Od problemu żarówek do nowego systemu szyfrowania

Andrzej Szablewski Radosław Peszkowski

Mateusz Janus Jakub Mazur

2016

Spis treści

1 *Wstęp* 3
2 *Problem żarówek* 3
3 *Zastosowanie* 8
5 *Szyfrowanie asymetryczne macierzy dwuwskaźnikowej stanów* 9
6 *Zakończenie* 11
7 *Spis użytych pojęć* 12
8 *Spis twierdzeń* 13
9 *Bibliografia* 15

Wstęp

Matematyka często kojarzona jest z rozwiązywaniem zadań. Zadania mogą być różnego rodzaju. Takie „słupki” z zeszytu z ćwiczeniami i takie, które motywują do myślenia i są punktem wyjścia do dalszych rozważań. Ta praca wyrosła właściwie z tego problemu. „Mamy 8 żarówek. Pod każdą żarówką znajduje się przełącznik. Kliknięcie przełącznika powoduje zapalenie lub zgaszenie (zmianę stanu) żarówki nad nim oraz żarówek bezpośrednio z nią sąsiadujących.”

	A	B	C	D	E	F	G	H
żarówki	0	0	0	0	0	0	0	0
przełączniki	0	0	0	0	0	0	0	0

Tab. 1

$\underline{Przykład\ 1}$

Kliknięcie przełącznika C powoduje zmianę stanu żarówek C oraz B i D.

Analogicznie kliknięcie przełącznika skrajnego (A, H) spowoduje zmianę stanu żarówki nad nim oraz tylko jednej sąsiadującej. Więc gdy zostanie kliknięty przełącznik A, zmienią stan żarówki A oraz B. Problem polegał na odgadnięciu jakie przyciski należy przełączyć, aby od stanu S_0, w którym wszystkie żarówki są zgaszone, przejść do stanu, w którym wszystkie żarówki są zapalone. Zaczęliśmy eksperymentować z innymi kombinacjami. Jedna z nich sprawiła nam trudność i odkryliśmy, że nie da się jej osiągnąć. Uznaliśmy, że jest to bardzo ciekawy problem, dlatego zaczęliśmy badać to zagadnienie. Oto wyniki naszej pracy.

W wierszu żarówki, 0 symbolizują żarówkę zgaszoną, natomiast 1 symbolizuje żarówkę zapaloną. Stanem żarówki nazwiemy to czy jest ona zgaszona (0) czy zapalona (1).

Problem żarówek

Nie ma powodów by nasze rozważania ograniczyć do 8 żarówek. Problem potraktujemy od razu ogólnie i przyjmiemy, że liczba żarówek wynosi N. W pracy będziemy posługiwać się następującym oznaczeniem operacji modulo $A \equiv B\ mod\ (C)$. Oznacza to, że reszta z dzielenia A przez C jest równa B.

$\underline{Zasada\ 1}$

Naciśnięcie przełącznika wpływającego na żarówkę zmienia jej stan na przeciwny.

Stanem układu żarówek nazwiemy ciąg stanów kolejnych żarówek. Jest to skończony ciąg, którego elementami są liczby 0 i 1. Dla $N = 8$ stanem może być 00001110.

$\underline{Twierdzenie\ 1}$

Każdy stan żarówek można zapisać w postaci stanu użytych do miejsca od stanu S_0 do danego stanu przycisków.

Na przykład, aby ze stanu S_0 uzyskać stan 00001110 należy użyć przycisku F, który spowoduje zapalenie się tych trzech żarówek. Przejście od jednego stanu do innego, odpowiada dodawaniu $modulo\ 2$ w **odpowiednich kolumnach**.

Zaczynając od stanu 00110110 i używając przycisku F dostajemy stan 00111000, ponieważ

$$\begin{array}{rr} & 00110110 \\ + & 00001110 \\ \hline mod\ (2) & 00111000 \end{array}$$

Tab. 2

<u>*Uwaga*</u>

Nie dodajemy liczb w systemie dwójkowym, dodawanie w każdej kolumnie jest niezależne!

<u>*Twierdzenie 2*</u>

Stan końcowy nie zależy od kolejności przyciskania przełączników.

