Jak bronić wszystkich frontów jednocześnie

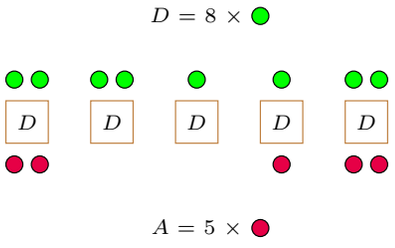
*Stanisław KAŹMIEROWSKI**

*Doktorant, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

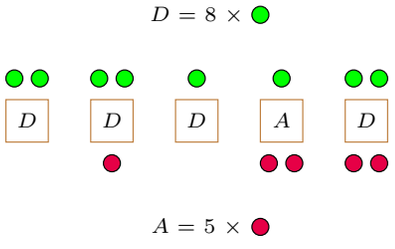
Napięcia graniczne pomiędzy Alandią i Delandią wzrastają od lat. Dwóch generałów, Acki i Decki, szykują swoje kraje do konfliktu zbrojnego. Delandzka doktryna wojenna jest ściśle **(D)**efensywna – po poprzedniej wojnie z Alandią, w której obie strony poniosły bardzo znaczące straty, sztab Delandii nie wyrazi zgody na żadne działania ofensywne. W związku z tym generał Decki może jedynie zadecydować o rozmieszczeniu delandzkich dywizji na przełęczach łączących obydwa kraje.

Alandzki sztab wyciągnął z poprzedniej wojny dokładnie odwrotne wnioski – **(A)**tak jest uważany za najskuteczniejszą metodę. Generał Acki ma zdecydować o kierunkach natarć przez przełęcze łączące obydwa kraje i przydzieleniu alandzkich dywizji do poszczególnych atakujących armii. W wypadku udanego ataku na dowolnej z przełęczy alandzkie armie zaleją Delandię, a ta będzie zmuszona kapitulować. Jeżeli żadnej z alandzkich armii nie uda się skutecznie przełamać frontu, gospodarka Alandii załamie się w związku z wysokimi kosztami prowadzenia ofensywnych działań wojennych, i to Alandia będzie zmuszona podpisać kapitulację. W związku ze stałą rotacją dywizji w obydwu krajach każdy z generałów podejmie decyzję niezależnie, nie znając rozmieszczenia dywizji przeciwnika. W jaki sposób obydwaj generałowie powinni przypisać dywizje, którymi dysponują?

Przy poniższym rozmieszczeniu dywizji Delandia wygra wojnę (nie straci żadnej przełęczy):



Z kolei takie rozmieszczenie dywizji zapewni zwycięstwo Alandii (która przeprawi się przez czwartą przełęcz):



Zabawmy się w strategów i spróbujmy znaleźć rozwiązanie dla tego problemu. W tym celu sformalizujemy powyższy scenariusz jako *grę strategiczną*. Gra strategiczna to następująca trójka: zbiór graczy, zbiór strategii każdego z graczy i funkcja wypłaty mówiąca o tym, jaki jest rezultat gry dla każdego z graczy przy każdej możliwej parze strategii. W rozważanym scenariuszu jest dwóch graczy (generałów): Acki i Decki. Każdy z nich zarządza pewną liczbą dywizji, opisanych odpowiednio przez liczby naturalne A i D. Pomiędzy dwoma krajami znajduje się pewna liczba n przełęczy. Strategią generała Ackiego jest rozmieszczenie A dywizji pomiędzy n przełęczy. Analogicznie, generał Decki przydziela D dywizji pomiędzy te same n przełęczy. Zakładamy, że każdy z generałów przydzieli wszystkie dywizje, którymi zarządza, w celu zmaksymalizowania szansy na wygranie konfliktu. Pojedyncza przełęcz będzie obroniona przed Delandię, jeżeli liczba delandzkich dywizji broniących tej przełęczy będzie nie mniejsza niż liczba atakujących dywizji z Alandii. W przeciwnym wypadku przełęcz zostanie stracona, a wojna przegrana przez Delandię. Delandia wygra wojnę tylko w przypadku skutecznego obronienia wszystkich przełęczy. Zwycięzca otrzyma wypłatę 1, a przegrany -1. Gra ta nazywana jest grą „Atak i Obrona” (*Attack and Defense*).

