

Piotr KAWALEC

POLITECHNIKA WARSZAWSKA, WYDZIAŁ TRANSPORTU

## Układy arytmetyki stochastycznej i ich implementacja w strukturach FPGA

Dr inż. Piotr KAWALEC

Ukończył studia na Wydziale Elektroniki Instytutu Transportu w Leningradzie w 1975 r., obronił pracę doktorską w 1979 r. w Instytucie Elektrotechnicznym w Leningradzie. Jest adiunktem na Wydziale Transportu Politechniki Warszawskiej. Jego zainteresowania naukowe to automatyka, elektronika, technika cyfrowa i ich zastosowanie w układach i systemach sterowania i teledystrybucji stosowanych w transporcie.



e-mail: pka@it.pw.edu.pl

### Streszczenie

W artykule przedstawiono podstawowe układy arytmetyki stochastycznej zrealizowane w technice cyfrowej. W celu zapewnienia maksymalnej szybkości działania, syntezę układów arytmetyki stochastycznej przeprowadzono na elementach logicznych i przerzutnikach. Dla specjalizowanych układów sumatorów, subtraktorów, oraz multiplikatorów i układów potęgujących, wyznaczono dokładność przetwarzania. Przeprowadzono ich syntezę i implementację w układach FPGA, wyznaczając szybkość działania.

**Słowa kluczowe:** arytmetyka stochastyczna, sumatory, subtraktory multiplikatory, dokładność przetwarzania, realizacja sprzętowa, układy FPGA.

### Stochastic arithmetic circuits and their implementation in FPGAs

#### Abstract

The paper presents fundamental circuits of stochastic arithmetic realized by means of digital technology. In order to ensure the maximum operational speed, synthesis of stochastic arithmetic circuits has been performed on logical elements and triggers. Specialized stochastic adders on NOT and NAND elements (Fig. 1) as well as on multiplexers (Fig. 3) both without and with randomization of the input data (Fig. 2) have been designed for disjoint events in binary random sequences. Specification of stochastic adders has been conducted in VHDL language, and their verification - in functional simulation mode (Fig. 4). The accuracy of the stochastic adder operation has been determined, whereas synthesis and implementation of these systems in FPGA structure allowed for showing the speed of stochastic adder operation with the frequency of timing exceeding 100 MHz. Similar investigations have been carried out for specialized stochastic subtractors. For independent binary random sequences, stochastic multipliers and squaring circuits (Fig. 6) have been designed, having a structure particularly useful for realization within programmable logical FPGA structures.

**Keywords:** stochastic arithmetic, adders, subtractors, multipliers, conversion accuracy, hardware implementation, FPGA devices.

## 1. Wstęp

W systemach sterowania ruchem w transporcie wiele atrybutów obiektów i procesów transportowych ma charakter losowy, przy czym przyjmuje się, że stosowane zmienne losowe są przedziałami stacjonarne (np. w metodzie sterowania ruchem drogowym HCM, zakłada się 15 minutową lub godzinną stacjonarność parametrów strumieni pojazdów) [1]. Możliwe jest więc zastosowanie, w tych systemach, do przetwarzania danych losowych, oraz do realizacji probabilistycznych algorytmów sterowania, specjalizowanych układów i systemów cyfrowych nazywanych komputerami stochastycznymi, lub stochastycznymi przetwornikami informacji [2, 3].

Mimo że algorytmy probabilistyczne cechuje mała zbieżność, to ich sprzętowa realizacja, a zwłaszcza ich implementacja w układach FPGA, pozwala na zastosowanie takich algorytmów nawet w sterowaniu w czasie rzeczywistym. Przykładem może być

zastosowanie stochastycznych układów arytmetycznych w różnego rodzaju sterownikach czasu rzeczywistego, np. w cyfrowych impulsowych regulatorach mocy PWM [4, 5].

Ogromną zaletą stosowania stochastycznych układów arytmetycznych jest ich odporność na przemijające uszkodzenia, co w przypadku urządzeń sterowania i kierowania ruchem w transporcie ma zasadnicze znaczenie dla bezpieczeństwa ruchu pojazdów w sieci transportowej [1].

