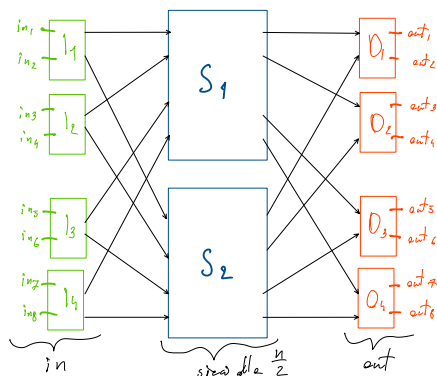


9. (2pkt) Jakie jest prawdopodobieństwo wygenerowania permutacji identycznościowej przez sieć Benesa-Waksmana, w której przełączniki ustawiane są losowo i niezależnie od siebie w jeden z dwóch stanów (każdy stan przełącznika jest osiągany z prawdopodobieństwem $1/2$).

Z obaczymy, jakie wygląda taka sieć.



Chcemy uzyskać permutację identycznościową, zatem każda dana na wejściu in_k musi wyjść w ten sam sposób co na wyjściu out_k .

Złóżmy sygnał wejściowy do układu głównego wyjściowego; spójnijmy oboje w ten sam sposób. Jest to trafia do S_1 , to do S_2 może dotrzeć tylko poprzez jego odpowiednie wejście. Wtedy out_k musi mieć ten sam układ, co in_k , ten, na którym było na końcu.

Możemy wnioskować, że istnieją odpowiednie sobie przełączniki in_i i out_i muszą być takie same.

Jestli sygnał trafia do S_1 lub S_2 przez i-te wejście, to przylatuje i-tego przełącznika wyjściowego. U takiego przełącznika, który wyszedł na i-tych przełączniku wyjściowym, musi wyjść i-tych wyjściem. U takiego przełącznika musi być ten sam układ identyfikacyjny.

Wyznaczymy prawdopodobieństwo

Prawdopodobieństwo, by oba wejścia (i i j) miały ten sam stan wynosi $\frac{1}{2}$ — oba nachodzą lub oba przebiegają, gośnią w ten sam sposób. Mamy $\frac{n}{2}$ przełączników w tych układach, zatem łączymy prawdopodobieństwo $\left(\frac{1}{2}\right)^{\frac{n}{2}}$. Podstawiamy, że wartość rzeczywista tego małego identyfikacyjnego, prawdopodobieństwo tego oznaczamy $P\left(\frac{n}{2}\right)$. Mamy dwa przełączniki w tym układzie, więc łączymy $P\left(\frac{n}{2}\right)^2$. Wtedy dla $n = 2^k$ mamy:

$$P(n) = \left(P\left(\frac{n}{2}\right)^2 \cdot \left(\frac{1}{2}\right)^{\frac{n}{2}} \right), \text{ w.p.p.}$$

$$P(n) = P\left(\frac{n}{2}\right)^2 \left(\frac{1}{2}\right)^{\frac{n}{2}} = \left(P\left(\frac{n}{4}\right)^2 \cdot \left(\frac{1}{2}\right)^{\frac{n}{4}} \right)^2 \left(\frac{1}{2}\right)^{\frac{n}{2}} = P\left(\frac{n}{4}\right)^4 \left(\frac{1}{2}\right)^{\frac{n}{2}} \cdot \left(\frac{1}{2}\right)^{\frac{n}{2}} =$$

$$= \left(P\left(\frac{n}{8}\right)^2 \cdot \left(\frac{1}{2}\right)^{\frac{n}{8}} \right)^4 \left(\frac{1}{2}\right)^{\frac{n}{2}} \cdot \left(\frac{1}{2}\right)^{\frac{n}{2}} = P\left(\frac{n}{8}\right)^8 \left(\frac{1}{2}\right)^{\frac{n}{2}} \cdot \left(\frac{1}{2}\right)^{\frac{n}{2}} = \dots =$$

$$= P\left(\frac{n}{2}\right)^{\frac{n}{2}} \cdot \left(\frac{1}{2}\right)^{\frac{n}{2}} \cdot \dots \cdot \left(\frac{1}{2}\right)^{\frac{n}{2}} = \left(\frac{1}{2}\right)^{\frac{n}{2}} \cdot \left(\frac{1}{2}\right)^{\frac{n}{2}} \cdot \log(n-1) \cdot \frac{n}{2} = \left(\frac{1}{2}\right)^{\log(n) \cdot \frac{n}{2}}$$

Wolno mówimy ten wzór indukcyjnie.

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

Podstawa: $k=1$

$$P(2) = \left(\frac{1}{2}\right)^{2^0} = \left(\frac{1}{2}\right)^1 = \frac{1}{2} \quad \checkmark$$

Krok: Zauważ, że tego potrzebujemy dla k i pokazujemy, że dotyczy jest $k+1$ o ile k jest prawdziwe.

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

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 w tablicy.

Przypomnienie metody z wykładu

5	1	1	1
9	1	8	6
8	1	9	1

Algorithm:

1. Pierwsza kolumna cytowania: liczebni z tabeli (sego punkty statowe)

2. Proszę koniecznie wypełnić wszystkie wartości komórek z kolumny z jej tytuł.

2. (1.5pkt) Ułóż algorytm, który dla danego ciągu znajduje długość najdłuższego jego podciaga, który jest palindromem.

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 $i = 1, \dots, r$.

```
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)
```