Yaroslav NYKOLAYCHUK
West Ukrainian National University

Volodymyr HRYHA
Vasyl Stefanyk Precarpathian National University

Nataliia VOZNA, Ihor PITUKH
West Ukrainian National University

Lyudmila HRYHA
Nadvirna Vocational College by NTU

HIGH-PERFORMANCE COMPONENTS OF HARDWARE MULTI-BIT SPECIFIC PROCESSORS FOR THE ADDITION AND MULTIPLICATION OF BINARY NUMBERS

The relevance of solving the priority improvement problem for functional and computational components of microelectronics for arithmetic and logic unit (ALU) of modern supercomputers is emphasized. It is shown that in the structures of ALU operations such as: comparison, multiplexing and adding affect the marginal productivity of ALU. It is substantiated that mathematical operations of addition, accumulation of sums, multiplication and division are crucial for ensuring extremely high speed of vector and scalar computers. The purpose of the work is the development of new calculation algorithms and microelectronic structures of multi-bit ALU coprocessors, which are characterized by extremely minimal parameters of speed, hardware and structural complexity. Such high-performance coprocessors are widely used as components of ALU when performing algorithmically complex calculations of statistical, correlation, spectral, cluster and entropy analysis. High-speed co-processors for multiplication and accumulation of digital data with the properties of crypto-protection of telecommunication channels are effectively used in the conditions of military operations and the modern information front, for example, in unmanned aerial vehicles, ground launchers and processors of air defense systems. The main areas for improving system characteristics of microelectronic components of the ALU processors of vector and scalar supercomputers are outlined. Structures of combinational and synchronized single-bit binary adders are systematized due to the characteristics of minimum hardware complexity and maximum speed. The theoretical foundations of double binary arithmetic are outlined. A new structure of a high-performance matrix multiplier based on synchronized adder-accumulators and Booth's algorithm is proposed, which is characterized by increased speed compared to known structures. Grounded perspective directions for further development improvement of the basic characteristics of the investigated class of computing equipment components.

Key words: structures, ALU, microelectronics, matrix multiplier, Booth's algorithm, supercomputers

Ярослав НИКОЛАЙЧУК
Західноукраїнський національний університет

Володимир ГРИГА
Прикарпатський національний університет імені Василя Стефаника

Наталія ВОЗНА, Ігор ПІТУХ
Західноукраїнський національний університет

Людмила ГРИГА
ВСП "Надвірнянський фаховий коледж"

ВИСОКОПРОДУКТИВНІ КОМПОНЕНТИ АПАРАТНИХ БАГАТОРОЗРЯДНИХ СПЕЦПРОЦЕСОРІВ СУМУВАННЯ ТА ПЕРЕМНОЖЕННЯ ДВІЙКОВИХ ЧИСЕЛ

Акцентована актуальність вирішення проблеми пріоритетного удосконалення функціонально-обчислювальних компонентів мікроелектроніки арифметико-логічних пристроїв (АЛП) сучасних суперком'ютерів. Показано, що у структурах АЛП операції типу: порівняння, мультиплексування та додавання впливає на граничну продуктивність АЛП. Обгрунтовано, що математичні операції додавання, накопичення сум, перемноження та ділення є визначальними для забезпечення гранично високої швидкодії векторних та скалярних комп'ютерів. Метою роботи є розробка нових алгоритмів обчислень та мікроелектронних структур співпроцесорів багаторозрядних АЛП, які характеризуються гранично мінімаксними параметрами швидкодії, апаратної та структурної складності. Такі високопродуктивні співпроцесори широко застосовуються у якості компонентів АЛП при реалізації алгоритмічно-складних обчислень статистичного, кореляційного, спектрального, кластерного та ентропійного аналізу. Максимально-швидкодіючі співпроцесори перемноження та накопичення цифрових даних з властивостями криптозахисту телекомунікаційних каналів, ефективно застосовуються в умовах військових операцій та сучасного інформаційного фронту. Наприклад, у безпілотних літальних апаратів, наземних пускових установках та процесорах систем протиповітряної оборони. Викладені пріоритетні напрямки покращення системних характеристик мікроелектронних компонентів процесорів АЛП векторних та скалярних суперком'ютерів. Систематизовані структури комбінаційних та синхронізованих однорозрядних двійкових суматорів з характеристиками мінімальної апаратної складності та максимальної швидкодії. Викладені теоретичні основи бінарної двійкової арифметики. Запропонована нова структура високопродуктивного матричного перемножувача згідно алгоритму Бута, який характеризується підвищеною швидкодією у порівнянні з відомими структурами. Обгрунтовані перспективні напрямки подальшого розвитку та покращення базових характеристик досліджуваного класу компонентів обчислювальної техніки.

