Politechnika Wrocławska

ORGANIZACJA I ARCHITEKTURA KOMPUTERÓW – PROJEKT

Sumatory resztowe realizowane jako układy odwracalne

Jakub Nowacki 281137

Maciej Pietrzak 281231

Jan Izdebski 281017

Prowadzący: dr hab. Inż. prof. Uczelni PWr Stanisław Piestrak

Spis treści:

1. Wstęp

W ramach niniejszego projektu zajęliśmy się tematyką sumatorów resztowych realizowanych jako układy odwracalne. Celem pracy było zbadanie możliwości implementacji sumatorów modularnych w systemie liczb resztowych (RNS) przy użyciu logiki odwracalnej oraz analiza efektywności wybranych rozwiązań.

Zakres projektu obejmował:

- Przegląd bramek odwracalnych, takich jak Feynmana, Peresa, HNG, Toffoliego i Fredkina.
- Omówienie ich właściwości i działania na przykładach.
- Implementację sumatorów typu CSA (Carry-Save Adder) oraz RCA (Ripple-Carry Adder) z końcowym przeniesieniem (EAC).

W projekcie skupiono się na rozwiązaniach energooszczędnych i zgodnych z wymogami obliczeń kwantowych, gdzie zachowanie informacji oraz brak emisji ciepła mają kluczowe znaczenie.

2. Bramki odwracalne

Bramki odwracalne to specjalny typ układów logicznych, w których każdej unikalnej kombinacji sygnałów wejściowych odpowiada jednoznaczny zestaw sygnałów wyjściowych. Taka konstrukcja umożliwia precyzyjne odtworzenie wartości wejściowych na podstawie wyjść, co eliminuje utratę informacji. W rezultacie bramki te nie tylko minimalizują emisję ciepła, ale również przyczyniają się do oszczędności energii, co jest kluczowe w projektowaniu nowoczesnych układów cyfrowych. W przeciwieństwie do tradycyjnych bramek, które w wyniku nieodwracalnych operacji mogą tracić dane, bramki odwracalne są starannie projektowane, aby zapewnić pełną kontrolę nad przepływem informacji.

2.1 Cechy

Bramki odwracalne wyróżniają się specyficznymi właściwościami, które odróżniają je od klasycznych bramek logicznych. Dzięki nim możliwe jest efektywne przetwarzanie informacji bez jej utraty, co ma istotne znaczenie w nowoczesnych układach cyfrowych. Poniżej przedstawiono kluczowe cechy tych bramek:

Właściwości	Opis
Możliwość odwrócenia operacji	Każda operacja logiczna może zostać odwrócona, co oznacza, że na podstawie wyjść można jednoznacznie odtworzyć wartości wejściowe.
Brak utraty informacji	

	Podczas przetwarzania sygnałów nie dochodzi do utraty danych, co zmniejsza emisję ciepła i poprawia efektywność energetyczną.
Brak konieczności powielania sygnałów	Każdy sygnał wejściowy jest wykorzystywany tylko raz, co eliminuje problem przeciążenia wyjść i konieczność dodatkowego wzmacniania sygnału.

Tabela 1 Kluczowe właściwości bramek odwracalnych w porównaniu do klasycznych bramek logicznych.

2.2 Rodzaje

1. Bramka Feynmana(CNOT)

Bramka Feynmana, nazywana również kontrolowanym NOT-em (CNOT), to podstawowy element wykorzystywany w obliczeniach kwantowych i odwracalnych. Składa się z dwóch wejść:

- **Wejście kontrolne** (np. bit A),
- **Wejście docelowe** (np. bit B).