<u>*Twierdzenie 3*</u>

Dla każdego N liczba stanów układu jest równa 2^N.

Tabele poniżej obrazują stany żarówek oraz odpowiadające im stany przełączników. Dla przełączników liczba 1 oznacza, że dany przełącznik został wciśnięty, a liczba 0, że nie. Rozpatrujemy przejścia od stanu początkowego S_0 do podanego stanu.

$$N = 3$$

Ż		P
000	⇔	000
001	⇔	110
010	⇔	111
100	⇔	011

Tab. 3

Jeżeli chcemy na przykład otrzymać stan 111 to możemy dodać do siebie odpowiednie „pojedyncze” jedynki oraz odpowiadające im przełączniki. Jeżeli którakolwiek cyfra wyniku jest większa od 1, wykonać na niej operację $mod\ (2)$. W tym przypadku będzie to:

$$\begin{array}{rccc} & \text{Ż} & & \text{P} \\ & 100 & \Leftrightarrow & 011 \\ & 010 & \Leftrightarrow & 111 \\ + & 001 & \Leftrightarrow & 110 \\ \hline mod\ (2) & 111 & \Leftrightarrow & 010 \end{array}$$

Tab. 4

Skoro mamy podstawowe stany mające jedną jedynkę oraz same zera, można z nich osiągnąć bardziej skomplikowane stany, złożone z paru jedynek, poprzez dodawanie.

$N = 4$

Ż		P
1000	⇔	1011
0100	⇔	0011
0010	⇔	1100
0001	⇔	1101

Tab. 5

$N = 5$

Ż		P
10000	⇔	-
01000	⇔	-
00100	⇔	11000 lub 00011
00010	⇔	-
00001	⇔	-

Tab. 6

Rodziną stanów nazwiemy taki ich zbiór, że możliwe jest przejście od jednego stanu w rodzinie do każdego innego stanu w tej rodzinie.

Dla $N = 5$ sprawa się komplikuje, niektóre stany są w jednej rodzinie, a inne w drugiej. Jeżeli stan początkowy jest w pierwszej rodzinie, a inny wybrany stan jest w drugiej rodzinie to nie da się przejść między nimi.

<u>*Twierdzenie* 4</u>

Gdy $N \equiv 0 \; mod \; (3)$*, lub* $N \equiv 1 \; mod \; (3)$ *to wszystkie stany tworzą jedną rodzinę, natomiast gdy* $N \equiv 2 \; mod \; (3)$ *to dzielą się one na dwie rodziny lub więcej.*

Po dokładnym zbadaniu stanów żarówek i przełączników $N = 5$ okazało się, że istnieje taki stan przełączników, który nie zmienia stanu żarówek. Patrząc na wcześniej wypisane kombinacje przycisków (Tab. 6) zauważyliśmy, że za tą samą żarówkę odpowiadają dwa różne stany przycisków. Oznacza to że po dodaniu ich do siebie powinniśmy otrzymać nic nie zmieniający stan przycisków. Taki stan przycisków nazwiemy *stanem MOM* ze względu na pewną sekwencję (11011), która się powtarza w tych stanach i znacznie ułatwia nam tworzenie stanów MOM.

	Ż		P
	00100	⇔	11000
+	00100	⇔	00011
$mod \; (2)$	00000	⇔	11011

Tab. 7

Sprawdziliśmy również stany MOM dla innych wartości N. Okazało się że takie stany występują tylko dla $N \equiv 2 \; mod \; (3)$. Tabela 8 pokazuje stany MOM dla różnych wartości N.

N	Stan przycisków MOM
2	11
5	11011
8	11011011
11	11011011011
14	11011011011011
17	11011011011011011
20	11011011011011011011
23	11011011011011011011011
26	11011011011011011011011011
29	11011011011011011011011011011

Tab. 8

$N = 6$

Ż		P
100000	⇔	011011
010000	⇔	111011
001000	⇔	110000
000100	⇔	000011
000010	⇔	110111
000001	⇔	110110

Tab. 9

Przy $N = 6$ zauważyliśmy, że części poszczególnych stanów są złożone ze stanów $N = 3$.

