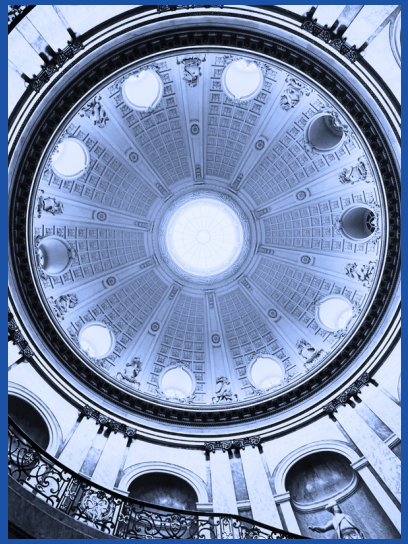
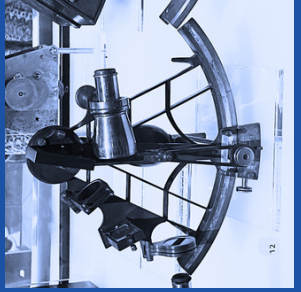
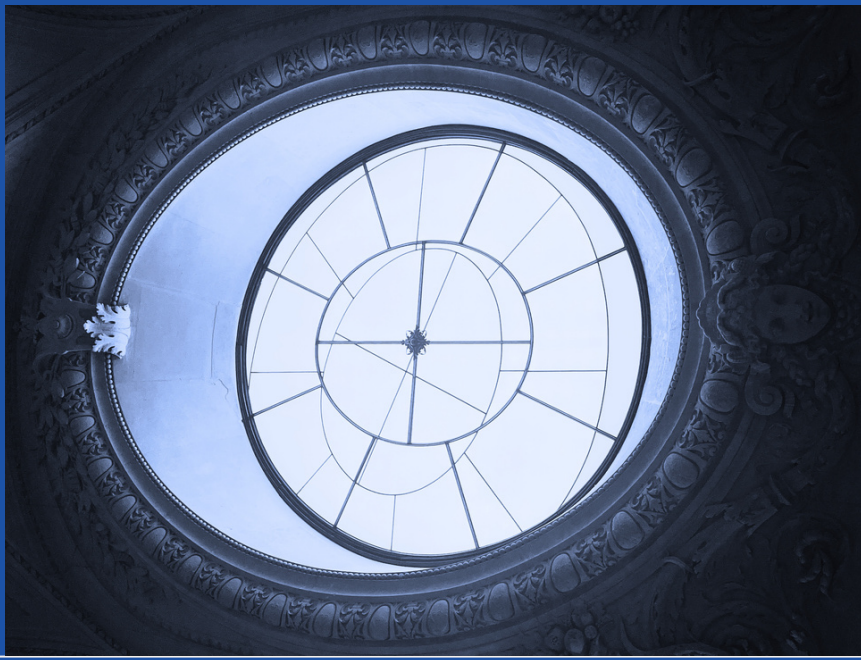
SIÁMATES







REVISTA ESTUDANTIL

FACULTADE DE MATEMÁTICAS USC

Introdución

Editores da revista

Un novo número desta revista ten lugar. Estamos moi contentos coa acollida que tivo, de primeiras, entre a xente que lle chegou a revista. Fixéronnos entrevistas dende "La Región" e tamén nos entrevistaron dende a Real Sociedade Española de Matemáticas, con vistas de coñecer que pretendemos.

Extracto

Neste segundo número contamos con diferentes artigos. Agradecemos pola súa redacción a Ibai, Santy, Nacho, Fran, Carlos e a Antón, do grupo Sementeira.

Historia

Santy achéganos como as matemáticas se meteron dentro dun parlamento e un mal exemplo de como aproximar π. Por outra parte, Fran relata a vida dunha grega pitagórica, Teano de Crotona, así como da súa aportación científica e filosófica.

Actualidade

Un problema que ven de case máis dunha centuria, ten sido explorado non fai moito (menos dun mes) con varias achegas importantes. Carlos actualízanos co traballo de Mattheus, S. e Verstraete, J. ademais de pornos en contexto co problema de Ramsey.

Retos

Dende Sementeira quéren mediarnos os exercicios, cóntanos a xeneralización da media e establecen as desigualdades máis coñecidas entre diferentes medias. Sorpréndennos coa visualización das mesmas e propoñen unha serie de exercicios resoltos e outros propostos.

Adxúntase un QR que contén as solucións dos exercicios do primeiro número.