Działanie:

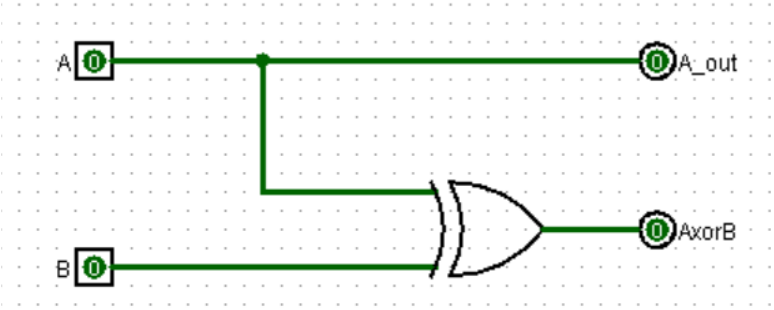
- Jeśli bit kontrolny ma wartość **1**, bit docelowy jest zanegowany
- Jeśli bit kontrolny ma wartość **0**, bit docelowy pozostaje bez zmian.

Przykład:

- Gdy A = 1 i B = 0 → wyjście to (A=1, B=1).
- Gdy A = 0 i B = 1 → wyjście to (A=0, B=1).

Zastosowanie:

- Kopiowanie sygnałów bez straty energii (np. tworzenie kopii bitu kontrolnego).
- Realizacja operacji logicznych, takich jak XOR (bit docelowy staje się wynikiem A $\oplus$ B).



Rysunek 1 Schemat działania bramki Feynmana (CNOT).

2. Bramka HNG

Bramka HNG (Himanshu-Nagaraj-Gopalakrishnan) to odwracalny pełny sumator, używany do wykonywania operacji dodawania bez utraty energii. Składa się z czterech wejść i czterech wyjść:

- **Wejścia**: Dwa bity danych (A, B), przeniesienie wejściowe (Cin) oraz stałe zero (0).
- **Wyjścia**: Dwa oryginalne bity (A, B), wynik sumy (A $\oplus$ B $\oplus$ Cin) oraz przeniesienie wyjściowe (Cout).

Działanie:

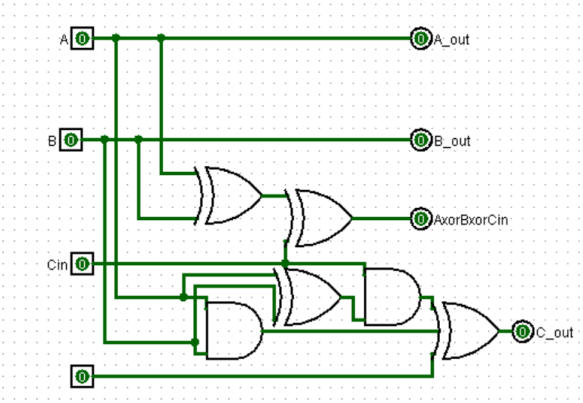
- Oblicza **s**umę trzech bitów (A, B, Cin) oraz przeniesienie (np. gdy A + B + Cin ≥ 2).
- Nie traci informacji: Na podstawie wyjść można odtworzyć wszystkie wejścia.

Przykład:

- Jeśli A=1, B=1, Cin=0:
  - Suma = 1 $\oplus$ 1 $\oplus$ 0 = **0**
  - Cout = 1 (bo 1 + 1 + 0 = 2 ≥ 2)
  - Wyjścia: A=1, B=1, Suma=0, Cout=1.

Zastosowanie:

- Kluczowa w modularnych sumatorach (np. RCA, CSA z EAC) opisanych w artykule.
- Umożliwia projektowanie energooszczędnych układów arytmetycznych dla RNS.



Rysunek 2 Bramka HNG

3. Bramka Toffoliego (CCNOT)

Bramka Toffoliego, zwana też kontrolowanym-kontrolowanym NOT-em (CCNOT), to uniwersalny element w logice odwracalnej i obliczeniach kwantowych. Składa się z trzech wejść i trzech wyjść:

- **Wejścia**: Dwa bity kontrolne (A, B) oraz jeden bit docelowy (C).
- **Wyjścia**: Dwa bity kontrolne (A, B) oraz zmodyfikowany bit docelowy.

