Pavel Pudlák

Abelova cena pro Aviho Wigdersona

Pokroky matematiky, fyziky a astronomie, Vol. 66 (2021), No. 3, 149–156

Persistent URL: http://dml.cz/dmlcz/149217

Abelova cena pro Aviho Wigdersona

Pavel Pudlák

Abstrakt. Abelovu cenu za rok 2021 získali společně László Lovász a Avi Wigderson za zásadní přínos v teoretické informatice a diskrétní matematice. V tomto článku představíme čtenářům Aviho Wigdersona a jeho práci výběrem tří důležitých výsledků z jeho mnoha publikací.

1. Wigdersonův stručný životopis a vědecké zaměření

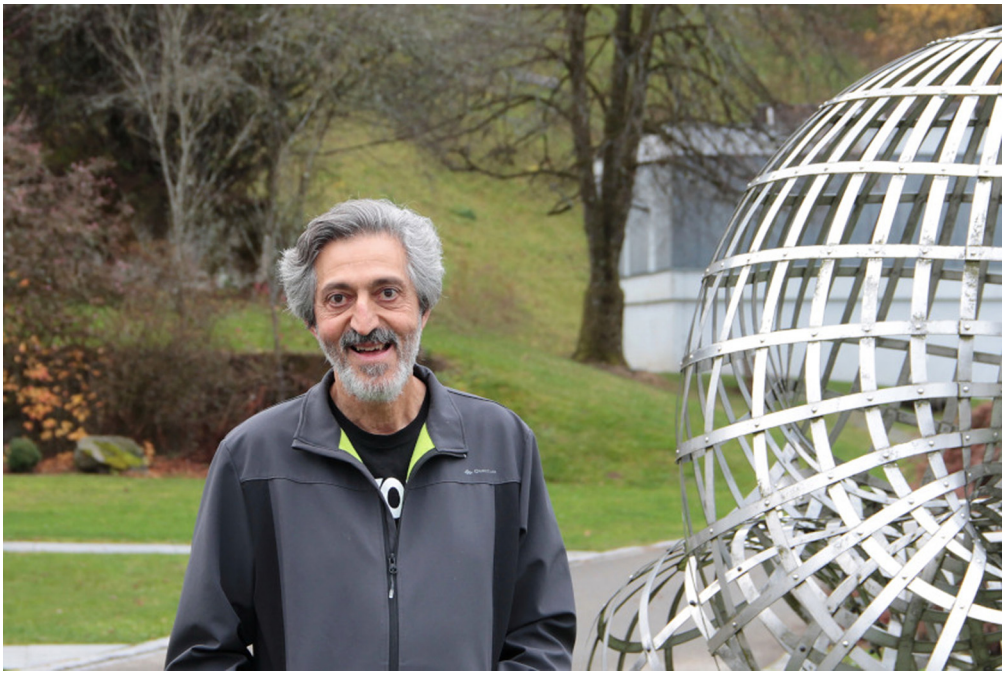
Avi Wigderson se narodil v Izraeli v Haifě v roce 1956. Ve stejném městě studoval na Technionu (Israel Institute of Technology). Titul bakaláře získal v roce 1980. Doktorské studium absolvoval v USA na Princetonské univerzitě pod vedením Richarda J. Liptona. V roce 1983 obhájil práci s názvem *Studies in Computational Complexity*. Od roku 1986 působil na Hebrejské univerzitě v Jeruzalémě. V roce 1999 získal místo v Institute for Advanced Study v Princetonu (v IAS má trvalé místo, zvané *faculty*, jen šest matematiků). Do roku 2003 působil na obou místech, později si ponechal jen místo v IAS, kde pracuje dodnes a v současné době v tomto ústavu řídí program teoretická informatika a diskrétní matematika. Kromě zmíněných dvou míst byl hostujícím profesorem na několika dalších amerických univerzitách a výzkumných ústavech.

Wigderson získal řadu ocenění. Na Mezinárodním matematickém kongresu v Curychu v roce 1994 obdržel Nevalinnovu cenu. Dále získal Gödelovu cenu v roce 2009, Knuthovu cenu v roce 2019 a konečně nejvyšší cenu Abelovu v roce 2021. Byl zvolen členem Americké akademie věd a umění, Národní akademie věd USA a členem Association for Computer Machinery.