Key words: структура, АЛП, мікроелектроніка, матричний перемножувч, алгоритм Бута, суперком'ютер

Introduction

One of the main and relevant directions for improving the ALU coprocessors of supercomputers is achieving the maximum possible speed of calculations of high capacity mono-binary codes (MBCs). Reduction in algorithmic and structural complexity, as well as the heat reduction released by the crystals of the ALU coprocessor chips is the main characteristic of improving the ALU coprocessors.

Such high-performance coprocessors are widely used as components of ALU when performing algorithmically complex calculations of statistical, correlation, spectral, cluster and entropy analysis. High-speed co-processors for multiplication and accumulation of digital data with the properties of crypto-protection of telecommunication channels are effectively used in the conditions of military operations and the modern information front, for example, in unmanned aerial vehicles, ground launchers and processors of air defense systems [1,2].

This is very effective when solving complex mathematical and algorithmic problems in the field of cryptography, holography and pattern recognition by processing RGB images in digital video cameras.

This type of calculation optimization devices can be improved when applying mathematical foundations of binary arithmetic and synchronized adder-accumulators.

Related works

Modern significant progress in the development of multi-core vector and scalar supercomputers is based on the application of achievements in microelectronics and nanotechnology [1-3]. The world's leading companies (Intel, IBM, DEC, Motorola, ARM, SPARC, MIPS, PowerPC) are replicating multi-bit processors for universal and specialized computers. The implementation of logical and computational operations in known supercomputers is usually realized in binary arithmetic of Rademacher's theoretical-numerical basis (TNB). Supercomputers of 64-bit architecture, including EM64T, Turion 64, Xeon, Core2, Corei3, Corei5, Intel (IA-64 (Itanium)), Ultra SPARC (Sun Microsystems) MIPS64 (MIPS) have a significant prospect of application in all branches of industry and military special equipment [4].

Ultra-high-performance supercomputers are used to perform complex engineering and scientific computations and other resource-intensive tasks of military equipment.

The type of such processors includes the ALU of vector and scalar supercomputers developed by Cray, Fujitsu, Hitachi, Nec, DLXV, IBM, HP [1-5].

Large bit-width hardware multipliers for binary codes, which contain n^2 of single-bit binary adders, are widely used in 32-, 64- and 128-bit coprocessors of universal computers (IBM, HP, Cray, Fujitsu, Hitachi) [6-8].

In [9-11], typical structures of ALUs in supercomputers were given, were corresponding ALU structures, which are served by the data bus without access to the accumulator registers of individual cores.

The availability of memory registers in structures of this type of ALUs provides wide possibilities of deeply synchronized and parallel algorithms for multiplication [12], division, exponentiation, etc.

The extremely widespread use of classical binary arithmetic with ripple carry-overs between bits in modern computer systems and superprocessors is a very negative factor for increasing the speed of large bit-width computing devices. For example, when adding and multiplying two n-bit MBCs, signals are delayed in the computing device by n and 2n+(n-1) clock cycles, respectively. That is, when the memory registers of the ALU cores in supercomputers are in the range of 128-2048 bits, the signal delay is, respectively, 256-4096 clock cycles when performing an addition operation in classical multi-bit binary adders (MBAs) [13] with direct data inputs and outputs. Similarly, the speed of matrix multipliers based on such components is 2048+(2048-1)=4095 clock cycles, respectively. It is obvious that such speed is insufficient and practically unacceptable to solve many modern problems, even on the basis of microelectronics of quantum computers.

Systematization of characteristics of single-bit combinational and synchronized binary adders with minimax characteristics

Today, in the field of development of microelectronic structures of single-bit half, full, combinational and synchronized binary adders, the structures proposed by us are characterized by minimal hardware complexity, maximum speed of executing ripple carry-overs and generating logical sum values [14-20].

Fig. 1 shows single-bit components of MBAs based on direct data inputs, direct inputs of ripple carry-overs and direct outputs of sums.

Such a full adder (right) has the following system characteristics:

1. A – hardware complexity: A = 7V (V - gates).

2. Input/output speed parameters: $\tau_1 (a_i y_i \rightarrow S_i) = 2\upsilon$, $\tau_2 (a_i y_i \rightarrow C_{out}) = 2\upsilon$, $\tau_3 (C_{in} \rightarrow C_{out}) = 2\upsilon$, υ - microcycles.

