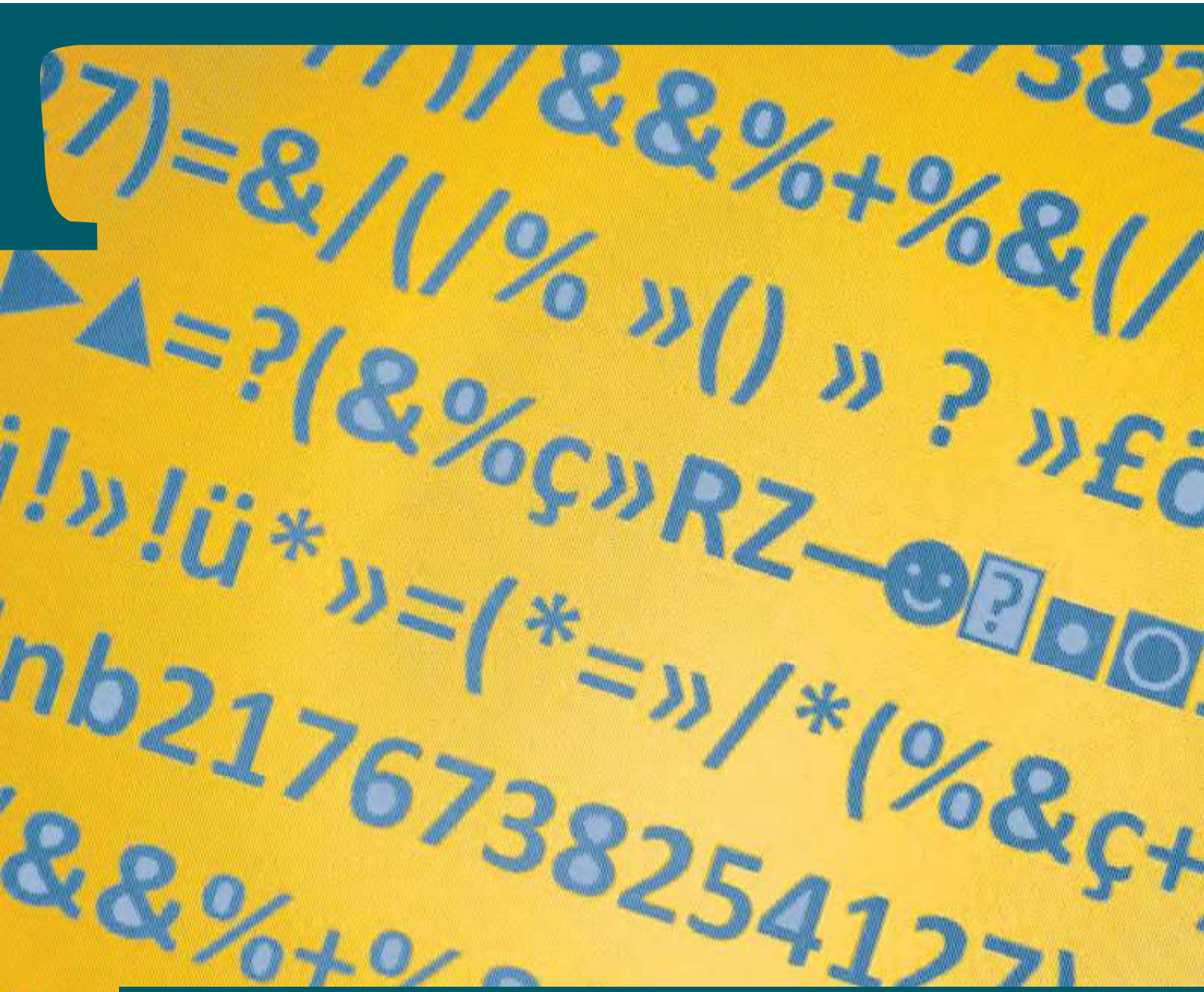

A IDENTIDADE TROPICAL $(x + y)^2 = x^2 + y^2$

Beites, P. D.[a] e Nicolás, A. P.[b]

[a]Universidade da Beira Interior e Centro de Matemática e Aplicações

[b]Universidad de Valladolid e Instituto de Investigación en Matemáticas

pbeites@ubi.pt[a] e alejandro.pinera@uva.es[b]

Mais vezes do que o desejável ocorre um erro: $(x+y)^2 = x^2 + y^2$. Mas será sempre um erro? Veremos que não! Mas, no rigor da matemática, há que saber o contexto em que se trabalha... Nomeadamente na Álgebra Tropical, área com aplicações na Criptografia, é uma identidade!

