УДК 004.032.2
DOI: 10.20535/1810-0546.2016.6.79723

О.З. Шологон, Ю.З. Шологон
Національний університет "Львівська політехніка", Львів, Україна

# МЕТОД ОЦІНЮВАННЯ СТРУКТУРНОЇ СКЛАДНОСТІ ПОМНОЖУВАЧА МАСТРОВІТО У $GF(p^m)$ З УРАХУВАННЯМ ВНУТРІШНІХ ЕЛЕМЕНТІВ

**Background.** In the multipliers which use Galois filed $GF(p^m)$ with large order the hardware complexity allows implementation on FPGA chip, but high structural complexity prevents to do it. That's why it is important to conduct research in Galois field $GF(p^m)$ to determine the field in which the structural complexity is the lowest.

**Objective.** Develop the method for evaluating structural complexity of Mastorovito multiplier in response to the internal elements.

**Methods.** Structural complexity of Mastorvito multiplier in Galois fields was determined by combining VHDL and SH models in a VHDL-SH model. In order to find the field with the least structural complexity, the extended Galois field $GF(p^m)$ with the same number of elements was analysed.

**Results.** The relationship between structural complexity of Mastrovito multiplier in Galois fields $GF(p^m)$ and number of field bit in the capacity of the field was identified. The results for structural complexity of Mastrovito multiplier in Galois field $GF(p^m)$ using internal elements were modified.

**Conclusions.** Method for calculating the structural complexity of Mastrovito multiplier in $GF(p^m)$ was developed. The structural complexity was calculated by combining VHDL and SH models in a VHDL-SH model. It was determined that structural complexity of the multiplier depends on capacity of the field $GF(p^m)$, wherein the calculations are carried out. The structural complexity of Mastrovito multiplier in $GF(p^m)$ with approximately the same number of elements was calculated, where $p^m \approx 625$, $p^m \approx 78502725751$, $p^m \approx 1,93485E+15$. In calculating the structural complexity without internal elements the structural complexity of the multiplier is less, when the difference between the capacity of the field and number of field bit in the field order is growing. In calculating the structural complexity with internal elements, structural complexity of multiplier is less when the difference between number of field bit and field capacity is equal. This method application can help to develop Galois field multipliers $GF(p^m)$ with big order.

**Keywords:** Galois field $GF(p^m)$; VHDL-SH model; Mastrovito multiplier; structural complexity.

## Вступ

В Україні практично всі реалізації засобів криптографічного захисту інформації є програмними, основними недоліками яких є недостатня стійкість до зламу, часто недостатня продуктивність, особливо при обробці інтенсивних потоків даних. Тому для підвищення надійності та продуктивності реалізації засобів криптографічного захисту інформації виникає необхідність у створенні їх апаратних реалізацій, особливо засобів для виконання операцій над елементами скінченних полів. Однією з можливих реалізацій є реалізація на програмованій логічній інтегральній схемі (ПЛІС).

Оцінка структурної складності помножувача дасть змогу визначити можливості використання ПЛІС для подальшої реалізації [1]. У роботі [2] проведено оцінку структурної складності помножувача Масторвіто в полях Галуа через об'єднання VHDL- та SH-моделей в одну VHDL-SH-модель. Визначення SH описане в праці [3]. У [4] запропонований метод визначення структурної складності помножувачів у поліноміальному базисі полів Галуа $GF(2^m)$ на основі їх представлення за допомогою елементарних перетворювачів. У роботах [5, 6] розглядалися поля Галуа з найменшою структурною складністю, а саме коли $GF(p^m) = p$. У [7] складність паралельного помножувача в полях $GF(2^m)$ обчислювалась з урахуванням внутрішніх елементів. У роботі [8] апаратна складність помножувачів зменшується за рахунок визначення елементів, які призводять до помилки; у [9] – зменшенням розрядності поля. У [10] розглядалася зміна складності при використанні подвійних умов.

