# Las Matemáticas en la era de la Computación Cuántica

F. Adrián F. Tojo
Franciso J. Fernández
Francisco J. Pena

CITMAGA
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

CESGA
GALICIA SUPERCOMPUTING CENTER

CITMAGA
GALICIAN CENTRE FOR MATHEMATICAL RESEARCH AND TECHNOLOGY

# ¿Cuál es el interés de un matemático en la computación cuántica?

# ¿Cuál es el interés de un matemático en la computación cuántica?

1. *Abstracto:* jugar con un nuevo paradigma computacional (aspectos formales, algorítmicos, lógicos…).

# ¿Cuál es el interés de un matemático en la computación cuántica?

1. *Abstracto:* jugar con un nuevo paradigma computacional (aspectos formales, algorítmicos, lógicos…).
2. *Concreto:* realizar cálculos necesarios para la resolución de problemas de manera más rápida y eficiente que con la computación clásica.

# ¿Qué espera un matemático de la computación?

# ¿Qué espera un matemático de la computación?

1. Cálculo de valores para funciones complicadas (e.g. invariantes).

# ¿Qué espera un matemático de la computación?

1. Cálculo de valores para funciones complicadas (e.g. invariantes).
2. Resultados de problemas combinatorios.

# ¿Qué espera un matemático de la computación?

1. Cálculo de valores para funciones complicadas (e.g. invariantes).
2. Resultados de problemas combinatorios.
3. Optimización de funciones.

# ¿Qué espera un matemático de la computación?

1. Cálculo de valores para funciones complicadas (e.g. invariantes).
2. Resultados de problemas combinatorios.
3. Optimización de funciones.
4. Resolución de sistemas lineales de grandes dimensiones.

# La ventaja cuántica

- La *ventaja cuántica* es la *capacidad de un ordenador cuántico para resolver un problema determinado (de entrada a salida) que un ordenador clásico no puede resolver o para la resolución del cual requeriría un tiempo inasumible*.

# La ventaja cuántica

- La *ventaja cuántica* es la *capacidad de un ordenador cuántico para resolver un problema determinado (de entrada a salida) que un ordenador clásico no puede resolver o para la resolución del cual requeriría un tiempo inasumible*.
- Que exista o no un tiempo razonable depende de que haya una diferencia entre la complejidad de los algoritmos en cuestión entre el ordenador clásico y el cuántico.

# La ventaja cuántica

- La *ventaja cuántica* es la *capacidad de un ordenador cuántico para resolver un problema determinado (de entrada a salida) que un ordenador clásico no puede resolver o para la resolución del cual requeriría un tiempo inasumible*.
- Que exista o no un tiempo razonable depende de que haya una diferencia entre la complejidad de los algoritmos en cuestión entre el ordenador clásico y el cuántico.
- Así, tomando una entrada suficientemente grande, si la complejidad del algoritmo cuántico es mejor que la del clásico, el ordenador cuántico podrá resolver el problema mientras que el clásico no.

# La ventaja cuántica

- El problema no reside tanto en obtener la complejidad del algoritmo cuántico, sino en demostrar que no puede existir algoritmo clásico que la iguale. A medida que se han descrito algoritmos cuánticos mejores, también han aparecido algoritmos clásicos nuevos que limitan la ventaja de estos (*descuantización*).

# La ventaja cuántica

- El problema no reside tanto en obtener la complejidad del algoritmo cuántico, sino en demostrar que no puede existir algoritmo clásico que la iguale. A medida que se han descrito algoritmos cuánticos mejores, también han aparecido algoritmos clásicos nuevos que limitan la ventaja de estos (*descuantización*).
- Muchos algoritmos cuánticos usan *oráculos*, esto es, cajas negras formales que dada una entrada devuelven la salida deseada de forma inmediata y sin limitaciones técnicas. El uso de estos oráculos puede ocultar la verdadera complejidad del problema.

# La ventaja cuántica

- El problema no reside tanto en obtener la complejidad del algoritmo cuántico, sino en demostrar que no puede existir algoritmo clásico que la iguale. A medida que se han descrito algoritmos cuánticos mejores, también han aparecido algoritmos clásicos nuevos que limitan la ventaja de estos (*descuantización*).
- Muchos algoritmos cuánticos usan *oráculos*, esto es, cajas negras formales que dada una entrada devuelven la salida deseada de forma inmediata y sin limitaciones técnicas. El uso de estos oráculos puede ocultar la verdadera complejidad del problema.
- Un ordenador cuántico capaz de resolver el problema debe poder construirse. Los ordenadores clásicos dejan de ser competitivos para problemas de alta complejidad cuando las entradas son muy grandes, pero cualquier ordenador cuántico que pretenda resolver el mismo problema debe ser capaz de gestionar dichas entradas. Eso requiere arquitecturas de ordenadores cuánticos escalables que eviten los problemas de ruido y decoherencia.