1. UM CONVITE TROPICAL

A surpresa do título culmina numa identidade que contraria, no contexto dos números reais, um conhecido caso notável. O despoletar dessa surpresa é assegurado pelo adjetivo tropical – alusão a uma homenagem de matemáticos franceses, fruto da sua visão do Brasil, ao colega brasileiro Imre Simon. Este foi pioneiro na aplicação do semianel tropical $(\mathbb{R} \cup \{\infty\}, \oplus, \odot)$, estrutura algébrica também conhecida pela designação min-mais, à Teoria da Otimização, [5, 9].

Tal surpresa, que poderia ser considerada uma provocação, é bem conseguida pela associação do símbolo $+$ à adição usual de números reais e, por conseguinte, da expressão $(x+y)^2$ ao chamado quadrado da soma dado por $(x+y)^2 = x^2 + 2xy + y^2$. Por este motivo, é habitual utilizar outro símbolo, como $\oplus$, para a adição no semianel $\oplus$ $\mathbb{R} \cup \{\infty\}$. Considerando a referida notação, a identidade tropical que contribui para o título escrever-se-ia assim na forma $(x \oplus y)^2 = x^2 \oplus y^2$.

O semianel tropical também marca presença na Ciência da Computação Teórica, destacando-se em aplicações a problemas de tipo Burnside em Teoria de Grupos e de Semigrupos, bem como a problemas de decidibilidade em Teoria de Linguagem Formal, [6]. Salientamos ainda a aplicação do mencionado semianel à Criptografia, a qual exploramos na secção 2. Em particular, destacamos as vantagens da utilização da Álgebra Tropical, com $\oplus$ e $\odot$, como suporte de esquemas criptográficos designados por tropicais.

Tópicos não diretamente criptográficos encontram-se em [9], introdução elementar que aborda aritmética, polinómios, curvas, filogenética e espaços lineares. Um maior grau de profundidade é alcançado em [5], que inclui as demonstrações do Teorema Fundamental da Geometria Algébrica Tropical e do Teorema de Estrutura para variedades tropicais. Na secção 3 focamo-nos numa vertente da Aritmética Tropical que se prende com o erro $(x+y)^2 = x^2 + y^2$ designado por *freshman's dream* para $x, y \in \mathbb{R}$, [4].

Outras designações associadas a este erro, na Didática da Matemática, são *linear misconception* e *illusion of linearity*, [1, 2]. O mesmo pode surgir por raciocínio indutivo, numa tentativa de estender a linearidade presente em certas situações a outras que dela carecem. Apesar de o raciocínio indutivo ser usado pelos matemáticos, uma conjetura tem de ser testada e demonstrada se for verdadeira. Mas, contrariamente aos matemáticos, a monitorização meta-discursiva não é uma prática generalizada entre alunos, [1].

2. CRIPTOGRAFIA TROPICAL

O semianel min-mais $(\mathbb{R} \cup \{\infty\}, \oplus, \odot)$ é por vezes denotado, seguindo a referida designação, por $(\mathbb{R} \cup \{\infty\}, \min, +)$. Salienta-se assim que as operações de adição tropical e de multiplicação tropical são definidas, essencialmente e respetivamente, como o mínimo e a adição usual de números reais:

$$x \oplus y := \begin{cases} \min\{x,y\}, & \text{se } x, y \in \mathbb{R} \\ x & \text{se } x \in \mathbb{R} \text{ e } y = \infty \\ y & \text{se } x = \infty \text{ e } y \in \mathbb{R} \\ \infty & \text{se } x = y = \infty \end{cases}$$

$$x \odot y := \begin{cases} x + y & \text{se } x, y \in \mathbb{R} \\ \infty & \text{se } x = \infty \text{ ou } y = \infty \end{cases}$$

Por exemplo, tem-se $3 \oplus 5 = 3$, $3 \odot 5 = 8$, $3 \oplus \infty = 3$ e $\infty \odot 5 = \infty$.