$N = 6$

Ż		P
100|000	⇔	011|011
010|000	⇔	111|011
001|000	⇔	110|000
000|100	⇔	000|011
000|010	⇔	110|111
000|001	⇔	110|110

Tab. 10

$N = 3$

Ż		P
000	⇔	000
001	⇔	110
010	⇔	111
100	⇔	011

Tab. 11

Co dalej za tym idzie, wszystkie stany $N \equiv 0 \; mod \; (3)$ możemy złożyć z poszczególnych stanów $N = 3$. Również wszystkie stany $N \equiv 1 \; mod \; (3)$ możemy złożyć ze stanów $N = 3$. Każde trzy żarówki licząc od lewej strony nazwiemy *trójką żarówek*. Dla $N \equiv 1 \; mod \; (3)$ ostatnia żarówka jest pierwszą żarówką nowej trójki.

Uznaliśmy, że pomocna przy wykonywaniu działań na żarówkach i przełącznikach będzie informacja ile minimalnie kroków, czyli ile przełączników należy wcisnąć, aby zmienić stan poszczególnych żarówek. Taką informację nazwaliśmy *mlk* – minimalna liczba kroków. Tabela 12 przedstawia ile wynosi mlk poszczególnych żarówek, $N = 6$.

$$N = 6$$

mlk	4	5	2	2	5	4
żarówki	1	1	1	1	1	1

Tab. 12

Po wykonaniu tabeli dla $N = 6$ zaczęliśmy tworzyć tabele dla większych wartości N, pamiętając jednak, że nie może to być $N \equiv 2 \; mod \; (3)$, ponieważ wtedy nie da się zapalić niektórych żarówek zaczynając od stanu początkowego S_0.

$$N = 7$$

mlk	5	4	2	5	2	4	5
żarówki	1	1	1	1	1	1	1

Tab. 13

Pierwszym uzasadnionym spostrzeżeniem było to, że zawsze trzecią żarówkę od początku i od końca można zapalić w dwóch ruchach.

Żarówki	0	0	0	0	0	0

Wystarczy użyć drugiego przycisku, który zapala pierwsze trzy żarówki.

Żarówki	1	1	1	0	0	0

Następnie wciskamy przycisk pierwszy, który gasi dwie pierwsze żarówki.

Żarówki	0	0	1	0	0	0

W ten sposób jako jedyna zostaje nam trzecia zapalona żarówka.

Na podstawie podobnych „obserwacji” udało nam się stworzyć wzory pozwalające na obliczanie mlk dla różnych N. Jednak do poprawnego zrozumienia zasady ich działania niezbędne jest wprowadzenie kilku oznaczeń.

p – pozycja danej żarówki w trójce

q – numer trójki

v – liczba trójek (ostatnia żarówka jest traktowana jako pierwsza żarówka następnej trójki)

$$\boldsymbol{N \equiv 0 \; mod \; (3)}$$

$$mlk = \begin{cases} 2\frac{N}{3} - 2q + 2, & p = 1 \\ 2\frac{N}{3} + 1, & p = 2 \\ 2q, & p = 3 \end{cases}$$

$$\boldsymbol{N \equiv 1\ mod\ (3)}$$

$$mlk = \begin{cases} N - \dfrac{N-1}{3}, & p = 1 \\ (N - v) - (2q - 2), & p = 2 \\ 2q, & p = 3 \end{cases}$$

$$\boldsymbol{N \equiv 2\ mod\ (3)}$$

Dla $N \equiv 2\ mod\ 3$ istnieje jedynie wzór na mlk co trzeciej żarówki, gdyż pozostałych żarówek nie da się pojedynczo zapalić zaczynając od stanu S_0.

$$mlk\ =\ 2q\ (p = 3)$$

Równocześnie z tworzeniem wzorów zauważyliśmy różne zależności mlk w trójkach żarówek.

Poniższa tabela prezentuje nasze spostrzeżenia. Zapis p_1 oznacza, że odwołujemy się do pierwszej żarówki w trójce.

