

Uniwersytet Wrocławski
Wydział Matematyki i Informatyki
Instytut Matematyczny

Maksymilian Adamczewski i Jadwiga Świerczyńska

Sieci przełączników

Praca zespołowa
napisana pod opieką
dr. hab. Jana Dymary, prof. UWr

Wrocław, 2023 r.

Streszczenie

W poniższej pracy przedstawiamy definicje przełącznika oraz sieci przełączników. Najpierw pokazujemy konstrukcje sieci realizujących symetrię, przesunięcie cykliczne czy dowolną permutację. Następnie przedstawiamy konstrukcję sieci Beneša–Waksmana realizującą wszystkie permutacje oraz jej optymalizację. Na końcu konstruujemy sieć realizującą wszystkie przesunięcia cykliczne oraz przesunięcia cykliczne o potęgi 2.

Spis treści

1	Wprowadzenie	3
2	Podstawy	3
2.1	Definicje	3
2.2	Najprostsze sieci	6
3	Sieć Beneša–Waksmana	8
3.1	Ograniczenie dolne	8
3.2	Konstrukcja i dowód poprawności	9
3.3	Optymalizacja	12
4	Sieć realizująca wszystkie przesunięcia cykliczne	12
4.1	Konstrukcja i poprawność	12
4.2	Rozmiar i głębokość	12
5	Sieć realizująca przesunięcia cykliczne o potęgi 2	12
5.1	Zmiana sposobu reprezentacji ciągu	13
5.2	Przesunięcia cykliczne o duże 2^k	13
5.3	Przesunięcia cykliczne o małe 2^k	14
5.4	Konstrukcja sieci	14
5.5	Głębokość i rozmiar	15

1 Wprowadzenie

Sieci przełączników to struktury, które można zinterpretować jako urządzenia zbudowane z tzw. *przełączników* pozwalające na permutowanie n rozróżnialnych sygnałów danych na wejściu. Naturalne jest, że dążymy do optymalizacji struktury sieci pod względem liczby użytych przełączników lub maksymalnej liczby przełączników, przez jakie przepływa sygnał w sieci. Jednakże ze względu na wysoce wyspecjalizowane zastosowania (m. in. sieci telefoniczne, trasowanie pakietów) brakuje źródeł wyczerpująco tłumaczących to zagadnienie w sposób przystępny na przykład dla studenta drugiego roku informatyki. W tej pracy przybliżymy podstawowe definicje (rozdział 2), przedstawimy konstrukcję najsłynniejszej sieci realizującej wszystkie permutacje, czyli sieci Beneša–Waksmana (rozdział 3), sieci realizującej wszystkie przesunięcia cykliczne (rozdział 4) i sieci realizującej przesunięcia cykliczne o potęgę 2 (rozdział 5).

Zastrzegamy jednak, że za względu na cel pracy, polegający na przystępnym przybliżeniu tematu, przy formułowaniu definicji i konstrukcji będziemy skupiać się na intuicji. Precyzyjną matematyczną formalizację pozostawimy jako ćwiczenie dla Czytelnika, które okaże się schematycznym zadaniem, gdy już się zrozumie idee stojące za sieciami przełączników.

Przez S_n będziemy oznaczać zbiór wszystkich permutacji $\{0, 1, \dots, n-1\}$, przez

$$\text{shift}_k^n : \{0, 1, \dots, n-1\} \rightarrow \{0, 1, \dots, n-1\}$$

permutację $\text{shift}_k^n(i) = (k+i) \bmod n$, a przez

$$\text{sym}_k^n : \{0, 1, \dots, n-1\} \rightarrow \{0, 1, \dots, n-1\}$$

permutację $\text{sym}_k^n(i) = (k-i) \bmod n$, natomiast przez

$$\text{id}_n : \{0, 1, \dots, n-1\} \rightarrow \{0, 1, \dots, n-1\}$$

permutację identycznościową.

Ponadto stosujemy następujące oznaczenia złożoności asymptotycznej (podobnie jak w [2]).

Definicja 1.1. Dla danych funkcji $f, g : \mathbb{N} \rightarrow \mathbb{R}$ mówimy, że:

- $f = O(g)$, gdy istnieją $n_0 \in \mathbb{N}$, $c > 0$, takie że

$$0 \leq f(n) \leq cg(n) \text{ dla wszystkich } n \geq n_0,$$

- $f = \Omega(g)$, gdy istnieją $n_0 \in \mathbb{N}$, $c > 0$, takie że

$$0 \leq cg(n) \leq f(n) \text{ dla wszystkich } n \geq n_0,$$

- $f = \Theta(g)$, gdy istnieją $n_0 \in \mathbb{N}$, $c_1 > 0$, $c_2 > 0$, takie że

$$0 \leq c_1g(n) \leq f(n) \leq c_2g(n) \text{ dla wszystkich } n \geq n_0.$$

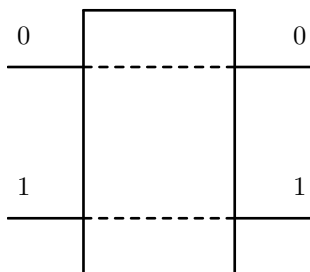
2 Podstawy

2.1 Definicje

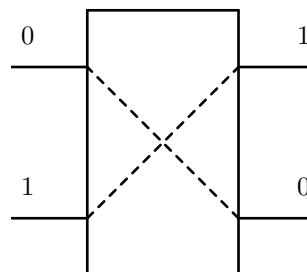
Zacznijmy od najistotniejszej dla tej pracy kwestii – czyli definicji przełącznika.

