

PONTO FIXO

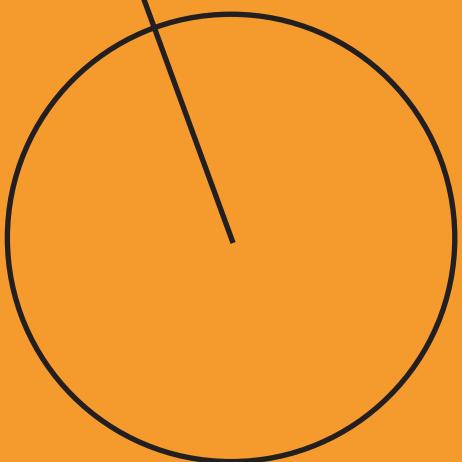
#5. EDIÇÃO 2025

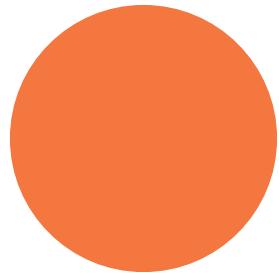
Matemática na Música

Medalhas Fields

Artigos de
professores e alunos

n{math}





Seja $f : X \rightarrow X$ uma função. Chama-se Ponto Fixo de f a todo o $x \in X$ tal que $f(x) = x$

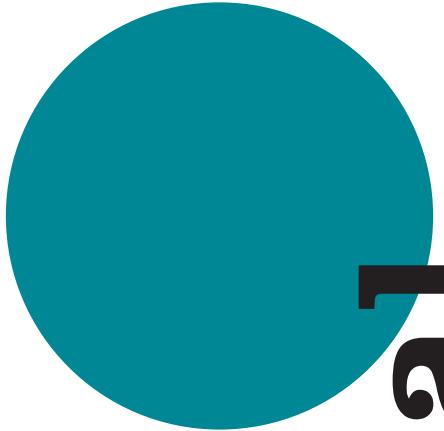
Índice

Parte I

A Matemática nos Instrumentos de Sopro	06
Maryna Viazovska	12
June Huh	14
Hugo Duminil-Copin	17
Intervalo	19

Parte II

Transformadas de Mellin e expansões assintóticas	21
Computação sobre dados privados com a Encriptação Homomórfica	25
Quantização Geométrica	28
Tirar o Doutoramento ou não: Eis a questão	32
Espetro de Dirac e Método das Soluções Fundamentais	38
Problema do Planeamento Probabilístico	42
Aliens Matemáticos	45
Operadores de Toeplitz e Métodos de Aproximação	49
O Jogo da Imitação	52



Após um interregno de 2 anos, *habemus* Ponto Fixo!

Qualquer edição de um jornal que fosse publicada dois anos após ter sido escrita correria o risco de perder o interesse para o público. Felizmente (para nós), a Matemática sobrevive ao teste do tempo, pois é um tópico quase intemporal, e acreditamos que esta 5.^a edição tem hoje o mesmo valor que teria há dois anos.

No fundo, para contar melhor a história, esta edição é como um bolo com muitas camadas, que começou a ser confeccionado há dois anos. Entretanto, novos pasteleiros acrescentaram mais algumas camadas, decoraram o bolo com uma belíssima cobertura, e acrescentam agora uma cereja no topo, celebrando esta edição finalizada.

A Revista conta com textos sobre três das quatro medalhas Fields atribuídas em 2022 (o texto sobre a 4.^a medalha Fields fica como exercício para o leitor), textos de alunos e uma crítica cinematográfica.

Conta também com duas entrevistas a (ex-)alunos, que pretendem ajudar a responder a “Tirar o doutoramento ou não, eis a questão”. Numa altura em que cada vez é exigido um grau académico maior, o mestrado parece ser o mínimo que é esperado, e o doutoramento já não é necessariamente apenas para quem pretende seguir uma carreira académica.

Num ano marcado por novidades do NMATH - o Time2Talk e o Integration Bee -, o Ponto Fixo é uma tradição que espero ver preservada daqui em diante, por estimular a conversa sobre diferentes tópicos (matemáticos e não só), dar voz aos alunos e professores, proporcionar uma pausa da azáfama das avaliações, e relembrar cada um do que o levou a escolher a Matemática.

Não obstante, o Ponto Fixo é uma revista que se destina a qualquer mente curiosa, não só para alunos de Matemática. Seja para desfrutar dos jogos, só para folhear, ou ler do início ao fim, todos são bem-vindos!

Termino deixando o meu maior agradecimento a todos os que contribuíram para o desenvolvimento desta edição, que prova que o espírito de partilha e busca de conhecimento continua vivo - e nunca deve parar -, mas depende de cada um de nós mantê-lo em movimento.

Boas leituras a todos!

Diana Morouço Gaspar

$$\text{maio de } 45^2 = 1^3 + 2^3 + 3^3 + 4^3 + 5^3 + 6^3 + 7^3 + 8^3 + 9^3$$



A Matemática nos Instrumentos de Sopro

Por: João Camarneiro

A música é uma forma de arte que tem acompanhado o ser humano desde tempos primordiais. Tomando forma através dos mais variados instrumentos, está presente em múltiplas vertentes das nossas vidas. Neste artigo, iremos ver como a matemática nos pode ajudar a compreender a música, mais concretamente a prever e explicar as diferenças que ouvimos entre diferentes instrumentos de sopro.

O Som

Para analisar um instrumento musical, é necessário antes de mais compreender a propagação do som e modelá-la matematicamente. O som resulta de uma oscilação das partículas do ar que é transmitida desde uma fonte até aos nossos ouvidos, através de ondas sonoras. Esta propagação pode ser estudada do ponto de vista da física, com base nos princípios da mecânica de fluidos. Acontece que a pressão acústica p (i.e. a variação de pressão do ar devida à propagação de som) satisfaz uma equação diferencial parcial (EDP):¹

$$\frac{\partial^2 p}{\partial x^2} + \frac{\partial^2 p}{\partial y^2} + \frac{\partial^2 p}{\partial z^2} = \frac{1}{c^2} \frac{\partial^2 p}{\partial t^2}$$

onde c é a velocidade do som no ar. Esta equação é conhecida como a equação das ondas, e surge como modelo de variadas situações relacionadas com fenómenos ondulatórios. Esta é uma das EDPs mais importantes e estudadas da matemática, sendo um exemplo representativo da classe das EDPs hiperbólicas.

Assim, para compreender a propagação do som e o funcionamento de instrumentos musicais, devemos estudar as soluções desta EDP. Isto pode não parecer um cenário muito agradável: em geral, resolver EDPs explicitamente é uma tarefa bastante difícil ou mesmo impossível! Apesar disto, nos casos que nos interessam aqui, veremos que é possível obter algumas soluções explícitas.

¹ Naturalmente, trata-se apenas de uma aproximação, que não reflete completamente a realidade, mas é consideravelmente próxima na maioria das situações. Os interessados podem consultar mais detalhes sobre esta análise no Capítulo I de Allan D. Pierce, *Acoustics. An Introduction to Its Physical Principles and Applications*, 3^a edição, Springer Cham, 2019.

Exemplos

Vamos considerar três exemplos de instrumento de sopro: a flauta, o clarinete e o oboé. Para cada um deles, veremos como as respetivas características geométricas constringem os tipos de soluções da equação das ondas, e como estas diferenças matemáticas se traduzem do ponto de vista musical.

Flauta

A flauta é um instrumento que pode ser idealizado como um tubo cilíndrico, aberto em ambas as extremidades. Devido às simetrias presentes, podemos considerar a hipótese simplificadora de que a pressão acústica no interior do tubo é constante em cada secção transversal, i.e. a pressão depende apenas da variável espacial associada ao comprimento do tubo. Na linguagem da física, isto corresponde a uma onda plana. A equação das ondas reduz-se, assim, à versão unidimensional, que é consideravelmente mais tratável:

$$\frac{\partial^2 p}{\partial x^2} = \frac{1}{c^2} \frac{\partial^2 p}{\partial t^2}$$

Aqui, podemos considerar que a pressão acústica $p(x, t)$ está definida para $x \in [0, L]$ e $t \in \mathbb{R}$, onde denotamos por L o comprimento da flauta.

A geometria do instrumento impõe ainda duas condições de fronteira nas extremidades: como estão em contacto com o ar exterior, a pressão nestes pontos é forçosamente igual à pressão de equilíbrio, $p(0, t) = p(L, t) = 0$.

Estamos agora prontos para procurar soluções da equação. Iremos utilizar o método de separação de variáveis, que consiste em procurar soluções da forma $p(x, t) = X(x)T(t)$. Do ponto de vista matemático, isto é apenas uma tentativa de adivinhar a solução que, à partida, não teria razão para funcionar, mas a física diz-nos que é expectável encontrar soluções desta forma. Substituindo a adivinha na equação, obtém-se:

$$X''(x)T(t) = \frac{1}{c^2}X(x)T''(t) \iff \frac{X''}{X} = \frac{T''}{c^2 T}$$

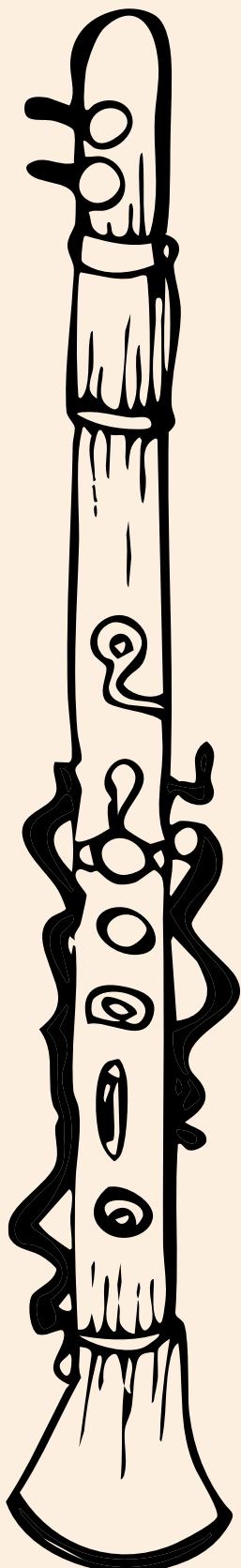
Um dos membros da equação depende apenas de x , enquanto o outro depende apenas de t . Isto implica que ambos os membros são na verdade iguais a uma constante k . Obtemos assim duas equações simultâneas:

$$\begin{cases} X''(x) = kX(x) \\ T''(t) = kc^2 T(t) \end{cases}$$

Estas são equações diferenciais ordinárias, que sabemos resolver explicitamente. A natureza das soluções depende do caráter positivo, negativo ou nulo da constante k . O leitor pode verificar que, se a constante k for positiva ou nula, a equação para X conjugada com as condições fronteira,

$$\begin{cases} X''(x) = kX(x) \\ X(0) = X(L) = 0 \end{cases}$$

tem apenas a solução identicamente nula $X = 0$.



Portanto, para obter soluções não triviais, devemos considerar k negativo. Nesse caso, seja $k = -\omega^2$. Sabemos que as soluções de $X'' = -\omega^2 X$ são da forma:

$$X(x) = a \sin(\omega x) + b \cos(\omega x),$$

onde a, b são constantes reais. Temos ainda de impor as condições de fronteira:

$$X(0) = b = 0, X(L) = a \sin(\omega L) = 0$$

Isto implica que a constante ω pode apenas tomar valores da forma $\omega = \frac{n\pi}{L}$ com n inteiro. Em conclusão, obtemos que:

$$X(x) = a \sin\left(\frac{n\pi x}{L}\right)$$

Para cada um destes valores de ω , a equação $T'' = -\omega^2 c^2 T$ pode também ser resolvida:

$$T(t) = A_n \sin\left(\frac{n\pi ct}{L}\right) + B_n \cos\left(\frac{n\pi ct}{L}\right).$$

Em conclusão, encontrámos para cada inteiro n uma solução dada por:

$$p_n(x, t) = \sin\left(\frac{n\pi x}{L}\right) \left(A_n \sin\left(\frac{n\pi ct}{L}\right) + B_n \cos\left(\frac{n\pi ct}{L}\right) \right).$$

Musicalmente, esta solução corresponde a um som puro com frequência² $f_n = \frac{nc}{2L}$. Na realidade, ao tocar uma flauta de comprimento L , não iremos ouvir uma destas soluções isoladamente, mas sim uma combinação de todas elas. A frequência $f_1 = \frac{c}{2L}$ é a frequência fundamental e corresponde à nota que o nosso ouvido perceciona. Em geral, a frequência f_n designa-se por n -ésimo harmónico, e a presença destas frequências mais elevadas enriquece e complexifica o som. É a proporção entre a fundamental e os vários harmónicos que confere aos instrumentos o seu timbre, a sua sonoridade característica que nos permite distingui-los uns dos outros.

Vimos assim que um tubo aberto, como a flauta, emite um som com frequência fundamental de $f = \frac{c}{2L}$, sendo L o comprimento do tubo, e com presença de todos os seus harmónicos, i.e. as frequências nf com n inteiro positivo.

Por esta altura, o leitor poderá estar a questionar-se, e bem, pois as flautas que conhece conseguem tocar mais do que uma nota. Isto é devido à possibilidade de abrir ou fechar orifícios na flauta, que efetivamente altera o comprimento acústico do instrumento, permitindo controlar e variar a nota que é emitida. Segundo a fórmula que obtivemos, quanto menor o comprimento do tubo, mais alta será a frequência, originando uma nota mais aguda.

² Recorda que a frequência f e a frequência angular ω satisfazem $\omega = 2\pi f$.

Clarinete

Atentemos agora no clarinete. À primeira vista, pode parecer praticamente idêntico à flauta, podendo também ser modelado como um tubo cilíndrico. Porém, o mecanismo de produção de som tem uma diferença importante. Num clarinete, a extremidade tocada pelo instrumentista está bloqueada por uma pequena peça de madeira, a *palheta*. O ar no interior do tubo não é posto em vibração diretamente através do sopro, mas sim através da vibração da palheta contra o bocal do clarinete. Assim, o clarinete é idealizado como um tubo cilíndrico com uma extremidade aberta e a outra fechada (que se designa neste contexto apenas por *tubo fechado*).

Do ponto de vista matemático, esta diferença altera as condições de fronteira que devemos impor à equação das ondas. Na extremidade aberta, continuamos a ter $p(L, t) = 0$. Já na extremidade fechada, a condição de fronteira passa a ser $\frac{\partial p}{\partial x}(0, t) = 0$, i.e. $x = 0$ é sempre um ponto de extremo local da pressão (maximizante ou minimizante).

Aplicamos novamente o método de separação de variáveis. Não repetimos todos os pormenores, mas destacamos apenas os pontos em que surgem diferenças. Assim sendo, temos

$$X(x) = a \sin(\omega x) + b \cos(\omega x)$$

mas, impondo as novas condições de fronteira, vem

$$X'(0) = \omega a = 0, \quad X(L) = b \cos(\omega L) = 0.$$

Neste caso, n pode tomar valores da forma $\omega = \frac{(2n+1)\pi}{2L}$, com n inteiro. No fim, obtemos para cada n uma solução dada por

$$p_n(x, t) = \cos\left(\frac{(2n+1)\pi x}{2L}\right) \left(A_n \sin\left(\frac{(2n+1)\pi c t}{2L}\right) + B_n \cos\left(\frac{(2n+1)\pi c t}{2L}\right) \right).$$

Concluímos que um tubo fechado, como o clarinete, emite um som com frequência fundamental de $f = \frac{c}{4L}$, sendo L o comprimento do tubo. Note-se que isto é metade da frequência fundamental emitida por uma flauta com o mesmo comprimento! Traduzindo para música, isto significa que um clarinete soa uma oitava mais grave do que uma flauta com o mesmo comprimento. Além disso, estão apenas presentes os harmónicos ímpares, devido ao fator $2n+1$. É esta característica que dá ao clarinete a sua sonoridade mais suave, mas menos brilhante.

Oboé

Para terminar, analisemos o caso do oboé. Tal como o clarinete, é um instrumento de palheta, sendo portanto modelado por um tubo fechado. Contudo, ao contrário da flauta e do clarinete, que são instrumentos cilíndricos, o oboé tem um formato ligeiramente cónico. Este facto faz com que devamos considerar não ondas planas como até agora, mas ondas esféricas, onde imaginamos o cone contido numa esfera centrada no bocal. Mudando para coordenadas esféricas, a equação das ondas toma a forma

$$\frac{1}{r} \frac{\partial^2}{\partial r^2} (rf) + \frac{1}{r^2 \sin \theta} \frac{\partial}{\partial \theta} \left(\sin \theta \frac{\partial f}{\partial \theta} \right) + \frac{1}{r^2 \sin^2 \theta} \frac{\partial^2 f}{\partial \varphi^2} - \frac{1}{c^2} \frac{\partial^2 p}{\partial t^2}.$$

A hipótese de ondas esféricas implica que p não tem dependência nas variáveis θ, φ , simplificando a equação:

$$\frac{1}{r} \frac{\partial^2}{\partial r^2} (rf) = \frac{1}{c^2} \frac{\partial^2 p}{\partial t^2} \Leftrightarrow \frac{\partial^2}{\partial r^2} (rp) = \frac{1}{c^2} \frac{\partial^2}{\partial t^2} (rp).$$

Assim, concluímos que a função $\varphi(r, t) = r p(r, t)$ satisfaz uma equação de onda unidimensional, que pode ser resolvida como nos casos anteriores.

Falta apenas estabelecer as condições de fronteira. Naturalmente, $\varphi(0, t) = 0$ por definição. Estando o tubo aberto na extremidade oposta, e denotando por L o comprimento do instrumento, temos como antes que $\varphi(L, t) = 0$. Prosseguindo novamente pelo método de separação de variáveis, obtemos soluções da forma

$$p_n(r, t) = \frac{1}{r} \sin\left(\frac{n\pi r}{L}\right) \left(A_n \cos\left(\frac{n\pi c t}{L}\right) + B_n \sin\left(\frac{n\pi c t}{L}\right) \right).$$

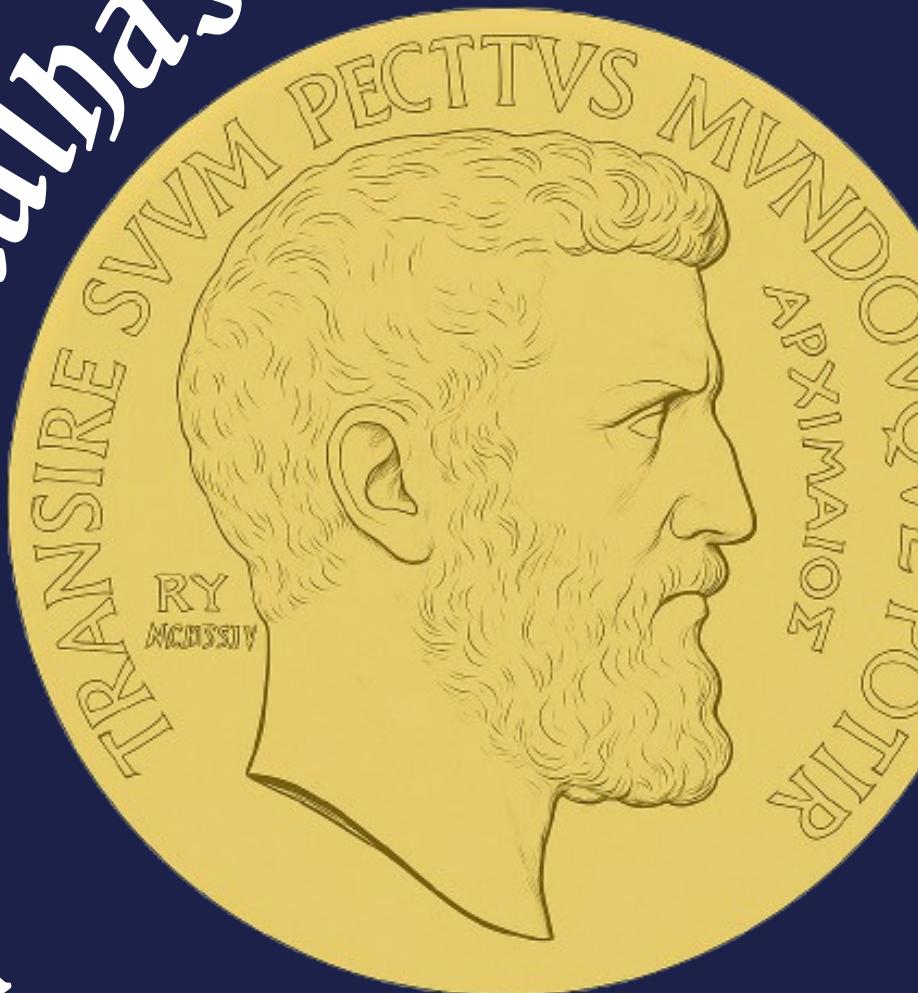
Note-se que a solução é praticamente idêntica ao caso da flauta, com a exceção do fator de $\frac{1}{r}$. Isto mostra que um oboé tem a mesma frequência fundamental que uma flauta com o mesmo tamanho, que é o dobro, ou uma oitava acima, relativamente a um clarinete com o mesmo tamanho. Além disto, estão novamente presentes todos os harmónicos, e não apenas os ímpares. Esta propriedade explica a sonoridade mais bri-lhante do oboé, em comparação com a do clarinete.