Gracz posiadający $C \in \{A, B\}$ dywizji może je rozmieścić pomiędzy n przełęczy na $\binom{n+C-1}{n-1}$ różnych sposobów. Aby to zobaczyć, wyobraźmy sobie, że gracz dysponuje $n + C - 1$ nierozróżnialnymi dywizjami ułożonymi w rzędzie. Usuwając $n - 1$ z nich, wybiera jednoznaczny podział C dywizji na n grup – pierwsza grupa zawiera dywizję od początku rzędu do pierwszej usuniętej dywizji, następne analogicznie. Liczba różnych rozmieszczeń jest zatem równa liczbie wyborów $n - 1$ elementów spośród $n + C - 1$. W związku z tym, że liczba strategii każdego z graczy jest wykładnicza względem parametrów gry, jest to *gra o zwięzłej reprezentacji*.

Warto zauważyć, że reprezentacja gry jest bardzo mała! Trójka (A, D, n) jednoznacznie definiuje zbiór strategii każdego z graczy i, co za tym idzie, całą grę. Ważną cechą opisanej gry jest bezpośrednie powiązanie wypłat obydwu graczy – sukces jednego z nich bezpośrednio łączy się z porażką drugiego, a suma wypłat obydwu graczy jest zawsze równa 0. Takie gry nazywamy *grami o sumie zerowej*.

Podstawową *koncepcją rozwiązania* gry strategicznej jest *równowaga Nasha*. Równowaga Nasha to para strategii, w której żaden z graczy nie może poprawić swojej wypłaty przez zmianę swojej strategi, gdy strategia drugiego z graczy pozostanie niezmieniona.

Okazuje się, że w grach o sumie zerowej wypłata ustalonego gracza w każdej równowadze Nasha jest zawsze taka sama. Jest to zatem wypłata, jaką może on sobie zagwarantować: niezależnie od tego, co zrobi przeciwnik, grając strategie z równowagi Nasha, uzyska on co najmniej taką wypłatę. Dlatego też strategie w równowadze Nasha w grach o sumie zerowej są w pewnym sensie optymalne. Wartość nieujemnej wypłaty w równowadze Nasha (jeden z graczy ma zawsze nieujemną wypłatę, drugi – niedodatnią) jest nazywana *wartością gry*.

Czy w tej grze istnieją równowagi Nasha? W niektórych przypadkach tak! Zauważmy, że jeżeli $A > D$ (Acki dysponuje większą liczbą dywizji niż Decki), to każda para strategii, w której Acki przypisuje wszystkie dywizje do jednego frontu, a Decki wybiera dowolny przydział swoich strategii, jest równowagą Nasha. W taki sytuacji Alandzkie dywizje przebiją się na froncie, do którego zostały przypisane niezależnie od strategii wybranej przez Deckiego. Podobna sytuacja zachodzi, gdy $D \geqslant n \cdot A$. W takim przypadku każda para strategii, gdzie Decki przypisuje do każdego frontu co najmniej A dywizji, a Acki wybiera dowolny podział swoich A dywizji, jest równowagą Nasha (tym razem to Delandia wygrywa wojnę).

W obu przypadkach wartość gry jest równa 1 – jeden z graczy może sobie zapewnić zwycięstwo.

Co się dzieje w pozostałych przypadkach, czyli gdy $A \leqslant D < n \cdot A$? Zacznijmy od rozważenia małego przykładu.

Przykładowa gra. Rozważmy przypadek, w którym Acki dysponuje dwoma dywizjami, Decki trzema, a państwa są połączone dwoma przełęczami, czyli grę zdefiniowaną przez trójkę $(A = 2, D = 3, n = 2)$. Decki dysponuje czterema strategiami – są to podziały dywizji $(3, 0), (2, 1), (1, 2)$ i $(0, 3)$, natomiast Acki ma do dyspozycji trzy strategie – $(2, 0), (1, 1)$ oraz $(0, 2)$. Tabelka na marginesie, zwana *macierzą wypłat*, opisuje wyniki gry (zwycięzcę) dla każdej pary strategii obydwu graczy.