Przełącznikiem nazywamy urządzenie mające dwa wejścia (oznaczone liczbami 0 i 1) i dwa wyjścia (oznaczone liczbami 0 i 1). Może się znaleźć w dwóch stanach:

- nieaktywnym – sygnał z wejścia i trafia do wyjścia i (dla $i \in \{0, 1\}$),
- aktywnym – sygnał z wejścia i trafia do wyjścia $(i + 1) \bmod 2$ (dla $i \in \{0, 1\}$).



Przełącznik w stanie nieaktywnym



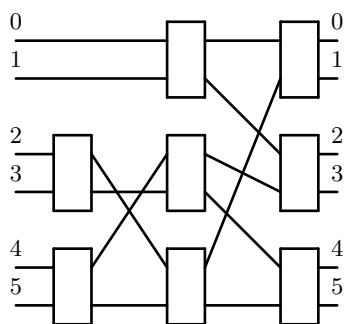
Przełącznik w stanie aktywnym

Przełączniki w naturalny sposób możemy ze sobą łączyć **przewodami** – sygnał z wyjścia jednego przełącznika może zostać przekierowany przewodem na wejście innego przełącznika.

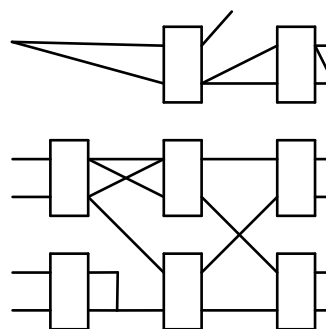
Połączone przewodniki tworzą **sieć przełączników**. Dokładniej, siecią przełączników o n wejściami i n wyjściami nazywamy zbiór przełączników i przewodów, w którym:

- z każdego wyjścia przełącznika w sieci wychodzi dokładnie jeden przewód,
- do każdego wejścia przełącznika w sieci wchodzi dokładnie jeden przewód,
- z każdego wejścia sieci wychodzi dokładnie jeden przewód,
- do każdego wyjścia sieci wchodzi dokładnie jeden przewód,
- żaden przewód nie jest podłączony dwoma końcami do tego samego przełącznika,
- wejście każdego przewodu jest wpięte do wyjścia pewnego przełącznika lub do wejścia sieci,
- wyjście każdego przewodu jest wpięte do wejścia pewnego przełącznika lub do wyjścia sieci,
- mamy n wejść i n wyjść sieci.

Ponadto wejścia i wyjścia sieci numerujemy liczbami od 0 do $n - 1$.



Przykład sieci przełączników

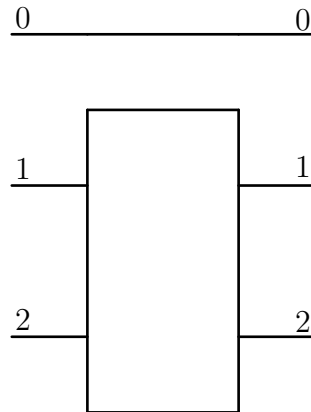


Przykład przełączników połączonych przewodami, które nie tworzą sieci przełączników

Definicja 2.1. Mówimy, że sieć przełączników o n wejściach i n wyjściach realizuje permutację $\sigma \in S_n$, gdy każdemu przewodnikowi możemy nadać stan (aktywny lub nieaktywny) tak, by dla sygnałów w kolejności $0, 1, \dots, n - 1$ na wejściu otrzymać sygnały w kolejności $\sigma(0), \sigma(1), \dots, \sigma(n - 1)$ na wyjściu.

TODO: sieć realizująca jakąś małą permutację

TODO: sieć, która nie może zrealizować jakiejś permutacji



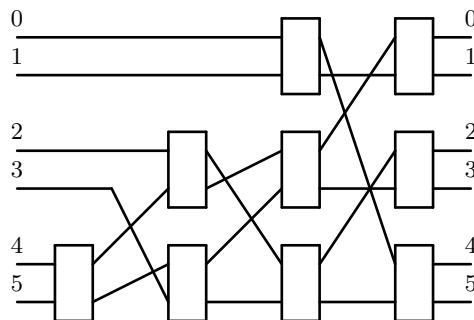
Przykład sieci która nie realizuje permutacji.

Definicja 2.2. Rozmiar sieci to liczba przełączników w sieci.

Definicja 2.3. Mówimy, że sieć przełączników o n wejściach i n wyjściach ma głębokość równą $d \in \mathbb{N}$, gdy

- dla dowolnego przypisania przełącznikom w stanów aktywny/nieaktywny i dowolnego $i \in \{0, 1, \dots, n - 1\}$ sygnał z wejścia i -tego przechodzi przez co najwyżej d przełączników oraz
- d jest najmniejszą liczbą o tej własności.

W celu zilustrowania powyższych definicji zamieszczamy sieć o rozmiarze równym 9 i głębokości równej 4 (ponieważ np. sygnał z wejścia o numerze 5 może przejść przez 4 przełączniki, natomiast żaden sygnał nie może przejść przez więcej niż 4 przełączniki).