Coda

Apesar de todos os instrumentos que vimos serem descritos pela mesma EDP, as suas diferentes propriedades geométricas influenciam fortemente o caráter das respetivas soluções. Estas diferenças matemáticas traduzem e explicam as características sonoras e musicais que distinguem estes instrumentos.

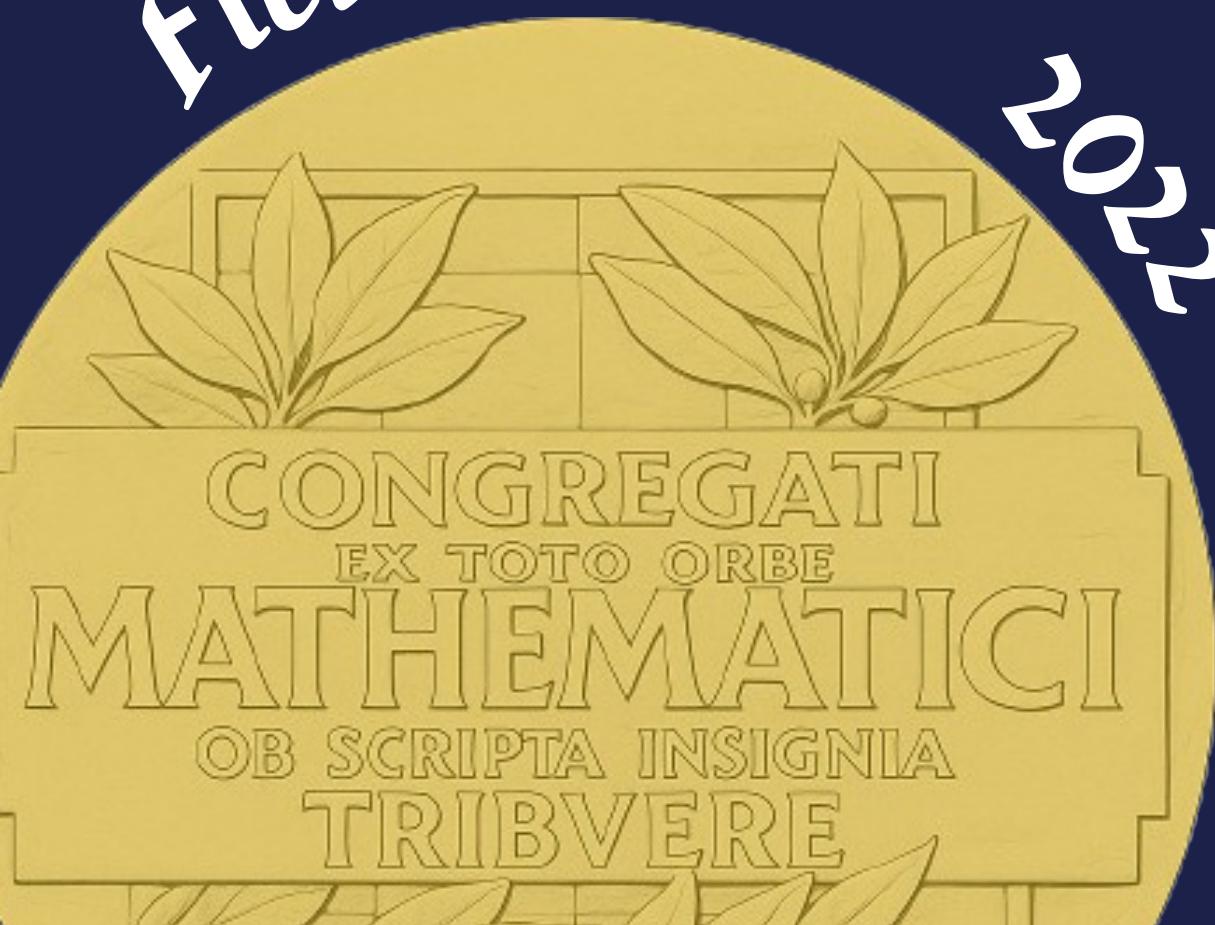
Claro está que tudo isto é uma simplificação da realidade. A equação das ondas, apesar de ser uma descrição bastante satisfatória dos fenómenos sonoros, não deixa de ser apenas uma aproximação, que tem os seus limites. Além disso, os instrumentos que considerámos têm outros modos de vibração além de ondas planas/esféricas, que são mais complexos de descrever, mas contribuem para a sua complexidade musical e tímbrica. No entanto, tudo isto não deixa de ser uma demonstração da grande versatilidade das EDPs enquanto modelos matemáticos, e da riqueza da respetiva teoria.

medallas



Fields

2022



Maryna Viazovska, Medalha Fields em \mathbb{R}^8

Por: Diogo Oliveira e Silva

O hiperespaço existe mesmo? Claro que sim – uma mensagem pode ser codificada por um vetor no espaço euclidiano d -dimensional. Se enviarmos uma mensagem $m \in \mathbb{R}^d$ que é recebida como m^* no outro extremo do canal de comunicação, em geral m^* difere de m uma vez que qualquer canal tem sempre um certo ruído associado. Se o canal tiver um nível de ruído $\varepsilon > 0$ e se m^* não distar de m mais do que ε , então faz sentido pensar na esfera de erro de raio ε centrada em cada mensagem m enviada. Para que a comunicação se faça sem erros, pode fixar-se à partida um dicionário finito $\{m_1, m_2, \dots, m_N\}$ de mensagens permitidas. Se as mensagens m_j e m_k estiverem demasiado próximas para alguns $j \neq k$, então as mensagens recebidas poder-se-ão confundir. Isto evita-se garantindo que todas as mensagens distam umas das outras pelo menos 2ε , por forma a que esferas de erro distintas não se intersectem. As esferas de erro formam assim um empacotamento esférico e, por uma questão de eficiência, queremos maximizar a densidade do empacotamento. Eis-nos chegados ao problema do empacotamento esférico, formulado em tempos imemoriais, mas cuja solução só era conhecida em dimensões $d \in \{1, 2, 3\}$ até há sete anos atrás.

Enter Maryna Sergiivna Viazovska. Trata-se de uma matemática ucraniana nascida em Kiev a 2 de dezembro de 1984, formada na Ucrânia (Kiev) e na Alemanha (Kaiserslautern, Bonn, Berlim) e que, depois de uma breve passagem pelos EUA (Princeton), ocupa atualmente a cátedra de Teoria dos Números na École Polytechnique Fédérale de Lausanne, na Suíça. A 14 de março (π -day) de 2016, Viazovska divulgou no arXiv a solução do problema do empacotamento esférico em \mathbb{R}^8 [9] que de um dia para o outro tornou numa celebridade matemática mundial [12, 13]. Uma semana depois, Viazovska e quatro colaboradores (Henry Cohn, Abhinav Kumar, Stephen Miller e Danylo Radchenko) anunciaram a solução do problema do empacotamento esférico em \mathbb{R}^{24} [3]. A história fascinante deste problema e algumas das ideias que possibilitaram a sua solução em dimensões 8 e 24, incluindo a caça épica à função mágica, são



abordadas em [1, 2, 6, 7, 10], e também no artigo [8] que apareceu na última edição do Ponto Fixo.

Ao êxito retumbante de Viazovska seguiu-se uma lista de cardinalidade considerável de prémios e distinções ao mais alto nível: Salem Prize (2016), Clay Research Award (2017), SASTRA Ramanujan Prize (2017), New Horizons Prize in Mathematics (2018), ICM Invited Speaker (2018), Ruth Lytle Satter Prize in Mathematics (2019), Fermat Prize (2019), EMS Prize (2020), National Latsis Prize (2020), Academia Europaea (2021), Senior Scholar at the Clay Mathematics Institute (2022), BBC 100 Women (2022). A cereja no topo do bolo chegou sob a forma da medalha Fields, que já se adivinhava desde 2018 e que foi atribuída a Viazovska no International Congress of Mathematicians (ICM) de 2022, em Helsínquia [11, 15]. A laudatio por Henry Cohn [2] começa do seguinte modo:

“On July 5th, 2022, Maryna Viazovska was awarded a Fields Medal for her solution of the sphere packing problem in eight dimensions, as well as further contributions to related extremal problems and interpolation problems in Fourier analysis.”

Viazovska tornou-se assim na segunda mulher a receber a mais alta distinção matemática desde que foi instituída em 1936 (a primeira tinha sido a matemática iraniana Maryam Mirzakhani em 2014). No ICM, Viazovska proferiu a palestra “Magic functions illuminate the mysteries of extremal geometry” que está disponível no YouTube [16] a partir de 6:46:15.

Nas palavras de Tom Hales¹ [14], “the fireworks have not stopped”. A equipa Cohn–Kumar–Miller–Radchenko–Viazovska (CKMRV) saiu dos projetos [3, 9] com uma visão, segundo a qual os métodos utilizados na solução do problema do empacotamento esférico em 8 e 24 dimensões deveriam funcionar em contextos mais gerais. E, de facto, em 2019 anunciaram uma prova [4] de que o reticulado E_8 e o reticulado de Leech são “universalmente ótimos” em \mathbb{R}^8 e \mathbb{R}^{24} . Quer isto dizer que são soluções de uma classe de problemas que inclui o empacotamento esférico como caso (muito) particular, resolvendo também outras questões prementes da física matemática formuladas em termos de forças de repulsão completamente monótonas, como as interações de Coulomb ou de Gauß. Pelo caminho, a equipa CKMRV descobriu um número infinito de funções mágicas, em bijeção com o conjunto de potenciais admissíveis, o que ao mesmo tempo demonstra a delicadeza da construção e revela uma razão mais conceptual para a existência e o poder da função mágica original de Viazovska. Que outras surpresas virão das dimensões 8 e 24?

Referências

- [1] Cohn, H. (2017). A conceptual breakthrough in sphere packing. *Notices of the American Mathematical Society*, 64(2), 102–115.
- [2] Cohn, H. (2022). The work of Maryna Viazovska. *Proceedings of the International Congress of Mathematicians* (Vol. I).
- [3] Cohn, H., Kumar, A., Miller, S., Radchenko, D., & Viazovska, M. (2017). The sphere packing problem in dimension 24. *Annals of Mathematics*, 185(3), 1017–1033.
- [4] Cohn, H., Kumar, A., Miller, S., Radchenko, D., & Viazovska, M. (2022). Universal optimality of the E_8 and Leech lattices and interpolation formulas. *Annals of Mathematics*, 196(3), 983–1082.
- [5] Hales, T. C. (2005). A proof of the Kepler conjecture. *Annals of Mathematics*, 162(3), 1065–1185.
- [6] Oesterlé, J. (2017). Densité maximale des empilements de sphères en dimensions 8 et 24. *Séminaire Bourbaki*, 69^e année, Exp. No. 1133, 455–478.
- [7] Okounkov, A. (2022). The magic of 8 and 24. In *Proceedings of the International Congress of Mathematicians* (Vol. I), 492–545.
- [8] Oliveira e Silva, D. (2022). Empacotamentos esféricos e o princípio da incerteza do sinal. Ponto Fixo, 4^a. edição.
- [9] Viazovska, M. S. (2017). The sphere packing problem in dimension 8. *Annals of Mathematics*, 185(3), 991–1015.
- [10] Viazovska, M. (2021). Almost impossible E_8 and Leech lattices. *European Mathematical Society Magazine*, 121, 4–8.
- [11] Chang, K. (2022). Maryna Viazovska: Second to none in any dimension. *The New York Times*. <https://www.nytimes.com/2022/07/05/science/maryna-viazovska-math.html>.
- [12] Thomson, H. (2016). New maths proof shows how to stack oranges in 24 dimensions. *New Scientist*. <https://www.newscientist.com/article/2082328-new-maths-proof-shows-how-to-stack-oranges-in-24-dimensions/>.
- [13] Castelvecchi, D. (2016). Sphere packing solved in higher dimensions. *Quanta Magazine*. <https://www.quantamagazine.org/sphere-packing-solved-in-higher-dimensions-20160330/>
- [14] Wolchover, N. (2019). Out of a magic math function, one solution to rule them all. *Quanta Magazine*. <https://www.quantamagazine.org/universal-math-solutions-in-dimensions-8-and-24-20190513/>
- [15] Wolchover, N. (2022). In times of scarcity, war and peace, a Ukrainian finds the magic in math. *Quanta Magazine*. <https://www.quantamagazine.org/ukrainian-mathematician-maryna-viazovska-wins-fields-medal-20220705/>
- [16] International Mathematical Union (2022). *The International Congress of Mathematicians 2022 (ICM 2022)*. YouTube. <https://www.youtube.com/watch?v=Uh2gqiEC6eM>

¹ Que em 1998 tinha resolvido o problema do empacotamento esférico em \mathbb{R}^3

June Huh, Medalha Fields em Combinatória Algébrica

Por: Raúl Penaguião

Num percurso habitual de um curso de Matemática, a influência que a Combinatória tem não se estende muito além da teoria de grafos e aplicações básicas em probabilidades. Mesmo considerando os cursos mais inclinados para as áreas puras, a aprendizagem de Combinatória contracena com tópicos adjacentes - geralmente algoritmia ou programação linear - em vez de tomar uma posição central. Isto reflete o que se passa no mundo de investigação matemática atual. Vamos andar um pouco para trás para contar a história do que poderá vir a ser identificado como a emergência de combinatoria nos cursos de matemática nas universidades.

Os temas lecionados em cursos de Matemática numa universidade é influenciado, em geral, pelo que é feito em investigação nessa mesma universidade. Estudantes da "La Sapienza" serão sempre premiados por geometria algébrica, alunos de licenciatura em Berkeley terão de saber calcular bases de Gröbner de um ideal como qualquer estudante sabe inverter matrizes, etc. De um ponto de vista empírico, os estudantes de Matemática da sua universidade mais próxima podem verificar isso e, a certo ponto, faz sentido: quem leciona as cadeiras de cursos de matemática são, de acordo com o modelo do século XX, investigadores de matemática. E é um facto que a investigação em Combinatória é rarefeita mesmo quando analisamos a evolução nos séculos passados.

Por exemplo, nenhum dos problemas do século de Hilbert ou problemas do Milénio pode ser classificado como combinatório. Um breve estudo das medalhas Fields revela que entre os 64 laureados há apenas cinco que se pode dizer que usem combinatoria na sua investigação (Timothy Gowers, Grigory Margulis, Terence Tao, Maryna Viazovska e June Huh). Considerando que um laureado se identifica, em média, com 4 áreas de matemática, isto revela que não há muitos matemáticos a tropeçar em teoremas combinatórios que interessem à comunidade. Um olhar atencioso para os resultados de

Timothy Gowers e Grigory Margulis revela que o contexto da combinatoria só se revela na estratégia das demonstrações. Eu teria escrito sobre Terence Tao se mo tivessem pedido, mas a história que vos vou contar hoje é sobre June Huh, e como no leito da investigação matemática pura emerge uma área insuspeita do saber matemático: a combinatoria algébrica.

June Huh é um matemático coreano-americano com uma entrada interessante na matemática, que escrevia poesia quando era criança. Na verdade, se lhe perguntassem na altura o que queria fazer quando fosse grande, a sua resposta seria poeta. Acabou por não terminar o ensino secundário para se focar na poesia, mas quando isso o aborreceu, a escrita em poesia tornou-se escrita sobre ciência e, pa-



ra tal inscreveu-se na universidade para aprender sobre astronomia. Seria aí que a matemática o ia apanhar. Curiosamente, foi outro laureado – Heisuke Hironaka – que despertou o interesse de Huh em seguir investigação em matemática, numa cadeira de geometria algébrica que se focava em teoria de singularidades. Tendo dificuldade em entrar numa universidade dos Estados Unidos, acabou por ser aceite num programa de doutoramento onde acabou por trabalhar no problema que o projetaria ao estrelato. Não teve, no entanto, o percurso habitual que matemáticos destinados ao estrelato têm. Federico Ardila, um matemático especialista em politopos e álgebras de Hopf, diz que quando descobriu que June Huh já tinha escrito poesia, disse: “pois, faz sentido, quando vocês o virem a escrever matemática vão perceber porquê”.

No seu doutoramento, em 2009, June Huh estabeleceu uma conjectura com, à data, 40 anos: Read's conjecture. Este é um problema de teoria de grafos relacionado com o polinómio cromático. Concretamente, se G for um grafo com vértices V , uma coloração do grafo com n cores é uma função $f : V \rightarrow \{1, \dots, n\}$ que satisfaz $f(v) \neq f(w)$ para vértices v, w que partilham uma aresta. Quantas colorações de um grafo G existem? Chamemos a esse número $\chi_G(n)$. Em termos práticos, contar o número de colorações de um grafo arbitrário é um problema difícil (é na verdade um dos 21 problemas originais que foram classificados como NP-completos, uma noção bastante aceite de “difícil”), mas este número satisfaz uma relação de recorrência: para qualquer aresta e do grafo temos

$$\chi_G(n) = \chi_{G \setminus e}(n) - \chi_{G/e}(n)$$

onde $G \setminus e$ é o grafo que resulta de remover a aresta e de G , e G/e é o grafo que resulta de contrair a aresta e , resultando num grafo com menos um vértice. É neste tipo de coisas que a combinatória pode ajudar. Usando esta recorrência, pode-se por exemplo calcular $\chi_G(n)$ para o grafo de Petersen (ver imagem), para o número de cores n genérico

$$\chi_G(n) = n^{10} - 15n^9 + 105n^8 - 455n^7 + 1353n^6 - 2861n^5 + 4275n^4 - 4305n^3 + 2606n^2 - 704n.$$

Desta forma, descobrimos que há zero colorações do grafo de Petersen com duas cores, mas há 120 colorações diferentes com três cores (conseguiste contá-las todas?). Mas... isto é um polinómio! Sim, sim, tinha-me esquecido de vos dizer, isto é um polinómio. Como é que sabemos isso? Na verdade, não é nenhum problema complicado. Por exemplo, pode-se usar a fórmula de recorrência apresentada acima para mostrar, por indução, que $\chi_G(n)$ é um polinómio para qualquer grafo G .

Quem gostar de numerologia já se entreve a observar que os coeficientes alternam de sinal. Isto é um facto que também pode ser provado usando a fórmula de recorrência. Para quem gosta de numerologia e de matemática, observa que o quadrado de qualquer dos coeficientes é sempre maior do que o produto dos números adjacentes. Sequências com esta propriedade chamam-se log-côncavas. A Conjectura de Read diz que os coeficientes do polinómio cromático de um grafo é sempre log-côncavo. As estratégias que foram tentadas nesta conjectura esgotaram as ferramentas dos matemáticos da altura.

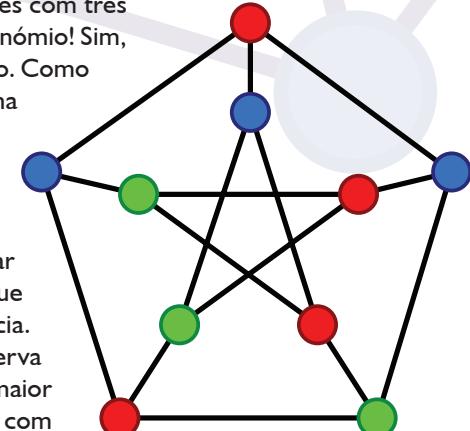


Figura 1: Grafo

Sequências log-côncavas ocorrem com alguma frequência em combinatória, e são normalmente uma indicação de que contam objetos familiares. Exemplos de sequências log-côncavas são as linhas do triângulo de Pascal que, curiosamente, contam o número de subconjuntos com uma certa cardinalidade. Sequências log-côncavas ocorrem também, por exemplo, no número de faces de um polítopo. Várias distribuições de probabilidades são log-côncavas, bem como a sequência de dimensões das cohomologias de uma variedade. Esta última é a relação que June Huh estabeleceu no seu doutoramento, de uma forma bastante engenhosa.