Avi Wigderson se zabývá teoretickou informatikou. Tento pojem je ovšem velice široký a oblast, které se Wigderson věnuje, by se spíše mohla označit jako základní výzkum v teoretické informatice. Základní problémy teoretické informatiky jsou motivované otázkami, jak efektivně se dají řešit konkrétní problémy, ale ve své podstatě to jsou matematické problémy, které nemají bezprostřední aplikace. Nejznámějším z těchto problémů je otázka, zda platí vztah $\mathrm{P} = \mathrm{NP}$, kde P je třída úloh řešitelných v polynomiálním čase a NP je, zhruba řečeno, třída úloh, pro které se dá řešení ověřit v polynomiálním čase, pokud nám je někdo předloží. (Formálně se NP definuje pomocí tzv. nedeterministických algoritmů pracujících v polynomiálním čase.) Při pohledu zvenku se může zdát, že tento obor stagnuje, protože padesát let od formulace problému P=NP nikdo nepřišel ani s teorií, která by mohla vést k řešení. Opak je však pravdou – obor se rozvíjí stále více a je uznáván jako matematická disciplína, na čemž má velkou zásluhu i Wigderson.

Jaké tedy jsou problémy, ve kterých se dosáhlo největšího pokroku? Je to řada věcí, ale většina nějakým způsobem souvisí s náhodností. Asi nejdůležitější oblast, kde se

Prof. RNDr. Pavel Pudlák, DrSc., Matematický ústav AV ČR, Žitná 25, 115 67 Praha 1, e-mail: pudlak@math.cas.cz



Obr. 1. Avi Wigderson (Archives of the Mathematisches Forschungsinstitut Oberwolfach)

objevuje náhodnost, jsou randomizované algoritmy. Tyto algoritmy potřebují generátor náhodných bitů. Výpočet není jednoznačný, závisí na náhodných bitech a s malou pravděpodobností neposkytne řešení, nebo odpoví špatně, pokud se testuje nějaká vlastnost. Přesto jsou často užitečné, protože pracují rychleji, nebo řeší úlohy, pro které deterministické polynomiální algoritmy nemáme. Jako příklad uveďme testování, zda polynom je identicky roven nule. Zde je nutno říci, jak je polynom zadán. Zadáme-li jej jako součet monomů, pak je úloha triviální. Netriviální je ovšem v případě, že polynom je zadán algebraickým výrazem $F(x_1, \ldots, x_n)$ s pomocí proměnných, násobení, sčítání a celočíselných konstant. Takto zadaný polynom sice můžeme převést na sumu monomů, ale při této transformaci často dostaneme exponenciálně velké výrazy. Např. výraz

$$(x+y)^{2n} - (x^2 + 2xy + y^2)^n,$$

kde umocňování je jenom zkratka za iterované násobení, evidentně definuje nulový polynom, ale roznásobením dostaneme exponenciálně mnoho monomů (které se nakonec vyruší). Tedy to není efektivní způsob jak zjistit, zda je polynom nulový. Existuje ale velmi jednoduchý a efektivní randomizovaný algoritmus. Jeho podstatou je fakt, že když je polynom nenulový a vyčíslíme jej na náhodně zvolených číslech z vhodně zvoleného intervalu, pak s velkou pravděpodobností dostaneme nenulové číslo. Na rozdíl od transformace polynomu na součet monomů lze vyčíslení výrazu $F(x_1, \ldots, x_n)$ provést v polynomiálním čase prostě proto, že násobení a sčítání je proveditelné v polynomiálním čase.

2. Nisanovy–Wigdersonovy pseudonáhodné generátory

Jedním z velkých problémů teorie složitosti je otázka, zda existují úlohy, které se dají řešit v polynomiálním čase pomocí randomizovaných algoritmů s velkou pravděpodobností, ale nedají se řešit v polynomiálním čase pomocí deterministických algoritmů. Tento problém je znám jako otázka, zda platí $\mathrm{BPP} = \mathrm{P}$, kde BPP je třída úloh řešitelných v polynomiálním čase randomizovanými algoritmy. Na rozdíl od problému P=NP, kde se domníváme, že $\mathrm{P} \neq \mathrm{NP}$, máme dobré důvody se domnívat, že $\mathrm{BPP} = \mathrm{P}$. Dokonce věříme, že existuje univerzální metoda, jak randomizovaný algoritmus *derandomizovat*. Idea je nahradit generátor náhodných bitů *pseudonáhodným generátorem*. Pseudonáhodný generátor je generátor bitů, které jsou závislé, ale vypadají v určitém smyslu jako úplně náhodné. Přesněji řečeno, výstup z pseudonáhodného generátoru se nedá odlišit od náhodných nezávislých bitů pomocí testu realizovatelného v polynomiálním čase. Elementární test náhodnosti je např. poměr počtu jedniček k počtu nul. Pokud se tato čísla liší o více než odmocninu z počtu všech bitů, máme právo se domnívat, že bity nejsou úplně náhodné. Definice pseudonáhodného generátoru ovšem připouští použití libovolného testu jen s tou podmínkou, že musí být vyčíslitelný v polynomiálním čase.[1]

