# Koła pamięci

*Aleksandra HORUBAŁA**

* Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni

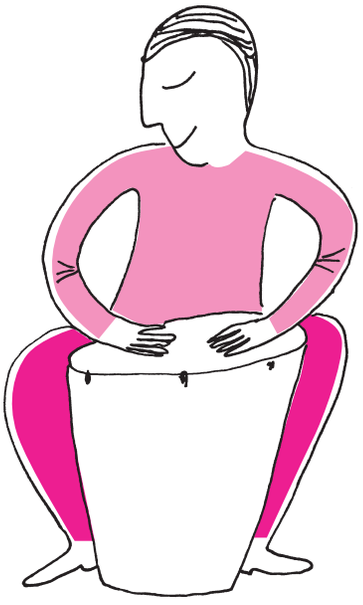
*Yamátárájabánasalagám*!

To nie magiczne zaklęcie, nie onomatopeja ani błąd drukarski... ale starożytne słowo w języku sanskryt, stworzone, aby ułatwić bębniarzom zapamiętanie rytmów. Słowo to jest wyjątkowe, ponieważ zawiera wszystkie potrójne kombinacje krótkich i długich sylab. W sanskrycie sylaba jest krótka, jeżeli pojawia się w niej litera *a*, a długa, kiedy występuje w niej litera akcentowana *á*. Analizując kolejne trójki sylab słowa, dostajemy różne rytmy:

*ya má tá* → krótka długa długa
*má tá rá* → długa długa długa
*tá rá ja* → długa długa krótka

*Yamátárájabánasalagám* – i problem z głowy – umiemy zagrać każdy rytm!

Sanskryt to język literacki starożytnych, średniowiecznych i wczesnonowożytnych Indii. Język literacki to odmiana języka o szczególnym prestiżu społecznym, mająca większy zasięg niż lokalne dialekty.

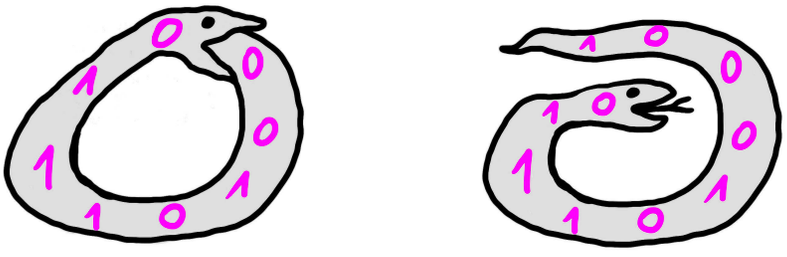


Koło pamięci czwórek powinno składać się z $2^4 = 16$ bitów, bo tyle jest różnych ciągów czterobitowych (na każdej z 4 pozycji możemy wybrać dowolną z 2 wartości: 0 lub 1). Uogólniając, koło pamięci kombinacji $n$-elementowych będzie składało się z $2^n$ bitów ustawionych na okręgu.

Jeśli jesteś matematykiem, a nie starożytnym bębniarzem, myślisz pewnie, że byłoby elegancko krótkim sylabom przyporządkować cyfrę 0, a długim cyfrę 1. Słowo *yamátárájabánasalagám* zamieni się wtedy w ciąg binarny: 0111010001 (cyfry 0 i 1 będziemy dalej nazywać bitami). Zauważmy, że w tym ciągu każda trójka bitów pojawia się dokładnie raz:

011 111 110 101 010 100 000 001.

Ale na tym nie koniec! Ostatnie dwie cyfry ostatniej trójki są takie same, jak pierwsze dwie cyfry pierwszej trójki. Wykorzystując ten fakt, możemy zaprezentować słowo nie jako ciąg znaków, ale jako okrąg.

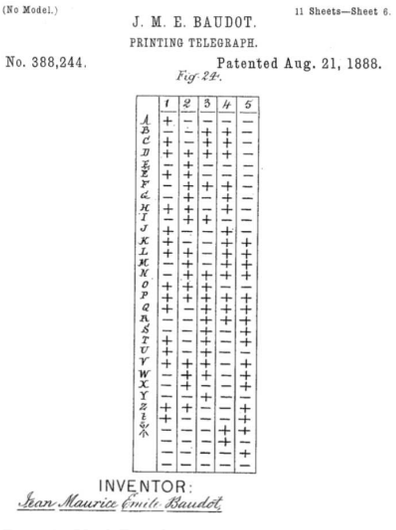



Rys. 1. Koło pamięci. Rysunek na podstawie artykułu S. Steina [1]

Tak skonstruowany okrąg nazywany jest *kołem pamięci (memory wheel) trójek.* Można wytworzyć analogiczne koła pamięci, które zawierają dłuższe kombinacje bitów. Spróbujcie sami skonstruować koło pamięci czwórek.