No que se segue, tentamos perceber a utilidade de $\oplus$ e $\odot$ na Criptografia, por esta razão dita tropical. De um modo geral, a Criptografia trata de encontrar técnicas que permitam a transmissão de informação através de um canal, usualmente a Internet, preservando a sua integridade e a sua confidencialidade. Quanto ao número de chaves, há três tipos de Criptografia: simétrica ou de chave privada (uma chave); assimétrica ou de chave pública (duas chaves); funções de Hash (num certo sentido, nenhuma chave).

No tipo de Criptografia adjetivada de assimétrica, os protocolos utilizados estão baseados no uso de duas chaves: uma pública e uma privada. A chave pública é utilizada pelo emissor para cifrar (ou encriptar) a mensagem que se pretende transmitir, é difundida pelo recetor e pode ser conhecida por qualquer pessoa. Contrariamente, a chave privada é apenas conhecida pelo recetor e será utilizada por este para decifrar (ou desencriptar) a mensagem recebida.

Os protocolos de Criptografia assimétrica, como o de Stickel em [10], podem ser utilizados para partilhar uma informação secreta, como, por exemplo, uma chave privada. O mencionado esquema criptográfico foi adaptado em [3] para proteger, recorrendo às operações tropicais $\oplus$ e $\odot$, o processo perante ataques de tipo algébrico. Com efeito, como detalhamos subsequentemente, os protocolos mostraram-se vulneráveis a ataques no domínio da Álgebra Linear com a adição e a multiplicação usuais de números reais, [3].

Suponhamos que os interlocutores A e B querem partilhar uma chave privada. Para isso, começam por escolher duas matrizes invertíveis com entradas em $\mathbb{R}$, públicas, a e b tais que $ab \neq ba$. Posteriormente, o interlocutor A gera aleatoriamente dois números naturais n e m e envia a B a palavra $u = a^n b^m$. De forma similar, B gera r e $s \in \mathbb{N}$ e envia a A a palavra $v = a^r b^s$. Neste ponto, A só deve calcular $K_A = a^n v b^m = a^{n+r} b^{m+s}$ enquanto B calcula $K_B = a^r u b^s = a^{n+r} b^{m+s}$ para os dois terem a mesma chave $K = K_A = K_B$.

Infelizmente, se um adversário que conhece a palavra u quer recuperar a chave K, então não precisa de encontrar os expoentes n, m, r e s. De facto, basta encontrar duas matrizes x e y tais que $xa = ax$, $yb = by$ e $xu = y$, [3]. Estas condições traduzem-se num sistema linear com $3k^2$ equações e $2k^2$ incógnitas, onde k denota a ordem das matrizes a e b, que neste caso pode ser resolvido de forma eficiente com um computador. A vulnerabilidade a este tipo de ataques algébricos pode evitar-se com modificações, como em [3].

A adaptação mais relevante consiste em substituir as matrizes a e b por dois elementos da álgebra tropical das matrizes $k \times k$ sobre $\mathbb{Z}$, em geral não invertíveis, tais que $a \otimes b \neq b \otimes a$, onde $\otimes$ denota a multiplicação usual de matrizes com a multiplicação e adição usuais de reais substituídas pelas respetivas versões tropicais. No contexto tropical, a equação $xy = u$ com u conhecido e x, y desconhecidos, não se traduz num sistema de equações lineares devido à não invertibilidade das matrizes. Além disso, $xa = ax$ e $yb = by$ determinam um sistema de equações lineares cuja resolução envolve uma maior complexidade computacional, possivelmente não polinomial.

Em suma, os esquemas criptográficos tropicais em [3] apresentam duas grandes vantagens:

- menor vulnerabilidade dos esquemas a ataques por, em geral, a resolução de sistemas de equações lineares ser computacionalmente impraticável;
- maior eficiência dos esquemas por não se fazerem multiplicações de números, uma vez que a multiplicação tropical é a adição usual.

