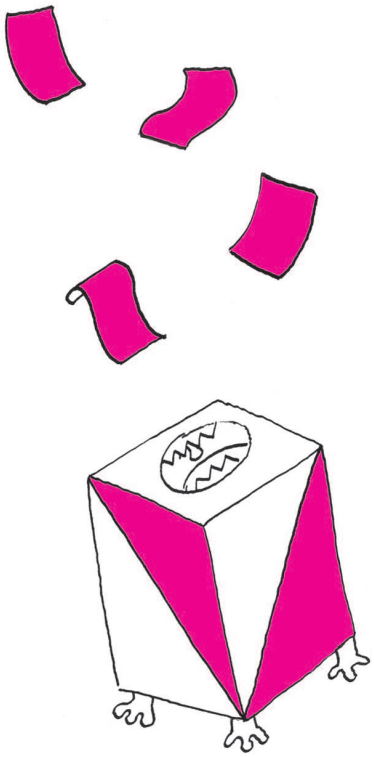
Demokracja i (*NP*-)trudne problemy

Andrzej DĄBROWSKI[*]



Podczas XXVII Kongresu Matematycznego, odbywającego się w Seulu między 13 a 21 sierpnia 2014 roku, prestiżową Nagrodę Nevanlinny (informatyczny odpowiednik Medalu Fieldsa) otrzymał pracujący w USA hinduski informatyk Subhash Khot. W laudacji poświęconej wynikom Khota jego mentor i współautor wielu prac, Sanjeev Arora, wspomniał o przełomowym wyniku uzyskanym przez profesora Uniwersytetu Warszawskiego, Krzysztofa Oleszkiewicza wraz z Elchananem Mosselem i Ryanem O'Donnellem. W pracy *Noise stability of functions with low influences: Invariance and optimality*, opublikowanej w *Annals of Mathematics* w 2010 roku, udowodniona została, istotnie związana z wynikami Subhasha Khota, hipoteza *Większość jest najbardziej stabilna* (*MiS*, *Majority is Stablest*). Hipotezę tę można interpretować w języku teorii zajmującej się systemami głosowania. Fascynujące jest jej powiązanie z należącymi do informatyki teoretycznej wynikami Khota, które z kolei są ściśle związane z nierozstrzygniętą hipotezą $P \neq NP$, wartego milion dolarów Problemu Milenijnego. Została ona postawiona na początku lat 70. niezależnie przez Stephena Cooka i Leonida Levina. Mimo upływu przeszło 40 lat nikomu nie udało się ani jej udowodnić, ani obalić. Jak każdy wielki problem, stała się źródłem wielu cennych wyników w różnych działach matematyki i informatyki teoretycznej, szczególnie w teorii złożoności obliczeniowej.

Problem $P \neq NP$ jest związany z konstrukcją efektywnych, czyli wykonywanych w realistycznym czasie, algorytmów. Czas wykonywania algorytmu zależy od wielkości użytych w nim danych. Mówimy, że jest on *wielomianowy*, jeśli istnieją takie stałe C i k, że dla danych o rozmiarze n algorytm potrzebuje co najwyżej Cn^k kroków. Klasę problemów, dla których istnieje algorytm rozwiązania w wielomianowym czasie, oznaczamy przez P. Istnieją problemy, o których nie wiadomo, czy należą do tej klasy, można jednak w czasie wielomianowym sprawdzić poprawność dowolnie zadanego rozwiązania. O takich problemach mówimy, że należą do klasy NP. Oczywiście, gdy problem jest klasy P, to jest również klasy NP, gdyż w takim przypadku możemy sprawdzić poprawność rozwiązania w czasie wielomianowym, po prostu sami je rozwiązując. Czy prawdziwe jest twierdzenie odwrotne, oznaczające, że każdy problem, którego rozwiązanie można efektywnie sprawdzić, ma efektywny algorytm jego rozwiązania? Gdyby umiejętność oceny poprawności rozwiązania pociągała zdolność do jego konstrukcji, czyli gdyby $NP \subset P$, to, jak powiedział profesor MIT Scott Aaronson, *każdy, kto umiałby docenić piękno symfonii, zostałby Mozartem. Każdy, kto potrafi śledzić rozumowanie krok po kroku, zostałby Gaussem.*