E para provar esta conjectura, Huh precisou de geometria. Especificamente, da “ventoinha de Bergman” de um grafo Σ_G . Um cone é o espaço gerado por combinações reais não-negativas de uma coleção finita de vetores. Uma ventoinha é uma coleção de cones em \mathbb{R}^n em que a interseção de quaisquer dois cones é uma face de cada um dos cones. Isto é um subespaço de \mathbb{R}^n que já foi estudado

em vários contextos, a realçar a geometria tropical.

A ideia de Huh foi estudar $C(G)$, o anel de funções polinomiais definidas só na ventoinha $f : \Sigma_G \rightarrow \mathbb{R}$. Qualquer polinómio $f : \mathbb{R}^n \rightarrow \mathbb{R}$ pode ser restrito a $C(G)$, mas também quaisquer funções polinomiais definidas em cada cone do moinho, desde que estas funções tomem o mesmo valor nas intersecções, é um elemento de $C(G)$. Este espaço $C(G)$ chama-se o anel de Chow. Como qualquer pessoa que estuda cohomologia de espaços algébricos pode confirmar, saber que funções polinomiais existem num espaço é como saber tudo sobre esse espaço. Fenómenos semelhantes acontecem noutras áreas: por exemplo em teoria de Hodge, equações diferenciais parciais são usadas para calcular a cohomologia de uma variedade. Na verdade, nos grafos a história é brilhante: os coeficientes de $\chi_G(n)$ estão diretamente relacionados com a dimensão das diferentes cohomologias de $C(G)$. A relação de log-concavidade é provada se Huh consegu

uir exibir um ciclo que se chama um elemento duro de Lefschetz do anel $C(G)$. E as consequências desta demonstração estendem-se além da prova da Conjectura de Read. A ideia de usar teoria de Hodge na Combinatória abriu as portas a uma extensa colaboração de Huh com Adiprasito e Katz, que generalizou o resultado a Matroides, uma extensão da noção de grafos, e que capturaram a noção de independência de vetores. A maior parte das Matroides não têm nenhuma geometria associada, pelo que o estudo de cohomologias em Matroides é consideravelmente novo e prova a mais geral Conjectura de Read. Isto deixou investigadores entusiasmados em encontrar anéis de funções polinomiais nos seus objetos favoritos. Por fim, deve também de ser realçado que a Conjectura de Read estava aberta há 40 anos sem nenhum progresso parcial e com pouca atividade na sua área. E assim, aos 32 anos, Huh encontrou na matemática a beleza que procurou na poesia. Num elemento duro de Lefschetz.

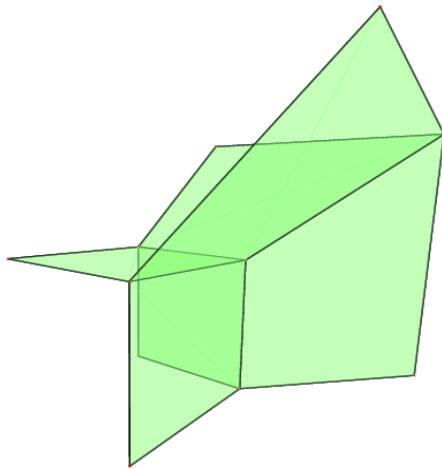


Figura 2: Ventoinha de Bergman

Referências

- [1] Wikipedia contributors. Petersen graph 3-coloring [Imagen]. Wikipedia. https://en.wikipedia.org/wiki/Graph_coloring#/media/File:Petersen_graph_3-coloring.svg
- [2] ResearchGate. Bergman fan of the $U_{3,4}$ matroid [Imagen]. https://www.researchgate.net/figure/Bergman-fan-of-the-U-3-4-matroid_fig2_356841692

Hugo Duminil-Copin,

Medalha Fields em Física Matemática

Por: Jean-Claude Zambrini

Hugo Duminil-Copin, professor no Dep. de Matemática da Universidade de Genève (e no IHES) obteve aos 36 anos a medalha Fields durante o recente Congresso internacional de matemática, em Helsínquia. Hugo DC é um físico-matemático que trabalha em teoria das probabilidades. Um daqueles que, durante os vinte últimos anos, regressou à fonte histórica de inspiração das matemáticas, a física teórica (após uma geração que tinha ignorado esta herança). Para Hugo DC, foi a teoria das transições de fase, em mecânica estatística, a desempenhar esse papel.

Quando um líquido tenta encontrar um caminho num meio poroso, o modelo matemático deve explicar a formação de grupos conexos das configurações que formam os caminhos, e seus comportamentos. É a teoria da Percolação, cujo sistema modelo é uma grelha infinita de configurações ligadas por arestas. Sobre cada uma delas, atirar uma moeda ao ar e escolher uma probabilidade que ela caia na face (a moeda pode estar enviesada, as probabilidades não serem só 1/2). Nesse caso, a aresta é colorida e o fluido pode passar entre esses dois pontos, se não fica bloqueado. Aumentando lentamente a probabilidade que todos os pares de pontos sejam ligados, observa-se uma transição de fase brutal do comportamento do sistema. Esta probabilidade crítica está no centro da teoria: abaixo dela não haverá quase nenhuma possibilidade de aparecer um caminho conectado infinitamente longo, acima haverá um caminho disponível: o fluido escorrerá. O mais simples modelo de percolação é o dito de Bernoulli, descrito acima. O programa de investigação de Hugo DC consiste em generalizar estas ideias a modelos bem mais sofisticados (sendo o segundo, em termos de dificuldade, o famoso modelo de Ising).

Hugo DC admite de boa vontade que duvida muito tempo das suas provas. Em matemática, ao contrário da física, uma certeza absoluta é acessível. Mesmo hesitando, como aluno, entre matemática e física, e defensor do papel da intuição, ele não poderia satisfazer-se completamente com argumentos físicos. No seu domínio, os físicos tinham previsto os seus resultados mas



as verificações semi-empíricas não o satisfaziam. Torna-se portanto matemático. O primeiro resultado, que valeu a Hugo DC a posição de professor em Genève, no mesmo dia da sua defesa de tese, foi obtido com o seu orientador, S. Smirnov. Numa rede hexagonal (em ninho de abelhas) devia calcular-se o número de caminhos que não voltam nunca ao mesmo vértice. Se N é o número de passos no caminho, este número é:

$$\left(\sqrt{2 + \sqrt{2}}\right)^N$$

A hipótese de lançamentos independentes de Bernoulli pode ser substituída pela de correlações entre partes distantes do sistema. Para uma larga classe de tais modelos, Hugo DC identificou os pontos críticos e seus comportamentos abaixo e acima desses valores. Quando os caminhos conexos infinitos aparecem, o modelo é dito contínuo se eles invadem progressivamente o sistema. Quando a sua densidade dá um salto, o fluido pode passar por todo o lado assim que a transição de fase se produz (é o caso da transição gelo-água). Para o modelo de Bernoulli a transição é contínua. Estes problemas podem parecer demasiado particulares. Mas só em aparência. As soluções dependem fortemente da sua dimensão d . O modelo de Ising (resolvido por Onsager em dimensão 2) é um bom exemplo. A transição é contínua em $d = 1, 2$ e $d \geq 4$. Quando $d > 4$ o modelo é dito trivial (i.e. Gaussiano). A primeira demonstração que a transição é contínua em dimensão 3 é devida a Hugo DC. De facto, segundo W. Werner (ETH Zürich) metade dos problemas em aberto neste domínio foram resolvidos por Hugo DC. Muitos dos seus resultados vão inspirar a teoria matemática dos campos quânticos. A noção de interseção (ou não) de caminhos aleatórios torna-se crucial. Resultados recentes de Aizenman e Hugo DC, em particular, ilustram estas profundas relações com a Percolação.

Em 2003, o GFMUL organizou o 14º Congresso de Física-Matemática em Lisboa. Entre os oradores plenários (uma honra académica) contava-se S. Smirnov, professor em Genève. Sete anos mais tarde ele obtinha a medalha Fields. Neste debate incessante entre investigação “de escolas” ou “individualista”, o par Duminil-Copin/Smirnov mostra que o efeito de escola pode funcionar. Sobretudo se a sua origem é devida a um cientista excepcional. Nos outros casos, as escolas não constituem por vezes senão lobbies académicos sem justificação científica.

Para uma descrição detalhada dos trabalhos de Hugo DC, pode consultar-se a análise de Martin Hairer (“The work of H. Duminil-Copin”, online).

[INTERVALO]

1 {Re, par, ti, ção}

A Beatriz e o Gustavo dispõem, cada um, de 2023 moedas de vários valores, mas ambos têm a mesma quantidade de dinheiro. A Beatriz propõe o seguinte jogo:

“Dispomos aleatoriamente as 4046 moedas numa fila e, ora eu, ora tu, retiramos uma moeda de uma das extremidades. Ficamos na mesma com 2023 moedas cada um, mas possivelmente com quantidades de dinheiro diferentes. Quem joga primeiro?”.

Qual deve ser a resposta do Gustavo para não ter prejuízo?

2 Chomp

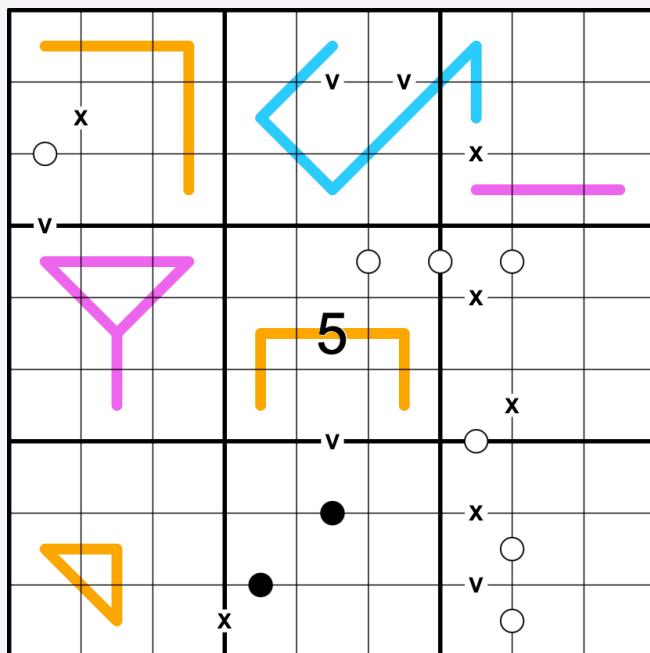
O Martim e a Sara dispõem de uma tablete de chocolate retangular, dividida em $m \times n$ pequenos quadrados ($m, n > 1$), e jogam o seguinte jogo: alternadamente, cada um seleciona um quadrado e come-o, bem como a todos os quadrados que se encontram para baixo e/ou para a direita desse. Perde quem tiver de comer o quadrado do canto superior esquerdo. Na primeira jogada, o Martim come apenas o quadrado do canto inferior direito. A Sara diz-lhe:

“Não sei se fizeste a jogada certa, mas acabaste de me fazer perceber que, jogando em segundo lugar, é impossível que eu tenha uma estratégia vencedora”.

Porque é que a Sara tem razão?

3 Sudoku

Preenche a grelha com os dígitos de 1 a 9 de forma a que cada dígito apareça exatamente uma vez por linha, coluna e caixa.



XV: Dígitos separados por um V devem somar 5. Dígitos separados por um X devem somar 10. Nem todos os X's nem V's são necessariamente dados.

Kropki: Dígitos separados por um círculo branco são consecutivos. Dígitos separados por um círculo preto têm um ráio 1:2. Nem todos os círculos Kropki são necessariamente dados.

Renban: Dígitos numa **linha rosa** devem formar um conjunto de dígitos consecutivos sem repetições. (Por exemplo, 3-7-5-6-4.)

Dutch Whispers: Dígitos adjacentes numa **linha laranja** devem ter uma diferença de pelo menos 4.

Entropic Lines: Cada conjunto de três dígitos seguidos numa **linha azul** deve conter exatamente um dígito baixo (1, 2 ou 3), um dígito médio (4, 5 ou 6) e um dígito alto (7, 8 ou 9). (Por exemplo, 3-5-7-3-6-9.)

Trasformadas de Mellin e expansões assintóticas

Por: Nuno Carneiro

Neste artigo, pretendem-se apresentar alguns resultados que relacionam uma transformada integral de uma função, a transformada de Mellin, com a sua expansão assintótica. Em particular, este resultado é facilmente aplicável a uma classe de funções conhecidas como somas harmónicas, que aparecem frequentemente na área da combinatória e na análise de algoritmos e estruturas de dados. As aplicações da transformada de Mellin na análise assintótica de funções e o artigo *Mellin Transforms and asymptotics: Harmonic Sums*, de P. Flajolet, X. Gourdon e P. Dumas [1], foram a base do trabalho desenvolvido. Este, foi realizado no âmbito das Bolsas Novos Talentos da Fundação Calouste Gulbenkian durante o ano letivo de 2021/2022, orientado pelo Prof. Pedro Freitas, do Departamento de Matemática do IST.

Transformada de Mellin e somas harmónicas

Definição 1.1 (Transformada de Mellin): Dada uma função $f: \mathbb{R}^+ \rightarrow \mathbb{R}$ integrável em $(0, +\infty)$, a sua transformada de Mellin é dada por:

$$f^*(s) = \mathcal{M}[f; s] = \int_0^\infty f(x) x^{s-1} dx$$

A maior faixa vertical aberta onde o integral converge, $\alpha < \Re(s) < \beta$, é chamada de faixa fundamental e denotada por $\langle \alpha, \beta \rangle$.

Lema 1.1 (Existência de transformada). Supomos que $f(x) = O(x^u)$ quando $x \rightarrow 0$ e $f(x) = O(x^v)$ quando $x \rightarrow \infty$. Se $u > v$, é garantido que $f^*(s)$ existe na faixa $\langle -u, -v \rangle$.

Teorema 1.1 (Inversão). Seja $f(x)$ integrável e contínua com faixa fundamental $\langle \alpha, \beta \rangle$. Dado c tal que $\alpha < c < \beta$ e $f^*(c + it)$ é integrável, então, para $x \in (0, +\infty)$:

$$f(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} f^*(s) x^{-s} ds$$

Alguns exemplos comuns de transformadas de Mellin encontram-se na seguinte tabela:

$f(x)$	$f^*(s)$	$\langle \alpha, \beta \rangle$
e^{-x}	$\Gamma(s)$	$\langle 0, \infty \rangle$
e^{-x^2}	$\frac{1}{2}\Gamma\left(\frac{s}{2}\right)$	$\langle 0, \infty \rangle$
$\sin(x)$	$\Gamma(s) \sin\left(\frac{\pi s}{2}\right)$	$\langle -1, 1 \rangle$
$\cos(x)$	$\Gamma(s) \cos\left(\frac{\pi s}{2}\right)$	$s \in \langle 0, 1 \rangle$

Tabela 1: Exemplos de transformadas de Mellin

Definição 1.2 (Soma harmónica). Uma soma harmónica é uma função f que pode ser escrita:

$$f(x) = \sum_{n=1}^{\infty} \lambda_n g(\mu_n x)$$

Os valores de λ_n e μ_n são chamados de amplitudes e frequências, respetivamente, e g é a função base.

Teorema 1.2 (Transformada de somas harmónicas). Dada a função $f(x) = \sum_{n=1}^{\infty} \lambda_n g(\mu_n x)$ seja $\Lambda(s) = \sum_{n=1}^{\infty} \frac{\lambda_n}{\mu_n^s}$ (série de Dirichlet) e $g^*(s)$ transformada da função base, com faixa fundamental $\langle \alpha, \beta \rangle$. Se $\Lambda(s)$ converge simplesmente no semi-plano $\langle \sigma_c, \infty \rangle$ que interseca $\langle \alpha, \beta \rangle$, então:

$$f^*(s) = \left(\sum_{n=1}^{\infty} \frac{\lambda_n}{\mu_n^s} \right) g^*(s) = \Lambda(s) g^*(s)$$

A faixa fundamental de $f^*(s)$ será a interseção da faixa fundamental de $g^*(s)$ e do semi-plano de convergência de $\Lambda(s)$.

Dem. Para as provas do Lema 1.1, Teorema 1.1 e Teorema 1.2, ver [I]. \square

Correspondência fundamental com a expansão assintótica

O seguinte teorema relaciona a transformada de Mellin de uma função com a sua expansão assintótica em 0 e ∞ .

Definição 2.1 (Expansão singular). Seja $\phi(s)$ meromorfa em Ω e \mathcal{S} um conjunto contendo os polos de ϕ em Ω . Uma expansão singular de ϕ será a soma formal das séries de Laurent de ϕ centradas nos elementos de \mathcal{S} truncadas em elementos de ordem $O(1)$ ou inferior, e denotamos $\phi(s) = E$, ($s \in \Omega$). Por exemplo, temos:

$$\frac{1}{s^2(s-1)} \asymp \left[\frac{1}{s+1} \right]_{s=-1} + \left[\frac{1}{s^2} - \frac{1}{s} \right]_{s=0}, \quad (s \in \langle -2, 2 \rangle)$$

Teorema 2.1 (Converse Mapping). Seja $f(x)$ contínua em $(0, \infty)$ com transformada de Mellin, $f^*(s)$, definida numa faixa fundamental não vazia $\langle \alpha, \beta \rangle$.

I. Assumimos que $f^*(s)$ admite uma continuação meromorfa na faixa $\langle \gamma, \beta \rangle$ para algum $\gamma < \alpha$ com um número finito de polos nessa faixa e é analítica em $\text{Re}(s) = \gamma$. Assumimos também que existe um real $\eta \in (\alpha, \beta)$ tal que:

$$f^*(s) = O(|s|^{-r}), \quad r > 1$$

quando $|s| \rightarrow \infty$ em $\gamma \leq \text{Re}(s) \leq \eta$ (esta condição pode ser enfraquecida para o decrescimento de $f^*(s)$ só se verificar num conjunto numerável de retas horizontais, o que permite ainda ter infinitos polos na faixa). Se $f^*(s)$ admite a expansão singular para $s \in \langle \gamma, \eta \rangle$:

$$f^*(s) \asymp \sum_{(\xi, k) \in A} d_{\xi, k} \frac{1}{(s - \xi)^k}$$

então a expansão assintótica de $f(x)$ com $x \rightarrow 0^+$ é:

$$f(x) = \sum_{(\xi, k) \in A} d_{\xi, k} \frac{(-1)^k}{(k-1)!} x^{-\xi} (\log x)^{k-1} + O(x^{-\gamma})$$

2. De forma análoga, assumimos que $f^*(s)$ admite uma continuação meromorfa em $\langle \alpha, \gamma \rangle$ para algum $\gamma > \beta$ e é analítica em $\operatorname{Re}(s) = \gamma$. Supomos ainda que a condição de decrescimento dada anteriormente se verifica em $\langle \eta, \gamma \rangle$ para algum $\eta \in (\alpha, \beta)$. Se $f^*(s)$ admite a mesma expansão singular dada anteriormente em $\langle \eta, \gamma \rangle$, então a expansão assintótica de $f(x)$ quando $x \rightarrow \infty$ é:

$$f(x) = - \sum_{(\xi, k) \in A} d_{\xi, k} \frac{(-1)^k}{(k-1)!} x^{-\xi} (\log x)^{k-1} + O(x^{-\gamma})$$

Dem. Apresentamos apenas as ideias gerais da prova para o caso I.

Queremos aplicar o teorema dos resíduos na fórmula de inversão da transformada de Mellin. Considere-se então um contorno retangular com vértices em $\{\gamma - it, \gamma + it, \eta + it, \eta - it\}$, como indicado na figura abaixo.

