')$. En ese caso, dado $y \in \Sigma^*$, tenemos $wy \in L \Leftrightarrow \hat{\delta}(s_0, wy)$ es un estado final $\Leftrightarrow \hat{\delta}(\hat{\delta}(s_0, w), y)$ es un estado final $\Leftrightarrow \hat{\delta}(\hat{\delta}(s_0, w'), y)$ es un estado final $\Leftrightarrow \hat{\delta}(s_0, w'y)$ es un estado final $\Leftrightarrow w'y \in L$. Tenemos, entonces, que las palabras que alcanzan el mismo estado pertenecen a la misma clase de equivalencia. Así, a lo sumo habrá el mismo número de clases de equivalencia que de estados del autómata y, al ser finito el número de estados, también lo es el de clases.

Para demostrar la *implicación de derecha a izquierda*, sean $[x_1], \ldots, [x_n]$ el conjunto de clases de equivalencia de $\sim_L$. Es posible construir un DFA a partir de estas clases de equivalencia. En primer lugar, consideramos el conjunto de estados $S = \{s_1, \ldots, s_n\}$ y tomamos como estado inicial aquel cuyo subíndice i verifique $\epsilon \in [x_i]$. Por otro lado, si $w, w' \in [x_i], a \in \Sigma$ y $z \in \Sigma^*$, tenemos que $waz \in L \Leftrightarrow w'az \in L$. Esto hace ver que wa y $w'a$ están en la misma clase de equivalencia $[x_j]$ para algún $j \in \{1, \ldots, n\}$. Entonces, para determinar las transiciones $\delta(s_i, a)$, tomamos un $w \in [x_i]$, comprobamos la clase $[x_j]$ a la que pertenece wa y establecemos $\delta(s_i, a) = q_j$. Por último, los elementos de una clase de equivalencia pueden estar contenidos en L (en cuyo caso lo estarán todos) o no estarlo (no estará ninguno). Consideramos estados finales aquellos que corresponden a clases de equivalencia cuyos elementos están en L. □

Para la siguiente demostración, también nos va a ser necesario definir la norma $\|\cdot\|_u : \ell_2(Q) \times \mathbb{C} \times \mathbb{C} \to \mathbb{R}$ sobre las configuraciones de un autómata MMQFA:

$$\|(|\psi\rangle, p_{acc}, p_{rej})\|_u = \frac{1}{2}(\||\psi\rangle\| + |p_{acc}| + |p_{rej}|)$$

Nótese que se trata de hecho de una norma dado que:

- $\|(|\psi\rangle, p_{acc}, p_{rej}) + (|\psi\rangle, p_{acc}, p_{rej})\|_u = \frac{1}{2}(\||\psi\rangle + |\psi'\rangle\| + |p_{acc} + p'_{acc}| + |p_{rej} + p'_{rej}|) \leq \frac{1}{2}(\||\psi\rangle\| + \||\psi'\rangle\| + |p_{acc}| + |p'_{acc}| + |p_{rej}| + |p'_{rej}|) = \|(|\psi\rangle, p_{acc}, p_{rej})\|_u + \left\|(|\psi'\rangle, p'_{acc}, p'_{rej})\right\|_u$
- $\|k(|\psi\rangle, p_{acc}, p_{rej})\|_u = \|(k|\psi\rangle, kp_{acc}, kp_{rej})\|_u = \frac{1}{2}(\|k|\psi\rangle\| + |kp_{acc}| + |kp_{rej}|) = \frac{1}{2}(|k|\,\||\psi\rangle\| + |k||p_{acc}| + |k||p_{rej}|) = |k|\,\frac{1}{2}(\||\psi\rangle\| + |p_{acc}| + |p_{rej}|) = |k|\,\|(|\psi\rangle, p_{acc}, p_{rej})\|_u$
- $0 = \|(|\psi\rangle, p_{acc}, p_{rej})\|_u = \frac{1}{2}(\||\psi\rangle\| + |p_{acc}| + |p_{rej}|) \Rightarrow \||\psi\rangle\|, |p_{acc}|, |p_{rej}| = 0 \Rightarrow (|\psi\rangle, p_{acc}, p_{rej}) = (0, 0, 0)$

En los tres casos hemos utilizado el hecho de que $\|\cdot\|$ y $|\cdot|$ son también normas. Es claro también que toda configuración alcanzable ha de estar en $\mathfrak{B} = \{v \in \ell_2(Q) \times \mathbb{C} \times \mathbb{C} \mid \|v\|_u \leq 1\}$. Además, relacionados con esta norma tenemos los dos siguientes lemas cuyas demostraciones se pueden ver en el Apéndice.

Lema 3.9.1. *Dados dos vectores $v, v' \in \mathfrak{B}$ y $\sigma \in \Sigma^*$, existe una constante c tal que $\|T_\sigma v - T_\sigma v'\|_u \leq c\,\|v - v'\|_u$.*

Lema 3.9.2. *Si tenemos un conjunto $A \subseteq \mathfrak{B}$ que verifica que existe un $\epsilon > 0$ tal que para todo $v, v' \in A$ se cumple $\|v - v'\|_u > \epsilon$, entonces A es finito:*

Estamos, ahora sí, en disposición de demostrar el siguiente resultado.

Teorema 3.9.2. *Todo lenguaje reconocido por un MMQFA es regular.*

Demostración. Sea M un MMQFA que reconoce el lenguaje L con cota de error $\frac{1}{2} - \epsilon$. Por el Teorema de Myhill-Nerode, L es regular si la relación de equivalencia $\sim_L$ determina un número finito de clases de equivalencia. Sea W un conjunto de cadenas en Σ^* todas no equivalentes entre sí. Veamos que este conjunto es finito.

Sean $w, w' \in W$ $(w \neq w')$. En este caso, tiene que existir $y \in \Sigma^*$ tal que $wy \in L$ si y sólo si $w'y \notin L$. Supongamos sin pérdida de generalidad que $wy \in L$ y $w'y \notin L$.

Consideramos ahora $v = T_w(|s_{init}\rangle, 0, 0)$ y $v' = T_{w'}(|s_{init}\rangle, 0, 0)$. Como $|p^{wy\$}_{accept}| \geq \frac{1}{2} + \epsilon$ $(|p^{wy\$}_{reject}| \leq \frac{1}{2} - \epsilon)$ y $|p^{w'y\$}_{reject}| \geq \frac{1}{2} + \epsilon$ $(|p^{w'y\$}_{accept}| \leq \frac{1}{2} - \epsilon)$, se cumple

$$\|T_{y\$}v - T_{y\$}v'\|_u > 2\epsilon$$

Entonces, tenemos $2\epsilon < \|T_{y\$}v - T_{y\$}v'\|_u \leq c\,\|v - v'\|_u$. Es decir, $\|v - v'\|_u > \frac{2\epsilon}{c}$ y, por el lema anterior, se tiene que $\{T_w(|s_{init}\rangle, 0, 0) : w \in W\}$ es finito. Así, W también es finito. □

3.9.2 $\{a,b\}^*a$ no puede ser reconocido por un MMQFA

Acabamos de comprobar que todos los lenguajes reconocidos con error acotado por un MMQFA son regulares. Sin embargo, existen lenguajes regulares que no pueden ser reconocidos por un MMQFA. El ejemplo más conocido es el del lenguaje $L = \{a,b\}^*a$. Para ver que, efectivamente, este lenguaje no puede ser reconocido por un MMQFA es necesario el siguiente lema, cuya demostración está incluida en el Apéndice de este trabajo.

Lema 3.9.3. *Sean* $|u\rangle, |v\rangle$ *dos vectores,* A *un operador lineal,* $0 < \epsilon < 1$, $\mu > 0$, $\|A(u-v)\| < \epsilon$ *y* $\|u\|, \|v\|, \|Au\|, \|Av\| \in [\mu, \mu+\epsilon]$. *Entonces* $\exists c$ *tal que* $\|u-v\| < c\epsilon^{1/4}$

Probemos entonces que $\{a,b\}^*a$ no puede ser reconocido por un MMQFA. Sea M un MMQFA que reconoce L. Para cada $w = \sigma_1 \cdots \sigma_n \in \Sigma^*$, escribimos

$$|\psi_w\rangle = P_{non}U_{\sigma_n} \cdots P_{non}U_{\sigma_1} |s_{init}\rangle$$

y denotamos $\mu = \text{ínf}\{\||\psi_w\rangle\| \mid w \in \{a,b\}^*\}$. Como $wa \in L$ y $wb \notin L$, μ ha de ser mayor que 0 para que M reconozca L con error acotado. Por tanto, tomamos $\mu > 0$. Sea $\epsilon > 0$, tomamos w tal que $\||\psi_w\rangle\| < \mu + \epsilon$. De ahí $\||\psi_{wy}\rangle\| \in [\mu, \mu+\epsilon)$ para todo $y \in \{a,b\}^*$. En particular, tenemos

$$\left\|(P_{non}U_b)^j |\psi_{wa}\rangle\right\| \in [\mu, \mu+\epsilon) \quad \forall j \geq 0 \tag{3.3}$$

Dado que $\{ \|(P_{non}U_b)^j \mid \psi_{wa}\rangle\| \}$ es una sucesión acotada en un espacio de Hilbert de dimensión finita, ha de tener un límite. Así, existen enteros $j \geq 0$ y $k \geq 1$ tales que $\left\|(P_{non}U_b)^j(|\psi_{wa}\rangle - (P_{non}U_b)^{j+k} |\psi_{wa}\rangle)\right\| < \epsilon$. Ahora, haciendo uso también de la ecuación (3.3) y del lema 3.9.3, existe una constante c' (independiente de ϵ) tal que

$$\left\||\psi_{wa}\rangle - (P_{non}U_b)^k |\psi_{wa}\rangle\right\| < c'\epsilon^{1/4}$$

y entonces, por el lema 3.9.1,

$$\|T_{wa\$}(|s_{init}\rangle, 0, 0) - T_{wab^k\$}(|s_{init}\rangle, 0, 0)\| < c''\epsilon^{1/4}$$

para una constante c''. Como ϵ es arbitrariamente pequeño y como M ha de aceptar wa y rechazar wab^k, no puede tener cota de error inferior a $\frac{1}{2}$.

Esto impide que L sea aceptado con error acotado por un MMQFA, pese a ser un lenguaje regular.

Nótese que a partir de este resultado, junto con el Teorema 3.9.2, se deduce inmediatamente que los lenguajes reconocidos por un MMQFA son un subconjunto propio de los lenguajes regulares.

3.9.3 Contrucciones no permitidas por un MMQFA

Hemos visto que los autómatas MMQFA pueden reconocer solamente un subconjunto propio de los lenguajes regulares. Sin embargo, no se conoce exactamente cuál es ese subconjunto. De todas formas, sí que son conocidas algunas construcciones que hacen que todo lenguaje regular que las presente no pueda ser reconocido por un MMQFA. La primera de estas construcciones fue presentada por Brodsky y Pippenger [9] y se muestra en la figura 3.1. Si el autómata finito determinista minimal que reconoce un lenguaje la presenta, entonces el lenguaje no puede ser reconocido por un MMQFA con error acotado. La segunda construcción fue presentada por Ambainis, Kikusts y Valdats [3] y aparece en la figura 3.2. Detallamos a continuación cada uno de estos dos casos.