# Algoritmo de Shor

**Problema:** *Encontrar la descomposición en factores primos de un número entero.*

*Complejidad clásica:* $O\left(e^{(\log N)^{1/3}(\log\log N)^{2/3}}\right)$.

*Complejidad cuántica:* $O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$.

# Algoritmo de Shor

**Problema:** *Encontrar la descomposición en factores primos de un número entero.*

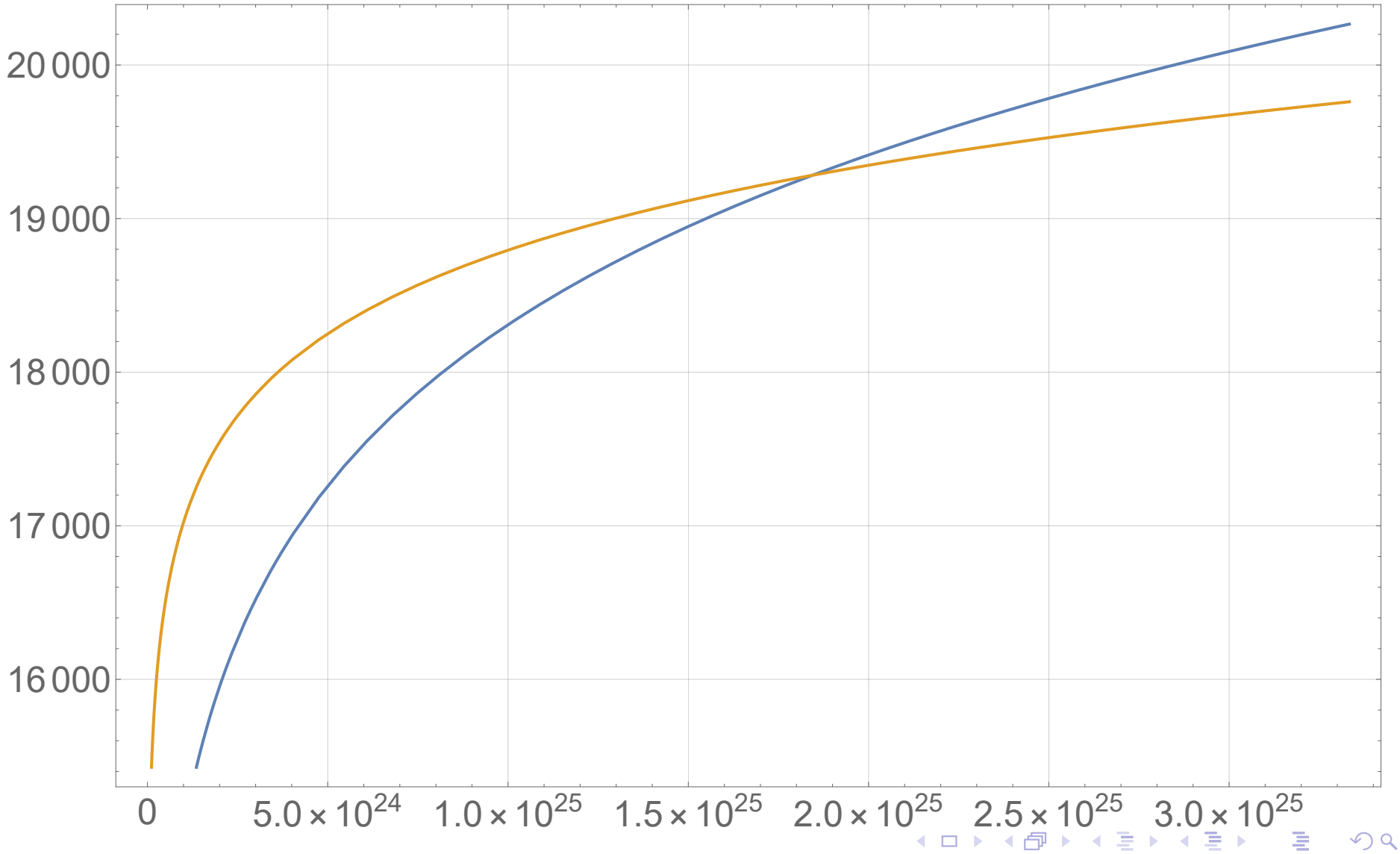
*Complejidad clásica:* $O\left(e^{(\log N)^{1/3}(\log\log N)^{2/3}}\right)$.

