

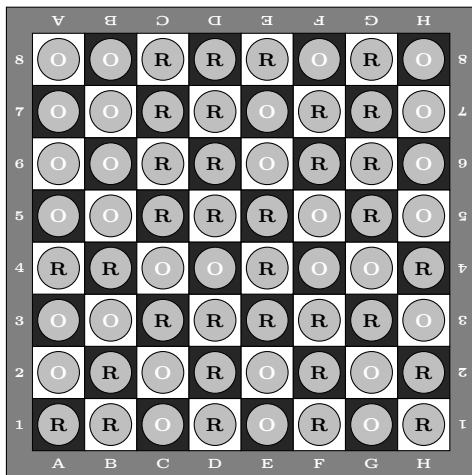
(Nie)możliwa do rozwiązania zagadka

Izabela MANDLA*

* Studentka, Wydział Matematyki i Informatyki, Uniwersytet Jagielloński

Wyobraźmy sobie taką sytuację: dwóch więźniów dostaje możliwość wydostania się na wolność pod warunkiem, że uda im się rozwiązać pewną zagadkę. (Chyba nie ma na świecie systemu penitencjarnego, który dopuszczałby taką ewentualność, ale nie psujmy opowieści roztrząsaniem takich szczegółów!). Strażnik, który ich pilnuje, przygotował dla nich problem logiczny, który na pierwszy rzut oka mógłby się wydawać niemożliwy do rozwiązania. A oto, co im powiedział:

W celi obok na stole leży zwykła szachownica 8 na 8. Jednak na jej polach nie leżą pionki, a monety. Na każdym polu leży dokładnie jedna moneta i może ona być odwrócona do góry orłem lub reszką. Za godzinę przyjdę po ciebie – tu wskazał na więźnia o imieniu Bob – zaprowadzę do tej celi i wskażę ci pewne pole na szachownicy. Następnie będziesz musiał odwrócić dokładnie jedną monetę. Potem do celi przyprowadzę Eda – tu pokazał na drugiego więźnia – i jego zadaniem będzie odgadnąć, które pole wskazałem. Jeśli mu się to uda, obaj wychodzicie na wolność.



Oto, co mógł zobaczyć Ed. Czy Bob mógł mu w ten sposób przekazać informację o polu wskazanym przez strażnika?

Czy jest możliwe, aby więźniowie mieli pewność wyjścia na wolność? Na pierwszy rzut oka wydaje się, że nie. Oczywiście nie bierzemy pod uwagę sytuacji, że pierwszy więzień powiedział drugiemu półgębkiem czy też pokazał na migi, które pole wskazał strażnik. Niezależnie od powodów, dla których wyładowali za kratkami, na pewno nie dopuściliby się zbrodni zepsucia dobrej zagadki, nawet gdy stawką jest ich wolność! Zostaje tylko plansza i to, co na niej leży. Dobrze, ale czy da się to wykorzystać? Czy jest jakaś strategia, na którą mogą umówić się więźniowie, przy której dzięki odwróceniu jednej monety da się przekazać informację o polu wskazanym przez strażnika?

O dziwo, odpowiedź jest twierdząca! Jest to wspaniała zagadka, która zdecydowanie zasługuje na odrobinę samodzielnego zastanowienia, aby należycie docenić jej trudność. Dlatego – by nie zepsuć zabawy Czytelnikowi Ambitnemu, który sam zechciałby się z nią zmierzyć – rozwiązanie przedstawione jest dopiero na stronie 18 tego wydania *Delty*.