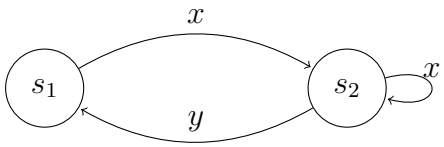

Figura 3.1: Primera construcción prohibida

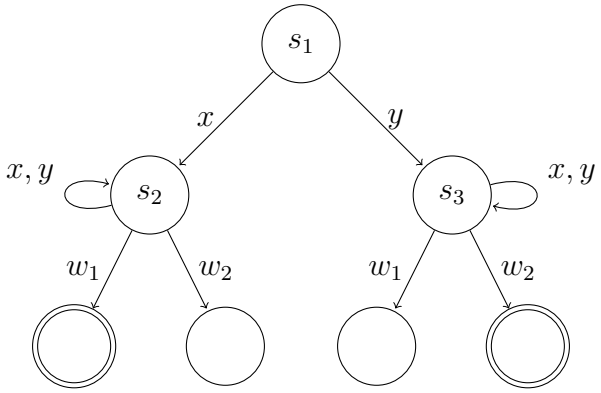

Figura 3.2: Segunda construcción prohibida

Primera construcción. Este primer caso es en el que se encuentra el ejemplo visto en la sección 3.9.2. Dado un lenguaje regular L, haremos uso del autómata finito determinista minimal M que reconoce este lenguaje. La construcción de la figura 3.1 representa la llamada *condición de orden parcial*.

Definición 3.9.1. Un autómata finito determinista M satisface la *condición de orden parcial* si no contiene dos estados distinguibles s_1, s_2 tales que existen cadenas $x, y \in \Sigma^+$ que verifican:

- $\delta(s_1, x) = \delta(s_2, x) = s_2$
- $\delta(s_2, y) = s_1$

Dos estados s_1 y s_2 se consideran *distinguibles* si existe alguna cadena $w \in \Sigma^*$ tal que $\delta(s_1, w)$ es un estado de aceptación y $\delta(s_2, w)$ no lo es (o viceversa).

Es claro que el lenguaje $\{a, b\}^*a$ presentado en la sección 3.9.2 no satisface la *condición de orden parcial*. Su autómata finito determinista minimal puede verse en la figura 3.3. Los estados s_1 y s_2 son distinguibles mediante la cadena ϵ y se tiene que $\delta(s_1, a) = \delta(s_2, a) = s_2$, $\delta(s_2, b) = s_1$.

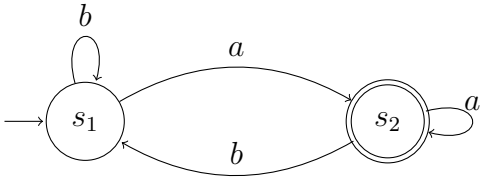

Figura 3.3: Autómata finito determinista minimal de $\{a, b\}^*a$

A partir de la condición de orden parcial se puede obtener el siguiente resultado [9].

Teorema 3.9.3. *Si el autómata finito determinista minimal M que reconoce el lenguaje regular L no satisface la condición de orden parcial, entonces no puede ser reconocido por un MMQFA con error acotado.*

Segunda construcción. La condición de la figura 3.2 puede formalizarse de la siguiente manera.

Definición 3.9.2. Un autómata finito determinista M satisface la condición presentada por Ambainis, Kikusts y Valdats si tiene estados s_1, s_2, s_3 y existen palabras $x, y, w_1, w_2 \in \Sigma^*$ tales que:

- s_2 y s_3 son estados distinguibles.
- $\delta(s_1, x) = s_2$.
- $\delta(s_2, x) = s_2$.
- $\delta(s_1, y) = s_3$.
- $\delta(s_3, y) = s_3$.
- Para toda palabra $z \in \{a, b\}^*$ existe una palabra $z_1 \in \{a, b\}^*$ tal que $\delta(s_2, zz_1) = s_2$.
- Para toda palabra $z \in \{a, b\}^*$ existe una palabra $z_2 \in \{a, b\}^*$ tal que $\delta(s_3, zz_2) = s_3$.
- $\delta(s_2, w_1)$ es un estado de aceptación.
- $\delta(s_2, w_2)$ no es un estado de aceptación.
- $\delta(s_3, w_1)$ no es un estado de aceptación.
- $\delta(s_3, w_2)$ es un estado de aceptación.

A partir de la condición anterior se puede obtener el siguiente resultado [3].

Teorema 3.9.4. *Si el autómata finito determinista minimal M que reconoce el lenguaje regular L no satisface la condición de Ambainis, Kikusts y Valdats, entonces no puede ser reconocido por un MMQFA con error acotado.*

3.9.4 Un MOQFA reconoce los mismos lenguajes que un GFA

En secciones anteriores hemos mostrado que un MOQFA puede ser simulado por un MMQFA. Por tanto, igual que los MMQFA, solo podrán reconocer lenguajes regulares. Sin embargo, a diferencia de los MMQFA, sí es conocido el conjunto de los lenguajes que pueden ser reconocidos por un MOQFA. Brodsky y Pippenger [9] probaron que los MOQFA son capaces de reconocer con error acotado exactamente los *group languages*. En esta sección veremos la prueba que ellos plantearon. Otra posible prueba es la planteada por Bertoni y Carpentieri [8]. Para probar este resultado es necesario primero introducir dos lemas, cuyas demostraciones están incluidas en el Apéndice.

Lema 3.9.4. *Si U es una matriz unitaria de orden m, entonces para cualquier $\varepsilon > 0$ existe un $k \in \mathbb{N}$ tal que $\left\| I_m - U^k \right\| \leq \varepsilon$. Por tanto, si tenemos un vector $|\psi\rangle$ que verifique $\||\psi\rangle\|^2 \leq 1$, para todo $\varepsilon > 0$ existe un $k \in \mathbb{N}$ tal que $\left\| (I_m - U^k) |\psi\rangle \right\| < \varepsilon$.*

Lema 3.9.5. *Sean dos vectores unitarios $|\psi\rangle, |\phi\rangle \in \mathbb{C}^n$ tales que $\||\psi\rangle - |\phi\rangle\| < \epsilon$. La distancia total entre las distribuciones de probabilidad obtenidas tras medir $|\psi\rangle$ y $|\phi\rangle$ es, a lo sumo, 4ϵ.*

Podemos pasar ahora a probar el siguiente resultado.

Teorema 3.9.5. *Un lenguaje L puede ser reconocido por un $MOQFA$ con error acotado si y sólo si puede ser reconocido por un GFA.*

Demostración. La condición necesaria es trivial, pues un GFA es un MOQFA ya que las matrices que determinan las transiciones de un GFA son unitarias (sus columnas forman una base ortonormal).

Supongamos ahora que L puede ser reconocido por un MOQFA con error acotado, pero no por un GFA. Por lo visto anteriormente, L ha de ser regular. Así, la relación de equivalencia $\sim_L$ determina un número finito de clases de equivalencia. Estas clases de equivalencia vienen definidas por los estados del DFA minimal que reconoce L.

Sean $|\psi\rangle$ y $|\phi\rangle$ dos estados alcanzables distintos. Como L no puede ser aceptado por un GFA, deben existir dos clases $[y], [y']$ distintas, otra clase $[x]$ y un símbolo $\sigma \in \Sigma$ tales que $[y\sigma] \sim_L [y'\sigma] \sim_L [x]$. Si $|\psi\rangle \in [y], |\phi\rangle \in [y']$, entonces $U_\sigma |\psi\rangle, U_\sigma |\phi\rangle \in [x]$.

Sea ϵ' la cota de error y $\epsilon = \frac{1}{2} - \epsilon'$. Por el lema 3.9.4, $\exists k > 0$ tal que

$$\left\|(I - U_\sigma^k)|\psi\rangle\right\| < \frac{\epsilon}{4}, \quad \left\|(I - U_\sigma^k)|\phi\rangle\right\| < \frac{\epsilon}{4}$$

Entonces, $U_\sigma^k |\psi\rangle \in [y]$ pues si

$$\left\|(I - U_\sigma^k)|\psi\rangle\right\| = \left\||\psi\rangle - U_\sigma^k |\psi\rangle\right\| = \left\|V(|\psi\rangle - U_\sigma^k |\psi\rangle)\right\| < \frac{\epsilon}{4}$$

para V una matriz unitaria cualquiera, por el lema 3.9.5, las probabilidades de medir $VU_\sigma^k |\psi\rangle$ y $V|\psi\rangle$ y obtener el subespacio de aceptación están a una distancia menor que ϵ. Se razona de forma similar para $U_\sigma^k |\phi\rangle$.

Tenemos entonces que $[y\sigma^k] \sim_L [y], [y'\sigma^k] \sim_L [y']$. Sea z la cadena que distingue las clases $[y], [y']$. Por tanto, $\sigma^{k-1}z$ parte $[x]$ en al menos dos clases distintas, lo que nos lleva a una contradicción. □

3.10 Reconocimiento con error no acotado

Esta sección está dedicada a estudiar los resultados en cuanto al reconocimiento de lenguajes con error no acotado por parte de los autómatas MOQFA y MMQFA. Veremos que en este caso la capacidad de aceptación de un MOQFA es menor que la de un PFA y sólo pueden reconocer un subconjunto de los lenguajes estocásticos. Sin embargo, los autómatas MMQFA son capaces de reconocer exactamente los lenguajes estocásticos. Consideraremos en esta sección autómatas MMQFA con símbolo #.

3.10.1 Un MMQFA reconoce los lenguajes estocásticos

Un autómata MMQFA tiene la misma capacidad de aceptación con error no acotado que los autómatas probabilísticos. Así, reconocen los lenguajes estocásticos, conjunto de lenguajes del que los lenguajes regulares son un subconjunto propio. Esto fue probado por Yakaryilmaz y Cem Say [25].

Lema 3.10.1. *Cualquier lenguaje reconocido por un PFA con n estados con punto de corte estricto $\frac{1}{2}$ puede ser reconocido por un MMQFA con $O(n^2)$ estados clásicos con punto de corte estricto $\frac{1}{2}$.*

Demostración. Sea $P = (\Sigma, S, \{A_\sigma \mid \sigma \in \Sigma\}, v_0, F)$ un autómata PFA que reconoce el lenguaje L con punto de corte no estricto $\frac{1}{2}$. En primer lugar, vamos a modificar P. Si $S = \{s_0, s_1, \ldots, s_{n-1}\}$, entonces consideraremos dos estados adicionales $s_n \in F$ y

$s_{n+1} \notin F$. Además, añadimos los símbolos # y \$ que marcan el comienzo y el final de una palabra. Representamos por e_i el vector que tiene todas las componentes iguales a cero menos la i-ésima, que es 1. Así, si consideramos como estado inicial $s_0 \in S$ tendremos la matriz $A_\#$ tal que $A_\#(1, 0, \ldots, 0)^T = v_0$. Para \$, tomamos la matriz $A_\$$ tal que $A_\$ e_i = e_n$ si $s_i \in F$ y $A_\$ e_i = e_{n+1}$ si $s_i \notin F$. Para el resto de matrices A_σ completamos las columnas ya determinadas añadiendo dos ceros y añadimos dos nuevas columnas de modo que $A_\sigma e_n = e_n$ y $A_\sigma e_{n+1} = e_{n+1}$.

Ahora, vamos a construir el autómata MMQFA que reconocerá L con punto de corte no estricto $\frac{1}{2}$. Sea $M = (\Sigma, H, \{U_\sigma \mid \sigma \in \tilde{\Sigma}\}, |q_0\rangle, H_{acc}, H_{rej}, H_{non})$. En este autómata, $H = \ell_2(Q)$ donde Q tiene $n + 2$ estados y $H_{acc} = \text{span}(|q_n\rangle)$, $H_{rej} = \text{span}(|q_{n+1}\rangle)$ y $H_{non} = \text{span}(|q_0\rangle, |q_1\rangle, \ldots, |q_{n-1}\rangle)$. Construiremos las matrices U_σ a partir de las matrices A_σ de P. Para ello será necesario añadir más estados clásicos a Q.