Aby byl pseudonáhodný generátor užitečný, je potřeba, aby se dal snadno realizovat. Proto musíme říci přesněji, o jakém matematickém objektu mluvíme. Pseudonáhodný generátor je funkce $G\colon \{0,1\}^k \to \{0,1\}^n$, kde $k < n$. Funkce G generuje n pseudonáhodných bitů tak, že se zvolí k náhodných bitů r a z nich se vypočítá $G(r)$. Jinými slovy, z uniformního rozložení na $\{0,1\}^k$ vytvoří G jakési rozložení na $\{0,1\}^n$, které má být pseudonáhodné ve výše uvedeném smyslu. Dále požadujeme, aby se hodnota $G(r)$ dala vypočítat v čase, který je polynomiální v n. Pro derandomizaci potřebujeme, aby vztah mezi k, n byl $k = O(\log n)$. Daný randomizovaný algoritmus A potom derandomizujeme takto: pro daný vstup necháme běžet A s bity $G(r)$ místo náhodných bitů. To uděláme pro všechna $r \in \{0,1\}^k$ a zvolíme odpověď, která se vyskytne nejčastěji. Algoritmus A se musí na $G(r)$ pro $r \in \{0,1\}^k$ chovat skoro stejně, jako by používal úplně náhodné bity, jinak bychom mohli A použít jako test, který by ukázal, že G není pseudonáhodný generátor.

Dosud nevíme, zda pseudonáhodné generátory existují. Pokud platí $\mathrm{P} = \mathrm{NP}$, pak neexistují, proto v současné době můžeme dokázat jejich existenci jenom z nějakých nedokázaných předpokladů. Noam Nisan a Avi Wigderson v článku [9] navrhli, jak takový generátor sestrojit, pokud máme k dispozici booleovskou funkci, která je v určitém smyslu těžká (nedá se ani přibližně počítat subexponenciálním booleovským obvodem) a zároveň není velmi těžká (dá se počítat v exponenciálním čase). Význam tohoto výsledku spočívá v tom, že spojuje centrální klíčové otázky: derandomizaci a dolní odhady pro složitost booleovských obvodů. Dolní odhady složitosti booleovských obvodů jsou zejména důležité z hlediska problému $\mathrm{P} = \mathrm{NP}$. Kdybychom dokázali superpolynomiální dolní odhad na složitost nějaké funkce, která je v NP, pak bychom dokázali $\mathrm{P} \neq \mathrm{NP}$. Pro generátory Nisana a Wigdersona potřebujeme exponenciální dolní odhady na obvody počítající funkce, které jsou vyčíslitelné v exponenciálním

[1] Pro jednoduchost předpokládáme, že testy jsou realizovány deterministickými algoritmy. Standardní definice povoluje i testy využívající randomizované algoritmy.

čase. Později se ukázalo, že tato souvislost je hlubší. Platí totiž, že kdybychom uměli derandomizovat testování, zda je polynom nulový, pak bychom také dostali určité dolní odhady na složitost obvodů [7]. Takže derandomizace a dolní odhady na složitost obvodů jsou v určitém smyslu ekvivalentní problémy.