Przekątna kwadratu nie jest współmierna z jego bokiem

* Wydział Matematyki i Fizyki Stosowanej, Politechnika Rzeszowska

Jarosław GÓRNICKI*



Ekspонат YBC 7298, Yale Babylonian Collection (New Haven). Więcej informacji o tabliczce można znaleźć tu: <https://news.yale.edu/2016/04/11/3800-year-journey-classroom-classroom>

W starożytnej Mezopotamii – kraju położonym między Eufratem a Tygrysem – około 4000 lat temu posługiwano się sześćdziesiątkowym systemem pozycyjnym. Oznacza to, że w charakterze cyfr używano liczb od 0 do 59 zamiast od 0 do 9 („podręczna” tabliczka mnożenia w tym systemie zawiera 1830 iloczynów, od 1×1 do 60×60). Przyjmowano wówczas, że długość przekątnej kwadratu jednostkowego jest równa

$$L = (1; 24\ 51\ 10)_{60} = 1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3} = 1,414213962962 \dots$$

To świetny wynik, bo liczba $[(1; 24\ 51\ 10)_{60}]^2 = (1; 59\ 59\ 59\ 38\ 1\ 40)_{60} \approx 1,999998$ jest bardzo bliska 2. Długość przekątnej kwadratu o boku a wyznaczano ze wzoru $L \cdot a$.

Dowodem na to, że starożytni mieszkańcy Mezopotamii posiadali taką wiedzę, jest babilońska gliniana tabliczka (około 1700 roku p.n.e.).

Rozwiązanie (nie)możliwej do rozwiązania zagadki ze strony 1

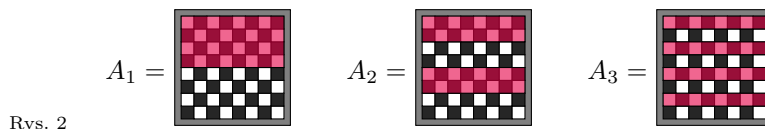
Na stronie 1 przeczytaliśmy już, że więźniowie wiedzieli wcześniej, na czym będzie polegać zadanie, i mogli się naradzić nad strategią. Jednak nie znali oni ułożenia monet na planszy. Co więcej, całej rozmowie mógł się przysłuchiwać strażnik i potem tak podwracać monety, żeby nieudolnie wybrany plan nie zadziałał. W takim przypadku nie ma miejsca na błąd. Strategia musi pozwolić pierwszemu więźniowi na wskazanie dowolnego pola na planszy.

Ponumerujemy pola planszy, zaczynając od zera. Nie róbmy tego jednak w systemie dziesiętnym, tylko binarnym. Tak więc pole A1 będzie miało numer 000000, pole A2 numer 000001 i tak dalej, aż do pola H8 o numerze 111111 (rys. 1).

	V	Б	С	Д	Е	Ж	З	И	
8	111 000	111 001	111 010	111 011	111 100	111 101	111 110	111 111	8
7	110 000	110 001	110 010	110 011	110 100	110 101	110 110	110 111	7
6	101 000	101 001	101 010	101 011	101 100	101 101	101 110	101 111	6
5	100 000	100 001	100 010	100 011	100 100	100 101	100 110	100 111	5
4	011 000	011 001	011 010	011 011	011 100	011 101	011 110	011 111	4
3	010 000	010 001	010 010	010 011	010 100	010 101	010 110	010 111	3
2	001 000	001 001	001 010	001 011	001 100	001 101	001 110	001 111	2
1	000 000	000 001	000 010	000 011	000 100	000 101	000 110	000 111	1
	A	B	C	D	E	F	G	H	

Rys. 1

Zdefiniujemy na szachownicy sześć obszarów – obszar A_i tworzą pola, których numery mają jedynkę na i -tym miejscu (rys. 2). Poniżej schematyczne przedstawienie pierwszych trzech z nich (kolejne trzy wyglądają podobnie, tylko zaznaczone są kolumny, nie wiersze).



Przyjmijmy ponadto, że każde ustawienie monet na szachownicy koduje pewne pole w następujący sposób: na i -tym miejscu numeru tego pola ma znajdować się reszta z dzielenia przez 2 liczby reszek w obszarze A_i . W przykładzie na rysunku 3 w kolejnych obszarach A_i znajduje się odpowiednio 16, 17, 16, 17, 20 i 18 reszek, więc koduje on pole o numerze 010100, czyli E3.