*Complejidad cuántica:* $O\left((\log N)^2(\log\log N)(\log\log\log N)\right)$.

El algoritmo de Shor consta de una parte clásica (que se realiza en un ordenador convencional) y de una parte cuántica.

Lamentablemente, el número de cúbits necesarios para factorizar números grandes está lejos de la capacidad de los ordenadores cuánticos actuales.

# Algoritmo de Shor



# Criptografía

El algoritmo de Shor podría permitir romper los sistemas criptográficos clásicos (RSA, Diffie-Hellman…). Este hecho ha derivado en la fundación de la *criptografía poscuántica*, en la que se busca algoritmos de encriptación clásicos que sean resistentes a los ataques cuánticos. El sistema AES, establecido como estándar por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST) en 2001, parece resistente a los ataques cuánticos conocidos.

# Criterios de primalidad

**Problema:** *Dado un número de n-bits buscamos decidir si es primo o no.*

*Complejidad clásica:* $O(n^4)$.

*Complejidad cuántica:* $O(n^2(\log\ n)^3\ \log\ \log\ n)$.

Este algoritmo está basado en otro de búsqueda cuántica del período que subyace al algoritmo de Shor.

# Subgrupo oculto abeliano

**Problema:** *Dado un grupo abeliano finitamente generado $G$, un subgrupo $H$ de $G$ tal que $G/H$ es finito y una función $f$ definida sobre $G$ tal que $f(g_1) = f(g_2)$ si y sólo si $g_1 - g_2 \in H$ (es decir, $f$ pasa al cociente $G/H$), encontrar un conjunto de generadores de $H$ a través de consultas a $f$.*

*Complejidad clásica:* $\Omega(|G|)$ .

*Complejidad cuántica:* $O(\log |G|)$.

# Subgrupo oculto abeliano

**Problema:** *Dado un grupo abeliano finitamente generado $G$, un subgrupo $H$ de $G$ tal que $G/H$ es finito y una función $f$ definida sobre $G$ tal que $f(g_1) = f(g_2)$ si y sólo si $g_1 - g_2 \in H$ (es decir, $f$ pasa al cociente $G/H$), encontrar un conjunto de generadores de $H$ a través de consultas a $f$.*

*Complejidad clásica:* $\Omega(|G|)$ .
*Complejidad cuántica:* $O(\log |G|)$.

El algoritmo, está basado en la Transformada de Fourier Cuántica y tiene aplicaciones a la compresión cuántica de información.

# Subgrupo oculto abeliano

**Problema:** *Dado un grupo abeliano finitamente generado $G$, un subgrupo $H$ de $G$ tal que $G/H$ es finito y una función $f$ definida sobre $G$ tal que $f(g_1) = f(g_2)$ si y sólo si $g_1 - g_2 \in H$ (es decir, $f$ pasa al cociente $G/H$), encontrar un conjunto de generadores de $H$ a través de consultas a $f$.*

*Complejidad clásica:* $\Omega(|G|)$ .
*Complejidad cuántica:* $O(\log |G|)$.

El algoritmo, está basado en la Transformada de Fourier Cuántica y tiene aplicaciones a la compresión cuántica de información.

*Problemas abiertos:* extender los resultados obtenidos al caso de grupos no conmutativos.

# Subgrupo oculto abeliano

**Problema:** *Dado un grupo abeliano finitamente generado $G$, un subgrupo $H$ de $G$ tal que $G/H$ es finito y una función $f$ definida sobre $G$ tal que $f(g_1) = f(g_2)$ si y sólo si $g_1 - g_2 \in H$ (es decir, $f$ pasa al cociente $G/H$), encontrar un conjunto de generadores de $H$ a través de consultas a $f$.*

*Complejidad clásica:* $\Omega(|G|)$ .

*Complejidad cuántica:* $O(\log |G|)$.

El algoritmo, está basado en la Transformada de Fourier Cuántica y tiene aplicaciones a la compresión cuántica de información.

*Problemas abiertos:* extender los resultados obtenidos al caso de grupos no conmutativos.