En primer lugar, para cada par de columnas de A_σ en las posiciones i, j (que denotamos por A^i_σ y A^j_σ, respectivamente) añadimos dos nuevos estados a Q: uno de aceptación y otro de rechazo. Ahora, si tenemos que el producto escalar de ambas columnas es α_{ij}, añadiremos a la columna A^i_σ el valor $-\sqrt{\frac{\alpha_{ij}}{2}}$ para las nuevas filas correspondientes a los dos nuevos estados. En el caso de A^j_σ, añadiremos el valor $\sqrt{\frac{\alpha_{ij}}{2}}$. Para el resto de columnas, añadiremos dos ceros. Tenemos ahora que el nuevo producto escalar de las dos columnas consideradas es $\alpha_{ij} - \frac{\alpha_{ij}}{2} - \frac{\alpha_{ij}}{2} = 0$ y ambas serán ortogonales. Esto obliga a añadir hasta dos estados por cada par de columnas, por lo que Q se verá ampliado en $O(n^2)$ estados.

Después del paso anterior, haremos que las columnas A^0_σ hasta A^{n+1}_σ tengan la misma norma. Para ello, si la mayor de las normas de las columnas es l, para cada columna A^i_σ de norma $k < l$ añadiremos dos nuevos estados a Q (uno de aceptación y otro de rechazo) de modo que para las dos nuevas filas de A^i_σ tomamos los valores $\sqrt{\frac{l^2-k^2}{2}}$. Al resto de columnas le añadiremos dos ceros en esas filas. Así, todas las columnas tienen ahora longitud l.

Después, completamos las columnas A^i_σ para $i > n+1$ añadidas en los pasos anteriores de forma que se preserve la ortogonalidad entre todo par de columnas de la matriz y todas tengan longitud l. Tras esto, multiplicamos la matriz por el escalar $c_\sigma = l^{-1}$. Ahora todas las columnas de la matriz son unitarias.

Para las n primeras columnas, por cada dos nuevos estados añadidos, las amplitudes del estado de aceptación y del estado de rechazo son iguales, por lo que ofrecerán misma probabilidad de rechazo y aceptación tras cada símbolo.

El estado inicial $|s_{init}\rangle$ de M será $(1, 0, \ldots, 0)^T$ y, tras la lectura de #, se llegará al estado

$$U_\# |s_{init}\rangle = c_\# \begin{pmatrix} v_0 \\ v_0' \end{pmatrix}$$

Llegado a este punto no se parará con probabilidad $(c_\# \|v_0\|)^2$, se aceptará con probabilidad $\frac{1-(c_\# \|v_0\|)^2}{2}$ y se rechazará con probabilidad $\frac{1-(c_\# \|v_0\|)^2}{2}$.

Si consideramos $c = (\prod_{i=1}^n c_{\sigma_i}) c_\#$ y haciendo uso de la función de evolución, la configuración del autómata tras leer $\#w = \#\sigma_1\sigma_2\cdots\sigma_n$ será

$$(c(v_n, 0, \ldots, 0)^T, p_{acc}, p_{rej})$$

Representamos por p_{acc} y p_{rej} las probabilidades de haber aceptado y rechazado antes de leer \$. Además, por las propiedades de las matrices construidas, sabemos que $p_{acc} =$

p_{rej}. Tras leer \$, la configuración será $(0, c^2 f_P(w) + p_{acc}, c^2(1 - f_P(w)) + p_{rej})$. Podemos ver entonces que

$$p_{acc} = c^2 f_P(w) + \frac{1 - c^2 f_P(w) - c^2(1 - f_P(w))}{2}$$
$$p_{rej} = c^2(1 - f_P(w)) + \frac{1 - c^2 f_P(w) - c^2(1 - f_P(w))}{2}$$

y la probabilidad final de aceptación del autómata es

$$f_M(w) = c^2 f_P(w) + \frac{1 - c^2 f_P(w) - c^2(1 - f_P(w))}{2} = \frac{1}{2} + \frac{c^2}{2}(2 f_P(w) - 1)$$

De este modo, $f_M(w) > \frac{1}{2}$ si $f_P(w) > \frac{1}{2}$ y $f_M(w) < \frac{1}{2}$ si $f_P(w) < \frac{1}{2}$. □

El siguiente resultado también está demostrado en [25].

Lema 3.10.2. *Para todo MMQFA M con n estados clásicos y función de aceptación $f_M : \Sigma^* \to [0,1]$ existe un GPFA P con $O(n^2)$ estados y función de aceptación $f_P : \Sigma^* \to \mathbb{R}$ tal que para toda cadena $w \in \Sigma^*$ se verifica*

$$f_M(w) = f_P(w)$$

Demostración. Sea un MMQFA M con n estados clásicos. El observable y el estado inicial del autómata pueden ser escritos de la siguiente forma: $Q_{non} = \{|q_1\rangle, \ldots, |q_{k_1}\rangle\}$, $Q_{acc} = \{|q_{k_1+1}\rangle, \ldots, |q_{k_1+k_2}\rangle\}$, $Q_{rej} = \{|q_{k_1+k_2+1}\rangle, \ldots, |q_{k_1+k_2+k_3}\rangle\}$, $H_{non} = \text{span}(Q_{non}), H_{acc} = \text{span}(Q_{acc}), H_{rej} = \text{span}(Q_{rej})$, $H = H_{non} \oplus H_{acc} \oplus H_{rej}$, $|s_{init}\rangle = |q_1\rangle$. Por tanto, cualquier autómata MMQFA puede escribirse con ese estado inicial sin más que cambiar la matriz $U_\#$ de manera apropiada.

Consideremos una palabra marcada con los símbolos inicial y final $\#w\$$. Al leer el símbolo j-ésimo ($1 \leq j \leq n+2$), el estado del autómata es $|\psi^j\rangle$ y podemos considerar los siguientes vectores:

- $|\psi^j_{non}\rangle = P_{non} |\psi^j\rangle$
- $|\psi^j_{acc}\rangle = P_{acc} |\psi^j\rangle$
- $|\psi^j_{rej}\rangle = P_{rej} |\psi^j\rangle$

Para $j = 0$, consideraremos $|\psi^j_{non}\rangle = |s_{init}\rangle$. Además, para la lectura del símbolo j-ésimo y el valor $k_1+1 \leq l \leq k_1+k_2$ consideramos el valor $p_{acc}^{q_{k_1+l}}(j)$ que representa la "probabilidad" de haber aceptado llegando a ese estado en esos j primeros pasos.

Podemos ver la matriz asociada al símbolo $\sigma \in \tilde{\Sigma}$ como

$$U_\sigma = \left(\begin{array}{c|c|c} U_{\sigma,k_1\times k_1} & U_{\sigma,k_1\times k_2} & U_{\sigma,k_1\times k_3} \\ \hline U_{\sigma,k_2\times k_1} & U_{\sigma,k_2\times k_2} & U_{\sigma,k_2\times k_3} \\ \hline U_{\sigma,k_3\times k_1} & U_{\sigma,k_3\times k_2} & U_{\sigma,k_3\times k_3} \end{array}\right)$$

Construimos entonces la matriz A_σ que nos servirá como primer paso para construir las matrices del GPFA

$$A_\sigma = \left(\begin{array}{c|c} U_{\sigma,k_1\times k_1} \otimes U^*_{\sigma,k_1\times k_1} & 0 \\ \hline U_{\sigma,k_2\times k_1}(1) \otimes U^*_{\sigma,k_2\times k_1}(1) & \\ \cdots & I_{k_2} \\ U_{\sigma,k_2\times k_1}(k_2) \otimes U^*_{\sigma,k_2\times k_1}(k_2) & \end{array}\right)$$

donde $U_{\sigma,k_2\times k_1}(1)$ representa la fila l-ésima de la matriz $U_{\sigma,k_2\times k_1}$. También vamos a considerar los dos siguientes vectores

$$v_0 = ((|s_{init}\rangle_{k_1} \otimes |s_{init}\rangle_{k_1}^*)^T, 0, \ldots, 0)^T$$

$$v_{acc} = (\overbrace{0, \ldots, 0}^{k_1^2}, \overbrace{1, \ldots, 1}^{k_2})^T$$

La notación $|s_{init}\rangle_{k_1}$ representa el vector formado sólo por las k_1 primeras componentes de $|s_{init}\rangle$ y la utilizaremos en más ocasiones. Con todo esto, si consideramos el símbolo j-ésimo de $\#w\$$, vamos a probar por inducción la siguiente igualdad:

$$v_j = ((|\psi_{non}^j\rangle_{k_1} \otimes |\psi_{non}^j\rangle_{k_1}^*)^T, p_{acc}^{q_{k_1+1}}(j), \ldots, p_{acc}^{q_{k_1+k_2}}(j))^T$$

Para esta parte de la demostración utilizaremos la siguiente propiedad del producto tensorial: si disponemos de dos vectores $|\psi_1\rangle \in H_1, |\psi_2\rangle \in H_2$ y dos operadores lineales (matrices) A y B en H_1 y H_2, respectivamente, entonces se cumple:

$$(A \otimes B)(|\psi_1\rangle \otimes |\psi_2\rangle) = (A\,|\psi_1\rangle) \otimes (B\,|\psi_2\rangle)$$

El caso base de la inducción es aquel en que $j = 1$. Veamos que se verifica $v_1 = A_{\sigma_1} v_0$. La primera parte del vector $v_1 = (\alpha_1, \ldots, \alpha_{k_1^2}, \alpha_{k_1^2+1} \ldots, \alpha_{k_1^2+k_2})^T$ es igual a

$$\begin{aligned}(U_{\sigma,k_1\times k_1} \otimes U_{\sigma,k_1\times k_1}^*)(|s_{init}\rangle_{k_1} \otimes |s_{init}\rangle_{k_1}^*) &= (U_{\sigma,k_1\times k_1}\,|s_{init}\rangle_{k_1}) \otimes (U_{\sigma,k_1\times k_1}^*\,|s_{init}\rangle_{k_1}^*) \\ &= |\psi_{non}^1\rangle_{k_1} \otimes |\psi_{non}^1\rangle_{k_1}^*\end{aligned}$$

La segunda parte de v_1 está formado por las componentes $\alpha_{k_1^2+l}$, $1 \le l \le k_2$, iguales a

$$\begin{aligned}\alpha_{k_1^2+l} &= (U_{\sigma,k_2\times k_1}(l) \otimes U_{\sigma,k_2\times k_1}^*(l))(|s_{init}\rangle_{k_1} \otimes |s_{init}\rangle_{k_1}^*) \\ &= (U_{\sigma,k_2\times k_1}(l)\,|s_{init}\rangle_{k_1}) \otimes (U_{\sigma,k_2\times k_1}^*(l)\,|s_{init}\rangle_{k_1}^*) \\ &= |\psi_{acc}^1\rangle_{k_1}(l) \otimes |\psi_{acc}^1\rangle_{k_1}^*(l) = |\psi_{acc}^1\rangle_{k_1}(l)\,|\psi_{acc}^1\rangle_{k_1}^*(l) = p_{acc}^{q_{k_1+l}}(1)\end{aligned}$$

