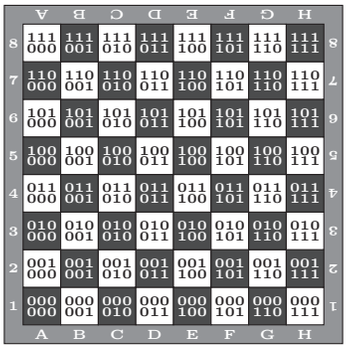
Rozwiązanie (nie)możliwej do rozwiązania zagadki ze strony 1

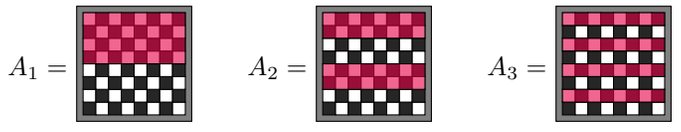
Na stronie 1 przeczytaliśmy już, że więźniowie wiedzieli wcześniej, na czym będzie polegać zadanie, i mogli się naradzić nad strategią. Jednak nie znali oni ułożenia monet na planszy. Co więcej, całej rozmowie mógł się przysłuchiwać strażnik i potem tak poodwracać monety, żeby nieudolnie wybrany plan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

Ponumerujmy 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).



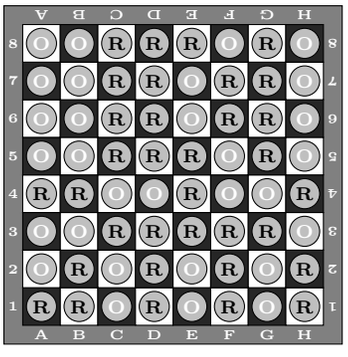
Rys. 1

Zdefiniujmy 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).



Rys. 2

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.



Rys. 3

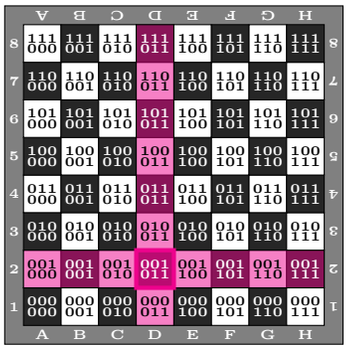
Mamy zatem jakiś pomysł na system kodowania, ale czy faktycznie pozwala on na rozwiązanie zagadki? Okazuje się, że tak. Zdefiniowaliśmy obszary A_i w taki sposób, że pole o numerze $w = \overline{w_1w_2w_3w_4w_5w_6}$ (po prawej stronie równości znajduje się sześciobitowy zapis dwójkowy) należy wyłącznie 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 $x \oplus w$.

O pożytkach z operacji XOR w kontekście zagadek logicznych pisał również Tomasz Janiszewski w artykule *Samotne zwierzę na Arce Noego* z Δ^9_{21}. W tym zaś numerze *Delty* 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.



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.

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.

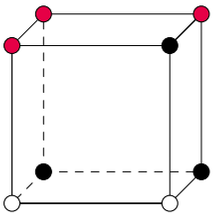
Jeśli się zastanawiasz, Czytelniku, czy metoda zastosowana w tej zagadce może się przydać gdziekolwiek indziej, to odpowiedź brzmi: tak, jeszcze jak! Być może pamiętasz, jak kiedyś zwracano uwagę na to, żeby płyty CD lub DVD trzymać za brzegi, bo inaczej mogą się zniszczyć? Mimo że nie zawsze tego przestrzegano, one nadal działały, nawet lekko porysowane. Jest to zasługa kodów korygujących, dzięki którym lekko uszkodzoną wiadomość adresat wciąż jest w stanie odczytać bez błędu. 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 jakiekolwiek wystąpią. Kod Hamminga działał jednak tylko wtedy, gdy błędów nie pojawiło się zbyt wiele. Metoda ta była dopracowywana, a cała dziedzina prężnie się rozwijała na przełomie wieków, ale to jest zupełnie inna historia.

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 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.