

XOR sprowadza się do sumy bez przeniesienia:

$$\begin{array}{r} 49_{10} \ 110001 \\ \oplus \ 3_{10} \ 000011 \\ \hline 50_{10} \ 110010 \end{array}$$

Na przykład:

$$\begin{array}{r} 10_{10} \ 01010 \\ 21_{10} \ 10101 \\ 19_{10} \ 10011 \\ 19_{10} \ 10011 \\ \oplus \ 10_{10} \ 01010 \\ \hline 21_{10} \ 10101 \end{array}$$

Widzimy, że operacja XOR jest przemienne ($A \oplus B = B \oplus A$) i łączna ($(A \oplus B) \oplus C = A \oplus (B \oplus C)$), a zatem wynik nie zależy od kolejności elementów. Oznacza to, że kiedy zastosujemy XOR do wszystkich elementów tablicy, to rezultat będzie taki sam, jak gdyby wszystkie pary takich samych elementów stały obok siebie. Ale przecież dla każdej liczby A zachodzi $A \oplus A = 0$. Wynikiem tej operacji będzie liczba, która występuje tylko raz! W ten sposób dostajemy rozwiązanie działające w czasie liniowym ($O(n)$), które potrzebuje stałej ilości pamięci.

```
function SZUKAJ(A)
  x := 0
  for i := 1 to n do
    x := x ⊕ A[i]
  return x
```



O błędach pozycji gwiazd i prędkościach cząsteczek gazu

Alex SCHWARZENBERG-CZERNY*

* Centrum Astronomiczne im. Mikołaja Kopernika w Warszawie

John Herschel (1792–1871) dokonał wielu pomiarów pozycji gwiazd na niebie, w tym po raz pierwszy w historii na tak dużą skalę na półkuli południowej, prowadząc obserwacje z przyłądka Dobrej Nadziei. Przy okazji zainteresował się błędami swoich pomiarów i tym, jaki może być ich rozkład. Na podstawie sposobu pomiaru i charakteru obrazu gwiazdy w teleskopie uznał, że

- (a) prawdopodobieństwo błędu zależy od jego wielkości r , ale nie od kierunku na niebie, oraz że
- (b) błędy we współrzędnych x i y są niezależne.

Ogólnie prawdopodobieństwo $P(A \cap B)$ zajścia na raz zdarzeń A i B , które mogą być zależne, wyraża się iloczynami $P(A \cap B) = P(A)P(B|A) = P(B)P(A|B)$, gdzie $P(B|A)$ to prawdopodobieństwo zajścia B , gdy wiadomo, że zachodzi A , i odwrotnie dla $P(A|B)$. W skrajnym wypadku, gdy muszą one zachodzić na raz, $P(B|A) = P(A|B) = 1$, tj. jedno jest pewną konsekwencją drugiego i odwrotnie. Natomiast, gdy są one niezależne, to można opuścić drugi argument i $P(B|A) = P(B)$, $P(A|B) = P(A)$.

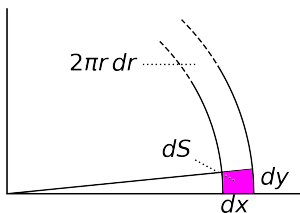
Dodatkowo prawdopodobieństwo błędu winno zmieniać się płynnie z pozycją gwiazdy, to znaczy być ciągłą funkcją współrzędnych. Na podstawie obserwacji z podpunktu (a) prawdopodobieństwo dP , że pomiar wypadnie w kawałku nieba o powierzchni dS w odległości r od prawdziwej pozycji, możemy zapisać jako $dP = g(r) dS$. Natomiast na podstawie (a) i (b) prawdopodobieństwo, że pomiar wypadnie w kawałku nieba o powierzchni dS , będzie równe $dP = f(x)f(y)dS$ dla pewnej funkcji ciągłej f . Mamy zatem

$$(1) \quad g(r) dS = dP = f(x)f(y) dS, \quad \text{co oznacza, że} \quad \ln g(r) = \ln f(x) + \ln f(y).$$

