INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE FÍSICA Y MATEMÁTICAS

Servicio Social

Apuntes sobre:

Introducción a Computo Cuántico

Juan Carlos Jiménez Cervantes

Director del proyecto:
Dr. Egor Maximenko

Ciudad de México, 2025

Índice

1. Introducción

Historia

Principios de la computación cuántica. En 1982, Richard Feynman observó que era imposible simular sistemas cuánticos de manera eficiente en computadoras clásicas. Tres años después, el físico británico David Deutsch estableció los fundamentos del modelo de computación cuántica actual en su revolucionario artículo titulado "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer". Este modelo generalizó la máquina de Turing clásica, permitiendo que operara de acuerdo con los principios de la mecánica cuántica. Además, Deutsch demostró cómo una computadora cuántica puede realizar múltiples cálculos simultáneamente gracias a la superposición de estados, lo que representa una ventaja categórica frente a las computadoras clásicas.

Objetivo

El objetivo principal de estos apuntes es desarrollar un marco conceptual claro y didáctico que permita comprender la estructura matemática sobre la cual se fundamenta la computación cuántica. Este marco busca ser accesible para estudiantes de matemáticas interesados en adentrarse en esta área. Presentamos los fundamentos matemáticos para el estudio de la computación cuántica, incluyendo herramientas de álgebra lineal y transformaciones de Fourier.

2. Preliminares de álgebra lineal

2.1. Espacio vectorial $\mathbb{C}^n$, producto interno y Notación de Dirac

Definimos el conjunto de índices $I_n \coloneqq \{j \in \mathbb{N} \mid 0 \leq j < n\}$ que también denotamos por $[\![0, n[\![$. Dado un número natural fijo n, consideramos el conjunto $\mathbb{C}^n$, definido como

$$\mathbb{C}^n \coloneqq \{z : I_n \to \mathbb{C} \mid z_j \coloneqq z(j) \in \mathbb{C} \text{ para todo } j \in I_n\}.$$

Junto con la adición y la multiplicación escalar, definidas componente por componente, $\mathbb{C}^n$ constituye un espacio vectorial complejo de dimensión n. El producto interno en $\mathbb{C}^n$ es una función $\langle \cdot, \cdot \rangle : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$, que satisface las siguientes propiedades para cualesquiera $u, v, w \in \mathbb{C}^n$ y cualquier $\lambda \in \mathbb{C}$:

- $\langle \lambda u + v, w \rangle = \lambda \langle u, w \rangle + \langle v, w \rangle$,

- $\langle u, v\rangle = \overline{\langle v, u\rangle}$,
- $\langle u, u\rangle \geq 0$ y $\langle u, u\rangle = 0$, si y sólo si, $u = 0$.

Si $u = (u_0, \ldots, u_{n-1})$ y $v = (v_0, \ldots, v_{n-1})$, definimos su producto interno como

$$\langle u, v\rangle \coloneqq \sum_{j=0}^{n-1} \overline{v}_j u_j = v^* u,$$

donde v^* denota el transpuesto conjugado de v. Asimismo, es útil llamar el **producto exterior** de u por v al producto uv^*. La expresión de las entradas de esta matriz es

$$(uv^*)_{j,k} = u_j \overline{v_k}. \tag{1}$$

Observación 2.1. Como se mencionó previamente, este texto está dirigido a matemáticos, y la notación introducida para el producto interno es común en esta disciplina. En este contexto, el producto interno se caracteriza por ser lineal (es decir, aditivo y homogéneo) en la primera entrada, y lineal conjugado (o antilineal) en la segunda. Sin embargo, para ciertos resultados e identidades, también emplearemos la notación de Dirac utilizada en mecánica cuántica. A continuación, se detalla la correspondencia entre ambas notaciones:

Notación matemática	Equiv. en Notación de Dirac
$u \in \mathbb{C}^n$	$\lvert u\rangle \in \mathbb{C}^n$
u^*	$\langle u\rvert$
$\langle u, v\rangle = v^* u$	$\langle v \vert u\rangle \coloneqq \langle v\rvert \lvert u\rangle$
uv^*	$\lvert u\rangle \langle v\rvert$

2.2. Producto de Kronecker

Definición 2.2 (Producto de Kronecker de vectores)**.** Sean $m, n \in \mathbb{N}$ y sean $a \in \mathbb{C}^m, b \in \mathbb{C}^n$ elementos de espacios vectoriales (posiblemente de distinta dimensión). Definimos el **producto de Kronecker** de a por b como

$$(a \otimes b)_{nx+r} = a_x b_r,$$

donde $x \in [\![0, m[\![$ y $r \in [\![0, n[\![$. De la definicón se sigue que $a \otimes b \in \mathbb{C}^{mn}$.

Definición 2.3. Sea m en $\mathbb{N}$, los vectores de la base canónica de $\mathbb{C}^m$ se definen por

$$e_x \coloneqq [\delta_{x,j}]_{j=0}^{m-1}$$

Lema 2.4. *Sean m, n en $\mathbb{N}$. Entoces, la función $h : [\![0, m[\![\times [\![0, n[\![\to [\![0, mn[\![$ definida por*

$$h(x, r) \coloneqq nx + r.$$

es biyectiva.

Demostración. Sean x, y en $[\![0, m[\![$ y r, s en $[\![0, n[\![$ y sin perdida de generalidad, supongamos que $r \leq s$ tal que $h(x, r) = nx + r = ny + s = h(y, s)$. Entonces,

$$0 \leq s - r = n(x - y) < n.$$

Por lo tanto, $(x, r) = (y, s)$ y luego h es inyectiva. Ahora, para z en $[\![0, mn[\![$, tomamos $x \coloneqq \left\lfloor \frac{z}{n} \right\rfloor$ y $r \coloneqq z - xn$. Es claro que h es suprayectiva y, así pues, es biyectiva. □

Proposición 2.5. *Sean m, n en $\mathbb{N}$, sea x en $[\![0, m[\![$ y sea r en $[\![0, n[\![$. Consideramos los vectores canónicos $e_x \in \mathbb{C}^m, e_r \in \mathbb{C}^n$. Entonces,*

$$e_x \otimes e_r \coloneqq e_{nx+r} \in \mathbb{C}^{mn}.$$

Demostración. De la definición del producto de Kronecker y del resultado del lema 2.4 se sigue que

$$(e_x \otimes e_r)_{nj+k} = (e_x)_j (e_r)_k = \delta_{x,j}\delta_{r,k} = \delta_{nx+r,nj+k} = (e_{nx+r})_{nj+k}.$$

□

Generalizamos la definición del **producto de Kronecker** a matrices.

