

1. Superpozycje

Zadanie 1

Trudność: łatwe

Punktów: 1

Na lotnisku znaleziono prostokątne pudło z dwoma oszklonymi otworami na przeciwległych ściankach. Nad jednym otworem jest napisane IN, a nad przeciwnym OUT. Ściany pudła są nieprzezroczyste.



Pudło może być jednym z dwojga:

(ATRAPA) Pudło jest puste, a okienka są ze zwykłego szkła.

(BOMBA) Za szybką IN umieszczono *dzielnik wiązki polaryzacyjnej* (polarizing beam splitter)¹. Wiązka spolaryzowana poziomo przechodzi do OUT. Wiązka pionowa aktywuje detonację bomby.

Chcemy ustalić, czy pudło jest atrapą czy bombą, nie wysadzając jednocześnie lotniska w powietrze. Wskaż procedurę, która używa jednego polaryzatora liniowego, dla atrapy zawsze powie ATRAPA, a dla bomby powie BOMBA z prawdopodobieństwem $\frac{3}{4}$, ale spowoduje wybuch tylko z prawdopodobieństwem $\frac{1}{2}$ ².

Zadanie 2

Trudność: średnie

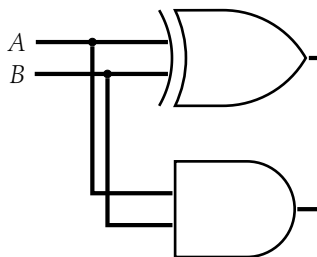
Punktów: 3

Dla dowolnie małego $\varepsilon > 0$ wskaż procedurę, która odróżnia bombę od atrapy bezbłędnie i doprowadza do wybuchu z prawdopodobieństwem $< \varepsilon$. Możesz korzystać z różnych polaryzatorów oraz lusterek.

Wskazówka: $\forall x \in \mathbb{R}_+ \sin x < x$.

2. Obwody logiczne

Na następnym wykładzie będziemy konstruować algorytmy w postaci obwodów logicznych, takich jak półsumator na rysunku. Obwód jest DAG-iem, którego wierzchołki źródłowe to wejście (bity). Wierzchołki wewnętrzne (o stałym stopniu) to bramki logiczne, a w ujściach jest wynik obliczenia.



Rysunek 2: Obwód realizujący półsumator. Użyto w nim bramek COPY, XOR i AND.

Zadanie 3

Trudność: trudne

Punktów: 5

Pokaż, że dla maszyny Turinga M , która na dowolnym n -bitowym wejściu wykona najwyżej $T(n)$ operacji, istnieje rodzina $\{C_n\}_{n \in \mathbb{N}}$ obwodów logicznych zbudowanych z $O(T(n)^2)$ bramek COPY, AND, OR i NOT, że C_n przyjmuje n bitów wejścia i zwraca wynik zgodny z maszyną M .

¹Można myśleć, że dzielnik to ustawiony poziomo filtr polaryzacyjny. Jeśli foton nie zostanie przepuszczony, to zgromadzona energia zamienia się w ciepło, które wywołuje wybuch bomby.

²Gdy bomba wybuchła, uważamy ją za wykrytą.

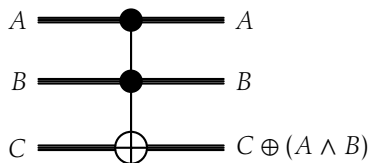
Wskazówka: Warto zainspirować się *drukarką igłową* i zastanowić, jak przerobić maszynę Turinga, by jej spacer po taśmie nie zależał od wejścia.

Zadanie 4

Trudność: łatwe

Punktów: 1

Bramka Toffoliego (CCNOT, *Controlled-Controlled-NOT*) działa jak na rysunku:



Jak zbudować za jej pomocą półsumator **nie rozdzielając kabelków** (używamy tylko bramek CCNOT, nie używamy bramek COPY)? Do wejścia można dołożyć pulę bitów jedynkowych.

Zadanie 5

Trudność: łatwe

Punktów: 1

Pokaż, że każdy obwód logiczny zbudowany z bramek COPY, AND, OR i NOT można zrealizować wyłącznie za pomocą bramek CCNOT (możemy dołożyć pulę bitów jedynkowych na wejściu oraz śmieci na wyjściu).

Zadanie 6

Trudność: łatwe

Punktów: 1

Pokaż, że obliczenia realizowane przez obwód logiczny zbudowany z bramek CCNOT są odwracalne.

Zadanie 7

Trudność: łatwe

Punktów: 1

Pokaż, że każdy obwód zbudowany z bramek CCNOT można przerobić na równoważny, planarny obwód z bramek CCNOT.

2.1 Odśmiecianie

Jak przekonaliśmy się dzięki poprzednim zadaniom, dla dowolnej funkcji $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ realizowanej przez obwód klasyczny zbudowany z bramek AND, OR i NOT można stworzyć odwracalny obwód złożony wyłącznie z bramek CCNOT realizujący tę samą funkcję — ale poszerzoną o wejście pomocnicze (*ancilla*) oraz wyjście-śmieci. Gdy zgodzimy się na bramki CCNOT i NOT, można założyć, że wszystkie bity pomocnicze mają wartość 0. To znaczy, nasz obwód C będzie przyjmował $n + a$ bitów wejścia i zwracał $m + b$ bitów wyjścia ($n + a = m + b$, gdyż obwód jest odwracalny). Gdy bity pomocnicze będą zainicjalizowane zerami, będzie on obliczał funkcję f :

$$C(\underbrace{x_1, \dots, x_n}_{a \text{ ancilla}}, \underbrace{0, \dots, 0}_{b \text{ bitów śmieciowych}}) = [f(x)_1, \dots, f(x)_m, g(x)_1, \dots, g(x)_b]$$

My jednakowoż chcielibyśmy zredukować użycie bitów śmieciowych.

Zadanie 8

Trudność: łatwe

Punktów: 2

Jak przekształcić obwód C na odwracalny obwód C' o następującej specyfikacji: Gdy C' dostanie na wejściu wektor $[x_1, \dots, x_n, 0^n, 0^a]$ (w sumie $2n + a$ bitów), to zwróci $[x_1, \dots, x_n, f(x)_1, \dots, f(x)_m, g(x)_1, \dots, g(x)_b]$ ($n + m + b$ bitów)?

Zadanie 9

Trudność: łatwe

Punktów: 2

Jak przekształcić obwód C na odwracalny obwód C'' o następującej specyfikacji: Gdy C'' dostanie na wejściu wektor $[x_1, \dots, x_n, 0^n, 0^a, y_1, \dots, y_m]$ (czyli $2n + a + m$ bitów; y jest dowolnym wektorem boolowskim), to zwróci $[x_1, \dots, x_n, 0^n, 0^a, y \oplus f(x)]$.