Jeśli za początek układu współrzędnych wybierzemy prawdziwą pozycję gwiazdy, to jak nauczał Pitagoras, $r^2 = x^2 + y^2$. Gdybyśmy funkcje $\ln f(x)$, $\ln g(r)$ mogli przedstawić w postaci szeregu („nieskończonego wielomianu”), czyli

$$\ln g(r) = -a - br - cr^2 - dr^3 - \dots,$$

to moglibyśmy zauważyć, że tylko dwa wyrazy (pierwszy i trzeci) powyższego szeregu można przedstawić w postaci sumy funkcji x i y , a zatem $\ln g(r) = -a - cr^2 = -a - c(x^2 + y^2)$. Rozwijanie w szereg to chleb powszedni wielu naukowców, których powinno ucieszyć to obrazowe uzasadnienie. Dla Czytelników, którym wydaje się ono niewystarczająco precyzyjne, przedstawimy też inne wyprowadzenie. Niech $\alpha(t) = \ln g(\sqrt{t})$, $\beta(x) = \ln f(x)$. Wstawiając do (1)



Obszar wokół rzeczywistej pozycji gwiazdy

**Rozwiązanie zadania M 1686.**

Jest to możliwe tylko dla nieparzystych n .

Załóżmy, że $2 \mid n$, i ustalmy kolumnę, w której wpisane są liczby kolejno a, b, c . Wówczas $n \mid ab + bc + ca$, więc w szczególności $2 \mid ab + bc + ca$, skąd wynika, że wśród liczb a, b, c jest co najwyżej jedna liczba nieparzysta. Wobec tego każda kolumna tablicy $3 \times n$ zawiera co najwyżej jedną liczbę nieparzystą – więc w całej tablicy jest ich nie więcej niż n . Z drugiej strony, każdy z wierszy zawiera $n/2$ liczb nieparzystych, więc łącznie w tablicy mamy $3n/2 > n$ liczb nieparzystych – sprzeczność.

Załóżmy teraz, że $2 \nmid n$. W tablicę wpisujemy liczby w następujący sposób:

- I, II wiersz: w i -te pole wpisujemy $2i \pmod{n}$, natomiast resztę 0 w ostatnim polu zastępujemy przez n .
- III wiersz: w i -te pole wpisujemy $n - i$, natomiast liczbę 0 w ostatnim polu zastępujemy przez n .

Ponieważ $2 \nmid n$, to w każdym wierszu wpisane są różne liczby. Ponadto dla trzech liczb a, b, c w jednej kolumnie mamy:

$$\begin{aligned} ab + bc + ca &\equiv 2i \cdot 2i + 2i \cdot (-i) + 2i \cdot (-i) \equiv \\ &\equiv 0 \pmod{n}. \end{aligned}$$

W odróżnieniu od ówczesnych chemików wielu fizyków nadal nie wierzyło w atomy i rozkład prędkości ruchu cząstek w gazie doskonałym (rozkład Maxwella) pozostawał ciekawostką. Dopiero gdy Ludwig Boltzmann (1877) wyprowadził go niezależnie ze statystyki cząstek, znajdując po drodze wzór na entropię, XIX-wieczna fenomenologiczna termodynamika zaczęła ewoluować ku fizyce statystycznej.

**Rozwiązanie zadania M 1684.**

Tak, istnieje, np.

- (a) $f(x) = x^2 - 1$,
 (b) i (c) $f(x) = 2x^2 - 8$.

wartość $y = 0$, dostajemy $\alpha(x^2) = \beta(x) + \beta(0)$, zatem $\alpha(x^2 + y^2) = \alpha(x^2) + \alpha(y^2) - 2\beta(0)$. Przyjmując $\gamma(t) = \alpha(t) - 2\beta(0)$, $u = x^2$, $v = y^2$, dostaniemy $\gamma(u + v) = \gamma(u) + \gamma(v)$. Jest to podstawowe równanie funkcyjne (tzw. *równanie Cauchy'ego*), którego jedynym ciągłym rozwiązaniem jest funkcja liniowa (więcej o tym równaniu można przeczytać np. w artykule Marka Kordosa w Δ_{08}^8). Niech zatem $\gamma(t) = -ct$, wówczas przyjmując $a = 2\beta(0)$, dostajemy znowu $\ln g(r) = -a - cr^2$. Zatem

$$(2) \quad dP = g(r)dS = Ce^{-cr^2} 2\pi r dr = -\frac{C\pi}{c} d(e^{-cr^2}),$$

gdzie $C = e^{-a}$. Ostatnia równość w (2) wynika z obliczenia przyrostu funkcji w nawiasie przy zmianie r o dr . Uzasadnimy to dokładniej na końcu artykułu, a na razie zajmijmy się jeszcze znalezieniem wartości C . Dodając do siebie wszystkie możliwe przyrosty prawdopodobieństwa z lewej strony równania (2), dostaniemy 1, a z prawej strony mamy

$$\Delta\left[-\frac{C\pi}{c} d(e^{-cr^2})\right] = -\frac{C\pi}{c} \left[e^{-cr^2}\right]_0^\infty = \frac{C\pi}{c}$$