Such a full adder (left) has the following system characteristics:

1. A – hardware complexity: A = 6V.

2. Input/output speed parameters: $\tau_1 (a_i b_i \rightarrow S_i) = 2\upsilon$, $\tau_2 (C_{in} \rightarrow \overline{C_{out}}) = 1\upsilon$, $\tau_3 (a_i b_i \rightarrow \overline{C_{out}}) = 2\upsilon$.
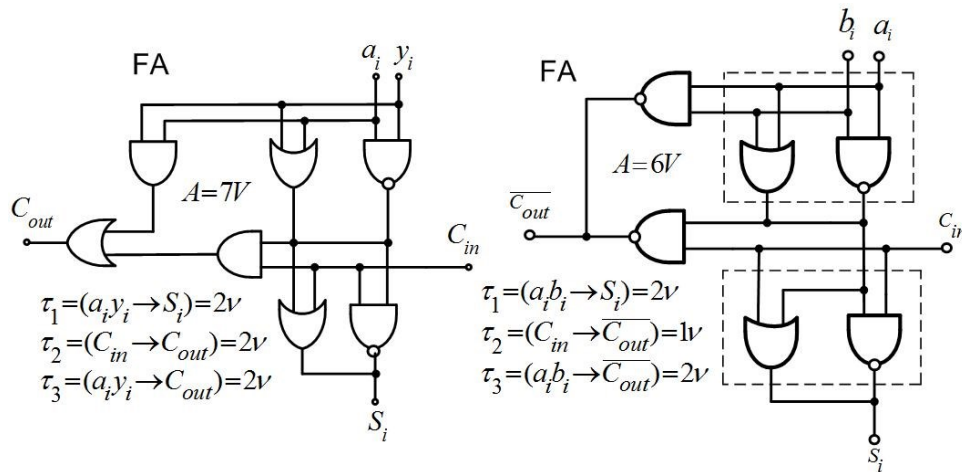
Fig.1. Microelectronic structures of single-bit full adders

Fig. 2a microelectronic shows structure of 6-gate single-bit binary full adder (FA) with paraphase data inputs and direct output of the sum, inverse inputs and outputs of ripple carry-overs and extended functionality of generating the inverse output of the sum ($\overline{S}_{Ni}$) of the first half adder (HA1).

 Fig. 2b shows the minimax structure of 8-gate full adder with paraphase data inputs (qubits), inverse sum output ($\overline{S}_i$) and inverse inputs / outputs of ripple carry-overs ($\overline{C}_{in}$, $\overline{C}_{out}$) .

a)   b)
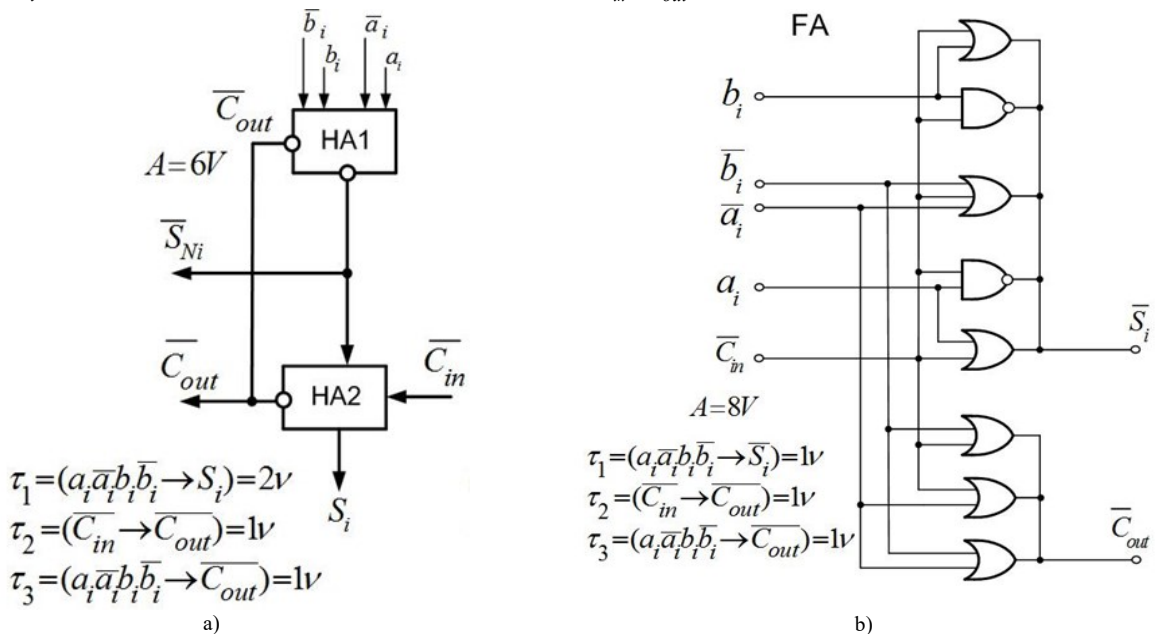**Fig.2. Microelectronic structures of single-bit adders: a) 6-gate structure of single-bit FA; b) 8-gate structure of single-bit FA**

Such a FA (fig.2a) has the following system characteristics:
1. A – hardware complexity: A = 6V.
2. Input/output speed parameters: τ_1($a_ib_i \to S_i$) = 2υ, τ_2 ($\overline{C}_{in} \to \overline{C}_{out}$) = 1$\upsilon$, τ_3 ($a_ib_i \to \overline{C}_{out}$) = 1$\upsilon$.