## 2. Stochastyczne sumatory i subtraktory

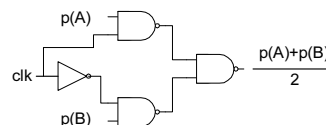
Zdarzenia wystąpienia symbolu 1 w przetwarzanych losowych ciągach binarnych oznaczmy  $A$  oraz  $B$ , natomiast prawdopodobieństwo wystąpienia symbolu 1 w każdym z ciągów, oznaczmy odpowiednio  $p(A)$  oraz  $p(B)$ .

Jeżeli  $A$  i  $B$  są zdarzeniami elementarnymi, to prawdopodobieństwo sumy zdarzeń ma postać [6]

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \quad (1)$$

Z zależności (1) wynika, że jeżeli zdarzenia  $A$  i  $B$  są zdarzeniami rozłącznymi, to prawdopodobieństwo sumy zdarzeń, równe jest sumie prawdopodobieństw tych zdarzeń. A więc, aby uzyskać najprostszą realizację układu sumującego, należy wykluczyć równoczesne podanie w wejściowych ciągach losowych  $A$  i  $B$  wartości 1.

Dla niezależnych, losowych ciągów binarnych, z prawdopodobieństwem wystąpienia symbolu 1 w każdym takcie w odpowiednich ciągach oznaczonym  $p(A)$  i  $p(B)$ , sprzętową realizację sumy, przedstawiono na rys. 1.



Rys. 1. Sumator stochastyczny na elementach NOT i NAND  
Fig. 1. Stochastic adder on NOT and NAND elements

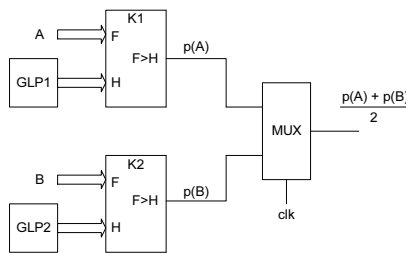
Rozłączność zdarzeń  $A$  i  $B$  w czasie, uzyskujemy wykorzystując inwertor w jednej z gałęzi sygnału taktującego  $clk$ . W każdym takcie zegarowym sygnał  $clk$ , przemienne, umożliwi przesłanie na wyjście układu wartość binarną 0 albo 1 z wejścia  $p(A)$  oraz z wejścia  $p(B)$ . Na wyjściu sumatora stochastycznego realizowana jest zależność logiczna

$$\overline{p(A) \cdot p(B)} = \overline{p(A)} + \overline{p(B)} = p(A) + p(B) \quad (2)$$

Uwzględniając, że dla danych binarnych, logiczne i arytmetyczne operacje sumy i iloczynu są identyczne, zależność (2) realizuje sumę arytmetyczną. Ponieważ w procesie losowania, każdy z kanałów uczestniczy w operacji sumowania średnio z wagą  $1/2$ , wynik operacji sumowania również jest równy połowie rzeczywistego wyniku. A więc układ przedstawiony na rys. 1, w istocie, jest układem mnożąco – sumującym. Przywrócenie właściwego wyniku sumowania w procesie derandomizacji, polega na przesunięciu estymatora wartości oczekiwanej zmiennej losowej liczby symboli 1 w ciągu wynikowym, w lewo o jeden bit.

Jeśli dane wejściowe są liczbami determinowanymi, bądź mają charakter losowy, lecz nie spełniają warunków schematu Bernoulliego, należy przeprowadzić randomizację danych wejściowych, wykorzystaniem losowania niezależnego, z wykorzystaniem generatorów liczb losowych, bądź pseudolosowych, o rozkładzie równomiernym GLP. Jako źródło losowości mogą być zastosowane sprzętowe generatory liczb pseudolosowych zbudowane na LFSR'ach [7, 8].