2.2 Najprostsze sieci

Zastanówmy się najpierw, czy istnieje sieć o 6 wejściach i 6 wyjściach mająca rozmiar równy 9, która realizuje wszystkie permutacje z S_6 ?

Odpowiedź to nie – łatwo zauważyć, że każdy przełącznik zwiększa liczbę permutacji realizowanych przez sieć co najwyżej dwukrotnie. Wobec tego taka sieć realizuje co najwyżej $2^9 = 512$ permutacji. Zarazem $6! = 720 > 512$, czyli taka sieć nie może istnieć.

Jakie sieci zatem istnieją? W poniższych rozważaniach pochylimy się nad sieciami głębokości co najwyżej 2 realizującymi identyczność i pewną inną permutację. Konstrukcje tych sieci przeprowadzamy tak, jak autorzy pracy [1]. Będą one pomocne przy tworzeniu sieci realizującej przesunięcia cykliczne o potęgach 2.

Lemat 2.4. *Dla dowolnego n oraz $k \in \{0, 1, \dots, n-1\}$ istnieje sieć o n wejściach i n wyjściach o głębokości 1 i rozmiarze co najwyżej $\lfloor \frac{n}{2} \rfloor$ realizująca id_n i sym_k^n .*

Dowód. Ustalmy n oraz $k \in \{0, 1, \dots, n-1\}$. Zauważmy, że

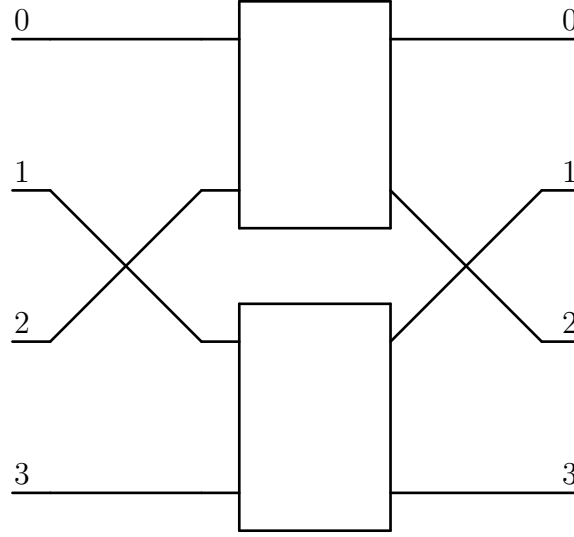
$$\text{sym}_k^n \circ \text{sym}_k^n = \text{id}_n.$$

Wobec tego permutacja sym_k^n jest inwolucją, a co za tym idzie – składa się z cykli o rozmiarze co najwyżej 2. Konstrukcja sieci wygląda następująco:

- każdemu cyklowi postaci (i, j) przypisujemy przełącznik, który na wejściach przyjmuje sygnały i oraz j z wejścia sieci, a przewody na jego wyjściach prowadzą do wyjść sieci o numerach i oraz j ,
- każdemu cyklowi jednoelementowemu postaci (i) przypisujemy przewód biegnący od i -tego wejścia do i -tego wyjścia sieci.

Oczywiście w ten sposób używamy co najwyżej $\lfloor \frac{n}{2} \rfloor$ przełączników. Ponadto jeśli wszystkie przełączniki są w stanie nieaktywnym, sieć realizuje id_n , natomiast jeśli wszystkie są w stanie aktywnym, to realizuje sym_k^n . \square

Zaobserwujmy konstrukcję z lematu 2.4 dla $n = 4$ i $k = 2$.



Lemat 2.4 można jednak uogólnić – zauważmy, że nie korzystamy z żadnych własności symetrii, poza tym, że $\text{sym}_k^n \circ \text{sym}_k^n = \text{id}_n$.

Lemat 2.5. *Dla dowolnego n oraz $\sigma \in S_n$, które jest inwolucją (to znaczy $\sigma \circ \sigma = \text{id}_n$) istnieje sieć o n wejściach i n wyjściach o głębokości 1 i rozmiarze co najwyżej $\lfloor \frac{n}{2} \rfloor$ realizująca id_n oraz σ .*

Dowód. Konstrukcja jest identyczna jak ta w lemacie 2.4. □

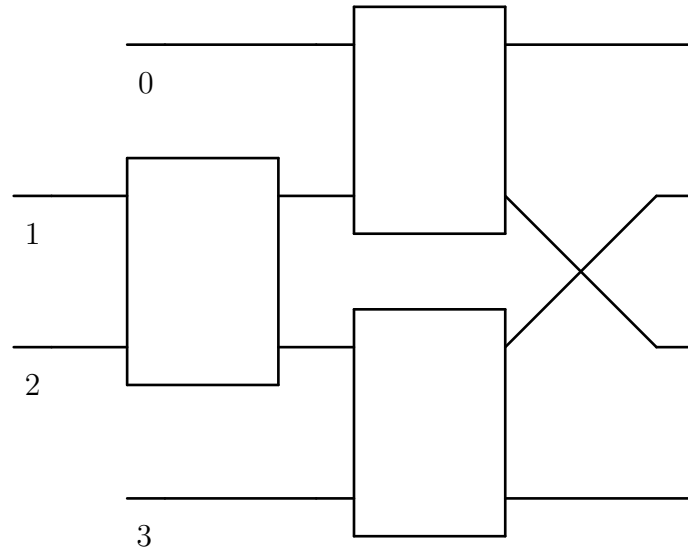
Lemat 2.6. *Dla dowolnego n oraz $k \in \{0, 1, \dots, n-1\}$ istnieje sieć o n wejściach i n wyjściach o głębokości 2 realizująca id_n i shift_k^n .*