This structure of a single-bit adder (Fig.2b), in comparison with the well-known high-speed adder with paraphase inputs and outputs [21-23], which is a component of streaming multi-bit matrix multipliers and contains 20 logic gates, has 2.5 times less hardware complexity and, respectively, characteristics of reduced power consumption and crystal heat release.

Such a FA (fig.2b) has the following system characteristics:
1. A – hardware complexity: A = 8V.
2. Input/output speed parameters: τ_1($a_ib_i \to S_i$) = 1υ , τ_2 ($\overline{C}_{in} \to \overline{C}_{out}$) = 1$\upsilon$, τ_3 ($a_ib_i \to \overline{C}_{out}$) = 1$\upsilon$

The developed single-bit combinational adders with minimax characteristics compared to the well-known classical structure [13], which contains 13 logic gates, has a signal delay of 6 clock cycles when generating the sum

and a ripple carry delay of 2 clock cycles, provide speed increase by 6 times when generating the sum signals and by 2 times when generating the ripple carry signals, as well as the reduction in hardware complexity by 1.6-2.2 times, respectively.

Fig. 3 show the proposed structure of single-bit synchronized full adder-accumulator (SFAA) with memory on D-triggers [16, 18].

Fig. 3. Microelectronic structures of synchronized full adder-accumulator

Such a SFAA has the following system characteristics:

1. A – hardware complexity: A = 10V.

2. Input/output speed parameters: $\tau_1(S_i \rightarrow NS_i) = 4\upsilon$, $\tau_2 (C_{in} \rightarrow C_{out}) = 3\upsilon$, $\tau_3 (a_i b_i \rightarrow C_{out}) = 4\upsilon$.

The developed single-bit synchronized combinational adders and synchronized adder-accumulators with minimax characteristics are the basic components of multi-bit synchronized adder-accumulators that perform computational operations of double binary arithmetic [24].

Theoretical foundations of double binary arithmetic

The basis of the binary arithmetic of the ALU in multi-bit supercomputers is the registration of the double binary code (DBC) for each bit, the sum bits ($\dot{S}_j$) and the ripple carry bits ($\dot{C}_j$) [24].

An example of generating DBC, as a result of adding two mono-binary codes (MBC) (x and y), is shown as the following graph:

$$x = (a_{n-1}, \quad \ldots \quad , a_i, \quad \ldots \quad , a_1, \quad a_0 \quad)$$
$$+y = (b_{n-1}, \quad \ldots \quad , b_i, \quad \ldots \quad , b_1, \quad b_0 \quad) ,$$
$$\dot{d} = (\dot{C}_n < \dot{S}_{n-1}, \ldots \quad , \dot{C}_{i+1} < \dot{S}_i, \ldots \quad \dot{C}_2 < \dot{S}_1, \ \dot{C}_1 < \dot{S}_0)$$

where $x = \sum_{i=0}^{n-1} a_i \times 2^i$; $y = \sum_{i=0}^{n-1} b_i \times 2^i$; $\dot{d} = \sum_{i=0}^{n-1} \dot{S}_i \times 2^i + \sum_{i=0}^{n-1} \dot{C}_{i+1} \times 2^i$.

Thus, each position of a double binary number is presented by two bits ($\dot{C}_j$ $\dot{S}_j$), which correspond to quadrilateral arithmetic according to Table 1.

Table 1

Notation of a DBC position

$\dot{C}_{i+1}$	$\dot{S}_i$	$\dot{d}_i$
0	0	0
0	1	S
1	0	2S
1	1	3S

Generation of a double binary code is shown on the example of adding two 8-bit Fermat and Mersenne numbers, which correspond to the following numbers in the decimal and mono-binary number systems: $255_{(10)} = 11111111_{(2)}$; $129_{(10)} = 10000001_{(2)}$.

Let us write these numbers in the form of a DBC and perform the operation of addition on them:

$$\dot{x} = (0 < 1, \quad \ldots \quad , 0 < 1, \quad \ldots \quad , 0 < 1, \quad 0 < 1)$$

$$+ \dot{y} = (0 < 1, \quad \ldots \quad , 0 < 0, \quad \ldots \quad , 0 < 0, \quad 0 < 1)$$

$$\dot{d} = (1 < 1, \quad \ldots \quad , 1 < 0, \quad \ldots \quad , 1 < 0, \quad 1 < 0)$$

