explícitament computable. Cap ni un. I aquí és on entren els treballs de Nisan-Wigderson [19] i Impagliazzo-Wigderson [8] de finals dels 90. La contribució és que, per tal de construir un generador que extengui m bits a n bits, i garantir que sigui pseudoaleatori respecte dels tests computables amb circuits de mida n^k, és suficient (i necessari) construir una funció booleana de $O(m)$ bits que no sigui computable per circuits de mida $O(n^k)$. Per exemple, si aconseguíssim demostrar que la funció $\lambda(N)$ de Liouville requereix circuits de mida n^3 per a nombres N de n bits, llavors podríem simular n bits aleatoris per a tests de mida n^2 amb, només, uns $O(n^{2/3})$ bits aleatoris reals.

La dualitat hardness vs. randomness que sorgeix de la transformació proposada per Wigderson i coautors té el mèrit de ser universal. De fet, la transformació és tan general, que dona lloc a moltíssimes derivades, algunes de les quals *incondicionals*, és a dir, sense que depenguin de conjectures per ara irresol·lubles com P $\neq$NP. Per exemple, Trevisan [23, 24] va ser el primer a adonar-se que els generadors de Nisan-Wigderson permetien produir *extractors* millors dels que es coneixien fins llavors.

Què és, doncs, un extractor? Un extractor és una funció booleana, eficientment computable, que purifica l'aleatorietat d'una font impura de bits aleatoris i n'extreu gairebé tota l'entropia. El descobriment de Trevisan va ser que el generador de Nisan-Wigderson és, de fet, un extractor explícit en si mateix! La clau de volta és el punt de partida que ens ha dut fins aquí: que gairebé totes les funcions booleanes de n bits són difícils per a circuits de mida $o(2^n/n)$. Fent números rodons, una font impura de n bits que tingui n^ϵ bits d'entropia proporciona una funció booleana d'uns $\epsilon \log n$ bits que no és computable amb circuits de mida $o(n^\epsilon/\log n)$, amb alta probabilitat. Per tant, aplicant-hi Nisan-Wigderson, obtenim un generador pseudoaleatori que proporciona uns $n^\epsilon/\log n$ bits aleatoris per a *tots* els tests. És a dir, proporciona un extractor.

El fet que extractors explícits es poguessin construir incondicionalment va inspirar molts d'altres a produir altres objectes pseudoaleatoris. Una de les fites més espectaculars és potser el treball del mateix Wigderson, en col·laboració amb Barak, Rao i Shaltiel [1], que va acabar produint la primera millora significativa en dècades per al problema de construcció de grafs de Ramsey. De saber construir grafs amb 2^n vèrtexs sense subconjunts homogenis de $2^{n^{1/2}}$ vèrtexs es va passar a saber construir-ne sense subconjunts homogenis de 2^{n^ϵ} vèrtexs per a qualsevol $\epsilon > 0$. El problema de construir grafs de 2^n vèrtexs sense subconjunts homogenis de $O(n)$ vèrtexs, que seria essencialment òptim, segueix obert. De ben segur, la feina de Wigderson en aquest camp inspirarà les generacions futures a resoldre aquest i molts altres dels problemes fonamentals que sorgeixen quan hom es planteja, seriosament, la pregunta de si l'atzar existeix i si es pot simular.

Combinatòria, grafs expansors i grafs límit

Oriol Serra, Departament Matemàtiques, UPC

Exposarem dos exemples de contribucions excepcionals a la matemàtica discreta degudes a Widgerson (grafs expansors) i Lovász (límits de grafs), i que exemplifiquen dues línies de recerca on l'interacció entre combinatòria i informàtica teòrica resulta cabdal.

Expansors

Els grafs expansors són un dels objectes més fascinants de la teoria de grafs. En la seva aplicació a les xarxes de comunicació, una de les característiques importants dels grafs és que no tinguin colls d'ampolla, de manera que el tràfic d'informació a la xarxa es pugui repartir de manera homogènia. Una manera de capturar aquesta propietat és demanar que el nombre de nodes que estan connectats als d'un conjunt X de nodes sigui proporcional al cardinal d'aquest conjunt. Si ∂X denota el conjunt de nodes fora de X que són adjacents a algun node de X la condició s'escriu $|\partial X| \geq c|X|$, on la constant c és la mateixa per tots els conjunts X que tenen com a molt $n/2$ nodes (aquesta darrera condició resulta suficient i és tècnicament millor). Les xarxes de comunicació tenen la característica que cada node té un nombre petit de veïns.