У зазначених вище працях не розглядались помножувачі, в яких би використовувались поля Галуа $GF(p^m)$ з великим порядком. У таких помножувачах апаратні можливості дають змогу проводити реалізації на кристалі ПЛІС, однак через велику структурну складність цього зробити не вдається. Тому важливо провести дослідження в полях Галуа $GF(p^m)$ для визначення поля, у якому структурна складність буде найменшою. Таке дослідження і описано в нашій роботі.

**Постановка задачі**

У проаналізованих роботах не визначалося, для якого з полів Галуа з приблизно однаковою кількістю елементів помножувач має найменшу структурну складність. Це є актуальною задачею при спробі реалізації помножувача в ПЛІС з лімітованою кількістю доріжок на кристалі та з обмеженнями на спосіб їх використання. Тому основним завданням є розробити метод оцінювання структурної складності помножувача Масторовіто у $GF(p^m)$ з урахуванням внутрішніх елементів.

**Обчислення структурної складності**

Структурна складність відображає ступінь нерегулярності міжзв'язків схеми деякого рівня ієрархії побудови апаратних засобів. Структурна складність помножувача в полях Галуа визначається за допомогою об'єднання VHDL- та SH-моделей в одну VHDL-SH-модель. SH-модель алгоритму (Software/Hardware – апаратно-програмна модель) враховує програмні та апаратні засоби. Наявність апаратних засобів у складі SH-моделі алгоритму за змістом наближає її до комп'ютерної системи [3].

Множина зв'язків у SH-моделі задає структурну складність. У VHDL зв'язки є елементами схеми, з'єднаннями, які не мають інтелектуального значення. VHDL не фіксує програмну та структурну складність, і для цього не має підстав, оскільки ієрархічний об'єкт – модуль – може мати будь-яку внутрішню складність. При об'єднанні SH- та VHDL-моделей в одну – VHDL-SH-модель – спочатку будується VHDL-модель, за необхідності послідовно вносяться зміни до SH-моделі (оптимізація) та VHDL-моделі. Проектування проводиться ітераціями з урахуванням оптимізації (мінімізації) характеристик складності.

У разі об'єднання моделей елементи VHDL-SH-моделі набувають усіх властивостей SH-моделі – вони є дискретними, детермінованими, мають елементарність і масовість. Характеристики складності розглядаються у їх ієрархічній побудові. Кожну з характеристик можна обчислювати для елементів різних рівнів ієрархій. Сумарна величина обчислених характеристик є складністю пристрою:

$$S = -E \cdot \log_2 \frac{E}{X \cdot U},$$

де $S$ – структурна складність; $X$ – кількість внутрішніх елементів; $U$ – множина орієнтованих міжз'єднань, у розглядуваному випадку кількість виходів: $U = X$; $E$ – кількість з'єднань кожного фрагмента схеми.

**Представлення елементів у $GF(p^m)$**

Представлення розрядів $GF(p^m)$ залежить від порядку поля $p$, а також від кількості бітів $r$, необхідних для кодування елементів поля $GF(p)$. У табл. 1 відображено базиси полів Галуа $GF(p)$ та кількість елементів у них.

Отже, для того щоб представити один розряд для поля $GF(5^m)$, потрібно 3 біти. Відповідно, у табл. 2 наведено таблицю істинності операції додавання за модулем 5 у полях у $GF(5)$.

***Таблиця* 1.** Базиси поля Галуа $GF(p)$ та кількість елементів у них

| GF($p$) | Кількість розрядів $r$ | Елементи базису поля |
|---|---|---|
| GF(2) | 1 | $a \in$ 0, 1 |
| GF(3) | 2 | $a \in$ 0, 1, 2 |
| GF(5) | 3 | $a \in$ 0, 1, 2, 3, 4 |
| GF(7) | 3 | $a \in$ 0, 1, 2, 3, 4, 5, 6 |
| GF($p$) | $r$ | $a \in$ 0, 1..., $p$ – 1 |

***Таблиця* 2.** Таблиця істинності за модулем 5 для елементів у $GF(5)$

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

### Обчислення структурної складності помножувача Мастровіто для $GF(p^m)$

Помножувач Мастровіто здійснює операції $c = ab \bmod q$ у полях $GF(p^m)$. Множення здійснюється утворенням матриці скорочень, що обчислюється як добуток нескорочуваного полінома $q$ і вхідного $a$. Далі матриця множиться на вхідне значення $b$. Для виконання цих операцій та збереження часткових результатів у полях $GF(2)$ над одним елементом поля достатньо одного біта, тоді як для полів $GF(p)$ потрібно $r$ бітів, де $r$ – кількість бітів, необхідних для кодування значення $p$. На рис. 1 зображено схему помножувача Мастровіто для $GF(p^m)$, де $m = 2$.