Działanie:

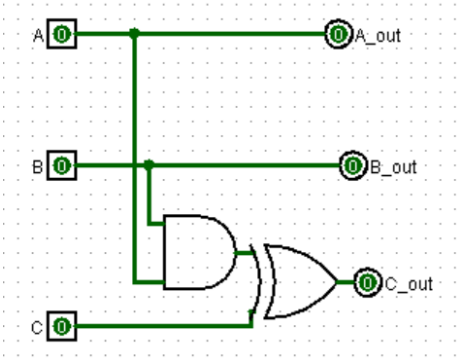
- Jeśli oba bity kontrolne (A i B) mają wartość 1, bit docelowy (C) jest zanegowany (0 → 1 lub 1 → 0).
- Jeśli przynajmniej jeden bit kontrolny ma wartość 0, bit docelowy nie zmienia się.

Przykład:

- Gdy A=1, B=1, C=0 → wyjście to (A=1, B=1, C=1).
- Gdy A=1, B=0, C=1 → wyjście to (A=1, B=0, C=1).

Zastosowanie:

- **Uniwersalność**: Może realizować dowolną funkcję logiczną w układach odwracalnych (np. AND, OR).
- Stosowana w zaawansowanych układach kwantowych i odwracalnych mnożnikach.



Rysunek 3 Bramka Toffoliego

4. Bramka Peresa

Bramka Peresa to odwracalny półsumator, który wykonuje dwie operacje naraz: oblicza sumę i przeniesienie, nie tracąc przy tym energii. Składa się z trzech wejść i trzech wyjść:

- **Wejścia**: Dwa bity danych (A, B) oraz stałe zero (C=0).
- **Wyjścia**: Oryginalny bit A, wynik sumy (A $\oplus$ B) oraz przeniesienie (A $\wedge$ B).

Działanie:

1. **Suma**: Wynik A $\oplus$ B (XOR) – np. 1 $\oplus$ 1 = 0, 1 $\oplus$ 0 = 1.
2. **Przeniesienie**: Wynik A $\wedge$ B (AND) – np. 1 $\wedge$ 1 = 1, 1 $\wedge$ 0 = 0.
3. **Stałe wejście (C=0)**: Umożliwia odwracalność – nie wpływa na wynik, ale pozwala odzyskać wejścia z wyjść.

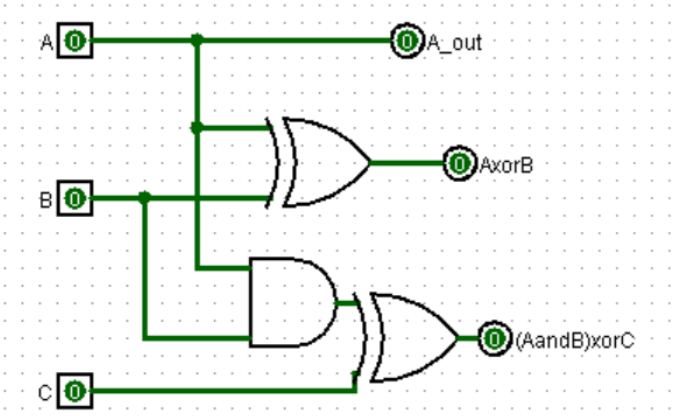
Przykład:

- Gdy A=1, B=1, C=0 → wyjście to (A=1, Suma=0, Przeniesienie=1).
- Gdy A=0, B=1, C=0 → wyjście to (A=0, Suma=1, Przeniesienie=0).

Zastosowanie:

- **Półsumatory**: Łączy operacje XOR i AND w jednej bramce, oszczędzając zasoby.

- **Energooszczędne układy**: Idealna dla RNS i logiki odwracalnej, gdzie liczy się brak strat energii.



Rysunek 4 Bramka Peresa

5.Bramka Fredkina

Bramka Fredkina to sterowana zamiana bitów, która działa w oparciu o wartość bitu kontrolnego. Jest odwracalna i nie traci informacji. Składa się z trzech wejść i trzech wyjść:

- **Wejścia:** Jeden bit kontrolny (A) oraz dwa bity docelowe (B, C).
- **Wyjścia:** Bit kontrolny (A) oraz zmodyfikowane bity docelowe.

