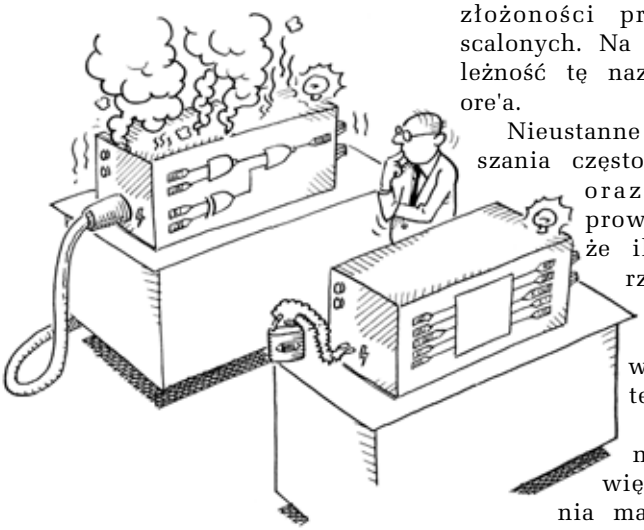
Logika odwracalna

Przełom w technice cyfrowej?

Prezentowany artykuł, jak na dotychczasową praktykę EP, jest nietypowy: autor porusza w nim bowiem wyłącznie zagadnienia teoretyczne (ach te wzory). Nie da się jednak inaczej, ponieważ układy, o których piszemy, poza kilkoma akademickimi opracowaniami, jeszcze nie istnieją...
W artykule przedstawiono ograniczenia fizyczne związane z wykonywaniem obliczeń maszynowych oraz wprowadzenie do obliczeń odwracalnych - metody umożliwiającej rozwiązanie problemu produkcji ciepła przez układy elektroniczne. Przedstawiono również praktyczną realizację tej techniki na przykładzie doświadczalnego procesora Pendulum.



Efektem ubocznym działania wszystkich urządzeń elektronicznych jest zamiana zasilającej je energii elektrycznej na ciepło. Musi być ono nieustannie odprowadzane, aby nie dopuścić do przekroczenia maksymalnej dozwolonej temperatury pracy układu i - w konsekwencji - jego uszkodzenia. Ilość ciepła wytwarzanego przez układ zależy od liczby elementów wchodzących w jego skład oraz od częstotliwości zegara ustalającego rytm pracy układu. Fakt ten jest dobrze znany wszystkim właścicielom szybkich procesorów oraz zaawansowanych kart graficznych - do poprawnego działania zazwyczaj wymagają one bardzo wydajnych systemów chłodzenia.

W latach sześćdziesiątych ubiegłego wieku Gordon Moore zauważył, że wraz z rozwojem technologii wytwarzania układów scalonych liczba tranzystorów możliwych do wykonania na ustalonej powierzchni kryształu półprzewodnika podwaja się średnio co 18 miesięcy. Obserwacja ta nie ma oczywiście rangi prawa fizyki, lecz duża zgodność jej przewidywań z rzeczywistym stopniem zaawansowania technologii półprzewodników uczyniła z niej bardzo wygodne narzędzie do szacowania złożoności przyszłych układów scalonych. Na cześć odkrywcy zależność tę nazwano prawem Moore'a.

Nieustanne dążenie do zwiększania częstotliwości taktowania oraz prawo Moore'a prowadzą do wniosku, że ilość ciepła wytwarzanego przez przyszłe układy scalone będzie rosła wraz z rozwojem techniki.

Naukowcy i inżynierowie rozpoczęli więc intensywne badania mające na celu opracowanie nowych sposobów odprowadzania ciepła. Na podstawie znaczących osiągnięć na tym polu oraz ciągłego spadku zapotrzebowania na energię wymaganą do działania pojedynczego tranzystora, będącego efektem postępującej miniaturyzacji, sądzono, że w przyszłości produkcja ciepła będzie mogła zostać ograniczona w dowolnym stopniu, co pozwoli uniknąć poważnych problemów z chłodzeniem struktury układu scalonego.