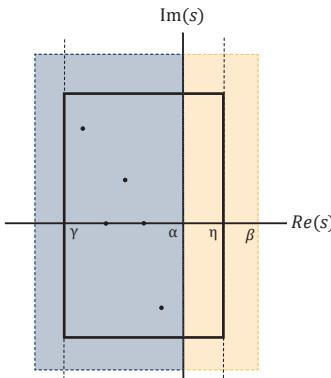


Figura 1: Ilustração do contorno retangular

Fazendo $T \rightarrow \infty$, o integral ao longo da reta vertical $\operatorname{Im}(s) = \eta$ tende para $f(x)$. Por outro lado, a condição de decrescimento garante-nos que os integrais ao longo dos lados horizontais do contorno tendem para 0 e que o integral ao longo da reta vertical $\operatorname{Im}(s) = \gamma$ é $O(x^{-\gamma})$. Finalmente, o cálculo dos resíduos nos polos no interior do contorno resulta nos termos da expansão assintótica apresentada no teorema.

A prova completa pode ser vista em [I]. \square

Exemplo 2.1. Tomamos a função $G(x) = \sum_{n=1}^{\infty} d(n)e^{-nx}$ onde $d(n)$ é a função que retorna o número de divisores inteiros de n . A transformada de Mellin de $G(x)$ é dada pela equação:

$$G^*(s) = \left(\sum_{n=1}^{\infty} \frac{d(n)}{n^s} \right) \Gamma(s) = \zeta(s)^2 \Gamma(s)$$

com faixa fundamental $\langle 1, \infty \rangle$. A transformada pode ser continuada de forma meromorfa para a esquerda da faixa fundamental, havendo polos simples em todos os inteiros não positivos (da função Gama) e um polo duplo em $s = 1$ (da função Zeta). A condição de decrescimento é verificada dado que a função Gama decai exponencialmente ao longo de retas verticais (pela aproximação de Stirling) enquanto que para a função Zeta se verifica $\zeta(\sigma + it) = O(|t|^{1-\sigma})$, para $\sigma < 1$. Temos a seguinte expansão singular para $G^*(x)$ em torno dos polos:

$$G^*(s) \asymp \left[\frac{1}{(s-1)^2} + \frac{\gamma}{s-1} \right]_{s=1} + \sum_{k=0}^{\infty} \left[\frac{(-1)^k \zeta(-k)^2}{k!(s+k)} \right]_{s=-k}$$

Assim, aplicando o Teorema 2.1, obtemos a expansão assintótica, para $x \rightarrow 0^+$:

$$G(x) \sim \frac{1}{x} (-\log(x) + \gamma) + \frac{1}{4} - \sum_{k=0}^{\infty} \frac{(\zeta(-2k-1))^2}{(2k+1)!} x^{2k+1}$$

Exemplo 2.2. Consideremos a função $H(x) = \sum_{n=1}^{\infty} \left(\frac{1}{n} - \frac{1}{n+x} \right) = \sum_{n=1}^{\infty} \frac{x/n}{n(1-x/n)}$. Note-se que se $k \in \mathbb{N}$, então $H(k) = \sum_{n=1}^k \frac{1}{n}$, que corresponde ao k -ésimo número harmónico. Temos que:

$$H^*(s) = -\frac{\pi}{\sin \pi s} \zeta(1-s)$$

com faixa fundamental $< -1, 0 >$. Esta transformada pode ser continuada de forma meromorfa para a direita da faixa fundamental e verifica a condição de decrescimento, obtendo-se a seguinte expansão singular:

$$H^*(s) \asymp \left[\frac{1}{s^2} - \frac{\gamma}{s} \right]_{s=0} - \sum_{n=1}^{\infty} \left[\frac{(-1)^n \zeta(1-n)}{(s-n)} \right]_{s=n}$$

Assim, obtemos a expansão assintótica para $x \rightarrow \infty$:

$$H(x) \sim \log x + \gamma + O\left(\frac{1}{x}\right)$$

Conclusão

Os resultados apresentados mostram a relação fundamental entre a transformada de Mellin e expansões assintóticas, de onde se obtém um método para a análise assintótica de funções. Os exemplos dados demonstram a aplicabilidade deste método a somas harmónicas, sendo muito útil quando estas envolvem funções aritméticas, pelo que é natural o seu uso no contexto da combinatória.

Referências

- [1] Flajoulet, P., Gourdon, X., Dumas, P. (1995). Mellin Transforms and asymptotics: Harmonic Sums. *Theoretical Computer Science*, 144, 3-58.

COMPUTAÇÃO SOBRE DADOS PRIVADOS COM A ENcriptação HOMOMÓRFICA

Por: Mariana Botelho Gama

0101011001
1011001001
0110011010
0100110101
1010110010
0110100110

A criptografia surgiu como um método de proteger mensagens, de forma a que estas não pudessem ser lidas por quem as intercetasse. Hoje em dia, com o aparecimento dos computadores modernos, esta adquiriu muitas outras funções. Milhões de pessoas guardam os seus dados na *cloud*, e podem assegurar-se da sua privacidade recorrendo a esquemas de encriptação. E se pudéssemos editar a informação que guardamos na *cloud* diretamente, sem que a tenhamos que descarregar, desencriptar, e encriptar de novo depois de efetuar as nossas alterações? Ou seja, será que podemos proteger não só informação que está a ser transmitida ou armazenada, mas também informação em uso? Isto permitir-nos-ia analisar, por exemplo, dados de saúde, informações financeiras, ou qualquer outro tipo de informação sensível sem que a sua privacidade fosse comprometida. E existem técnicas que permitem isso mesmo. Nomeadamente, os **protocolos de encriptação homomórfica**, ou HE (*homomorphic encryption*).

A encriptação homomórfica, como o nome indica, permite operar sobre textos encriptados e obter um resultado equivalente à realização da mesma operação sobre textos simples.

Existem esquemas de encriptação de chave pública que têm esta propriedade, tal como a versão *naive* do RSA ou o ElGamal, que são homomórficos relativamente à multiplicação. Isto significa que se tivermos dois textos encriptados c_1 e c_2 que representam encriptações de m_1 e m_2 , respetivamente, então temos que $c_3 = c_1 \cdot c_2$ será uma encriptação de $m_3 = m_1 \cdot m_2$. No entanto, estes protocolos não são homomórficos relativamente à adição, sendo apenas parcialmente homomórficos.

Para que possamos realizar qualquer operação homomorficamente, precisamos de um protocolo de encriptação que seja homomórfico relativamente à adição e à multiplicação (uma vez que qualquer programa pode ser representado como um circuito com estas duas operações). Estes protocolos são então chamados **FHE - fully homomorphic encryption**.

Apesar do conceito da encriptação homomórfica ter surgido no final dos anos 70, o primeiro protocolo de FHE foi proposto apenas em 2009, quando Craig Gentry introduziu o conceito de *bootstrapping*. É possível obter esquemas homomórficos relativamente à multiplicação e à adição recorrendo ao problema de aprendizagem com erros (LWE - *learning with errors*). Vejamos por exemplo o protocolo DGHV. Este protocolo encripta mensagens binárias $m \in \{0, 1\}$ da seguinte forma:

$$c = p \cdot q + 2r + m$$

onde p (a chave secreta) é um número ímpar, q é um inteiro aleatório, e r é um termo denominado ruído.

Para desencriptar, basta calcular $(c \bmod p)$ mod 2. Observemos agora o que acontece ao ruído quando operamos sobre estes textos encriptados:

$$\begin{aligned} c_1 + c_2 &= p \cdot (q_1 + q_2) + 2(r_1 + r_2) + (m_1 + m_2) \\ c_1 \cdot c_2 &= (p \cdot q_1 \cdot q_2 + \dots) + 2(2 \cdot r_1 \cdot r_2) + (m_1 \cdot m_2) \end{aligned}$$

A realização de operações sobre os textos encriptados leva a um aumento progressivo do termo de ruído, até que deixa de ser possível desencriptar corretamente. Assim que o limite de ruído é atingido, devemos utilizar o *bootstrapping*. Este processo consiste, em termos gerais, na avaliação homomórfica do próprio circuito de desencriptação com uma versão encriptada da chave secreta, por forma a obter uma nova encriptação do texto original com um nível de ruído mais baixo. Esta operação é geralmente dispendiosa, o que leva a que a sua utilização seja evitada. Na prática, a forma como o *bootstrapping* é realizado, assim como o seu custo, depende do protocolo específico de FHE que estamos a utilizar. Alguns dos protocolos mais relevantes são o BGV (Brakerski-Gentry-Vaikuntanathan), o CKKS (Cheon-Kim-Kim-Song) ou o TFHE (Torus FHE). A segurança destes esquemas está baseada no problema em reticulados LWE, para o qual não se conhecem algoritmos eficientes, incluindo algoritmos quânticos. Isto significa que a encriptação homomórfica permanecerá segura mesmo perante ataques de computadores quânticos.

Um exemplo de uma aplicação da encriptação homomórfica é a pesquisa de contactos. Quando descarregamos uma nova aplicação de mensagens, como por exemplo o WhatsApp ou o Signal, queremos saber quais dos nossos contactos também utilizam essa mesma aplicação. Ou seja, queremos saber a interseção entre o conjunto dos nossos contactos e o conjunto de todos os utilizadores de determinada aplicação. Utilizando encriptação homomórfica, podemos obter o resultado desta interseção sem expor a



Fig. 1: Craig Gentry

nossa lista de contactos. Cada contacto y_i é enviado de forma encriptada para o servidor do serviço de mensagens, onde por sua vez são calculados os valores $[d_i]$ representados na Figura 2. Quando y_i é igual a algum dos contactos x presentes no servidor, teremos que $d_i = 0$. O próprio servidor não terá acesso a essa informação, uma vez que apenas nós, o utilizador, temos a chave secreta que nos permite desencriptar $[d_i]$. Note-se que esta descrição corresponde a uma aplicação *naive* de HE para resolver o problema de descoberta de contactos. Na prática, existem várias otimizações que nos permitem minimizar o número de operações homomórficas necessárias e melhorar a eficiência do algoritmo.

A utilização da encriptação homomórfica na prática é limitada pelo seu elevado custo computacional. Contudo,

o desenvolvimento de aceleração de hardware para FHE tem ajudado a contornar este obstáculo, sendo a sua praticidade uma realidade cada vez mais próxima. Um outro problema relacionado com HE diz respeito à verificação das operações realizadas homomórficamente. Se por um lado utilizamos HE porque não confiamos nas entidades a quem fornecemos a nossa informação encriptada, como podemos saber que estas mesmas entidades irão realizar as operações que pretendemos sobre os nossos dados e que o resultado final obtido tem o significado correto? Apesar de ser possível verificar algumas computações recorrendo a provas de conhecimento nulo (*zero knowledge proofs*), a verificação eficiente de qualquer sequência de operações permanece um problema em aberto.

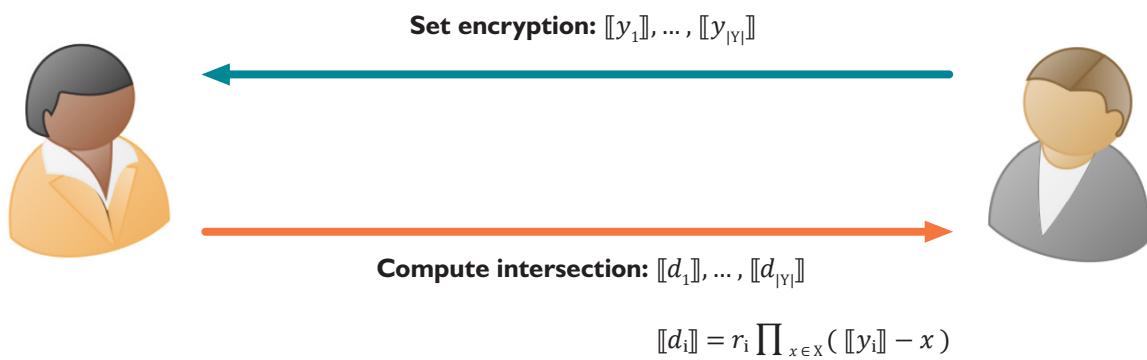


Figura 2: O utilizador (à direita) envia textos encriptados ao servidor (à esquerda), que devolve o resultado encriptado da intersecção com a sua própria base de dados.

QUANTIZAÇÃO GEOMÉTRICA

\mathbb{R}^n

\uparrow

\mathbb{R}^n

Por: António Gouveia

Com o surgimento da física quântica como ferramenta conceptual para fazer previsões ao nível atómico, surgiu também a ideia de *quantização*, que em poucas palavras, corresponde a obter sistemas quânticos através de sistemas clássicos. Assim, o objetivo da quantização geométrica é tentar dar uma interpretação geométrica da quantização dentro de uma extensão da armação matemática da mecânica clássica (geometria simplética). Deste modo, o propósito deste texto é apresentar, de uma forma elementar, a ideia da quantização geométrica.

Antes de começarmos a ver algumas destas ideias, vamos apresentar de forma muito resumida alguns conceitos:

Um **campo vetorial** X em \mathbb{R}^n pode ser escrito da seguinte forma:

$$X(x) = (X_1(x), \dots, X_n(x)) = X_1(x) \frac{\partial}{\partial x_1} + \dots + X_n(x) \frac{\partial}{\partial x_n}$$

em que X_i são funções suaves e podemos pensar que $\frac{\partial}{\partial x_i} = e_i$, onde e_i é o i -esimo elemento da base canónica de \mathbb{R}^n . Dada uma função suave $f : \mathbb{R}^n \rightarrow \mathbb{R}$, podemos obter a função $Xf : \mathbb{R}^n \rightarrow \mathbb{R}$ definida da seguinte forma:

$$(Xf)(p) = \sum_{i=1}^n X_i(p) \frac{\partial f}{\partial x_i}(p)$$

A operação denominada **Lie bracket**, que recebe dois campos vetoriais e devolve um campo vectorial, é definida da seguinte forma:

$$[X, Y] := (XY_1 - YX_1, \dots, XY_n - YX_n)$$

Fixemos o nosso espaço como sendo \mathbb{R}^{2n} e representamos as primeiras n coordenadas por x_i e as restantes por y_i , $i \in \{1, \dots, n\}$, assim, um ponto genérico é $(x_1, \dots, x_n, y_1, \dots, y_n)$. No espírito da Física, as coordenadas x_i representam a posição, enquanto as y_i representam o momento.

Vamos agora definir uma operação semelhante para funções, chamada **Poisson Bracket**, que definimos como sendo:

$$\{f, g\} := \sum_{i=1}^n \left(\frac{\partial f}{\partial x_i} \frac{\partial g}{\partial y_i} - \frac{\partial g}{\partial x_i} \frac{\partial f}{\partial y_i} \right)$$

Um **campo hamiltoniano** é um campo vetorial associado a uma função H dado por:

$$X_H := \left(\frac{\partial H}{\partial y_1}, \dots, \frac{\partial H}{\partial y_n}, -\frac{\partial H}{\partial x_1}, \dots, -\frac{\partial H}{\partial x_n} \right)$$

Uma forma diferencial de grau 1 é uma aplicação linear que recebe um vetor em \mathbb{R}^{2n} e devolve um escalar. Por exemplo dx_i é tal que $dx_i(x_1, \dots, x_n, y_1, \dots, y_n) = x_i$ $i \in \{1, \dots, n\}$. Em particular, quando integramos em \mathbb{R} , o $f(x)dx$ corresponde a uma forma diferencial de grau 1! Temos uma operação entre fórmulas diferenciais chamada **produto antissimétrico**:

$$(dx_i \wedge dx_j)((p, q)) = \det \begin{pmatrix} dx_i(p) & dx_j(p) \\ dx_i(q) & dx_j(q) \end{pmatrix}$$

Por exemplo em \mathbb{R}^2 temos

$$dx_1 \wedge dx_2((1, 2), (4, 3)) = \begin{vmatrix} 1 & 4 \\ 2 & 3 \end{vmatrix} = 3 - 8 = -5$$

Note-se que isto nos diz que $dx_1 \wedge dx_2$ representa a área euclidiana de \mathbb{R}^2 e que $dx_1 \wedge dx_2 = -dx_2 \wedge dx_1$, ou seja, é alternante e $dx \wedge dx = 0$. Assim, uma forma diferencial de grau 2 é descrita como

$$\alpha = \sum_{i \neq j} f_{ij} dx_i \wedge dx_j, \quad f_{ij} \in C^\infty(\mathbb{R}^n)$$

Pode-se de igual forma definir k -formas, da mesma maneira. Uma **forma simplética** ω é uma 2-forma diferencial que é fechada e não degenerada. Em \mathbb{R}^2 a forma simplética standard é $dx \wedge dy$ e em \mathbb{R}^4 é $dx_1 \wedge dy_1 + dx_2 \wedge dy_2$. Um **potencial simplético** α é uma 1-forma tal que $\omega = -d\alpha$, onde d representa o diferencial de uma forma. Por exemplo

$$d(f(x, y)dx) = \frac{\partial f}{\partial y} dy \wedge dx$$

Em particular, em \mathbb{R}^2 temos que $\omega = dx \wedge dy = -dy \wedge dx = -d(ydx)$, logo ydx é um possível potencial.



Fig. I William Rowan Hamilton

Um sistema clássico é composto por uma variedade simplética (M, ω) e uma função escalar $H(x, y)$ que irá descrever o sistema dinâmico, chamado de hamiltoniano. O tuplo (M, ω, H) diz-se um **sistema Hamiltoniano**.

Segundo Dirac, para proceder à quantização é necessário fixar um subespaço $\mathfrak{a} \subset C^\infty(M)$ e encontrar um espaço de Hilbert \mathbb{H} e uma aplicação \mathbb{C} -linear

$$q : \mathfrak{a} \rightarrow \text{Op}(\mathbb{H})$$

tais que as seguintes condições sejam feitas:

- $q(1) = \text{id}_{\mathbb{H}}$,
- $[q(f), q(g)] = cq(\{f, g\}), \quad \forall f, g \in \mathfrak{a}$.
- Se o conjunto de $\{f_1, \dots, f_n\}$ é completo, isto é $\{g, f_i\} = 0, \quad \forall i \in \{1, \dots, n\}$ implica que g é constante, então $\{q(f_1), \dots, q(f_n)\}$ também é completo, ou seja, se $[A, q(f_i)], \quad \forall i \in \{1, \dots, n\}$ então $A = \alpha \text{id}_{\mathbb{H}}$ para algum $\alpha \in \mathbb{H}$.
- $q(f)$ é auto-adjunto.

Estas condições dizem-nos que \mathfrak{a} é um subespaço linear e em particular, uma subálgebra da álgebra de Poisson $C^\infty(M)$ e, pela terceira condição, que a representação de \mathbb{H} é irreduzível. Por outro lado, a constante c requer algum cuidado uma vez que se não for imaginária o operador não é auto-adjunto. Assim, é comum escolher $c = i$ ou $c = \frac{i}{\hbar}$ ou $c = \frac{-1}{2\pi i}$, onde \hbar é a constante de Planck. Iremos optar pela última.

Em geral, é impossível encontrar um operador que satisfaça todas estas condições, daí ser necessário enfraquecer as mesmas. Porém, as técnicas da quantização geométrica levam-nos a espaços quânticos \mathbb{H} ricos do ponto vista geométrico e a técnicas que misturam ideias da geometria simplética, complexa, Riemanniana e algébrica.

Mesmo no caso mais simples, não há uma receita standard para encontrar o espaço de Hilbert \mathbb{H} nem a aplicação q . Porém, em geral, o primeiro passo a tomar é chamado de **Prequantização**.

Comecemos por observar a seguinte função que associa funções ao seu campo hamiltoniano

$$\begin{aligned} \Phi : C^\infty(M) &\rightarrow \mathfrak{X}(M) \\ f &\mapsto -X_f \end{aligned}$$

que é \mathbb{C} -linear e “respeita” o Lie bracket:

$$\Phi(\{f, g\}) = -X_{\{f, g\}} = [X_f, X_g] = [\Phi(f), \Phi(g)].$$

Assim, uma primeira ideia (e natural) é definir o nosso operador da seguinte forma:

$$q(f) := -cX_f$$

Logo, temos a linearidade e a segunda condição sai de graça quando tomamos $\mathfrak{a} = C^\infty(M)$. Porém, a primeira condição não é satisfeita, pois $1 \in \mathfrak{a}$ mas $q(1) = 0$, logo esta definição não funciona de todo.