Dowód. Ustalmy n . Zauważmy, że

$$\text{sym}_k^n(\text{sym}_0^n(i)) = \text{sym}_k^n(-i \bmod n) = (k - (-i)) \bmod n = (k + i) \bmod n = \text{shift}_k^n(i)$$

dla każdego $i \in \{0, 1, \dots, n-1\}$. Wobec tego $\text{shift}_k^n = \text{sym}_k^n \circ \text{sym}_0^n$. Stwórzmy zatem sieć przełączników o dwóch warstwach – pierwsza z nich niech będzie siecią realizującą id_n i sym_0^n , a druga siecią realizującą id_n i sym_k^n (jak w lemacie 2.4). Taka sieć ma głębokość 2. Jeśli wszystkie przełączniki są nieaktywne, to realizuje id_n , natomiast jeśli wszystkie są aktywne, to z powyższego rachunku wynika, że realizuje shift_k^n . □

TODO: przykład konstrukcji



TODO: poprawić!

Lemat 2.7. Dla dowolnego n oraz $\sigma \in S_n$ istnieje sieć o n wejściach i n wyjściach o głębokości 2 realizująca id_n i σ .

Dowód. Ustalmy n oraz $\sigma \in S_n$. Oczywiście σ może być przedstawiona jako złożenie cykli rozłącznych:

$$\sigma = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_k.$$

Prostą konsekwencją lematu 2.6 jest to, że istnieje sieć o głębokości 2, która realizuje id_n oraz σ_i dla każdego i . Konstrukcja żądanej sieci polega na złożeniu tych sieci dla każdego σ_i . Z rozłączności cykli wynika, że będzie miała ona głębokość równą 2. \square

3 Sieć Beneša–Waksmana

W tym rozdziale będziemy zajmować się siecią, która realizuje wszystkie możliwe permutacje dla ustalonego n . Dla uproszczenia przyjmujemy, że $n = 2^k$ dla pewnego $k \in \mathbb{N}$.

3.1 Ograniczenie dolne

Najpierw zastanówmy się nad ograniczeniem dolnym – czy istnieje asymptotyczne oszacowanie minimalnej liczby przełączników potrzebnych do zrealizowania wszystkich permutacji z S_n ?

Twierdzenie 3.1. Dowolna sieć, która realizuje wszystkie permutacje z S_n , ma $\Omega(n \log n)$ przełączników.

Dowód. Ustalmy $n \in \mathbb{N}$ i sieć realizującą wszystkie permutacje z S_n . Oznaczmy liczbę przełączników w tej sieci przez p . Zauważmy, że każdy przełącznik, zwiększa liczbę realizowanych permutacji co najwyżej dwukrotnie. Wobec tego $\log(n!) \leq p$. Ze wzoru Stirlinga z możemy oszacować $n!$ z dołu przez $(n/e)^n$. Otrzymujemy zatem

$$\log(n!) \geq \log((n/e)^n) = n(\log n - \log e) = \Omega(n \log n)$$

\square

3.2 Konstrukcja i dowód poprawności

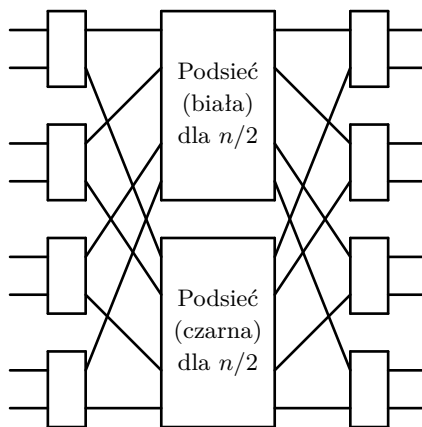
Konstrukcja polega na podzieleniu problemu na dwa identyczne podproblemy i pomysłowym połączeniu odpowiadających im podsieci w pełne rozwiązanie.

Ustalmy n . Rekurencyjnie konstruujemy dwie identyczne sieci realizujące wszystkie permutacje z $S_{n/2}$. Jedną z nich nazwijmy *białą*, a drugą *czarną*.

Tworzymy warstwę wejściową przewodników. Przewody z n wejść sieci kierujemy do $n/2$ przewodników w taki sposób, że do k -tego przełącznika trafiają przewody z wyjść $2k$ (na wejście 0) oraz $2k + 1$ (na wejście 1) dla $k = 0, 1, \dots, n/2 - 1$. Natomiast z przewody z wyjścia 0 i 1 k -tego przewodnika kierujemy do k -tego wejścia odpowiednio białej i czarnej podsieci.

Analogicznie tworzymy warstwę wyjściową przełączników. Dokładniej kładziemy $n/2$ przełączników tak, że przewody z wyjścia 0 i 1 k -tego przewodnika prowadzą odpowiednio do wyjść sieci o numerach $2k$ i $2k + 1$. Natomiast do wejść 0 i 1 k -tego przewodnika prowadzimy przewód z k -tego wyjścia odpowiednio białej i czarnej podsieci.

Konstrukcję schematycznie przedstawiono na poniższym rysunku.