Suponiendo cierto el resultado para $j-1$, veamos qué sucede para j. En primer lugar, la primera parte del vector es igual a

$$\begin{aligned}(U_{\sigma,k_1\times k_1} \otimes U_{\sigma,k_1\times k_1}^*)(|\psi_{non}^{j-1}\rangle_{k_1} \otimes |\psi_{non}^{j-1}\rangle_{k_1}^*) &= (U_{\sigma,k_1\times k_1}\,|\psi_{non}^{j-1}\rangle_{k_1}) \otimes (U_{\sigma,k_1\times k_1}^*\,|\psi_{non}^{j-1}\rangle_{k_1}^*) \\ &= |\psi_{non}^j\rangle_{k_1} \otimes |\psi_{non}^j\rangle_{k_1}^*\end{aligned}$$

La segunda parte del vector es igual a

$$\begin{aligned}\alpha_{k_1^2+l} &= (U_{\sigma,k_2\times k_1}(l) \otimes U_{\sigma,k_2\times k_1}^*(l))(|\psi_{non}^{j-1}\rangle_{k_1} \otimes |\psi_{non}^{j-1}\rangle_{k_1}^*) + p_{acc}^{q_{k_1+l}}(j-1) \\ &= (U_{\sigma,k_2\times k_1}(l)\,|\psi_{non}^{j-1}\rangle_{k_1}) \otimes (U_{\sigma,k_2\times k_1}^*(l)\,|\psi_{non}^{j-1}\rangle_{k_1}^*) + p_{acc}^{q_{k_1+l}}(j-1) \\ &= |\psi_{acc}^1\rangle_{k_1}(l) \otimes |\psi_{acc}^1\rangle_{k_1}^*(l) + p_{acc}^{q_{k_1+l}}(j-1) \\ &= |\psi_{acc}^{j-1}\rangle_{k_1}(l)\,|\psi_{acc}^{j-1}\rangle_{k_1}^*(l) + p_{acc}^{q_{k_1+l}}(j-1) = p_{acc}^{q_{k_1+l}}(j)\end{aligned}$$

Esta propiedad que acabamos de ver nos lleva al siguiente vector tras leer todos los símbolos de la palabra

$$v_{n+2} = ((|\psi_{acc}^{n+2}\rangle \otimes |\psi_{acc}^{n+2}\rangle^*)^T, p_{acc}^{q_{k_1+1}}(n+2), \ldots, p_{acc}^{q_{k_1+k_2}}(n+2))^T$$

$$v_{acc}v_{n+2} = \sum_{l=1}^{k_2} p_{acc}^{q_{k_1+l}}(n+2) = f_M(w)$$

Las matrices que hemos considerado hasta ahora son complejas, pero es necesario que sean reales para poder construir un GPFA. Para ello, vamos a tener en cuenta que cualquier número complejo $a + bi$ puede ser expresado en forma matricial como

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \tag{3.4}$$

Modificamos entonces las matrices y los vectores anteriores de modo que cada número complejo tiene la representación de la ecuación 3.4. Así, obtenemos las matrices v'_0 (de dimensiones $2(k_1^2 + k_2) \times 2$), v'_{acc} $(2 \times 2(k_1^2 + k_2))$ y A'_σ $(2(k_1^2 + k_2) \times 2(k_1^2 + k_2))$ de modo que

$$v'_{acc}A'_{\$}A'_wA'_{\#}v'_0 = \begin{pmatrix} f_M(w) & 0 \\ 0 & f_M(w) \end{pmatrix}$$

Podemos entonces tomar como vector inicial $\overline{v_0}$ la primera columna de $A'_{\#}v'_0$ y como vector de aceptación $\overline{v_{acc}}$ la primera fila de $v'_{acc}A'_{\$}$. De ese modo, tenemos

$$\overline{v_{acc}}A'_w\overline{v_0} = f_M(w)$$

y el autómata GPFA $P = (\Sigma, S, \{A'_\sigma \mid \sigma \in \Sigma\}, \overline{v_0}, \overline{v_{acc}})$ donde S tiene $k_1^2 + k_2$ estados ($O(n^2)$ estados). Este autómata cumple la condición requerida

$$f_P(w) = f_M(w)$$

□

Los dos lemas anteriores, juntos con los resultados conocidos acerca de la capacidad de aceptación de los PFAs y los GPFAs, sirven para probar el siguiente resultado acerca de la capacidad de aceptación con error no acotado por parte de los autómatas MMQFA.

Teorema 3.10.1. *El conjunto de lenguajes reconocidos por un MMQFA con error no acotado es exactamente el de los lenguajes estocásticos.*

3.10.2 Un MOQFA reconoce un subconjunto propio de los lenguajes estocásticos

Hemos visto en el ejemplo 3.8.2 un lenguaje no regular que puede ser reconocido por un MOQFA con error no acotado. Por tanto, un MOQFA es capaz de reconocer lenguajes no regulares con error no acotado. A su vez, sabemos por la sección anterior que como mucho podrá reconocer los lenguajes estocásticos. En esta sección veremos que sólo son capaces de reconocer un subconjunto propio de esos lenguajes, ya que no son capaces de reconocer lenguajes con un número finito de palabras a excepción del lenguaje vacío. El siguiente resultado fue enunciado y demostrado por Bertoni y Carpentieri [7].

Lema 3.10.3. *Si L es el lenguaje reconocido con error no acotado por un autómata MOQFA M, entonces para cualquier $x \in \Sigma^*$ y para cualquier $w \in L$ existe un entero positivo l tal que $wx^l \in L$.*

Demostración. Si escribimos el subespacio de aceptación del autómata como $H_{acc} = \text{span}(|q_1\rangle, |q_2\rangle, \ldots, |q_m\rangle)$ y hacemos uso de las propiedades del valor absoluto y de la norma, para cualquier $k \in \mathbb{N}$ tenemos que

$$\begin{aligned}
|f(w) - f(wx^k)| &= |\|P_{acc}U_w |s_{init}\rangle\|^2 - \|P_{acc}U_{wx^k} |s_{init}\rangle\|^2| \\
&= |\sum_{i=1}^{m} |\langle q_i| U_w |s_{init}\rangle|^2 - |\langle q_i| U_{wx^k} |s_{init}\rangle|^2| \\
&\leq 2\sum_{i=1}^{m} ||\langle q_i| U_w |s_{init}\rangle| - |\langle q_i| U_{wx^k} |s_{init}\rangle|| \\
&\leq 2\sum_{i=1}^{m} |\langle q_i| U_w |s_{init}\rangle - \langle q_i| U_{wx^k} |s_{init}\rangle| \\
&= 2\sum_{i=1}^{m} |\langle q_i| (I - U_x^k) U_w |s_{init}\rangle| \\
&\leq 2\sum_{i=1}^{m} \left\|I - U_x^k\right\| = 2m \left\|I - U_x^k\right\|
\end{aligned}$$

Si λ es el punto de corte no estricto de L, sabemos que $f(w) > \lambda$, es decir, $f(w) - \lambda = \delta > 0$. Por el lema 3.9.4, sabemos que existe un l tal que

$$\left\|I - U_x^l\right\| \leq \frac{\delta}{4m}$$

y por la ecuación anterior, sabemos que

$$|f(w) - f(wx^l)| \leq \frac{\delta}{2}$$

Entonces, se tiene que

$$f(wx^l) - \lambda \geq f(w) - \frac{\delta}{2} - \lambda = \delta - \frac{\delta}{2} = \frac{\delta}{2} > 0$$

Por tanto, $wx^l \in L$. □

La consecuencia del lema que acabamos de probar es que cualquier lenguaje reconocido con error no acotado por un MOQFA es vacío o contiene infinitas palabras. Esto hace que un MOQFA sólo sea capaz de reconocer un subconjunto propio de los lenguajes estocásticos.

Capítulo 4

Autómatas finitos cuánticos bidireccionales

Los autómatas presentados en la sección anterior eran unidireccionales, es decir, sólo permitían la lectura de una cadena de izquierda a derecha, símbolo a símbolo. Es posible definir autómatas finitos cuánticos de modo que tengamos una cinta de lectura sobre la que se encuentra la cadena w y que nos permita desplazarnos tanto a izquierda como a derecha. Son estos los autómatas finitos cuánticos bidireccionales.

En el caso clásico, también es posible definir una versión bidireccional de los autómatas finitos deterministas. Sin embargo, esta versión no aporta ningún poder adicional al de la versión unidireccional y sólo puede reconocer lenguajes regulares. En el caso cuántico, esto no es así. Veremos ejemplos de lenguajes no regulares que pueden ser reconocidos con error acotado por un autómata bidireccional, algo que no era posible con los autómatas unidireccionales.

4.1 Definición de 2QFA

Definición 4.1.1. Un *autómata finito cuántico bidireccional* (2QFA) es una 5-tupla

$$M = (\Sigma, Q, \delta, |q_0\rangle, R)$$

donde

- Σ es un alfabeto de entrada.
- Q es un conjunto de estados clásicos como los que describíamos para los autómatas unidireccionales.
- $|q_0\rangle$ es un estado inicial.
- Las transiciones vienen dadas por la función $\delta : Q \times \tilde{\Sigma} \times Q \times \{-1, 0, 1\} \to \mathbb{C}$ que en breve detallaremos.
- R es la regla de aceptación de los autómatas MMQFA con una pequeña salvedad que comentaremos más adelante.

Antes considerábamos el espacio de Hilbert $H = \ell_2(Q)$. Sin embargo, ahora consideramos el espacio $H = \ell_2(Q \times \mathbb{Z}_m)$. El valor m representa la longitud de la cinta y $k \in \mathbb{Z}_m$ su

posición k-ésima. La posición 1 vendrá ocupada siempre por el símbolo # y la posición m, por el símbolo \$. Entonces, un estado de un autómata bidireccional es una combinación lineal

$$|\psi\rangle = \alpha_{1,1}\,|q_1, 1\rangle + \ldots + \alpha_{1,m}\,|q_1, m\rangle + \ldots + \alpha_{n,1}\,|q_n, 1\rangle + \ldots + \alpha_{n,m}\,|q_n, m\rangle$$

que verifica la condición

$$|\alpha_{1,1}|^2 + \ldots + |\alpha_{1,m}|^2 + \ldots + |\alpha_{n,1}|^2 + \ldots + |\alpha_{n,m}|^2 = 1 \tag{4.1}$$

Para $|q_1\rangle, |q_2\rangle \in Q$, $\sigma \in \Sigma$ y $d \in \{-1, 0, 1\}$, $\delta(|q_1\rangle, \sigma, |q_2\rangle, d)$ representa la amplitud con que un autómata en el estado $|q_1\rangle$ pasará al estado $|q_2\rangle$ tras leer σ y moverá la cabeza de la cinta d posiciones. Esta función determina un operador lineal U_δ^m que, para un elemento $|q, k\rangle \in Q \times \mathbb{Z}_m$ es

$$U_\delta^m\,|q, k\rangle = \sum_{\substack{|q'\rangle \in Q \\ d \in \{-1,0,1\}}} \delta(|q\rangle, w_j, |q'\rangle, d)\;|q', k + d \pmod m\rangle$$

Cabe remarcar que w_j representa el símbolo σ que se encuentra en la posición j de la cinta. Además, se ha añadido el operador $\pmod m$ a la hora de actualizar la posición de la cabeza de la cinta. Esto es así para no salirnos de la longitud de la misma. De ese modo, tenemos una cinta circular en la que se puede pasar de la última posición a la primera, y viceversa. Esto hace que el autómata no pare si tras leer \$ se obtiene el subespacio de no parada como sucedía en el caso unidireccional. Ahora sólo se parará al obtener el subespacio de aceptación o el de rechazo.

