Esta última hoja está dedicada al algoritmo cuántico más famoso. Su fama radica en que, en caso de implementarse, lograría romper el criptosistema RSA que es la base de muchos sistemas de seguridad. Es muy posible que te hayan hablado de este criptosistema en uno o más cursos del grado. En cualquier caso, es fácil encontrar buenas referencias (como [5]) y deberías incluir una pequeña descripción en tu trabajo para dar un contexto al algoritmo.

1) Escribe unas líneas explicando el criptosistema RSA y su relación con la factorización.

La criptografía se basa en gran medida en "funciones trampa", operaciones que son fáciles de hacer y difíciles de deshacer sin información adicional. En relación con RSA, en cualquiera de nuestros ordenadores sería sencillo multiplicar dos primos p y q de miles de cifras (incluso de más) para obtener $N = pq$. sin embargo, fuera de elecciones especiales, ningún superordenador es capaz de recuperar p y q a partir de N. Ya para cientos de cifras se considera que el sistema es seguro.

El *algoritmo de Shor* que trataremos en esta hoja es un algoritmo introducido en 1997 por P.W. Shor [6] para encontrar factores no triviales de un número impar $N \in \mathbb{Z}_{>2}$. En un ordenador clásico sería extremadamente lento e inútil, mientras que, teóricamente, en un ordenador cuántico sería mucho más rápido que los algoritmos conocidos para números grandes. Por otro lado, su implementación práctica es a día de hoy un problema no resuelto. Hasta 2001 el mayor número factorizado con el algoritmo de Shor en un ordenador cuántico era $N = 15$ y creo que todavía no se ha llegado a ninguno de tres cifras. La dificultad no es un obstáculo teórico (en este caso, no hay "oráculos" no descritos), sino práctica, porque se necesitan muchos qubits entrelazados y puertas cuánticas que funcionen libres de errores durante cierto tiempo[1].

Comencemos con la descripción matemática del algoritmo de Shor para después adentrarnos en la realización cuántica de uno de sus pasos. Debes tener en mente que calcular el máximo común divisor de números grandes, el cual indicaremos con gcd, y calcular potencias módulo un número grande, admite algoritmos eficientes en un ordenador clásico (en el primer caso, es el algoritmo de Euclides).

El algoritmo de Shor es probabilista en el sentido de que a veces no funciona y hay que probar de nuevo. Además la parte cuántica añade otra componente probabilista. Los pasos son los siguientes:

A. Se elige un entero al azar $a \in [2, N)$. Si $\gcd(a, N) \neq 1$, es un factor no trivial de N y el algoritmo termina.

B. Se calcula el orden r de a en $(\mathbb{Z}/NZ)^*$. Es decir, el menor $r \in \mathbb{Z}^+$ tal que $a^r \equiv 1 \pmod{N}$.

C. Si r es impar o si r es par con $a^{r/2} \equiv -1 \pmod{N}$, el algoritmo no funciona y hay que probar con otro a. En otro caso, $\gcd\left(N, a^{r/2} + 1\right)$ es un factor no trivial de N.

[1] Posiblemente, el mayor impedimento actual para que la computación cuántica se vuelva cotidiana es que no hay buenos sistemas para impedir ruido y errores, lo que limita mucho los algoritmos que se pueden usar.

2) Explica por qué si r es par y $a^{r/2} \not\equiv -1 \pmod N$, realmente $\gcd(N, a^{r/2}+1)$ es un factor no trivial de N.

3) Aplica el algoritmo anterior para $N = 15$ con $a = 7$. ¿Qué factor de N se obtiene?

Al ser probabilista, es crucial preguntarse si es muy improbable que para un a elegido al azar se cumpla que su orden r sea par y, a la vez, que $a^{r/2} \not\equiv -1 \pmod N$. La respuesta es que no, pero una prueba detallada nos obligaría a dar un rodeo y no entraremos en ello. Está basada el isomorfismo $(\mathbb{Z}/pq\mathbb{Z})^* \cong C_{p-1} \oplus C_{q-1}$ con $-\bar{1} \mapsto (\frac{p-1}{2}, \frac{q-1}{2})$ donde $p, q > 2$ son primos y C_k es el grupo cíclico de k elementos.