3. Extraktory a ramseyovské grafy

Také další výsledek, na kterém se Wigderson podstatnou měrou podílel, se týká náhodnosti a vlastně i pseudonáhodnosti. Představme si, že máme nějaký generátor náhodných bitů, které však ve skutečnosti nejsou úplně náhodné, např. házíme mincí, která nedává obě možnosti se stejnou pravděpodobností. Chceme-li získat jeden bit, který by byl blízký úplně náhodnému, můžeme vzít n bitů vyprodukovaných generátorem a zjistit paritu jejich součtu. Tím získáme bit, pro nějž pravděpodobnosti jedničky a nuly budou mnohem blíže k 1/2. Pokud jsou ale bity generátoru závislé, parita nemusí fungovat. Jednotlivé bity mohou být perfektní, ale když se n-tý bit shoduje s paritou předchozích $n-1$ bitů, parita všech n bitů bude vždy 0. Pokud tedy chceme získat kvalitní náhodné bity z nekvalitního generátoru, musíme použít buď náhodné semínko (podobně jako u pseudonáhodných generátorů), nebo nějakou vlastnost daného generátoru. Algoritmy, které takto vyrobí pravděpodobnostní rozdělení blízké uniformnímu ze zdroje, který není blízký uniformnímu pravděpodobnostnímu rozdělení, se nazývají *extraktory*.

Dále nás bude zajímat situace, kdy polovina bitů je z jednoho generátoru, druhá z druhého a oba generátory jsou *nezávislé*. V této situaci můžeme získat téměř nezávislé náhodné bity bez použití náhodného semínka. K tomu účelu ovšem musí být v obou generátorech nějaká náhodnost, přesněji řečeno, výstup z každého ze dvou generátorů musí mít dostatečnou entropii. Teď jde o to, kolik entropie je potřeba a zda se dají náhodné bity extrahovat efektivně, tj. pomocí polynomiálního algoritmu.

Nyní krátce odbočíme do teorie grafů, zdánlivě jiné oblasti, ale rychle se dostaneme zpět k teorii extraktorů. V roce 1947 Paul Erdős dokázal [6], že každý neorientovaný graf obsahuje kliku nebo nezávislou množinu velikosti k, kde $k \geqq (\frac{1}{2} - o(1)) \log n$. (Klika je množina vrcholů, které jsou všechny spojené hranou, nezávislá množina je množina vrcholů, kde žádné dva nejsou spojené hranou.) Je to výsledek, který se řadí do důležité oblasti (nejen konečné) kombinatoriky zvané Ramseyova teorie. Erdős také dokázal, že existuje graf, který neobsahuje žádnou kliku ani nezávislou množinu velikosti $k \geqq (2 + o(1)) \log n$. Důkaz existence grafů bez malých klik a nezávislých množin je nekonstruktivní. Byl to asi první důkaz v extremální kombinatorice, který použil tzv. pravděpodobnostní metodu. Proto Erdős předložil problém sestrojit takový graf explicitně.

Nyní se budeme zabývat problémem, který je variantou zmíněného problému pro bipartitní grafy. Bipartitní grafy si můžeme nejlépe představit jako matice nul a jedniček, a proto dále budeme mluvit jen o maticích a nikoliv o grafech. Dále se omezíme jen na čtvercové matice o rozměrech $n \times n$. Podobná tvrzení, jako dokázal Erdős ve svém zásadním článku, lze dokázat i pro bipartitní verzi. V řeči matic to znamená, že uvažujeme všechny čtvercové nula-jedničkové matice a zajímá nás, zda daná matice má podmatici $k \times k$ tvořenou samými nulami nebo samými jedničkami. Odhady pro k se liší od předchozího problému jen konstantními faktory. Porovnáme-li Erdősův problém

s problémem pro bipartitní grafy, je hned zřejmé, že problém konstrukce pro bipartitní grafy je těžší, protože musíme vyloučit všechny podmatice o rozměrech $k \times k$ tvořené samými nulami nebo jedničkami, nejen hlavní podmatice jako v původním problému.[2] Hadamardovy matice (s minus jedničkami nahrazenými nulami) dávají konstrukci pro $k = \sqrt{n}$, což byl dlouho nejlepší odhad, který bylo možno konstruktivně dokázat.

Vraťme se k extraktorům. Dva náhodné zdroje můžeme reprezentovat výběrem dvou čísel $i, j \in \{1, 2, \ldots, n\}$. Vybíráme i a j nezávisle na sobě, ale ne uniformně z $\{1, 2, \ldots, n\}$. Z hlediska extraktorů se můžeme bez újmy na obecnosti omezit na speciální pravděpodobnostní rozložení, kde se i vybírá uniformně z nějaké podmnožiny I a j uniformně z nějaké podmnožiny J, přičemž $|I| = |J| = k$. Extraktor je potom matice M, která pro každou dvojici takových množin I, J má přibližně stejný počet jedniček i nul na podmatici s řádky I a sloupci J. Tato vlastnost matice M je samozřejmě mnohem silnější než vlastnost, že takové podmatice nejsou utvořeny ze samých nul nebo samých jedniček. Ukázalo se však, že dívat se na ramseyovský problém z hlediska extraktorů bylo zásadní pro dosažení pokroku v obou směrech, jak v Ramseyově teorii, tak v teorii extraktorů.