$\boldsymbol{N \equiv 0\ mod\ (3)}$	$\boldsymbol{N \equiv 1\ mod\ (3)}$
$p_1 + p_3 = constans$	$p_2 + p_3 = constans$
$p_2 = constans$	$p_1 = constans$
$p_1 = p_2 - p_3 + 1$	$p_1 = p_2 + p_3 - 1$
$p_2 = p_1 + p_3 - 1$	$p_2 = p_1 - p_3 + 1$
$p_3 = p_2 - p_1 + 1$	$p_3 = p_1 - p_2 + 1$

Zastosowanie

Po wielu godzinach tworzenia nowych wzorów i zależności uznaliśmy, że należy znaleźć jakieś zastosowanie dla naszej pracy. Oprócz tego do czego żarówki służą (a służą one do oświetlania pomieszczeń) wymyśliliśmy, że przy ich pomocy można stworzyć różne systemy kryptograficzne. Niejako przy okazji stworzyliśmy też aplikację komputerową oraz na smartfony, która pomaga testować różne hipotezy, a ponadto może być użyta jako „Gra w żarówki”.

Szyfrowanie asymetryczne macierzy dwuwskaźnikowej stanów

Zauważyliśmy, że mając dany stan przełączników, wypisanie jak wpływa on na stan żarówek nie jest trudne. Jednak mając dany stan żarówek odgadnięcie stanu przełączników, który je zapalił jest znacznie trudniejsze.

Klucz publiczny

Należy stworzyć macierz wypełnioną 0 oraz 1 – czyli tzw. klucz publiczny. Ta macierz odpowiada połączeniu żarówek do przełączników.

Pierwszy wiersz macierzy szyfrującej oznacza, które żarówki zmienią stan po kliknięciu pierwszego przełącznika. Drugi wiersz oznacza, które żarówki zmienią stan po kliknięciu drugiego przełącznika. I tak dalej aż do N-tego wiersza, który będzie oznaczał, które żarówki zmienią stan po kliknięciu N-tego przełącznika.

Przykład:

$$\begin{matrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{matrix}$$

Powyższa macierz odpowiada połączeniom takim, jakie zostały opisane we wprowadzającym zadaniu. W tym przypadku dotyczy to sześciu żarówek.

Macierz połączeń (klucz publiczny) musi spełniać poniższe warunki:

- Ilość kolumn oraz wierszy jest taka sama i wynosi N
- Jej wiersze ani kolumny nie mogą się powtarzać
- Macierz nie może mieć kolumny wypełnionej samymi zerami, oraz wiersza wypełnionego samymi zerami
- Suma wierszy nie może być równa innemu wierszowi
- Macierz musi być $jednoznaczna$, czyli nie da się osiągnąć tego samego stanu dodając różne wiersze

Przykład macierzy *niejednoznacznej*:

$$\begin{matrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{matrix}$$

Po dodaniu wierszy nr 1, 2 oraz 3 uzyskujemy 010000, a dodając dwa ostatnie wiersze również otrzymujemy 010000. Niejednoznaczność uniemożliwia poprawne odszyfrowanie wiadomości.

Szyfrowanie

Wybierana jest wiadomość m, o dowolnej długości. Najczęściej wiadomość nie będzie długości N. Wtedy wiadomość należy podzielić na ciągi o długości N. Należy je zaszyfrować tak jak poniżej, a następnie połączyć w jedną, zaszyfrowaną wiadomość. Przykład:

$$m = 101000$$

Wiadomość oznacza, które wiersze macierzy mamy do siebie dodać w $mod\ 2$. Przykład:

$$\begin{array}{c|cccccc}
m & & & & & & \\
\downarrow & & & & & & \\
1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1
\end{array}
\qquad
\begin{array}{lr}
 & 110000 \\
+ & 011100 \\
\hline
mod\ (2) & 101100
\end{array}$$

W ten sposób powstaje c – zaszyfrowana wiadomość.

$$c = 101100$$

Klucz prywatny i Deszyfrowanie

Aby odszyfrować wiadomość c należy stworzyć macierz, której działanie jest odwrotne do macierzy szyfrującej. Macierz ta musi mieć następującą własność. Wiadomość c oznacza, które wiersze macierzy deszyfrującej należy do siebie dodać aby uzyskać wiadomość m. Poniżej znajduje się macierz deszyfrująca dla powyższej macierzy szyfrującej – jest to tzw. klucz prywatny.