El operador U_δ^m ha de ser unitario. Para ello, es necesario que se cumplan las siguientes condiciones:

1. $\displaystyle\sum_{|q'\rangle, d} \delta^*(|q_1\rangle, \sigma, |q'\rangle, d)\delta(|q_2\rangle, \sigma, |q'\rangle, d) = \begin{cases} 1 & \text{si } |q_1\rangle = |q_2\rangle \\ 0 & \text{si } |q_1\rangle \neq |q_2\rangle \end{cases}$
2. $\displaystyle\sum_{|q'\rangle} \delta^*(|q_1\rangle, \sigma_1, |q'\rangle, 1)\delta(|q_2\rangle, \sigma_2, |q'\rangle, 0) = 0$
3. $\displaystyle\sum_{|q'\rangle} \delta^*(|q_1\rangle, \sigma_1, |q'\rangle, 0)\delta(|q_2\rangle, \sigma_2, |q'\rangle, -1) = 0$
4. $\displaystyle\sum_{|q'\rangle} \delta^*(|q_1\rangle, \sigma_1, |q'\rangle, 1)\delta(|q_2\rangle, \sigma_2, |q'\rangle, -1) = 0$

En primer lugar, para verificar que U_δ^m es un operador unitario necesitamos ver que todos los vectores $U_\delta^m\,|q, k\rangle$ son unitarios. Claramente, por la condición 1, para cualquier $|q\rangle \in Q$ y para cualquier $k \in \mathbb{Z}_m$, se cumple que $\|U_\delta^m\,|q, k\rangle\| = 1$.

Además, también necesitamos que se cumpla que para cualquier par de estados $|q_1, k_1\rangle$, $|q_2, k_2\rangle$ tales que $|q_1, k_1\rangle \neq |q_2, k_2\rangle$, $U_\delta^m\,|q_1, k_1\rangle$ y $U_\delta^m\,|q_2, k_2\rangle$ sean ortogonales. La condición 1 nos muestra que esto se cumple para cualquier par de vectores $|q_1, k\rangle, |q_2, k\rangle$ con $|q_1\rangle \neq |q_2\rangle$. Si tenemos dos estados $|q_1, k_1\rangle, |q_2, k_1\rangle$ que cumplan $|k_1 - k_2| = 1$, entonces por las condiciones 2 y 3 es fácil comprobar que $U_\delta^m\,|q_1, k_1\rangle$ y $U_\delta^m\,|q_2, k_2\rangle$ serán ortogonales. Si los dos estados anteriores cumplen $|k_1 - k_2| = 2$, por la condición 4 sus imágenes por U_σ^m son ortogonales. Por último, si $|k_1 - k_2| > 2$, es evidente que sus imágenes por U_σ^m son ortogonales ya que no es posible llegar desde ambos al mismo estado.

Definición 4.1.2. Un autómata que verifica las cuatro condiciones anteriores se dice que es un autómata *bien formado*.

Las condiciones de un autómata bien formado se cumplen siempre para un tipo de autómata fácil de especificar y que veremos a continuación.

4.1.1 Autómata bidireccional simple

Definición 4.1.3. Un autómata finito cuántico bidireccional M es *simple* si para todo símbolo $\sigma \in \tilde{\Sigma}$ existe una matriz unitaria U_σ y una función $D : Q \to \{-1, 0, 1\}$ tales que

$$\delta(|q\rangle, \sigma, |q'\rangle, d) = \begin{cases} \langle q'|U_\sigma|q\rangle & D(q') = d \\ 0 & D(q') \neq d \end{cases}$$

para cualquier $|q\rangle \in Q$ y $\sigma \in \tilde{\Sigma}$. $\langle q'|U_\sigma|q\rangle$ representa la componente de $U_\sigma |q\rangle$ correspondiente a $|q'\rangle$.

Lema 4.1.1. *Un autómata bidireccional simple es un autómata bien formado si y sólo si*

$$\sum_{|q'\rangle} \langle q'|U_\sigma|q_1\rangle^* \langle q'|U_\sigma|q_2\rangle = \begin{cases} 1 & |q_1\rangle = |q_2\rangle \\ 0 & |q_1\rangle \neq |q_2\rangle \end{cases}$$

Demostración. Supongamos que tenemos un autómata simple que cumple la condición del lema. Si $d_1 \neq d_2$, $\delta^*(|q_1\rangle, \sigma, |q'\rangle, d_1)\delta(|q_2\rangle, \sigma, |q'\rangle, d_2) = 0$, pues en ambos casos se llega al estado $|q'\rangle$, pero con movimientos distintos de la cabeza de la cinta y eso, por la definición de autómata simple, hace que alguna de las dos amplitudes sea 0. Entonces, las condiciones 2,3 y 4 se cumplen.

Para probar la condición 1, primero observamos que por la definición de autómata simple se cumple

$$\sum_d \delta^*(|q_1\rangle, \sigma, |q'\rangle, d)\delta(|q_2\rangle, \sigma, |q'\rangle, d) = \delta^*(|q_1\rangle, \sigma, |q'\rangle, d')\delta(|q_2\rangle, \sigma, |q'\rangle, d')$$

donde $d' = D(q')$. Entonces,

$$\begin{aligned} \sum_{|q'\rangle, d} \delta^*(|q_1\rangle, \sigma, |q'\rangle, d)\delta(|q_2\rangle, \sigma, |q'\rangle, d) &= \sum_{|q'\rangle} \delta^*(|q_1\rangle, \sigma, |q'\rangle, d')\delta(|q_2\rangle, \sigma, |q'\rangle, d') \\ &= \sum_{|q'\rangle} \langle q'|U_\sigma|q_1\rangle^* \langle q'|U_\sigma|q_2\rangle = \begin{cases} 1 & |q_1\rangle = |q_2\rangle \\ 0 & |q_1\rangle \neq |q_2\rangle \end{cases} \end{aligned}$$

Cabe destacar que el valor de d' no es único, sino que depende del estado $|q'\rangle$.

El argumento que acabamos de utilizar para probar la condición 1 es reversible y nos permite probar la otra implicación. □

Mediante los autómatas simples podemos construir autómatas bidireccionales de manera similar a como hicimos en el caso unidireccional. El único añadido tiene que ver con la necesidad de definir la función D que, para cada estado, determina un movimiento en una dirección.

4.2 Ejemplos

Los autómatas 2QFA son más poderosos que los 1QFA. Kondacs y Watrous probaron que todo lenguaje regular puede ser reconocido con error acotado por un 2QFA. Además, estos autómatas son capaces de reconocer algunos lenguajes no regulares (e incluso algunos lenguajes que no son independientes del contexto, como $\{a^n b^n c^n \mid n \geq 1\}$). En esta sección nos limitaremos a ver esto último mediante algunos ejemplos. En primer lugar, veremos un ejemplo sencillo de un lenguaje no regular que puede ser reconocido con punto de corte aislado por un 2QFA.

Ejemplo 4.2.1. Consideremos el lenguaje $EQ = \{w \in \{a,b\}^* \mid |w|_a = |w|_b\}$. Sea M un autómata tal que $Q = \{|q_0\rangle, |q_1\rangle, |q_2\rangle, |q_{acc}\rangle, |q_{rej}\rangle\}$, donde $|q_0\rangle$ es el estado inicial, $Q_{acc} = \{|q_{acc}\rangle\}$ y $Q_{rej} = \{|q_{rej}\rangle\}$. Consideramos las matrices unitarias dadas por:

- Símbolo #:
$$U_{\#} |q_0\rangle = \frac{1}{\sqrt{2}} |q_0\rangle + \frac{1}{\sqrt{2}} |q_1\rangle$$
- Símbolo a:
$$U_a |q_0\rangle = |q_2\rangle\,,\ U_a |q_1\rangle = |q_1\rangle\,,\ U_a |q_2\rangle = |q_0\rangle$$
- Símbolo b:
$$U_b |q_0\rangle = |q_0\rangle\,,\ U_b |q_1\rangle = |q_2\rangle\,,\ U_b |q_2\rangle = |q_1\rangle$$
- Símbolo \$:
$$U_{\$} |q_0\rangle = \frac{1}{\sqrt{2}} |q_{acc}\rangle + \frac{1}{\sqrt{2}} |q_{rej}\rangle\,,\ U_{\$} |q_1\rangle = \frac{1}{\sqrt{2}} |q_{acc}\rangle - \frac{1}{\sqrt{2}} |q_{rej}\rangle$$

Las imágenes de D para cada estado clásico son

$$D(|q_2\rangle) = 0, D(|q_0\rangle) = D(|q_1\rangle) = +1$$

El autómata, tras leer #, entra en el estado $\frac{1}{\sqrt{2}} |q_0\rangle + \frac{1}{\sqrt{2}} |q_1\rangle$. Cada símbolo a hace que la componente correspondiente a $|q_0\rangle$ mueva su cabeza de la cinta una posición a la derecha en dos pasos ($U_a |q_0\rangle = |q_2\rangle$, la cabeza de la cinta queda en la misma posición y $U_a |q_2\rangle = |q_0\rangle$, moviéndola una posición a la derecha). En el caso de la componente correspondiente a $|q_1\rangle$, mueve la cabeza una posición a la derecha en un sólo paso ($U_a |q_1\rangle = |q_1\rangle$ y $D(|q_1\rangle) = +1$). Es al revés en el caso de que se lea una b. De este modo, si $|w|_a = |w|_b$, ambas configuraciones alcanzan \$ a la vez. Es decir, llegan a \$ en el estado $\frac{1}{\sqrt{2}} |q_0\rangle + \frac{1}{\sqrt{2}} |q_1\rangle$. La aplicación de $U_{\$}$ sobre este estado da como resultado

$$\left(\frac{1}{2} |q_{acc}\rangle + \frac{1}{2} |q_{rej}\rangle\right) + \left(\frac{1}{2} |q_{acc}\rangle - \frac{1}{2} |q_{rej}\rangle\right) = |q_{acc}\rangle$$

En el caso de que w no tenga el mismo número de as que de bs, uno de los dos llegará antes que el otro. De este modo, se acepta el input con probabilidad $\frac{1}{2}$.

Se reconoce, entonces, el lenguaje EQ con punto de corte aislado.

Ahora veremos el ejemplo más representativo del poder de los 2QFA. Fue el primer ejemplo con que se probó que un 2QFA puede reconocer lenguajes no regulares con error acotado [17].