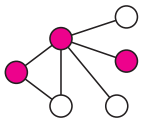
Przykładem zagadnienia ściśle powiązanego z tą problematyką jest próba znalezienia minimalnego pokrycia grafu niezorientowanego. W roku 1972 Richard M. Karp z Uniwersytetu Kalifornijskiego w Berkeley wykazał, że jeśli $P \neq NP$, to nie istnieje efektywny (czyli działający w wielomianowym czasie) sposób rozwiązania tego zadania. Rozważmy jednak następujący, prosty algorytm:

1. Wybierz krawędź grafu. Dołącz do pokrycia oba wierzchołki połączone tą krawędzią.
2. Usuń z grafu te wierzchołki i *wszystkie* krawędzie zawierające co najmniej jeden z tych wierzchołków.
3. Powtarzaj kroki 1–2 aż do wyczerpania krawędzi grafu.

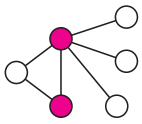
Nietrudno zauważyć, że ten algorytm znajduje pokrycie grafu. Nie musi być ono minimalne, zawiera jednak co najwyżej dwukrotnie więcej wierzchołków niż rozwiązanie idealne (wśród każdej pary usuwanych wierzchołków musi znaleźć się co najmniej jeden należący do pokrycia minimalnego). Skonstruowaliśmy zatem przykład *algorytmu przybliżonego* ze współczynnikiem 2. Ogólniej:

> Algorytm rozwiązania problemu minimum jest *przybliżony ze współczynnikiem* $\alpha \geqslant 1$, jeśli znalezione za jego pomocą rozwiązanie x spełnia dla każdej instancji warunek $f(x) \leqslant \alpha f(x_0)$, gdzie f jest minimalizowaną funkcją, a x_0 rozwiązaniem optymalnym.

Mówimy, że podzbiór wierzchołków grafu jest jego pokryciem, gdy każda krawędź zawiera co najmniej jeden z wierzchołków tego podzbioru, tak jak zbiór kolorowych wierzchołków na rysunku poniżej.

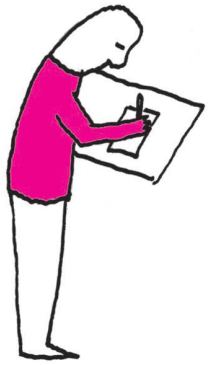


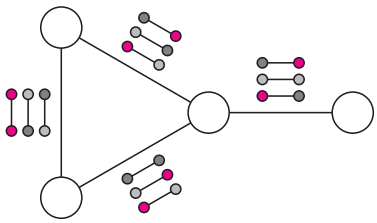
Minimalne pokrycie to pokrycie wykorzystujące najmniejszą możliwą liczbę wierzchołków, na przykład tak:



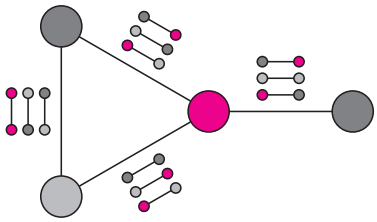
Instancja to egzemplarz problemu, np. zadanego grafu.

[*]Instytut Matematyczny, Uniwersytet Wrocławski

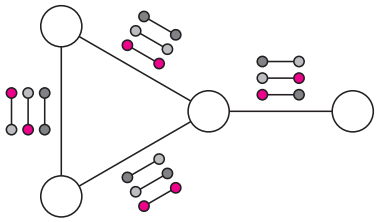


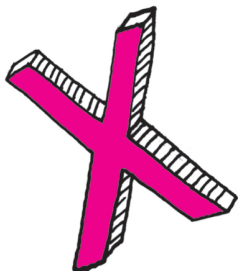


Powyższy graf z zadanym zestawem ograniczeń ma rozwiązanie – i to nawet trzy. Jednym z nich jest poniższe.



Dla takiego samego grafu z innym systemem ograniczeń (poniżej) możliwe jest spełnienie co najwyżej trzech z nich.