4) Usando el isomorfismo anterior, comprueba que para $N = 15$ todo $\bar{a} \in (\mathbb{Z}/N\mathbb{Z})^*$ distinto de $\bar{1}$ tiene orden r par y halla cuántas clases cumplen $a^{r/2} \equiv -1 \pmod N$.

En un ordenador clásico, A y C son fáciles de implementar, sin embargo no se conocen algoritmos eficientes para calcular el orden que se pide en B. Algunos criptosistemas se basan en este hecho. Por otro lado, lo que mostró Shor es que hay un algoritmo cuántico teórico eficiente para resolver este problema. Está estrechamente relacionado con otro algoritmo llamado *estimación de fase cuántica* y con la *transformada de Fourier cuántica*. Por brevedad, no aparecerán explícitamente. Si tienes curiosidad mira [3].

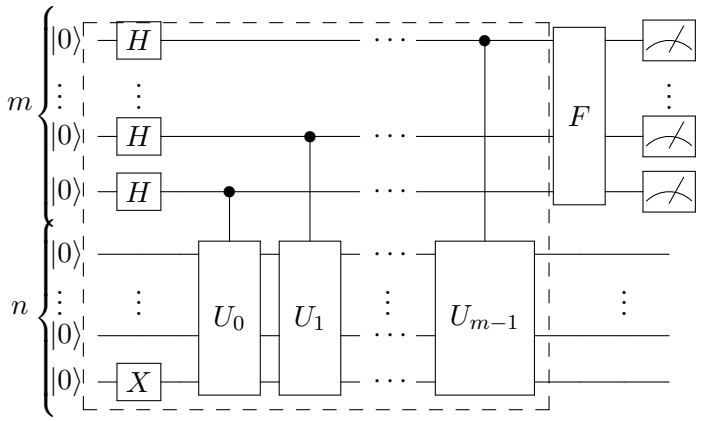
Antes de nada, recordaremos una variante del *núcleo de Dirchlet* de cursos de análisis y un resultado de aproximación diofántica del curso de teoría de números. No hace falta que repases nada.

5) Para $M \in \mathbb{Z}^+$ y $x \in \mathbb{R}$ sea $D_M(x) = \frac{1}{M}\sum_{k=0}^{M-1} e^{2\pi i k x}$. Prueba $|D_M(x)|^2 = \frac{\operatorname{sen}^2(\pi M x)}{M^2 \operatorname{sen}^2(\pi x)}$ para $x \notin \mathbb{Z}$. En particular, $D_M(a/q) = 0$ para $a \in \mathbb{Z}$, $q \in \mathbb{Z}^+$ si $q \mid M$ y $q \nmid a$.

Esto asegura que $|D_M(x)|^2$, para $x \in [-1/2, 1/2]$ y M grande, es prácticamente 1 cuando $|x|$ es bastante menor que M^{-1} y es pequeño si $|x|$ es bastante mayor que M^{-1}. Si quieres, haz un dibujo con $M = 40$, para que veas el aspecto.

Lo que tienes que recordar de teoría de números es más profundo. Si tenemos un número real α y una fracción irreducible a/q que lo aproxima bien en el sentido de que $\left|\alpha - \frac{a}{q}\right| < \frac{1}{2q^2}$, entonces necesariamente a/q es una convergente de la fracción continua de α (si quieres ver una prueba, mira [1, Prop. 2.2.6], [2] o [4]). Las convergentes son fáciles de determinar algorítmicamente y tienen denominadores que crecen exponencialmente, por tanto hay del orden de $\log N$ que cumplen $q < N$, lo cual hace que sea fácil hallar y almacenar todas las que verifican esta condición incluso si N tiene cientos de cifras. No hace falta que recuerdes cómo se hallaban las fracciones continuas. Solo que sepas que hay un algoritmo sencillo y eficiente para determinar todas las fracciones irreducibles que cumplen $\left|\alpha - \frac{a}{q}\right| < \frac{1}{2q^2}$ con $q < N$ aunque N sea gigantesco. Es eso lo que debes reflejar en tu trabajo, acompañado de referencias adecuadas.