Ejemplo 4.2.2. El lenguaje $L = \{a^m b^m \mid m \geq 1\}$ puede ser reconocido por un 2QFA con punto de corte aislado. Dado un entero positivo N, definimos el autómata bidireccional M_N de modo que:

- $\Sigma = \{a, b\}$
- $Q = \{|q_0\rangle, |q_1\rangle, |q_2\rangle, |q_3\rangle\} \cup \{|r_{j,k}\rangle \mid 1 \leq j \leq N, 0 \leq k \leq \text{máx}(j, N-j+1)\} \cup \{|s_j\rangle \mid 1 \leq j \leq N\}$
- $H_{acc} = \text{span}(s_N)$
- $H_{rej} = \text{span}(\{q_3\} \cup \{s_j \mid 1 \leq j \leq N\})$

Las transiciones entre estados (sólo las relevantes) vienen dadas por las siguientes matrices:

- Símbolo #:

$$U_\# |q_0\rangle = |q_0\rangle, U_\# |q_1\rangle = |q_3\rangle$$

$$U_\# |r_{j,0}\rangle = \frac{1}{\sqrt{N}} \sum_{l=1}^{N} e^{\frac{2\pi i j l}{N}} |s_l\rangle, 1 \leq j \leq N$$

- Símbolo a:

$$U_a |q_0\rangle = |q_0\rangle, U_a |q_1\rangle = |q_2\rangle, U_a |q_2\rangle = |q_3\rangle,$$

$$U_a |r_{j,0}\rangle = |r_{j,j}\rangle, 1 \leq j \leq N$$

$$U_a |r_{j,k}\rangle = |r_{j,k-1}\rangle, 1 \leq j \leq N, 1 \leq k \leq j$$

- Símbolo b:

$$U_b |q_0\rangle = |q_1\rangle, U_b |q_2\rangle = |q_2\rangle$$

$$U_b |r_{j,0}\rangle = |r_{j,N+1-j}\rangle, 1 \leq j \leq N$$

$$U_b |r_{j,k}\rangle = |r_{j,k-1}\rangle, 1 \leq j \leq N, 1 \leq k \leq N+1-j$$

- Símbolo \$:

$$U_\$ |q_0\rangle = |q_3\rangle, U_\$ |q_2\rangle = \frac{1}{\sqrt{N}} \sum_{j=1}^{N} |r_{j,0}\rangle$$

Además, las imágenes de la función D para cada estado clásico son las siguientes:

$$D(|q_0\rangle) = +1,\ D(|q_1\rangle) = -1,\ D(|q_2\rangle) = +1,\ D(|q_3\rangle) = 0$$

$$D(|r_{j,k}\rangle) = 0,\ 1 \leq j \leq N,\ 0 \leq k \leq \text{máx}(j, N-j+1)$$

$$D(|r_{j,0}\rangle) = -1,\ D(|s_j\rangle) = 0,\ 1 \leq j \leq N$$

Puede verse claramente que, para cada $\sigma \in \Sigma$, los vectores de la forma $U_\sigma |q_i\rangle$ son todos ortogonales entre sí y, además, tienen norma uno (son ortonormales). Para obtener el autómata completo basta con establecer las transiciones restantes de modo que completen una base ortonormal para cada $\sigma \in \Sigma$.

Este autómata tiene dos partes: en primer lugar, comprueba que la cadena leída es de la forma $a^m b^n$, $m, n > 0$ y, después, comprueba $m = n$.

Durante la primera parte, distinguimos tres casos:

- Palabra que no comienza por a: si la palabra es vacía, se realiza la transformación $U_\$ |q_0\rangle = |q_3\rangle$ y es rechazada. Si no, el primer símbolo será b y la transformación $U_b |q_0\rangle = |q_1\rangle$. Como $D(|q_1\rangle) = -1$, el siguiente símbolo es #. $U_\# |q_1\rangle = |q_3\rangle$, por lo que también se rechaza la palabra.

- Palabra sin ninguna b: tras leer todas las as, llega al símbolo \$ en el estado q_0. $U_\$ |q_0\rangle = |q_3\rangle$ y la palabra es rechazada.

- Palabra correcta $a^m b^n$, $m, n > 0$: tras leer la primera b, pasa al estado $|q_1\rangle$ y la cabeza de la cinta vuelve a la última a. $U_a |q_1\rangle = |q_2\rangle$ y la cabeza de la cinta vuelve a la primera b. Lee el resto de la palabra manteniéndose en el estado $|q_2\rangle$ hasta llegar al símbolo \$.

- Palabra de la forma $a^m b^n a\omega$: tras leer $a^m b^n$, el autómata está en estado $|q_2\rangle$ y la cabeza de la cinta en la posición de la siguiente a. $U_a |q_2\rangle = |q_3\rangle$ y la palabra es rechazada.

Al empezar la segunda fase, la cabeza de la cinta está sobre el símbolo \$ y el sistema en el estado $|q_2\rangle$. Entonces, se deriva el cómputo en N caminos $|r_{j,0}\rangle$, $1 \leq j \leq N$, cada uno con amplitud $\frac{1}{\sqrt{N}}$. A lo largo del camino j, tras leer una b mantiene la cabeza fija durante $N+1-j$ pasos y después mueve una posición a la izquierda. Tras leer una a, se mantiene fija durante j pasos y después mueve hacia la izquierda una posición. El camino j necesita $1+(N+1-j)n+(j+1)m$ pasos para llegar desde \$ hasta #. Así, si otro camino j' llega a la vez que el camino j, se verifica $1+(N+1-j)n+(j+1)m = 1+(N+1-j')n+(j'+1)m$. Por tanto, en ese caso se tiene $j(m-n) = j'(m-n)$. Como $j \neq j'$, necesariamente $m = n$. Es decir, si $m = n$, todos los caminos llegan a # a la vez. Sin embargo, si $m \neq n$, ningún par de caminos distintos llega a la vez a #.

Al llegar al símbolo # la transformación unitaria aplicada sobre el estado $|r_{j,0}\rangle$ es la transformada cuántica de Fourier sobre los estados $\{|s_N, 0\rangle, |s_1, 0\rangle, \ldots, |s_{N-1}, 0\rangle\}$:

$$U_\# |r_{j,0}\rangle = \frac{1}{\sqrt{N}} \sum_{l=1}^{N} e^{\frac{2\pi i}{N} jl} |s_l, 0\rangle, \ 1 \leq j \leq N$$

En caso de que cada uno de los N caminos iniciales lleguen a # a la vez ($m = n$), el estado en que se encuentra el autómata es

$$\begin{aligned} \frac{1}{\sqrt{N}} \sum_{j=1}^{N} \frac{1}{\sqrt{N}} \sum_{l=1}^{N} e^{\frac{2\pi i}{N} jl} |s_l, 0\rangle &= \frac{1}{N} \sum_{l=1}^{N} \sum_{j=1}^{N} (e^{\frac{2\pi i}{N} j})^l |s_l, 0\rangle \\ &= \frac{1}{N} \sum_{l=1}^{N} \sum_{j=0}^{N-1} (e^{\frac{2\pi i}{N} j})^l |s_l, 0\rangle \end{aligned}$$

Si consideramos $\{\alpha_j = e^{\frac{2\pi i j}{N}} \mid 0 \leq j \leq N-1\}$ el conjunto de las raíces N-ésimas de la unidad, encontramos dos casos:

- Caso $l = N$: $\alpha_j^N = 1$, por lo que $\sum_{j=0}^{N-1} \alpha_j^l = \sum_{j=0}^{N-1} 1 = N$.

- Caso $l < N$: tenemos la suma parcial de una serie geométrica de razón α_1^l y término inicial 1. Por tanto, $\sum_{j=0}^{N-1} \alpha_j^l = \frac{1-\alpha_1^N}{1-\alpha_1} = 0$.

De este modo, si $m = n$, el estado en que se encuentra el autómata es $|s_N, 0\rangle$ y acepta con probabilidad 1.

En caso de que m y n sean distintos, cada uno de los N caminos llegan a c en momentos distintos. Al llegar el camino j, éste deriva en N caminos $e^{\frac{2\pi ijl}{N}} |s_l, 0\rangle$ $(1 \leq l \leq N)$, cada uno de ellos con amplitud $\frac{1}{\sqrt{N}}$. Por tanto, en cada uno de los N caminos se aceptará con probabilidad $\frac{1}{N^2}$ y rechazará con probabilidad $\frac{1}{N} - \frac{1}{N^2}$. Como hay N caminos, el autómata acabará aceptando la cadena con probabilidad $\frac{1}{N}$ y rechazándola con probabilidad $1 - \frac{1}{N}$.

El ejemplo anterior nos facilita el desarrollo del siguiente, donde veremos un lenguaje que no es independiente del contexto y puede ser reconocido con error acotado por un 2QFA.

Ejemplo 4.2.3. Sea $L = \{a^m b^m c^m \mid m \geq 1\}$. Vamos a modificar el autómata del ejemplo 4.2.1 de la forma que describimos a continuación.

Añadimos los estados de no parada $|q_4\rangle, |q_5\rangle, |r'_{j,k}\rangle$ con $1 \leq j \leq N, 0 \leq k \leq \text{máx}(j, N - j + 1)$. También añadimos los estados $|s'_j\rangle$ con $j \in \{1, \ldots, N\}$. Estos estados están todos en Q_{rej} a excepción de $|s'_N\rangle$, que se encuentra en Q_{non}. Todo estado que tuviéramos en el autómata anterior se mantiene, así como su condición de estado de aceptación, rechazo o no parada.

Las matrices nuevas o modificadas que nos interesan son las siguientes:

- Símbolo a:

$$U_a |q_5\rangle = |q_1\rangle$$

$$U_a |r'_{j,0}\rangle = \frac{1}{\sqrt{N}} \sum_{l=1}^{N} e^{\frac{2\pi ijl}{N}} |s'_l\rangle, \ 1 \leq j \leq N$$

- Símbolo b:

$$U_b |q_1\rangle = |q_0\rangle, \ U_b |q_4\rangle = |q_5\rangle, \ U_b |q_5\rangle = |q_3\rangle$$

$$U_b |r'_{j,0}\rangle = |r'_{j,j}\rangle, \ 1 \leq j \leq N$$

$$U_b |r'_{j,k}\rangle = |r'_{j,k-1}\rangle, \ 1 \leq j \leq N, \ 1 \leq k \leq j$$

- Símbolo c:

$$U_c |q_0\rangle = |q_3\rangle, \ U_c |q_1\rangle = |q_1\rangle, \ U_c |q_2\rangle = |q_4\rangle, \ U_c |q_5\rangle = |q_5\rangle$$

$$U_c |r'_{j,0}\rangle = |r'_{j,N+1-j}\rangle, \ 1 \leq j \leq N$$

$$U_c |r'_{j,k}\rangle = |r'_{j,k-1}\rangle, \ 1 \leq j \leq N, \ 1 \leq k \leq N + 1 - j$$

- Símbolo \$:

$$U_\$ |q_2\rangle = |q_1\rangle$$

Las imágenes de los nuevos estados por la función D son:

$$D(|q_4\rangle) = -1, \ D(|q_5\rangle) = +1$$

$$D(|r'_{j,0}\rangle) = -1, \ D(|s'_j\rangle) = 0, \ 1 \leq j \leq N$$

$$D(|r'_{j,k}\rangle) = 0, \ 1 \leq j \leq N, \ 1 \leq k \leq N + 1 - j$$

Las transiciones del ejemplo 4.2.1 que no hemos mencionado se mantienen igual. La modificación más notable es la de la transición correspondiente a la lectura de \$ en el estado $|q_2\rangle$, que ahora es $U_\$ |q_2\rangle = |q_1\rangle$. Puede comprobarse fácilmente que todas las transformaciones siguen siendo unitarias.

Este nuevo autómata se divide en tres fases, a diferencia de las dos del caso anterior. La primera comprueba que la cadena leída es de la forma $a^+b^+c^+$, la segunda verifica que el número de bs es igual al de cs y la tercera verifica que el número de as coincide con el de bs.

Para la primera fase distinguimos los siguientes casos:

- Palabra que no empieza por a: si la cadena es vacía o empieza por b, la situación es la misma que antes. Si la cadena empieza por el símbolo c, se realiza la transformación $U_c |q_0\rangle = |q_3\rangle$ y se rechaza.

- Palabra en que el primer símbolo que sigue a una a no es una b: si la palabra sólo tiene as, $U_\$ |q_0\rangle = |q_3\rangle$. Si la palabra es continuada por una c, $U_c |q_0\rangle = |q_3\rangle$.