Prolomit bariéru $\sqrt{n}$ se podařilo až v roce 2004 v našem společném článku s Vojtěchem Rödlem [10]. Pak se daly věci rychle do pohybu. Bylo to díky v té době již rozvinuté teorii extraktorů a jednomu výsledku z teorie čísel. Historie tohoto výsledku sahá do roku 1983, kdy Endre Szemerédi a Paul Erdős dokázali, že existují konstanty $\epsilon > 0$ a c takové, že pro každou neprázdnou množinu reálných čísel A platí

$$\max(|A + A|, |A \cdot A|) \geqq c|A|^{1+\epsilon}.$$

V devadesátých letech minulého století si Wigderson všiml, že pokud by podobná věta platila i v konečných tělesech, umožňovalo by to konstrukci zajímavých extraktorů. V roce 2004 tuto domněnku dokázali Jean Bourgain, Nets Katz a Terence Tao pro prvočíselná tělesa za předpokladu, že množina A je dostatečně malá vzhledem k velikosti tělesa [4]. To byl klíčový moment, který odstartoval závod sestrojit matici, která by neměla podmatice $k \times k$ ze samých nul nebo samých jedniček pro co nejmenší k. Dalo to ještě hodně práce, ale výsledkem byla konstrukce, která podstatně vylepšila dosavadní rekord a vedla k hodnotě $k = 2^{2^{(\log\log n)^{1-\epsilon}}}$, $\epsilon > 0$. Tím autoři nejen dostali podstatně menší k pro bipartitní případ, ale překonali i dosavadní rekordy pro původní Erdősův problém. Konstrukce je vlastně značně komplikovaný polynomiální algoritmus pro výpočet prvků matice. Wigdersonův šedesátistránkový článek [2] napsaný se spoluautory vyšel v roce 2012 v Annals of Mathematics.[3]

4. Zig-zag součin a expandery

Důležitou roli v informatice hrají grafy, které se nazývají *expandery*. Mají mnoho aplikací, např. v derandomizaci, samoopravných kódech a konstrukci třídicích sítí. Expander je neorientovaný d-regulární graf G (tj. graf, ve kterém jsou stupně všech vrcholů

[2] Hlavní podmatice je matice, která vznikne odstraněním určitého počtu řádků a sloupců s *týmiž indexy*.

[3] Vylepšování jejich konstrukce ještě pokračovalo dále, ale toho se už Wigderson nezúčastnil. Nejlepší současná konstrukce [5] dává $(\log n)^{(\log\log\log n)^{O(1)}}$.

rovné d) takový, že všechny ne příliš velké množiny expandují. Expanzi definujeme tak, že pro každou podmnožinu vrcholů X, jejíž mohutnost je nanejvýš polovina mohutnosti množiny všech vrcholů V, porovnáme velikost množiny vrcholů sousedících s X s velikostí X. Označíme-li ∂X množinu vrcholů sousedících s X, pak expanze je

$$e := \min_{0<|X|\leqq\frac{1}{2}|V|} \frac{|\partial X|}{|X|}.$$

Vlastnost býti expanderem je asymptotická, proto definujeme expandery jako nekonečnou posloupnost grafů, kde mohutnosti množin vrcholů rostou, stupeň d je konstanta a expanze je alespoň e pro nějakou kladnou konstantu.

Expandery lze definovat také pomocí vlastnosti spektra (tj. vlastních čísel) matice sousednosti grafu. Vypočítat vlastní čísla je také nejlepší způsob, jak dokázat, že graf je expander. Nechť G je d-regulární graf. Pak d je největší vlastní číslo matice sousednosti. Označme λ_G druhé největší vlastní číslo. Pro posloupnost d-regulárních grafů je nutné a stačí, aby poměr λ_G/d byl shora omezen nějakou konstantou menší než 1. Rozdíl $d - \lambda_G$ nazveme *spektrální mezerou*.