Teoría

Os nosos compañeiros σ-teóricos explican dous temas bastante diferentes. Ibai describe o teorema de Minkoswky con varios exemplos gráficos e proponnos demostrar algunhas cousiñas. Nacho métese de cheo en modelización de computación cuántica, quere que nos actualicemos neste tema, para que sexamos quen de poder manexar o ordenador cuántico do CESGA.

Cartas al lector

Tes algunha curiosidade ou pequena dúbida matemática que cres que tamén voa pola cabeza dos teus compañeiros ou que simplemente non fuches quen de preguntar nunca a ninguén? Escríbenos ao noso correo, e recompilaremos de xeito anónimo as máis interesantes coas súas respectivas contestacións no próximo número de Máis Mates! Ou ata ao mellor pode servir de inspiración para algún dos artigos.

Difusión

Proximamente difundiremos por redes sociais un cartel informativo para que a xente se una neste proxecto. Calquera dúbida podedes mandala ao noso correo

Agradecementos

Queremos agradecer ao Servizo de Normalización Lingüística da Universidade a súa revisión do primeiro número da revista. Esperemos que nos apoien nesta tarefa, para ser o máis correctos posibles e difundir ciencia en galego.

CORREO:

REVISTAMAISMATES@GMAIL.COM

O parlamento de Indiana e a cuadratura do círculo

Santiago González Gómez

Ao longo da historia, numerosas persoas alleas ás matemáticas teñen participado nelas con diversos graos de éxito: dende Fermat, que era avogado, ata o artigo médico de 1993 que redescobre a noción da integral de Riemann. Porén, poucos casos involucraron a tantas persoas dun xeito tan espectacular como aquela vez na que o médico Edward J. Goodwin creu atopar a solución a un problema tan famoso e antigo como o da cuadratura do círculo.

O PROBLEMA

Dende o tempo dos antigos gregos, innumerables matemáticos se enfrontaron ao problema seguinte: dado un círculo dun determinado raio, atopar un cadrado de área equivalente empregando só regra e compás, é dicir, "cuadrar o círculo". Este problema ten que ver co desexo máis profundo de atopar de xeito sinxelo a área pechada por unha curva antes da invención do cálculo integral. Porén, tódalas solucións propostas ata o século XIX non foron máis que meras aproximacións, que se traducen en formas diversas de aproximar π. No 1882, Lindemann pechou o problema demostrando que o número π é trascendente, é dicir, que non pode ser obtido como solución de ningunha ecuación alxébrica con coeficientes racionais. Así, a cuadratura do círculo é imposible, pois calquera procedemento gráfico non é máis que a representación e resolución dunha ecuación deste tipo.

Mellor dito, o problema *semellaba* pechado, pois trala proba de Lindemann, non foron poucos os afeccionados que seguiron atacando o problema do mesmo modo que hoxe en día aparecen decote resolucións da hipótese de Riemann. Un destes pseudomatemáticos foi Edward Goodwin.

A SOLUCIÓN

En 1894, Goodwin publicou un artigo no *American Mathematical Monthly*, que daquela tiña pouco material e estaba aberto á publicación de calquera texto que lle enviasen coa única precaución de engadir unha advertencia baixo o título avisando de que o artigo aparecía publicado "a petición do autor". Nel, Goodwin aseguraba achar dunha vez por todas a solución ao problema de cuadrar o círculo.

O texto publicado por Goodwin comeza definitivamente mal, ao asumir que, se un círculo e un cadrado teñen o mesmo perímetro, entón teñen a mesma área. Dende este punto en adiante, Goodwin aborda o problema intentando rectificar a circunferencia (obter a súa lonxitude) para construír o cadrado, facendo que o lector se perda nun mar de supostas proporcións achadas entre raios, cordas, diagonais e lados. Durante unha exposición case que inintelixible, Goodwin é capaz de, inadvertidamente, dar resultados que se corresponden con empregar cinco valores diferentes para π: 4 (o necesario para que se cumpra a asunción sobre o perímetro), 3,160494, 3,232488, 3,235606 e 3,2, aos que en textos posteriores se lles engaden outros catro. Ningún deles é unha mellor aproximación que aquelas que xa se manexaban na Antigüidade. O valor $\pi = 3{,}2$ é o máis famoso dado por Goodwin, pois é o que el estipula explicitamente como ratio entre o diámetro e circunferencia.