Mamy zatem jakiś pomysł na system kodowania, ale czy faktycznie pozwala on na rozwiązanie zagadki? Okazuje się, że tak. Zdefiniowaliśmy obszary A_i w taki sposób, że pole o numerze $w = \overline{w_1w_2w_3w_4w_5w_6}$ (po prawej stronie równości znajduje się sześciobitowy zapis dwójkowy) należy wyłącznie do tych obszarów A_i , dla których $w_i = 1$. Odwrócenie monety na polu w powoduje zatem zmianę parzystości liczby reszek w tych właśnie obszarach (i tylko w nich). Oznacza to, że jeśli początkowe ustawienie monet przez strażnika koduje pole o numerze $x = \overline{x_1x_2x_3x_4x_5x_6}$, to nowe ustawienie (po odwróceniu monety) koduje pole o numerze, w którym zamienione zostały cyfry (bity) z x na pozycjach i takich, że $w_i = 1$. Informatycy powiedzieliby, że jest to XOR liczb x i w , oznaczany często jako $x \oplus w$.

	V	Б	С	Д	Е	Ж	З	И	
8	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	8
7	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	7
6	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	6
5	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	○ ○ R R R ○ R ○	5
4	R R ○ ○ R ○ ○ R	R R ○ ○ R ○ ○ R	R R ○ ○ R ○ ○ R	R R ○ ○ R ○ ○ R	R R ○ ○ R ○ ○ R	R R ○ ○ R ○ ○ R	R R ○ ○ R ○ ○ R	R R ○ ○ R ○ ○ R	4
3	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	3
2	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	○ R ○ R ○ R ○ R	2
1	R R ○ R ○ R ○ R	R R ○ R ○ R ○ R	R R ○ R ○ R ○ R	R R ○ R ○ R ○ R	R R ○ R ○ R ○ R	R R ○ R ○ R ○ R	R R ○ R ○ R ○ R	R R ○ R ○ R ○ R	1
	A	B	C	D	E	F	G	H	

Rys. 3

O pożytkach z operacji XOR w kontekście zagadek logicznych pisał również Tomasz Janiszewski w artykule *Samotne zwierze na Arce Noego z Δ_{21}^9* . W tym zaś numerze *Delta* Bartosz Klin opisuje, jak XOR przydaje się w szyfrowaniu.

Pierwszy więzień ma niejako do rozwiązania problem odwrotny: strażnik wskazuje mu pewne pole o numerze $y = \overline{y_1y_2y_3y_4y_5y_6}$ i więzień ma znaleźć takie z , dla którego $x \oplus z = y$. Wystarczy jednak, że wybierze pole, które zmienia wszystkie cyfry x różne od odpowiadających im cyfr y . Jest to zatem pole $z = \overline{z_1z_2z_3z_4z_5z_6}$ takie, że $z_i = 1$ dokładnie wtedy, gdy $y_i \neq x_i$. To swoją drogą również można zgrabnie wyrazić przy użyciu operacji XOR, $z = x \oplus y$.

Jeśli kogoś odstrasza formalizm powyższego opisu, proponuję analizę następującego przykładu. Rozważmy takie ułożenie monet jak na rysunku 3. Załóżmy, że strażnik wskazał na pole H4 o numerze 011111.

