



Królowa Śnieżka wezwała siedmiu krasnoludków i oświadczyła, że w związku z wielkim świętem w najbliższą niedzielę postanowiła nagrodzić ich pracowitość.

– Przygotowałam dla was białe i kolorowe czapeczki. Nie powiem wam ani ile białych, ani ile kolorowych czapeczek przygotowałam. Każdemu z was nałożę jedną z czapeczek na głowę, ale by było bardziej uroczyście, przedtem zgaszę światło. Po zapaleniu światła, zobaczycie czapeczki u swoich kolegów, ale swojej nie będziecie mogli zobaczyć. Każdy z was dostanie 2 kartki ze swoim imieniem i napisem: **Mam białą czapeczkę** albo **Mam kolorową czapeczkę**. Jeśli któryś z was zechce, powinien wybrać jedną z nich i wrzucić do koszyka na środku sali. Ale pamiętajcie! Nie wolno wam się porozumiewać! Wspaniała nagroda – tu Królowa uśmiechnęła się tajemniczo – będzie wam wręczona, jeśli okaże się, że nikt się nie pomylił, a przynajmniej jedna osoba zgadła, jaką ma czapeczkę na głowie.

Krasnoludki udały się na naradę. Gapcio zauważył, że jeśli nie będzie można się porozumiewać, to nikt nie zgadnie koloru swojej czapeczki, bo królowa była bardzo złośliwa.

– Tak – potwierdził Gburek – nawet gdyby wszyscy dookoła mnie mieli takie same czapeczki, to i tak nie będę wiedział, co mam na głowie.

Nieśmiałek zauważył skromnie, że przecież nawet gdy nie możemy mieć pewności, to może chociaż zwiększymy szansę na wygraną. Wesołek wtedy zaproponował:

– Nieśmiałek wrzuci kartkę **Mam białą czapeczkę** do koszyka, a reszta niech nic nie wrzuca.

– Dobry pomysł – pochwalił Mędrak – przynajmniej mamy szansę pół na pół na zdobycie nagrody. Ale mamy jeszcze trochę czasu, może uda nam się powiększyć szansę?

Następnego dnia do Mędrka przyszedli Śpioszek, Apsik i Gapcio. Powiedzieli, że mają bardzo dobry pomysł. Podstawowa zasada ich działania miała być taka, że tylko jeden z nich będzie mógł wrzucić kartkę, a reszta krasnoludków musi wstrzymać się od wrzucania. Apsik wytłumaczył Mędrkowi na przykładzie, co miał na myśli.

– Patrząc na czapeczki Śpioszka i Gapcia i jeśli są tego samego koloru, to wrzucam kartkę z innym kolorem. Tu, na przykład (rys. 1), wrzuciłbym kartkę **Mam kolorową czapeczkę**. Gdy moi dwaj koledzy będą mieli różne czapeczki (rys. 2), zrezygnuję z wrzucania kartki. Tak samo postąpią moi koledzy.

Tutaj Mędrak musiał mocno wyteńczyć się i narysował wszystkie możliwe sytuacje z trzema czapeczkami, gdy metoda, wymyślona przez kolegów jest skuteczna (rys. 3) i wszystkie sytuacje, kiedy skuteczna nie jest (rys. 4).

– No tak – ucieszył się Śpioszek – na osiem możliwych sytuacji aż w sześciu udaje nam się zgadnąć! Szansa wygranej jest teraz $3/4$. To o wiele lepiej, niż gdybyśmy posłuchali Wesołka.

Gdy koledzy wyszli, Mędrak zasepił się. Teraz on musi pokazać, że nie na próżno nazywają go Mędrkiem. Wyjął kartkę i narysował.



Rys. 5

– Co powinienem zrobić, gdybym stał na przedostatnim miejscu?

Nie tylko Mędrak miał trudności z ulepszeniem pomysłu trzech krasnali.

Zagadka o czapeczkach stała się popularna wśród matematyków w roku 1998.