3. A VERSÃO TROPICAL DO CLÁSSICO

Como conjunto, o semianel tropical $(\mathbb{R} \cup \{\infty\}, \oplus, \odot)$ é apenas o conjunto dos números reais reunido com o conjunto formado pelo elemento ∞ que representa o infinito, no qual foram redefinidas as operações aritméticas básicas de adição e de multiplicação de números reais. Muitas propriedades familiares da Aritmética permanecem válidas em contexto tropical. Por exemplo, a multiplicação tropical é comutativa.

Note-se ainda que a estrutura algébrica de semianel de $\mathbb{R} \cup \{\infty\}$, munido das operações internas $\oplus$ e $\odot$, é conferida pelas propriedades:

- comutatividade de $\oplus$
  para quaisquer $x, y \in \mathbb{R} \cup \{\infty\}$, $x \oplus y = y \oplus x$;
- associatividade de $\oplus$
  para quaisquer $x, y, z \in \mathbb{R} \cup \{\infty\}$,
  $(x \oplus y) \oplus z = x \oplus (y \oplus z)$;
- associatividade de $\odot$
  para quaisquer $x, y, z \in \mathbb{R} \cup \{\infty\}$,
  $(x \odot y) \odot z = x \odot (y \odot z)$;
- distributividade de $\odot$ em relação a $\oplus$
  para quaisquer $x, y, z \in \mathbb{R} \cup \{\infty\}$,
  $x \odot (y \oplus z) = x \odot y \oplus x \odot z$ e
  $(x \oplus y) \odot z = x \odot z \oplus y \odot z$;
- existência de elemento neutro de $\oplus$,
  existe $u \in \mathbb{R} \cup \{\infty\}$ tal que, para qualquer
  $x \in \mathbb{R} \cup \{\infty\}$, $u \oplus x = x = x \oplus u$.

Por outras palavras, trata-se de uma estrutura algébrica similar à de anel mas sem a exigência de cada elemento ter um oposto aditivo. Relativamente à última propriedade, ∞ é o elemento neutro da adição tropical. No que se refere à distributividade, note-se a dispensa habitual de parêntesis à direita desde que se respeite a ordem de prioridade usual das operações, ou seja, as multiplicações tropicais devem ser efetuadas antes das adições tropicais.

No que se segue, apresentamos a versão tropical do clássico quadrado da soma. Concretamente, demonstramos dois resultados relativos ao *freshman's dream*, o qual é tropicalmente estabelecido no Teorema 3.1. No Teorema 3.3 mostramos que uma extensão do *freshman's dream* se torna realidade em contexto tropical. O caso particular $n = 2$ permite obter o Teorema 3.1 como corolário do Teorema 3.3.

Teorema 3.1. *Para quaisquer* $x, y \in \mathbb{R}$, $(x \oplus y)^2 = x^2 \oplus y^2$.

Demonstração. Sejam $x, y \in \mathbb{R}$, quaisquer. Tem-se

$$\begin{aligned}(x \oplus y)^2 &= (x \oplus y) \odot (x \oplus y)\\ &= x \odot x \oplus x \odot y \oplus y \odot x \oplus y \odot y\\ &= x \odot x \oplus (x \odot y \oplus x \odot y) \oplus y \odot y\\ &= x \odot x \oplus x \odot y \oplus y \odot y\\ &= \min\{2x, x+y, 2y\}\\ &= \min\{2x, 2y\}\\ &= x \odot x \oplus y \odot y\\ &= x^2 \oplus y^2,\end{aligned}$$

onde a antepenúltima igualdade é consequência de, para quaisquer $x, y \in \mathbb{R}$,

$$x \geq y \vee y \geq x \Leftrightarrow x + y \geq 2y \vee x + y \geq 2x. \qquad \square$$

Lema 3.2. *Para quaisquer* $n \in \mathbb{N}$ *e* $x, y \in \mathbb{R}$,

$$n \min\{x, y\} = \min\{nx, ny\}.$$

Demonstração. Sejam $n \in \mathbb{N}$ e $x, y \in \mathbb{R}$, quaisquer. Então $x = y$ ou $x < y$ ou $x > y$. No primeiro caso, a igualdade no enunciado é claramente válida. Se $x < y$ então $nx < ny$, pelo que $n \min\{x, y\} = nx$ e $\min\{nx, ny\} = nx$. Quanto ao terceiro caso, o raciocínio é análogo ao do caso precedente. $\square$