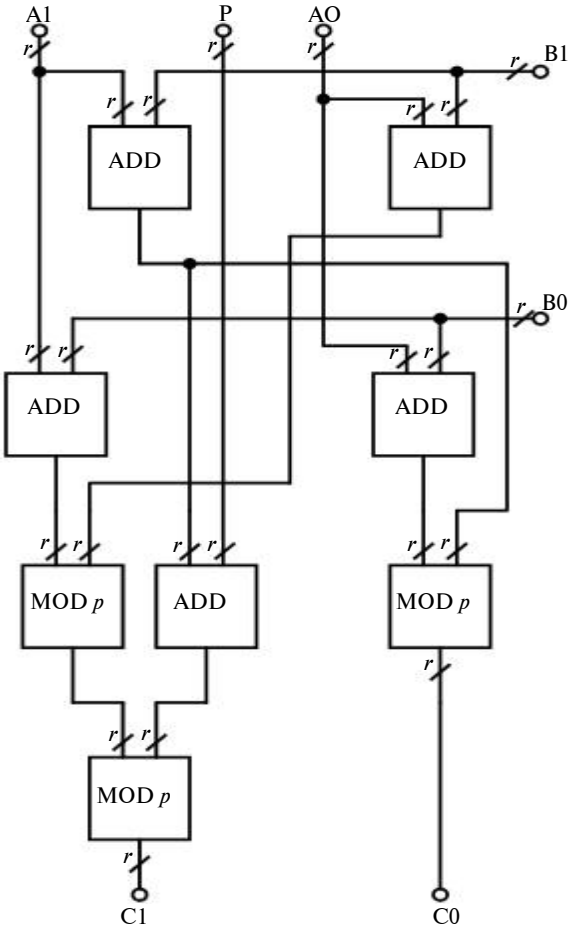


Рис. 1. Помножувач Масторовіто для $GF(p^m)$, де $m = 2$

За схемою помножувача на рис. 1 можна вивести формулу обчислення структурної складності помножувача Мастровіто для полів $GF(p^m)$.

Структурна складність помножувача визначається на основі кількості з'єднань між елеметами схеми.

Кількість елементів схеми (тобто блоків) $X$ для $GF(p^m)$ буде залежати від кількості розрядів поля і матиме такий вигляд:

$$X = (M \cdot r)\,\mathrm{ADD} + ((M-1)\cdot r)\,\mathrm{ADD} + ((M-1)\cdot r)\times$$
$$\times\,\mathrm{XOR} + ((2\cdot \mathrm{r})\,\mathrm{ADD} + (2\cdot \mathrm{r})\,\mathrm{MOD})\cdot (M-1)^2,$$

де $m$ – розрядність поля Галуа, ADD і MOD – умовні позначення логічних блоків, $r$ – кількість бітів, необхідних для кодування значення $p$.

Оскільки ADD і MOD є умовними позначеннями, то для подальшого зведення формули їх можна опустити:

$$X = (M \cdot r) + (M-1)\cdot r + (M-1)\cdot r +$$
$$+ ((2\cdot \mathrm{r}) + (2\cdot \mathrm{r}))\cdot (M-1)^2 =$$
$$= 3\cdot M \cdot R - 2\cdot R + 4\cdot R\cdot (M-1)^2.$$

Формули для обчислення множини орієнтованих з'єднань $U$ та множини елементарних перетворювачів $E$ залишаються тими ж самими:

$$U = X,$$
$$E = 3\cdot X.$$

Відповідно, структурна складність помножувача буде визначатись таким чином:

$$S = -E\cdot \log_2 \frac{E}{X\cdot U} = -E\cdot \log_2 \frac{3}{X}. \qquad (1)$$

### Результати досліджень

У табл. 3 наведено результати обчислення структурної складності помножувачів для полів $GF(p^m)$ з приблизно однаковою кількістю елементів поля.