- Palabra de la forma a^+b^+w donde w no empieza por una c: si $w = \epsilon$, $U_\$ |q_2\rangle = |q_1\rangle$ y volvemos a la última b. $U_b |q_1\rangle = |q_0\rangle$ y regresamos a \$. Por último, $U_\$ |q_0\rangle = |q_3\rangle$. Si w empieza por a, $U_a |q_2\rangle = |q_3\rangle$.

- Palabra de la forma $a^+b^+c^+aw$ o $a^+b^+c^+bw$: en el primer caso, $U_a |q_5\rangle = |q_1\rangle$ y la cabeza se desplaza a la última c. Como $U_c |q_1\rangle = |q_1\rangle$, nos desplazaremos hacia atrás hasta la última b. Allí, $U_b |q_1\rangle = |q_0\rangle$ y volveremos a la primera c. Por último, $U_c |q_0\rangle = |q_3\rangle$. En el segundo caso, $U_b |q_5\rangle = |q_3\rangle$.

Si no se ha rechazado hasta ahora, entramos en la siguiente fase. La segunda fase transcurre de manera análoga a la segunda fase del ejemplo anterior hasta llegar al estado $|s'_N\rangle$. Si el número de bs es igual al de cs se llegará a este estado con probabilidad 1. Si no, se llegará con probabilidad $\frac{1}{N}$. A partir de aquí, nos mantendremos en este estado moviendo la cabeza hacia la derecha hasta llegar a la primera c. En este momento, pasamos a la tercera fase.

En la tercera fase se repite el proceso de la segunda fase del ejemplo anterior otra vez. Si el número de as es igual al de bs, la probabilidad de estar en $|s_N\rangle$ (y, por tanto, aceptar) será igual a la que obtuvimos en la segunda fase. Si no, esta probabilidad será $\frac{1}{N}$ veces la probabilidad anterior. Por tanto, si la palabra está en L se aceptará con probabilidad 1; si sólo coincide el principio o el final de la palabra, con probabilidad $\frac{1}{N}$; y si ambas partes de la palabra son inválidas, con probabilidad $\frac{1}{N^2}$.

De manera parecida a lo que hemos hecho en el ejemplo 4.2.3, es posible adaptar el autómata construido en el ejemplo 4.2.1 para otros lenguajes, como por ejemplo $\{a^n b^{2n} \mid n \geq 1\}$.

Capítulo 5

Conclusiones

Este trabajo nos ha permitido introducirnos en el mundo de la computación cuántica. Hemos introducido los formalismos matemáticos de los que hace uso esta disciplina y los postulados que conectan estos formalismos con el mundo físico. Todo esto sienta las bases para desarrollar modelos de computación cuánticos como pueden ser los autómatas finitos cuánticos.

En segundo lugar, hemos podido estudiar dos modelos de autómatas finitos cuánticos unidireccionales: los autómatas MOQFA y MMQFA. Hemos visto cuál es la relación entre ambos modelos, siendo posible simular un autómata MOQFA cualquiera mediante un autómata MMQFA. Además, hemos estudiado la capacidad de reconocimiento de lenguajes de ambos autómatas de dos formas distintas. Primero, hemos visto cómo estos autómatas son capaces de reconocer con error acotado menos lenguajes que los que reconoce un autómata finito clásico. Los autómatas MOQFA reconocen los *group languages*, mientras que los autómatas MMQFA reconocen un subconjunto propio de los lenguajes regulares. Todavía no se conoce una caracterización concreta de este subconjunto, pero sí disponemos de algunas construcciones que determinan lenguajes que no es posible reconocer mediante un MMQFA con error acotado. Después, hemos comprobado que la capacidad de reconocimiento de lenguajes con error no acotado es bastante superior que en el caso del reconocimiento con error acotado. Los autómatas MMQFA reconocen exactamente los mismo lenguajes que los autómatas probabilísticos: los lenguajes estocásticos. Por su parte, los autómatas MOQFA reconocen un subconjunto propio de los lenguajes estocásticos que no es el de los lenguajes regulares, ya que se conocen algunos lenguajes no regulares que son reconocidos por un MOQFA.

Por último, hemos presentado la definición de autómata finito cuántico bidireccional. De esta versión hemos visto tres ejemplos: dos de autómatas que reconocían un lenguaje no regular con error acotado y otro de un autómata que reconocía un lenguaje que no era independiente del contexto con error acotado. En el caso clásico, los autómatas bidireccionales reconocían solo lenguajes regulares, por lo que podemos ver que el modelo cuántico con reconocimiento con error acotado aporta una clara mejora.

Bibliografía

[1] A. Ambainis, M. Beaudry, M. Golovkins, A. Kikusts, M. Mercer, and D. Therien. Algebraic results on quantum automata. *Theory of Computing Systems*, 39:165–188, 2006.

[2] A. Ambainis and R. Freivalds. 1-way quantum finite automata: strengths, weaknesses and generalizations. In *39th Annual Symposium on Foundations of Computer Science, FOCS'98*, pages 332–341. IEEE, 1998.

[3] A. Ambainis, A. Kikusts, and M. Valdats. On the class of languages recognizable by 1-way quantum finite automata. In *8th Annual Symposium on Theoretical Aspects of Computer Science, STACS'01, LNCS 2010*, pages 75–86, 2001.

[4] A. Ambainis and A. Yakaryılmaz. Automata and quantum computing. https://arxiv.org/abs/1507.01988, 2018.

[5] P. Benioff. Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics*, 29:515–546, 11 1982.

[6] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[7] A. Bertoni and M. Carpentieri. Analogies and differences between quantum and stochastic automata. *Theoretical Computer Science*, 262(1):69–81, 2001.

[8] A. Bertoni and M. Carpentieri. Regular languages accepted by quantum automata. *Information and Computation*, 165(2):174–182, 2001.

[9] A. Brodsky and B. Pippenger. Characterizations of 1-way quantum finite automata. *SIAM Journal on Computing*, 31, 04 1999.

[10] A. C. Cem Say and A. Yakaryılmaz. Quantum finite automata: A modern introduction. In C. S. Calude, R. Freivalds, and I. Kazuo, editors, *Computing with New Resources*, pages 208–222. Springer, 2014.

[11] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London Series A*, 400(1818):97–117, July 1985.

[12] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences*, 439:553 – 558, 1992.

[13] R. P. Feynman. Simulating physics with computers. *International journal of theoretical physics*, 21(6/7):467–488, 1982.

[14] L. K. Grover. A fast quantum mechanical algorithm for database search. In *28th Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219. ACM Press, 1996.

[15] J. Gruska. *Quantum Computing*. McGraw-Hill, 1999.

[16] J. Hopcroft and J. Ullman. *Introduction to Automata Theory, Languages and Computation*. Addison-Wesley, 1979.

[17] A. Kondacs and J. Watrous. On the power of quantum finite state automata. In *38th Annual Symposium on Foundations of Computer Science, FOCS'97*, pages 66–75. IEEE, 1997.

[18] C. Moore and J. Crutchfield. Quantum automata and quantum grammars. *Theoretical Computer Science*, 237:275–306, 04 2000.

[19] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *40th Annual Symposium on Foundations of Computer Science, FOCS'99*, pages 369–376. IEEE, 1999.

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

[21] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, FOCS'94*, pages 124–134. IEEE, 1994.

[22] A. Shur and A. Yakaryılmaz. Quantum, stochastic, and pseudo stochastic languages with few states. In *13th Int. Conf. on Unconventional Computation and Natural Computation, UCNC'14. LNCS 8553*, pages 327–339. Springer, 2014.

[23] P. Turakainen. On stochastic languages. *Information and Control*, 12(4):304–313, 1968.

[24] A. Yakaryılmaz and A. C. Cem Say. Efficient probability amplification in two-way quantum finite automata. *Theor. Comput. Sci.*, 410:1932–1941, 05 2009.

[25] A. Yakaryılmaz and A. C. Cem Say. Languages recognized with unbounded error by quantum finite automata. In A. Frid, A. Morozov, A. Rybalchenko, and K. W. Wagner, editors, *Computer Science - Theory and Applications*, pages 356–367, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

Apéndice A

Pruebas de algunos resultados auxiliares

En este apéndice presentamos las pruebas de algunos lemas que hemos utilizado en el capítulo 3.

Lema 3.9.1 Dados dos vectores $v, v' \in \mathfrak{B}$ y $w \in \Sigma^*$, existe una constante c tal que $\|T_w v - T_w v'\|_u \leq c \|v - v'\|_u$.

Demostración. Sean los vectores

$$v = (|\psi\rangle, p_{acc}, p_{rej}), v' = (|\psi'\rangle, p'_{acc}, p'_{rej}) \in \mathfrak{B}$$

Para un símbolo $\sigma \in \Sigma$, tenemos que

$$\begin{aligned}
\|T_\sigma v - T_\sigma v'\|_u &= \frac{1}{2}(\|P_{non}U_\sigma |\psi\rangle - P_{non}U_\sigma |\psi'\rangle\| + |p_{acc} + \|P_{acc}U_\sigma |\psi\rangle\|^2 - p'_{acc} \\
&- \left\|P_{acc}U_\sigma |\psi\rangle'\right\|^2| + |p_{rej} + \|P_{rej}U_\sigma |\psi\rangle\|^2 - p'_{rej} - \left\|P_{rej}U_\sigma |\psi\rangle'\right\|^2|) \\
&\leq \frac{1}{2}(\|P_{non}\| \||\psi\rangle - |\psi'\rangle\| + |\|P_{acc}U_\sigma |\psi\rangle\|^2 - \|P_{acc}U_\sigma |\psi'\rangle\|^2| \\
&+ |\|P_{rej}U_\sigma |\psi\rangle\|^2 - \|P_{rej}U_\sigma |\psi'\rangle\|^2| + |p_{acc} - p'_{acc}| + |p_{rej} - p'_{rej}|) \\
&\leq \frac{1}{2}(\|P_{non}\| \||\psi\rangle - |\psi'\rangle\| + |(\|P_{acc}U_\sigma |\psi\rangle\| + \|P_{acc}U_\sigma |\psi'\rangle\|)(\|P_{acc}U_\sigma |\psi\rangle\| \\
&- \|P_{acc}U_\sigma |\psi'\rangle\|)| + |(\|P_{rej}U_\sigma |\psi\rangle\| + \|P_{rej}U_\sigma |\psi'\rangle\|)(\|P_{rej}U_\sigma |\psi\rangle\| \\
&- \|P_{rej}U_\sigma |\psi'\rangle\|)| + |p_{acc} - p'_{acc}| + |p_{rej} - p'_{rej}|) \\
&\overset{(1)}{\leq} \frac{1}{2}(\|P_{non}\| \||\psi\rangle - |\psi'\rangle\| + 4\|P_{acc}\| \|\|P_{acc}U_\sigma |\psi\rangle\| - \|P_{acc}U_\sigma |\psi'\rangle\|| \\
&+ 4\|P_{rej}\| \|\|P_{rej}U_\sigma |\psi\rangle\| - \|P_{rej}U_\sigma |\psi'\rangle\|| + |p_{acc} - p'_{acc}| + |p_{rej} - p'_{rej}|) \\
&\leq \frac{1}{2}(\|P_{non}\| \||\psi\rangle - |\psi'\rangle\| + 4\|P_{acc}\| \|\|P_{acc}U_\sigma |\psi\rangle - P_{acc}U_\sigma |\psi'\rangle\|| \\
&+ 4\|P_{rej}\| \|\|P_{rej}U_\sigma |\psi\rangle - P_{rej}U_\sigma |\psi'\rangle\|| + |p_{acc} - p'_{acc}| + |p_{rej} - p'_{rej}|) \\
&\leq \frac{1}{2}((\|P_{non}\| + 4\|P_{acc}\|^2 + 4\|P_{rej}\|^2) \||\psi\rangle - |\psi'\rangle\| + |p_{acc} - p'_{acc}| \\
&+ |p_{rej} - p'_{rej}|)
\end{aligned}$$