## Telegramy

Koła pamięci były używane do konstrukcji teleprinterów, czyli maszyn wykorzystywanych do przesyłania telegramów. Pierwszy zrobił to Émile Baudot w 1874 roku. System Baudota składał się z nadajnika i odbiornika. Aby wysłać tekst telegramu, trzeba było go najpierw przedstawić jako ciąg bitów. Ponieważ w alfabecie jest 26 liter, do zakodowania ich trzeba użyć co najmniej 5 bitów ($2^5 = 32$ różne kombinacje pozwalają zakodować wszystkie litery). Kod Baudota, w którym bitowi 0 odpowiada znak −, a bitowi 1 znak +, zaprezentowano na rysunku 2.


(No Model.) 11 Sheets—Sheet 6.

J. M. E. BAUDOT.

PRINTING TELEGRAPH.

No. 388,244. Patented Aug. 21, 1888.

Fig 22.

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| A | + | − | − | + | − |
| B | + | − | + | + | − |
| C | + | + | − | − | − |
| D | + | − | + | − | − |
| E | + | + | − | + | − |
| F | − | + | + | − | − |
| G | + | − | + | + | − |
| H | − | + | − | + | − |
| I | + | + | − | − | + |
| J | + | − | − | + | + |
| K | + | − | + | + | + |
| L | − | + | − | − | + |
| M | + | + | + | − | + |
| N | + | + | − | + | + |
| O | − | − | + | + | + |
| P | + | − | + | + | + |
| Q | + | + | + | + | + |
| R | − | − | + | − | + |
| S | + | − | − | + | + |
| T | − | + | − | + | + |
| U | + | − | − | − | + |
| V | + | − | + | − | + |
| W | − | + | + | + | + |
| X | − | − | + | + | + |
| Y | − | + | − | + | + |
| Z | + | − | + | − | + |
| ⁂ | − | − | − | + | + |
| | − | − | − | − | + |

INVENTOR:

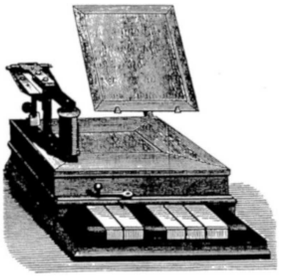
Jean Maurice Émile Baudot

Rys. 2. Kod Baudota

Operator nadajnika musiał wciskać przyciski maszyny, pamiętając, który kod odpowiada której literze (dwa klawisze lewą ręką, trzy prawą ręką, jak widać na rysunku 3).

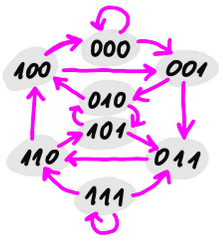
Nie było to łatwe zadanie i powodowało wiele technicznych problemów (operatorzy musieli pracować w tempie nadanym przez maszynę!). Na szczęście Baudotowi udało się skonstruować odbiornik automatycznie drukujący tekst telegramów, a wykorzystał do tego koła pamięci.

Teleprinter Baudota wykorzystywał układ zsynchronizowanych obracających się kół. Koła pamięci zamodelowane zostały jako metalowe dyski z literami



Rys. 3. Nadajnik systemu Baudota

Rys. 4




Rys. 5. Graf odpowiadający kołu pamięci trójek. Rysunek na podstawie artykułu S. Steina [1]

wytłoczonymi na obwodzie (rys. 4). Po otrzymaniu kodu litery obracający się dysk był automatycznie zatrzymywany w pozycji, którą wskazywały bity kodu (wysuwane i chowane metalowe słupki), a litera zapisana na obwodzie była przyciskana do papieru. Teleprinter Baudota był przełomowym wynalazkiem – dopiero ponad 40 lat później, w 1916 roku, Edward Kleinschmidt skonstruował maszynę drukującą telegramy na kartkach papieru (jak współcześnie znane maszyny do pisania).

Powróćmy jednak do kół pamięci. Zastanówmy się, co jeżeli chcielibyśmy zakodować nie tylko litery, ale też cyfry? I jeszcze znaki interpunkcyjne? Będziemy potrzebowali coraz większych kół pamięci. Czy istnieje koło pamięci dowolnego rozmiaru?