Such operation of generating a DBC by adding two mono-binary codes (x, y) and generating their sum ($\dot{d}$) is performed using the structure of the n-bit combinational adder, which is shown in Fig. 4.
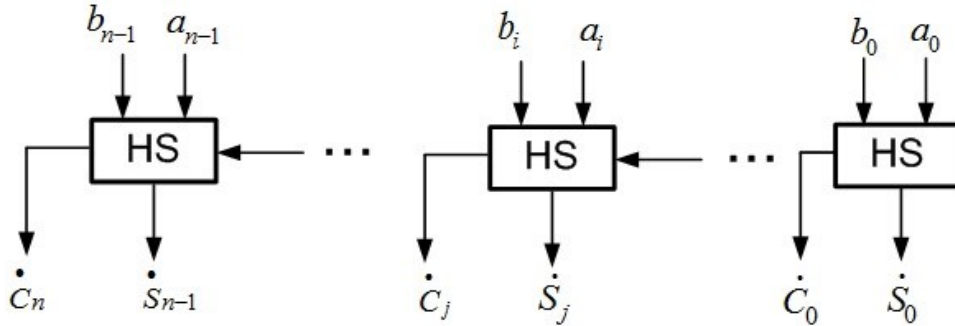
Fig. 4. Structure of n-bit sumator of DBC

An important feature of addition of two multi-bit binary mono-codes, which is implemented according to the structure shown in Fig. 4, is its maximum achievable speed, i.e., 1 clock cycle regardless of the capacity of the input codes.

The theory of double binary arithmetic developed by Professor Ya. Nykolaychuk [24] refers to a new, previously unknown, number system (YaN), the use of which allows us to increase the speed of digital data processing, presented by multi-bit binary codes, by several orders.

The use of DBCs in the ALU structures of supercomputers allows us to increase the speed of calculations and the performance of digital data processing by 1-3 orders.

Synchronized multi-bit adder-accumulators

This type of adders is widely used in processors for statistical, correlation and spectral analysis, as well as in the structures of high-performance synchronized matrix multipliers based on Booth's algorithm [25].

In Fig. 5, the structure of a synchronized multi-bit adder-accumulator (SMAA) [15], which is a component of the device for determining the selective mathematical expectation, is proposed.
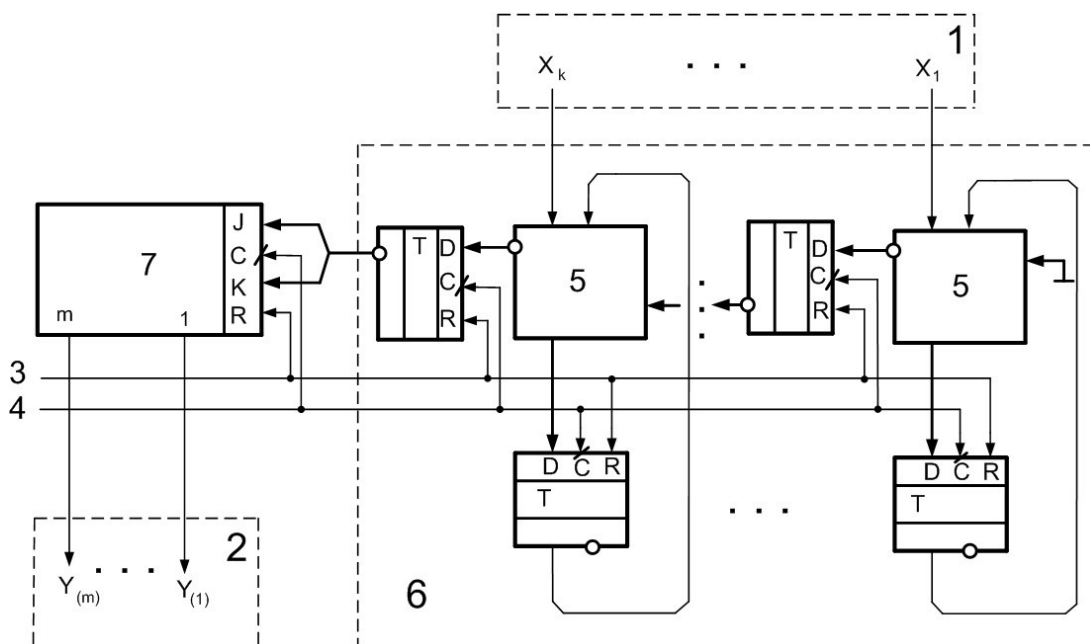

Fig. 5. Structure of the device for determining mathematical expectation

The device consists of the following components: 1 – input n-bit data bus; 2 – output m-bit data bus; 3 – channel for resetting triggers to zero state; 4 – synchronization channel; 5 – single-bit FSA; 6 – synchronized multi-bit adder accumulator; 7 – synchronized binary counter on JK triggers.