Sprawdzamy, co się dzieje na obszarze odpowiedzialnym za pierwszą pozycję. Liczba orłów jest parzysta. Liczba, którą chcemy zakomunikować drugiemu więźniowi, ma na tej pozycji 0, czyli liczbę parzystą, więc nie chcemy tego zmieniać. Teraz kolej na drugą pozycję. Tutaj też się zgadza – nieparzysta liczba orłów oraz cyfra 1 w naszej liczbie. Co z trzecią? O! Tutaj się nie zgadza! Co to oznacza? Monetę, którą będziemy odwracać, trzeba wybrać spośród tych z obszaru odpowiedzialnego za tę pozycję. Jednak zauważmy, że jednocześnie nie możemy przy tym nic zmienić w strefach przypisanych pierwszej i drugiej pozycji. W takim razie jasno wskazuje to, że musimy zmienić coś w drugim wierszu.



	V	B	C	D	E	F	G	H	
8	111 000	111 001	111 010	111 011	111 100	111 101	111 110	111 111	8
7	110 000	110 001	110 010	110 011	110 100	110 101	110 110	110 111	7
6	101 000	101 001	101 010	101 011	101 100	101 101	101 110	101 111	6
5	100 000	100 001	100 010	100 011	100 100	100 101	100 110	100 111	5
4	011 000	011 001	011 010	011 011	011 100	011 101	011 110	011 111	4
3	010 000	010 001	010 010	010 011	010 100	010 101	010 110	010 111	3
2	001 000	001 001	001 010	001 011	001 100	001 101	001 110	001 111	2
1	000 000	000 001	000 010	000 011	000 100	000 101	000 110	000 111	1
	A	B	C	D	E	F	G	H	

Rys. 4

Artykuł powstał na podstawie filmiku *The almost impossible chessboard puzzle* na kanale Stand-up Maths oraz filmiku *How to send a self-correcting message (Hamming codes)* na kanale 3Blue1Brown. Oba są dostępne w serwisie youtube.com.

Komentarz na deser. Wyobraźmy sobie, że strażnik w przypływie pozorowanej dobroci oznajmił więźniom, że zamiast szachownicy 8×8 przygotował dla nich szachownicę 7×7 . Wszak mniej pól do odgadnięcia powinno ułatwić problem! Nie jest to jednak prawda – okazuje się, że aby więźniowie mieli pewność wyjścia na wolność, liczba pól na szachownicy musi być potęgą dwójki! Uzasadnienie nie jest bardzo skomplikowane i chyba najprościej prześledzić je na przykładzie trzech pól (choć wtedy ciężko ułożyć je w szachownicę...).

Jeśli mamy do dyspozycji 3 pola, to możliwych ustawień monet jest $2^3 = 8$. Możemy przyjąć, że ustawienia te odpowiadają współrzędnym punktów w trójwymiarze (np. orzeł koduje 0, a reszka 1, wtedy ustawienie ORR odpowiada punktowi $(0, 1, 1)$). Wszystkie ustawienia układają się zatem w wierzchołki sześcianu jednostkowego.

Początkowe ustawienie monet przez strażnika odpowiada wyborowi jednego wierzchołka sześcianu, odwrócenie zaś jednej monety przez więźnia to przejście do jednego z sąsiadów wspomnianego wierzchołka. Na przykład, jeśli strażnik wybrał wierzchołek $(0, 1, 0)$, to więzień może uzyskać ustawienia odpowiadające wierzchołkom $(1, 1, 0)$, $(0, 0, 0)$ i $(0, 1, 1)$ – wszystkie są sąsiadami $(0, 1, 0)$ w sześcianie.

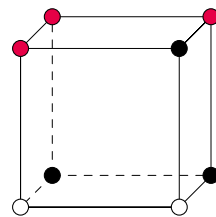
Każde ustawienie musi być możliwe do zinterpretowania przez drugiego więźnia jako jedno z trzech pól (tylko w taki sposób pierwszy więzień może drugiemu przekazać informację). Innymi słowy, jeśli pola mają

Teraz to samo rozumowanie będziemy przeprowadzać na ostatnich trzech pozycjach, czyli będziemy patrzyli na kolumny planszy. I tak na czwartej pozycji widzimy, że się zgadza, natomiast na piątej i szóstej nie. Stąd szukamy wiersza, który jest częścią obszaru związanego z pozycją 5 i 6, ale nie z pozycją 4. Widzimy, że jest to czwarta kolumna. W takim razie pierwszy więzień powinien odwrócić monetę na polu D2 (rys. 4). Korzystając z wcześniejszych rozważań, moglibyśmy dojść do tego inaczej: obliczając $010100 \oplus 011111 = 001011$ – ciąg po prawej stronie koduje właśnie pole D2.