Pasamos por fin a la realización cuántica del cálculo del orden de a módulo N. Responde a un circuito de la forma:



La línea de puntos no indica nada, es solo para referencia posterior. En la entrada, como se indica, hay $m+n$ ceros. Tomando $m = 2n+1$ ya se tiene un algoritmo aceptable y con m mayor se consigue que el resultado sea menos probabilista. La n hay que escogerla de forma que 2^n sea mayor que N. Entenderemos $\left|a^k\right\rangle$ como una abreviatura del registro de n qubits $|R\rangle$ donde R es el resto al dividir a^k por N. Esto es, las potencias las consideraremos siempre módulo N.

Con lo que sabes de hojas anteriores, el paso por las puertas de Hadamard y la puerta X (también llamada NOT) da lugar al estado

$$|\phi\rangle = \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle \otimes |1\rangle$$

donde $|k\rangle$ y $|1\rangle$ se entienden, respectivamente, como registros de m y n qubits. Si no lo ves claro, piénsalo e incluye unas líneas para explicártelo a ti misma.

Definimos los estados normalizados

$$|u_j\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{-2\pi i \ell j/r} \left|a^\ell\right\rangle, \qquad \text{con } j = 0, 1, \ldots, r-1.$$

Aunque no sepamos construirlos, porque no conocemos r, es posible escribir $|\phi\rangle$ en términos de ellos.

6) Prueba

$$|\phi\rangle = \frac{1}{2^{m/2}\sqrt{r}} \sum_{k=0}^{2^m-1} \sum_{j=0}^{r-1} |k\rangle \otimes |u_j\rangle\,.$$

Si $k = b_{m-1}2^{m-1} + \cdots + b_1 2^1 + b_0$, consideremos para cada $0 \le j < m$ la puerta cuántica U_j que efectúa la multiplicación por a^{2^j} módulo N controlada por b_j. Es decir, para $0 \le \ell < 2^n$ se tiene

$$U_j \left|\ell\right\rangle = \begin{cases} \left|a^{2^j}\ell \ (\text{mód } N)\right\rangle & \text{si } 0 \le \ell < N \text{ y } b_j = 1, \\ \left|\ell\right\rangle & \text{en otro caso.} \end{cases}$$

7) Muestra que $|u_\ell\rangle$ es un autovector de U_j con autovalor $e^{2\pi i b_j 2^j \ell/r}$. Concluye con ello que la parte del circuito encerrada en línea de puntos da lugar al estado

$$\left|\psi\right\rangle = \frac{1}{2^{m/2}\sqrt{r}} \sum_{k=0}^{2^m-1} \sum_{j=0}^{r-1} e^{2\pi i k j/r} \left|k\right\rangle \otimes \left|u_j\right\rangle .$$

La puerta F del circuito actúa sobre registros de m qubits de la forma siguiente:

$$F : \left|k\right\rangle \longmapsto \frac{1}{2^{m/2}} \sum_{\ell=0}^{2^m-1} e^{-2\pi i k\ell/2^m} \left|\ell\right\rangle .$$

Si conoces la DFT del análisis de Fourier discreto, notarás la analogía.

8) Prueba que F es realmente una puerta cuántica, esto es, que define una aplicación lineal unitaria.