The mathematical expectation is calculated according to the expression [12]:

$$M_x = \frac{1}{n} \sum_1^n x_i \ , \qquad (1)$$

where, n – sample size; k, m – bits of input and output codes.

The main advantage of the synchronized adder- accumulator as part of the device for determining selective mathematical expectation is the implementation of the addition operation in 4 clock cycles regardless of the capacity of the input binary codes, which provides an increase in the speed of such processors by 1-2 orders compared to the accumulation of the binary numbers sum in combinational adders with ripple carry-overs [13].

An advantage of such a device for determining the selective mathematical expectation is that the accumulated DBCs are not needed to be decoded, since in the most significant bits a synchronous binary counter is used based on JK-triggers, which with a delay of 2 clock cycles in each microcycle generates the output code of the most significant bits of the adder in the binary code of the Rademacher number system.

Matrix multiplier based on Booth's algorithm

The analyses of the system characteristics of known structures of matrix multipliers based on Brown's, Dadda, Booth's and other algorithms were given in [22, 25-28], where it was shown that the speed of these processors with n-bit input MBCs is not less than $2n+(n-1)$ clock cycles.

The disadvantage of these known structures in the multiplication cycle is the simultaneous use of all components of the adder matrix, which leads to significant power consumption and heat release of the crystals. The use of multiplier structures based on Booth's algorithm [25] also does not lead to a significant increase in speed, since in known structures, multi-bit binary combinational adders with ripple carry-overs are used in each pair of multiplied bits.

For the first time, the proposed structure of the synchronized matrix multiplier, which contains synchronized multi-bit adder-accumulators and implements Booth's algorithm, is presented in Fig. 6.
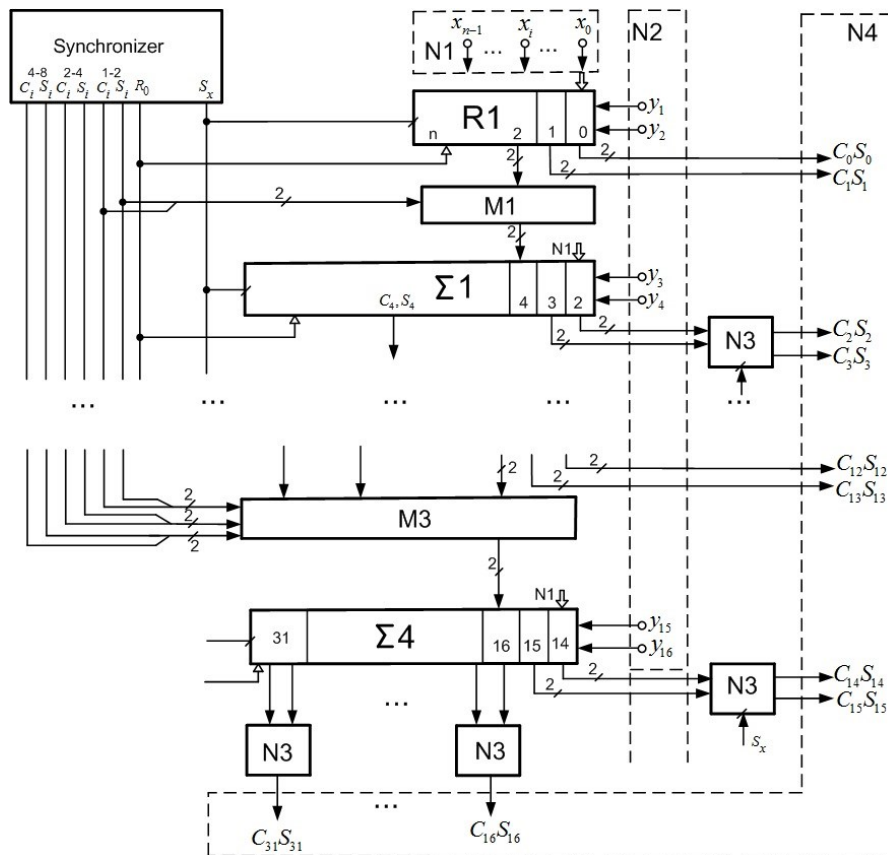
Fig.6. Structural and functional scheme of a synchronized multi-bit matrix multiplier

Such a synchronized multiplier of binary codes consists of the following components: 1 – the first n-bit input data bus of the binary code $(x_{n-1},\dots,x_i,\dots,x_0)$; 2 – the second n-bit input data bus of the binary code $(y_n,\dots,y_{i+1},\dots,y_1)$;

3 – synchronizer; 4 – output 4n-bit data bus of the binary code; 5 – 4n-bit memory register; 6 – n-bit synchronized adder- accumulators; 7 – synchronized multiplexers (M7.1, M7.2, …, M7.log₂n).