Autorem jej jest Amerykanin, Todd Ebert, który postawił ten problem w swojej

Rys. 1



Rys. 2



Rys. 3



Rys. 4





pracy doktorskiej, jako **zagadkę siedmiu więźniów**. Była ona tematem dyskusji przede wszystkim w środowisku informatyków, aż dotarła w czasie konferencji w Nowym Orleanie do profesora Elwyna Berlekampa, profesora matematyki na Uniwersytecie Kalifornijskim w Berkeley. Berlekamp od razu zauważył rozwiązanie dla trzech czapeczek, rozwiązanie dla siedmiu objawiło mu się zaraz po przebudzeniu następnego dnia rano. Rozwiązanie, które podał, było tak sensacyjne, że trafiło nawet na czołówki gazet. Oto tytuł artykułu z *The New York Times* z 10 kwietnia 2001.

The New York Times

Why Mathematicians Now Care About Their Hat Color

By SARA ROBINSON

Pomysł rozwiązania zagadki podany przez Berlekampa opierał się na tym, by każdemu układowi czapeczek przypisać pewien ciąg zer i jedynek, a następnie skorzystać z teorii kodowania, która takimi zero-jedynkowymi „słowami” zajmuje się od dawna. Jeśli mamy bowiem do czynienia z zadaniem zwiększenia prawdopodobieństwa, łatwiej zapewne operować na liczbach niż na kolorach. Żeby jednak zrozumieć, na czym w istocie polegało rozwiązanie Berlekampa, musimy głębiej wniknąć w teorię kodów.

Kody

Z kodami spotykamy się na co dzieńⁱ. Pismo jest kodem, pozwalającym utrwalić dźwięki lub nawet, jak w przypadku pisma chińskiego, całe pojęcia. Na opakowaniach spotykamy kod kreskowy, wreszcie w komputerach – kod dwójkowy, gdzie informacje zapisywane są jako układy zer i jedynek. Układ czapeczek można zapisać w postaci dwójkowej, jeśli umówimy się, że białe czapeczki będą kodowane jako „1”, a kolorowe jako „0”. Na przykład, układ

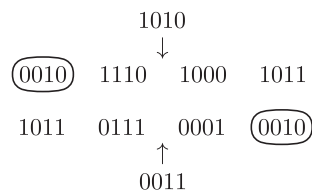


Rys. 6

można zakodować jako 0111000.

Współczesne kody służą nie tylko do zapisywania informacji. Mają wbudowaną funkcję samoobronną – sygnalizują, że w słowie kodowym pojawił się błąd, czasami wskazują, gdzie ten błąd się pojawił, a nawet, bez naszej wiedzy, ten błąd poprawiają. Dla kodów dwójkowych wskazanie miejsca jest równoważne możliwości korekty błędu. Bez możliwości wykrycia lub korekty błędów nasz komputer co chwilę odmawiałby posłuszeństwa, a płyty kompaktowe prawie nigdy nie mogłyby być odczytane.

Kodem K nazywać będziemy zbiór słów kodowych, czyli ciągów o ustalonej długości n . Poniżej ograniczymy się do kodów dwójkowych, czyli takich, w których występują tylko zera i jedynki. Pojawienie się błędu w słowie kodowym polega w tym przypadku na zamianie znaku „0” na „1” lub „1” na „0”. Na przykład, popełniając jeden błąd w słowie 1010, otrzymamy jedno z czterech słów: 0010, 1110, 1000, 1011. Zauważmy, że słowo 0010 możemy otrzymać również, popełniając jeden błąd w słowie 0011 (rys. 7). A zatem w kodzie, w którym występują słowa 1010 i 0011, nie można wykryć pojedynczego błędu, gdyż słowo 0010 może pochodzić zarówno od słowa 1010, jak i od słowa 0011.