*Líneas de investigación:* ampliar la familia de grupos no abelianos para los cuales se dispone de algoritmos eficientes.

# Obtención de autovalores

**Problema:** *Dado un hamiltoniano $H$, calcular el autovector asociado a su menor autovalor.*

- El algoritmo VQE permite calcular el autovector asociado al menor autovalor del hamiltoniano, minimizando el valor esperado.

# Obtención de autovalores

**Problema:** *Dado un hamiltoniano $H$, calcular el autovector asociado a su menor autovalor.*

- El algoritmo VQE permite calcular el autovector asociado al menor autovalor del hamiltoniano, minimizando el valor esperado.
- Se trata de un algoritmo de computación híbrida.

# Obtención de autovalores

**Problema:** *Dado un hamiltoniano $H$, calcular el autovector asociado a su menor autovalor.*

- El algoritmo VQE permite calcular el autovector asociado al menor autovalor del hamiltoniano, minimizando el valor esperado.
- Se trata de un algoritmo de computación híbrida.
- *Dificultades:* Incapacidad de evadir los numerosos puntos críticos locales que presenta el espacio de optimización ("barren plateaus", zonas donde los gradientes se vuelven nulos). Se han propuesto algunas soluciones como el Quantum Particle Swarm Optimization (QPSO).

# Análisis cuántico de datos topológicos

- El *análisis topológico de datos* (ATD) consiste en el análisis de conjuntos de datos utilizando técnicas topológicas. Permite la extracción de información de conjuntos de datos de dimensión alta, incompletos o ruidosos.

# Análisis cuántico de datos topológicos

- El *análisis topológico de datos* (ATD) consiste en el análisis de conjuntos de datos utilizando técnicas topológicas. Permite la extracción de información de conjuntos de datos de dimensión alta, incompletos o ruidosos.
- Las técnicas del ATD buscan obtener la *forma* de los mismos. La herramienta principal es la *homología persistente*, una adaptación de la homología a datos de nubes de puntos.

# Análisis cuántico de datos topológicos

- El *análisis topológico de datos* (ATD) consiste en el análisis de conjuntos de datos utilizando técnicas topológicas. Permite la extracción de información de conjuntos de datos de dimensión alta, incompletos o ruidosos.
- Las técnicas del ATD buscan obtener la *forma* de los mismos. La herramienta principal es la *homología persistente*, una adaptación de la homología a datos de nubes de puntos.

**Problema:** *Obtener la homología (números de Betti)*

*Complejidad clásica:* $O(2^{2n})$.
*Complejidad cuántica:* $O(n^5)$.

Esta mejora es posible al almacenar los $n$ vértices del grafo en $n$ cúbits que codifican la información combinatoria de los mismos (orden de $2^n$).

# Análisis cuántico de datos topológicos

- El *análisis topológico de datos* (ATD) consiste en el análisis de conjuntos de datos utilizando técnicas topológicas. Permite la extracción de información de conjuntos de datos de dimensión alta, incompletos o ruidosos.
- Las técnicas del ATD buscan obtener la *forma* de los mismos. La herramienta principal es la *homología persistente*, una adaptación de la homología a datos de nubes de puntos.

**Problema:** *Obtener la homología (números de Betti)*

*Complejidad clásica:* $O(2^{2n})$.
*Complejidad cuántica:* $O(n^5)$.

Esta mejora es posible al almacenar los $n$ vértices del grafo en $n$ cúbits que codifican la información combinatoria de los mismos (orden de $2^n$).

Existen indicios de que la mejora exponencial de estos algoritmos frente a los clásicos es *genuina*.

# Algoritmo de resolución de sistemas lineales (HHL)

**Problema:** Dada una matriz hermitiana $A \in \mathcal{M}_{N\times N}(\mathbb{C})$, con $N = 2^{n_b}$, y un vector unitario $b \in \mathcal{M}_{N\times 1}(\mathbb{C})$, estimar el valor de $x \in \mathcal{M}_{N\times 1}(\mathbb{C})$ tal que $Ax = b$.

El *algoritmo HHL* (Harrow-Hassidim-Lloyd) soluciona este problema. Cuando $A$ es dispersa, el algoritmo HHL presenta una mejora exponencial en el orden de complejidad frente al mejor algoritmo clásico.

*Complejidad clásica:* $O(d^4\kappa^2 \log(N)/\varepsilon)$.

*Complejidad cuántica:* $O(Nd\kappa \log(1/\varepsilon))$ .