***Таблиця* 3.** Структурна складність помножувачів для полів $GF(p^m)$, де $p = 2, 3, 5, 7, 13, 131$

| $p$ | $m$ | $p^m$ | $r$ | $S$ |
|---|---|---|---|---|
| 2 | 7 | 128 | 1 | 2843 |
| 3 | 5 | 243 | 2 | 1363 |
| 5 | 4 | 625 | 3 | 2286 |
| 7 | 3 | 343 | 3 | 936 |
| 13 | 2 | 169 | 4 | 327 |
| 131 | 1 | 131 | 8 | 33 |

З результатів табл. 3 видно, що для полів з приблизно однаковою кількістю елементів струк-

турна складність помножувача загалом зменшується, коли збільшується різниця $r - m$. Також видно, що для помножувача Мастровіто структурна складність є найменшою, коли обчислення здійснюються в $GF(131)$.

Однак при обчисленні структурної складності в табл. 3 не враховувалась складність внутрішніх елементів помножувача. Згідно з рис. 1, помножувач Мастровіто використовує 2 функціональних елементи: ADD і MOD.

У блоці ADD відбувається додавання двох вхідних значень. На рис. 2 наведено структурну схему блоку ADD $p$ для $GF(p^m)$ для $p = 2$.

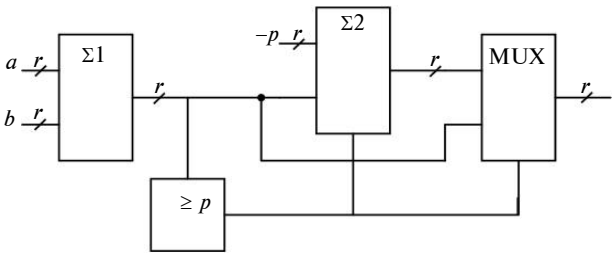


Рис. 2. Схема блоку ADD $p$ для $GF(p^m)$

Структурна схема блоку ADD складається з двох суматорів: основного (Σ1) та коректувального (Σ2), компаратора та мультиплексора. Принцип роботи блоку ADD є таким: на вхід першого суматора подаються два $r$-розрядних доданки, далі сума перевіряється компаратором. Якщо сума є більшою за $p$, результат подається на другий суматор.

Блоки (Σ1) і (Σ2) є паралельними багаторозрядними суматорами, які складаються з послідовності однорозрядних суматорів. У такому випадку кількість елементів суматора буде рівна кількості розрядів доданків: $X_{\Sigma 1} = r$ і $X_{\Sigma 2} = r$.

Кількість елементів компаратора залежить від кількості розрядів $p$. Порівняння суми і значення $p$ починається від старших розрядів. Якщо значення $A > B$, то на виході отримаємо 1. На рис. 3 наведено структурну схему компаратора для $r = 2$, який складається з двох елементів AND, одного XOR та двох NOT – разом 5 логічних елементів.

На основі рис. 3 можна вивести формулу кількості елементів компаратора:

$$X_k = r \cdot 2 + 1.$$

Отже, сумарну кількість елементів блоку ADD можна обчислити таким чином:

$$X_{\text{ADD}} = X_{\Sigma 1} + X_{\Sigma 2} + X_k + X_{\text{MUX}},$$

де $X_{\text{MUX}}$ – кількість елементів компаратора (формула обчислення буде наведена нижче).

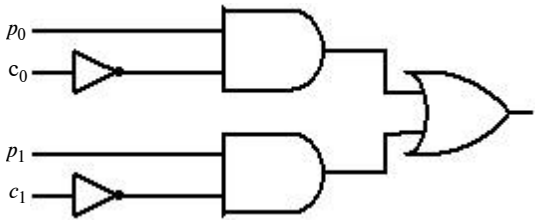


Рис. 3. Структурна схема компаратора $r = 2$

Для реалізації блоку MOD $p$ у полях $GF(p^m)$, при $r = 4$, можна використати мультиплексор з 4-ма входами і одним виходом.