Definición 2.6 (Producto de Kronecker de matrices)**.** Sean A en $\mathcal{M}_{p,q}(\mathbb{C})$ y B en $\mathcal{M}_{m,n}(\mathbb{C})$. Definimos su producto de Kronecker como la matriz de clase $\mathcal{M}_{pm,qn}(\mathbb{C})$:

$$(A \otimes B)^{nk_1+k_2}_{mj_1+j_2} \coloneqq A^{k_1}_{j_1} B^{k_2}_{j_2}.$$

Ejemplo 2.7. Sean

$$A = \begin{bmatrix} 3 & 1 \\ -2 & 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 2 & 4 & 1 \\ -1 & 0 & 3 \end{bmatrix},$$

el producto de Kronecker de estas dos matrices es el siguiente:

$$A \otimes B = \begin{bmatrix} 6 & 12 & 3 & 2 & 4 & 1 \\ -3 & 0 & 9 & -1 & 0 & 3 \\ -4 & -8 & -2 & 0 & 0 & 0 \\ 2 & 0 & -6 & 0 & 0 & 0 \end{bmatrix}.$$

Observemos que el producto de Kronecker es una función

$$\otimes : \mathcal{M}_{p,q}(\mathbb{C}) \times \mathcal{M}_{m,n}(\mathbb{C}) \to \mathcal{M}_{pm,qn}(\mathbb{C}).$$

Proposición 2.8 (Producto de Kronecker de productos exteriores)**.** *Sean m, n en $\mathbb{N}$ y sean a en $\mathbb{C}^m$, b en $\mathbb{C}^n$. Entonces,*

$$(ab^*) \otimes (cd^*) = (a \otimes c)(b \otimes d)^*.$$

Demostración. De la defición anterior, del producto exterior de vectores (1) y de la definición del producto de Kronecker de vectores se tiene que

$$\begin{aligned}((ab^*) \otimes (cd^*))^{nk_1+k_2}_{mj_1+j_2} &= (ab^*)^{k_1}_{j_1}(cd^*)^{k_2}_{j_2} = (a_{j_1}b^*_{k_1})(c_{j_2}d^*_{k_2}) \\ &= (a_{j_1}c_{j_2})(b^*_{k_1}d^*_{k_2}) = (a \otimes c)_{mj_1+j_2}(b \otimes d)^*_{nk_1+k_2}.\end{aligned}$$

□

Denotando por $E^y_x \coloneqq e_x e^*_y$ el producto exterior de vectores canónicos (posiblemente de distinta dimensión) tenemos el siguiente resultado útil.

Proposición 2.9. *Sean x, r, y, s en $\mathbb{N}$, tal que x en $[\![0, m[\![$, $r \in [\![0, m[\![$ y y, s en $[\![0, n[\![$.*

$$E^y_x \otimes E^s_r = E^{ny+s}_{mx+r}.$$

Demostración. Usando las proposiciones 2.5 y 2.8 tenemos que

$$E^y_x \otimes E^s_r = (e_x e^*_y) \otimes (e_r e^*_s) = (e_x \otimes e_r)(e_y \otimes e_s)^* = (e_{mx+r})(e_{ny+s})^* = E^{ny+s}_{mx+r}.$$

□

Proposición 2.10. *Sean $a, c \in \mathbb{C}^m$ y $b, d \in \mathbb{C}^n$, entonces se cumple que*

$$\langle a \otimes b | c \otimes d \rangle = \langle a|c\rangle\langle b|d\rangle.$$

Demostración. Por definición del producto interno, producto de Kronecker en vectores y el lema 2.4 tenemos que

$$\begin{aligned}\langle a \otimes b | c \otimes d \rangle &= \sum_{j=0}^{mn-1} (a \otimes b)_j (c \otimes d)^*_j \\ &= \sum_{x=0}^{m-1}\sum_{r=0}^{n-1}(a_x b_r)(c^*_x d^*_r) = \left(\sum_{x=0}^{m-1} a_x c^*_x\right)\left(\sum_{r=0}^{n-1} b_r d^*_r\right) = \langle a|c\rangle\langle b|d\rangle.\end{aligned}$$

□

2.3. Algebra $\mathbb{C}^n$

Regresando al espacio vectorial complejo $\mathbb{C}^n$, definiendo una operación adicional sobre este conjunto, a saber, la *multiplicación por componentes*, que llamaremos simplemente multiplicación en $\mathbb{C}^n$.

Definición 2.11. Dados $a, b \in \mathbb{C}^n$ definimos a la operación $\odot : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}^n$ como:

$$a \odot b \coloneqq [a_j b_j]_{j=0}^{n-1}.$$

La operación $\odot$ es bilineal, por lo que $\mathbb{C}^n$ dotado de esta operación constituye un **álgebra** sobre los complejos. Además, la multiplicación en $\mathbb{C}^n$ es asociativa, conmutativa y posee un elemento identidad, definido como:

$$1_n \coloneqq [1]_{j=0}^{n-1}.$$

Proposición 2.12. *Un elemento $a = (a_0, \ldots, a_{n-1}) \in \mathbb{C}^n$ tiene inverso multiplicativo si y solo si $a_j \neq 0$, con $0 \leq j < n$. Así pues, denotemos por $\mathrm{Inv}(\mathbb{C}^n)$ a los elementos invertibles de la álgebra $\mathbb{C}^n$.*