Com base nisto, podemos considerar a seguinte correção:

$$q(f) := -cX_f + f.$$

É agora óbvio que a primeira condição é satisfeita. No entanto, através do seguinte exemplo, vemos que a segunda condição não é satisfeita: consideremos $M = \mathbb{R}^2$ com coordenadas x, y ; podemos ver que $\{x, y\} = 1$ e então temos que $q(\{x, y\}) = 1$. Os campos hamiltonianos são $X_x = -\frac{\partial}{\partial y}$ e $X_y = \frac{\partial}{\partial x}$, logo $q(x) = c\frac{\partial}{\partial y} + x$ e $q(y) = -c\frac{\partial}{\partial x} + y$ e podemos ver que $[q(x), q(y)] = 2c \neq 1$.

Vamos agora considerar uma outra correção

$$q(f) := -cX_f + f + \alpha(X_f),$$

onde α é uma 1-forma diferencial.

É evidente que q é \mathbb{C} -linear irá satisfazer a primeira condição, independentemente da escolha de α . Fazendo umas pequenas contas é fácil de ver que $q(f)$ **satisfaz a segunda condição se e só se α é potencial simplético de ω** . Operador $q(f)$ é conhecido como **operador prequântico**.

Assumimos que o potencial existe. É um facto elementar da geometria simplética que uma variedade simplética admite uma forma de volume dada por ω^n . Assim podemos integrar! E definimos o espaço Hilbert prequântico como sendo o completamento do espaço $\{\phi \in C^\infty(M) : \int_M |\phi|^2 \omega^n < \infty\}$ com respeito à norma induzida pelo produto interno:

$$\langle \phi, \psi \rangle := \int_M \phi \bar{\psi} \omega^n.$$

A vida, claro, não é assim tão simples. Existem algumas limitações para este tipo de abordagem:

◆ Nem sempre existe um potencial simplético (global). Em particular, se a variedade simplética é compacta, então o potencial nunca existe, por consequência do teorema de Stokes.

◆ Mesmo que o potencial exista, a nossa definição de q depende da escolha do potencial.

◆ O espaço de Hilbert prequântico obtido é “demasiado grande”, no sentido em que depende de $2n$ variáveis. A mecânica quântica diz-nos que as funções de ondas devem depender de apenas n variáveis. O espaço de Hilbert encontrado está muito longe de ser irredutível sob a ação dos operadores de posição e momento quantizados.

Existem formas de ultrapassar estas limitações, usando diversas técnicas e ferramentas da geometria. A título de exemplo, a questão da dimensão pode ser resolvida tomando polarizações, que basicamente vão definir n direções nas quais vamos requerer que as funções sejam constantes, tornando o \mathbb{H} irredutível. Mas com isto surge um outro problema: pode implicar que $\mathbb{H} = \{0\}$.

Há diferentes tipos de polarizações, em particular temos polarizações reais e polarizações complexas. As reais são muito mais difíceis de estudar do que as complexas (e, consequentemente, as respetivas quantizações). Mas em variedades como a esfera (ditas de Kähler) existe uma forma de obter polarizações reais através das complexas da seguinte forma: a esfera tem associada uma função de altura que leva a esfera num intervalo em \mathbb{R} ; aqui podemos considerar funções estritamente convexas e, quando consideramos o fluxo do campo hamiltoniano destas funções em tempo imaginário, permite relacionar diferentes polarizações complexas. Em particular, quando fazemos o tempo tender para $+i\infty$, estas polarizações degeneram-se em polarizações reais, permitindo assim estudar as quantizações associadas de uma forma mais fácil. Na minha tese, irei estudar o que acontece quando tomamos uma função cuja segunda derivada é uma *bump function*.

Referências

- [1] Nunes, J. (2014). Degenerating Kähler structures and geometric quantization. *Reviews in Mathematical Physics*, 26(10), I430009.
- [2] Hall, B. (2013). *Quantum theory for mathematicians*. Springer.
- [3] Schottenloher, M. (2022). *Lecture notes on geometric quantization*. Mathematisches Institut der Universität München. <https://www.mathematik.uni-muenchen.de/~schotten/GEQ/GEQ.pdf>.
- [4] Kirwin, W. D., Mourão, J. M., & Nunes, J. P. (2016). Complex symplectomorphisms and pseudo-Kähler islands in the quantization of toric manifolds. *Mathematische Annalen*, 364, 1–28.
- [5] Cannas da Silva, A. (2008). *Lectures on symplectic geometry* (Vol. 1764). Springer.
- [6] Lee, J. M. (2013). *Introduction to smooth manifolds* (Vol. 218). Springer.
- [7] Blau, M. (2007). *Symplectic geometry and geometric quantization*. <http://www.blau.itp.unibe.ch/lecturesGQ.pdf>
- [8] Godinho, L., & Natário, J. (2014). *An introduction to Riemannian geometry: With applications to mechanics and relativity*. Springer.

Tirar doutoramento ou não: eis a questão

entrevistas a alumni

... Pedro Nogueira

Entrevistas por: Madalena Preto

Pedro Nogueira entrou no IST em 2016. Após um ano em Engenharia Mecânica, mudou para LMAC por via interna. Completou a licenciatura e continuou para o mestrado MMAC, no perfil de Aplicações, na área da resolução de EDPs numérica e analiticamente. Terminou o mestrado em 2021 e, ainda hoje, está a fazer o doutoramento no IST.

1) Tens gostado da tua experiência no Técnico?

Sim, se me dissessem que podia voltar atrás, repetia tudo outra vez, como é óbvio. Se calhar a única coisa que mudava era entrar diretamente em Matemática. Acho que o curso de Matemática está muito bem feito, está bem estruturado. Foi uma boa experiência. Pessoalmente preferi muito mais o mestrado, que é quando começas a fazer as cadeiras de que gostas mesmo a sério. Também tive sorte de ter apanhado fora dos quarters.

2) E agora, estás a fazer o doutoramento no Técnico.

Sim. Não é que eu tenha entrado sem querer no doutoramento, mas, quando comecei a fazer a tese de mestrado, ao mesmo tempo meti-me numa bolsa de investigação e gostei. Foi uma boa experiência que me motivou a tentar ver já, durante o mestrado, se continuava para o doutoramento.

Eu estudo as equações de Navier-Stokes, relacionadas com problemas de controlo ótimo. Isso foi o tema da minha tese de mestrado e dessa bolsa de investigação. Agora estou a fazer uma coisa muito mais generalizada, a meu ver, mais interessante, e bem mais complicada.

Em 2021 acabei a tese de mestrado, depois estive cerca de um ano com essa bolsa de investigação. E depois, quando abriram as vagas de FCT em 2022, eu candidatei-me. Na altura as candidaturas abriam em abril ou maio. Depois oficialmente só começas mais para o fim do ano. O meu doutoramento começou em novembro de 2022.

3) Achaste difícil o processo de candidatura, e encontrar o doutoramento certo?

Isso é uma coisa que uma pessoa só quando tem que se candidatar é que percebe. Ou seja, escolher o tema do doutoramento não é como por exemplo escolher o tema da tese [do mestrado] ou cadeiras. Quando submetes o tema da tese de doutoramento, tem de estar muito bem estipulado, ou seja, tens que ter um plano de trabalhos muito bem estruturado com timelines, ou seja, ao fim de x meses pensamos já ter isto feito, simulações feitas naquela parte, x papers. Quando submetes a tua candidatura para o doutoramento, *a priori* já sabes um pouco sobre o tema que vais investigar.

4) Como tem sido o teu percurso, em relação a ficar em Portugal, no IST, e ir para o estrangeiro?

Agora estou no estrangeiro, em Berlim. Uma pessoa quando sai do mestrado tem uma mentalidade um bocadinho diferente, em que nós conseguimos fazer tudo na nossa bolha: com os meus orientadores daí, eu consigo acabar a tese e ter bons resultados e isso tudo. [No doutoramento,] não é que não consigas, grande parte da minha parte da tese de doutoramento foi feita aí em Lisboa. A questão é que, depois, se pretenderes continuar na vida académica, não só é benéfico sair e teres outros contactos com outras pessoas e outras metodologias, mas também é benéfico no sentido em que, Lisboa também tem poucas pessoas, e como consequência tem poucas ideias nesse sentido. Por exemplo, quando uma pessoa vai para fora, por exemplo na Alemanha, onde há mais centros de investigação, também há muito mais gente e mais dinheiro é uma zona muito mais fértil para criar novas ideias e ter novos resultados, se calhar até a

um ritmo muito mais rápido.

Por questões de conforto, decidi ficar na base. Claro que agora, depois de ter outra experiência, sim, se tivesse de voltar atrás, isso sim seria uma das coisas que talvez mudasse. Acho muito benéfico sair, criar outras pontes.

5) Claramente estás a gostar da experiência. Queres continuar na vida académica e nesta área?

Eu estou a gostar e gostaria de continuar. Outra coisa que uma pessoa só quando entra no doutoramento e se calhar só mais lá para o fim é que se começa a aperceber, e isto não pode ser visto como um conselho para as pessoas que querem entrar no doutoramento: isto não é um mar de rosas. O doutoramento em si já é uma coisa complicada de se fazer, é uma montanha-russa de emoções: uma pessoa ou está muito contente com os resultados ou não sabe o que há de fazer. Mas, esquecendo essa parte, o após o doutoramento é ainda mais assustador no sentido em que é uma vida muito instável. Uma pessoa tem de fazer pós-docs e para fazer pós-docs há todo aquele processo de se candidatar, e uma pessoa tem de ver onde fica. Eu agora, por exemplo, em Berlim, tenho falado com muitas pessoas que estão nessa situação. O complicado é se queres ter uma vida pessoal estável ao mesmo tempo. Por esta instabilidade de ter sempre de andar a saltitar de um lado para o outro, que não é necessariamente uma coisa má, pode até ser bom: uma pessoa, lá está, tem mais contactos. Mas acho que para mim isso não é uma coisa que me desmotive muito. Claro que há sempre aquele medo de: o que é que vai acontecer no futuro? Há sempre uma incógnita. Mas a parte de fazer investigação e dar aulas é uma componente tão boa, pelo menos para mim que, de certa forma, consegue sobrepor-se a essa possível instabilidade.

“o verdadeiro teste, [...] será mesmo a tese de mestrado”

6) Que aspectos do doutoramento dirias que podem assustar ou surpreender pela positiva?

OK, vamos começar pelas coisas boas. Uma pessoa tem bastante flexibilidade, exceto alguns doutoramentos que são muito particulares. Por exemplo, se uma pessoa tiver de fazer muita coisa relacionada com computação pesada, muitas vezes tem que estar associada a um laboratório, ou um centro qualquer onde exista um supercomputador; nesse sentido, uma pessoa acaba por ter menos flexibilidade porque tem de estar nesse sítio. Mas se for um doutoramento um bocadinho teórico, como o meu, que é mais teórico e prático ao mesmo tempo, as simulações que eu tenho de fazer - um portátil ou um [computador] fixo faz bem em algum tempo. Nisso uma pessoa tem mais flexibilidade, basicamente podes decidir o teu horário. Claro que tens de trabalhar, como é óbvio. E definir o teu ritmo de trabalho. E depois há todas as coisas boas: estás a estudar aquilo de que tu gostas, estás sempre a aprender, estás focado num determinado problema, e aquela coisa de resolver um puzzle - que para algumas pessoas é boa, para outras é mau. Claro que depende. Às vezes fica-se um bocadinho obcecado, o que se pode tornar mau.

Em relação às partes negativas, isso aí fica ao critério de cada um. Relacionado com a investigação, há aquela parte em que tu nunca sabes se aquilo que estás a estudar vai servir para alguma coisa, isso pode ser uma perda de tempo. Não há uma estrutura, do género, estudas isto, consegues resolver aquilo, que é aquilo a que os alunos estão habituados até à tese de mestrado. É estudar para resolver um teste. No doutoramento tu não estás a estudar para resolver um exercício. Tens um problema e vais ver o que já foi feito que pode ajudar a resolver aquele problema: geralmente, nada foi feito, ou foi metade do caminho feito e tu tens que adaptar. Para mim isso é uma parte engraçada, ver o que tem de encaixar, para outras pessoas isso é péssimo; o que eles querem é uma receita: eu quero resolver aquele problema, tenho de saber esta matéria e pronto.

Depois há coisas intrinsecamente más. Uma delas não tem propriamente a ver com o doutoramento em si, acho que é uma coisa do país. Os bolseiros têm uma vida um bocado má. Não temos subsídios, não recebemos propriamente bem, quando comparas com pessoas que estão fora da academia pode ser mau porque recebem mais, trabalham menos, é sempre aquela coisa assim da comparação. Mas pronto, acho que se pusermos isso de parte, se o dinheiro não for muito importante, se o mais importante for o gostar de fazer matemática, acho que isso não deve ser visto como uma coisa negativa.

Para o doutoramento tem de ser sempre alguém que goste mesmo daquilo. Isso já se pode ver um bocadinho na tese de mestrado: há muitas pessoas que se vão abaixo na tese de mestrado porque, não é que não gostem de matemática ou de uma engenharia qualquer, do curso que estão a tirar, mas é aquele ambiente de estar sempre a marrar a mesma coisa. Acho que no doutoramento isso é multiplicado por cem. Uma pessoa tem de ser resiliente nesse aspeto. Não é que as pessoas que não queiram tirar o doutoramento tenham menos capacidade, é apenas uma questão de feitio.

7) Como é que alguém pode tentar decidir se o doutoramento é para eles?

Eu acho que o verdadeiro teste, ou um dos grandes testes a isso, será mesmo a tese de mestrado. Se forem pessoas que, no fim da tese de mestrado, puderem dizer que globalmente foi uma coisa de que gostaram imenso, não foi uma seca, não foi doloroso nem nada, como é a maioria dos casos de que oiço; isso já é um indicativo de que se calhar são pessoas que têm feitio para investigação. Vou só repetir: não é que sejam mais inteligentes que os outros nem nada isso, porque há muito essa coisa de só vai para o doutoramento quem é inteligente. Não, há muitas pessoas que são bastante inteligentes, simplesmente não gostam de estar sentados sem aquela estrutura, que era o que eu estava a dizer, ou seja, vou ver se isto funciona, se não funcionar pronto, vemos outra coisa. Gostam mais de ir para a indústria ou para o corporate ou assim. Aqui tem de haver uma certa autoavaliação, uma avaliação pessoal. Mas claro que há muitos outros fatores do doutoramento que ditam todo o teu percurso, por exemplo, os teus orientadores, o sítio onde estás a trabalhar, o próprio tema.

Muitas vezes, pensa-se que, quando se faz o mestrado, dita logo o percurso académico: se eu faço o mestrado em Probabilidades, tenho de fazer a tese de doutoramento em Probabilidades, e aí a diante. Vou sempre trabalhar em Probabilidades. Não é verdade. Claro que se forem áreas muito opostas é complicado. Mas posso dar o meu exemplo. O meu mestrado foi na área das numéricas com alguma análise, mas aquilo que estou a fazer agora é muito mais teórico do que eu alguma vez pensei. Trabalho com muita análise, uma coisa que no início parecia muito mais numérica, mas é muito mais de análise funcional.

... Bernardo Almeida

Bernardo Almeida, de 26 anos, entrou na licenciatura em Matemática Aplicada e Computação em 2016 e, em 2020, ingressou no mestrado de Matemática Aplicada e Computação, no perfil de Lógica e Computação. Hoje em dia, trabalha como Custom Software Engineer na Accenture.

1) Gostaste do teu percurso no IST?

Gostei mais do mestrado que da licenciatura. A licenciatura pode ser um bocado diferente daquilo de que estás à espera e de onde vens. No mestrado já tens um bocadinho mais de escolha sobre o que queres... Em termos de cadeiras, gostei mais das cadeiras que envolviam programação.

2) Depois do mestrado, o que decidiste ir fazer?

Quando estava a acabar a tese de mestrado, comecei a candidatar-me para empregos. Sempre foi esse o objetivo, então comecei a mandar currículos para começar a trabalhar. E foi assim um bocado para a área de informática. Acabou por ser um bocadinho consultoria, mas na área de informática. Depois entrei na empresa onde estou atualmente. O trabalho tem sido mais ou menos sempre o mesmo, porque sempre envolveu desenho de aplicações e programação das aplicações, desde o dia em que entrei.

3) Antes de escolheres esse emprego, sabias que era isso que querias fazer?

Mais ou menos, não tinha bem a certeza daquilo que queria fazer. Mesmo quando entrei para a licenciatura, quando me candidatei, também não tinha a certeza que era esta a licenciatura. Se calhar o mestrado foi a coisa em que tinha mais certeza. O resto foi: vou-me candidatar, mandar currículos para vários sítios, às vezes nem era bem para a mesma coisa, mas depois, se eventualmente não gostar, vou mudar. À medida que fui ficando... agora gosto daquilo que faço, então mantive-me lá. Mas não quer dizer que seja isso que vou fazer a vida toda.

4) Então vês-te a mudar de carreira no futuro?

Mais longínquo. Diria que agora, assim, no mais próximo, vou manter.

O que é que isso engloba? Programação de aplicações personalizadas para o cliente e a análise dos requisitos do cliente, a nível técnico e mesmo funcional do negócio deles e do que eles querem. Também há que testar o que tu desenvolves ou o que outras pessoas desenvolvem para verificar se está tudo OK. E depois tens a parte – em que também estou muito envolvido hoje em dia – que é a manutenção dessas aplicações. Há sempre que manter aquilo operacional. É a isso que se resume o meu trabalho e o de muita gente nesta área.

5) Nunca pensaste em fazer o doutoramento?

Acho que não. Sempre foi claro que não queria fazê-lo, queria ir trabalhar. Não sei bem porquê, mas nunca pensei nisso muito. Acho que, ao fim de 5 anos, já chegava de estudar. Se calhar para ti é diferente, porque estás aqui [no IST], presencialmente. Mas eu tive azar, que o meu mestrado foi basicamente todo feito durante COVID. Eu estava em casa, 24 horas por dia, e, na tese, a única coisa que eu fazia o dia inteiro era trabalhar nela. Não me encontrava com o meu orientador, era chamadas – às vezes nem uma vez por semana. Portanto, acaba por ser um bocado cansativo, porque estás todos os dias a fazer a mesma coisa, não vês ninguém, quase não falei com ninguém. Isso se calhar também influenciou a minha decisão de não querer continuar para o doutoramento. Mas, na realidade, nunca pensei nisso, nem quando entrei para a licenciatura. Pensei que ia fazer o mestrado, sim, mas nunca pensei em continuar para o doutoramento.

6) Do que é que gostas mais ao trabalhar numa empresa?

No geral, diria que é bom.

As principais vantagens, e aquilo que eu sinto que gosto mais, é, por exemplo, o desenvolvimento profissional e pessoal. Na empresa onde estou, dão-te muitas oportunidades de fazer formações e na área em que trabalho isso é essencial porque está sempre a mudar e evoluir. E depois também tens o contacto com as pessoas de diferentes áreas. Por exemplo, podes trabalhar só com pessoas de mais uma área, mas às vezes tens projetos com pessoas de diferentes áreas e vais fazendo contacto com coisas que não conheces, e com pessoas que percebem essas coisas e te explicam – e ficas a perceber. Acabas por ter contacto com muitas coisas que se calhar de outra forma não terias. E trabalhas em equipa, o que é bom.

Tens sempre aquele lado negativo: são empresas grandes, se calhar eles não querem saber muito só de uma pessoa, e tomam as decisões sem conhecer as pessoas. Mas é uma questão de ires conseguindo equilibrar as coisas e às vezes mudar, se não te sentes feliz naquela, e ir para outra.

Trabalho mais horas, sim. Eu já faço um horário um bocado estranho. Saio às sete (19h), tirando à sexta, que saio às cinco (17h). Depois tenho mais 12 dias de férias, que não sei se compensa. Tem sempre entregas para fazer, coisas prioritárias, então há sempre aqueles dias em que trabalhas mais um bocadinho, às vezes muito, mas não é constante. Há pessoas que conseguem – chega às sete e acabou-se. Mas se calhar essas pessoas também não evoluem muito. Ficam ali porque não se esforçam por fazer mais um bocadinho, para acabar aquilo dentro do prazo. Tens sempre esse balanço que é preciso fazer.

7) Disseste que trabalhas mais em informática. Sentes que estavas confortável nisso, e ao nível dos outros, saindo do MMAC?