O PARLAMENTO DE INDIANA

En 1897, Goodwin contactou co seu representante local no Parlamento de Indiana e convenceuno para propoñer constituír en lei estatal a súa "nova verdade matemática". Goodwin coidárase xa de patentar o seu descubrimento nos Estados Unidos, Reino Unido, Alemaña, Bélxica, Francia e España, pero nun arrebato de humildade, se a lei era aprobada e se fixaba o novo valor para π, permitiríalle ensinar ao estado de Indiana a súa fórmula nos libros de texto sen pagar *royalties*! A proposta de lei foi enviada ao Comité de Canais, que considerou adecuado reenviarlla ao Comité de Educación. A estas alturas, os xornais de Indiana xa se facían eco do novo descubrimento. O Comité de Educación recomendou que se aprobase o proxecto de lei. O parlamento aprobouno por absoluta unanimidade e foi enviado ao Senado. Ao recibir o proxecto, os senadores non puxeron pegas nunha primeira lectura na cámara, pero trala segunda, pospuxérono indefinidamente, pois consideraron que non era competencia súa lexislar sobre unha verdade matemática ("esta cámara podería mandar por lei que a auga correse cara a arriba"). Agora ben, temos que remarcar que a razón dada para esta postergación non foi que os senadores atopasen erros na solución de Goodwin, pois a meirande parte dos ponentes admitíronse ignorantes sobre o tema a tratar.

Que levaría ao Senado a un cambio tan drástico entre a primeira e a segunda lectura? Oficialmente, nada en especial, pero podemos atopar respostas na testemuña do profesor de matemáticas C.A. Waldo, que se atopaba no edificio mentres remataba a primeira lectura. Segundo el, un dos membros da cámara explicoulle o asunto que se estaba tratando e ofreceulle presentarlle ao autor do descubrimento, ao cal Waldo respondeu cun "grazas, xa coñezo a suficientes loucos". Tras isto, os senadores foron supostamente asesorados, e o proxecto de lei de Goodwin perdeuse para sempre.

REFERENCIAS

[1] BERGGREN, L., BORWEIN, J. M., BORWEIN, P. B. (1997), *Pi: a source book* (Vol. 617) 230-239, New York: Springer.

Teano de Crotona, a grega pitagórica

Francisco Estévez Lengua

Fig. 1: Unha "aproximación" dun retrato de Teano

Vida e contexto sociocultural

Nace no ano 546 a.C. en Crotona, situada na Magna Grecia, actual sur de Italia.

É ben sabido que a Antiga Grecia é cuna do coñecemento occidental, nela florece a filosofía e a ciencia grazas a unha longa lista de personaxes pensadores adicados á Ciencia e ás Matemáticas.

O pai de Teano era un rico patricio chamado Milón, que adicou parte da súa fortuna persoal ao mecenazgo, valorando o coñecemento das ciencias e das artes. Entre os protexidos de Milón estaba o filósofo e matemático Pitágoras, quen fundara a escola de Crotona.

Milón promulgaba unha corrente relixiosa coñecida como orfismo, que propoñía unha concepción innovadora do ser humano, composta por corpo e alma, influenciando así o pensamento de Teano.

A escola pitagórica

Os órficos adoptaron moitas das crenzas da mitoloxía exipcia, o que supuxo que Teano establecera un vínculo coa escola pitagórica, pois esta escola era coñecida pola aceptación dalgunha destas crenzas.

Cabe destacar que Pitágoras defendía a estrita selección dos seus alumnos, alegando que o coñecemento en "mans erradas"podería ser perigoso. A pesar diso, na súa escola non se opoñían á entrada de mulleres, sempre que se considerase que eran válidas para a aceptación e difusión das súas teorías.

O círculo de Pitágoras foi o primeiro coñecido no que as mulleres podían aprender e desenvolver o seu propio pensamento, pois naquela época, as mulleres estaban apartadas das actividades científicas. Era unha escola onde se estudaba con devoción e total liberdade de pensamento.

Milón envía a Teano a estudar á escola de Pitágoras, daquela había dezasete mulleres nela. Alí foi unha boa alumna e chegou a ser mestra. A súa xuventude e intelixencia non pasaron desapercibidas para Pitágoras, que se namorou dela.

Teano casou con Pitágoras, tiveron unha filla e dous fillos. A pesares das trabas que supuña a maternidade naqueles tempos, Teano non abandonou a escola.

Aportación científica e filosófica

Adicouse ao estudo da cosmoloxía, á redacción de tratados de matemáticas, física e medicina. Despois da morte de Pitágoras, continuou co seu traballo na escola e, xunto cos seus fillos, expandiu por toda Grecia a obra que Pitágoras iniciara.

Teano era unha firme defensora da orde e da harmonía non só nas matemáticas, senón en todos os aspectos da vida; sentía a necesidade de manter a tradición.

Na área de Matemáticas, desenvolveu as teorías pitagóricas relacionadas coa existencia de números naturais en todas as cousas e coa posibilidade de poder expresar numericamente a medida de calquera elemento da natureza.