Analogicznie możemy zdefiniować przybliżony algorytm rozwiązania problemu *maksimum* ze współczynnikiem $\alpha \leqslant 1$. Takie rozwiązania mają wielkie znaczenie praktyczne – skoro nie można osiągnąć efektywnego rozwiązania optymalnego, sięga się po prostsze rozwiązania przybliżone. Powstaje naturalne pytanie, czy aktualnie funkcjonujące rozwiązania można jeszcze choć trochę polepszyć, a więc dla jakich α istnieją przybliżone rozwiązania efektywne o tym współczynniku. Okazuje się, że istnienie takich granic efektywności również związane jest z omawianą hipotezą. W roku 2002 Irit Dinur i Shmuel Safra pokazali, że jeśli $P \neq NP$, to dla problemu minimalnego pokrycia grafu nie istnieje nawet przybliżony algorytm o wielomianowym czasie działania o współczynniku mniejszym niż $\alpha = 10\sqrt{5} - 21 \approx 1{,}36$.

W roku 2001 pojawił się inny ciekawy problem optymalizacyjny, który przedstawił swojemu promotorowi, Sanjeevowi Arorze, 23-letni student Uniwersytetu Princeton, Subhash Khot. Zadanie jest wariantem problemu kolorowania wierzchołków grafu na k kolorów w taki sposób, aby wierzchołki połączone krawędzią miały różne kolory. Istnieje prosty i efektywny algorytm rozstrzygający, czy pokolorowanie jest możliwe dla $k = 1$ i $k = 2$. Dla $k \geqslant 3$ jest to problem *NP-trudny*, czyli problem, do którego można w czasie wielomianowym przekształcić *każdy* problem *NP*. Oznacza to, że gdy $P \neq NP$, to nie istnieje efektywny algorytm kolorowania.

To, co odróżnia przypadek $k < 3$ od przypadku $k \geqslant 3$ i co jest jednym z powodów tak nagłego wzrostu złożoności, to fakt, że w tym drugim przypadku kolor wierzchołka nie wyznacza jednoznacznie koloru jego sąsiadów. Khot zaproponował, by dla każdej krawędzi wyznaczony był zestaw dopuszczalnych pokolorowań końców, zwanych ograniczeniami, w którym kolor jednego końca krawędzi jednoznacznie wyznacza kolor drugiego. Czasami taki zestaw ograniczeń jest sprzeczny – nie istnieje pokolorowanie grafu spełniające wszystkie ograniczenia. I tu Khot zażądał, aby znaleźć pokolorowanie spełniające maksymalną liczbę ograniczeń. Innymi słowy, dla każdego grafu z ograniczeniami poszukuje się pokolorowania o maksymalnej *wartości*, czyli ułamka liczby krawędzi grafu, spełniających przypisane im ograniczenia. Ta maksymalna wartość wynosi 1 w grafie, dla którego istnieje pokolorowanie spełniające wszystkie ograniczenia, jeśli natomiast nie istnieje pokolorowanie spełniające którekolwiek z ograniczeń, wynosi 0. Maksymalna wartość w grafie z drugiego przykładu wynosi $\frac{3}{4}$.

Gdy maksymalna wartość grafu jest równa 1, to szybko można znaleźć właściwe pokolorowanie. Wystarczy rozpatrzeć wszystkie przypadki pokolorowania *jednego* węzła, gdyż determinują one jednoznacznie pokolorowanie całego grafu. Takie grafy łatwo rozpoznać, jest to jednak znacznie trudniejsze dla grafów z maksymalną wartością nawet nieznacznie mniejszą od 1. Okazuje się bowiem, że odróżnienie dwóch skrajnych typów grafów:

- graf, dla którego najlepsze pokolorowanie ma wartość co najmniej równą $1 - \varepsilon$ dla danego z góry $\varepsilon > 0$ (przypadek *TAK*),
- graf, dla którego najlepsze pokolorowanie ma wartość co najwyżej równą δ dla danego z góry $\delta > 0$ (przypadek *NIE*),

jest bardzo problematyczne, jeśli dysponujemy dużą liczbą kolorów (i tym samym dużą liczbą ograniczeń dla krawędzi). Trudność tę formalnie wyraża sformułowana przez Khota w 2002 roku hipoteza *Unique Games Conjecture* (*UGC*).