Demostración. Claramente, si a_j es distinto de cero en todas las componentes y definiendo a^{-1} como $(a_1^{-1}, \ldots, a_{n-1}^{-1})$ tenemos que

$$a \odot a^{-1} = [a_j a_j^{-1}]_{j=0}^{n-1} = 1_n.$$

Por otro lado, supongamos que $a \in \mathrm{Inv}(\mathbb{C}^n)$, entonces existe $b \in \mathbb{C}^n$ tal que

$$a \odot b = [a_j b_j]_{j=0}^{n-1} = 1_n.$$

Por lo tanto, para toda j, a_j es distinto de cero. □

Definición 2.13. Le llamamos **espectro** de a elemento del álgebra $\mathbb{C}^n$ al siguiente conjunto:

$$\mathrm{sp}(a) \coloneqq \{\lambda \in \mathbb{C} \mid a - \lambda 1_n \notin \mathrm{Inv}(\mathbb{C}^n)\}.$$

2.4. Operadores hermitianos, unitarios, positivos y proyecciones

Definición 2.14. Sea $\mathcal{H}$ un espacio de Hilbert, y sea $A : \mathcal{H} \to \mathcal{H}$ un operador lineal. Decimos que A es **acotado** si

$$\exists\, C \geq 0, \quad \forall\, v \in \mathcal{H}, \quad \|Av\| \leq C\|v\|.$$

Definimos a $\mathcal{B}(H)$ como el conjunto de operadores lineales acotados en $\mathcal{H}$.

Teorema 2.15. *Sea $A \in \mathcal{B}(\mathcal{H})$. Entonces existe un único $A^* \in \mathcal{B}(\mathcal{H})$ tal que para todo $u, v \in \mathcal{H}$*

$$\langle u|Av\rangle = \langle A^*u|v\rangle\,.$$

El operador anterior A^* se llama **operador adjunto** de A. Cuando $A = A^*$, decimos que A es **hermitiano**.

Lema 2.16. *Sean $A \in \mathcal{M}_n(\mathbb{C})$, $U \in \mathrm{GL}_n(\mathbb{C})$ y $\lambda \in \mathbb{C}^n$ tal que $U = \begin{bmatrix} u_0 \dots u_{n-1} \end{bmatrix}$, donde $u_0, \dots, u_{n-1} \in \mathbb{C}^n$. Entonces $AU = U\,\mathrm{diag}(\lambda)$ si y solo si para todo k en $[\![0, n[\![$ se tiene que $Au_k = \lambda_k u_k$.*

Demostración. Es claro que AU y $U\,\mathrm{diag}(\lambda)$ son iguales si y solo si sus columnas son iguales. Así pues, observamos que dado k en $[\![0, n[\![$,

$$(AU)_{:,k} = Au_k, \qquad (U\,\mathrm{diag}(\lambda))_{:,k} = \lambda_k u_k.$$

Por lo tanto, las matrices coinciden si y solo si $Au_k = \lambda u_k$ para k en $[\![0, n[\![$. □

Proposición 2.17. *Sea $A \in \mathcal{M}_n(\mathbb{C})$. Entonces son equivalentes las siguientes:*

(i) Existen $U \in \mathcal{M}_n(\mathbb{C})$ matriz unitaria y $D \in \mathcal{M}_n(\mathbb{C})$ matriz diagonal tal que

$$U^{-1} A\, U = D. \tag{2}$$

(ii) Existen una base ordenada ortonormal $(\beta_0, \dots, \beta_{n-1})$ y un $\lambda \in \mathbb{C}^n$ tal que

$$A = \sum_{j=0}^{n-1} \lambda_j \beta_j \beta_j^*. \tag{3}$$

Demostración. (i) $\Longrightarrow$ (ii). Naturalmente, tomamos $\lambda \in C^n$ tal que $\mathrm{diag}(\lambda) = D$ y sea β_j la j-ésima columna de la matriz U. Dado que U es unitaria, $\langle \beta_j|\beta_k\rangle = \delta_{j,k}$ y por lo tanto la base ordenada $(\beta_0, \dots, \beta_{n-1})$ es ortonormal. Pasamos a mostrar (3) entrada por entrada considerando que $U = \begin{bmatrix} \beta_0 \dots \beta_{n-1} \end{bmatrix}$ y $U^{-1} = U^*$.

$$\begin{aligned}\left(UDU^{-1}\right)_{j,k} &= \sum_{r=0}^{n-1} (UD)_{j,r}\,(U^*)_{r,k} = \sum_{r=0}^{n-1} \left(\sum_{s=0}^{n-1} U_{j,s} D_{s,r}\right) \overline{U}_{k,r} \\ &= \sum_{r=0}^{n-1} \left(\sum_{s=0}^{n-1} (\beta_s)_j (\lambda_r \delta_{s,r})\right) \overline{(\beta_r)_k} = \sum_{r=0}^{n-1} \lambda_r (\beta_r)_j \overline{(\beta_r)_k}\end{aligned}$$

Dado que $(\beta_r)_j\overline{(\beta_r)_k} = (\beta_r\beta_r^*)_{j,k}$, tenemos

$$\left(UDU^{-1}\right)_{j,k} = \sum_{r=0}^{n-1} \lambda_r \left(\beta_r\beta_r^*\right)_{j,k} = \left(\sum_{r=0}^{n-1} \lambda_r\beta_r\beta_r^*\right)_{j,k}.$$

$(ii) \implies (i)$. Para cualquier k en $[\![0, n[\![$, obtenemos

$$A\beta_k = \left(\sum_{r=0}^{n-1} \lambda_j\beta_j\beta_j^*\right)\beta_k = \sum_{r=0}^{n-1} \lambda_j\beta_j\left(\beta_j^*\beta_k\right) = \sum_{r=0}^{n-1} \lambda_j\beta_j\delta_{j,k} = \lambda_k\beta_k.$$

Del lema anterior, con $U \coloneqq \left[\beta_0 \dots \beta_{n-1}\right]$, concluimos que $U^{-1}AU = \operatorname{diag}(\lambda)$. □

Cuando A cumple alguna de las propiedades anteriores decimos que es **unitariamente diagonalizable**. Usando la notación de computación cuántica, esto es, para $0 \leq j \leq n$ $|j\rangle \coloneqq \beta_j$, solemos escribir (3) como

$$A = \sum_{j=0}^{n-1} \lambda_j |j\rangle \langle j|. \tag{4}$$

Definición 2.18. Decimos que $A \in \mathcal{B}(\mathcal{H})$ es un **operador positivo** si para cualquier $u \in \mathcal{H}$ se tiene que $\langle u|Au\rangle$ es un número real no negativo.