Escribiu importantes tratados sobre matemáticas, filosofía, física, medicina e incluso cosmoloxía.

Unha pequena lenda

Conta a lenda que un discípulo novo de Pitágoras, fascinado pola matemática, preguntoulle pola idade da súa muller Teano. Pitágoras respondeulle: "*Teano é perfecta e a súa idade é un número perfecto*".

O alumno, quedando insatisfeito coa resposta, insistiu en pedir máis información.

Pitágoras respondeulle:

"*A idade de Teano, ademais de ser un número perfecto, é o número das súas extremidades multiplicado polo número dos seus admiradores, que é un número primo*".

Desta resposta xurdiu o coñecido *Problema Theaniano*, déixase como exercicio averiguar a idade de Teano naquel momento. Unha pista sería pensar en formular un sistema de ecuacións, e pensar como escribir a idade dende o número de admiradores de forma que se relacione cos seus divisores (propios).

Referencias

[1] Gleichauf, Ingeborg. (2019), *Mujeres filósofas en la historia.* ICARIA.

Teoría de Ramsey ou por que saímos de noite e vemos sempre á mesma xente

Carlos Cao López

Introdución.

A teoría de Ramsey é unha área das matemáticas sostida pola filosofía de que en calquer estructura suficientemente grande, existe unha subestructura que, dalgunha maneira, conserva certas propiedades. Por exemplo, se falamos de grafos, podemos considerar o conxunto de vértices (**Fig.1**) sen ningunha liña entre eles ou o conxunto de vértices con tódalas posibles liñas entre eles (de agora en adiante, ciclos). Isto, podemos abrevialo coa seguinte notación:

$$r(s,t)$$

onde s representa o cardinal do conxunto de puntos sen liñas e t o cardinal do conxunto de puntos que son parte dun ciclo. Un exemplo clásico é o de que en calquera festa con 6 persoas ou máis, polo menos 3 coñeceranse entre si, ou 3 non se coñecerán entre si. Desta forma, a resposta ao problema $r(3,3) = 6$. Como o espírito de todo matemático é, por natureza, inconformista, parece lóxico buscar solucións agora para $r(4,4)$, $r(5,5)$, $r(4,t)$... creo que pode verse por onde imos. Ben, pois se a resposta a $r(4,4)$ é 18, $r(5,5)$ segue sendo incerta, no pasado mes atopamos avances no conxetura sobre $r(4,t)$.

Avances en $r(4,t)$ tras (case) unha centuria.

Pero, por que é tan complicado de probar algo así se parece un xogo de combinatoria? Vexámolo cun exemplo, digamos que sabemos, grazas a certas cotas, que a resposta a $r(5,5)$ atópase entre 40 e 50. Con 45 vértices, o número de grafos posibles é maior que 10^{234}. Dados n vértices, o número de grafos simples ven dado pola fórmula

$$2^{\frac{n(n-1)}{2}} - \left(\begin{array}{c} \frac{n(n-1)}{2} \\ 0 \end{array} \right) - \left(\begin{array}{c} \frac{n(n-1)}{2} \\ n-1 \end{array} \right).$$

Non foi ata fai 4 anos, que os matemáticos Verstraete e Dhruv Mubayi descubriron que os grafos pseudoaleatorios poderían axudar ao avance desta antiga cuestión. Xa o gran Paul Erdös descubriu en 1937 que os grafos pseudoaleatorios poderían aportar boas cotas inferiores. Do que se decataron Verstraete e Mubayi, foi de que o muestreo de grafos pseudoaleatorios aportaba frecuentemente mellores cotas (a maxia da estatística!).

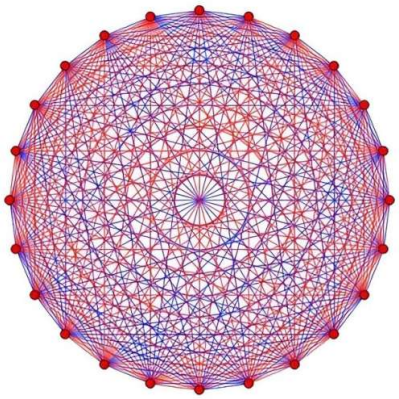


Fig. 1: Idea do grafo: escollemos os vértices nunha circunferencia e trazamos liñas entre eles.