Teorema 3.3. *Para quaisquer* $n \in \mathbb{N}$ *e* $x, y \in \mathbb{R}$,

$$(x \oplus y)^n = x^n \oplus y^n.$$

Demonstração. Sejam $n \in \mathbb{N}$ e $x, y \in \mathbb{R}$, quaisquer. O resultado é óbvio para $n = 1$. Suponha-se assim que $n \geq 2$. Nomeadamente tendo em conta o lema precedente, tem-se

$$\begin{aligned}(x \oplus y)^n &= (x \oplus y) \odot \ldots \odot (x \oplus y)\\ &= (x \oplus y) + \ldots + (x \oplus y)\\ &= n(x \oplus y)\\ &= n \min\{x, y\}\\ &= \min\{nx, ny\}\\ &= nx \oplus ny\\ &= (x + \ldots + x) \oplus (y + \ldots + y)\\ &= x \odot \ldots \odot x \oplus y \odot \ldots \odot y\\ &= x^n \oplus y^n.\end{aligned}$$

$\square$

4. REFERÊNCIAS

[1] Bagni, G. (2000) "'Simple' Rules and General Rules in Some High School Students' Mistakes", *Journal für Mathematik-Didaktik*, 21 (2), 124–138.

[2] de Bock, D., van Dooren, W., Janssens, D., Verschaffel, L. (2007) *The Illusion of Linearity*, New York: Springer.

[3] Grigoriev, D., Shpilrain, V. (2014) "Tropical Cryptography", *Communications in Algebra*, 42 (6), 2624–2632.

[4] Hungerford, T. W. (1974) *Algebra*, New York: Springer.

[5] Maclagan, D., Sturmfels, B. (2015) *Introduction to Tropical Geometry*, Providence: American Mathematical Society.

[6] Pin, J.-E. (1998) "Tropical Semirings", In J. Gunawardena (Ed.), *Idempotency* (pp. 50–69), Cambridge: Cambridge University Press.

[7] Simon, I. (1978) "Limited Subsets of a Free Monoid", In *Proceedings of the 19th Annual Symposium on Foundations of Computer Science* (pp. 143–150), Washington: IEEE Computer Society.

[8] Simon, I. (1988) "Recognizable Sets with Multiplicities in the Tropical Semiring", In Chytil, M. P., Koubek, V., Janiga, L. (Eds.), *Mathematical Foundations of Computer Science* (pp. 107–120), Berlin: Springer.

[9] Speyer, D., Sturmfels, B. (2009) "Tropical Mathematics", *Mathematics Magazine*, 82 (3), 163–173.

[10] Stickel, E. (2005) "A New Method for Exchanging Secret Keys", In He, X., Hintz, T., Piccardi, M., Wu, Q., Huang, M., Tien, D. (Eds.), *Proceedings of the Third International Conference on Information, Technology and Applications* (pp. 426–430), Los Alamitos: IEEE Computer Society.

AGRADECIMENTOS

Beites, P. D. e Nicolás, A. P. agradecem o apoio do Ministerio de Economía y Competitividad (España), projeto MTM2013-45588-C3-1-P. Beites, P. D. agradece ainda ao Governo Português através da Fundação para a Ciência e a Tecnologia (Portugal), projeto PEst-OE/MAT/UI0212/2015 do CMA–UBI.

SOBRE OS AUTORES

Patrícia Damas Beites é professora auxiliar do Departamento de Matemática da Universidade da Beira Interior. Os seus principais interesses de investigação prendem-se com tópicos de Álgebra, em particular Não Associativa, e de Didática da Matemática.

Alejandro Piñera Nicolás é professor associado na Universidad de Valladolid (Espanha). Os seus interesses de investigação centram-se na Teoria de Códigos Detetores e Corretores de Erros, na Álgebra Não Associativa e na Teoria de Carateres de Grupos Finitos.