Dodatkowo założono, że dane wejściowe A i B przedstawione są w postaci liczb stałoprzecinkowych tak, aby zarówno dane wejściowe jak i liczby pseudolosowe miały ten sam zakres (0,1). Alternatywnym rozwiązaniem jest skalowanie liczb pseudolosowych z GLP, do zakresu danych wejściowych A i B. Przy tych założeniach sumator stochastyczny może być zbudowany poprzez dodanie do wyżej przedstawionego schematu (rys. 1) układów randomizujących. Prostsza realizację sumy, z zapewnieniem rozłączności zdarzeń A i B, można uzyskać zastępując elementy NOT i NAND, multiplexerem MUX (rys. 2).



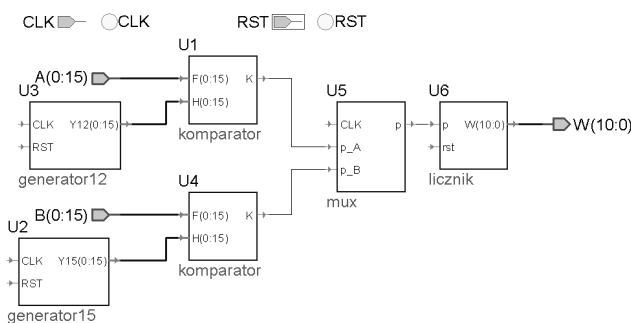
Rys. 2. Stochastyczny sumator z randomizacją danych wejściowych  
Fig. 2. Stochastic adder with randomisation of input data

Układ randomizujący, zbudowany na komparatorach K1 i K2, umożliwi przeprowadzenie niezależnego losowania, poprzez porównanie danych A oraz B z liczbami pseudolosowymi uzyskiwanymi z niezależnych kanałów GLP1 oraz GLP2 generatora wielokanałowego GLP o rozkładzie równomiernym [7]. Zastosowanie różnych generatorów liczb pseudolosowych zwiększa pewność niezależności generowanych binarnych ciągów losowych na wyjściach komparatorów K1 oraz K2. Oczywiście, ponieważ w każdym kanale GLP produkowane liczby pseudolosowe są niezależne, to można było w procesie randomizacji wykorzystać liczby pseudolosowe generowane przez jeden wspólny generator.

Jeśli porównywana liczba A lub B jest większa od liczby pseudolosowej wygenerowanej odpowiednio przez generator GLP1 lub GLP2 (rys. 2), to na wyjściu komparatora K1 lub K2, pojawia się wartość 1. W wyniku wielokrotnego przeprowadzenia losowania niezależnego, na wyjściach komparatorów formują się losowe ciągi binarne o rozkładzie zerowyjedyńkowym, z prawdopodobieństwem wystąpienia wartości 1 oznaczonym odpowiednio  $p(A)$  lub  $p(B)$ . Multiplexer MUX, przekazujący sygnał z jednego wejść na wyjście zgodnie z wartością sygnału zegarowego clk, zapewnia rozłączność zdarzeń w kanałach A i B.

Derandomizację wyniku przetwarzania można przeprowadzić zliczając ilość pozytywnych wyników niezależnych losowań, tzn. zliczając ilość symboli o wartości 1 w wyjściowym losowym ciągu binarnym. Zliczanie przeprowadza się z zastosowaniem licznika o pojemności nie mniejszej niż liczba przeprowadzanych losowań niezależnych.

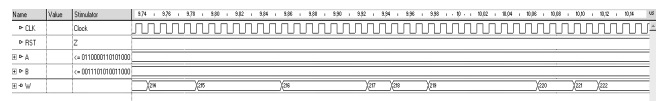
Specyfikację, w środowisku języka VHDL, przedstawionych koncepcji sumatorów stochastycznych, przeprowadzono w sposób strukturalny, w edytorze schematów blokowych BDE. Jako źródła losowości wykorzystano generatory nazwane *generator12* i *generator15* generatora wielokanałowego GLP [7] (rys. 3).