Macierz wypłat w grze $(A = 2, D = 3, n = 2)$ – kolumny odpowiadają strategiom Ackiego, a wiersze strategiom Deckiego.

	$(2,0)$	$(1,1)$	$(0,2)$
$(3,0)$	D	A	A
$(2,1)$	D	D	A
$(1,2)$	A	D	D
$(0,3)$	A	A	D

Zauważmy, że przypisanie trzech dywizji do jednej przełęczy nie jest rozsądne z perspektywy Deckiego, gdyż wystarczą tylko dwie dywizje, aby uczynić daną przełęcz całkowicie chronioną przed atakiem Ackiego. W związku z tym założymy, że Decki dopuszcza jedynie strategie $(2, 1)$ lub $(1, 2)$. W konsekwencji Acki nigdy nie chce wybrać strategii $(1, 1)$, gdyż przegrywa ona z każdą ze strategii dopuszczanych przez Ackiego.

Uproszczona macierz wypłat po usunięciu nieopłacalnych strategii:

	$(2,0)$	$(0,2)$
$(2,1)$	D	A
$(1,2)$	A	D

Po takiej analizie dostajemy uproszczoną macierz wypłat, przedstawioną na marginesie. Gra opisana przez tę macierz wypłat nie ma równowagi Nasha – dla każdej pary strategii gracz przegrywający może zwiększyć swoją wypłatę z przegranej na wygraną poprzez zmianę swojej strategii.

Bardziej precyzyjnie – nie ma równowagi Nasha w *strategiach czystych* (niewtajemniczonym Czytelnikom zaraz wytłumaczymy, co to znaczy).

Analogiczny argument pokazuje, że zawsze gdy $A \leqslant D < n \cdot A$, równowaga Nasha nie istnieje. Jeżeli rozpatrywana para strategii rozstrzyga konflikt na korzyść Delandii, zawsze istnieje strategia Alandii, która gwarantuje jej zwycięstwo. Jest tak, ponieważ na którymś z frontów Delandia musi przypisać mniej niż A dywizji (jako że $D < n \cdot A$), więc strategia Alandii, w której wszystkie dywizje będą przypisane do tej przełęczy, zmienia wynik konfliktu na korzystny dla Alandii. Analogicznie, dla każdej pary strategii, która zapewnia zwycięstwo Alandii, Delandia może przypisać swoje dywizje w sposób wyrównujący liczby dywizji przypisane przez Alandię do odpowiednich frontów (ponieważ $A \leqslant D$).

Strategie mieszane. Czy możemy coś zrobić, gdy nie istnieje równowaga Nasha w rozpatrywanym modelu? Tak! Zauważmy, że każdy z graczy, zamiast wybierać jedną ze swoich strategii, może zdecydować się na „wylosowanie” strategii według pewnego rozkładu prawdopodobieństwa. Takie rozkłady prawdopodobieństwa na zbiorze strategii gracza nazywamy *strategiami mieszanymi*. Jak należy je interpretować? Powiedzmy, że generał Acki wybierze strategię mieszaną, która przypisze równe prawdopodobieństwo każdej z paru wybranych strategii. Interpretacja jest następująca: generał Acki numeruje wybrane strategie, następnie wrzuca do urny ponumerowane kulki. Każda kulka odpowiada numerowi dokładnie jednej strategii. W momencie podjęcia decyzji Acki losuje kulkę z urny i wybiera przypisanie dywizji odpowiadające strategii, której numer znajdował się na wylosowanej kulce.

Warto zauważyć, że każda ze „zwykłych” strategii, czyli podziałów dywizji, odpowiada strategii mieszanej, która przypisuje temu podziałowi prawdopodobieństwo 1. Takie strategie mieszane nazywane są *strategiami czystymi*.