Ograniczenia termodynamiczne

Przekonanie to uległo zmianie po opublikowaniu przez Rolfa Landauera z centrum badawczego IBM im. Watsona wyników badań nad fizyczną stroną procesu przetwarzania informacji. Stało się jasne, że straty spowodowane niedoskonałością budowy układu scalonego nie są jedynym źródłem ciepła. Drugim jego źródłem okazał się być proces kasowania informacji. Entropia informacyjna Shannona:

$$S = -\sum_{i=1}^{n} p_i \cdot log_2\, p_i$$

układu mogącego znajdować się w jednym $n \in \mathbb{N}$ rozróżnialnych stanów, gdzie p_i jest prawdopodobieństwem znalezienia układu w stanie o numerze i, jest związana z entropią termodynamiczną Gibbsa wzorem:

$$G = (k_B \cdot ln\ 2) \cdot S,$$

gdzie k_B=1,380*10^{-23} [J/K] jest stałą Boltzmanna.

Definicja temperatury bezwzględnej T wiąże zmiany entropii układu ΔG ze zmianami zawartej w nim energii cieplnej ΔQ wzorem:

$$\frac{1}{T} = \frac{\Delta G}{\Delta Q}.$$

Stąd w procesach izotermicznych dostarczenie ciepła do układu powoduje zwiększenie jego entropii. Istotnie, rozważmy urządze-

nie służące do przechowywania jednego bitu, a więc układ mogący znajdować się tylko w jednym z dwóch rozróżnialnych stanów w danym momencie. Ponieważ nie wiemy niczego o początkowym stanie układu, to prawdopodobieństwo p_0, że znajduje się on w pierwszym stanie, jest równe prawdopodobieństwu p_1, że znajduje się on w stanie drugim, a więc p_0=p_1=0,5. Entropia informacyjna tego układu wynosi:

$$S_? = -(\frac{1}{2}\cdot log_2\frac{1}{2} + \frac{1}{2}\cdot log_2\frac{1}{2}) = 1 \text{ bit.}$$

Przeniesienie systemu do nowego stanu oznacza, że prawdopodobieństwo znalezienia go w żądanym stanie wynosi 1, a prawdopodobieństwo zajmowania przez układ stanu przeciwnego jest równe 0. Entropia układu wynosi wówczas:

$$S_! = -(1\cdot log_2\ 1 + 0\cdot log_2\ 0) = 0 \text{ bitów.}$$

Zmiana entropii termodynamicznej wynosi więc:

$$\Delta G = (k_B\cdot ln\ 2)\cdot(S_! - S_?) = -k_B\cdot ln\ 2.$$

Z definicji temperatury wyznaczamy ciepło pochłonięte przez układ:

$$\Delta Q = T\Delta G = -k_B\cdot T\cdot ln\ 2,$$

czyli k_B*T*ln 2 dżuli energii zostało wydzielone do otoczenia w postaci ciepła. Obserwacja ta nosi nazwę zasady Landauera i określa dolne ograniczenie ilości ciepła, które należy rozproszyć podczas kasowania jednego bitu informacji.

W powszechnie spotykanych zakresach temperatur pracy układów scalonych jest to niezwykle mała energia, np. w temperaturze T=333 [K] (60° Celsjusza) wynosi ona:

$$\Delta Q = 333[\text{K}]\cdot 1,380\times10^{-23}[\text{J/K}]\cdot ln\ 2 = 3,185\times10^{-21}[\text{J}].$$

Dla porównania [3], układy rodziny G12 firmy LSI Logic, wykonane w technologii CMOS 0,13µm w wersji zasilanej napięciem 1 V zużywają średnio 7,1*10^{-15} [J] na zmianę stanu pojedynczej bramki. Jest to około 2,3*10^6 raza więcej, niż teoretyczne minimum wynikające z zasady Landauera. Wartość ta jest duża, lecz będzie ona szybko maleć wraz z rozwojem technologii półprzewodników. Oszacowania wynikające z analizy szybkości spadku zużycia energii przez bramki na przestrzeni ostatnich lat wskazują, że granica Landauera zostanie osiągnięta w czasie krótszym niż 35 lat. Z tego powodu w wielu ośrodkach akademickich i przemysłowych rozpoczęto badania zmierzające do opracowania technik umożliwiających pokonanie ograniczeń termodynamicznych.