## Problem Teleprintera

Problem konstrukcji kół pamięci został nazwany Problemem Teleprintera, a sformułowano go w następujący sposób:

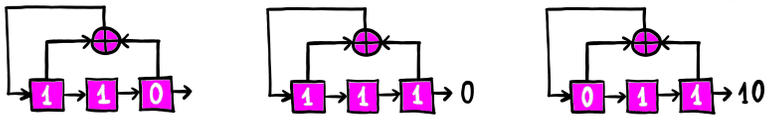
*Skonstruuj najdłuższy ciąg okresowy, składający się z elementów 0 i 1, taki że żaden podciąg r-elementowy nie pojawi się w nim więcej niż raz.*

Problem został rozwiązany w 1940 roku przez Irvinga Gooda – brytyjskiego matematyka, który pracował jako kryptolog w Bletchley Park z Alanem Turingiem. W swoim dowodzie Good użył teorii grafów. Rzeczywiście możemy skonstruować graf, w którym kombinacje bitów odpowiadają wierzchołkom, a krawędź z kombinacji $A$ do $B$ oznacza, że $B$ można uzyskać z $A$, kasując pierwszy znak i dodając jakiś nowy na koniec. Dla trójek bitów będzie to graf przedstawiony na rysunku 5.

Znalezienie szukanego ciągu odpowiada przejściu przez graf w taki sposób, aby odwiedzić wszystkie wierzchołki, ale żadnego dwa razy. Aby skonstruować koło pamięci, należy zakończyć spacer po grafie w punkcie, od którego został rozpoczęty – takie przejście przez graf nazywane jest cyklem Hamiltona. Good pokazał, że w grafach reprezentujących $n$–bitowe kombinacje zawsze istnieje cykl Hamiltona.

## Generacja kół pamięci

Wiemy zatem, że da się skonstruować koło pamięci dowolnego rozmiaru. Jednak rysowanie grafów jest odrobinę uciążliwe, wolelibyśmy prostszą metodę. Z ratunkiem nadciągnął amerykański matematyk Solomon Golomb (znany skądinąd jako pomysłodawca figur *polyomino*, które wykorzystali twórcy gry Tetris). Pokazał on, że koła pamięci można generować, używając liniowych rejestrów przesuwnych ze sprzężeniem zwrotnym.[†] Przykład takiego rejestru zaprezentowano na rysunku:




Zasada działania takiego rejestru jest następująca. W każdą komórkę rejestru należy wstawić jeden bit. Następnie należy wyobrazić sobie tykający zegar. Przy każdym tyknięciu następuje przesunięcie bitów w rejestrze zgodnie z kierunkiem strzałek. Jeżeli dwa bity napotkają na drodze symbol +, należy je dodać modulo 2 (tak by w wyniku otrzymać bit 0 lub 1). Kiedy ostatni bit wypadnie na zewnątrz, a bit otrzymany z sumowania trafi do pierwszej komórki rejestru, czekamy na kolejne tyknięcie zegara i cykl zaczyna się od nowa. Bity, które wypadają z rejestru, tworzą tak zwany *ciąg generowany przez rejestr*.

Ciągi generowane przez rejestry tego typu są zawsze cykliczne, ponieważ liczba różnych sekwencji bitów, które mogą pojawić się w rejestrze, jest skończona. W końcu w komórkach rejestru musi pojawić się ciąg, który był tam już wcześniej – od tej pory wszystko będzie się dziać cyklicznie.

[†]Rejestr nazywamy przesuwnym, gdy bity są przesuwane między jego komórkami. Mówimy, że rejestr ma sprzężenie zwrotne, jeżeli w każdym takcie zegara pewna funkcja bitów z komórek rejestru trafia z powrotem do początkowej komórki. Określenie *liniowy* odnosi się do liniowości wybranej funkcji – operacji sumowania.

[1] Sherman K. Stein, *Mathematician as an explorer*, Scientific American, www.scientificamerican.com/article/stein-the-mathematician-as-an-explorer/
[2] Solomon Golomb, *Shift Register Sequences*, World Scientific Publishing Company, 2017.