Proposición 2.19. *Todo operador positivo es hermitiano.*

Demostración. Sea $A \in \mathcal{B}(\mathcal{H})$ un operador positivo y sea $u \in \mathcal{H}$. De (5), tenemos que

$$\begin{aligned} 0 \leq \alpha \coloneqq \langle u|Au\rangle &= \langle u|Bu\rangle + i\langle u|Cu\rangle = \overline{\langle u|Bu\rangle} + i\overline{\langle u|Cu\rangle}, \\ 2\alpha &= 2\operatorname{Re}(\langle u|Bu\rangle) + 2i\operatorname{Re}(\langle u|Cu\rangle). \end{aligned}$$

Lo anterior implica que $\operatorname{Re}(\langle u|Cu\rangle) = 0$. Más aún, tenemos que

$$0 = \langle u|Bu\rangle - \overline{\langle u|Bu\rangle} + i(\langle u|Cu\rangle - \overline{\langle u|Cu\rangle}) = 2i\operatorname{Im}(\langle u|Bu\rangle) - 2\operatorname{Im}(\langle u|Cu\rangle).$$

Así pues, $\operatorname{Im}(\langle u|Cu\rangle) = 0$, luego $C = 0$ y de la definición de C en (5) concluimos que $A = A^*$. □

Ejercicios

Ejercicio 2.20. Dado $A \in \mathcal{B}(\mathcal{H})$ existen $B, C \in \mathcal{B}(\mathcal{H})$ operadores hermitianos tales que

$$A = B + iC. \tag{5}$$

Demostración. Definimos $B \coloneqq (A + A^*)/2, C \coloneqq (A - A^*)/2i$. Es fácil verificar que B y C cumplen 5. Más aún, B y C son hermitianos. En efecto,

$$B^* = (1/2)(A + A^*)^* = (1/2)(A^* + A) = B,$$
$$C^* = (-1/2i)(A - A^*)^* = (-1/2i)(A^* - A) = C.$$

□

Ejercicio 2.21. Sean $A, B \in \mathcal{B}(H)$. Si el conmutador $[A, B] = 0$, el anticonmutador $\{A, B\} = 0$ y A es invertible, entonces $B = 0$.

Demostración. Por suposición,

$$[A, B] = AB - BA = 0 = AB + BA = \{A, B\}.$$

Luego, tenemos que $2BA = 0$ y operando por la derecha por A^{-1} concluimos que $0 = 2B(AA^{-1}) = 2B$. Por lo tanto, B debe ser el operador 0. □

Para un sencillo contraejemplo en el caso de un operador A no invertible consideremos

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \; B = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

Ejercicio 2.22. Sean $A, B \in \mathcal{B}(H)$ operadores hermitianos. Entonces $i[A, B]$ tambien es hermitiano.

Demostración. Recordamos las siguientes propiedades del operador adjunto:

$$(A + B)^* = A^* + B^*,$$
$$(AB)^* = B^* A^*,$$
$$(\lambda A)^* = \bar{\lambda} A^*.$$

Así pues, dado que $A^* = A$ y $B^* = B$ vemos que

$$(i[A, B])^* = -i(AB - BA)^* = -i(B^* A^* - A^* B^*) = i(AB - BA) = i[A, B].$$

□

3. Preliminares de computación cuántica

Uno de los muchos retos de la computación cuántica es el replantamiento de todos los avances e invenciones que se han hecho en más de tres cuarto de siglo en las ciencias de la computación y extrapolarlos a una arquitectura y paradigma diferente. Esto implica que el área sea, al menos, tan vasta como el de las ciencias de la computación.

Teorema 3.1. *Teorema de no clonación. Sea $s \in S(\mathbb{C}^2)$. No existe un operador unitario $U \in \mathcal{U}(\mathbb{C}^2)$ tal que, para todo $v \in S(\mathbb{C}^2)$, se cumpla*

$$U(v \otimes s) = v \otimes v.$$

Demostración. Sean $v, w \in S(\mathbb{C}^2)$ y supongamos que existe un operador unitario U tal que

$$U(v \otimes s) = v \otimes v, \tag{6}$$
$$U(w \otimes s) = w \otimes w. \tag{7}$$

De acuerdo con la definición en 2.10, y dado que U es unitario, se tiene que

$$\begin{aligned}\langle v|w\rangle &= \langle v|w\rangle \langle s|s\rangle = \langle v \otimes s|w \otimes s\rangle \\ &= \langle U(v \otimes s)|U(w \otimes s)\rangle = \langle v \otimes v|w \otimes w\rangle = \langle v|w\rangle^2 .\end{aligned}$$

Lo anterior implica que $\langle v|w\rangle$ es igual a 0 o 1. Por lo tanto, el operador U que cumple las ecuaciones (2.1) y (2.2) solo lo hace si $v \perp w$ o $v \sim w$. □

En particular, continuando con la demostración anterior, se seguiría que

$$\begin{aligned}U(-v \otimes s) = (-v \otimes -v) = v \otimes v = U(v \otimes s),\\ U(iv \otimes s) = iv \otimes iv = -(v \otimes v) = -U(v \otimes s).\end{aligned}$$

Es decir, en cualquiera de los dos casos se obtiene una contradicción.

3.1. Esfera de Bloch

Plano proyectivo

Se estudia el espacio complejo proyectivo $\mathbb{P}(\mathbb{C})$, también denotado por $\mathbb{CP}^1$. En particular, se construye una biyección entre $\mathbb{CP}^1$ y la esfera unitaria $\mathbb{S}^2$ en $\mathbb{R}^3$, usando las coordenadas esféricas en $\mathbb{S}^2$.