Rys. 7

$$\begin{array}{r} 1110010 \\ \oplus \\ 1010110 \\ \hline 0100100 \end{array}$$

Rys. 8

Liczbę błędów w słowie k , gdy odczytamy je jako słowo l , można łatwo określić, odpowiednio „dodając” słowa k oraz l . Na przykład weźmy $k = 1110010$ oraz $l = 1010110$, gdzie l jest błędnie zapisanym słowem k . Widzimy, że błędy wystąpiły na pozycji 2 i 5. W l popełniono więc 2 błędy. Błędy w słowie l są na pozycjach, w których występują cyfry 1 w następującej sumie $k \oplus l$ słów k i l (rys. 8). Dodawanie cyfr jest zdefiniowane tu jako: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Liczbę błędów określa waga słowa $w(k \oplus l)$ równa liczbie

ⁱ Można przeczytać mój artykuł *Kody na co dzień* (*Delta* 9/2004).

ⁱⁱ Richard Wesley Hamming (1915–1988), amerykański matematyk, członek zespołu Manhattan Project, który skonstruował bombę atomową. Od 1946 roku pracował w laboratoriach Bella. Jest twórcą teorii kodów wykrywających i korygujących błędy. Był wybitnym specjalistą w teorii metod numerycznych, teorii informacji i statystycznej obróbki sygnałów. Jego prace wykonywane w 1956 na komputerze IBM 650 doprowadziły do powstania języków programowania wysokiego rzędu.

jedynek w słowie $k \oplus l$. Liczba $d(k, l) = w(k \oplus l)$ zwana jest **odległością Hamminga**ⁱⁱ słów k i l , gdyż spełnia wszystkie warunki, jakie odległość powinna spełniać:

$$\begin{aligned} d(k, l) &= 0 \quad \text{tylko wtedy, gdy } k = l, \\ d(k, l) &= d(l, k), \\ d(k, l) &\leq d(k, m) + d(m, l). \end{aligned}$$

Wszystkie słowa, które są w odległości d od danego słowa k , a więc leżące na sferze Hamminga o promieniu d i środku k , powstają z k przez popełnienie dokładnie d błędów. Na przykład rozważane wcześniej słowa 0010, 1110, 1000, 1011 leżą na sferze Hamminga o promieniu 1 i środku 1010. Z kolei słowa 1011, 0111, 0001 oraz 0010 leżą na sferze o promieniu 1 i środku w 0011. Obie te sfery stykają się w „punkcie” 1011.

Interesować się będziemy kodami liniowymi K , które charakteryzują się tym, że wraz ze słowami k i l , należącymi do K , ich suma $k \oplus l$ też należy do K .

Kodem liniowym jest, na przykład, zbiór słów $K_0 = \{01011, 10101, 11110, 00000\}$. Do kodu K_0 o 4 elementach należy słowo, składające się z samych cyfr „0”, nazywane słowem zerowym i oznaczone jako 0. Podobnie, dla dowolnego kodu liniowego

- $0 \in K$,
- K ma 2^j elementów.

Kody liniowe o słowach mających długość n i 2^j elementów oznacza się symbolem (n, j) .

Kod liniowy można scharakteryzować przez rozdzielczość d kodu, określoną jako minimalna odległość słów kodu od 0: $d = \min\{w(k) : k \in K, k \neq 0\}$. Rozdzielczość d w kodzie (n, j) spełnia nierówność: $d \leq n - j + 1$.

Rozdzielczość kodu świadczy o jego zdolności do wykrywania błędów. Zachodzi bowiem

Twierdzenie. Kod K lokalizuje s błędów wtedy i tylko wtedy, gdy $d > 2s$.

Wynik ten jest intuicyjnie oczywisty: jeżeli w słowie kodu popełniono s błędów, to w jego otoczeniu o promieniu $2s$ nie powinno być więcej niż jedno słowo kodu. A zatem odległość dowolnych dwóch słów kodu musi być większa niż $2s$.

Zbiór słów $K_0 = \{01011, 10101, 11110, 00000\}$ jest kodem $(5, 2)$ o rozdzielczości $d = 3$, więc można w nim wykryć jeden błąd, ale dwa i więcej już nie.