Rys. 3. Specyfikacja sumatora stochastycznego na multiplexserze  
Fig. 3. Stochastic adder specification on multiplexer

Dla uproszczenia schematu, sygnałom: zegarowemu CLK, oraz ustawiającemu RST, nadano atrybut sygnałów globalnych. Wyjściowy losowy ciąg binarny został podany na wejście licznika asynchronicznego *licznik*, o pojemności  $2^{11}$ , co zapewnia możliwość przeprowadzania derandomizacji losowych ciągów binarnych o liczebności próbki do 2048. Przedstawiony na rys.3, sumator po wyspecyfikowaniu w języku VHDL, został poddany weryfikacji w trybie symulacji funkcjonalnej. Wyniki symulacji potwierdziły poprawność działania układu.

Na przebiegach czasowych symulacji funkcjonalnej (rys. 4) dla przykładowych, podanych w postaci binarnej, wartości  $A = 25000$ , oraz  $B = 15000$  (co odpowiada prawdopodobieństwom  $p(A) = 0,38$ , oraz  $p(B) = 0,23$ ), widoczna jest na wyjściu W, w postaci dziesiętnej, liczba zliczonych wartości 1 w czasie niezależnego losowania. Odnosząc zawartość licznika do liczby przeprowadzonych prób (liczby taktów zegara CLK), uzyskujemy wartość średnią pozytywnych wyników losowań do ogólnej liczby losowań, a więc estymator prawdopodobieństwa  $[p(A) + p(B)]/2$ .



Rys. 4. Przebiegi symulacji funkcjonalnej sumatora stochastycznego  
Fig. 4. Functional simulation courses of stochastic adder

Wyznaczając dokładność wykonywania operacji sumowania przedstawionych powyżej sumatorów stochastycznych, należy uwzględnić, że zmienna losowa K, odpowiadająca liczbie wartości 1 w wynikowym losowym ciągu binarnym, ma rozkład dwumianowy, dla którego funkcja prawdopodobieństwa ma postać [6]

$$P(k) = C_n^k p^k (1-p)^{n-k} = \frac{n!}{k!(n-k)!} p^k (1-p)^{n-k}$$

Wartość oczekiwana i wariancja dla rozkładu dwumianowego

$$E(K) = np ; Var(K) = np(1-p)$$

Uwzględniając, że błędy, przy losowaniu niezależnym, dla dużych n mają rozkład normalny, błąd względny sumowania stochastycznego wyniesie

$$\delta(K) = \lambda_p \frac{\sqrt{Var(K)}}{E(K)} = \lambda_p \frac{\sqrt{np(1-p)}}{np} \leq \frac{\lambda_p}{\sqrt{n}} \quad (3)$$

Z wyrażenia (3) wynika, że dokładność przetwarzania jest proporcjonalna do kwadratu liczby losowań. Dla zapewnienia błędu względnego  $\delta(Z) \leq 5\%$ , z prawdopodobieństwem 0,95 (kwantyl rozkładu normalnego  $\lambda_p = 1,645$ ), licznik stosowany do derandomizacji, powinien być licznikiem co najmniej 10 bitowym.

W wyniku syntezy i implementacji opracowanych sumatorów stochastycznych w układach FPGA, uzyskano częstotliwość pracy powyżej 100 MHz, przy znikomym wykorzystaniu zasobów struktury. Przy tej częstotliwości taktowania, sumator stochastyczny wykonuje operacje sumowania, z dokładnością 5%, w ciągu 10  $\mu$ s, a więc kolejne wyniki sumowania mogą być uzyskiwane z częstotliwością 100 kHz.

Układy realizujące odejmowanie zmiennych losowych przedstawionych w postaci losowych ciągów binarnych, można nazwać analogicznie do nazwy sumatorów stochastycznych, subtraktorami stochastycznymi. W układach tych operacja odejmowania zastępowana jest operacją sumowania zdarzeń, w której zdarzenie odpowiadające odjemnikowi, zastępowane jest zdarzeniem przeciwnym. W przypadku losowych ciągów binarnych, zdarzenia przeciwne uzyskuje się dokonując inwersji poszczególnych bitów ciągu losowego. Operacja ta jest bardzo prosta do realizacji sprzętowej przy wykorzystaniu najprostszego elementu logicznego NOT, umieszczonego na wejściu odjemnika do multiplexsera MUX (rys. 3).

