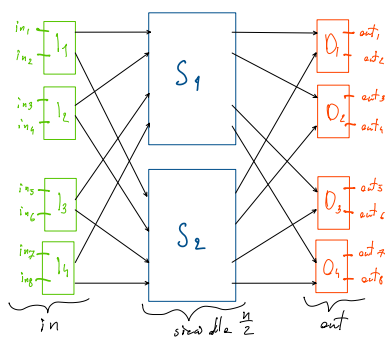


9. (2pkt) Jakże jest prawdopodobieństwo wygenerowania permutacji identycznościowej przez sieć Beneša Waksmana, w której przełączniki ustawiane są losowo i niezależnie od siebie w jednym z dwóch stanów (każdy stan przełącznika jest osiągany z prawdopodobieństwem  $1/2$ ).

2 składowy, jak wygląda taka sieć.



Chcemy uzyskać permutację identycznościową, zatem kodła dane na wejściu  $in_k$  musi opuścić układ wyjściem  $out_k$ .

2. Jeśli sygnał wejściowy do układu głównego wejściowego, opóźni go o jedną in, wyjściem. Jeśli trafi do  $S_2$ , to do  $out_k$  może dotrzeć tylko poprzez jego drugie wejście. Wtedy  $out_k$  musi mieć ten sam układ, co  $in_k$ , ten, na przykład na kąt.

Możemy ustalić, że stany odpowiedziałych sobie przełączników  $in_i$  i  $out_{i+k}$  są takie same.

Jeśli sygnał trafi do  $S_1$ , lub  $S_2$  przez  $i$ -te wejście, to przejdzie  $i$ -tego przełącznika wyjściowego. W takim razie, żeby uzyskać na  $i$ -tym przełączniku wyjściowym, musi wyjść  $i$ -tym wejściem. W takim razie przełącznik musi, być z sobą identyfikowalny.

### Wyznaczymy prawdopodobieństwo

Prawdopodobieństwa, by dwa wejścia ( $in$  i  $out$ ) miały ten sam stan wynosi  $\frac{1}{2}$  — dwa niezależne losy dało prostą, gdzie mamy 4 możliwości stanów. Mamy  $\frac{1}{2}$  prawdopodobieństwa w tych stanach, zatem  $\frac{1}{2}$  mamy prawdopodobieństwo  $(\frac{1}{2})^{\frac{n}{2}}$ . Podstawiając powyższe, że wartość rekurencyjna tego możemy rozwiązywać, prawdopodobieństwo tego oznaczmy  $P(\frac{n}{2})$ . Mamy dwa przełączniki w tym momencie, więc  $P(\frac{n}{2})^2$ . Wtedy dla  $n = 2^k$  mamy:

$$P(n) = \begin{cases} P(\frac{n}{2})^2 \cdot (\frac{1}{2})^{\frac{n}{2}}, & \text{w.p.p.} \end{cases}$$

$$\begin{aligned} P(n) &= P(\frac{n}{2})^2 \cdot (\frac{1}{2})^{\frac{n}{2}} = \left( P(\frac{n}{4})^2 \cdot (\frac{1}{2})^{\frac{n}{4}} \right)^2 \cdot (\frac{1}{2})^{\frac{n}{2}} = P(\frac{n}{4})^4 \cdot (\frac{1}{2})^{\frac{n}{2}} \cdot (\frac{1}{2})^{\frac{n}{2}} = \\ &= \left( P(\frac{n}{8})^2 \cdot (\frac{1}{2})^{\frac{n}{8}} \right)^4 \cdot (\frac{1}{2})^{\frac{n}{2}} \cdot (\frac{1}{2})^{\frac{n}{2}} = P(\frac{n}{8})^8 \cdot (\frac{1}{2})^{\frac{n}{2}} \cdot (\frac{1}{2})^{\frac{n}{2}} \cdot (\frac{1}{2})^{\frac{n}{2}} = \dots = \\ &= P(\frac{n}{2})^{\frac{n}{2}} \cdot \underbrace{(\frac{1}{2})^{\frac{n}{2}} \cdot \dots \cdot (\frac{1}{2})^{\frac{n}{2}}}_{\text{Też to } \log_2(n-1) \text{ wyrazów}} = (\frac{1}{2})^{\frac{n}{2}} \cdot (\frac{1}{2})^{\log_2(n-1) \cdot \frac{n}{2}} = (\frac{1}{2})^{\log_2(n) \cdot \frac{n}{2}} \end{aligned}$$