9) Establece la identidad

$$\left(F \otimes I^{\otimes n}\right) \left|\psi\right\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{2^m-1} \sum_{j=0}^{r-1} D_{2^m}\Big(\frac{j}{r} - \frac{k}{2^m}\Big) \left|k\right\rangle \otimes \left|u_j\right\rangle .$$

Supongamos que $\left|D_{2^m}(x)\right|^2$ es exactamente la función característica de $|x| < 2^{-m}$ en lugar de una aproximación suya, entonces, después de la medición que indica el circuito, si obtenemos $|k_0\rangle$, el estado $\left(F \otimes I^{\otimes n}\right)|\psi\rangle$ colapsará a un estado proporcional a

$$\left|k_0\right\rangle \otimes \sum_{j \in J} \left|u_j\right\rangle \qquad \text{con} \quad J = \Big\{ j \ : \ \Big|\frac{j}{r} - \frac{k_0}{2^m}\Big| < \frac{1}{2^m} \Big\}.$$

10) Explica por qué si $m > 2n$ estamos en condiciones de aplicar el resultado de teoría de números con $\alpha = k_0/2^m$ y, a partir de k_0 (lo que hemos obtenido en la medición), calcular todas las posibilidades para j/r con denominador menor que N.

Concluimos con unos comentarios acerca de dos cabos sueltos en esta parte final. Realmente, $\left|D_{2^m}(x)\right|^2$ no es la función característica de $|x| < 2^{-m}$. Si lo piensas, todo lo que necesitamos es que sean muy pequeño cuando $|x| > 1/(2r^2)$, porque esto se traduce en que haya una

probabilidad muy pequeña de que obtengamos j/r erróneos. Se puede conseguir con precisión arbitraria tomando m muy por encima de $2n$ para que el decaimiento de D_{2^m} sea mayor.

El otro cabo suelto es más importante. Consiste en que si j y r tienen factores comunes, entonces j/r no es irreducible y no podemos recuperar r a partir de los posibles valores simplificados para j/r, que es lo que nos dan las convergentes. En vez de r se obtendría un divisor de r. En breve, el denominador de j/r como elemento de $\mathbb{Q}$ no es r si la fracción no es irreducible. Ahora bien, si repitiendo el algoritmo unas cuantas veces, tenemos suficientes divisores de r, se puede reconstruir r calculando el mínimo común múltiplo. En el apartado *Continued fraction algorithm to retrieve the period* de [7] está explicado este punto. Por supuesto, podríamos tener muy mala suerte y con ejecuciones sucesivas obtener siempre el mismo divisor, pero eso tiene una probabilidad despreciable.

El resumen de la parte cuántica del algoritmo de Shor para hallar el orden r de a, es que después de aplicar el circuito, en la medición obtendremos un registro $|k_0\rangle$ de m qubits. Considerando los denominadores menores que N de las convergentes de $\alpha = k_0/2^m$ obtendremos candidatos a valores de r o divisores suyos. Con suficientes divisores es posible reconstruir r. Es fácil decidir si un candidatos a r es realmente r, simplemente hay que comprobar $a^r \equiv 1$ (mód N). Recordemos que halla restos de potencias es fácil en un ordenador convencional.

Tarea a entregar. Escribe un documento que combine las soluciones de los ejercicios anteriores. Trata de ajustarte a 8 páginas. Debes encontrar un balance entre lo que explicas y lo que citas, sobre todo en relación con temas de teoría de números.

El documento debe dar lugar a un quinto y último capítulo de tu TFG llamado *El algoritmo de Shor* o alguna variante que te parezca adecuada.

Referencias

[1] F. Chamizo. Apuntes del curso de teoría combinatoria y analítica de números. `https://matematicas.uam.es/~fernando.chamizo/asignaturas/2223tenum/2223tenum.html`, 2022.

[2] S. J. Miller and R. Takloo-Bighash. *An invitation to modern number theory.* Princeton University Press, Princeton, NJ, 2006. With a foreword by P. Sarnak.

[3] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, 2000.

[4] H. E. Rose. *A course in number theory*. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, second edition, 1994.

[5] K. H. Rosen. *Elementary number theory and its applications*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, third edition, 1993.

[6] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[7] Wikipedia contributors. Shor's algorithm — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Shor%27s_algorithm&oldid=1221004007`, 2024. [Online; accessed 28-April-2024].