Definición del espacio $\mathbb{P}(\mathbb{C})$

Denotemos por $\mathbf{0}$ al vector cero en $\mathbb{C}$.

Definición 3.2. En el espacio $\mathbb{C}^2 \setminus \{\mathbf{0}\}$ definimos una relación binaria $\sim$ mediante la siguiente regla:

$$a \sim b \qquad \Longleftrightarrow \qquad \exists\, \lambda \in \mathbb{C} \setminus \{0\} \qquad a = \lambda b.$$

Proposición 3.3. *$\sim$ es una relación de equivalencia.*

Demostración. La relación es trivialmente *reflexiva* tomando $\lambda = 1$. Si $a \sim b$ entonces $a = \lambda b$ para algún $\lambda \neq 0$, luego $b = \lambda^{-1} a$ por lo que la relación es *simétrica*. Finalmente, si $a = \lambda_1 b$ y $b = \lambda_2 c$ (es decir, $a \sim b$ y $b \sim c$) entonces $a = \lambda_1 \lambda_2 c$ y así es *transitiva*. □

Definición 3.4. Para cada punto a en $\mathbb{C}^2 \setminus \{\mathbf{0}\}$, denotemos por $[a]$ a su clase de equivalencia respecto $\sim$:

$$[a] \coloneqq \Big\{ b \in \mathbb{C}^2 \setminus \{\mathbf{0}\} \colon\ b \sim a \Big\}.$$

Denotemos por $\mathbb{P}(\mathbb{C})$ al conjunto de estas clases de equivalencia, a este nuevo conjunto se le conoce como **espacio complejo proyectivo** de dimensión 1.

Parametrización del espacio $\mathbb{P}(\mathbb{C})$

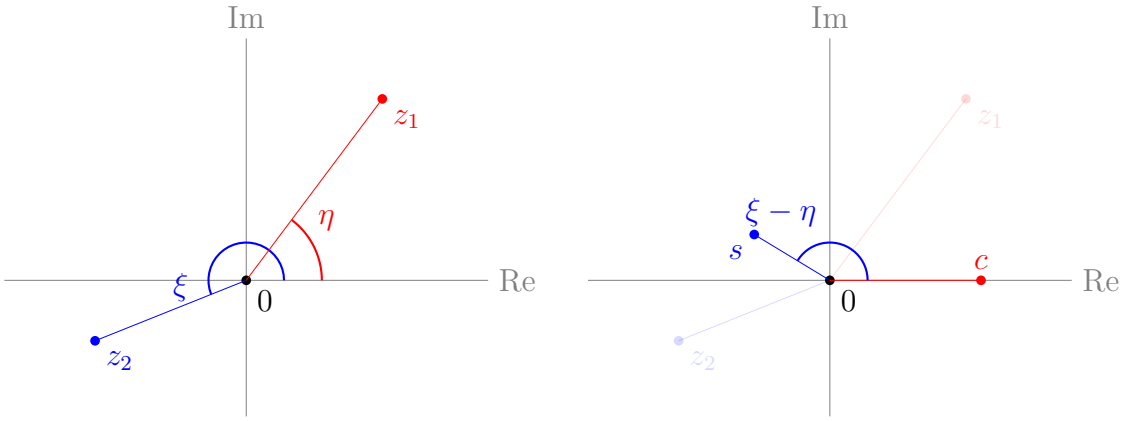
Proposición 3.5. *Para cada (z_1, z_2) en $\mathbb{C}^2 \setminus \{\mathbf{0}\}$, existen ϑ en $[0, \pi]$ y φ en $[0, 2\pi)$ tales que*

$$(z_1, z_2) \sim \left(\cos(\vartheta/2), \operatorname{sen}(\vartheta/2)\ \mathrm{e}^{\mathrm{i}\varphi} \right). \tag{8}$$

Demostración. Sean $z_1 = r_1 e^{i\eta}, z_2 = r_2 e^{i\xi} \in \mathbb{C}$ tal que alguno de los módulos r_1, r_2 es distinto de cero. Luego, factorizando $\lambda \coloneqq \sqrt{r_1^2 + r_2^2}\, e^{i\eta}$ tenemos

$$(z_1, z_2) = \sqrt{r_1^2 + r_2^2}\, e^{i\eta} \left(\frac{r_1}{\sqrt{r_1^2 + r_2^2}}, \frac{r_2}{\sqrt{r_1^2 + r_2^2}} e^{i(\xi - \eta)} \right) = \lambda (c, s e^{i\varphi}) \sim (c, s e^{i\varphi}).$$

En la derecha tenemos un nuevo par complejo con c y s números reales en [0,1], donde se cumple que $c^2 + s^2 = 1$, y si $\varphi \coloneqq \xi - \eta \mod 2\pi$, entonces $\varphi \in [0, 2\pi)$.



Finalmente, existe $\vartheta \in [0, \pi]$ tal que $c = \cos(\vartheta/2), s = \operatorname{sen}(\vartheta/2)$ y nos queda (8). □

Definición 3.6. Definimos $f\colon [0,\pi] \times [0, 2\pi) \to \mathbb{P}(\mathbb{C})$ mediante la siguiente regla:

$$f(\vartheta, \varphi) := \left(\cos(\vartheta/2), \operatorname{sen}(\vartheta/2)\ \mathrm{e}^{\mathrm{i}\varphi}\right).$$

Debido a la proposición 3.5, la función f es sobre.

Proposición 3.7. *La función f no es inyectiva. En particular,*

$$f^{-1}\Big[[(1,0)]\Big] = \{0\} \times [0, 2\pi), \qquad f^{-1}\Big[[(0,1)]\Big] = \{\pi\} \times [0, 2\pi).$$

La restricción de f al conjunto $(0,\pi) \times [0, 2\pi)$ es una función inyectiva.