> Dla każdej pary $\varepsilon, \delta > 0$ istnieje taka liczba kolorów $n = n(\varepsilon, \delta)$, że odróżnienie grafu spełniającego przypadek *TAK* od grafu spełniającego przypadek *NIE* jest *NP*-trudne.

Hipoteza *UGC* do dziś nie została rozstrzygnięta. Jej istnienie pozwala jednak spojrzeć na znane problemy z nowego punktu widzenia. Gdyby była prawdziwa, to znalezienie nawet przybliżonego rozwiązania dla wielu problemów okazałoby się niezwykle trudne. Wiemy już, na przykład, że w problemie minimalnego pokrycia grafu nie ma nawet przybliżonego efektywnego rozwiązania o współczynniku mniejszym niż 1,36. Znamy za to proste rozwiązanie o współczynniku 2.

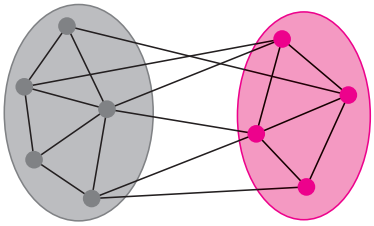
W 2003 roku Khot i Regev wykazali, że

gdy hipoteza *UGC* jest prawdziwa, to znalezienie przybliżonego rozwiązania o dowolnym współczynniku *mniejszym* od 2 jest *NP*-trudne.

Oznacza to, że zaproponowane przez nas proste rozwiązanie przybliżone jest najlepszym nietrudnym sposobem podejścia do zadania.

Kolejnym znanym problemem jest znalezienie maksymalnego cięcia w grafie (problem *MAXCUT*). Polega on na podziale wierzchołków grafu na dwa podzbiory (tzn. dokonaniu *cięcia*). Jego rozmiarem nazwiemy liczbę krawędzi „granicznych", których wierzchołki należą do różnych podzbiorów. Należy oczywiście znaleźć cięcie o największym rozmiarze. *MAXCUT* jest problemem *NP*-trudnym, a więc (o ile $P \neq NP$) nie istnieje efektywny sposób znalezienia maksymalnego cięcia. Sensownym rozwiązaniem jest znalezienie algorytmu przybliżonego. Pierwszy algorytm o współczynniku $\alpha = \frac{1}{2}$ znaleziono w roku 1976. Po 18 latach Goemans i Williamson znaleźli lepszy algorytm, oparty na rozumowaniu czysto geometrycznym, co wprawiło w zdumienie znawców zagadnienia. Wyznaczony przez nich współczynnik α wynosi

Rozmiar cięcia na poniższym rysunku wynosi 6.

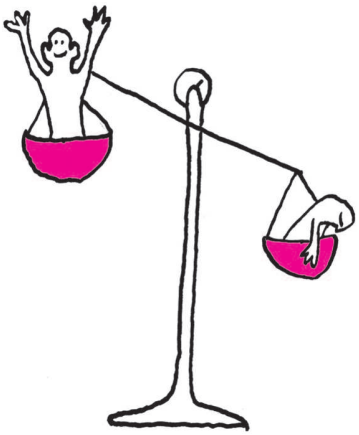


$$\alpha_{GW} = \min_{0<\theta<\pi} \frac{2\theta}{\pi(1-\cos\theta)} \approx 0{,}878567.$$

Podobnie, jak w przypadku minimalnego pokrycia grafu, hipoteza *UGC* wyjaśnia sprawę do końca, to znaczy

Jeżeli hipoteza *UGC* jest prawdziwa, to każdy przybliżony algorytm w problemie *MAXCUT* o współczynniku większym niż α_{GW} jest *NP*-trudny.

Rezultat ten został opublikowany w 2005 roku, ale przy dodatkowym założeniu o prawdziwości wówczas jeszcze nierozstrzygniętej hipotezy *MiS*. Dowód jej prawdziwości ogłoszono jednak jeszcze w tym samym roku w materiałach pewnej konferencji poświęconej podstawom informatyki – jednym ze współautorów tego wyniku jest wspomniany już Krzysztof Oleszkiewicz. Najlepsze przybliżone rozwiązanie problemu *MAXCUT* zależy więc tylko od prawdziwości hipotezy *UGC*.