(suma przyrostów funkcji na półprostej to po prostu różnica wartości funkcji na krańcach). Porównując, otrzymujemy $C = \frac{c}{\pi}$, skąd dostajemy

$$g(r) = \frac{c}{\pi} e^{-cr^2} = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}},$$

wprowadzając tradycyjne oznaczenie $c = 1/(2\sigma^2)$. Ostatecznie mamy

$$(3) \quad f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2}}.$$

Jest to podstawowy w statystyce rozkład prawdopodobieństwa, zwany rozkładem Gaussa lub rozkładem normalnym. Za sprawą de Moivre'a i następców pojawił się on jako graniczny przypadek paru innych znanych rozkładów prawdopodobieństwa. Gauss (1800) podał niezależne wyprowadzenie i pierwszy zastosował go do analizy błędów obserwacji. Laplace (1810, 1812) zauważył, że jeśli obserwowany wynik jest sumą wielu zmiennych losowych o tym samym rozkładzie, to (przy rozsądnych założeniach) rozkład prawdopodobieństwa tej wielkości (odpowiednio unormowanej) dąży do rozkładu normalnego. Ta pierwsza wersja *Centralnego Twierdzenia Granicznego* do czasów obecnych została znacznie uogólniona na sumy zmiennych o różnych rozkładach. Fascynujące jest, że (poza czynnikiem normalizującym C) Herschel wyprowadził rozkład normalny z tak prostych założeń. Dziesięć lat później to rozumowanie zainspirowało Maxwella do wyprowadzenia rozkładu prędkości cząsteczek gazu, przy założeniu (a) i (b). Dla $v^2 = v_x^2 + v_y^2 + v_z^2$ i dla przyrostu objętości $dV = 4\pi v^2 dv$ w 3-wymiarowej przestrzeni prędkości v otrzymał on $dP = g(v)dV = Ce^{-cv^2} v^2 dv$. Stałe C i c można obliczyć, wykorzystując sumowanie się przyrostów prawdopodobieństwa do 1 oraz proporcjonalności temperatury absolutnej do ważonej prawdopodobieństwem średniej energii kinetycznej cząsteczek $\frac{3}{2}kT = \int \frac{mv^2}{2} dP$. Wynik końcowy to

$$(4) \quad dP = \left(\frac{m}{2\pi kT}\right)^{3/2} e^{-\frac{mv^2}{2kT}} 4\pi v^2 dv \quad \text{oraz} \quad f(v_x) = \sqrt{\frac{m}{2\pi kT}} e^{-\frac{mv_x^2}{2kT}}.$$

Pozostaje nam dokładniej uzasadnić ostatnią równość w (2). Dla Czytelników biegłych w rachunku różniczkowym jest ona oczywista, pozostałych zaś prosimy o uwierzenie, że dla małych wartości przyrostu dr zachodzi $\frac{e^{dr}-1}{dr} \approx 1$ (ponieważ rozwinięcie e^{dr} w szereg dla małego dr to w przybliżeniu $e^{dr} \approx 1 + dr + \dots$). Mnożąc obustronnie przez e^r , dostajemy $\frac{e^{r+dr}-e^r}{dr} \approx e^r$, zatem wyrażając to w naszej „przyrostowej notacji”, mamy $d(e^r) = e^r dr$. Ponadto dla małych wartości dr jest

$$\frac{(r + dr)^2 - r^2}{dr} = 2r + dr \approx 2r,$$

więc możemy napisać $d(r^2) = 2r dr$. Ostatecznie

$$d(e^{-cr^2}) = e^{-cr^2} d(-cr^2) = -ce^{-cr^2} d(r^2) = -2rce^{-cr^2} dr.$$

Przedstawione tutaj rozumowanie może wydawać się miejscami nieściśle, istnieją jednak matematyczne narzędzia pozwalające na sformalizowanie tych fragmentów, a poznanie choćby intuicji wydaje się w tym przypadku pouczające.