Porównując nierówności $d > 2s$ oraz $d \leq n - j + 1$, widzimy, że w kodzie (n, j) nie można wykryć $(n - j + 1)/2$ i więcej błędów. W dowolnym kodzie $(5, 2)$ można wykryć co najwyżej 1 błąd. Kodując 2^j symboli tak, aby móc wykryć s błędów, trzeba użyć słów liniowego kodu dwójkowego o długości większej niż $j + 2s - 1$. Tylko jak to zrobić?

Kody wykrywające jeden błąd

Zajmiemy się teraz liniowymi kodami dwójkowymi (n, j) , które wykrywają jeden błąd. Dla takich kodów zachodzi nierówność, udowodniona przez Hamminga: $2^j \leq \frac{2^n}{n+1}$.

Zainteresowani jesteśmy konstrukcją kodów jak najbardziej oszczędnych, to znaczy takich, że przy danym j ⁱⁱⁱ różnica między prawą i lewą stroną nierówności Hamminga jest jak najmniejsza.

Kodami optymalnymi (n, j) nazywamy takie, które spełniają równość $2^j = \frac{2^n}{n+1}$, a więc^{iv} $n = 2^p - 1$, $j = n - p$ dla naturalnego p . W kodach optymalnych słowa kodowe stanowią $1/(n+1)$, czyli $1/2^p$ wszystkich słów^v.

Kody optymalne zawsze istnieją i odgrywają ważną rolę w teorii kodowania. W takich kodach wszystkie ciągi, składające się z n zer i jedynek, są w odległości 1 od słów kodowych lub same są słowami kodowymi.

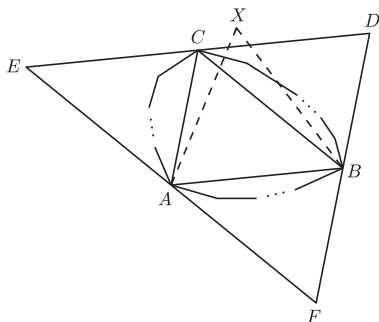
Optymalne są kody $(3, 1)$, $(7, 4)$, $(15, 11)$, $(31, 26)$. Słowa kodowe stanowią odpowiednio $1/4$, $1/8$, $1/16$, $1/32$ wszystkich ciągów o długości 3, 7, 15, 31.

3



Rozwiązanie zadania M 1104.

Niech ABC będzie trójkątem o największym polu spośród wszystkich trójkątów mających wierzchołki w wierzchołkach danego wielokąta. Przez punkty A, B, C prowadzimy proste równoległe odpowiednio do boków BC, CA, AB , uzyskując trójkąt DEF . Wówczas pole trójkąta DEF nie przekracza 4. Wykażemy, że trójkąt DEF zawiera dany wielokąt.



Przypuśćmy, że pewien wierzchołek X danego wielokąta leży poza trójkątem DEF oraz przyjmijmy bez straty ogólności, że punkt X leży po przeciwnej stronie prostej DE niż punkt F . Wówczas trójkąt XAB ma wierzchołki w wierzchołkach danego wielokąta i jego pole jest **większe** od pola trójkąta ABC . Uzyskaliśmy sprzeczność.

ⁱⁱⁱ j zależy od liczby symboli, które chcemy zakodować. Jeśli chcemy zakodować s symboli, to j musi spełniać nierówność $2^j \geq s$.

^{iv} Przekształcając równanie, otrzymamy $n + 1 = 2^{n-j}$.

^v Słów kodowych jest 2^j , wszystkich ciągów o długości n jest 2^n . Proporcja słów kodowych wśród wszystkich ciągów jest więc równa $2^j/2^n = 1/(n+1)$.

^{vi} Kod musi zawierać słowo zerowe i słowo odległe od niego o co najmniej 3 (warunek wykrycia jednego błędu), czyli słowo 111.



Rys. 9

Kod (3, 1) składa się ze słów {000, 111}^{vi}. Zauważmy, że gdy „1” koduje białe, a „0” kolorowe czapeczki, to kod ten jest zapisem dwóch układów (rys. 9), w których Śpioszek, Apsik i Gapcio popełniają błąd. Pozostałych 6 układów, spoza kodu (3, 1), jest przez nich bezbłędnie rozszyfrowanych.