Twierdzenie 3.2. Sieć Beneša–Waksmiana realizuje wszystkie permutacje.

Dowód. Przeprowadzimy dowód przez indukcję, korzystając z rekurencyjnej struktury sieci.

1. Podstawa indukcji dla $n = 1$ oraz $n = 2$.
Dla $n = 1$ sieć Beneša–Waksmiana jest prostu przewodem. Z kolei dla $n = 2$ jest to pojedynczy przełącznik.
2. Krok indukcyjny. Weźmy dowolne $n = 2^k$ dla pewnego k naturalnego i założmy, że sieć dla $n/2$ konstruowana w sposób opisany powyżej realizuje wszystkie permutacje $n/2$ -elementowe. Ustalmy $\pi \in S_n$.

Zauważmy, że wystarczy wskazać podział zbioru $\{0, 1, \dots, n - 1\}$ na dwa podzbiory $n/2$ -elementowe (nazwijmy je *białym* i *czarnym*) o następującej własności: dla dowolnego $k = 0, 1, \dots, n/2 - 1$ liczby $2k$ i $2k + 1$ należą do różnych zbiorów podziału oraz analogicznie liczby $\pi(2k)$ i $\pi(2k + 1)$ należą do różnych zbiorów podziału.

Istotnie – zakładając, że istnieje taki podział, ustawienie przełączników realizujące π wygląda następująco:

- jeśli $2k$ jest w białym zbiorze, a $2k+1$ w czarnym, to k -temu przełącznikowi z warstwy wejściowej nadajemy stan nieaktywny,
- w przeciwnym przypadku k -temu przełącznikowi z warstwy wyjściowej nadajemy stan aktywny.

dla $k = 0, 1, \dots, n/2 - 1$. Analogicznie nadajemy stan k -temu przełącznikowi na wyjściu:

- jeśli $\pi(2k)$ jest w białym zbiorze, a $\pi(2k+1)$ w czarnym, to k -temu przełącznikowi nadajemy stan nieaktywny,
- w przeciwnym przypadku k -temu przełącznikowi nadajemy stan aktywny.

Natomiast o właściwe ustawienie liczb wewnątrz *białego* i *czarnego* zbioru „zadbają” rekurencyjnie skonstruowane sieci.

Stwórzmy zatem podział spełniający powyższe warunki.

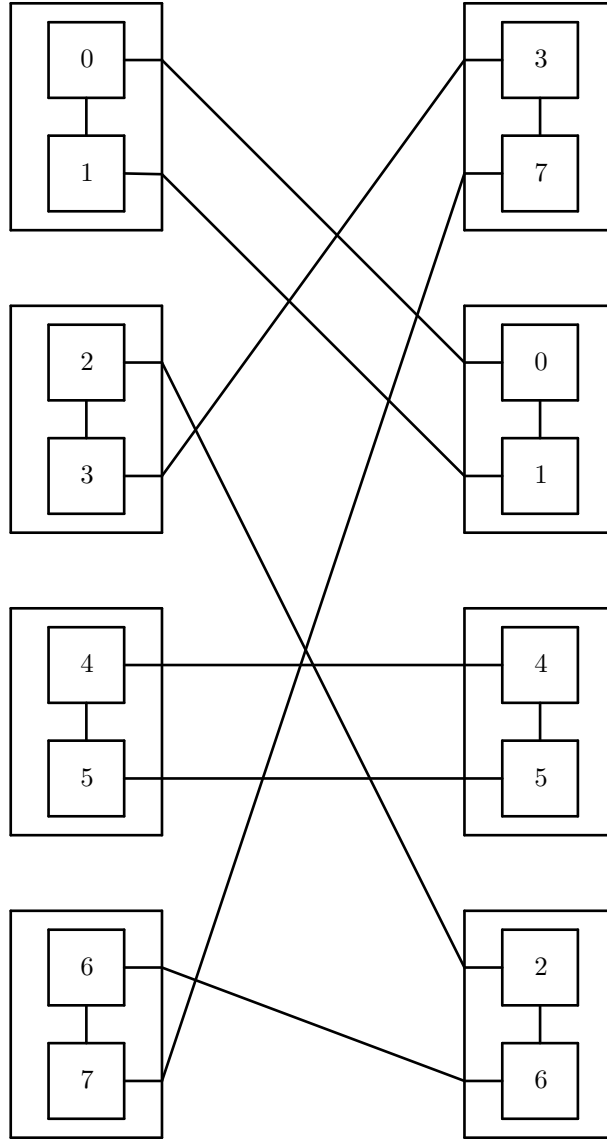
Niech $V_i = \{0, 1, \dots, n-1\}$ będzie zbiorem wierzchołków odpowiadających portom wejściowym sieci (j -ty port wejściowy utożsamiamy z wierzchołkiem j). Łączymy ze sobą wierzchołki, które odpowiadają wejściom tego samego przełącznika z warstwy wejściowej. Dokładniej łączymy krawędzią wierzchołki 0 i 1 , 2 i 3 , \dots , $n-2$ i $n-1$.

Niech $V_o = \{0', 1', \dots, (n-1)'\}$ będzie zbiorem wierzchołków, które odpowiadają portom wyjściowym sieci (j -ty port wyjściowy utożsamiamy z k' , takim że $\pi(j) = k$). Łączymy krawędzią te, które są ze sobą w jednym przełączniku w warstwie wyjściowej (czyli $\pi(2j)'$ oraz $\pi(2j+1)'$ dla $j = 0, 1, \dots, n/2 - 1$).