Finalmente, coa axuda de Matheus, matemático especializado en xeometría finita, atoparon o grafo pseudoaleatorio que buscaban, e resulta que $r(4,t)$ está preto dunha función cúbica de t, máis concretamente,

$$r(4,t) = \Omega\left(\frac{t^3}{\log^4 t}\right) \quad \text{se } t \to \infty.$$

Co cual, a próxima vez que necesitedes saber cantas persoas son necesarias nunha festa para que 4 coñézanse entre sí e t non o fagan, podedes partir da nosa aproximación e, en base a iso, pensar como se vai desenvolver todo!

BIBLIOGRAFÍA

[1] Discusión de Quora “How do you calculate the number of possible simple graphs with n vertices?". Quora, https://www.quora.com/How-do-you-calculate-the-number-of-possible-simple-graphs-with-n-vertices, Consultado o 14 de novembro de 2023.

[2] Mattheus, S., Verstraete, J. "The asymptotics of r(4,t)". arXiv, preprint: 2306.04007 (2023), https://arxiv.org/pdf/2306.04007.pdf

[3] University of California - San Diego. "Math problem of the century solved". Phys.org, 31 de outubro de 2023, https://phys.org/news/2023-10-math-problem-century.html.

Retos Matemáticos

SEMENTEIRA

DESIGUALDADES DE MEDIAS

As medias son funcións que *mesturan* un conxunto de números. Aportan un valor intermedio, entre o máximo e o mínimo do mesmo. Dende o punto de vista da resolución de problemas, é tanto ou máis importante que as propias medias, a cadea de desigualdades que podemos establecer entre elas:

$$0 < \underbrace{\frac{n}{\frac{1}{x_1}+\frac{1}{x_2}+\cdots+\frac{1}{x_n}}}_{\text{Media harmónica (HM)}} \leq \underbrace{\sqrt[n]{x_1 x_2 \cdots x_n}}_{\text{Media xeométrica (GM)}} \leq \underbrace{\frac{x_1+x_2+\cdots+x_n}{n}}_{\text{Media aritmética (AM)}} \leq \underbrace{\sqrt{\frac{x_1^2+x_2^2+\cdots+x_n^2}{n}}}_{\text{Media cuadrática (QM)}}.$$

Estas desigualdades, pese a que non se adoitan traballar na carreira, aparecen en multitude de problemas. Vexamos un exemplo:

Exemplo. *Sexan $a,b,c \in \mathbb{Z}^+$ tal que $a+b+c=3$. Cales son os valores de a, b e c para que $a\cdot b\cdot c$ sexa máximo?*

Solución. Aplicaremos neste caso a desigualdade entre a media aritmética e a xeométrica (AM-GM):

$$\frac{a+b+c}{3} \geq \sqrt[3]{a\cdot b\cdot c}.$$

Disto deducimos que: $a\cdot b\cdot c \leq 1$, e como para $a=b=c=1$ se cumpre a igualdade, o máximo de $a\cdot b\cdot c$ acadarase cando a, b e c tomen o mesmo valor.

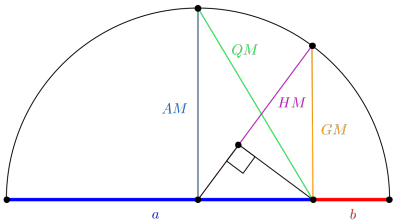
En xeral estas medias pódense deducir da fórmula xeralizada das medias:

$$M_p(x_1,\ldots,x_n) = \left(\frac{1}{n}\sum_{i=1}^{n} x_i^p\right)^{1/p}.$$

Onde para $p<q$, se dá a desigualdade:

$$M_p(x_1,\ldots,x_n) \leq M_q(x_1,\ldots,x_n).$$

Tamén é interesante sinalar que para o caso bidimensional, onde consideramos dous valores positivos a e b, as medias teñen a seguinte interpretación xeométrica:



Que ademais tamén aporta unha certa intuición ao sentido das distintas desigualdades. Rematamos esta sección deixando un exercicio proposto:

Exercicio. *Sexa $f:[0,1]\longrightarrow\mathbb{R}^+$ integrable e tales que $f(x)f(1-x)=1$ para todo $x\in[0,1]$. Probar que*

$$\int_0^1 f(x)dx \geq 1$$

Pista. Aplicar a desigualdade AM-GM ou a desigualdade de Cauchy-Schwarz.

PROBLEMAS PROPOSTOS

1. Algúns anos pódense expresar como sumas, restas e multiplicacións de números cun mesmo e único díxito, por exemplo:

   $$2009 = 7\times7\times7\times7-7\times7\times7-7\times7, \qquad 2010 = 66\times6\times6-66\times6+6\times6-6.$$

   Poderíase facer algo semellante co 2011 sen repetir sumandos iguais? (Por exemplo, non sería admisible: $2011 = 1+1+1+\ldots$). E para o 2023? De cantas formas?