# Condiciones y limitaciones del HHL

Para alcanzar la mejora exponencial es necesario:

- Poder acceder a los elementos de la matriz $A$ de forma eficiente.

# Condiciones y limitaciones del HHL

Para alcanzar la mejora exponencial es necesario:

- Poder acceder a los elementos de la matriz $A$ de forma eficiente.
- La matriz $A$ debe ser dispersa o debe poderse descomponer como producto de matrices dispersas.

# Condiciones y limitaciones del HHL

Para alcanzar la mejora exponencial es necesario:

- Poder acceder a los elementos de la matriz $A$ de forma eficiente.
- La matriz $A$ debe ser dispersa o debe poderse descomponer como producto de matrices dispersas.
- El condicionamiento de $A$ tiene que escalar como polilog$(N)$.

# Condiciones y limitaciones del HHL

Para alcanzar la mejora exponencial es necesario:

- Poder acceder a los elementos de la matriz $A$ de forma eficiente.
- La matriz $A$ debe ser dispersa o debe poderse descomponer como producto de matrices dispersas.
- El condicionamiento de $A$ tiene que escalar como polilog$(N)$.

*Dificultades:*

- La preparación del estado inicial es un problema abierto.

# Condiciones y limitaciones del HHL

Para alcanzar la mejora exponencial es necesario:

- Poder acceder a los elementos de la matriz $A$ de forma eficiente.
- La matriz $A$ debe ser dispersa o debe poderse descomponer como producto de matrices dispersas.
- El condicionamiento de $A$ tiene que escalar como polilog$(N)$.

*Dificultades:*

- La preparación del estado inicial es un problema abierto.
- Puesto que la solución viene dada en un estado cuántico, obtener el valor de cada una de las componentes es un problema en sí mismo.

# Condiciones y limitaciones del HHL

Para alcanzar la mejora exponencial es necesario:

- Poder acceder a los elementos de la matriz $A$ de forma eficiente.
- La matriz $A$ debe ser dispersa o debe poderse descomponer como producto de matrices dispersas.
- El condicionamiento de $A$ tiene que escalar como polilog$(N)$.

*Dificultades:*

- La preparación del estado inicial es un problema abierto.
- Puesto que la solución viene dada en un estado cuántico, obtener el valor de cada una de las componentes es un problema en sí mismo.
- El condicionamiento de $A$ tiene que escalar a lo sumo polilog$(N)$, lo cual es una condición muy restrictiva que limita el rango de aplicación del algoritmo.

# Ecuaciones diferenciales ordinarias

**Problema:** *Dado un problema de valores iniciales en* $\mathbb{R}^n$, $\mathrm{d}\,\mathbf{x}/\,\mathrm{d}\,t = \mathbf{f}(t, \mathbf{x})$, $\mathbf{x}(t_0) = \mathbf{x}_0$, *aproximar numéricamente su solución en un determinado tiempo o conjunto finito de tiempos.*

- El método consiste en partir de esquemas numéricos clásicos para la resolución de EDOs para llegar a un sistema lineal que puede ser abordado con algoritmos QLSA (Quantum Lineal Solver Algorithm) del tipo HHL.

# Ecuaciones diferenciales ordinarias

**Problema:** *Dado un problema de valores iniciales en* $\mathbb{R}^n$, $\mathrm{d}\,\mathbf{x}/\,\mathrm{d}\,t = \mathbf{f}(t, \mathbf{x})$, $\mathbf{x}(t_0) = \mathbf{x}_0$, *aproximar numéricamente su solución en un determinado tiempo o conjunto finito de tiempos.*

- El método consiste en partir de esquemas numéricos clásicos para la resolución de EDOs para llegar a un sistema lineal que puede ser abordado con algoritmos QLSA (Quantum Lineal Solver Algorithm) del tipo HHL.
- Los algoritmos QLSA nos proporcionan la solución en forma de estado cuántico, lo cual dificulta el acceso a la información completa sobre la solución.

# Conclusiones

- A día de hoy, ni la tecnología, ni los algoritmos existentes son competitivos frente a la computación clásica.

# Conclusiones

- A día de hoy, ni la tecnología, ni los algoritmos existentes son competitivos frente a la computación clásica.
- Hay algoritmos prometedores en el ámbito de los invariantes y propiedades de grafos debido a que el tipo de problema es propicio para la computación cuántica.