The synchronizer has output channels: R_0 – a channel for resetting all device triggers to the 0-th state; S_x – data recording synchronization channel on D-inputs of synchronized adder triggers; C_iS_i – channels for generating permits for performing the addition operation between adders (1-2, 2-4, 4-8).

The device operates according to the following algorithm:

1. The potential '0' is fed to the R-inputs of the D-triggers of all registers and adders to set them to the zero state.

2. With a delay of 3 clock cycles, a synchronizer generates a rising edge on the D-inputs of the trigger registers and synchronized adders, where Booth codes (0,X,2X,3X) are written depending on the logical values (x_i) and (y_iy_j) in each n-th digit of the multiplier.

3. The information received at the outputs of the 2 least significant bits of registers and odd adders in the form of codes $\dot{C}_j, \dot{S}_j$ та $\dot{C}_{j+1}, \dot{S}_{j+1}$ is written into the triggers of the output data bus (4), after which the gates x and y are closed and then they do not participate in the operation of the device.

4. Synchronization signals, fed to each multiplexer lasting 12 clock cycles, add code to the adders - 4 clock cycles $\dot{S}_j$ and 8 clock cycles $\dot{C}_j$.

5. The signals of the synchronizer (4, 8, 12, 16, ...) activate the multiplexers, which initiate the addition of the corresponding DBCs in pairs of adders (1-2,2-4, 4-8).

Thus, the total signal delay in this multiplier structure is calculated according to the following expression due to the bit width n=1024: $T = 3 + 12 \times (\log_2 n - 2) = 99$ (clock cycles).

Compared to the known Brown's multiplier, in which the signal delay is 2n+(2n-1) and when n=1024 it equals 4095 clock cycles, the signal delay in the proposed 1024-bit multiplier based on binary arithmetic is 99 clock cycles, respectively.

That is, the speed of the proposed multiplier is increased by 41 times in comparison with the known one.

The main advantage of the developed structure of the synchronized matrix multiplier, compared to the known ones, is the possibility of significant reduction of power consumption and heat release of crystals by disconnecting the input memory registers and odd adder-accumulators from the power supply that provides a corresponding reduction in the power consumption of the crystal in the multiplication cycle by 42%.

Conclusions

Above mentioned areas of application and the main directions for improvement of high-performance multi-bit matrix multipliers as components of ALU coprocessors in multi-core supercomputers, determine the perspective of their effective applications in solving complex computing problems, which include exponentiation, multiplication, division, square root extraction, etc. in statistical, correlation, spectral, cluster and entropy analysis.

The proposed structure of the synchronized matrix multiplier based on Booth's algorithm increases the speed by 1-2 orders compared to the speed of known matrix multipliers. The obtained results of multiplication in the form of a double binary code allow you to significantly speed up further calculations due to the absence of ripple carry-overs in DBCs.

References

1. A.O. Melnyk. "Cyber-physical systems multilayer platform and research framework. Advances in cyber-physical systems", Lviv Polytechnic National University Publishing, 2016, № 1 (1), p.1-6
2. Edward R. Miller-Jones Modern Supercomputers. The most powerful computer in the world // FastBook Publishing, 2012, – 136 p.
3. MIPS official website. URL: https://www.mips.com (дата звернення 15.06.2023).
4. IBM official website. URL: https://www.ibm.com (дата звернення 15.06.2023).
5. Intel official website. URL: https://www.intel.com (дата звернення 15.06.2023).
6. ARM official website. URL: https://www.arm.com (дата звернення 15.06.2023).
7. HP official website. URL: https://www.hp.com (дата звернення 15.06.2023).
8. Cray official website. URL: https://www.cray.com (дата звернення 15.06.2023).
9. W. Robert and Jr. Heath, "Introduction to Wireless Digital Communication," 1 Ed. Prentice Hall, 2017, p.464.
10. A.O. Melnyk, Computer architecture. Scientific ed., Lutsk: Volyn Regional Printing House, 2008, 470 p.
11. Y. Nyckolaychuk, N. Vozna, A. Davletova, I. Pitukh, O. Zastavnyy, V. Hryha Microelectronics Structures of Arithmetic Logic Unit Components // Advanced Computer Information Technologies. International Conference. ACIT'2021. – Deggendorf, Germany, September 2021. – P. 682-685.
12. Specialized Computer Technologies in Informatics: Monograph edited by Y. M. Nykolaychuk, Ternopil: Beskydy, 2017. 919 p.
13. A. Anand Kumar Fundamentals of Digital Circuits / Prentice-Hall of India Pvt.Ltd, 2007. – 664 p.
14. Patent of Ukraine. No. 115861 Single-bit half-adder Bull. No. 8, 2017
15. Patent of Ukraine. No. 150332 Binary adder-accumulator. Bul. No. 5, 2022
16. Patent of Ukraine. No. 146833 Single-bit synchronized full-adder Bull. No. 12, 2021
17. Patent of Ukraine. No. 150331 Carry-look-ahead adder. Bul. No. 5, 2022
18. Patent of Ukraine. No.147625 Single-bit synchronized half-adder. Bul. No. 21, 2021