Ponadto łączymy krawędzią wierzchołki o etykietach j oraz j' .

Poniżej przedstawiamy schematyczny graf dla $n = 8$ oraz

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 0 & 1 & 4 & 5 & 2 & 6 \end{pmatrix}.$$



Zauważmy teraz, że w tak powstałym grafie każdy wierzchołek ma stopień dokładnie 2. W związku z tym graf ten jest sumą cykli. Ponadto każdy cykl ma parzystą długość – jeśli pewien wierzchołek należy do cyklu, to należy do niego także jego „sąsiad” z przełącznika.

Wobec tego graf stworzony opisanymi wyżej regułami jest dwukolorowalny. Ustalmy zatem pewne kolorowanie na kolor *biały* i *czarny*. Otrzymujemy w ten sposób podział wierzchołków z V_i na zbiór wierzchołków *białych* i *czarnych*. Jest to podział spełniający wymagania opisane wyżej. Istotnie: dla każdego $j = 0, 1, \dots, n/2 - 1$ dzięki krawędziom pomiędzy wierzchołkami z V_i zapewniamy, że liczby $2j$ oraz $2j+1$ należą do różnych zbiorów podziału, natomiast dzięki krawędziom pomiędzy wierzchołkami z V_o zapewniamy, że $\pi(2j)$ oraz $\pi(2j+1)$ należą do różnych zbiorów podziału.

Zatem permutacja π może być zrealizowana przez sieć Beneša–Waksmana.

□

TODO: obrazek do dwukolorowania

TODO: Przykład małej sieci

3.3 Optymalizacja

Zauważmy, że można usunąć po jednym przełączniku na każdym rekurencyjnym poziomie sieci. Istotnie, w dowodzie powyżej ustaliliśmy *dowolne* dwukolorowanie skonstruowanego grafu. Możemy jednak narzucić kolor wierzchołków w jednym przełączniku z warstwy wejściowej lub wyjściowej, np. ustalamy, że $0 \in V_i$ ma kolor *biały* oraz $1 \in V_i$ ma kolor *czarny*. Wówczas nie potrzebujemy zerowego przełącznika w warstwie wejściowej, gdyż możemy po prostu poprowadzić przewód z zerowego wejścia sieci do *białej* podsieci oraz ten z pierwszego wejścia sieci do *czarnej* podsieci.

4 Sieć realizująca wszystkie przesunięcia cykliczne

Zastanówmy się teraz nad konstrukcją sieci, które realizują dowolne przesunięcia cykliczne. Dokładniej dla ustalonego $n \in \mathbb{N}$ chcemy stworzyć sieć realizującą $\{\text{shift}_0^n, \text{shift}_1^n, \dots, \text{shift}_{n-1}^n\}$.

Fakt 4.1. Dla dowolnych $n, a, b \in \mathbb{N}$ zachodzi

$$\text{shift}_a^n \circ \text{shift}_b^n = \text{shift}_{a+b}^n.$$

4.1 Konstrukcja i poprawność

Skonstruujmy sieć w następujący sposób: złożmy ze sobą sieci realizujące $\text{shift}_{2^0}^n, \text{shift}_{2^1}^n, \dots, \text{shift}_{2^k}^n$ dla k , takiego że $2^k < n$ (sieci z lematu 2.6).

Ustalmy teraz $j \in \{0, 1, \dots, n-1\}$. Aby zrealizować shift_j^n należy aktywować sieci realizujące $\text{shift}_{2^l}^n$, takie że na l -tej pozycji w zapisie binarnym j występuje jedynka. Z faktu 4.1 wynika, że w ten sposób zrealizujemy shift_j^n .

4.2 Rozmiar i głębokość

Zauważmy, że stwarzamy $\Theta(\log n)$ podsieci, a każda z nich ma rozmiar $\lfloor \frac{n}{2} \rfloor$ i głębokość 1. Wobec tego rozmiar skonstruowanej sieci wynosi $\Theta(n \log n)$, a głębokość $\Theta(\log n)$.

TODO: Zrobić rysunek tej sieci

5 Sieć realizująca przesunięcia cykliczne o potęgach 2

W tym rozdziale chcemy zastanowić się nad konstrukcją sieci o n wejściach i n wyjściach realizującej przesunięcia cykliczne o potęgach 2 nie większe niż n , to znaczy chcemy zrealizować zbiór

$$\text{TwoShift}_n = \{\text{id}_n, \text{shift}_{2^0}^n, \text{shift}_{2^1}^n, \dots, \text{shift}_{2^l}^n\},$$

gdzie $2^l \leq n$ oraz $2^{l+1} > n$. Dla uproszczenia przyjmujemy, że $n = 2^{2^r}$ dla pewnego $r \in \mathbb{N}$ i oznaczmy $m = \sqrt{n} = 2^{2^{r-1}}$. Uogólnienie konstrukcji dla dowolnego $n \in \mathbb{N}$ zostało przedstawione w [1].

5.1 Zmiana sposobu reprezentacji ciągu

W tym rozdziale będziemy wyobrażać sobie zbiór $\{0, 1, 2, \dots, n-1\}$ jako macierz o wymiarach $m \times m$ – to uzasadnia wybór n , które jest kwadratem liczby naturalnej. Na przykład dla $r = 2$ mamy $n = 2^{2^2} = 2^4 = 16$, a macierzowa reprezentacja zbioru wygląda następująco:

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Zastanówmy się teraz, jak wyglądają przesunięcia cykliczne o 2^k w tej reprezentacji.