Rozszerzenie zbioru strategii wymaga również rozszerzenia funkcji wypłat obydwu graczy. W przypadku pary strategii mieszanych nie znamy wypłaty graczy, bo nie wiemy, jaka para strategii została wylosowana. Mówimy zatem o *oczekiwanej wypłacie* gracza – opisuje ona, jaka będzie „średnia” wypłata gracza z zadanej pary strategii przy wielokrotnym powtarzaniu rozgrywki. Oczekiwana wypłata jest obliczana przy założeniu, że rozkłady

prawdopodobieństwa zadane przez strategie mieszane obydwu graczy są niezależne – to, jaka strategia zostanie „wylosowana” przez jednego z graczy, nie zmienia prawdopodobieństwa „wylosowania” konkretnych strategii przez drugiego gracza. Aby obliczyć oczekiwaną wypłatę gracza, należy zsumować prawdopodobieństwo wystąpienia każdej pary strategii czystych pomnożonych przez wypłatę rozważanego gracza przy zadanej parze strategii.

Dla przykładu popatrzmy znów na uproszczoną macierz wypłat w rozpatrywanej wyżej grze. Załóżmy, że Acki wybierze pierwszą strategię $(2,0)$ z prawdopodobieństwem $1/3$ (więc drugą $(0,2)$ z prawdopodobieństwem $2/3$), a Decki wybierze pierwszą strategię $(2,1)$ z prawdopodobieństwem $3/4$ (i drugą $(1,2)$ z prawdopodobieństwem $1/4$). Oczekiwana wypłata Ackiego to zatem:

$$\left(\frac{1}{3}\cdot\frac{1}{4}+\frac{2}{3}\cdot\frac{3}{4}\right)-\left(\frac{1}{3}\cdot\frac{3}{4}+\frac{2}{3}\cdot\frac{1}{4}\right)=\frac{1}{6}.$$

Z rozszerzeniem zbiorów strategii obydwu graczy do strategi mieszanych pojęcie równowagi Nasha rozszerza się do *równowagi Nasha w strategiach mieszanych*. Taka równowaga to para strategii mieszanych, w której żaden z graczy nie może zwiększyć swojej oczekiwanej wypłaty, wybierając inną strategię, gdy strategia przeciwnika nie ulegnie zmianie. Chociaż poszukiwanie równowag Nasha w strategiach mieszanych jest znacznie bardziej wymagające niż w strategiach czystych, twierdzenie Nasha z 1951 roku gwarantuje, że w każdej grze skończonej (o skończonej liczbie graczy i ich strategii) taka równowaga istnieje!

W tej równowadze Decki z prawdopodobieństwem $\frac{1}{2}$ przydziela $A=2$ dywizje na każdą z przełęczy. Bardziej ogólnie, gdy $A \leqslant D < n \cdot A$, to gdyby istniała przełęcz, na której Decki zawsze przydziela mniej niż A dywizji, to Acki mógłby zagwarantować sobie wygraną, gdyby to on przydzielił tam A dywizji. Decki nie może do tego dopuścić, a zatem w każdej równowadze musi bronić każdej przełęczy co najmniej A dywizjami z dodatnim prawdopodobieństwem.

Wróćmy na chwilę do naszej przykładowej gry. Jak wygląda równowaga Nasha w strategiach mieszanych? Jest to para strategii mieszanych, w której każdy z graczy wybiera każdą ze swoich dwóch nieodrzuconych strategii z prawdopodobieństwem $\frac{1}{2}$. Jeżeli Decki częściej broni dwoma dywizjami którejś przełęczy, to Acki powinien zawsze atakować tę drugą, a wtedy Decki będzie wolał zmienić strategię. W równowadze Decki musi zatem wybierać obie strategie z takim samym prawdopodobieństwem. Analogiczna analiza dla Ackiego prowadzi do wniosku, że w równowadze również on musi wybierać każdą ze swoich strategii z prawdopodobieństwem $\frac{1}{2}$. Łatwo sprawdzić, że żadnemu z graczy nie opłaca się wówczas zmienić swojej strategii. Oczekiwana wypłata każdego z generałów jest równa 0, więc taka jest też wartość gry.

W powyższym przykładzie okazało się, że niektórych podziałów dywizji w ogóle nie opłaca się używać, co pozwoliło nam znacząco uprościć grę. Czy zawsze tak jest? Okazuje się, że nie. Pokażemy teraz, że w pewnych konfiguracjach, w jedynej równowadze Nasha w strategiach mieszanych każda ze strategii obydwu graczy jest grana z niezerowym prawdopodobieństwem.