Para la desigualdad (1) se han empleado las propiedades de la norma y que $\||\psi\rangle\|, \||\psi'\rangle\| \leq 2$. Ahora, si consideramos el valor $c_\sigma = \text{máx}\{(\|P_{non}\| + 4\|P_{acc}\|^2 + 4\|P_{rej}\|^2), 1\}$, se verifica

$$\|T_\sigma v - T_\sigma v'\|_u \leq c_\sigma \|v - v'\|_u$$

Por último, si para una palabra $w = \sigma_1 \cdots \sigma_n \in \Sigma^*$ consideramos el valor $c = \prod_{i=1}^{n} c_{\sigma_i}$, obtenemos el resultado del enunciado. □

Lema 3.9.2 Si tenemos un conjunto $A \subseteq \mathfrak{B}$ que verifica que existe un $\epsilon > 0$ tal que para todo $v, v' \in A$ se cumple $\|v - v'\|_u > \epsilon$, entonces A es finito:

Demostración. En primer lugar, es fácil ver que las métricas dadas por las normas $\|\cdot\|_u$ y $\|\cdot\|$ son equivalentes. Si tenemos un vector $v = (|\psi\rangle, p_{acc}, p_{rej}) \in \mathbb{C}^{n+2}$, vemos que

$$\|v\| = \sqrt{\||\psi\rangle\|^2 + |p_{acc}|^2 + |p_{rej}|^2} \leq \sqrt{\||\psi\rangle\|^2} + \sqrt{|p_{acc}|^2} + \sqrt{|p_{rej}|^2} = \|v\|_u$$

Por otro lado, por la desigualdad de Cauchy-Schwarz se tiene que

$$\|v\|_u = \sqrt{\||\psi\rangle\|^2} + \sqrt{|p_{acc}|^2} + \sqrt{|p_{rej}|^2} \leq \sqrt{1+1+1}\sqrt{\||\psi\rangle\|^2 + |p_{acc}|^2 + |p_{rej}|^2} = \sqrt{3}\,\|v\|$$

Por tanto, las dos normas inducen la misma topología. Ahora, como $\|v\| \leq \|v\|_u$, se cumple $\mathfrak{B} \subset \overline{B(0,1)}$ donde $\overline{B(0,1)}$ es la bola cerrada de radio 1 con la distancia inducida por la norma $\|\cdot\|$. Sabemos que $\overline{B(0,1)}$ es un conjunto compacto en $\mathbb{C}^{n+2}$. Veamos ahora que A también es cerrado. Supongamos ahora que tenemos un conjunto infinito A que verifica la condición del enunciado. Este conjunto es cerrado. Veámoslo:

Sea un punto $x \notin A$. Existen dos opciones:

- Si no existe ningún $a \in A$ tal que $\|x - a\|_u < \epsilon$, entonces podemos tomar la bola $B_u(x, \epsilon) \subset \mathbb{C}^{n+2} \setminus A$.
- Si existe algún $a \in A$ tal que $\|x - a\|_u < \epsilon$, entonces podemos tomar un valor $r = \min\{\|x - a\|_u, d(x, \partial B_u(a, \epsilon))_u\}$ y considerar la bola $B_u(x, \frac{r}{2}) \subset \mathbb{C}^{n+2} \setminus A$.

Tenemos, por tanto, que A es un conjunto cerrado dentro de un compacto, por lo que es también compacto. Entonces, podemos recubrir A con un conjunto de bolas $B_u(v, \epsilon)$ del que no se puede obtener un subrecubrimiento finito pues cada $v \in A$ está cubierto por una única bola $B_u(v, \epsilon)$. Sin embargo, esto no es posible ya que A es compacto. Por tanto, A ha de ser finito. □

La siguiente demostración está tomada de [15].

Lema 3.9.3 Sean $|u\rangle, |v\rangle$ dos vectores, A un operador lineal, $0 < \epsilon < 1$, $\mu > 0$, $\|A(u - v)\| < \epsilon$ y $\|u\|, \|v\|, \|Au\|, \|Av\| \in [\mu, \mu + \epsilon]$. Entonces $\exists c$ tal que $\|u - v\| < c\epsilon^{1/4}$

Demostración. En primer lugar, calculamos la expresión

$$\begin{aligned}\|u - v\|^2 - \|A(u - v)\|^2 &= \langle u - v \mid u - v\rangle - \langle Au - Av \mid Au - Av\rangle \\ &= \|u\|^2 + \|v\|^2 - \langle u \mid v\rangle - \langle v \mid u\rangle \\ &\quad - \|Au\|^2 - \|Av\|^2 + \langle Au \mid Av\rangle + \langle Av \mid Au\rangle\end{aligned}$$

Como $\|u\|, \|Au\| \in [\mu, \mu + \epsilon]$, tenemos

$$\|u\|^2 - \|Au\|^2 \leq (\mu + \epsilon)^2 - \mu^2 = \mu^2 + \epsilon^2 + 2\mu\epsilon - \mu^2 = \epsilon^2 + 2\mu\epsilon$$

Análogamente, $\|v\|^2 - \|Av\|^2 \leq \epsilon^2 + 2\mu\epsilon$. Por otra parte, tenemos

$$\begin{aligned}\left\|A^\dagger Au - u\right\|^2 &\leq \left\|A^\dagger Au\right\|^2 + \|u\|^2 - 2\,\|Au\|^2 \\ &\leq \|u\|^2 - \|Au\|^2 \leq \epsilon^2 + 2\mu\epsilon\end{aligned}$$

Entonces

$$\langle v \mid A^\dagger Au - u\rangle \leq \|v\| \left\|A^\dagger Au - u\right\| \leq (\mu + \epsilon)\sqrt{\epsilon^2 + 2\mu\epsilon}$$

Esto es análogo para $\langle u \mid A^\dagger Av - v\rangle$. Tenemos entonces

$$\|u - v\|^2 - \|A(u - v)\|^2 \leq \sqrt{\epsilon}(2(2\sqrt{\epsilon}\mu + \epsilon 3/2) + 2(\mu + \epsilon)\sqrt{\epsilon + 2\mu})$$

Si ahora tomamos $c' > 2(2\sqrt{\epsilon}\mu + \epsilon 3/2) + 2(\mu + \epsilon)\sqrt{\epsilon + 2\mu}$, tenemos

$$\|u - v\|^2 < \|A(u - v)\|^2 + c'\sqrt{\epsilon}$$

Por tanto,

$$\begin{aligned}\|u - v\| &< \sqrt{\|A(u - v)\|^2 + c'\sqrt{\epsilon}} < \sqrt{\epsilon^2 + c'\sqrt{\epsilon}} \\ &= \sqrt{\epsilon^{1/2}(\epsilon^{3/2} + c')} \leq \sqrt{c' + 1}\epsilon^{1/4}\end{aligned}$$

□

La siguiente demostración está tomada de [7].

Lema 3.9.4 Si U es una matriz unitaria de orden m, entonces para cualquier $\varepsilon > 0$ existe un $k \in \mathbb{N}$ tal que $\left\|I_m - U^k\right\| \leq \varepsilon$. Por tanto, si tenemos un vector $|\psi\rangle$ que verifique $\||\psi\rangle\|^2 \leq 1$, para todo $\varepsilon > 0$ existe un $k \in \mathbb{N}$ tal que $\left\|(I_m - U^k)\,|\psi\rangle\right\| < \varepsilon$.

Demostración. Con la norma matricial inducida por la norma vectorial, es posible trabajar con el espacio vectorial de las matrices de orden m. En este espacio, el conjunto de las matrices unitarias es un conjunto compacto. Así, dada una matriz unitaria U toda sucesión $\{U^n\}_{n\in\mathbb{N}}$ en este conjunto posee una subsucesión de Cauchy $\{U^{n_p}\}_{p\in\mathbb{N}}$. En ese caso, para cualquier $\varepsilon > 0$ existe un $l \in \mathbb{N}$ tal que para todo $n_{p_1}, n_{p_2} > l$ se tiene que

$$\|U^{n_{p_2}} - U^{n_{p_1}}\| \leq \varepsilon$$

Tomando dos valores fijos $n_{p_2} > n_{p_1} > l$ y un valor $k = n_{p_2} - n_{p_1}$, tenemos

$$\begin{aligned}\left\|I_m - U^k\right\| &= \left\|U^{-n_{p_1}}U^{n_{p_1}} - U^{-n_{p_1}}U^{n_{p_1}+k}\right\| \\ &= \left\|U^{-n_{p_1}}(U^{n_{p_1}} - U^{n_{p_1}+k})\right\| = \left\|U^{n_{p_1}} - U^{n_{p_2}+k}\right\| \leq \varepsilon\end{aligned}$$

Ahora, si tenemos que el vector $|\psi\rangle$ con $\||\psi\rangle\| \leq 1$ y y un valor $\varepsilon > 0$ sabemos que para cualquier $\varepsilon' < \varepsilon$ existe un $k \in \mathbb{N}$ tal que

$$\left\|(I_m - U^k)\,|\psi\rangle\right\| \leq \left\|(I_m - U^k)\right\| \||\psi\rangle\| \leq \left\|(I_m - U^k)\right\| \leq \varepsilon' < \varepsilon$$

□

La siguiente demostración está tomada de [6].

Lema 3.9.5 Sean dos vectores unitarios $|\psi\rangle, |\phi\rangle \in \mathbb{C}^n$ tales que $\||\psi\rangle - |\phi\rangle\| < \epsilon$ para $\epsilon \in (0, 2]$. La distancia total entre las distribuciones de probabilidad obtenidas tras medir $|\psi\rangle$ y $|\phi\rangle$ es, a lo sumo, 4ϵ.

Demostración. Sean los vectores $|\psi\rangle = \sum_{i=1}^{n} \alpha_i |i\rangle$ y $|\phi\rangle = \sum_{i=1}^{n} \beta_i |i\rangle$ y $|\varphi\rangle = |\psi\rangle - |\phi\rangle = \sum_{i=1}^{n} (\alpha_i - \beta_i) |i\rangle = \sum_{i=1}^{n} \gamma_i |i\rangle$. La probabilidad de observar el estado $|i\rangle$ al realizar una medición en la base computacional es $|\alpha_i|^2$ en el caso de $|\psi\rangle$ y $|\beta_i|^2$ en el caso de $|\phi\rangle$. Esta última probabilidad se puede expresar como

$$|\beta_i|^2 = \beta_i^* \beta_i = (\alpha_i + \gamma_i)^* (\alpha_i + \gamma_i) = |\alpha_i|^2 + |\gamma_i|^2 + \alpha_i \gamma_i^* + \alpha_i^* \gamma_i$$

Entonces, la diferencia entre ambas distribuciones es

$$\begin{aligned} \sum_{i=1}^{n} ||\alpha_i|^2 - |\beta_i|^2| &\leq \sum_{i=1}^{n} |\gamma_i|^2 + |\alpha_i \gamma_i^*| + |\alpha_i^* \gamma_i| \leq \||\varphi\rangle\|^2 + \langle\varphi|\psi\rangle + \langle\psi|\varphi\rangle \\ &< \epsilon^2 + 2 \||\psi\rangle\| \, \||\varphi\rangle\| \leq \epsilon^2 + 2\epsilon \leq 2\epsilon + 2\epsilon = 4\epsilon \end{aligned}$$

□