Przyjrzyjmy się bliżej hipotezie *MiS*. Jest ona związana z analizą harmoniczną funkcji boolowskich. Definicje i twierdzenia w tej dziedzinie zazwyczaj formułowane są w języku polityki i teorii wyboru socjalnego (np. współczynnik siły koalicji Banzhafa czy twierdzenie Arrowa o dyktaturze). Hipoteza dotyczy stabilności systemu głosowania, w którym głosuje się na jedną z alternatyw, tak jak w wyborach prezydenckich w Stanach Zjednoczonych. System wyborów w tym kraju jest pośredni: wyborcy głosują na kolegium elektorskie, a następnie elektorzy dokonują wyboru prezydenta. W wielu krajach panuje bezpośredni system większościowy, gdzie większość głosów wyborców decyduje o wyborze.

Spektakularnym przykładem występowania niestabilności systemu elektorskiego był przypadek wyborów prezydenckich w roku 2000. Rywalizowali wtedy George W. Bush i Al Gore. Językiem u wagi w tych wyborach okazało się głosowanie na Florydzie. Wyniki we wszystkich stanach, bez Florydy, wskazywały na wygraną Busha w większości stanów, ale Gore miał więcej głosów elektorskich. Różnica głosów na Florydzie była niewielka, a co więcej, niestarannie przygotowana karta do głosowania mogła spowodować błędne zakwalifikowanie głosu przez maszynę zliczającą. Walka toczyła się o decydujące 25 głosów elektorskich Florydy. Ostatecznie Bush otrzymał na Florydzie 2 912 790 głosów, Al Gore 2 912 253 głosy. Przewaga Busha wyniosła tylko 537 głosów (przewaga 0,009%). Gdyby w Stanach Zjednoczonych panował system większościowy bezpośredni, wybory wygrałby Gore. W obowiązującym systemie elektorskim wygrał jednak Bush.

Niestabilność systemu objawiła się zbytnią wrażliwością systemu elektorskiego na niepewne wyniki u niewielkiej liczby głosujących. W tym przypadku wady tej nie miał system bezpośredni. Spróbujmy ją opisać za pomocą matematycznego formalizmu. Niech $x_1, x_2, \ldots, x_n$ będą wynikami głosowania na jednego z dwóch kandydatów, które koduje się jako -1 i 1. System głosowania jest funkcją n zmiennych $f(x_1, x_2, \ldots, x_n)$ o wartościach w zbiorze $\{-1, 1\}$. System,

w którym istnieje taki wskaźnik $1 \leqslant d \leqslant n$, że $f(x_1, x_2, \ldots, x_n) = x_d$, nazywa się *dyktaturą*, a wyborca o indeksie d – dyktatorem. System opisany funkcją

$$\mathrm{Maj}_n(x_1, x_2, \ldots, x_n) = \mathrm{sgn}(x_1 + x_2 + \ldots + x_n)$$

System większościowy określony jest tylko dla n nieparzystego, co w praktyce nie jest żadnym ograniczeniem.

nazywany jest *większościowym*. *Wpływem i-tego wyborcy* na wynik głosowania jest liczba

$$\mathrm{Inf}_i(f) = \mathrm{P}(f(x) \neq f(x^i)),$$

gdzie $x^i = (x_1, \ldots, x_{i-1}, -x_i, x_{i+1}, \ldots, x_n)$ jest głosowaniem, w którym i-ty wyborca zmienił swoją decyzję. Wpływ i-tego wyborcy jest zatem prawdopodobieństwem zauważenia skutku zmiany decyzji tego wyborcy. Dla dyktatury $\mathrm{Inf}_i(f) = 0$, gdy $i \neq d$ oraz $\mathrm{Inf}_d(f) = 1$. Dyktator ma absolutny wpływ na wynik wyborów, inni wyborcy nie mają żadnego. System uważa się za *daleki od dyktatury*, gdy dla pewnego małego $\tau > 0$ zachodzi $\mathrm{Inf}_i(f) \leqslant \tau$ dla każdego wyborcy i. O liczbie τ można zatem myśleć jako o poziomie niezależności od dyktatury. Dla systemu większościowego

$$\mathrm{Inf}_i(\mathrm{Maj}_n) = \frac{\binom{n-1}{\frac{n-1}{2}}}{2^{n-1}} \approx \frac{1}{2\sqrt{\pi(n-1)}}.$$