Podstawowe narzędzia używane do rozwiązywania gier o sumie zerowej bazują na jednym z dwóch założeń – zbiór strategii obydwu graczy jest niewielki (wielomianowy względem parametrów gry) lub istnieją równowagi Nasha w strategiach mieszanych, gdzie strategie mieszane obydwu graczy mają niewielkie (wielomianowe względem parametrów modelu) *nośniki*. Nośnik strategii mieszanej to zbiór wszystkich strategii czystych gracza, które są grane z dodatnim prawdopodobieństwem przy danej strategii mieszanej. W związku z tym, że zbiór strategii każdego z graczy jest duży (wykładniczy) względem parametrów modelu oraz istnieją równowagi, w których wszystkie strategie znajdują się w nośniku, badana przez nas gra jest trudna do rozwiązania w czasie wielomianowym.

Równe liczby dywizji. Załóżmy, że każde z państw dysponuje taką samą liczbą dywizji opisaną przez liczbę naturalną k ($k = A = D$). Ponieważ obaj gracze dysponują taką samą liczbą dywizji, ich zbiory strategii są równe. Co więcej, jeżeli obydwaj generałowie wybiorą ten sam podział dywizji pomiędzy fronty, Delandia wygra wojnę, zatrzymując przeciwnika na każdym froncie. W każdym innym przypadku (gdy gracze wybiorą różne strategie), na pewnym froncie Alandia będzie dysponowała większą od Delandii liczbą dywizji, co doprowadzi do wygranej Alandii na tym froncie i w konsekwencji w całej wojnie.

Ustalmy parę strategii mieszanych, w której każdy z graczy przypisuje takie samo prawdopodobieństwo p każdej z dostępnych strategii czystych. Czy ta para strategii mieszanych opisuje równowagę Nasha? Żeby odpowiedzieć na to pytanie, musimy zastanowić się, czy któryś z graczy może zwiększyć swoją oczekiwaną wypłatę przez zmianę swojej strategii mieszanej. Rozważmy zmianę strategii mieszanej przez generała Ackiego. Każda strategia czysta gwarantuje wygraną Alandii z takim samym prawdopodobieństwem, równym $1-p$ (z takim prawdopodobieństwem Decki wylosuje strategię odpowiadającą innemu przypisaniu dywizji pomiędzy fronty niż strategia czysta wybrana przez Ackiego). W związku z tym każda strategia mieszana wybrana przez Ackiego zagwarantuje wygraną Alandii z takim samym prawdopodobieństwem, równym $1-p$. Oznacza to, że Acki nie może zwiększyć prawdopodobieństwa wygranej Alandii, a zatem i oczekiwanej wypłaty, przez zmianę swojej strategii mieszanej. Analogiczny argument pokazuje, że to samo dotyczy Deckiego, zatem rozważana para strategii opisuje równowagę Nasha! Oczekiwana wypłata Ackiego przy tych strategiach jest równa $1-2p$, taka jest zatem wartość gry. Oznacza to, że przy takiej samej liczbie dywizji generał Acki jest w nieporównanie lepszej sytuacji.

Jako ćwiczenie dla Wnikliwego Czytelnika pozostawiam poszukanie odpowiedzi na pytanie, dlaczego żadna inna para strategii mieszanych nie jest równowagą Nasha, gdy obaj gracze dysponują taką samą liczbą dywizji.

Czego dowiedzieliśmy się o rozważanej grze? Po pierwsze, przy odpowiedniej dysproporcji liczby dywizji, którymi dysponują gracze, istnieją równowagi Nasha w strategiach czystych, w których jeden z graczy ma zagwarantowaną wygraną. Po drugie, w sytuacji, gdy $A \leqslant D < A \cdot n$, nie istnieją równowagi Nasha w strategiach czystych, a żaden z graczy nie jest w stanie zagwarantować swojej wygranej z prawdopodobieństwem 1. W takich scenariuszach dla każdej przełęczy obrońca powinien z dodatnim prawdopodobieństwem przypisywać A dywizji, aby atakujący nie miał w odpowiedzi strategii, przy której na pewno wygra. Okazuje się zatem, że w każdej sytuacji, gdy atakujący nie może zagwarantować swojej wygranej, obrońcy opłaca się bronić na wszystkich frontach równocześnie.