Původní konstrukce expanderů byly založeny na Cayleyho grafech některých grup. Pro konečnou grupu G a množinu S prvků grupy G je Cayleyho graf $C(G, S)$ definován následovně: Množinu vrcholů grafu $C(G, S)$ tvoří prvky grupy G a dva prvky $a, b \in G$ jsou spojeny hranou, pokud $ab^{-1} \in S \cup S^{-1}$. Cayleyho graf $C(G, S)$ je d-regulární pro $d = |S|$. Dokázat, že konkrétní Cayleyho grafy jsou expandery, vyžaduje použití netriviálních výsledků z teorie grup a jejich reprezentací.

V roce 2000 Omer Reingold, Salil Vadhan a Avi Wigderson navrhli čistě kombinatorickou konstrukci [11][4], která z daného grafu, jenž je dostatečně dobrým expanderem, vyrobí nekonečnou posloupnost stále větších expanderů, a to iterací dvou operací na grafech. První operace je jednoduchá: Z daného grafu G sestrojíme graf G^2 tak, že vezmeme stejnou množinu vrcholů a dva vrcholy spojíme, pokud v původním grafu mezi nimi vede cesta délky 2. Druhá operace je složitější, je to nový druh součinu, který autoři nazvali *zig-zag product*. Nechť G je d-regulární graf s n vrcholy a H je c-regulární graf s d vrcholy. Zig-zag součin $G \otimes_z H$ dostaneme následujícím způsobem:

1. Každý vrchol v grafu G nahradíme d-prvkovou množinou $\{v_{e_1}, \ldots, v_{e_d}\}$, kde $e_1, \ldots, e_d$ jsou hrany grafu G spojené s v. Potom spojíme hranou všechny dvojice vrcholů v_e, u_e, kde e je hrana spojující vrcholy v, u, pokud taková hrana existuje.
2. Pro každý vrchol v grafu G položíme na množinu $\{v_{e_1}, \ldots, v_{e_d}\}$ kopii grafu H. Takto získáme pomocný graf F, kde některé hrany pochází z G a jiné pochází z kopií grafu H.
3. Na množině vrcholů grafu F nyní definujeme graf $G \otimes_z H$ tak, že spojíme hranou každé dva vrcholy, které spojuje nějaká cesta h_1, g, h_2 v F, kde h_1, h_2 jsou hrany v kopiích H a g je hranou z G.

Všimněme si, že $G \otimes_z H$ má nd vrcholů a jejich stupně jsou c^2.

Smysl první operace spočívá ve zvětšení spektrální mezery. Matice sousednosti grafu G^2 je mocnina matice sousednosti grafu G, proto dostaneme $\lambda_{G^2} = \lambda_G^2$, čímž se zmenší λ_G/d na $(\lambda_G/d)^2$. Nevýhodou této operace je, že zvýší stupeň grafu z d na d^2.

[4] Za tuto práci Reingold a Wigderson obdrželi Gödelovu cenu.

Úlohou druhé operace je snížit stupeň na c^2. Nevýhodou je, že se sníží spektrální mezera, ale úbytek není velký. Dá se odhadnout, že

$$\lambda_{G \otimes_z H} \leqq \lambda_G + \lambda_H + \lambda_H^2.$$

Při vhodné volbě H můžeme střídavě graf umocňovat a násobit H a přitom udržet stupeň rovný c^2 a dostatečně malé λ. Taková posloupnost grafů je definována rekurentně:

$$G_1 = H^2, \quad G_{i+1} = G^2 \otimes_z H.$$

Konkrétní volba parametrů grafu H, pro které se takto dá sestrojit posloupnost expanderů, je $d = c^4$ a $\lambda_H \leqq 1/5$, čímž se dostane $\lambda_{G_i} \leqq 2/5$. Myšlenka, proč to funguje, je založena na tom, že autoři si představují expander jako pseudonáhodný objekt a sledují „jak se šíří entropie“, když se procházejí hrany grafu.

Pomocí této konstrukce se také podařilo vyřešit problém týkající se Cayleyho grafů, totiž otázku, zda skutečnost, že Cayelyho graf je expander, záleží na volbě d-prvkové množiny S. Bylo známo, že záleží na volbě grupy, protože např. pro komutativní grupy nemůžeme nikdy dostat expander. Noga Alon, Alexander Lubotzky a Avi Wigderson nalezli grupy, kde pro jednu volbu S velikosti d vznikne expander, ale pro jinou nikoliv [1]. Jak je možné dokázat něco o Cayleyho grafech pomocí zig-zag součinu? Vtip je v tom, že za určitých předpokladů o grupách a množinách S je Cayleyho graf semidirektního součinu dvou grup totéž co zig-zag součin Cayleyho grafů těchto grup.