Działanie:

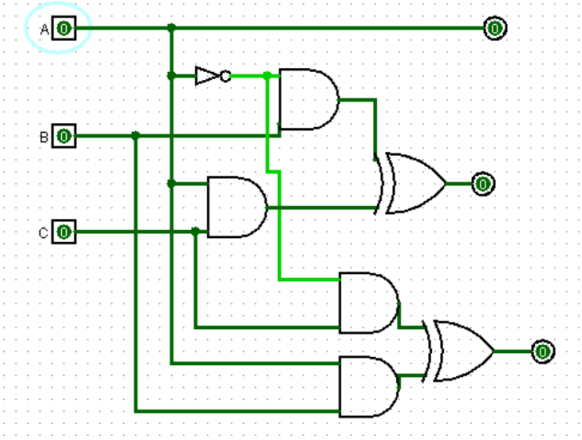
- Jeśli bit kontrolny (A) ma wartość 1, bity docelowe (B i C) są zamieniane miejscami.
- Jeśli bit kontrolny (A) ma wartość 0, bity docelowe pozostają bez zmian.

Przykład:

- Gdy A=1, B=0, C=1 → wyjście to (A=1, B=1, C=0).
- Gdy A=0, B=1, C=0 → wyjście to (A=0, B=1, C=0).

Zastosowanie:

- Sortowanie danych: Umożliwia warunkową zamianę wartości.
- Zarządzanie przepływem sygnałów: Stosowana w układach, gdzie trzeba kontrolować ścieżki danych w zależności od warunków.
- Obliczenia kwantowe: Wykorzystywana do tworzenia odwracalnych operacji warunkowych.



Rysunek 5 Bramka Fredkina

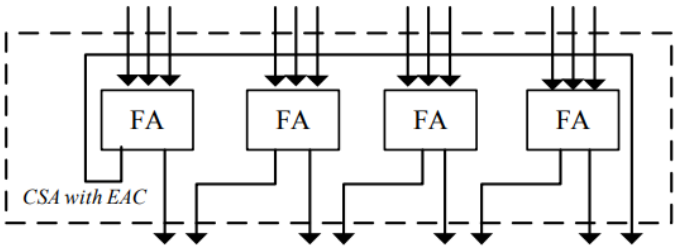
3. Rodzaje sumatorów resztowych z użyciem bramek odwracalnych i ich charakterystyka

W systemie liczb resztowych (RNS), suma dwóch liczb wykonywana jest osobno dla każdego z kanałów (modułów) w oparciu o działanie modulo. Aby operacje te były wydajne, stosuje się specjalne sumatory modularne – najczęściej zbudowane w oparciu o **3-do-2 sumatory typu carry-save (CSA)** oraz **sumatory z propagacją przeniesienia (CPA)**. W architekturach energooszczędnych oraz układach kwantowych czy nanotechnologicznych coraz częściej projektuje się te sumatory z wykorzystaniem **bramek odwracalnych**.

3.1. CSA z końcowym przeniesieniem ?cyklicznym? (EAC – End-Around Carry)

CSA z EAC to struktura zbudowana z pełnych sumatorów (FAs), które przetwarzają trzy wejściowe operandy i generują dwa wektory wyjściowe w formacie carry-save. W przypadku CSA z EAC, przeniesienie z najstarszego bitu (MSB) jest zawracane do bitu najmłodszego (LSB), co realizuje operację dodawania modulo 2n−12^n - 12n−1. Struktura ta charakteryzuje się:

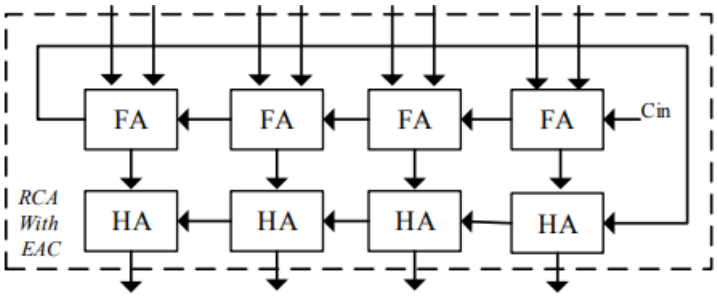
- **Niskim opóźnieniem** – zależy tylko od pojedynczego pełnego sumatora,
- **Liniową zależnością powierzchni od szerokości słowa**,
- **Brakiem propagacji przeniesienia przez całą szerokość słowa**.



Rysunek 6 Przykładowy schemat sumatora CSA z przeniesieniem 4 bitowy

3.2. CSA z uzupełnieniem końcowego przeniesienia ?odwracalnego? (CEAC – Complemented End-Around Carry)

To wariant CSA z EAC, w którym końcowe przeniesienie jest **komplementowane** (odwracane), co umożliwia bardziej złożoną manipulację wartościami w kanałach modulo 2n+12^n + 12n+1. CEAC jest używane do zwiększenia dokładności lub uproszczenia dalszych operacji odwrotnych konwersji (reverse conversion).



Rysunek 7 Przykładowy schemat sumatora resztowego RCA z przeniesieniem

3.3. sumatory z propagacją przeniesienia (CPA)

Poza CSA, w systemach RNS potrzebne są również klasyczne sumatory z propagacją przeniesienia – najczęściej dla operacji końcowego dodawania po CSA. Wśród nich wyróżniamy:

- **Ripple Carry Adders (RCA)** – prosta i energooszczędna architektura o dużym opóźnieniu,
- **Parallel Prefix Adders (PPA)** – szybka, skalowalna struktura wykorzystywana w wysokowydajnych układach RNS, pozwala na szybką propagację przeniesienia w strukturze drzewa.

Bramki odwracalne w RNS

W kontekście projektowania sumatorów modularnych w technologiach niskomocowych, istotne staje się użycie **bramek odwracalnych**, takich jak:

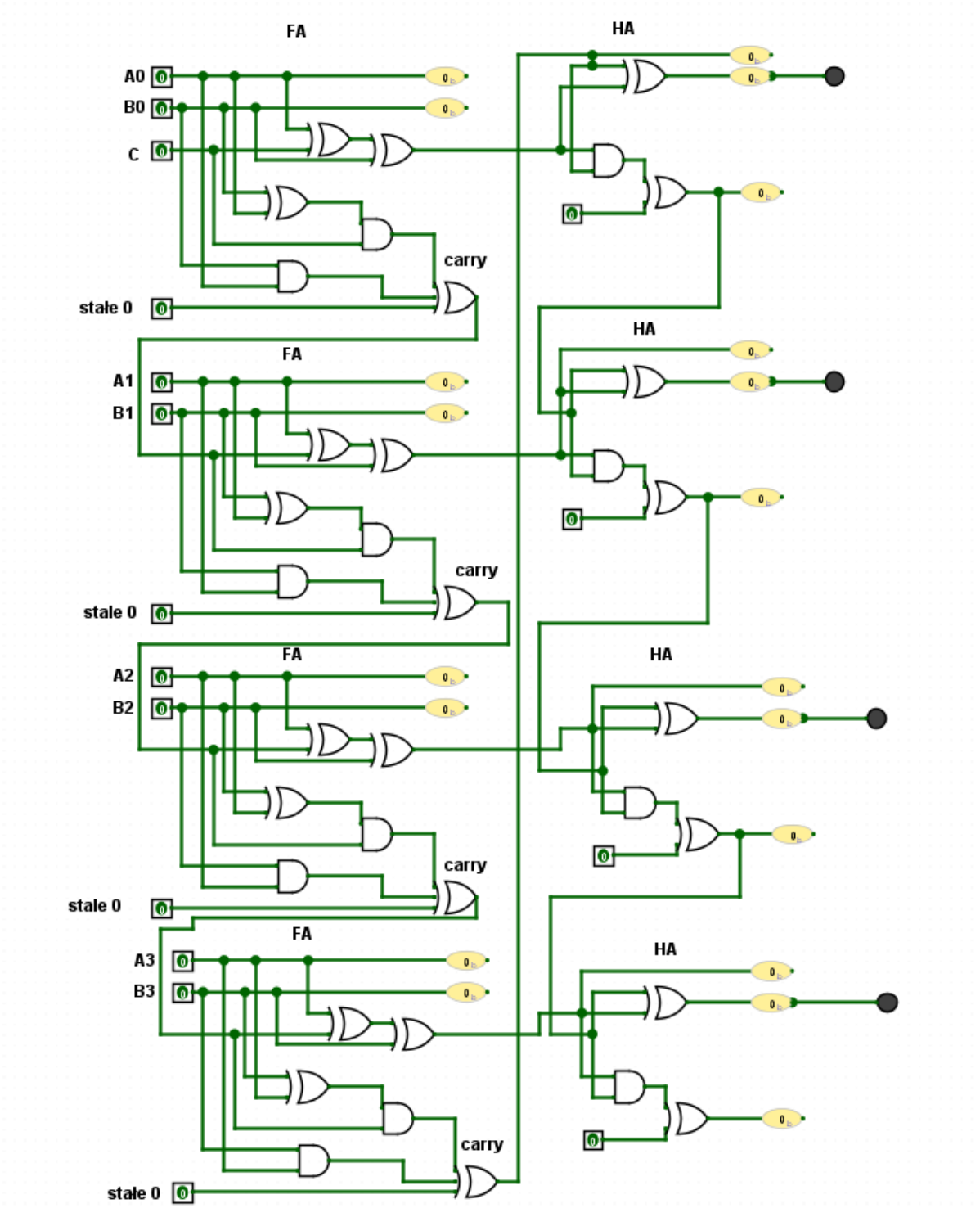
- **Bramka Toffoliego**,
- **Bramka Fredkina**,
- **Bramka Peresa**,

- **Bramka Feynmana**

Ich główną zaletą jest to, że nie tracą informacji (nie generują entropii), co pozwala na projektowanie układów:

- **Bezstratnych** (zachowujących informację),
- **O niskim zużyciu energii** (zgodnie z zasadą Landauera),
- **Zgodnych z wymaganiami komputerów kwantowych**.

Sumatory zbudowane z bramek odwracalnych mogą być implementacją CSA lub CPA, ale w formie, która umożliwia całkowicie odwracalny przepływ danych.



Rysunek 8 Schemat sumatora resztowego 4 bitowego $2^n - 1$

3.4 Resztowe sumatory prefiksowe równoległe z propagacją przeniesienia (PPA – Parallel Prefix Adders)

Parallel Prefix Adders (PPA) to klasa sumatorów o wysokiej wydajności, które umożliwiają bardzo szybką propagację przeniesienia w strukturze drzewa. W odróżnieniu od klasycznych sumatorów typu Ripple Carry Adders (RCA), w których przeniesienie musi przejść liniowo

przez kolejne bity, PPA równolegle obliczają grupy sygnałów generujących i propagujących przeniesienie, co pozwala na skrócenie opóźnienia całkowitego.

Zasada działania PPA:
Sumatory PPA działają na zasadzie trójfazowej:

1. **Faza generowania sygnałów** – obliczane są sygnały *generate* (G) i *propagate* (P) dla każdego bitu.
2. **Faza łączenia prefixów** – za pomocą struktur drzewiastych (np. Kogge-Stone, Brent-Kung, Han-Carlson) propagowane są zależności przeniesienia dla wielu bitów jednocześnie.
3. **Faza końcowa** – obliczana jest ostateczna suma bitów na podstawie uzyskanego przeniesienia.