Pseudopierwsze zoo

*Mikołaj ROTKIEWICZ**

* Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

O liczbach pseudopierwszych pisaliśmy w Δ^3_{22}. Przypomnijmy, że liczba pseudopierwsza (Fermata, przy podstawie a) to liczba złożona n, która „udaje" liczbę pierwszą w tym sensie, że spełnia podzielność $n|a^n - a$. O takim kamuflażu można mówić na wiele różnych sposobów.

Weźmy na warsztat (w miejsce ciągu geometrycznego (a^n)) ciąg $V_n = \alpha^n + \beta^n$, gdzie α, β są pierwiastkami, być może zespolonymi, trójmianu kwadratowego $f(X) = X^2 - aX + b$, natomiast a, b są liczbami całkowitymi. Początkowe wyrazy tego ciągu można szybko obliczyć, stosując rekurencję: $V_0 = 2$, $V_1 = a$, $V_{n+1} = aV_n - bV_{n-1}$ dla $n \geqslant 1$. Stąd widać również, że (V_n) jest ciągiem liczb całkowitych. Małe twierdzenie Fermata ma następujące uogólnienie:

Przedstawiony wzór rekurencyjny dla ciągu (V_n) wynika ze zsumowania następujących dwóch równości, prawdziwych na mocy definicji liczb α, β;
$$\alpha^{n+2} = a\alpha^{n+1} - b\alpha^n,$$
$$\beta^{n+2} = a\beta^{n+1} - b\beta^n.$$

Lemat 1. *Jeśli p jest liczbą pierwszą, to $V_p \equiv V_1 \pmod p$.*

Dowód. Niech $p > 2$. Zastosujemy wzory na pierwiastki równania kwadratowego. Mamy $V_p = \left(\frac{a+\sqrt{\Delta}}{2}\right)^p + \left(\frac{a-\sqrt{\Delta}}{2}\right)^p$, gdzie $\Delta = a^2 - 4b$. Po rozwinięciu część wyrazów sumy zredukuje się i otrzymamy

$$V_p = 2^{-p+1}\left(a^p + \sum_{j=1}^{(p-1)/2} \binom{p}{2j} a^{p-2j}\Delta^j\right).$$

W powyższej sumie $a^p \equiv a \pmod p$, a pozostałe składniki sumy są całkowite i podzielne przez p, gdyż $p \mid \binom{p}{2j}$. Ponadto $2^{p-1} \equiv 1 \pmod p$ i dlatego

$$V_p \equiv 2^{p-1}V_p \equiv a + 0 = V_1 \pmod p.$$

Przypadek $p = 2$ pozostawiamy Czytelnikowi. □

Lemat 1 prowadzi do pierwszego egzemplarza w naszym zoo. Liczbę złożoną n nazywa się *pseudopierwszą Dicksona*, jeśli

(D) $$V_n \equiv V_1 \pmod n$$

i $\mathrm{NWD}(n, 2b\Delta) = 1$. Warunek na NWD jest po to, by pominąć trywialne rozwiązania kongruencji (D). Okazuje się, że sprawdzenie warunku (D) można wykonać niemalże tak szybko jak sprawdzenie, czy $a^n \equiv a \pmod n$ (patrz ćwiczenie 1).

Obliczenia wartości $(a^n \mod n)$ można dokonać w czasie $O(\log n)$ – jak? Odpowiedź w dalszej części artykułu.

W poprzednim artykule wspominaliśmy o *liczbach Carmichaela*, które spełniają $a^n \equiv a \pmod n$ dla dowolnej liczby naturalnej a. Powstaje naturalne pytanie, czy istnieją liczby, które są liczbami pseudopierwszymi Dicksona dla dowolnych liczb całkowitych a, b? Odpowiedź jest twierdząca, najmniejszą z nich jest

$$n = 443372888629441 = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331.$$

W dalszej części artykułu przyjrzymy się własnościom ciągu (A_n), który zdefiniowany jest przez analogiczną rekurencję, lecz tym razem jest ona rzędu 3:

(1) $$A_0 = 3, \quad A_1 = 0, \quad A_2 = 2, \quad A_{n+1} = A_{n-1} + A_{n-2} \text{ dla } n \geqslant 2.$$