$$\begin{array}{cccccc}
0 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 1 & 0
\end{array}$$

Pierwszy wiersz macierzy deszyfrującej oznacza, które przełączniki należy wcisnąć aby otrzymać zapaloną żarówkę tylko na pierwszej pozycji. Drugi wiersz oznacza, które przełączniki należy wcisnąć aby otrzymać zapaloną żarówkę tylko na drugiej pozycji. I tak dalej aż do N-tego wiersza, który będzie oznaczał, które przełączniki należy wcisnąć aby otrzymać zapaloną żarówkę tylko na N-tej pozycji. Macierz ta ma działanie odwrotne do macierzy szyfrującej.

$$\begin{array}{c|cccccc}
c & & & & & & \\
\downarrow & & & & & & \\
1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0
\end{array}
\qquad
\begin{array}{lr}
 & 011011 \\
 & 110000 \\
+ & 000011 \\
\hline
mod\ (2) & 101000
\end{array}$$

Po dodaniu wierszy otrzymujemy wiadomość m.

$$m = 101000$$

Poniżej prezentujemy niektóre losowe i niesymetryczne macierze szyfrujące oraz deszyfrujące, których tworzenie jest dosyć trudne, wystarczająco aby móc w ten sposób przesyłać ważne dane.

Macierz szyfrująca i deszyfrująca $N = 6$

$$\begin{array}{cccccc|cccccc}
1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0
\end{array}$$

Macierz szyfrująca i deszyfrująca $N = 6$

$$\begin{array}{cccccc|cccccc}
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0
\end{array}$$

Bezpieczeństwo

Bezpieczeństwo tego kryptosystemu opiera się na trudności wyznaczenia macierzy odwrotnej. Złożoność obliczeniowa tej operacji jest rzędu $O(N^{2,373})$, patrz [CLRS]. Nie jest to złożoność imponująca w porównaniu z RSA, ale za to użycie naszego kryptosystemu wymaga tylko pozycyjnego dodawania modulo 2. Oznacza to, że liczba N może być wybrana bardzo duża np. 2^{32}. Taki wybór zapewnia dostateczne bezpieczeństwo dla krótkotrwałych sesji bezpiecznych np. wymiany kluczy wg. schematu Diffiego- Hellmana.

Zakończenie

Pierwszy raz słysząc zagadkę nie sądziliśmy, że będzie ona inspiracją do napisania pracy matematycznej. Udało nam się zdecydowanie rozwinąć zagadnienie i znaleźć zastosowanie praktyczne. Problem szyfrowania jest nadal otwarty i będzie przez nas rozwijany. Mamy nadzieję, że nasz system znajdzie jakieś zastosowanie w praktyce. Myśleliśmy też o modyfikacjach matematycznych. Na przykład zamiast dwóch stanów żarówek; zapalona i zgaszona, można wprowadzić stany opisane kolorami np.: zielona, żółta, czerwona. Podobnie, zamiast rozważać jeden rząd żarówek i przycisków, można rozważać ich macierze. Te pomysły otwierają drzwi do ciekawych uogólnień. Dziękujemy za pomoc w przygotowaniu pracy Paniom Annie Ochel oraz Dorocie Baniak – nauczycielkom matematyki z Gimnazjum w Zabierzowie, oraz Panu Profesorowi Tomaszowi Szembergowi z Uniwersytetu Pedagogicznego w Krakowie.

Spis użytych pojęć

N – liczba żarówek

$Stan\ żarówki$ – każda żarówka może być wyłączona (0) lub włączona (1).

$S - Stan$, jest to określony zbiór żarówek z których każda jest zgaszona lub zapalona. Przykład: Dla $N = 5$ stanem może być 01001 lub 11001 lub kilka innych.

$S_0 - Stan\ początkowy$, stan złożony z samych zer.

$S_1 - Stan\ końcowy$, stan odwrotny do stanu początkowego, stan złożony z samych jedynek.

$Stan\ MOM -$ stan przycisków, który nie zmienia stanu żarówek.