2. Sexan en $\mathbb{R}^2$, 3 círculos de radio 1 que non se intersecan. Probar que o conxunto de puntos dos círculos que "non se ven" dende ningún dos outros dous ten lonxitude 2π.
   Un par de puntos (P,Q) das circunferencias "vense" cando o segmento $\overline{PQ}$ non pasa polo interior de ningunha das 3 circunferencias.

3. Atopar as solucións enteiras de:

   $$85^m - n^4 = 4.$$

Xa podedes consultar as solucións dos problemas propostos do mes pasado escaneando ou premento no seguinte QR:

O Teorema de Minkowski

Ibai Otero Gómez

Consideramos o grupo $\mathbb{Z}^2$ como subgrupo de $\mathbb{R}^2$. Esta distribución de puntos no plano coñécese como o retículo básico. A finais do século XIX, Minkowski fíxose a seguinte pregunta: se pinto un recinto no plano, cando podo asegurar que o meu debuxo conterá puntos de $\mathbb{Z}^2$?

Froito destas reflexións xorde en 1889 o Teorema de Minkowski que pretende responder a esta pregunta.

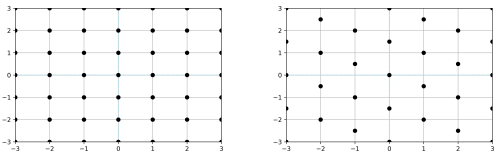


Fig. 1: Exemplos de retículos en $\mathbb{R}^2$.

Sen perda da xeralidade supoñamos que temos o noso recinto $\mathscr{S}$ centrado na orixe. Queremos atopar condicións para que esta figura interseque ao retículo básico, sen contar a orixe, por suposto. Comecemos pintando algunhas formas sinxelas. É doado ver que se pintamos un cadrado centrado na orixe e de lado estritamente menor ca dous, o conxunto non vai conter ningún punto de coordeadas enteiras. Polo tanto, parece razoable supoñer como condición que a área do conxunto debe ser maior ca 4: $\mathrm{A}(\mathscr{S})>4$.

Ademais, se facemos figuras raras que vaian rodeando aos puntos, podemos obter recintos de área arbitraria que non intersequen nunca o noso retículo. Polo tanto, imos engadir a maiores que o conxunto que consideremos sexa convexo[1]. Isto, ademais, facilítanos falar da condición sobre a área. A formalización precisa do que chamamos área ou volume non é un tema sinxelo en matemáticas, pero ao restrinxir a nosa atención a conxuntos convexos, descartamos unha morea de exemplos patolóxicos para os que quizais nin puidéramos falar do que entendemos por volume dun xeito razoable. Formalmente, dicimos que os conxuntos convexos son J-medibles, é dicir, que podemos aproximar a súa área pola suma de cadrados pequenos que os recubran.

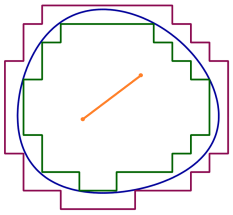


Fig. 2: Representación da medibilidade dos conxuntos convexos.

Se tratamos de pensar nun conxunto que cumpra as propiedades anteriores sen conter a ningún punto do retículo, vemos que é máis complicado. Non obstante, seguro que o lector consegue atopar algún contraexemplo ao noso intento de teorema. Cómpre engadir unha condición máis para asegurar que o conxunto conteña algún punto de $\mathbb{Z}^2$. Queremos que o conxunto estea dalgunha forma simetricamente repartido para que ningunha dirección sexa beneficiada e $\mathscr{S}$ poida "escapar" por aí. Isto podémolo formalizar dicindo que o conxunto ten que ser simétrico respecto á orixe ($x \in \mathscr{S} \Rightarrow -x \in \mathscr{S}$). Finalmente enunciamos o teorema:

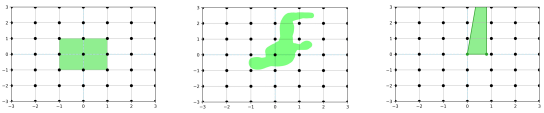


Fig. 3: Exemplos que amosan a necesidade das hipóteses do teorema.