Obliczenia odwracalne

Fundamentalna natura nowo odkrytych ograniczeń uniemożliwiła ich bezpośrednie pokonanie za pomocą udoskonalenia technologii wytwarzania układów scalonych. Ewentualny przełom mógł nastąpić jedynie na drodze zmian w samym sposobie prowadzenia obliczeń.

Jedną z takich alternatyw badał w 1973 roku Charles Bennett, również pracujący w IBM. Na podstawie zasady Landauera doszedł on do wniosku, że skoro emisja ciepła jest nieodłącznym skutkiem procesu kasowania informacji, to obliczenia należy prowadzić tak, by cała przetwarzana informacja została zachowana. Pomysł ten zaowocował powstaniem nowego sposobu przetwarzania informacji, nazwanego obliczeniami odwracalnymi.

Entropia...

...informacyjna - nieokreśloność źródła, z którego są dostarczane (wysyłane) wiadomości.

...termodynamiczna - funkcja stanu oznaczająca miarę stopnia nieuporządkowania określonego układu fizycznego, wynikająca z drugiej zasady termodynamiki.

Dwuargumentowe operacje logiczne mające kluczowe znaczenie dla techniki cyfrowej nie są niestety funkcjami różnowartościowymi, przez co nie mogą być one odwracalne - podczas wykonywania obliczeń występuje utrata przetwarzanej informacji. Dla przykładu rozważmy funkcję:

$$\text{AND}: \{0,1\}\times\{0,1\}\rightarrow\{0,1\}$$

Zgodnie z jej definicją argumentem może być dowolny element zbioru {(0,0),(0,1),(1,0),(1,1)}. Nie zakładamy niczego na temat roli pełnionej przez tę bramkę w układzie, a więc musimy przyjąć, że każdy z argumentów funkcji jest jednakowo prawdopodobny:

$$p_{(0,0)} = p_{(0,1)} = p_{(1,0)} = p_{(1,1)} = \frac{1}{4}.$$

Przed wykonaniem operacji układ ma entropię:

$$S_{przed} = -\sum_i p_i\cdot log_2\ p_i = -4\cdot(\frac{1}{4}log_2\frac{1}{4}) = 2 \text{ bity.}$$

Przeciwdziedziną funkcji jest zbiór {0,1}, przy czym wartość 1 jest osiągana tylko dla argumentu (1,1), więc prawdopodobieństwa przyjęcia określonego wyniku wynoszą odpowiednio p_0=$^3/_4$ i p_1=$^1/_4$.

Entropia układu po wykonaniu operacji to:

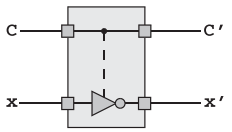
$$S_{po} = -(\frac{3}{4}log_2\frac{3}{4} + \frac{1}{4}log_2\frac{1}{4}) \approx 1 \text{ bit,}$$

a więc straciliśmy S_{przed}-S_{po} bitów informacji. Zgodnie z zasadą Landauera oznacza to, że podczas obliczania funkcji musiało dojść do rozproszenia energii w postaci ciepła. Nieróżnowartościowość n-argumentowych (dla n > 1) funkcji logicznych $f: \{0,1\}^n \rightarrow \{0,1\}$ wynika wprost ze zbyt małej liczby elementów przeciwdziedziny - jest oczywiste, że nie można przyporządkować każdemu elementowi zbioru 2^n-elementowego innego elementu zbioru dwuelementowego.

Wynika stąd wniosek, że wynik odwracalnych funkcji odtwarzających n-argumentowe operacje logiczne będzie krotką składającą się nie z jednego, lecz co najmniej n bitów. W ogólnym przypadku będą to więc funkcje wektorowe.

Praktyczna przydatność funkcji odwracalnych zależy bezpośrednio od liczby układów cyfrowych, które można zrealizować w oparciu o nie. Sprawdźmy więc jak wiele daje się policzyć w sposób odwracalny.