Quan aquest nombre és el mateix per a tots els nodes el graf és regular. Donada una constant positiva c i un grau d (cada vèrtex té d veïns), l'objectiu és trobar, per a cada natural n, un graf G_n amb n vèrtexs que tingui constant d'expansió c (comuna a tots els grafs de la successió). Una successió G_n de grafs d–regulars amb aquesta propietat és un *c–expansor*.

Per a una família d'expansors G_n, el diàmetre, o distància màxima entre nodes és de l'ordre de $\log n$, l'ordre de magnitud més petit que pot tenir el diàmetre d'un graf de n nodes i grau fitat. A més el graf té bones propietats de connectivitat: hi ha un nombre gran de camins disjunts que connecten qualsevol parell de subconjunts de nodes. Aquestes són propietats desitjables en una xarxa de comunicació.

Es pot provar per mètodes probabilistes que, per a cada c prou petit i cada grau d fixat, gairebé *tots* els grafs amb un nombre prou gran de vèrtexs són expansors amb aquesta constant. Tot i això, trobar una construcció explícita d'una família d'expansors és un problema difícil. El gran matemàtic rus Grigori Margulis, que per política antisemita va anar a parar a l'Institut de Transmissió de la Informació de Moscou (un centre molt reputat en tecnologia però poc adient per a un especialista en teoria de grups i en teoria ergòdica com Margulis, guanyador d'una Medalla Fields el 1978 i del Premi Abel el 2020), va topar amb aquest problema i va obtenir la primera construcció explícita d'una familía d'expansors, cosa que li va merèixer un gran reconeixement. Aprofundint en aquesta construcció i integrant-hi elements de teoria de nombres i de teoria de grups, Lubotzky, Phillips i Sarnak van obtenir una formulació encara més explícita. La monografia de Lubotzky [15] sobre aquest tema va guanyar el Premi Ferran Sunyer i Balaguer (de fet, en dues ocasions, cosa singular). En la seva conferència a Barcelona en recollir aquest premi, Lubotzky va comentar que la construcció era fruit d'una alineació màgica i inusual d'astres diversos, una conjectura de Ramanujan en teoria de nombres, elements de la teoria de varietats i l'existència de subgrups adequats d'un grup lliure.

Mentrestant, les aplicacions dels expansors s'estenien més enllà del context de les xarxes de comunicació a àrees molt diverses. A la convergència ràpida de processos aleatoris, al càlcul de volum de cossos (amb una participació de decisiva de Lovász), al disseny d'algorismes eficients en teoria de la computació, a l'estudi espectral d'operadors en geometria o al disseny de codis que assoleixen asimptòticament la raó de transmissió òptima en un canal amb soroll, per citar-ne algunes de les més rellevants.

En aquest punt, Avi Widgerson va fer una contribució dramàtica en proposar una construcció combinatòria que resol de manera més efectiva el problema de donar construccions explícites d'expansors, l'anomenat *producte zig–zag*. La idea és construir una familía infinita d'expansors a partir d'un graf donat, que sempre admet alguna constant d'expansió, de manera que aquesta constant es transmeti (de forma més dèbil però suficient) a tots els grafs de la seqüència. La idea del producte està basada en el producte cartesià ordinari de grafs. Donats dos grafs G i H, es defineix un graf al producte cartesià dels seus conjunts de vèrtexs establint adjacències entre parells quan una de les coordenades es manté fixa i l'altra segueix l'adjacència de l'altra factor del producte. La idea de Widgerson és introduir un element aleatori en la tria d'una de les dues menes d'adjacència que manté el grau del graf resultant fitat i fa que el producte resultant mantingui les propietats d'expansió dels grafs factors. La universalitat d'aquesta construcció fa accessibles construccions explícites i la seva aplicació en models concrets ha permès obtenir famílies d'expansors amb valors òptims de la constant d'expansió.

Una de les aplicacions més espectaculars del producte zig-zag, que d'alguna manera revela la profunditat de visió en la seva construcció, ha estat el disseny d'un algorisme d'exploració de grafs d'eficiència òptima. L'exploració eficient d'un graf és un dels problemes fonamentals en la teoria de la complexitat algorísmica. Es tracta de saber dirigir-se a un node de destí en un graf desconegut fent servir el mínim d'informació possible. Una altra vegada trobem Lovász en el disseny d'un algorisme probabilista que fa servir només una quantitat d'informació logarísmica sobre la mida del graf. El problema de convertir aquest algorisme probabilista en un que no ho és (les màquines fan servir algorismes deterministes) es va resoldre de manera enginyosa fent servir la sequència de grafs obtinguts

amb el prodcute zig-zag a partir del graf donat fent servir la propietat d'expansió d'aquesta seqüència.