Não. No primeiro projeto que tive, era em Python. Sabia minimamente como as outras pessoas, e era mais fácil pesquisar coisas na net. Trabalhava com um módulo de Python que eu não conhecia, mas foi uma questão de me ir habituando. Mas depois esse projeto acabou e trabalhei em Java, e eu só tinha tido uma cadeira

“acabas por ter contacto com muitas coisas, que de outra forma não terias”

brava-me mais ou menos como é que aquilo funcionava... Depois vais aprendendo e desenrascas-te facilmente. As aplicações em que trabalho atualmente são em Cloud, não sabia nada disso também. Ainda hoje, e lá está, o que sei é das formações que fiz. Mas nada do que eu aprendi na universidade me preparou para isso. É uma questão de, se fores com o espírito aberto e com vontade de continuar a aprender, acho que te consegues desenrascar. Mas não diria que o nosso curso em específico nos prepare para isso.

8) Atualmente trabalhas em Portugal. Nunca pensaste em ir para fora?

Acho que não. Quero dizer, pensar, pensar, todas as pessoas pensam. Mesmo atualmente penso: se eu estivesse lá fora, se calhar estava a receber o dobro do que estou a receber em Portugal. Mas na altura, quando me comecei a candidatar, foi tudo para Portugal. Depois entrei e nunca pensei: vou desistir agora e começar a procurar no estrangeiro. Sinto-me feliz em Portugal.

9) Como correu a primeira procura de emprego, ainda durante o mestrado?

Até foi fácil, na realidade. Estava a escrever a tese, ainda a acabar, comecei a mandar currículos, e tive, se não me engano, logo uma proposta. Fiquei à espera, já tinha tido uma entrevista para onde estou atualmente e tinham-me ligado, quando recebi a proposta, a dizer que ainda estavam a analisar, mas que havia forte possibilidade. Então ainda recusei a outra e fiquei à espera desta, porque achei que ia ser melhor. Nem foi muito difícil para mim, mas conheço um amigo meu que, começou a procurar antes de mim, e acabou depois. Depende do que estás à procura. Se for muito específico... (Ele fez o mestrado no perfil de Estatística e estava a procurar mais em modelos de machine learning.)

10) Tens algum conselho para alunos que estão indecisos – ou que não sabem sequer como começar a procurar?

Para começar a procurar, é só procurar. O LinkedIn é das melhores ferramentas. Tens as vagas que quiseres, é só uma questão de escolheres. Se ainda não souberes aquilo que queres, eu diria que é começar a procurar, porque vais eventualmente perceber que há coisas que não te interessam e há coisas que te interessam. E mesmo depois de entrares – eu entrei com aquela mentalidade de, se eu não gostar disto, eu vou procurar outra coisa. Eu acho que nos primeiros anos, tu não perdes nada em fazer isso. Por um lado, estás a ganhar experiência naquele trabalho, que depois vai contar quando estiveres à procura de outro. E também ficas a conhecer outras coisas. E eu acho que não é tão difícil arranjar trabalho em Portugal como às vezes se diz.

II) Com o nosso curso e mestrado...

É isso. Outros cursos conseguem arranjar. Com o nosso é se calhar mais fácil, não tenho muitas dúvidas. Até mesmo as pessoas vão mais preparadas que nos outros cursos, a exigência é outra.

12) E que conselho darias a alunos que estão na dúvida entre ir já trabalhar ou continuar a estudar?

Das pessoas que conheço que andam no doutoramento, acho que é um bocadinho diferente. Ir trabalhar é ir fazer logo algo prático, ganhar experiência a pôr em prática algo. Pode não ser o que aprendeste, ou pode ser o que aprendeste, pode ser um bocadinho dos dois. O doutoramento é mais para quem gosta de estudar e quer seguir outra área – de ensino ou investigação – sendo que investigação também podes fazer em certas empresas. Mas acho que a diferença principal é essa: o trabalho é logo algo prático.

“ir trabalhar é [...] ganhar experiência a pôr em prática algo”

Espetro de Dirac e Método das Soluções Fundamentais

- um estudo numérico

Por: Francisco Bento

Resultados sob a orientação dos professores Juha Videman e Pedro Antunes

De entre todos os possíveis tambores de área fixa, qual é o tambor capaz de produzir a frequência mais baixa, isto é, o som mais grave? Em 1887, Lord Rayleigh conjecturou no livro *The Theory of Sound* que tal tambor seria o círculo. Porém, problemas muito semelhantes a este, além de se prolongarem até ao presente (de formas distintas como iremos ver) são, na realidade, muito antigos. Um destes problemas é o famoso problema de *Dido*, a lendária fundadora e primeira rainha de Cartago, que nos questiona qual é a figura plana de maior área para um dado perímetro. Este tipo de problemas é conhecido como um *problema isoperimétrico* e, tal como o problema de Rayleigh, também para o problema de Dido foi conjecturado que o círculo seria a solução óptima. E, tal como a conjectura de Rayleigh, provou-se que, de facto, o domínio ótimo é o círculo. No entanto, este tipo de questões é surpreendentemente difícil de resolver: enquanto o problema de Dido apenas foi resolvido no século XIX, dando azo ao desenvolvimento do Cálculo das Variações, também Rayleigh não viveu para ver a prova à sua conjectura.

Hoje, este famoso resultado é conhecido como a *desigualdade de Rayleigh-Faber-Krahn* que é enunciada da seguinte forma:

Teorema (Rayleigh-Faber-Krahn): Seja $\Omega \subset \mathbb{R}^d$ um domínio limitado e Ω^* uma bola com o mesmo volume de Ω . Então, o primeiro valor próprio $\lambda_1(\Omega)$ da equação

$$-\Delta u = \lambda u, \text{ em } \Omega \quad u = 0, \text{ na } \partial\Omega$$

satisfaz a desigualdade $\lambda_1(\Omega^*) \leq \lambda_1(\Omega)$.

A equação acima, $-\Delta u = \lambda u$ é conhecida como a equação de Helmholtz, que descreve o espetro do operador de Laplace, e surge, neste contexto, através da equação das ondas $u_{tt} = c^2 \nabla_x u$, onde as frequências da membrana vibratória (neste caso um tambor) com as extremidades fixas (daí as condições de fronteira acima) são dadas por $\kappa = \sqrt{\lambda}$. Porém, não é um resultado trivial que tais valores próprios existam, e em que condições podem existir: tal resultado é um importante teorema em Análise Funcional. Assim, será de esperar que problemas semelhantes sejam também eles tortuosos e difíceis de abordar. E é aqui que métodos numéricos entram.

O método que vamos abordar é atualmente conhecido como o *Método das Soluções Fundamentais* (MFS), embora durante vários anos tenha tido diferentes nomes em diferentes áreas. Introduzido por Kupradze e Aleksidze, o MFS é diferente dos típicos métodos numéricos para resolver Equações de Derivadas Parciais (EDPs), onde é necessário discretizar numa malha o domínio em que estamos interessados. É, na realidade, um método sem malha, *meshless*, e é particularmente poderoso para equações do tipo elíptico, como acima, onde é possível de serem extraídas soluções fundamentais Φ que satisfazem $p(\partial)\Phi = \delta$, onde $p(\partial) = \sum_{i=1}^d c_i \frac{\partial}{\partial x_i}$ e δ é o conhecido Delta de Dirac (Dirac que inclusivamente reaparecerá à frente). No caso da equação de Helmholtz acima, a duas dimensões, a solução fundamental que nos interessa é dada por $\Phi_\lambda(x) = \frac{i}{4} H_0^{(1)}(\sqrt{\lambda}\|x\|)$ onde $H_0^{(1)}$ é chamada da função de Hankel de primeiro tipo e grau zero.

O interessante de tal solução fundamental é que, para cada λ, Φ_λ é, por construção, solução da equação de Helmholtz no interior e, consequentemente, qualquer combinação linear destas soluções fundamentais! Assim, tomando $\tilde{u} = \sum_{i=1}^n \alpha_i \Phi_\lambda(x - y_i)$ como a nossa aproximação numérica, onde os pontos y_i são tomados numa fronteira artifical $\hat{\Gamma}$ no exterior de Ω , basta descobrirmos os coeficientes α_i que satisfazem a equação na fronteira, reduzindo assim a dimensão do problema. Aqui, porém, não nos iremos tanto focar no método em si, mas no problema em mão. Ainda assim, convém ressalvar que, embora intuitiva, a aproximação numérica acima não é trivial: prova-se que o conjunto

$$S_{\Gamma, \hat{\Gamma}, \Omega} = \text{span} \left\{ \Phi_\lambda(x - y) \Big|_{\Omega} : y \in \hat{\Gamma}, \lambda \in I \right\}$$

com $I = \mathbb{R}^+$, é denso em $L^2(\Omega)$, o espaço das funções cujo quadrado é integrável em Ω .

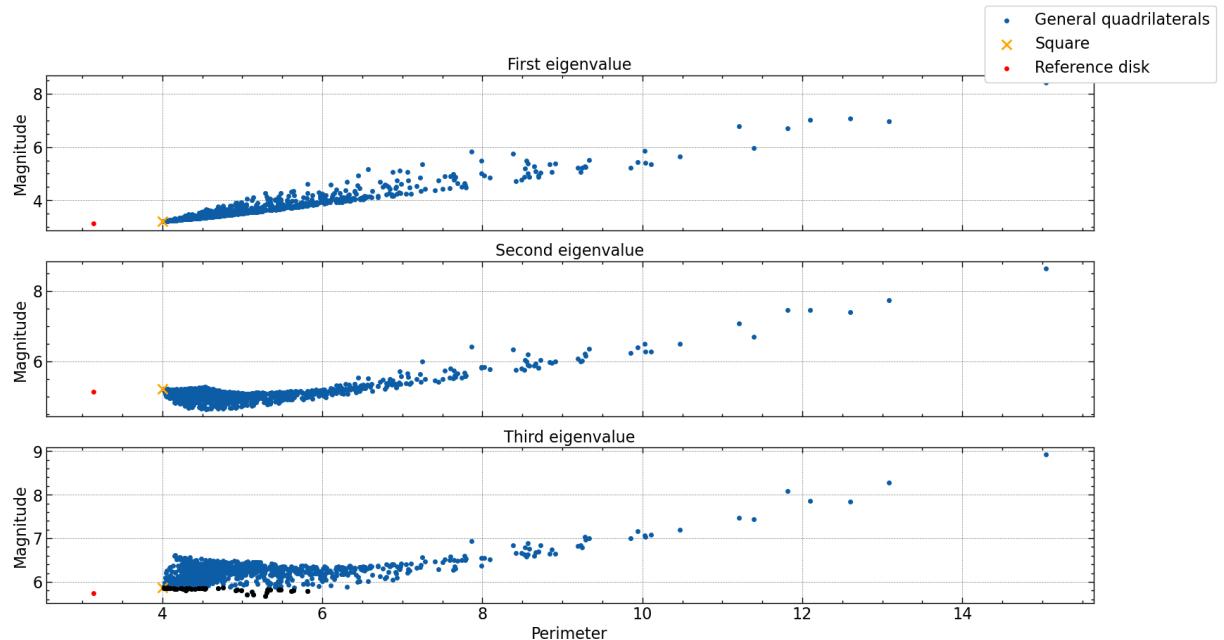
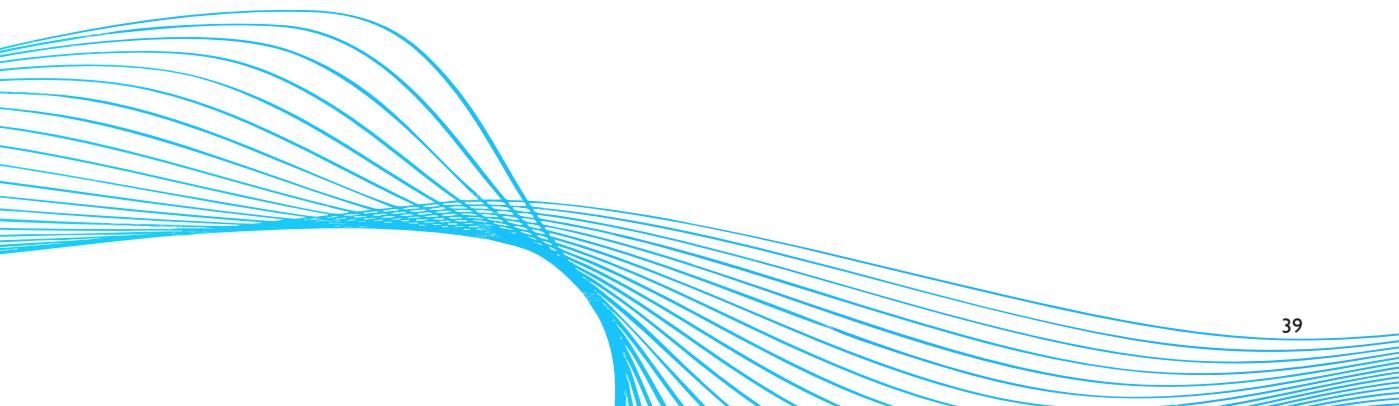
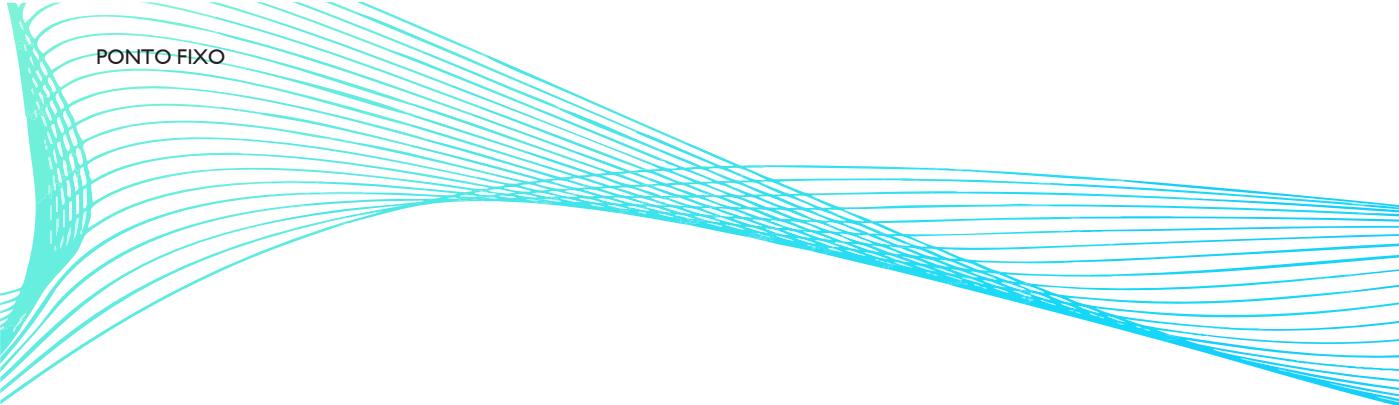


Figura 1: Simulações numéricas para os três primeiros valores próprios. A preto, assinalamos alguns “outliers”. Estes resultados tomam $m = 1$.





No entanto, o problema de determinar as frequências produzidas por um tambor não se prende exclusivamente à música: na mecânica quântica, a equação de Schrödinger (independente do tempo), é um caso particular da equação de Helmholtz acima, onde os valores próprios representam os níveis de energia que uma partícula pode tomar; e no caso relativístico, obtemos a equação de Dirac, que nos permite uma descrição ainda mais fiel da realidade. Esta equação interessa-nos pois têm sido descobertos, nos últimos anos, vários materiais (chamados de *Dirac materials*) cuja estrutura é descrita através desta, como é o caso dos eletrões em moléculas de grafeno. Num domínio limitado $\Omega \subset \mathbb{R}^2$, a equação de Dirac é dada por

$$\begin{pmatrix} m & -i(\partial_1 - i\partial_2) \\ -i(\partial_1 + i\partial_2) & m \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = E \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$$

onde são impostas as condições de fronteira $u_2(x) = i(n_1 + in_2)u_2$ (onde $m \geq 0$ é a massa da partícula, n_1 e n_2 são as componentes da normal exterior unitária e $u_1, u_2 : L^2(\Omega) \rightarrow \mathbb{C}^2$). O problema desta formulação é que é bastante mais difícil de abordar do que a equação de Helmholtz acima (embora esta possa ser transformada numa forma da equação de Helmholtz!) e resultados como o Teorema acima não passam de conjecturas. Porém, usando o nosso método numérico, conseguimos obter incríveis aproximações numéricas capazes de criar novas (e destruir antigas!) conjecturas.

Na Figura 1 apresentamos os três primeiros valores próprios de quadriláteros arbitrários (com área unitária). Uma constatação interessante é o facto de, aparentemente, termos uma versão análoga do Teorema acima para quadriláteros, algo que também acontece no operador de Laplace. Mas mais interessante ainda, é que o terceiro valor próprio do operador de Dirac não segue o terceiro valor próprio do operador de Laplace, que também ele aparenta ser minimizado no disco. Aliás, existem quadriláteros cujo terceiro valor próprio não só é menor do que o terceiro valor próprio no quadrado, mas também é menor que o do disco, o que vai contra todas as expectativas que tínhamos!

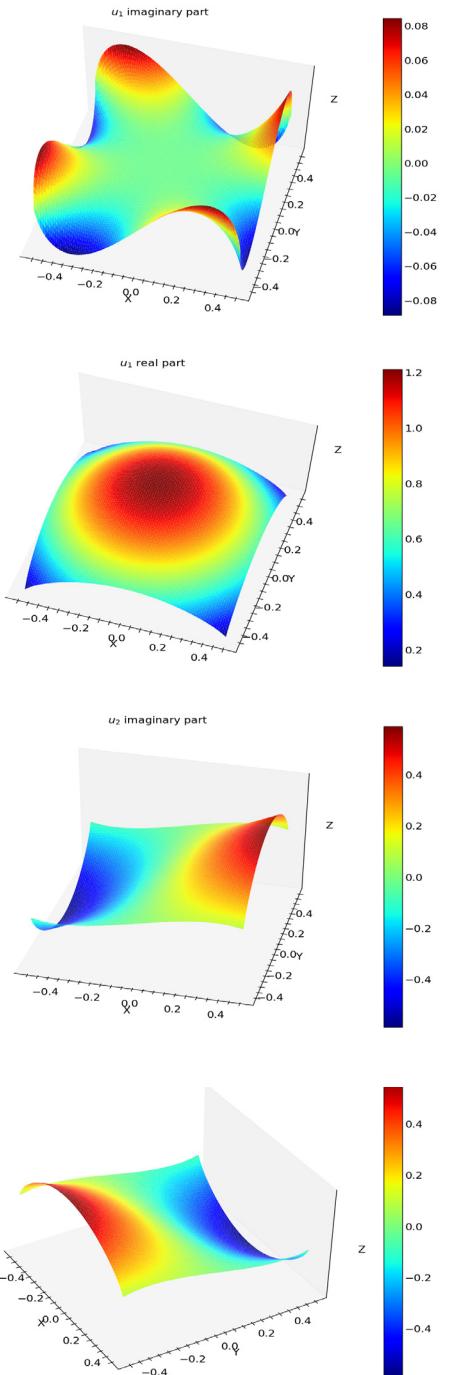


Figura 2: Aproximação numérica da primeira função própria do operador de Dirac no quadrado. Estes resultados tomam $m = 1$.

Há ainda muito por fazer: desde problemas mais “simples” como o estudo do espetro em domínios como triângulos e retângulos até a um tão desejado análogo ao Teorema de Rayleigh Faber-Krahn, o estudo da configuração geométrica otimal para o espetro do operador de Dirac é uma área extremamente rica em problemas em aberto. Para os curiosos, deixamos as funções próprias associadas ao primeiro valor próprio do quadrado cujo valor é $\lambda_1 \approx 3.204825$ (ver Figura 2), assim como a comprovação numérica que, entre todos os retângulos de área unitária, o primeiro valor próprio é minimizado pelo quadrado (ver Figura 3).

Quem sabe se talvez estes resultados não sejam, um dia, fundamentais para desenhar os materiais do futuro...?