Z logiki matematycznej wiadomo, że wszystkie jedno- i dwuargumentowe funkcje logiczne można wyrazić za pomocą operacji NAND albo NOR (w przykładzie



C	x	C'	x'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Rys. 1. Bramka CN

pokazano rekonstrukcję funkcji mających najważniejsze znaczenie dla techniki cyfrowej):

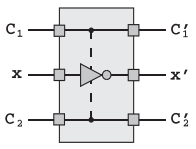
$$\begin{aligned}
\mathtt{NOT}(x) &= \mathtt{NAND}(x,x),\\
\mathtt{AND}(x,y) &= \mathtt{NOT}(\mathtt{NAND}(x,y)),\\
\mathtt{OR}(x,y) &= \mathtt{NOT}(\mathtt{AND}(\mathtt{NOT}(x),\mathtt{NOT}(y))),\\
\mathtt{NOR}(x,y) &= \mathtt{NOT}(\mathtt{OR}(x,y)),\\
\mathtt{XOR}(x,y) &= \mathtt{OR}(\mathtt{AND}(x,\mathtt{NOT}(y)),\mathtt{AND}(\mathtt{NOT}(x),y)),\\
&\ldots
\end{aligned}$$

W roku 1925 E. Żyliński udowodnił, że NAND oraz NOR to jedyne funkcje mające tę własność. Wynika stąd, że dowolny cyfrowy układ kombinacyjny można zbudować za pomocą jakichkolwiek bramek odwracalnych wtedy i tylko wtedy, gdy da się z nich zbudować bramkę NAND (albo NOR).

Historycznie najstarszym i najprostszym rozwiązaniem umożliwiającym zbudowanie odwracalnego urządzenia liczącego jest pokazana na **rys. 1** bramka Toffoliego. Składa się ona z linii sterującej stanem inwertera *C*-*C'*, wejścia *x* oraz wyjścia *x'*. Stan panujący na wyprowadzeniu *C* jest przekazywany bez zmian na wyprowadzenie *C'*. Stan wyjścia jest dany następującym wzorem:

$$x' = \begin{cases} \mathtt{NOT(x)} & \text{dla } C = 1,\\ x & \text{dla } C = 0. \end{cases}$$

Układ ten pełni więc rolę sterowanego inwertera i z tego powodu nosi nazwę bramki CN (od *controlled NOT*). Pod względem funkcjonalnym odpowiada on bramce XOR. Zgodnie z dowodem Żylińskiego bramka CN nie wystarcza do odtworzenia wszystkich dwuargumentowych funkcji logicznych. Toffoli zmodyfikował więc bramkę CN dodając do niej kolejną linię sterującą, uzyskując pokazaną na **rys. 2**. bramkę CCN (od *controlled controlled NOT*).



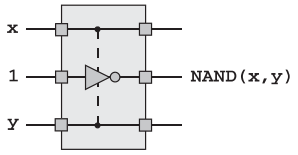
C_1	C_2	x	C_1'	C_2'	x'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Rys. 2. Bramka CCN

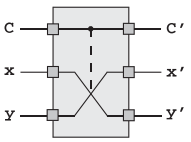
Stany wejść sterujących C_1 oraz C_2 są przenoszone przez bramkę bez zmian na odpowiadające im wyjścia C_1' i C_2', a wzór opisujący działanie inwertera ma postać:

$$x' = \begin{cases} \mathtt{NOT}(x) & \text{dla } C_1 = 1 \wedge\ C_2 = 1,\\ x & \text{w przeciwnym przypadku.} \end{cases}$$

Bramka CCN umożliwia wykonanie operacji NAND (**rys. 3**), a więc można za jej pomocą obliczyć dowolną jedno- albo dwuargumentową funkcję logiczną. Wynika stąd, że za pomocą bramek odwracalnych da się odtworzyć dowolny układ kombinacyjny.



Rys. 3. Realizacja funkcji NAND za pomocą bramki CCN



C	x	y	C'	x'	y'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

Rys. 4. Bramka Fredkina

Funkcja *f* jest odwracalna, jeśli dla każdego $\vec{y} = f(\vec{x})$ można jednoznacznie odtworzyć odpowiadającą mu wartość argumentu $\vec{x}$. Dzięki tej własności informacja zawarta w argumencie $\vec{x}$ może zostać odzyskana, a więc podczas obliczania funkcji *f* nie zachodzi utrata informacji i związana z tym emisja ciepła - obliczenia takie mogą być więc wykonywane przy dowolnie małym zużyciu energii. Łatwo sprawdzić, że warunkiem koniecznym i dostatecznym odwracalności funkcji *f* jest jej różnowartościowość [1].