19. Nyckolaychuk, V. Hryha, N. Vozna, A. Voronych, A. Segin, P. Humennyi High-performance coprocessors for arithmetic and logic operations of multi-bit cores for vector and scalar supercomputers // Advanced Computer Information Technologies. 12th International Conference. ACIT 2022. – Spišská Kapitula, Slovakia, September 2022. – P. 410-414

20. Patent of Ukraine. No. 150330 Single-bit full-adder. Bul. No. 5, 2022

21. Patent of Ukraine. No. 132520 Matrix multiplier. Bul. No. 4, 2019

22. Patent of Ukraine. No. 150331 Matrix multiplier. Bul. No. 4, 2019

23. Patent of Ukraine. No. 123752 Multipler of multi-bit data streams. Bul. No. 21, 2021

24. Y. Nyckolaychuk, V. Hryha, N.Vozna, I.Pitukh and L. Hryha High-performance multi-bit adder-accumulators as component of the ALU in supercomputers // publ. on CEUR Workshop Proceedings, 2023, P. 649-661.

25. Barun Biswas, Bidyut B. Chaudhuri Generalization of Booth's Algorithm for Efficient Multiplication, Procedia Technology, Volume 10, 2013, P. 304-310.

26. V. Gryga, I. Kogut, V. Holota, R. Kochan, S. Rajba, T. Gancarczyk, U. Iatsykovska Spatial-Temporal Transformation of Matrix and Multilayer Algorithms of Binary Number Multiplications // Proceedings of 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. IDAACS'2019. – Metz, France, September 18-21, 2019. – P. 691-694.

27. J.W. Lee, C.Y. Meher, P. K. Patra. Concurrent Error Detection in Bit-Serial normal Basis Multiplication Over GF(2m). Using Multiple Parity Prediction Schemes in Large Scale Integration (VLSI) Systems, IEEE Transactions on Very Large Scale integration (VLSI) Systems: 2009-08-25.

28. James Reinders and Jim Jeffers, High Performance Parallelism Pearls Volume One: Multicore and Many-core Programming Approaches, 2014, 600p.

Yaroslav Nykolaychuk **Ярослав Николайчук**	DrS on Engineering, Professor of Specialized Computer System Department, West Ukrainian National University, Ternopil, Ukraine e-mail: ya.nykolaichuk@wunu.edu.ua orcid.org/0000-0002-2393-2332, Scopus Author ID: 24179012300, Researcher ID: H-4325-2017	доктор технічних наук, професор кафедри спеціалізованих комп'ютерних систем, Західноукраїнський національний університет, Тернопіль, Україна
Volodymyr Hryha **Володимир Грига**	PhD, Associate Professor of Computer Engineering and Electronics Department, Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, Ukraine e-mail: volodymyr.gryga@pnu.edu.ua orcid.org/0000-0001-5458-525X, Scopus Author ID: 57188576389, Researcher ID: HKE-6775-2023	кандидат технічних наук, доцент кафедри комп'ютерної інженерії та електроніки, Прикарпатський національний університет імені Василя Стефаника, Івано-Франківськ, Україна
Nataliia Vozna **Наталія Возна**	DrS on Engineering, Professor of Specialized Computer System Department, West Ukrainian National University, Ternopil, Ukraine e-mail: n.vozna@wunu.edu.ua orcid.org/0000-0002-8856-1720, Scopus Author ID: 24178221500, Researcher ID: H-4297-2017	доктор технічних наук, професор кафедри спеціалізованих комп'ютерних систем, Західноукраїнський національний університет, Тернопіль, Україна
Ihor Pitukh **Ігор Пітух**	PhD, Associate Professor of Specialized Computer System Department, West Ukrainian National University, Ternopil, Ukraine e-mail: i.pitukh@wunu.edu.ua orcid.org/0000-0002-3329-4901, Scopus Author ID: 37122611700, Researcher ID: H-5367-2017	кандидат технічних наук, доцент кафедри спеціалізованих комп'ютерних систем, Західноукраїнський національний університет, Тернопіль, Україна
Lyudmila Hryha **Людмила Грига**	Teacher, Teacher of Programming and Informatics Department, Nadvirna Vocational College by NTU, Nadvirna, Ukraine e-mail: hrihaludmila31@gmail.com orcid.org/0000-0002-6260-7559, Scopus Author ID: 57188576389, Researcher ID: ITV-4046-2023	викладач, викладач циклової комісії програмування та інформатики, ВСП "Надвірнянський фаховий коледж", Надвірна, Україна