Demostración. En efecto, sean $\vartheta, \eta \in (0, \pi)$, $\varphi, \psi \in [0, 2\pi)$ tales que

$$\left(\cos(\vartheta/2), \operatorname{sen}(\vartheta/2)\, e^{i\varphi}\right) = \left(\cos(\eta/2), \operatorname{sen}(\eta/2)\, e^{i\psi}\right)$$

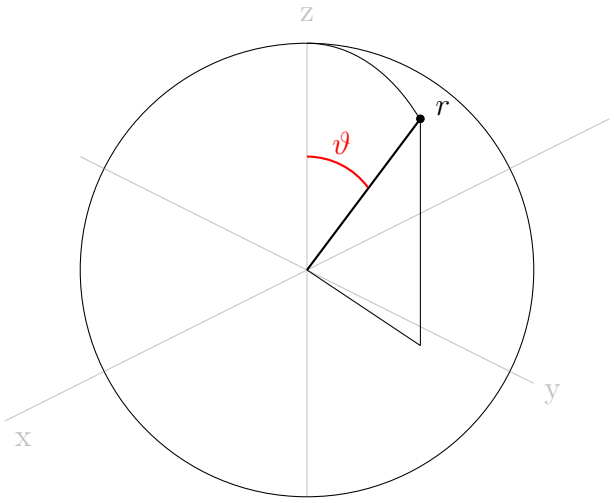
Luego $\cos(\vartheta/2) = \cos(\eta/2)$ y $\operatorname{sen}(\vartheta/2) = \operatorname{sen}(\eta/2)$. Como las funciones sen y cos son inyectivas en $(0, \pi/2)$ tenemos que $\vartheta = \eta$. Por último, dado que $\varphi, \psi \in [0, 2\pi)$ se debe tener que $\varphi = \psi$, por lo tanto f es inyectiva. □

Coordenadas esféricas en $\mathbb{S}^2$

Denotemos por $\mathbb{S}^2$ a la esfera unitaria en $\mathbb{R}^3$. Se sabe que cada punto de $\mathbb{S}^2$ se escribe en coordenadas esféricas como

$$\left(\operatorname{sen}\vartheta\ \cos\varphi,\ \operatorname{sen}\vartheta\ \operatorname{sen}\varphi,\ \cos\vartheta\right),$$

donde $\vartheta \in [0, \pi]$, $\varphi \in [0, 2\pi)$.



Definición 3.8. Definimos $g\colon [0,\pi]\times[0,2\pi)\to\mathbb{S}^2$ mediante la siguiente regla:

$$g(\vartheta,\varphi) \coloneqq \Big(\operatorname{sen}\vartheta\,\cos\varphi,\ \operatorname{sen}\vartheta\operatorname{sen}\varphi,\ \cos\vartheta\Big).$$

Se sabe que la función g es sobre.

Proposición 3.9. *La función g no es inyectiva. En particular,*

$$g^{-1}[(0,0,1)] = \{0\}\times[0,2\pi), \qquad g^{-1}[(0,0,-1)] = \{\pi\}\times[0,2\pi).$$

La restricción de g al conjunto $(0,\pi)\times[0,2\pi)$ es una función inyectiva.

Demostración. En efecto, sean $\vartheta,\eta\in(0,\pi)$ y $\varphi,\psi\in[0,2\pi)$ tales que

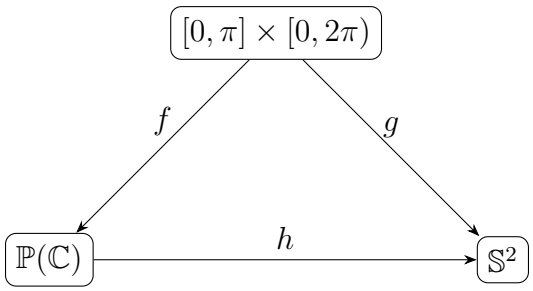
$$(\operatorname{sen}\vartheta\cos\varphi, \operatorname{sen}\vartheta\cos\varphi, \cos\vartheta) = (\operatorname{sen}\eta\cos\psi, \operatorname{sen}\eta\operatorname{sen}\psi, \cos\eta)\,.$$

En la tercera entrada, como la función coseno es inyectiva en $(0,\pi)$ tenemos que $\vartheta=\eta$. Luego tenemos que $\cos(\varphi)=\cos(\psi)$ y por la restricción en el intervalo concluimos que $\varphi=\psi$.

□

Correspondencia entre $\mathbb{P}(\mathbb{C})$ y $\mathbb{S}^2$

Queremos construir h tal que el siguiente diagrama sea conmutativo.



Usaremos el hecho que las funciones f y g, restringidas a $(0,\pi)\times[0,2\pi)$, son inyectivas, y consideraremos aparte los puntos excepcionales.

puntos de $\mathbb{P}(\mathbb{C})$	puntos de $[0,\pi]\times[0,2\pi)$	puntos de $\mathbb{S}^2$
$(1,0)$	$(\vartheta,\varphi)\in\{0\}\times[0,2\pi)$	$(0,0,1)$
$f(\vartheta,\varphi)\in\mathbb{P}(\mathbb{C})\setminus\{(1,0),(0,1)\}$;	$(\vartheta,\varphi)\in(0,\pi)\times[0,2\pi)$	$g(\vartheta,\varphi)\in\mathbb{S}^2\setminus\{(0,0,1),(0,0,-1)\}$
$(0,1)$	$(\vartheta,\varphi)\in\{\pi\}\times[0,2\pi)$	$(0,0,-1)$

Proposición 3.10. *Existe una única función $h\colon \mathbb{P}(\mathbb{C})\to\mathbb{S}^2$ tal que $h\circ f=g$. h es una biyección.*

Demostración. La proposición afirma que f es biyectiva en $E\coloneqq\mathbb{P}(C)\setminus\{(1,0),(0,1)\}$, y por lo tanto tiene una única inversa $f\big|_E^{-1}:\mathbb{P}\to(0,\pi)\times[0,2\pi)$. Se sigue que la siguiente función esta bien definida.

$$h((z_1,z_2))\coloneqq\begin{cases}(0,0,1), & (z_1,z_2)=(1,0),\\ (0,0,-1), & (z_1,z_2)=(0,1),\\ g\circ f_E\big|^{-1}(z_1,z_2), & (z_1,z_2)\in E.\end{cases}$$