To ten pomysł, który przyszedł do głowy Berlekampowi. Aby rozszyfrowywać układy 7 czapeczek, trzeba nauczyć się odróżniać układy niestanowiące słów kodu (7, 4), czyli układy różniące się od nich na jednym miejscu. Wtedy prawdopodobieństwo pomyłki będzie równe 1/8, a prawdopodobieństwo sukcesu 7/8.

Wykrywanie błędów w kodzie (7,4)

Wszystkie słowa zerojedynkowe o długości 7 dzielą się na dwie grupy:

- $2^4 = 16$ słów kodu (7, 4),
- $2^7 - 16 = 112$ słów spoza kodu (7, 4), które będą podstawą naszej strategii zgadywania.

Jak je rozróżnić?

Zdefiniujemy tablicę zerojedynkową, pełniącą rolę dekodera (rys. 10). Dekoder ma 3 kolumny i 7 wierszy, w kolejnych wierszach dekodera są liczby naturalne 1, 2, ..., 7, zapisane w systemie dwójkowym: w pierwszym wierszu liczba 001, w drugim 010, ..., w ostatnim 111.

Aby sprawdzić, czy słowo o długości 7 należy do kodu (czyli aby dekodować), wystarczy to słowo pomnożyć przez dekodera.

Wynik mnożenia słowa 0100101 to słowo o długości 3, otrzymane w sposób przedstawiony na rysunku 11.

Wynik tego mnożenia jest w kolejnym wierszu:

- słowem zerowym, gdy literą w dekodowanym słowie jest 0,
- słowem dekodera, gdy literą w dekodowanym słowie jest 1.

Otrzymane słowa dodaje się według wcześniej wprowadzonej reguły \oplus .

Pomnożmy przez dekodera słowo 0110101 powstałe z poprzedniego słowa przez zamianę znaku na trzecim miejscu od lewej (rys. 12). Pierwsze z tych słów należy do kodu (7,4), drugie – nie należy do kodu, a wynik dekodowania 011, będący liczbą 3, zapisaną w systemie dwójkowym, wskazuje na miejsce wystąpienia błędu. Prawdziwe jest ogólne

Twierdzenie. Słowa kodu (7, 4) pomnożone przez dekodera dają w wyniku słowo zerowe. Słowa nienależące do kodu (7, 4) pomnożone przez dekodera dają słowo, które odczytane jako liczba dwójkowa wskazuje na miejsce wystąpienia błędu.

Rozwiązanie zagadki

Zgodnie z umową, krasnoludek ma prawo wrzucić kartkę, jeśli układ czapeczek nie należy do kodu (7, 4), a błąd wystąpił w miejscu, w którym stoi ten krasnoludek. Wtedy tylko jeden krasnoludek wrzuci kartkę. Tak postępowywały krasnoludki, gdy decydowały trzy czapeczki. Krasnoludek stojący na piątym miejscu, widząc, co mają na głowach jego koledzy,



Rys. 13

wrzuci kartkę **Mam kolorową czapeczkę**, gdyż wynik dekodowania wynosi wtedy^{vii} 101, co jest numerem jego miejsca (rys. 14).

Układ, nad którym zastanawiał się Mędrek,



Rys. 15

001
010
011
100
101
110
111

Rys. 10

001	0	000
010	1	010
011	0	000
100	* 0	= 000
101	1	101
110	0	000
111	1	<u>111</u> \oplus
		= 000

Rys. 11

001	0	000
010	1	010
011	1	011
100	* 0	= 000
101	1	101
110	0	000
111	1	<u>111</u> \oplus
		= 011

Rys. 12

001	0	000
010	1	010
011	1	011
100	* 1	= 100
101	0	000
110	0	000
111	0	<u>000</u> \oplus
		= 101

Rys. 14

^{vii} Umowa: kolorowe czapeczki reprezentowane są przez 0, białe – przez 1.

nie upoważnia go do wrzucenia kartki. Gdyby bowiem miał na głowie kolorową czapkę, to wynikiem dekodowania byłoby słowo 101, co nie jest numerem miejsca, na którym on stoi. Gdyby miał na głowie czapkę białą, to wynikiem dekodowania byłoby słowo 011, co też nie jest jego miejscem. Kartkę wrzuci krasnoludek stojący na trzecim bądź na piątym miejscu, w zależności od tego, czy Mędek będzie miał czapkę białą czy kolorową. Biedny Mędek, znów nie będzie mógł się wykazać...