5.2 Przesunięcia cykliczne o duże 2^k

Gdy 2^k jest *duże*, to znaczy $2^k \geq m$ (równoważnie $k \geq 2^{r-1}$), to $m \mid 2^k$. Wobec tego $\text{shift}_{2^k}^n$ jest przesunięciem cyklicznym o $2^k/m = 2^k/2^{2^{r-1}} = 2^{k-2^{r-1}}$ na zbiorze wierszy. Na przykład dla $n = 64 = 2^{2^3}$ oraz $2^k = 2^4 = 2 \cdot \sqrt{64}$ mamy

0	1	2	...	7
8	9	10	...	15
...	
48	49	50	...	55
56	57	58	...	63

Zbiór przed wykonaniem shift_{16}^{64} .

16	17	18	...	23
24	25	26	...	31
...	
56	57	58	...	63
0	1	2	...	7
8	9	10	...	15

Zbiór po wykonaniu shift_{16}^{64} .

Możemy także pomyśleć o tym nieco inaczej. Dokładniej, $\text{shift}_{2^k}^n$ może być wykonany w 3 etapach:

1. transpozycja macierzy,
2. $\text{shift}_{2^k/m}^m$ na wierszach tak otrzymanej macierzy,
3. transpozycja macierzy.

Przeanalizujmy to na powyższym przykładzie – $n = 64$ oraz $2^k = 16$.

0	1	2	...	7
8	9	10	...	15
...	
48	49	50	...	55
56	57	58	...	63

Początkowy zbiór.

0	8	16	...	56
1	9	17	...	57
...	
6	14	22	...	62
7	15	23	...	63

Zbiór po wykonaniu transpozycji.

16	24	...	0	8
17	25	...	1	9
...	
22	30	...	6	14
23	31	...	7	15

Zbiór po wykonaniu shift_2^8 na wierszach macierzy.

16	17	...	22	23
24	25	...	30	31
...	
0	1	...	6	7
8	9	...	14	15

Zbiór po wykonaniu transpozycji.

5.3 Przesunięcia cykliczne o małe 2^k

Co się dzieje, gdy 2^k jest *małe* (to znaczy $2^k < m$)? Wtedy zmiany w układzie liczb zachodzą także wewnątrz wierszy. Istotnie – $\text{shift}_{2^k}^n$ możemy wówczas przedstawić jako dwa etapy:

1. $\text{shift}_{2^k}^m$ wewnątrz każdego wiersza,
2. shift_1^m wewnątrz ostatnich 2^k kolumn.

Przyjrzyjmy się tym etapom na przykładzie – niech $n = 64$ oraz $2^k = 2$.

0	1	2	...	7
8	9	10	...	15
...	
48	49	50	...	55
56	57	58	...	63

Początkowy zbiór.

2	3	...	0	1
10	11	...	8	9
...	
50	51	...	48	49
58	59	...	56	57

Zbiór po wykonaniu shift_2^8 na każdym wierszu.

2	3	...	7	0	1
10	11	...	15	8	9
...	
50	51	...	56	48	49
58	59	...	63	56	57

Kolumny, na których należy wykonać shift_1^8 .

2	3	...	8	9
10	11	...	16	17
...	
50	51	...	56	57
58	59	...	0	1

Zbiór po wykonaniu shift_1^8 na 2 ostatnich kolumnach.

5.4 Konstrukcja sieci

Podsumowując, przesunięcia cykliczne o 2^k realizujemy w następujący sposób:

- gdy 2^k jest małe, wykonujemy $\text{shift}_{2^k}^m$ wewnątrz każdego wiersza, a następnie shift_1^m wewnątrz ostatnich 2^k kolumn,
- gdy 2^k jest duże, transponujemy macierz, wykonujemy $\text{shift}_{2^k/m}^m$ na wierszach i znowu transponujemy macierz.

To pozwala już sformułować przybliżoną konstrukcję sieci. Aby skonstruować P_n – sieć realizującą TwoShift_n , potrzebujemy następujących podsieci (zwanych dalej *blokami*):

- sieci realizującej transpozycję i id_n (oznaczymy ją T_1),

- m sieci realizujących TwoShift_m – czyli m kopii sieci P_m (nazwijmy je *blokiem wierszowym*),
- m sieci realizujących shift_1^m oraz id_m dla każdej kolumny, takich jak w lemacie 2.6 – nazwijmy je *blokiem kolumnowym*
- oraz drugiej sieci realizującej transpozycję i id_n (oznaczmy ją T_2).

TODO: schematyczny rysunek bloków

Oczywiście transpozycja jest inwolucją – w związku z tym sieci T_1 i T_2 mogą zostać utworzone tak jak w lemacie 2.5. W terminach tak skonstruowanej sieci zrealizowanie przesunięcia cyklicznego o 2^k wygląda następująco:

- gdy 2^k jest małe, aktywujemy blok wierszowy, tak by wykonał $\text{shift}_{2^k}^m$ na każdym wierszu, a następnie aktywujemy blok kolumnowy, tak by wykonał shift_1^m na ostatnich 2^k kolumnach,
- gdy 2^k jest duże, aktywujemy sieć T_1 , tak by wykonała transpozycję, aktywujemy blok wierszowy, tak by wykonał $\text{shift}_{2^k/m}^m$ na każdym wierszu, a na końcu aktywujemy sieć T_2 , tak by wykonała transpozycję.