Más aún, dado que $g\big|_E$ es biyectiva (3.9) tenemos que h es biyectiva en E y claramente lo es en $\mathbb{P}(\mathbb{C})$. □

Observación 3.11. En otras palabras, si

$$A=\left[\left(\cos(\vartheta/2),\ \operatorname{sen}(\vartheta/2)\ \mathrm{e}^{\mathrm{i}\varphi}\right)\right],$$

entonces

$$h(A)\coloneqq\Big(\operatorname{sen}\vartheta\cos\varphi,\operatorname{sen}\vartheta\cos\varphi,\cos\vartheta\Big).$$

3.2. Puertas Cuánticas

Los operadores unitarios preservan la norma del sistema, así pues, deben ser representados por matrices unitarias 2×2. Algunas de las más importantes son las puertas dadas por las **matrices de *Pauli***. así como la **puerta de *Hadamard*** (denotada como H), la **puerta de fase** (S) y la **puerta** $\frac{\pi}{8}$ (T).

Matrices de *Pauli*:

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \tag{9}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{10}$$

Definición 3.12 (Puerta de Hadamard)**.** Definimos la puerta de Hadamard como la siguiente matriz:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{11}$$

Ejemplo 3.13. Encontrar los eigenvectores, eigenvalores y la representación diagonal de las matrices de Pauli X, Y, Z.

$$\det(X - \lambda I) = \begin{vmatrix} -\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = \lambda^2 - 1, \tag{12}$$

$$\det(Y - \lambda I) = \begin{vmatrix} -\lambda & -i \\ i & -\lambda \end{vmatrix} = \lambda^2 - (-i^2) = \lambda^2 - 1, \tag{13}$$

$$\det(Z - \lambda I) = \begin{vmatrix} 1 - \lambda & 0 \\ 0 & -(1 + \lambda) \end{vmatrix} = \lambda^2 - 1. \tag{14}$$

Por lo tanto, todas las matrices de Pauli tienen eigenvalores $\lambda = \pm 1$.

Proposición 3.14. *La puerta de Hadamard es una matriz unitaria.*

Demostración. $z, w \in \mathbb{C}$, $z = (z_1, z_2)$ y $w = (w_1, w_2)$.

$$\langle z, w \rangle := z_1\overline{w_1} + z_2\overline{w_2}.$$

$$Hz = \frac{1}{\sqrt{2}}(z_1 + z_2, z_1 - z_2), Hw = \frac{1}{\sqrt{2}}(w_1 + w_2, w_1 - w_2).$$

Finalmente,

$$\begin{aligned} \langle H_z, H_w \rangle &= \frac{1}{2}\Big[(z_1 + z_2)\overline{(w_1 + w_2)} + (z_1 - z_2)\overline{(w_1 - w_2)}\Big] \\ &= \frac{1}{2}\Big[(z_1 + z_2)(\overline{w_1} + \overline{w_2}) + (z_1 - z_2)(\overline{w_1} - \overline{w_2})\Big] \\ &= z_1\overline{w_1} + z_2\overline{w_2}. \end{aligned}$$

Otra manera de demostrar que la matriz (11) es unitaria es verificar que $H^\dagger H = I$:

$$H^\dagger H = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

□

Ejercicio 3.15. Encontrar los eigenvalores, eigenvectores y representación diagonal de la compuerta de Hadamard.

Dado λ en $\mathbb{C}$,

$$\det(\lambda I_2 - H) = \begin{vmatrix}\lambda - \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}} & \lambda + \frac{1}{\sqrt{2}}\end{vmatrix} = \lambda^2 - 1.$$

Así pues, los eigenvalores son $\lambda_1 = 1, \lambda_2 = -1$. Calculamos los eigenvectores de λ_1 y λ_2, respectivamente,

$$\begin{bmatrix}1 - \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}} & 1 + \frac{1}{\sqrt{2}}\end{bmatrix} \sim \begin{bmatrix}\sqrt{2} - 1 & -1\\ -1 & \sqrt{2} + 1\end{bmatrix} \sim \begin{bmatrix}1 & -\sqrt{2} - 1\\ 0 & 0\end{bmatrix},$$

$$\begin{bmatrix}-1 - \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}} & -1 + \frac{1}{\sqrt{2}}\end{bmatrix} \sim \begin{bmatrix}\sqrt{2} + 1 & 1\\ -1 & 1 - \sqrt{2}\end{bmatrix} \sim \begin{bmatrix}1 & \sqrt{2} - 1\\ 0 & 0\end{bmatrix}.$$

Por lo tanto, los eigenvectores (normalizados) son

$$u_1 = \frac{1}{\sqrt{4 + 2\sqrt{2}}}\begin{pmatrix}1 + \sqrt{2}\\ 1\end{pmatrix}, \qquad u_2 = \frac{1}{\sqrt{4 - 2\sqrt{2}}}\begin{pmatrix}1 - \sqrt{2}\\ 1\end{pmatrix}.$$

Más aún, se verifica que la puerta de Hadamard es unitariamente diagonalizable (2) de lo siguiente:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}\frac{1+\sqrt{2}}{\sqrt{4+2\sqrt{2}}} & \frac{1}{\sqrt{4+2\sqrt{2}}}\\ \frac{1-\sqrt{2}}{\sqrt{4-2\sqrt{2}}} & \frac{1}{\sqrt{4-2\sqrt{2}}}\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}\frac{1+\sqrt{2}}{\sqrt{4+2\sqrt{2}}} & \frac{1-\sqrt{2}}{\sqrt{4-2\sqrt{2}}}\\ \frac{1}{\sqrt{4+2\sqrt{2}}} & \frac{1}{\sqrt{4-2\sqrt{2}}}\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}.$$

Ejercicio 3.16. Dado $n \in \mathbb{N}$. Demostrar que

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x,y=0}^{2^n-1}(-1)^{x\cdot y}\left|x\right\rangle\left\langle y\right|.$$

3.3. Desigualdad de Bell

En el modelo clásico, durante la etapa de experimentación, se realizan mediciones mediante aparatos que interactúan con el sistema físico en estudio. Uno de los principales desafíos es evitar alterar el sistema de tal forma que la medición obtenida permita predecir y modelar con precisión la propiedad física del sistema en futuras iteraciones del experimento. Sin embargo, en el modelo de la mecánica cuántica, realizar una medición no consiste simplemente en *revelar* una propiedad física preexistente, sino que dicha propiedad se *determina* como consecuencia de la medición. Sorprendentemente, numerosos experimentos, entre ellos los relacionados con la conocida Desigualdad de Bell, han llevado a interpretar que las partículas cuánticas no poseen propiedades físicas determinadas antes de ser medidas. Establecemos dicha expresión matemática de la siguiente manera.