Wpływ każdego z wyborców jest taki sam i jest niewielki, gdy liczba wyborców jest duża – przy takiej liczbie wyborców system większościowy jest zatem daleki od dyktatury.

Badanie jakości systemu głosowania prowadzi się poprzez analizę jego własności w najbardziej nieprzewidywalnych warunkach, to znaczy wtedy, gdy wyborcy głosują niezależnie i z tym samym prawdopodobieństwem na każdego z kandydatów. Jeśli wówczas $\mathrm{E}f(x) = 0$, to mówimy, że system wyborczy jest *zrównoważony*. Aby zbadać jego podatność na zmiany, rozważymy sytuację, w której każdy z wyborców zmienił decyzję z ustalonym prawdopodobieństwem. Niech zatem $x = (x_1, x_2, \ldots, x_n)$ będzie wektorem wyników głosowania oraz niech $y = (y_1, y_2, \ldots, y_n)$ będzie wektorem, jaki powstałby z wektora x, gdyby każdy z wyborców losowo i z prawdopodobieństwem $p \leqslant \frac{1}{2}$ zmienił swoją decyzję. Wtedy $\mathrm{P}(y_i = -x_i) = p$ i $\mathrm{P}(y_i = x_i) = 1 - p$. Wektory x i y są ze sobą ściśle związane. Ich współczynnik korelacji wynosi $\rho = 1 - 2p$, jest nieujemny i jest malejącą funkcją p. Funkcjonał

$$S_\rho(f) = \mathrm{P}(f(x) = f(y)) - \mathrm{P}(f(x) \neq f(y))$$

nazywa się *stabilnością na poziomie* ρ systemu f. Wartości S_ρ zbliżone do zera charakteryzują systemy stabilne. Dla dyktatury $S_\rho(f) = \rho$. Dla systemu większościowego stabilność jest skomplikowaną funkcją ρ, można jednak obliczyć granicę

$$\lim_{n\to\infty} S_\rho(\mathrm{Maj}_n) = \frac{2 \arcsin(\rho)}{\pi}.$$

Teraz wreszcie można sformułować hipotezę *MiS*.

Zadane są: współczynnik korelacji ρ i mała liczba $\varepsilon > 0$. Istnieje wtedy takie $\tau > 0$, że dla wszystkich zrównoważonych systemów wyborczych o poziomie niezależności od dyktatury τ zachodzi

$$S_\rho(f) \leqslant \frac{2 \arcsin(\rho)}{\pi} + \varepsilon.$$

Hipoteza została udowodniona we wspomnianej pracy Mossela, O'Donnella i Oleszkiewicza. W tej samej pracy została udowodniona jeszcze jedna niezwykle interesująca hipoteza, występująca pod barokową nazwą *It Ain't Over Till It's Over*. Mówi ona, że dla zrównoważonych systemów wyborczych istnieje taki poziom niezależności od dyktatury, że nawet gdy ujawni się frakcję $\rho < 1$ głosów losowo wybranych wyborców, to niezależnie od wartości ρ z dużym prawdopodobieństwem wynik wyborów jest jeszcze niezdecydowany.
W systemach dalekich od dyktatury ujawnienie nawet dużej frakcji wyników wyborów jeszcze nie daje pewności co do ostatecznego rezultatu. Boleśnie przekonał się o tym Al Gore i zapewne niewielkim pocieszeniem byłaby dla niego świadomość, z jak doniosłym matematycznym problemem związana była jego porażka w walce o prezydencki fotel.

Autor artykułu nie wie, czy nazwa ta wiąże się z piosenką Lenniego Kravitza o tym samym tytule.