Teorema 1. (de Minkowski) *Sexa $\mathscr{S}$ un subconxunto convexo de $\mathbb{R}^2$ simétrico respecto á orixe tal que $\mathrm{A}(\mathscr{S})>4$, entón $\mathscr{S}$ contén algún punto de $\mathbb{Z}^2$ distinto da orixe.*

Unha vez entendida a razón de ser de cada unha das hipóteses, o teorema parece case trivial. Non obstante, cómpre probalo para asegurarnos de que non se nos escapou ningún caso. A demostración procede recubrindo $\mathscr{S}$ en cadrados de área 4. Unha vez feito isto, desprazamos todos os cadrados á orixe e, pola condición da área, as rexións deben solaparse nalgún punto. A partir de aquí, é sinxelo atopar, usando as condicións de convexidade e simetría, que existe algún punto que cumpre o pedido.

Ademais de ser un problema moi interesante, ten importantes aplicacións en diversas áreas das matemáticas. En problemas de Teoría de Números, por exemplo, é de grande interese coñecer o número de puntos dun retículo xeral contidos nun certo recinto. Estes retículos poden codificar información de diferentes tipos. Atopar puntos en certos conxuntos pode probar entón moitos teoremas.

Exercicio: Definimos un retículo xeral en $\mathbb{R}^2$ como calquera retículo que pode ser obtido a partir do retículo básico mediante un cambio de base. É dicir, calesquera dous vectores independentes xeran un retículo[2]. Trátase de probar o teorema dos cadrados de Fermat:

Teorema 2. *Calquera primo $p \equiv 1 \pmod 4$ pode descompoñerse como suma de dous cadrados.*

Sexa p un primo congruente con 1 módulo 4.

a) Utiliza o determinante para xeralizar o teorema de Minkowski a retículos arbitrarios de $\mathbb{R}^2$.

b) Reordena os termos do teorema de Wilson para probar que existe un $i \in \mathbb{Z}/p\mathbb{Z}$ tal que $i^2 \equiv -1 \pmod p$.

c) Considera o retículo dado polos vectores $(1,i)$ e $(0,p)$ e o conxunto $\mathscr{S} := \{x \in \mathbb{R}^2 : \|x\|_2^2 < 2p\}$ e aplica o teorema de Minkowski para obter certo $x \in \mathbb{R}^2$.

d) Proba que p divide a $\|x\|_2^2$ e conclúe que $p = \|x\|_2^2$, demostrando o teorema.

Nota 1. *(Teorema de Wilson)* $p \in \mathbb{Z}$ é primo se e só se $(p-1)! \equiv -1 \pmod p$.

[1] É dicir, o segmento que une dous puntos sempre queda contida no recinto.

[2] Un retículo é un homomorfismo $\varphi : \mathbb{Z}^n \longrightarrow \mathbb{R}^n$ cuxa imaxe xera $\mathbb{R}^n$.

Introdución á modelización de algoritmos cuánticos: Parte I

Ignacio Garbayo Fernández

Dise que a computación cuántica vai substituír aos ordenadores tradicionais. Por iso, o propósito deste artigo é facer unha breve aproximación á teoría dos «ordenadores cuánticos» (ou **computación cuántica**) desde a súa perspectiva máis matemática, aplicable logo ao deseño e modelado de algoritmos para estas tecnoloxías.

Primeiro, imos construír o noso espazo de ***qubits*** (sistema cuántico), o análogo compositivo dos computadores cuánticos cos bits das máquinas tradicionales, que seguen o modelo de von Neumann. Tamén definiremos o concepto de **estado**, que establece comparativa cos 1 ou 0, que significan paso ou non de corrente eléctrica respectivamente, dos ordenadores actuais.

Preliminares

É conveniente lembrar os seguintes conceptos.

Definición 1 (**Espazo de Hilbert**). Un espazo con produto interior (S,p) dise que é un espazo de Hilbert se (S,d_p) é un espazo métrico completo, tomando d_p a distancia definida pola métrica e coas definicións de distancia e métrica habituais.

Ademais, denotaremos o produto tensorial de dous vectores φ e ψ como $\varphi\otimes\psi$. Sexa agora S un sistema cuántico.

Definición 2. O conxunto de estados dun sistema cuántico, $\mathscr{H}$, é un espazo de Hilbert sobre $\mathbb{C}$. Cada vector ou **estado** de S será un vector unitario de $\mathscr{H}$.

Como diciamos, o noso interese estará en establecer un sistema cuántico similar ao bit.

Definición 3 (**Qubit**). Un qubit é un sistema cuántico bidimensional.