Funkcja $f: X \to Y$ jest różnowartościowa, jeśli dla różnych argumentów przyjmuje różne wartości.

Kolejnym rozwiązaniem umożliwiającym przeprowadzenie dowolnych obliczeń w sposób odwracalny jest bramka Fredkina (**rys. 4**). Ma ona dwa wejścia: *x* i *y*, wyjścia *x'* i *y'* oraz linię sterującą *C*-*C'*. Podobnie jak w przypadku bramek Toffoliego, stan wejścia sterującego *C* jest przekazywany bez zmian na wyjście *C'*. Stany wyjść są określone zależnością:

$$x' = \begin{cases} x & \text{dla } C = 0,\\ y & \text{dla } C = 1, \end{cases} \quad y' = \begin{cases} y & \text{dla } C = 0,\\ x & \text{dla } C = 1, \end{cases}$$

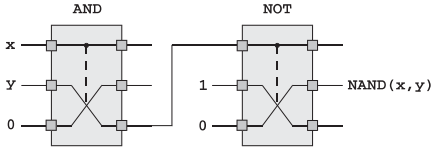
a więc bramka Fredkina pełni rolę przełącznika sterowanego stanem linii *C*.

Bramka Fredkina również umożliwia obliczenie funkcji NAND, lecz realizujący ją układ (**rys. 5**) jest bardziej skomplikowany, niż w przypadku implementacji wykorzystującej bramkę CCN.

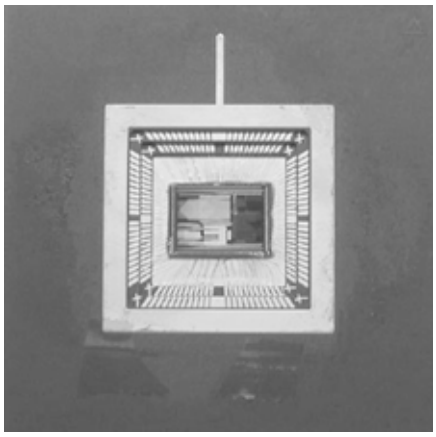
Powyższe przykłady pokazały, że jest możliwe obliczenie prostych funkcji nieodwracalnych w sposób odwracalny, a więc teoretycznie bez rozpraszania ciepła do otoczenia. W przypadku bardziej złożonych obliczeń, np. zawierających pętle o ciele wykonywanym nieznaną w momencie kompilacji liczbę razy, złożenie bramek odwracalnych nie daje się niestety bezpośrednio zastosować. Konieczne staje się więc wprowadzenie odwracalności również na poziomie samego algorytmu służącego do obliczania interesującej nas funkcji. Odwracalność dowolnego elementarnego kroku algorytmu nazywa się odwracalnością lokalną, w odróżnieniu od globalnej odwracalności całego algorytmu. Posługując się indukcją matematyczną można udowodnić, że algorytm jest globalnie odwracalny wtedy i tylko wtedy, gdy każdy jego krok ma własność odwracalności lokalnej.

Głównymi cechami odróżniającymi algorytmy odwracalne od nieodwracalnych jest sposób prowadzenia obliczeń oraz zapotrzebowanie na pamięć operacyjną.

Pierwszy etap działania algorytmu odwracalnego jest taki sam, jak w przypadku metod klasycznych: dane dostarczone przez użytkownika są w odpowiedni sposób prze-



Rys. 5. Realizacja funkcji NAND za pomocą bramek Fredkina



Fot. 6. Pendulum - pierwszy procesor wykonany na bazie logiki odwracalnej

kształcane na wynik. Po jego uzyskaniu procedura nieodwracalna niezwłocznie kończy działanie. Działanie algorytmu odwracalnego jest inne. Uzyskany wynik jest kopiowany do środowiska zewnętrznego i przekazywany użytkownikowi, po czym następuje odwrócenie kierunku przepływu sterowania i algorytm jest wykonywany wstecz, przekształcając wynik z powrotem na dane wejściowe.