Skomentujmy jeszcze sytuację, gdy numer wskazywany przez szachownicę zgadza się z numerem pola wskazanego przez strażnika. Może to budzić pewien niepokój, przecież więzień *musi* odwrócić jakąś monetę. Którą więc powinien wybrać, gdy wszystko jest w porządku? Zauważmy, że jeśli rozważylibyśmy wszystkie z naszych obszarów na raz, to żaden z nich nie zawiera pola numer 000000. Stąd w takim wypadku wystarczy, że odwrócimy monetę właśnie na tym polu, bo ona jako jedyna nie wpływa na wiadomość, którą możemy odczytać z planszy.

Jeśli się zastanawiasz, Czytelniku, czy metoda zastosowana w tej zagadce może się przydać gdziekolwiek indziej, to odpowiedź brzmi: tak, jeszcze jak! Być może pamiętasz, jak kiedyś zwracano uwagę na to, żeby płyty CD lub DVD trzymać za brzegi, bo inaczej mogą się zniszczyć? Mimo że nie zawsze tego przestrzegano, one nadal działały, nawet lekko porysowane. Jest to zasługa kodów korygujących, dzięki którym lekko uszkodzoną wiadomość adresat wciąż jest w stanie odczytać bez błędów. Jednym z pierwszych tego typu kodów był kod Hamminga, który korzystał z technik bardzo podobnych do przedstawionego rozwiązania zagadki. Jego algorytm można uprościć właśnie do sprawdzania parzystości w wyznaczonych obszarach wiadomości. Ma to zapewnić znalezienie błędów, jeśli oczywiście jakiegokolwiek wystąpią. Kod Hamminga działał jednak tylko wtedy, gdy błędów nie pojawiło się zbyt wiele. Metoda ta była dopracowywana, a cała dziedzina pręźnie się rozwijała na przełomie wieków, ale to jest zupełnie inna historia.

kolory (powiedzmy, biały, czarny i ciemnoróżowy), to więźniowie muszą ustalić pewne kolorowanie wierzchołków sześcianu na te trzy kolory. Będą oni mieli pewność zwycięstwa tylko wtedy, gdy sąsiedzi dowolnego wierzchołka będą reprezentowali wszystkie możliwe kolory.



Rys. 5. Lewy dolny wierzchołek ma sąsiadów we wszystkich kolorach, ale prawy dolny już nie

Ponieważ zarówno sąsiadów, jak i kolorów, jest po 3, oznacza to, że każdy wierzchołek musi mieć dokładnie jednego sąsiada każdego z kolorów. Z tego ostatniego stwierdzenia wynika, że każdemu czarnemu wierzchołkowi odpowiada dokładnie jedna czarno-biała krawędź. Z kolei każdemu białemu wierzchołkowi odpowiada... cóż, też dokładnie jedna czarno-biała krawędź. Wynika stąd, że białych i czarnych wierzchołków musi być tyle samo! A że żaden z tych kolorów nie był szczególnie wyróżniony, tyleż samo musi być również wierzchołków ciemnoróżowych. Oznacza to, że liczba wszystkich wierzchołków (8) jest podzielna przez liczbę kolorów (3), a to jest sprzeczność. Proste uogólnienie tego rozumowania dowodzi, że aby zagadka miała rozwiązanie, liczba pól (n) musi być dzielnikiem liczby wszystkich ustawień monet (2^n), co oznacza, że n musi być potęgą dwójki.