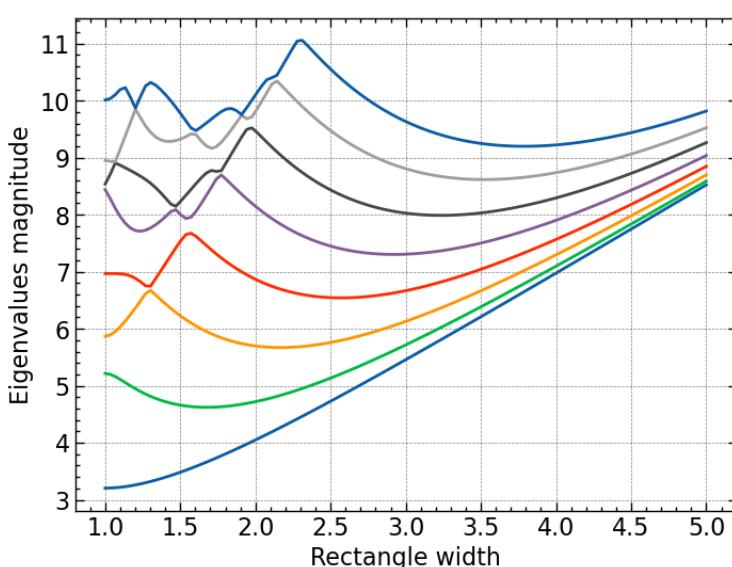


Figura 3: Simulações numéricas para os oito primeiros valores próprios, para retângulos de lados (a, a^{-1}) . A interseção de alguns valores próprios representa a multiplicidade algébrica do valor próprio. Estes resultados tomam $m = 1$.

Referências

- [1] Alves, C. J. S., & Chen, C. S. (2005). A new method of fundamental solutions applied to nonhomogeneous elliptic problems. *Advances in Computational Mathematics*, 23, 125–142.
- [2] Antunes, P. R. S. et al. (2021). A variational formulation for Dirac operators in bounded domains. Applications to spectral geometric inequalities. *Communications in Mathematical Physics*, 386(2), 781–818.
- [3] Briet, P., & Krejčířík, D. (2022). Spectral optimization of Dirac rectangles. *Journal of Mathematical Physics*, 63(1).
- [4] Olmo, I., & Beltrán, C. (2021, January). Sobre mates y mitos. *El País*. <https://elpais.com/ciencia/2021-01-04/sobre-mates-y-mitos.html>
- [5] Courant, R., & Hilbert, D. (2008). *Methods of mathematical physics: Partial differential equations*. John Wiley & Sons.
- [6] Daners, D. (2011). Krahn's proof of the Rayleigh conjecture revisited. *Archiv der Mathematik*, 96(2), 187–199.
- [7] Kac, M. (1966). Can one hear the shape of a drum? *The American Mathematical Monthly*, 73(4, Part 2), 1–23.

Problema do Planeamento Probabilístico

Por: Diogo Vieira

O problema do planeamento trata-se de um dos mais antigos e estudados problemas no mundo da inteligência artificial: como poderá um agente, partindo de um estado inicial, atingir um certo objetivo tendo à sua disposição um conjunto de ações que pode realizar sequencialmente?

Nas primeiras abordagens a este tema faziam fortes assunções relativas ao conhecimento e controlo do agente sobre o mundo. Uma delas é a de que, por hipótese, as consequências das ações são previsíveis e determinísticas. Traduzindo para linguagem de teoria da computação: o estado inicial é conhecido, as consequências de cada ação são também conhecidas e não há mudanças de origem externa no estado do sistema. Neste caso, basta deduzir um conjunto de ações que levem o sistema do estado inicial ao estado objetivo.

No entanto, como bem sabemos, no nosso mundo reina a imprevisibilidade, pelo que esta abordagem é algo utópica e não apresenta grandes aplicações práticas. De modo a tentar criar um modelo que melhor simulasse processos do mundo real, procurou-se relaxar algumas das assunções feitas anteriormente. O que aconteceria se as consequências de cada ação não fossem determinísticas? E se, para além disso, não conseguíssemos saber com certeza em que estado se encontra o sistema? Ou se, porventura, o estado do sistema pudesse ser alterado por fatores externos? Todos estes cenários são bastante plausíveis se estivermos a estudar fenómenos e processos relacionados com a vida real. Ao problema de planeamento em que existe incerteza sobre os resultados das ações e sobre o estado do sistema chamamos **Problema do Planeamento Probabilístico**.

Problema do Planeamento Clássico	Problema do Planeamento Probabilístico
O estado inicial é conhecido	Distribuição de probabilidade sobre o estado inicial
Consequências das ações determinísticas	Transições estocásticas
Capacidade total de saber o estado do sistema	Observações parciais do estado do sistema
Não há influência de fatores externos	Fatores externos podem provocar transições de estado

Tabela 1: Planeamento clássico vs. probabilístico

Repare-se que, uma vez que no modelo antigo o estado inicial é conhecido e as ações são determinísticas, não é sequer necessária qualquer capacidade de observar o estado atual do sistema (basta calcular sucessivamente a transição de estados a cada ação realizada). A capacidade do agente de prever sem falhas o que irá acontecer compensa a sua falta de capacidade de observar o mundo.

Uma evolução natural desta última abordagem é olhar para o problema de planeamento como uma cadeia de Markov.

Definição: Uma Cadeia de Markov é composta por um tuplo $(\mathbb{Q}, \Sigma, t, \mathbf{M}_a, \mathbf{R}_a)$ tal que:

- \mathbb{Q} : conjunto de n estados
- Σ : conjunto de ações
- Tempo discretizado ($t = 0, 1, \dots$)
- $\mathbf{M}_a \in M_{n,n}(\mathbb{R})$: matriz de transição associada à ação a
- $\mathbf{R}_a \in M_{1,n}(\mathbb{R})$: vetor de recompensa associado à ação a

Em cada instante o sistema ocupa um só estado. Se o sistema estiver no estado s_i e a ação a for executada, a probabilidade de transitar para o estado s_j é dada por $\mathbf{M}_a[i, j]$ e é obtida uma recompensa dada por $\mathbf{R}_a[j]$. Note-se que a soma de cada linha da matriz \mathbf{M}_a é igual a 1. Dizemos que matrizes com esta propriedade são estocásticas por linhas.

É fácil perceber a relação entre uma Cadeia de Markov e o modelo previamente descrito, sendo a principal diferença a introdução de um sistema de recompensas.

No seu artigo, *On the undecidability of probabilistic planning and related stochastic optimization problems*, Omid Madani, Steve Hanks e Anne Condon estudam este problema interpretando-o não como uma cadeia de Markov mas como um autómato probabilístico finito.

Definição: Um Autómato Probabilístico Finito é composto por:

- \mathbb{Q} : conjunto de n estados
- Σ : alfabeto de entrada
- T : conjunto de matrizes estocásticas por linhas $n \times n$
- $s_1 \in \mathbb{Q}$: o estado inicial
- $s_n \in \mathbb{Q}$: o estado de aceitação

Este ocupa um só estado em \mathbb{Q} em qualquer instante e em cada passo transita estocasticamente para outro estado. A transição de estado dá-se da seguinte forma: o atual símbolo de entrada, a , determina uma matriz de transição M_a ; o estado atual s_i determina a linha $M_a [i, .]$, uma distribuição de probabilidade sobre os próximos estados, o sistema altera-se de acordo com essa distribuição de probabilidade.

Definição: Dizemos que um Autómato Probabilístico Finito *aceita a palavra* $w \in \Sigma^*$ se o autómato termina no estado de aceitação após a ler, caso contrário dizemos que a rejeita.

Fixemos $0 < p < 1$. A pergunta “será que existe um conjunto de ações que leva o sistema do estado inicial para o estado final com probabilidade superior a p ?” traduz-se para “será que existe uma palavra que o autómato aceita com probabilidade superior a p ?”.

Para responder a esta pergunta os autores reduzem o problema em questão a um dos mais conhecidos problemas indecidíveis no mundo da teoria da computação, o *Halting Problem* ou Problema da Terminação: dado um programa e um *input* será que o programa para?

De modo a poder explorar esta pergunta, introduzimos a seguinte definição:

Definição: Um conjunto D diz-se decidível se existir uma função total computável, h , tal que $h(x) = 1$ se $x \in D$ e $h(x) = 0$ caso contrário.

Indecidibilidade do Halting Problem

Consideremos uma pergunta mais específica. Se aplicarmos um programa a si próprio, conseguimos saber se este irá parar?

Suponhamos que sim, sendo f a função que, dado

um programa, nos responde à pergunta (retorna 1 se o programa para quando lhe é dado como *input* o próprio programa, e 0 caso contrário) e seja P a função que retorna 1 se receber um programa e 0 caso contrário. Considere-se o seguinte programa:

```
def T(W):
    if P(W) == 0:
        return 1
    else:
        if f(W) == 1:
            loop forever
        else:
            return 1
```

Como podemos ver, T termina se e só se:

1. W não for um programa ou
2. W não terminar

O que acontece se dermos T como *input* a si próprio, $T(T)$? Como T é um programa, o caso 1 não se verifica, logo T só termina se o caso 2 se verificar. Ou seja, T só termina se T não terminar. Chegamos a uma contradição, pelo que a suposição inicial de que a função f existe é falsa. Assim sendo, o Problema da Terminação não é decidível.

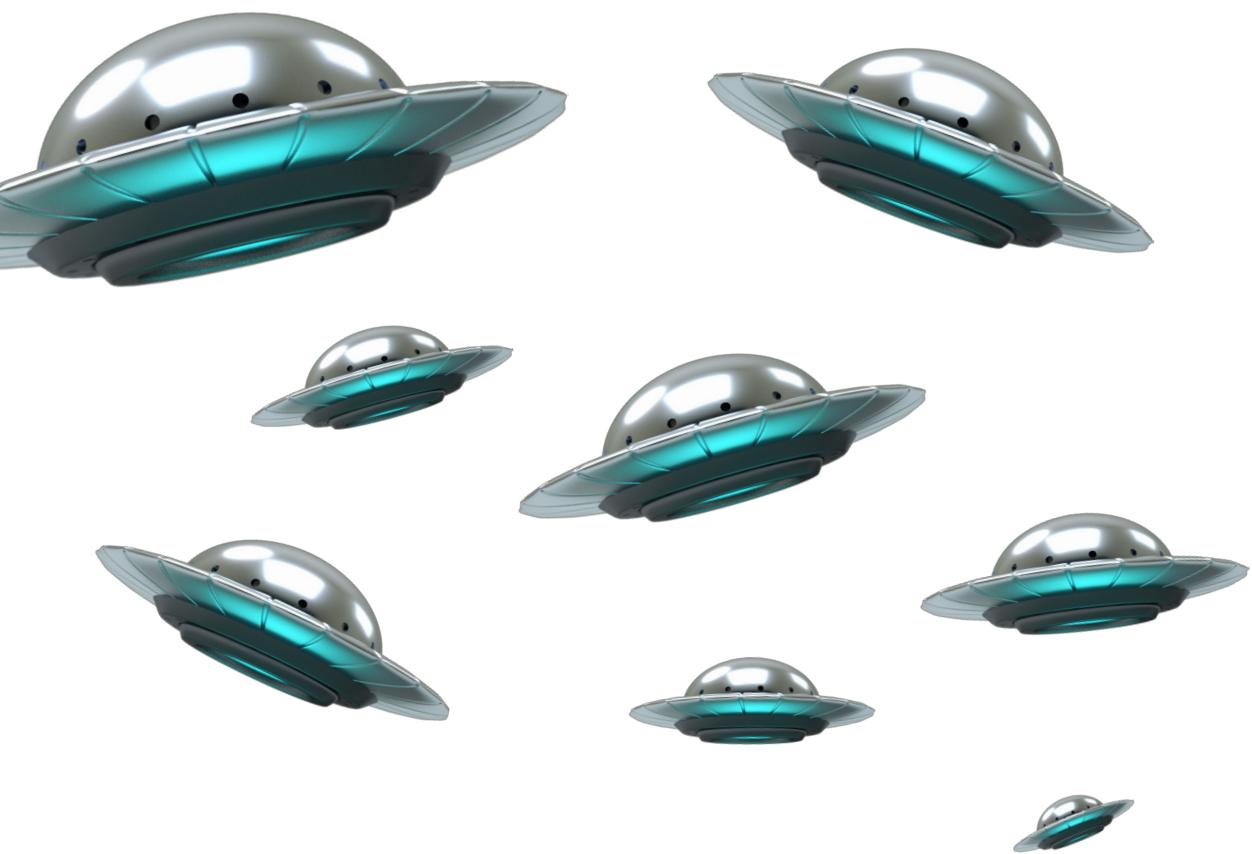
Da indecidibilidade do Problema da Terminação deduzimos então a indecidibilidade do Problema do Planeamento Probabilístico. Isto permite-nos concluir que se o agente apenas tiver conhecimento e controlo parcial do mundo não conseguimos ter quaisquer garantias quanto à probabilidade de este atingir um estado objetivo definido.

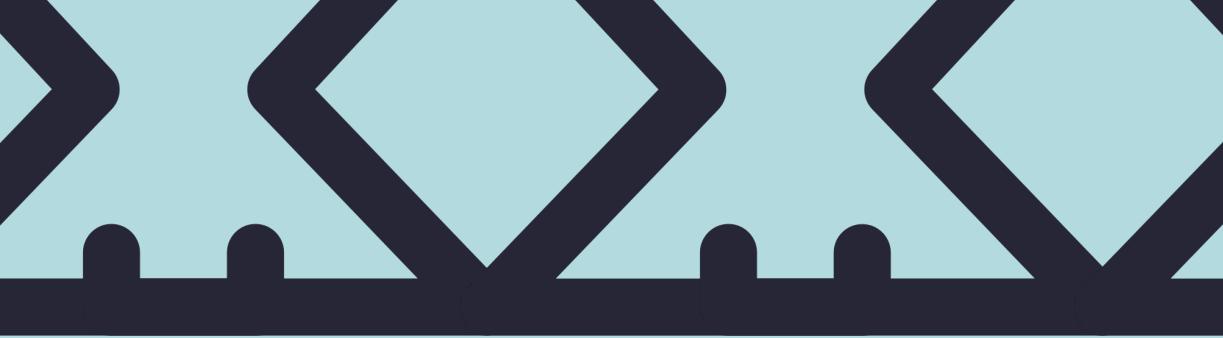
Referências

- [1] Madani, O., Hanks, S. & Condon, A. (2001). *On the undecidability of probabilistic planning and related stochastic optimization problems*.

Aliens Matemáticos

Por: Duarte Fragoso





A Magia das Séries

É muito fácil para um matemático apaixonar-se por séries de Taylor. Parece surreal descrever totalmente uma função usando apenas uma quantidade numerável de coeficientes. Podemos talvez, com pouco cuidado, tentar usar estas séries para tentar atacar problemas matemáticos mais complexos.

Olhemos para a equação $y'(x) = y(x)$ com $y(0) = 1$, que qualquer matemático conhece bem. Se procurarmos uma solução na forma de série, $y = \sum_{n=0}^{+\infty} a_n x^n$ facilmente verificamos que a equação diferencial acima se reduz à equação

$$\sum_{n=1}^{+\infty} a_n n x^{n-1} = \sum_{n=0}^{+\infty} a_n x^n$$

Comparando termos da mesma ordem obtemos a seguinte fórmula recursiva,

$$a_{n+1} = \frac{1}{n+1} a_n \Rightarrow a_n = \frac{1}{n!}$$

que nos dá a solução $y(x) = \sum_{n=0}^{+\infty} \frac{1}{n!} x^n$ (fixando $a_0 = 1$). Esta solução é exatamente o que esperávamos inicialmente: a nossa querida função exponencial!

Depois deste sucesso, um jovem matemático distraído poderá sentir-se preparado para resolver qualquer equação diferencial que o enfrente. Mas será que a história realmente acaba assim?

Problemas

Desconfiado, um matemático mais experiente decide experimentar o método noutra equação (com a mesma condição inicial): $x^2 y'(x) + y(x) = x$.

Agora, a série obtida $\sum_{n=0}^{+\infty} (-1)^n n! x^n$, é completamente divergente! O que poderemos fazer com ela? Certamente terá alguma informação sobre a solução, mas não é uma série de Taylor... Em física chamaríamos a este percalço de “fenômeno não-perturbativo”, em matemática diríamos que foi cometido um erro. Vejamos se, de alguma forma, conseguimos extrair da nossa série divergente uma função.

O primeiro ingrediente desta nova receita é a função *gamma*, que tem a importante propriedade $\Gamma(n+1) = n!$, para números naturais. Agora podemos reescrever a nossa série:

$$\begin{aligned} \sum_{n=0}^{+\infty} (-1)^n n! x^n &= \sum_{n=0}^{+\infty} (-1)^n \Gamma(n+1) x^n \\ &= \sum_{n=0}^{+\infty} \left((-1)^n x^n \int_0^{+\infty} e^{-\xi} \xi^n d\xi \right). \end{aligned}$$

Se substituirmos a variável de integração $\xi \mapsto \frac{\xi}{x}$ obtemos

$$\sum_{n=0}^{+\infty} \int_0^\infty e^{-\frac{\xi}{x}} (-1)^n \xi^n d\xi.$$

A expressão acima é precisamente a série divergente inicial, mas relembraremos o nosso objetivo: gostaríamos de extrair uma função de alguma forma relacionada com a série. Para tal, troquemos a ordem do somatório e do integral

$$\int_0^\infty \sum_{n=0}^{+\infty} e^{-\frac{\xi}{x}} (-1)^n \xi^n d\xi = \int_0^\infty \frac{e^{-\frac{\xi}{x}}}{1+\xi} d\xi.$$

Note-se que este último passo é matematicamente ilegal! O matemático experiente poderá, neste ponto, sentir-se tentado a abandonar toda esta ideia. Mas, como por magia, o resultado obtido por estes meios questionáveis é a solução da equação diferencial!

A coragem de Borel

A razão pela qual o nosso método funciona na equação diferencial anterior é bastante profunda e interessante, dando origem a resultados clássicos em Análise Assimptótica.

Em geral, o método anterior define uma operação que transforma séries (possivelmente divergentes) em funções,

$$\sum_{n=0}^{\infty} a_n x^n \mapsto \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n \mapsto \int_0^{\infty} \left(\sum_{n=0}^{\infty} \frac{a_n}{n!} x^n \right) e^{-\xi} d\xi,$$

chamada *Ressomação de Borel*¹, e usamos $\mathcal{S}_0(\sum_{n=0}^{+\infty} a_n x^n)$ para prever a expressão final obtida acima.

Claro que há ainda séries tão divergentes que dividir cada termo por $n!$ não resolve o problema de convergência. Temos portanto de nos restringir aos casos em que tal não ocorre. Adicionalmente, vamos considerar que a função definida por $\sum_{n=0}^{+\infty} \frac{a_n}{n!} x^n$ se estende a quase todo² o plano complexo. A este procedimento chamamos *continuação analítica* e é altamente não-trivial!

Os aliens

A operação definida pode ter, no entanto, uma outra obstrução: o que aconteceria se a função dada por $\sum_{n=0}^{+\infty} \frac{a_n}{n!} x^n$ tivesse alguma singularidade em \mathbb{R}^+ ? Neste caso, o integral diverge e parecemos voltar a um problema desastroso... A única forma de evitar tudo isto é contornar a singularidade ou por cima ou por baixo.

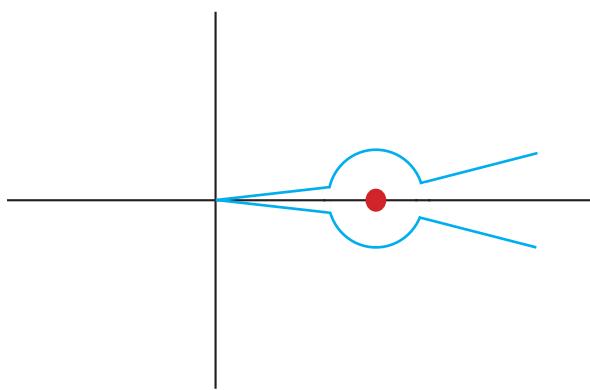


Figura 1: Singularidade em \mathbb{R}^+ .