O expanderech pojednává ještě dalších deset Wigdesonových článků.

5. Další výsledky

Z četných dalších výsledků zmíníme stručně jen dva. V oblasti složitosti booleovských obvodů hraje důležitou roli tzv. *Karchmerova–Wigdersonova hra*. Wigderson ve společné práci s Mauriciem Karchmerem nalezl charakterizaci hloubky obvodů pomocí komunikační hry, která nyní nese jejich jméno [8]. Pomocí této hry sice neumíme dokázat dolní odhady na hloubku obecných booleovských obvodů, ale lze dokázat takové odhady alespoň pro speciální třídy obvodů. Wigderson dosáhl významných výsledků i v důkazové složitosti. Nejznámější z nich vyšel ve společné práci s Eli Ben-Sassonem [3], ve které nalezli vztah mezi šířkou a velikostí rezolučních důkazů. Protože šířka se dá často snadno odhadnout, umožňuje tento vztah dokazovat jednoduše dolní odhady na velikost rezolučních důkazů.

Čtenář si jistě všiml, že všechny zmíněné Wigdersonovy publikace mají spoluautory. To jen dokumentuje styl, jakým Wigderson pracuje. Je vždy ochoten se nezištně podělit o svoje nápady, nebo pomoci radou, aniž by očekával odměnu ve formě spoluautorství. Jeho kolegové to oceňují a rádi s ním spolupracují. Takto se mu podařilo vytvořit kolem sebe skupinu studentů a mladých vědců, která byla úspěšnější, než kdyby každý pracoval sám.

Nakonec ještě musíme zmínit jeho nedávno vyšlou knihu *Mathematics and Computation: A Theory Revolutionizing Technology and Science* [12]. V ní se čtenář může nejlépe seznámit s oborem, ve kterém Avi Wigderson pracuje. Obálka knihy znázorňuje blok popsaný rukou, což vyjadřuje Wigdersonův životní postoj: nedbat na formality.

Poděkování. Článek byl podpořen grantem RVO: 67985840.

L i t e r a t u r a

[1] Alon, N., Lubotzky, A., Wigderson, A.: *Semi-direct product in groups and zig-zag product in graphs: Connections and applications*. 42nd IEEE Symposium on Foundations of Computer Science, Las Vegas, NV, 2001, IEEE Computer Soc., Los Alamitos, CA, 2001, 630–637.

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

[3] Ben-Sasson, E., Wigderson, A.: *Short proofs are narrow – resolution made simple*. J. ACM 48 (2001), 149–169.

[4] Bourgain, J., Katz, N., Tao, T.: *A sum-product estimate in finite fields, and applications*. Geom. Funct. Anal. 14 (2004), 27–57.

[5] Cohen, G.: *Towards optimal two-source extractors and Ramsey graphs*. STOC'17 – Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, ACM, New York, 2017, 1157–1170.

[6] Erdős, P.: *Some remarks on the theory of graphs*. Bull. Amer. Math. Soc. 53 (1947), 292–294.

[7] Kabanets, V., Impagliazzo, R.: *Derandomizing Polynomial Identity Tests means proving circuit lower bounds*. Comput. Complexity 13 (2004), 1–46.

[8] Karchmer, M., Wigderson, A.: *Monotone circuits for connectivity require superlogarithmic depth*. SIAM J. Discrete Math. 3 (1990), 255–265.

[9] Nisan, N., Wigderson, A.: *Hardness vs randomness*. J. Comput. System Sci. 49 (1994), 149–167.

[10] Pudlák, P., Rödl, V.: *Pseudorandom sets and explicit constructions of Ramsey graphs*. In: J. Krajíček (ed.): Complexity of Computations and Proofs, Quaderni di Matematica, vol. 13, Caserta, 2004, 327–346.

[11] Reingold, O., Vadhan, S., Wigderson, A.: *Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors*. Ann. of Math. 155 (2002), 157–187.

[12] Wigderson, A.: *Mathematics and computation: A theory revolutionizing technology and science*. Princeton University Press, 2019.