$przejście$ – operacja zmiany stanów samych zer na same jedynki (zmiana stanu początkowego na stan końcowy). Minimalna liczba kroków potrzebna do wykonania przejścia (mlk_p).

$Rodzina$ – maksymalny (względem zawierania) zbiór R stanów żarówek taki, że dla każdego stanu $S \in R$ możliwe jest przejście do każdego innego stanu $T \in R$.

$trójka\ żarówek$ – pierwsza trójka żarówek to pierwsze trzy żarówki licząc od lewej strony. Druga trójka to żarówki 4,5,6 itd. Dla $N \equiv 1\ mod\ (3)$ ostatnia żarówka jest pierwszą żarówką nowej trójki.

v – liczba trójek (ostatnia żarówka jest traktowana jako pierwsza żarówka następnej trójki)

q – numer trójki

p – pozycja danej żarówki w trójce

mlk – minimalna liczba kroków do zapalenia danej żarówki, lub stanu.

Spis twierdzeń

<u>$Twierdzenie\ 1$</u>

Każdy stan żarówek można zapisać w postaci stanu użytych przycisków.

<u>$Twierdzenie\ 2$</u>

Kolejność przyciskania przełączników jest nieważna.

<u>$Twierdzenie\ 3$</u>

Dla każdego N liczba stanów jest równa 2^N.

<u>$Twierdzenie\ 4$</u>

Gdy $N \equiv 0\ mod\ (3)$, lub $N \equiv 1\ mod\ (3)$ to stany dzielą się na jedną rodzinę, natomiast gdy $N \equiv 1\ mod\ (3)$ dzielą się one na dwie rodziny.

<u>$Twierdzenie\ 5$</u>

Dla $N \geq 3$ zawsze można zapalić co trzecią żarówkę, licząc od lewej lub prawej strony, lub innej zapalonej żarówki.

<u>$Twierdzenie\ 6$</u>

Jeżeli naciśniemy dany przełącznik parzystą ilość razy to nie zmienia to jego stanu, natomiast jeżeli zastanie naciśnięty nieparzystą ilość razy, jest to równoznaczne z jednorazowym wciśnięciem.

<u>$Twierdzenie\ 7$</u>

Dla ilości żarówek $N \equiv 0\ mod\ (3)$ można obliczyć mlk dla każdej żarówki korzystając ze wzorów:

$$mlk = \begin{cases} 2\frac{N}{3} - 2q + 2, & p = 1 \\ 2\frac{N}{3} + 1, & p = 2 \\ 2q, & p = 3 \end{cases}$$

Jeżeli $N \equiv 1\ mod\ (3)$ korzystając ze wzorów:

$$mlk = \begin{cases} N - \frac{N-1}{3}, & p = 1 \\ (N - v) - f(q), & p = 2 \\ 2q, & p = 3 \end{cases}$$

Natomiast gdy $N \equiv 2\ mod\ (3)$, wtedy jedynym regularnym wzorem będzie wzór na zapalenie co trzeciej żarówki zarówno od lewej jak i od prawej strony. Więc:

$$mlk = 2q$$

$\underline{Twierdzenie\ 8}$

Zaczynając od stanu początkowego możemy przejść do każdego stanu kiedy $N \equiv 0\ mod\ (3)$ *oraz* $N \equiv 1\ mod\ (3)$*, natomiast gdy* $N \equiv 2\ mod\ (3)$*, wtedy możemy przejść jedynie do jednej z rodzin, w której stan początkowy się znajduje.*

Bibliografia

- [Szk] Szkibiel, Grzegorz: Wstęp do teorii informacji i kodowania, Szczecin 2013
- [Urb] Urbański, Andrzej: Kryptografia na potrzeby Internetu, strona internetowa autora http://www.cs.put.poznan.pl/aurbanski/
- [KPiS] Konfiguracje prostych i stożkowych, praca zbiorowa, red. T. Szemberg. Wydawnictwo Szkolne Omega 2015
- [CLRS] Cormen, Thomas H., Leiserson, Charles E., Rivest, Ronald, Stein, Clifford: Wprowadzenie do algorytmów PWN 2013