Widgerson [26] és un dels coautors d'un excellent article d'exposició, assequible amb una formació matemàtica no especialitzada, que recull la història, els resultats més rellevants i les aplicacions més importants de la teoria dels grafs expansors.

Límits de grafs

Un dels problemes centrals que va emergir amb força a finals del segle XX va ser el desenvolupament d'eines d'anàlisi de grans xarxes. L'eclosió de la xarxa d'internet en va ser una de les motivacions, però les grans xarxes han estat sempre presents; xarxes biològiques, físiques o socials. La mida d'aquestes xarxes, de l'ordre de bilions de nodes, comporta l'ús d'eines, resultats i anàlisis distinctives que no estaven a l'abast. Del 1996 al 2006 Lovász va acceptar una oferta al Microsoft Research Center de Seattle amb l'encàrrec de desenvolupar un marc matemàtic adient per al tractament de grans xarxes que fins aleshores havien estat analitzades sobretot des d'una perspectiva heurística. En aquest període va desenvolupar la teoria de límits de grafs que ha resultat una eina fonamental en l'estudi de grans xarxes i ha tingut un impacte enorme en aquesta àrea.

La idea de límit apareix ja a Aristòtil, no és una idea nova. El desenvolupament del càlcul infinitessimal al segle XVIII fins a la seva maduresa a principis del segle XX va proporcionar un fonament sòlid a la noció de límit que es va estendre de límits de nombres a límits de funcions i d'objectes més abstractes. El que no s'havia abordat és la noció de límit d'estructures combinatòries discretes, la més senzilla de les quals és la dels grafs, precisament el model matemàtic de les xarxes. La idea fonamental és que la manera més eficaç d'analitzar grans grafs és interpretar-los com a integrants d'una successió de grafs amb n nodes per a $n \to \infty$ i estudiar-ne el límit. Per això cal concebre un espai on aquests límits tinguin sentit i dotar-lo d'una mètrica que permeti identificar les successions convergents de grafs de manera que el límit en capturi les propietats més característiques.

Una manera natural de construir aquest espai s'obté identificant els grafs amb les seves matrius d'adjacència. La matriu d'adjacència d'un graf de n vèrtexs és una matriu A quadrada $n \times n$ que a la posició A_{ij} té un 1 si hi ha una aresta $\{i, j\}$ al graf i zero altrament. Si s'escriu una d'aquestes matrius per un graf de bilions de nodes en un paper es veuen simplement zones de la matriu amb més densitat d'uns i d'altres més buides, amb zeros. El resultat s'assembla al d'una funció $W : [0, 1] \times [0, 1] \to [0, 1]$ que pinta punts més pròxims a 1 on hi ha més densitat d'uns i punts més pròxims a zero on n'hi ha pocs. Una funció així que és simètrica, $W(x, y) = W(y, x)$ (les matrius d'adjacència dels grafs són simètriques) i que és mesurable (un mínim d'estructura que permeti aplicar les eines de l'anàlisi matemàtica) és un *grafó* (contracció de graf i funció). L'espai dels grafons resulta l'espai apropiat per bastir la teoria de límits de grafs.

El programa per construir la teoria de grafs límits es va desenvolupar sobre aquesta idea a través d'una llarga sèrie d'articles, i Lovász el va recollir en una extensa monografia [13] que no només descriu de manera rigorosa tots els detalls analítics de la construcció, que té vessants probabilístics, combinatòris, topològics i analítics, sinó que desenvolupa també una sèrie d'aplicacions que il·lustren l'eficàcia d'aquesta construcció per a l'anàlisi de grans xarxes des d'una fonamentació matemàtica sòlida. A més, planteja preguntes intrigants sobre les característiques d'algunes classes de grafons que obren línies de recerca de consequències encara imprevisibles.

Com va recordar el mateix Lovász en el discurs que va donar amb motiu del Premi Hipatia, que li va ser atorgat per l'Academia Europaea i l'Ajuntament de Barcelona fa pocs anys, els límits de grafs es poden pensar com un intent de millorar la nostra comprensió de l'univers, vist com una immensa xarxa d'interaccions.