Tomemos agora como sistema ambiente un qubit Q.
Q está dotado da **base computacional**, dada por:

$$\mathbf{0}=\begin{pmatrix}1\\0\end{pmatrix},\qquad \mathbf{1}=\begin{pmatrix}0\\1\end{pmatrix},$$

de tal forma que para todo $\varphi\in Q$, existen $\alpha,\beta\in\mathbb{C}$ tales que

$$\varphi=\alpha\,\mathbf{0}+\beta\,\mathbf{1}.$$

Estes escalares verifican a condición de normalización: $|\alpha|^2+|\beta|^2=1$. Deste xeito, podemos establecer a analoxía co modelo probabilístico **cuántico**, pois, combinando linealmente estes dous parámetros, atopámonos en $\mathbf{0}$ con probabilidade $|\alpha|^2$ e en $\mathbf{1}$ con probabilidade $|\beta|^2$.

Operacións

Sexa agora S un sistema cuántico formado por composición de qubits (tomamos varios).

Definición 4. Unha porta cuántica P é unha transformación unitaria de S.

Esta é a analoxía coherente coas portas lóxicas habituais, como o `NOT`, o `AND` ou o `XOR`. Un **exemplo** relevante das portas aplicadas a un só qubit é a **porta de Hadamard**:

$$\texttt{Had}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix},$$

sendo o seu efecto para a base computacional:

$$\texttt{Had}(\mathbf{0})=\frac{1}{\sqrt{2}}\left(\mathbf{0}+(-1)^0\,\mathbf{1}\right),$$
$$\texttt{Had}(\mathbf{1})=\frac{1}{\sqrt{2}}\left(\mathbf{0}+(-1)^1\,\mathbf{1}\right).$$

Esta transforma a base computacional en estados onde os seus elementos están combinados con mesma probabilidade.

Algoritmos

De forma similar que con computación actual, os problemas que se poden resolver poden ser clasificados segundo a súa complexidade (desta vez, complexidade cuántica); se ben este análise quedará para vindeiros números.

O noso obxectivo será introducir, en esta e seguintes publicacións, algúns dos algoritmos cuánticos de maior relevancia presente ou potencial. Neste caso, un **algoritmo cuántico** non será máis que unha sucesión finita de portas cuánticas aplicadas a un rexistro de n qubits. Presentamos a primeira cuestión:

Problema 1 (**HSP, do subgrupo oculto**). Dado G un grupo finitamente xerado, $K<G$ e X un conxunto finito, definimos $f:G\to X$ como $f(x)=f(y)$ se, e só se, $xK=yK$. Encontrar un subconxunto xerador de K sen coñecer f.

Definición 5 (**Porta oráculo**). Se $f:\{0,1\}^n\to\{0,1\}^m$ é unha aplicación, coñécese como porta oráculo de f a:

$$\texttt{O}_f:\mathbf{x}\otimes\mathbf{y}\to\mathbf{x}\otimes(\mathbf{y}\oplus f(\mathbf{x})),\quad \forall\mathbf{x}\in\{0,1\}^n,\mathbf{y}\in\{0,1\}^m.$$

O **algoritmo de Deutsch** emprega a porta oráculo para, no caso de $G=\{0,1\}$ coa operación $\oplus$ e $X=\{0,1\}$, realizar:

(1) `v = `$\mathbf{0}\otimes\mathbf{1}$ (2) `w = Had(v)`
(3) `z = `$\texttt{O}_f$`(w)` (4) `res = primerQubit[(Had`$\oplus I$`)(z)]`

Se `res`$=0$, $f(0)=f(1)$ e $K=\{0,1\}$; e se `res`$=1$, entón as imaxes son distintas e $K=\{0\}$. Pola extensión do artigo, déixase como exercicio a comprobación desta propiedade.

Próximos números

En vindeiras tiradas desenvolveremos o **algoritmo de Shor**, empregado para calcular á factorización única en producto de primos dun $N\in\mathbb{Z}$ (Teorema Fundamental da Aritmética), e de resolución a **problemas de búsqueda** en grandes conxuntos de datos.

Referencias

[1] Pastor Díaz, Ulises. *Algoritmos fundamentales en Computación Cuántica*. Do autor de *Toda computación, a la vez, en todas partes*, impartida o 6 de xuño de 2023 na Facultade de Matemáticas.

Dirección e Produción
Francisco Estévez Lengua

Sección Historia
Santiago González Gómez
Francisco Estévez Lengua

Sección Teoría
Ignacio Garbayo Fernández
Ibai Otero Gómez

Sección Actualidade
Carlos Cao López

Sección Retos
Sementeira

AGRADECEMENTOS

A Carmen Rodríguez e a Rafael Muñoz pola súa implicación e desexo de mellora na revisión (lingüística e matemática).

Á Facultade de Matemáticas pola difusión.

Ás e aos lectores desta revista.

Revista Máis Mates
Número 2
Novembro de 2023