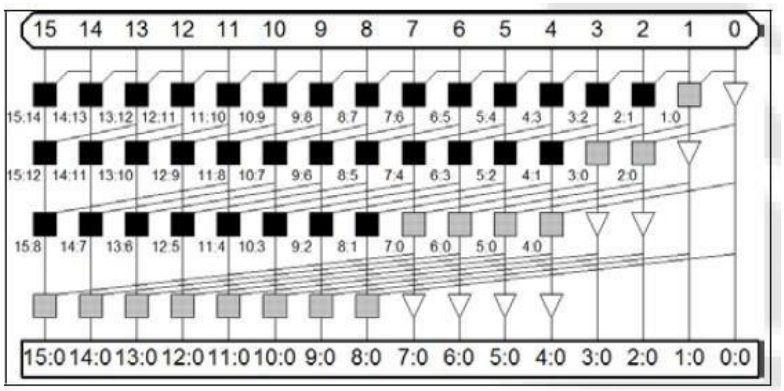
Propagacja - określa, czy przeniesienie może zostać przekazane dalej.

Generacja - określa, czy przeniesienie zostaje wygenerowane niezależnie od przeniesienia z poprzedniej pozycji

Obliczenia dla sygnałów generacji i propagacji:

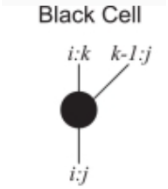
Propagacja: $P = a \oplus b$

Generacja: G = a·b



Rysunek 9 Sumator równoległy prefiksowy PPA – struktura 32-bitowa.

W architekturze *Parallel Prefix Adder* (PPA), **białe (szare)** i **czarne kropki** reprezentują różne operacje na sygnałach **generate (G)** i **propagate (P)** w celu wyznaczenia przeniesień w strukturze drzewiastej. Oto ich znaczenie:



Rysunek 10 Czarny węzeł w PPA

Czarny węzeł oblicza nowe sygnały generate i propagate dla grupy bitów w sposób następujący:

Wejścia:

$$Gi, P_i \quad - sygnały\ dla\ bitu\ niższego$$

$$Gj, P_j \quad - sygnały\ dla\ bitu\ wyższego$$

Wyjścia:

$$\boldsymbol{G_{i:j} = G_j + (P_i \cdot G_j)}$$

$$\boldsymbol{P_{i:j} = P_i \cdot P_j}$$

Rysunek 11 Biały węzeł w PPA

Biały węzeł oblicza tylko nowy sygnał *generate* (czyli przeniesienie), bez aktualizacji propagacji.

Wejścia:

$$G_i, P_i, G_j$$

Wyjście:

$$G_{i:j}\boldsymbol{=G_j + (P_i \cdot G_j)}$$

4. Wnioski

Bramki odwracalne to specjalny typ układów logicznych, w których każdej unikalnej kombinacji sygnałów wejściowych odpowiada dokładnie jeden zestaw wyjściowy, co umożliwia precyzyjne odtworzenie wartości wejściowych na podstawie wyjść. Dzięki temu nie tracimy informacji, co minimalizuje emisję ciepła i przyczynia się do oszczędności energii. W oparciu o taką logikę można zbudować modularne sumatory modulo $2^n - 1$ które mimo dodatkowych nakładów związanych z odwracalnością (takich jak użycie bramek HNG i Peresa

czy wstawianie bitów stałych i pomijalnych wyjść), dają się zrealizować z akceptowalnym wzrostem parametrów. Konstrukcje oparte na sieciach prefixowych (np. Brent–Kung) wykazują wyraźną przewagę nad prostymi kaskadami ripple carry, co dowodzi, że logika odwracalna może być praktycznym rozwiązaniem do budowy energooszczędnych, szeroko równoległych jednostek arytmetycznych w układach RNS, szczególnie tam, gdzie istotna jest minimalizacja zużycia energii.

Literatura

[1] A. S. Molahosseini *et al*., ”Towards efficient modular adders based on reversible circuits,”w: *Proc. IEEE Int. Symp. on Circuits and Systems (ISCAS)*, Florence, Italy, 2018, ss. 1-5.