5.5 Głębokość i rozmiar

Udało nam się skonstruować sieć realizującą TwoShift_n . Zbadajmy teraz jej głębokość i rozmiar.

Lemat 5.1. *Sieć przedstawiona wyżej ma głębokość równą $D(n) = \Theta(\log \log n)$.*

Dowód. Zauważmy, że zarówno blok T_1 , jaki i blok T_2 , mają głębokość równą 1. Blok kolumnowy ma głębokość równą 2, a blok wierszowy – $D(m) = D(\sqrt{n})$. Wobec tego głębokość sieci wyraża się następującym równaniem rekurencyjnym:

$$D(n) = D(\sqrt{n}) + O(1).$$

Do rozwiązania tej rekurencji zastosujemy metodę podstawiania. Niech $s = \log n$. Mamy wówczas

$$D(2^s) = D(2^{s/2}) + O(1).$$

Oznaczmy $B(s) = D(2^s)$. Dla B rekurencja przedstawia się następująco:

$$B(s) = B\left(\frac{s}{2}\right) + O(1).$$

Na mocy twierdzenia o rekurencji uniwersalnej (ang. *master theorem*, [2]) otrzymujemy

$$B(s) = \Theta(\log s),$$

a zapisując powyższą równość w terminach D , dostajemy

$$D(n) = D(2^s) = B(s) = \Theta(\log s) = \Theta(\log \log n).$$

□

Lemat 5.2. *Sieć przedstawiona wyżej ma rozmiar równy $S(n) = \Theta(n \log \log n)$.*

Dowód. Zauważmy, że sieci T_1 i T_2 mają rozmiar równy $\left\lfloor \frac{n-\sqrt{n}}{2} \right\rfloor$. Ponadto rozmiar całego bloku kolumnowego wynosi co najwyżej $m \cdot \frac{m}{2} \cdot 2$, gdzie $m = \sqrt{n}$, a rozmiar bloku wierszowego to $mS(m)$. Otrzymujemy zatem następujące równanie rekurencyjne

$$S(n) = 2 \cdot \left\lfloor \frac{n-\sqrt{n}}{2} \right\rfloor + O\left(\sqrt{n} \cdot \frac{\sqrt{n}}{2} \cdot 2\right) + \sqrt{n}S(\sqrt{n}) = \sqrt{n}S(\sqrt{n}) + \Theta(n).$$

Przypomnijmy, że $n = 2^{2^r}$. Mamy zatem równoważnie

$$\begin{aligned} S(2^{2^r}) &= 2^{2^{r-1}} S(2^{2^{r-1}}) + \Theta(2^{2^r}) \\ &= 2^{2^{r-1}} \left(2^{2^{r-2}} S(2^{2^{r-2}}) + \Theta(2^{2^{r-1}}) \right) + \Theta(2^{2^r}) \\ &= 2^{2^{r-1}+2^{r-2}} S(2^{2^{r-2}}) + 2^{2^{r-1}} \Theta(2^{2^{r-1}}) + \Theta(2^{2^r}) \\ &= 2^{2^{r-1}+2^{r-2}} S(2^{2^{r-2}}) + \Theta(2^{2^r}) + \Theta(2^{2^r}) \\ &= 2^{2^{r-1}+2^{r-2}} \left(2^{2^{r-3}} S(2^{2^{r-3}}) + \Theta(2^{2^{r-2}}) \right) + \Theta(2^{2^r}) + \Theta(2^{2^r}) \\ &= 2^{2^{r-1}+2^{r-2}+2^{r-3}} S(2^{2^{r-3}}) + \Theta(2^{2^r}) + \Theta(2^{2^r}) + \Theta(2^{2^r}) \\ &= \dots \\ &= 2^{2^{r-1}+2^{r-2}+\dots+2^0} S(2^{2^0}) + r\Theta(2^{2^r}) \\ &= 2^{2^r-1} S(2^{2^0}) + \Theta(r2^{2^r}) \\ &= \Theta(2^{2^r}) + \Theta(r2^{2^r}) = \Theta(r2^{2^r}) \end{aligned}$$

Intuicyjnie: widzimy, że wykładnik wykładnika maleje o 1 w zależności rekurencyjnej. Wobec tego jeśli będziemy iterować wstawianie zależności rekurencyjnej do prawej strony równania, wykonamy r iteracji, a każda dołoży do ostatecznej sumy składnik $\Theta(2^{2^r})$.

Podstawiając $n = 2^{2^r}$ do otrzymanej równości, otrzymujemy

$$S(n) = \Theta(n \log \log n).$$

□

Literatura

- [1] Juraj Hromkovič, Przemysław Kanarek, Ralf Klasing, Krzysztof Lorys, Walter Unger, et al.. *On the Size of Permutation Networks and Consequences for Efficient Simulation of Hypercube Algorithms on Bounded-Degree Networks*. SIAM Journal on Discrete Mathematics, 2009, 23 (3), pp.1612–1645. [ff10.1137/060669164ff](#). [fhal-00402764f](#)
- [2] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, *Introduction to Algorithms*, The MIT Press, 2022