Referències

[1] B. Barak, A. Rao, R. Shaltiel, A. Wigderson. *2-source dispersers for $n^{o(1)}$ entropy, and Ramsey graphs beating the Frankl-Wilson construction* Ann. of Math., Vol. 176: 1483–1544 (2012)

[2] M. Becker, J. Doenhardt, S. Hertel, G. Kaninke, W. Kerber, K. Mehlhorn, S. Näher, H. Rohnert, T. Winter. *A probabilistic algorithm for vertex connectivity of graphs.* Inf. Process. Letters, 15(3): 135–136 (1982)

[3] J. Cheriyan, J. Reif. *Directed s-t Numberings, Rubber Bands, and Testing Digraph k-Vertex Connectivity.* Combinatorica 14 (4): 435-–45 (1994)

[4] S. Even. *Graph Algorithms.* Computer Science Press, (1979)

[5] Z. Galil. *Finding the vertex connectivity of graphs.* SIAM J. Computing, 5: 618–623 (1982)

[6] T. Kathuria, Y.P. Liu, A. Sidford. *Unit capacity maxflow in almost $o(m^{4/3})$ time.* Proc. 61st IEEE FOCS, 119—130 (2020)

[7] M. R. Henzinger, S. Rao, H. N. Gabow. *Computing Vertex Connectivity: New Bounds from Old Techniques.* J. of Alg., 34 (2): 222–250, (2000)

[8] R. Impagliazzo, A. Wigderson. *$P = BPP$ if E* Requires Exponential Circuits: Derandomizing the XOR Lemma. En Proc. 29th ACM STOC: 220–229 (1997)

[9] A. Lenstra, H. Lenstra, L. Lovász. *Factoring polynomials with rational coefficients.* Math Ann. 261: 515–534 (1982)

[10] J. Li, D. Nanongkai, D. Panigrahi, T. Saranurak, S. Yingchareonthawornchai. Vertex Connectivity in Poly-logarithmic Maxflows, En Proc. 53st ACM STOC, (2021)

[11] N. Linial, L. Lovász, A. Wigderson. *A physical interpretation of graph connectivity and its algorithmic applications.* En Proc. 27th IEEE FOCS, 39–48 (1986)

[12] N. Linial, L. Lovász, A. Wigderson. *Rubber bands, convex embeddings, and graph connectivity.* Combinatorica, 8: 91–102 (1988)

[13] L. Lovász. *Large Networks and Graph Limits.* Colloquium Publications AMS, vol. 60 (2012)

[14] L. Lovász. *Graphs and Geometry.* Colloquium Publications AMS, vol. 65 (2019)

[15] A. Lubotzky. *Discrete groups, expanding graphs and invariant measures*, vol. 125 of Progress in Mathematics. Birkhäuser Verlag, Basel (1994)

[16] C. Moore, S. Mertens. *The Nature of Computation.* Oxford Univ. Press (2011)

[17] D. Nanongkai, T. Saranurak, S. Yingchareonthawornchai. *Breaking quadratic time for small vertex connectivity and an approximation scheme.* En Proc. 51st ACM STOC, 241-252 (2019)

[18] P. Q. Nguyen, B. Vallée (eds); *The LLL Algorithm: Survey and Applications.* Springer V. (2010)

[19] N. Nisam, A. Widgerson. *Hardness vs Randomness.* J. Comput. Syst. Sci. 49 (2): 149–167 (1994)

[20] A. M. Odlyzko, H. J. J. te Riele. *Disproof of the Mertens conjecture.* J. reine angew. Math., 357: 138-160 (1985)

[21] A. Shamir. *A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem.* En Proc. 23rd IEEE FOCS, 145–152, (1982)

[22] D. Simon. *Selected applications of LLL in number theory*, dins de ([18])

[23] L. Trevisan. *Construction of extractors using pseudo-random generators (extended abstract).* En Proc. 31st ACM STOC: 141-148 (1999)

[24] L. Trevisan. *Extractors and Pseudorandom Generators.* J. ACM, 48(4):860-879 (2001)

[25] W. T. Tutte. *How to draw a graph.* Proc. London Math. Soc. 13, 743–768 (1963)

[26] S. Hoory, N. Linial, A.Widgerson. *Expander Graphs and their applications.* Bull. Amer. Math. Soc. 43: 439-561 (2006)

[27] A. C.-C. Yao. *Theory and Applications of Trapdoor Functions (Extended Abstract)*, En *Proc. 23rd IEEE FOCS*: 80–91 (1982)