# Conclusiones

- A día de hoy, ni la tecnología, ni los algoritmos existentes son competitivos frente a la computación clásica.
- Hay algoritmos prometedores en el ámbito de los invariantes y propiedades de grafos debido a que el tipo de problema es propicio para la computación cuántica.
- Hay algoritmos cuya mejora es necesaria para que sean competitivos. Es crucial mejorar los algoritmos de resolución de sistemas lineales (e.g. HHL) en los que se basan un gran número de métodos.

# Conclusiones

- A día de hoy, ni la tecnología, ni los algoritmos existentes son competitivos frente a la computación clásica.
- Hay algoritmos prometedores en el ámbito de los invariantes y propiedades de grafos debido a que el tipo de problema es propicio para la computación cuántica.
- Hay algoritmos cuya mejora es necesaria para que sean competitivos. Es crucial mejorar los algoritmos de resolución de sistemas lineales (e.g. HHL) en los que se basan un gran número de métodos.
- En general, es necesario dedicar tiempo al descubrimiento de nuevos algoritmos básicos que no dependan de los clásicos (Shor, Grover, etc.) para conseguir un rendimiento competitivo.

# Conclusiones

- A día de hoy, ni la tecnología, ni los algoritmos existentes son competitivos frente a la computación clásica.
- Hay algoritmos prometedores en el ámbito de los invariantes y propiedades de grafos debido a que el tipo de problema es propicio para la computación cuántica.
- Hay algoritmos cuya mejora es necesaria para que sean competitivos. Es crucial mejorar los algoritmos de resolución de sistemas lineales (e.g. HHL) en los que se basan un gran número de métodos.
- En general, es necesario dedicar tiempo al descubrimiento de nuevos algoritmos básicos que no dependan de los clásicos (Shor, Grover, etc.) para conseguir un rendimiento competitivo.
- La investigación en algoritmos cuánticos ha supuesto una gran mejora en algoritmos clásicos.

# El informe

*Las Matemáticas en la era de la Computación Cuántica: nuevas fronteras*

# El informe

*Las Matemáticas en la era de la Computación Cuántica: nuevas fronteras*

- El informe cuenta con tres versiones, en castellano, gallego e inglés.

# El informe

*Las Matemáticas en la era de la Computación Cuántica: nuevas fronteras*

- El informe cuenta con tres versiones, en castellano, gallego e inglés.
- Se divide en dos partes: una de introducción a la computación cuántica y otra sobre problemas y algoritmos.

# El informe

*Las Matemáticas en la era de la Computación Cuántica: nuevas fronteras*

- El informe cuenta con tres versiones, en castellano, gallego e inglés.
- Se divide en dos partes: una de introducción a la computación cuántica y otra sobre problemas y algoritmos.
- Tiene por objetivo acercar a los matemáticos a la computación cuántica sin necesidad de conocimiento previo.

# El informe

*Las Matemáticas en la era de la Computación Cuántica: nuevas fronteras*

- El informe cuenta con tres versiones, en castellano, gallego e inglés.
- Se divide en dos partes: una de introducción a la computación cuántica y otra sobre problemas y algoritmos.
- Tiene por objetivo acercar a los matemáticos a la computación cuántica sin necesidad de conocimiento previo.
- También se incluyen problemas abiertos, casos de uso, recursos y una amplia bibliografía.

# Fin

*¡Gracias por vuestra atención!*

# Las Matemáticas en la era de la Computación Cuántica

F. Adrián F. Tojo
Franciso J. Fernández
Francisco J. Pena

CITMAGA
UNIVERSIDADE DE SANTIAGO DE COMPOSTELA



GALICIAN CENTRE FOR
MATHEMATICAL RESEARCH
AND TECHNOLOGY

A iniciativa do Polo de Tecnoloxías Cuánticas de Galicia conta con financiamento de:

**Fondos REACT EU**

AXENCIA GALEGA DE INNOVACIÓN

UNIÓN EUROPEA

Xacobeo 21·22

CESGA
Centro de Supercomputación de Galicia

Despregamento dunha infraestrutura baseada en tecnoloxías cuánticas da información que permita impulsar a I+D+i en Galicia.

Apoiar a transición cara a unha economía dixital.

Operación financiada pola Unión Europea, a través do FONDO EUROPEO DE DESENVOLVEMENTO REXIONAL (FEDER), como parte da resposta da Unión á pandemia da COVID-19.

PROGRAMA OPERATIVO
FEDER GALICIA
2014-2020

*Unha maneira de facer Europa*