As duas fórmulas obtidas nas duas situações, denotadas por $\mathcal{S}_+(\sum_{n=0}^{+\infty} a_n x^n)$ e $\mathcal{S}_-(\sum_{n=0}^{+\infty} a_n x^n)$ em geral vão ser diferentes. A pergunta natural agora é se se relacionam de alguma forma. Podemos definir, esperançosamente, um operador \mathfrak{S} que obedeça à seguinte equação:

$$\mathcal{S}_+ = \mathfrak{S} \circ \mathcal{S}_-$$

Assim, toda a informação sobre o que ocorre quando "saltamos" acima³ de \mathbb{R}^+ está codificada por \mathfrak{S} . A definição e o estudo deste operador foi feito pelo fundador⁴ da Ressurgência, uma área da matemática relativamente recente! Se não fixarmos a condição inicial da equação diferencial, deixando-a como variável, σ , o teorema de Écalle diz-nos que se a solução $u(x, \sigma)$ de uma equação diferencial é dada por Ressomação de Borel de alguma série, numa região "abaixo" de \mathbb{R}^+ , então a solução da equação na região acima é dada por $u(x, \mathfrak{S}(\sigma))$, para uma função \mathfrak{S} relativamente fácil de calcular. Em suma, o teorema diz-nos o seguinte:

$$\mathfrak{S}u(x, \sigma) = u(x, \mathfrak{S}(\sigma))$$

Na literatura diz-se que o operador \mathfrak{S} é um exemplo de um operador alien. Tem este nome porque tem como elementos básicos operadores (quase)diferenciais chamados derivadas alien, erroneamente traduzido do francês étranger. Pelo facto de se parecerem tanto com derivadas comuns, é possível desenvolver toda uma teoria "diferencial" que tem o nome de Cálculo alien⁵.

À volta da superfície

Antes de ver as implicações do teorema acima, temos de nos perguntar o seguinte: O que queremos dizer realmente com uma solução de uma equação diferencial em \mathbb{C} ?

Quando aplicável, sabemos que o teorema de Picard-Lindelof nos fornece uma solução única numa vizinhança da condição inicial. Podemos então utilizar continuação analítica para definir o resto da nossa função. Esta definição tem consequências surpreendentes quando, por exemplo, olhamos para a equação diferencial do logaritmo. Se fizemos a continuação analítica partindo do ponto $z_0 \in \mathbb{C} \setminus \{0\}$ por um caminho que dê uma volta à origem e retorne ao mesmo ponto descobrimos que adquirimos um fator de $2\pi i$ na nossa continuação analítica. Desta forma, o logaritmo está definido mais naturalmente na seguinte superfície:

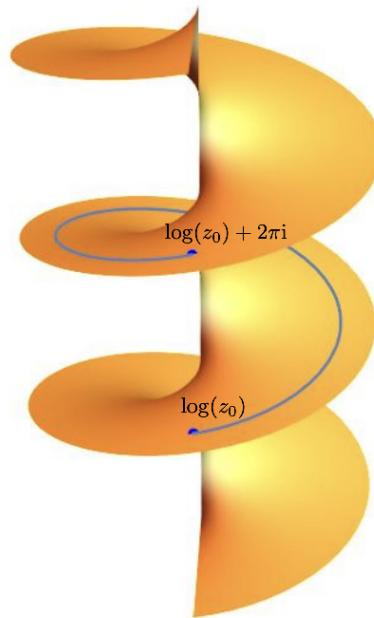
¹ Traduzido do inglês *Borel Resummation*.

² Com isto queremos dizer que se estende a todo \mathbb{C} exceto num conjunto de pontos isolados.

³ Em prática, as diferentes regiões são sectores de \mathbb{C} cujas divisórias são todos os raios que começam na origem e passam em cada singularidade de $\sum_{n=0}^{+\infty} \frac{a_n}{n!} x^n$.

⁴ Jean Écalle, em *Les Fonctions Résurgentes*.

⁵ Descobre mais sobre o impacto destas ideias em física em <https://www.quantamagazine.org/alien-calculus-could-save-particle-physics-from-infinities-20230406/> onde, entre outros cientistas, o professor Ricardo Schiappa do departamento de Matemática foi retratado.



Outro exemplo natural é a função raiz quadrada que desta vez, se define naturalmente numa superfície com duas “voltas”:



Figuras 2 e 3: Superfícies do logaritmo e raíz quadrada.

O mágico teorema de Écalle permite-nos então conhecer o número de voltas da superfície associada a uma equação diferencial olhando apenas para a função \mathbb{S} . Este resultado é particularmente interessante porque através de informação que aparenta ser local conseguimos desvendar um comportamento global da solução!

Referências

- [1] Aniceto, I., Başar, G., & Schiappa, R. (2019). A primer on resurgent transseries and their asymptotics. *Physics Reports*, 809, 1.
- [2] Écalle, J. (1981, 1985). Les fonctions résurgentes. *Prépublications Mathématiques* 81-05, 81-06, 85-05. Université Paris-Sud.
- [3] Mitschi, C., & Sauzin, D. (2016). Divergent series, summability and resurgence I: Monodromy and resurgence. *Lecture Notes in Mathematics* (Vol. 2153).
- [4] Loday-Richaud, M., & Remy, P. (2011). Resurgence, Stokes phenomenon and alien derivatives for level-one linear differential systems. *Journal of Differential Equations*, 250(3).
- [5] Fragoso, D. *Compactifying resurgence* (BSc Thesis).

Operadores de Toeplitz e Métodos de Aproximação

Por: Luís Carlos Miguelote Dias



A álgebra linear pode descrever-se de forma simples e resumida como o estudo de sistemas de equações lineares finitas. Esta tem uma irmã mais velha, a análise funcional, que por sua vez lida com o caso infinito. Não é difícil ver que cada sistema linear de equações finito pode ser reduzido ao caso infinito. Assim, podemos de certa forma dizer que a álgebra linear está “contida” na análise funcional. Mas e o contrário? Que pode a álgebra linear dizer acerca da análise funcional? Isto é exatamente uma das perguntas que o estudo de métodos de aproximação em análise numérica tenta responder.

Para poder analisar estes problemas começamos por introduzir o essencial: um espaço vetorial X complexo (possivelmente de dimensão infinita) equipado com uma norma $\|\cdot\|$ diz-se um espaço de *Banach* se é completo (cada sequência de Cauchy é convergente). Um operador linear $T: X \rightarrow Y$ entre espaços de Banach é definido de forma análoga ao caso finito onde, fixando as bases, podemos representar T como uma matriz infinita. Se munirmos um espaço de Banach X com um produto que faça de X um anel tal que $\|xy\| \leq \|x\| \|y\|$, diz-se que X é uma álgebra de Banach. Como exemplos de espaços de Banach temos $\ell^p(\mathbb{N}) = \{(x_k)_{k \in \mathbb{N}} : \sum_k |x_k|^p < \infty\}$ com norma $\|(x_k)\| = \sqrt[p]{\sum_k |x_k|^p}$ e operações ponto-a-ponto. Outro exemplo comum é o espaço de operadores limitados: se X é um espaço de Banach, então $\mathcal{L}(X) = \{T: X \rightarrow X \mid \exists M \geq 0 : \forall x \in X, \|Tx\| \leq M\|x\|\}$ com norma $\|T\| = \inf\{M \geq 0 : \forall x, \|Tx\| \leq M\|x\|\}$ que é uma álgebra de Banach sendo o produto a composição de operadores.

Finalmente podemos atacar o problema original, sendo o nosso foco dirigido para o espaço $\ell^2(\mathbb{Z})$ com a base canónica (e_k) . Dados $T \in \mathcal{L}(X)$ e $y \in \ell^2(\mathbb{N})$, resolver uma equação

$$Tx = y \quad (1)$$

não é uma tarefa trivial em dimensão infinita. Como sugerido na introdução, podemos considerar truncções do sistema de dimensão infinita para o caso $n \times n$ e analisar o comportamento das soluções com $n \rightarrow \infty$. Formalmente, considerando $P_n : \ell^2(\mathbb{N}) \rightarrow \ell^2(\mathbb{N})$ projeções tal que $P_n((x_k)) = (x_1, x_2, \dots, x_n, 0, \dots)$ queremos resolver

$$P_n T P_n x_n = P_n y_n. \quad (2)$$

Este é um método de aproximação conhecido como o *método da secção finita* (MSF) e é um dos mais utilizados devido à sua simplicidade. Outros métodos podem ser obtidos alterando as projeções e a sequência de operadores ($P_n T P_n$).

Contudo, o método só por si não é muito útil já que não temos garantias que as soluções x_n nos digam algo sobre x . Assim, para um operador T , dizemos que o MSF é *aplicável* a T , se, a partir de uma certa ordem, cada sistema do tipo (2) tem uma solução única para cada $y \in \ell^2(\mathbb{N})$, e estas soluções convergem para uma solução do tipo (1). A parte da existência e unicidade da solução pode ser resumida na seguinte condição: uma sequência de operadores limitada (A_n) diz-se *estável* se existe uma ordem n_0 tal que para todo $n \geq n_0$, os operadores A_n são invertíveis e $\sup_{n \geq n_0} \|A_n^{-1}\| < \infty$. Com esta propriedade, conseguimos dar condições necessárias e suficientes para a aplicabilidade do MSF (que se generaliza para qualquer método de aproximação arbitrário).

Teorema I (Polski). Seja $T \in \mathcal{L}(\ell^2(\mathbb{N}))$. O MSF é aplicável a T se e só se T é invertível e a sequência $(P_n T P_n)$ é estável.

Uma classe importante de operadores é a dos operadores de *Toeplitz*. Estes são operadores $T : \ell^2(\mathbb{N}) \rightarrow \ell^2(\mathbb{N})$ que são constantes nas diagonais, ou seja, que têm a seguinte forma matricial

$$\begin{bmatrix} a_0 & a_{-1} & a_{-2} & \cdots \\ a_1 & a_0 & a_{-1} & \ddots \\ a_2 & a_1 & a_0 & \ddots \\ \vdots & \ddots & \ddots & \ddots \end{bmatrix}. \quad (3)$$

Entre outras propriedades úteis, uma que se destaca é que se pode construir operadores de Toeplitz a partir de funções $a \in C(S^1)$ onde $S^1 \subseteq \mathbb{C}$ é o círculo unitário, usualmente denominadas de *símbolos*. Dado $a \in C(S^1)$, definimos os coeficientes de Fourier

$$\hat{a}_k := \frac{1}{2\pi} \int_0^{2\pi} a(e^{it}) e^{-itk} dt$$

e o operador de Toeplitz $T(a) = [\hat{a}_{i-j}]_{i,j \in \mathbb{N}}$. Conversamente, dado um operador de Toeplitz com a forma dada em (3), podemos recuperar o símbolo definindo $a(t) = \sum_{k \in \mathbb{Z}} a_k e^{ikt}$. Estes operadores são úteis em várias áreas da matemática como processamento de sinais, análise harmónica, e mais recentemente em redes neurais onde uma convolução 1D (resp. 2D) é dada por um operador de Toeplitz (resp. duplamente Toeplitz por blocos).

Como será que o MSF se comporta para esta classe especial de operadores? Para compreendermos a aplicabilidade do MSF a $T(a)$, segundo o Teorema de Polski, temos que entender a sua invertibilidade. Felizmente, recorrendo ao seu

símbolo, conseguimos uma boa caracterização. Se $0 \notin a(S^1)$, define-se *wind* a como o número de voltas que a dá em torno do 0 (*winding number*).

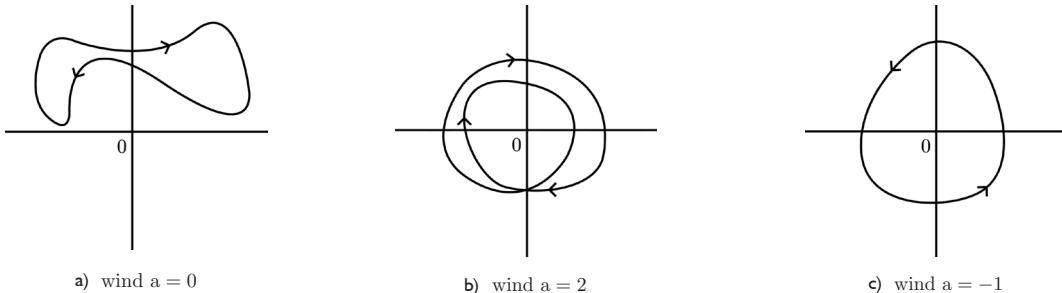


Figura 1: *winding number* de diferentes funções a .

Teorema 2. Se $a \in C(S^1)$, então $T(a)$ é invertível se e só se $0 \notin a(S^1)$ e $\text{wind } a = 0$.

Assim, metade das condições para a aplicabilidade do MSF estão caracterizadas. A boa notícia é que, na verdade, a invertibilidade de $T(a)$ é também suficiente para a estabilidade de $(P_n T(a) P_n)!$ Temos assim uma condição necessária e suficiente para conseguirmos resolver um sistema infinito $T(a)x = y$ utilizando apenas os métodos comuns da álgebra linear.

Teorema 3. Se $a \in C(S^1)$, o MSF é aplicável a $T(a)$ se e só se $T(a)$ é invertível.

Em geral, a parte interessante da aplicabilidade é a estabilidade da sequência. Para analisar a estabilidade é comum considerar a álgebra de Banach onde os elementos são sequências limitadas de operadores, usualmente denotada por \mathcal{F} . Neste contexto, a estabilidade de um elemento de \mathcal{F} corresponde exatamente à sua invertibilidade no quociente $\mathcal{F} / \mathcal{G}$, onde $\mathcal{G} \subseteq \mathcal{F}$ é o ideal das sequências que tendem para 0 em norma. O objetivo final é caracterizar a estabilidade em termos de invertibilidade de operadores limite. Para além do operador do limite (forte) $P_n T P_n \xrightarrow{s} T$, outros exemplos de operadores limites são $s\text{-lim } W_n T W_n$ e $s\text{-lim } V_{-\lceil nx \rceil} T V_{\lceil nx \rceil}$ com $x \in \mathbb{R}$, onde $W_n((x_k)) = (x_k, x_{k-1}, \dots, x_1, 0, \dots)$ e $V_m((x_k)_{k \in \mathbb{Z}}) = (x_{k-m})_{k \in \mathbb{Z}}$ é o operador de shift para a direita de $\lceil nx \rceil$ entradas. O s associado aos limites indica que se trata do limite forte.

Para além dos operadores de Toeplitz, outros exemplos considerados são operadores de Toeplitz de coeficiente variável, e operadores de banda. Contudo, a álgebra \mathcal{F} é demasiado grande e usualmente consideram-se subálgebras geradas por certas classes de operadores. No caso de operadores de Toeplitz, o facto de termos um símbolo gerador do operador permitiu uma simples caracterização da aplicabilidade do MSF, o que é mais um motivo pelo qual estes operadores são tão importantes.

Referências

- [1] Böttcher, A., & Silbermann, B. (2006). *Analysis of Toeplitz operators*. Springer.
- [2] Böttcher, A., & Silbermann, B. (1999). *Introduction to large truncated Toeplitz matrices*.
- [3] Hagen, R., Roch, S., & Silbermann, B. (2000). *C*-Algebras and Numerical Analysis*. CRC Press.
- [4] Mascarenhas, H., & Silbermann, B. (2016). Sequences of variable-coefficient Toeplitz matrices and their singular values. *Journal of Functional Analysis*, 270(4), 1479–1500.



Crítica por: Ana Sousa

“Well, then, it seems that your great big expensive machine doesn’t work.”

No mundo da matemática e da computação, o nome do inglês Alan Turing ocupa uma das posições de maior renome devido às suas importantes contribuições no que hoje conhecemos como computador. No entanto, para o cidadão comum, este nome poderá não despertar qualquer memória de quem este matemático terá sido. O que pouca gente sabe (porque assim teve de ser) é que, durante a Segunda Guerra Mundial, Turing foi capaz de desenvolver uma máquina que decifrava mensagens alemãs encriptadas, e estima-se que este feito acelerou a vitória dos Aliados em mais de dois anos, tendo previnido a morte de cerca de 14 milhões de pessoas.

**Nas palavras de Winston Churchill:
“Turing made the single biggest contribution
to Allied victory.”**

O filme biográfico “O Jogo da Imitação” (2014) mostra a corrida contra o tempo enfrentada por Turing e os seus colegas na descodificação de uma máquina encriptadora de informações vitais acerca dos planos de guerra alemães, conhecida como Enigma, durante a Segunda Guerra Mundial, na instalação militar secreta Bletchley Park.

Tratando-se de uma personagem com contribuições tão importantes para a História e uma vida altamente conturbada, as expectativas para este filme eram altas, e, de facto, ficou à altura. Com uma atuação fenomenal de Benedict Cumberbatch, que deixa transparecer as mágoas e aflições de Turing, e a capacidade do realizador norueguês Morten Tyldum de nos levar aos anos 40 e 50, com imagens comoventes do estado da Grã-Bretanha durante a Segunda Guerra Mundial, é difícil não ficar totalmente embrenhado no filme desde o primeiro minuto.

O filme não segue uma ordem cronológica, e alterna entre três épocas diferentes. A narrativa principal decorre-se em Bletchley, onde nos são mostrados os desafios de Turing e do resto da equipa ao desenvolver a máquina que ia decifrar o Enigma. Embora este seja o foco principal da história, o filme não entra muito em detalhe em relação ao funcionamento da máquina (o que também não era esperado), nem mostra a equipa de facto a trabalhar em algo matematicamente palpável. Matemáticas à parte, este lapso é compensado pelo resto que o filme tem para oferecer.

Uma das cenas que mais me tocou ocorre perto do início, em que Turing publica umas palavras cruzadas desafiadoras no jornal, de modo a atrair aqueles que as conseguissem resolver, e assim alargar a equipa. Vemos então, numa Grã-Bretanha degradada, pessoas abrigadas das incessantes bombas a tentar resolvê-las: soldados, idosos, mulheres. É uma cena poderosa, pois mostra a esperança das pessoas na existência de um futuro melhor, bem como uma tentativa de distração perante a calamidade ao seu redor.

A segunda narrativa do filme ocorre uns anos antes, nos anos 20, no colégio onde Turing estudou. É-nos mostrado, através da atuação brilhante e comovente de Alex Lawther, a vida já turbulenta de Turing, que sofria de bullying, bem como a bonita, embora curta, história de amor que este viveu com o seu colega Christopher, que o introduziu à criptografia, área para a qual Turing contribuiu em favor dos Aliados. Infelizmente, os seus feitos foram silenciados durante 50 anos, por ter sido um trabalho realizado em segredo.

Embora Turing tenha sido um dos pais da revolução tecnológica do final do século XX, isso não o impediu de ser julgado e condenado à castração química por ser homossexual, o que nos leva à terceira narrativa, que retrata a desumanidade com que foi tratado no final da sua vida.

Com uma atuação tão autêntica e realista de Cumberbatch, é difícil conter as lágrimas perante a miséria que tanto atormentou Turing no seu último ano de vida. Esta é certamente a cena mais impactante do filme, dando-lhe uma atmosfera emotiva da qual não saí ilesa.

A história de Alan Turing é comovente por si só, mas este filme trouxe à tona aquilo que antes só conseguíamos imaginar. Repleto de cenas emocionantes, qualquer espectador consegue perceber o papel crucial que Turing desempenhou durante a Segunda Guerra Mundial, ficando ao mesmo tempo a par da angústia que foi a sua vida.

Com uma conciliação harmoniosa entre os elementos a cumprir num filme biográfico e a interpretação comovente que nos é oferecida, este é um filme que me agradou muito pela experiência emocional que pude partilhar com a personagem, tendo-me dado a sensação de ter conhecido o próprio Alan Turing. Contando com um forte leque de atores, capazes de transparecer as emoções sentidas nos momentos vividos o mais autenticamente possível, bem como uma adaptação realista da Segunda Guerra Mundial, é impossível não se sentir dentro do filme do início ao fim.

Agradecimentos:

O NMATH quer agradecer a todos aqueles que nos apoiaram na realização deste projeto, seja na forma de aconselhamento, divulgação ou apenas incentivo, nomeadamente, ao Departamento de Matemática do Instituto Superior Técnico.

Ficha Técnica:

Ponto Fixo:
NMATH-IST
Avenida Rovisco Pais, nº1
Lisboa

Tipos de letra principais:

Humanst521 BT
Trebuchet MS
Cambria Math

Edição e revisão:

Diana Gaspar
Francisco Malaca
Isabel Nogueira
Laura Amorim
Madalena Preto
Mafalda Pires
Maria Madrugo
Martim Rêgo
Sofia Afonso

Design:

Francisco Gonçalves
Luísa Gonçalves

Intervalo:

André Guimarães
Madalena Preto