A co będzie, jeśli Śnieżka wymyśli więcej rodzajów czapek? Co ma zrobić teraz Mędek, gdy królewna przygotowała białe, kolorowe i pasiaste czapki, a jego koledzy zostali ubrani w następujący sposób.



Rys. 16

Można udowodnić, i nie jest to trudne, że jeżeli jest q różnego rodzaju czapek na głowach n osób, to prawdopodobieństwo p popełnienia błędu przy dowolnej strategii postępowania spełnia nierówność^{viii}

^{viii} Metoda, którą przedstawiliśmy dla $q = 2$, jest optymalna, bo wtedy $p = 1/(n + 1)$, a więc zachodzi równość.

$$p \geq \frac{q - 1}{n + q - 1}.$$

W pracy N. Alon, *Problems and Results in Extremal Combinatorics – II*, dostępnej w Internecie, udowodniono, że istnieje metoda, która gwarantuje, że to prawdopodobieństwo nie przekracza liczby

$$\frac{1 + (q - 1) \log n}{n} + \left(1 - \frac{1}{q}\right)^n.$$

Niestety, dowód jest nieefektywny i nie wskazuje, jak to zrobić.



Zadania

Redaguje Mikołaj KORZYŃSKI

F 647. Kolejka gondolowa, gdy nie jedzie, często huśta się razem z liną (rys. 1), pod wpływem wiatru bądź z powodu gwałtownego zatrzymania. Kiedy jednak porusza się, chociażby z niewielką prędkością, huśtanie niemal nie występuje. Wyjaśnić to zjawisko.

Rozwiązanie na str. 12

F 648. W słoneczny dzień w odległości d od obserwatora leży płat śniegu o powierzchni A . Obserwator dostrzega na śniegu k odbłyśków światła słonecznego. Ocenic gęstość rozmieszczenia drobinek śniegu na powierzchni płata. Jako rozmiar kątowy Słońca przyjąć α .

Rozwiązanie na str. 16

Redaguje Waldemar POMPE

M 1102. W trójkącie ABC dwusieczna kąta ACB przecina bok AB w punkcie D (rys. 2). Okręgi opisane na trójkątach BCD i ACD przecinają boki AC i BC odpowiednio w punktach E i F . Wykazać, że $AE = BF$.

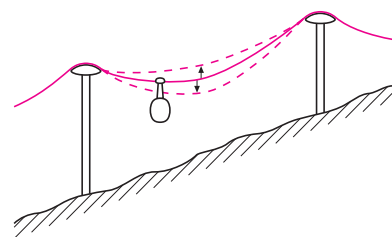
Rozwiązanie na str. 13

M 1103. Ciąg p_1, p_2, \dots jest określony następująco: $p_1 = 2$, a dla $n \geq 1$ liczba p_{n+1} jest największym dzielnikiem pierwszym liczby $p_1 p_2 \dots p_n + 1$. Udowodnić, że w ciągu tym nie występuje liczba 5.

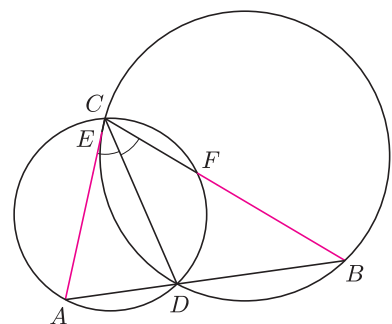
Rozwiązanie na str. 12

M 1104. Dany jest wielokąt wypukły o polu 1. Wykazać, że wielokąt ten można nakryć trójkątem o polu 4.

Rozwiązanie na str. 3



Rys. 1



Rys. 2