Dla zachowania jednoznacznej postaci zapisu estymatora wartości oczekiwanej wyniku, należy przeprowadzić wstępne porównanie operandów, tak aby wartość bezwzględna odjemnej była zawsze większa od wartości bezwzględnej odjemnika. Operacja porównania liczb jest bardzo prosta dla postaci deterministycznej operandów, natomiast, jeśli przetwarzane są losowe ciągi binarne odpowiadające atrybutom obiektów lub procesów transportowych, z kontekstu atrybutu można przeprowadzić porównanie wartości jego estymatorów. Tak sytuacja ma miejsce np. przy modelowaniu rozplywu strumieni pojazdów w ruchu drogowym.

Ponieważ w procesie odejmowania przeprowadzane są losowania niezależne zgodnie ze schematem Bernoulliego, dokładność i szybkość działania subtraktorów stochastycznych wyznacza się z tych samych zależności jak dla sumatorów stochastycznych. Weryfikacja prototypów subtraktorów zaimplementowanych w układach FPGA w pełni potwierdziła poprawność ich działania, a uzyskane parametry dokładności i szybkości działania odpowiadają parametrom sumatorów stochastycznych.

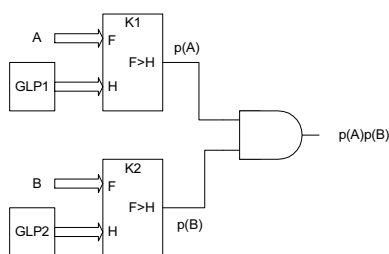
### 3. Stochastyczne multiplikatory i układy potęgujące

Dla niezależnych zdarzeń A i B, prawdopodobieństwo iloczynu zdarzeń jest równe iloczynowi prawdopodobieństw zdarzeń

$$P(A \cap B) = P(A) \cdot P(B) \quad (4)$$

Zależność (4) jest podstawową zależnością wykorzystywaną do realizacji operacji mnożenia zmiennych probabilistycznych, odwzorowywanych w postaci niezależnych losowych ciągów binarnych. A więc operacja mnożenia może być zrealizowana sprzętowo na jednym elemencie logicznym AND. Specjalizowane układy mnożące losowe ciągi binarne, nazywane będą multiplikatorami stochastycznymi.

Jeśli dane wejściowe są zdeterminowane, bądź są zmiennymi losowymi niespełniającymi warunków losowania niezależnego zgodnego ze schematem Bernoulliego, należy przeprowadzić proces randomizacji przetwarzanych danych wejściowych. Multiplikator stochastyczny, z randomizacją danych wejściowych, przedstawiono na rys. 5.



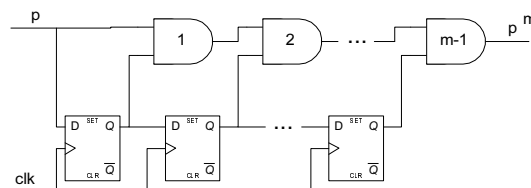
Rys. 5. Multiplikator stochastyczny z randomizacją danych wejściowych  
Fig. 5. Stochastic adder with random channel choice

Układ randomizacji danych wejściowych działa analogicznie jak w przypadku sumatorów stochastycznych, zakres zmiennych wejściowych jest taki sam jak zakres generowanych liczb pseudolosowych (0,1), natomiast niezależność generowanych losowych ciągów binarnych  $p(A)$  oraz  $p(B)$ , zapewniają zarówno parametry generowanych liczb pseudolosowych, oraz, dodatkowo, zastosowanie dwóch niezależnych generatorów GLP1 oraz GLP2 z wielokanałowego generatora liczb pseudolosowych GLP [7].