4. Matriz de Fourier

La transformada de Fourier es una herramientas fundamental para representar funciones periódicas y señales discretas. En computación cuántica, esta es esencial para algoritmos como el algoritmo de Shor y la transformada cuántica de Fourier (QFT). En lo que sigue del capítulo consideremos fijo a un $n \in \mathbb{N}$ (como el número de qubits en una computadora).

4.1. Transformada Finita de Fourier

Definición 4.1. Definiendo $\epsilon_n \coloneqq \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}}$. La transformada discreta de Fourier es un operador $\mathcal{F}_n : \mathbb{C}^n \to \mathbb{C}^n$ dado por la siguiente matriz:

$$\mathcal{F}_n \coloneqq [\epsilon_n^{-jk}]_{j,k=0}^{n-1}.$$

También definimos a los siguiente vectores $f_{n,j} \coloneqq \frac{1}{\sqrt{n}} \left[\epsilon_n^{jk}\right]_{k=0}^{n-1}$, con $j \in [\![0, n[\![$.

Proposición 4.2. *La lista ordenada $(f_{n,j})_{j=0}^{n-1}$ es una base ortonormal en $\mathbb{C}^n$.*

Demostración. Sean $p, q \in [\![0, n[\![$.

$$\langle f_{n,p} | f_{n,q} \rangle = \sum_{k=0}^{n-1} (f_{n,p})_k \overline{(f_{n,q})_k} = \frac{1}{n} \sum_{k=0}^{n-1} \epsilon_n^{pk} \epsilon_n^{-qk} = \frac{1}{n} \sum_{k=0}^{n-1} \epsilon_n^{(p-q)k} = \delta_{p,q}.$$

De lo anterior se sigue que cada vector es normal y más aún son ortogonales por lo que son linealmente independientes y se concluye que forman una base ortonormal en $\mathbb{C}^n$. □

Definición 4.3. Sea $v \in \mathbb{C}^n$, definimos como la **transformada finita de Fourier** de z al vector

$$\hat{v} \coloneqq \left[\sum_{k=0}^{n-1} v_k \epsilon_n^{-jk}\right]_{j=0}^{n-1} = \mathcal{F}_n v.$$

Notemos que $\hat{v}_j = \sqrt{n}\,\langle f_{n,j}|v\rangle$.

Proposición 4.4. *El operador* $\frac{1}{\sqrt{n}}\mathcal{F}_n$ *es unitario.*

Demostración. Recordemos que por definición un operador es unitario si se cumple que el producto por la izquierda con su operador adjunto resulta en la identidad, en este caso I_n. Por lo tanto,

$$\left(\frac{1}{\sqrt{n}}\mathcal{F}_n^*\right)\left(\frac{1}{\sqrt{n}}\mathcal{F}_n\right) = \frac{1}{n}\left[\epsilon_n^{pq}\right]_{p,q=0}^{n-1}\left[\epsilon_n^{-pq}\right]_{p,q=0}^{n-1} = \frac{1}{n}\left[\sum_{k=0}^{n-1}\epsilon_n^{pr}\epsilon_n^{-rq}\right]_{p,q=0}^{n-1} = \left[\delta_{p,q}\right]_{p,q=0}^{n-1} = I_n.$$

□

De lo anterior, hemos demostrado que el operador inverso de $\mathcal{F}_n$ es $\frac{1}{n}\mathcal{F}_n^*$ y por lo tanto

$$v = \mathcal{F}_n\hat{v} = \left(\frac{1}{n}\mathcal{F}_n^*\right)\hat{v} = \frac{1}{n}\left[\sum_{k=0}^{n-1}\hat{v}_k\epsilon_n^{jk}\right]_{j=0}^{n-1} = \frac{1}{\sqrt{n}}\left[\sum_{k=0}^{n-1}\hat{v}_k f_{n,j}\right]_{j=0}^{n-1}.$$

Se sigue que la transformada finita de Fourier de v son los coeficientes del mismo vector en la base ortonormal $(f_{n,j})_{j=0}^{n-1}$ (también llamada la **base de Fourier**) multiplicados por una constante.

4.2. Matrices Circulantes

Para la definición de matriz circulante consideramos los índices como elementos del grupo aditivo $(\mathbb{Z}_n, +)$.

Definición 4.5. Sea $a \in \mathbb{C}^n$. La **matriz circulante** asociada al vector a se define como

$$\operatorname{circ}(a) \coloneqq \left[a_{j-k}\right]_{j,k=0}^{n-1}.$$

Referencias

[1] Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information* (10th anniversary ed.). Cambridge University Press. doi:10.1017/CBO9780511976667.

[2] Shor, P. W. (1995). *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. *SIAM Journal on Computing*, *26*(5), 1484–1509. arXiv:quant-ph/9508027. doi:10.1137/S0097539795293172.

[3] Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., & Chuang, I. L. (2001). *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*. *Nature*, *414*, 883–887. doi:10.1038/414883a.

[4] M. H. Wong, *Discrete Fourier Analysis*, Birkhäuser, 2011. doi:10.1007/978-3-0348-0116-4.

[5] Bernhardt, C. (2019). *Quantum Computing for Everyone*. MIT Press, Cambridge, MA. ISBN: 978-0-262-53953-1.