Ustalając ten wzór indukcyjnie.

$$\text{Teza: } P(2^k) = (\frac{1}{2})^{\log_2 2^k \cdot \frac{2^k}{2}} = (\frac{1}{2})^{k \cdot 2^{k-1}}$$

Podstawa:  $k=1$

$$P(2) = (\frac{1}{2})^{2^1} = (\frac{1}{2})^1 = \frac{1}{2} \quad \checkmark$$

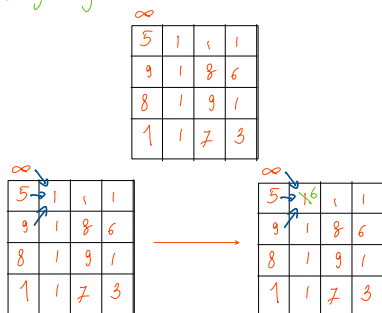
Krok: 2. Pokażemy, że teza jest spełniona dla  $k$  i pokazywać, że jeśli jest spełniona dla  $k-1$ .

$$P(2^{k+1}) = P(\frac{2^{k+1}}{2})^2 \cdot (\frac{1}{2})^{\frac{2^{k+1}}{2}} = \underbrace{P(2^k)^2}_{\text{ind.}} \cdot (\frac{1}{2})^{\frac{2^{k+1}}{2}} = (\frac{1}{2})^{k \cdot 2^{k-1} \cdot 2} \cdot (\frac{1}{2})^{\frac{2^{k+1}}{2}} = (\frac{1}{2})^{(k+1) \cdot 2^k}$$

### Lista 3

1. (1pkt) Ułóż algorytm znajdujący najtańszą drogę przejścia przez tablicę, w którym oprócz ruchów dopuszczalnych w wersji problemu prezentowanej na wykładzie, dozwolone są także ruchy w górę i w dół tablicy.

Przypomnienie metody z wykładu



Kodła komórek wykonują tablicę zawsze dopuszczającą się do najtańszej drogi, która nie ma przeszkód.

Algorytm:

1. Przenieś kolumnę cyfrową do tablicy (są to punkty startowe)

5			
9			
8			
1			

2. Pozostałe kolumny wypełnij licząc sumy wartości kolumny z lewej i jej trzech sąsiadów i wybierając z nich najmniejszą.

5	6		
9			
8			
1			

3. Wypełnij taką całą tabelę, wynik otrzymasz skłajając prawą kolumnę.

copy paste presentation.

3. (1.5pkt) Chcemy obliczać wartości współczynników dwumianowych modulo liczba pierwsza. Ułóż algorytm, który dla danej liczby pierwszej  $p$  oraz ciągu par  $(n_1, k_1), (n_2, k_2), \dots, (n_r, k_r)$  obliczy wartości  $\binom{n_i}{k_i} \bmod p$ . Twój algorytm powinien wypisywać wartości  $\binom{n_i}{k_i} \bmod p$  po czasie nie większym niż  $O(\max\{n_1, n_2, \dots, n_r\})$ .  
Możesz założyć, że  $k_i \leq n_i < p$  dla każdego  $i = 1, \dots, r$ .

```
N_max <- max(n_1, n_2, ...)  
factorials[0] <- 1  
  
for i from 1 to N_max do:  
    factorials[i] <- (factorials[i-1] * i) % p
```



```
inverse_p <- [1]  
for i from 2 to N_max do:  
    inverse_p <- (-floor(p / i) * inverse_p[p % i]) % p  
  
inverse_factorials[0] <- 1  
for i from 1 to N_max do:  
    inverse_factorials[i] <- (inverse_factorials[i-1] * inverse_p[i]) % p
```

```
pairs = [ [n_1, k_2], [n_2, k_2], ... [n_r, k_r] ]  
  
for i from 1 to r do:  
    n = pairs[i][0]  
    k = pairs[i][1]  
    print(factorials[n] * inverse_factorials[n - k] * inverse_factorials[k] % p)
```