Ponieważ uczestniczące w operacji mnożenia, losowe ciągi binarne są ciągami niezależnymi, więc i wynikowy losowy ciąg binarny jest ciągiem niezależnym. A więc, dokładność wykonania operacji określana jest zależnością (3), a uzyskana szybkość działania multiplikatora determinowana jest szybkością taktowania GLP, i przy implementacji w układzie Spartan 3, częstotliwość taktowania przekracza 100MHz.

Do realizacji operacji podnoszenia do dowolnej całkowitoliczbowej potęgi  $m$ , można wykorzystać przedstawione powyżej

multiplikatory stochastyczne, jednak znacznie prostszą realizację można uzyskać, podając na wejścia elementu AND ten sam losowy ciąg binarny, którego realizację przesunięte są o jeden, lub więcej taktów zegarowych. Przesunięcie to można uzyskać stosując przerzutniki D w jednym z kanałów (rys. 6).



Rys. 6. Stochastyczny układ podnoszący do  $m$  potęgi  
Fig. 6. Stochastic circuit raising to  $m$  power

Specjalizowane układy potęgowania (rys. 6) są implementowane w programowalnych strukturach logicznych FPGA, w których realizacja funkcji logicznej AND o dowolnej liczbie wejść nie stanowi żadnego problemu. Więc, jeśli pośrednie wartości potęg nie są nam niezbędne, celowa jest realizacja układu podnoszącego do potęgi  $m$ , z wykorzystaniem  $m-1$  bitowego rejestru przesuwającego, oraz  $m$  wejściowego elementu logicznego AND.

### 4. Wnioski

Przedstawione w artykule układy arytmetyki stochastycznej wraz z wcześniej opracowanymi probabilistyczno – czasowymi układami dzielącymi [9], pozwalają na stwierdzenie, że został opracowany funkcjonalnie pełny zbiór układów arytmetyki stochastycznej, zbudowany z elementów logicznych i rejestrów przesuwających. Zaimplementowanie opracowanych układów w strukturach FPGA, pozwala na przetwarzanie z częstotliwością taktowania przekraczającą 100 MHz.

Dzięki temu możliwe jest uzyskanie estymatorów danych losowych przedstawionych w postaci ciągów binarnych z częstotliwością przekraczającą 100 kHz, co pozwala na tworzenie efektywnych modeli procesów transportowych, działających w czasie rzeczywistym.

### 5. Literatura

- [1] Adamski A.: Inteligentne systemy transportowe. Wydawnictwa AGH, Kraków, 2003.
- [2] Gaines B.R.: Stochastic computing systems. Advances in Information Systems Science, New York, 1969, pp. 37 – 172.
- [3] Kawalec P.: Badanie stochastycznych przetworników informacji i ich implementacja w programowalne struktury logiczne FPGA. Sprawozdanie z grantu JM Rektora PW, Wydział Transportu PW, Warszawa, 2001.
- [4] Nerto S., Bolognani S., Ceschia M. i in.: FPGA-based random PWM with real-time dead time compensation. Proc. IEEE PESC'03, vol. 2, 2003, pp.15 – 19.
- [5] Zhang D., Li H., Foo S. Y.: A simplified FPGA implementation of neural network algorithms integrated with stochastic theory for power electronics applications. IEEE-IECON, 2005, pp.1018 – 1023.
- [6] Bobrowski D.: Probabilistyka w zastosowaniach technicznych. WNT, Warszawa, 1986.
- [7] Kawalec P.: Synteza i weryfikacja wielokanałowego generatora liczb pseudolosowych zaimplementowanego w układzie FPGA. Materiały IV Krajowej Konferencji Naukowej „Reprogramowalne układy cyfrowe RUC'2001”, Szczecin, 2001, str. 291 – 298.
- [8] Marsaglia G.: Xorshift RNGs. Jurnal of statistical software, vol. 8, iss.14, 2003.
- [9] Kawalec P.: Analiza probabilistyczno – czasowych przetworników informacji i ich implementacja w układach FPGA. Pomiary Automatyka Kontrola, 8 – 2008, vol.54, Wydawnictwo PAK, Warszawa, 2008, str. 602 – 604.