Po zakończeniu tego procesu program oraz maszyna znajdują się w tym samym stanie, w którym były one przed rozpoczęciem obliczeń. Przywrócenie stanu początkowego oznacza, że cała przekształcana informacja została zachowana, a więc obliczenia mogły zostać przeprowadzone bez wydzielenia ciepła do otoczenia.

Powtórne wykorzystanie zasobów sprzętowych procesora odwracalnego, będące niezbędnym warunkiem możliwości jego praktycznego zastosowania, wymusza zapamiętanie informacji potrzebnej do odwrócenia obliczeń. Z tego powodu algorytmy odwracalne wymagają dodatkowej porcji pamięci operacyjnej na przechowywanie wyników pośrednich. Rozmiar tej pamięci zależy od liczby *t* wykonanych kroków elementarnych. Intuicja podpowiada, że zależność ta powinna być ograniczona od dołu przez funkcję liniową względem *t*, lecz szczegółowe badania teoretyczne [4, 5] obniżyły to oszacowanie do Ω(log t). Zachodzi przy tym ciekawy związek między czasem potrzebnym na wykonanie obliczeń oraz zużyciem pamięci - im mniej dodatkowej pamięci jesteśmy skłonni przeznaczyć, tym dłużej muszą potrwać obliczenia. Osiągnięcie teoretycznego minimum zapotrzebowania na pamięć oznacza jednak wykładnicze (w najgorszym przypadku) wydłużenie czasu obliczeń, co zwykle jest nieakceptowalne. Znaczenie praktyczne tego wyniku jest więc niewielkie.

Pendulum - fakty

Mikroprocesor *Pendulum* składa się z 200000 tranzystorów, ma 180 wyprowadzeń (w tym 32 służą do doprowadzenia zasilania do struktury) i może być programowany za pomocą 18 instrukcji. Jednostka sterująca Pendulum obsługuje 74-stopniowy potok przyspieszający obliczenia.

Zastosowania praktyczne

Pierwsze próby zbudowania doświadczalnych układów scalonych realizujących obliczenia odwracalne podjęto w latach 1995-1999 w Massachusetts Institute of Technology. Zespół naukowców pracujący pod kierunkiem Michaela P. Franka zaprojektował m.in. pierwszy odwracalny mikroprocesor RISC, któremu nadano nazwę *Pendulum* (wahadło). Układ ten wykonano w technologii SCRL (*Split-level Charge Recovery Logic* - przedstawimy ją w jednym z najbliższych numerów - Red.).

Wymaganie pełnej odwracalności obliczeń zostało spełnione poprzez zaprojektowanie odwracalnego zbioru instrukcji, wykonywanych przez odwracalny układ sprzętowy. Dzięki temu kierunek przepływu sterowania może zostać zmieniony na dowolnym etapie działania programu - wówczas procesor rozpocznie proces przekształcania wyniku na dane wejściowe.

Korzystnym efektem ubocznym możliwości cofania biegu programu o dowolną liczbę kroków jest znaczne ułatwienie wyszukiwania błędów w jego kodzie, co jest bardzo istotne dla twórców oprogramowania.

Oprócz wykorzystania obliczeń odwracalnych w klasycznych technikach przetwarzania informacji pełnią one kluczową rolę w obliczeniach kwantowych. Ewolucja układu bitów kwantowych jest określona przez operatory unitarne mające własność lokalnej odwracalności, dzięki czemu jest ona odwracalna globalnie.

Piotr Wyderski

Bibliografia:

1. Rasiowa H., Wstęp do matematyki współczesnej, PWN, Warszawa, 1998
2. Smith W. D., Fundamental physical limits on computation, http://citeseer.nj.nec.com/smith95fundamental.html
3. Smith W. D., Notes on reversible computation, http://citeseer.nj.nec.com/smith98notes.html
4. Li M., Vitanyi P., Reversibility and adiabatic computation: trading time and space for energy, http://citeseer.nj.nec.com/li96reversibility.html
5. Lange K., McKenzie P., Tapp A., Reversible space equals deterministic space, http://citeseer.nj.nec.com/lange98reversible.html
6. Abramsky S., A structural approach to reversible computation, http://citeseer.nj.nec.com/abramsky01structural.html