Na przykładzie dodaliśmy bity z pierwszej i trzeciej komórki rejestru, ale tę zasadę działania możemy wybrać dowolnie, i różne wybory prowadzą do konstrukcji rejestrów o różnych własnościach. Golomb pokazał, jak wybrać komórki rejestru do sumowania tak, żeby ciąg wygenerowany przez rejestr odpowiadał kołu pamięci. W języku rejestrów mówimy o takim ciągu, że ma maksymalny okres. Ponieważ pojawiły się w nim wszystkie możliwe stany, to ten sam stan pojawił się drugi raz najpóźniej, jak to tylko możliwe – stąd cykl, który się będzie powtarzał, ma najdłuższy możliwy okres. Golomb identyfikował wybór komórek rejestru ze współczynnikami wielomianu. Na przykład rejestr z rysunku 5 przy sumowaniu wykorzystuje komórki 1 i 3, co odpowiada wielomianowi $1 + x^1 + x^3$. Można pokazać, że wygenerowany ciąg jest maksymalny wtedy i tylko wtedy, gdy wielomian odpowiadający komórkom rejestru jest *pierwotny* [2]. Oznacza to między innymi, że nie da się go rozłożyć na iloczyn wielomianów niższego stopnia. Zainteresowanego Czytelnika odsyłamy do książki Golomba zatytułowanej *Shift Register Sequences*.

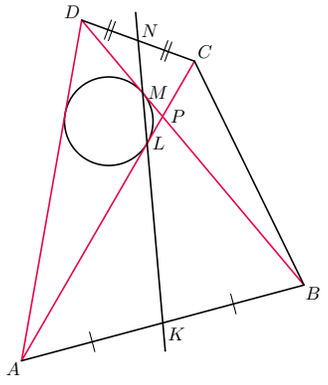
Ciągi o maksymalnym okresie generowane przez dostatecznie długie rejestry są trudne do odróżnienia od ciągów losowych (zakładając, że widzimy ich skończony fragment, niezawierający cyklu). Dzięki tej własności rejestry przesuwne ze sprzężeniem zwrotnym mają szerokie zastosowania w kryptografii, m.in. są wykorzystywane do generowania ciągów pseudolosowych i konstrukcji szyfrów strumieniowych. Na koniec zauważmy, że aby wygenerować ciąg odpowiadający zawołaniu indyjskich bębniarzy, można użyć pokazanego wcześniej rejestru. Może umiesz znaleźć rejestr, który pozwoli wygenerować koło pamięci czwórek?

# Zadania

*Przygotował Dominik BUREK*

**M 1726.** Jaką najmniejszą liczbę wież szachowych można ustawić na szachownicy $8 \times 8$ tak, aby każde białe pole było zagrożone? (Wieża atakuje pole, na którym stoi, oraz każde pole w tym samym wierszu i kolumnie).
Rozwiązanie na str. 6

**M 1727.** W czworokącie wypukłym $ABCD$ zachodzi $AC = BD = AD$. Punkty $K$ i $N$ są środkami boków odpowiednio $AB$ i $CD$. Przekątne $AC$ i $BD$ przecinają się w punkcie $P$. Okrąg wpisany w trójkąt $APD$ jest styczny do boków $PA$ i $PD$ w punktach odpowiednio $L$ i $M$ (rys. 1). Udowodnić, że punkty $K$, $L$, $M$ i $N$ leżą na jednej prostej.
Rozwiązanie na str. 13




Rys. 1

**M 1728.** Dane są liczby rzeczywiste $a$, $b$ i $c$ takie, że

$$(a-b)^2 + (b-c)^2 + (c-a)^2 \geqslant 2.$$

Udowodnić, że

$$|a-b| + |b-c| + |c-a| \geqslant 2.$$

Rozwiązanie na str. 14

*Przygotował Andrzej MAJHOFER*

**F 1059.** Prędkości gwiazd układu podwójnego wynoszą $v_1$ i $v_2$, a okres, z jakim obiegają środek masy układu, wynosi $T$. Gwiazdy poruszają się po orbitach kołowych. Wyznacz masy gwiazd i odległość między nimi.
Rozwiązanie na str. 5

**F 1060.** W temperaturze $T$ ciśnienie pary nasyconej nad płaską powierzchnią jednorodnej cieczy wynosi $p_0$. Ile wynosi ciśnienie pary nasyconej w temperaturze $T$ nad powierzchnią tej samej cieczy o kształcie wycinka sfery o promieniu $r$ (np. nad kroplą tej cieczy)? Masa molowa cieczy wynosi $\mu$, napięcie powierzchniowe $\gamma$, stała gazowa $R$, przyspieszenie ziemskie $g$.
*Wskazówka:* powierzchnia cieczy w wąskiej kapilarze o przekroju kołowym ma kształt wycinka sfery i jeśli promień tej sfery wynosi $r$, to dodatkowe ciśnienie pod meniskiem wypukłym wynosi $2\gamma/r$.
Rozwiązanie na str. 7