Для визначення структурної складності блоку MOD $p$ необхідно знати кількість AND-, XOR- і NOT-елементів, необхідних для реалізації мультиплексора. На рис. 4 зображено структурну схему мультиплексора 4:1. З рис. 4 видно, що для реалізації мультиплексора необхідні елементи 4 AND, 3 OR і 2 NOT – разом 9 логічних елементів.

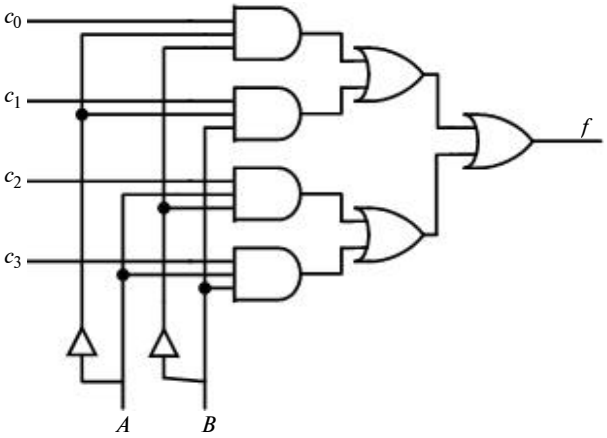


Рис. 4. Структурна схема мультиплексора 4:1

Для здійснення операції MOD у $GF(2^m)$ потрібен 1 мультиплексор із кількістю входів 4 і кількістю виходів 1. Відповідно, для $GF(3^m)$ необхідні 3 мультиплексори.

Отже, кількість елементів мультиплексора буде дорівнювати

$$X_{\text{MUX}} = 9 \cdot N_{\text{MUX}},$$

де $N_{\text{MUX}}$ – кількість мультиплексорів.

***Таблиця* 4.** Структурна складність помножувачів з урахуванням внутрішніх елементів для полів $GF(p^m)$, де $p$ = 2, 3, 5, 7, 13, 131

| $p$ | $m$ | $r$ | $N_{\text{MUX}}$ | $S$ |
|---|---|---|---|---|
| 2 | 7 | 1 | 1 | 16770 |
| 3 | 5 | 2 | 3 | 52533 |
| 5 | 4 | 3 | 8 | 133077 |
| 7 | 3 | 3 | 16 | 122620 |
| 13 | 2 | 4 | 53 | 166235 |
| 131 | 1 | 8 | 5713 | 847 |

***Таблиця* 5**. Структурна складність помножувачів з урахуванням внутрішніх елементів для полів $GF(p^m)$, де $p$ = 2, 23, 61, 149, 151, 523

| $p$ | $m$ | $p^m$ | $r$ | $N_{\text{MUX}}$ | $S$ |
|---|---|---|---|---|---|
| 2 | 36 | 68719476736 | 1 | 11170472 | 2,40549E + 13 |
| 23 | 8 | 78310985281 | 5 | 12729588 | 5,46184E + 12 |
| 61 | 6 | 51520374361 | 6 | 8374727 | 2,07416E + 12 |
| 149 | 5 | 73439775749 | 8 | 11937764 | 2,73071E + 12 |
| 151 | 5 | 78502725751 | 8 | 12760756 | 2,92745E + 12 |
| 523 | 4 | 74818113841 | 10 | 12161816 | 2,10223E + 12 |

***Таблиця* 6.** Структурна складність помножувачів з урахуванням внутрішніх елементів для полів $GF(p^m)$, де $p$ = 2, 43, 71, 127, 139, 352

| $p$ | $m$ | $p^m$ | $r$ | $N_{\text{MUX}}$ | $S$ |
|---|---|---|---|---|---|
| 2 | 49 | 5,6295E + 14 | 1 | 91508506624 | 5,76202E + 20 |
| 43 | 9 | 5,02593E + 14 | 6 | 81697314440 | 3,88862E + 20 |
| 71 | 8 | 6,45754E + 14 | 7 | 1,04968E + 11 | 4,5163E + 20 |
| 127 | 7 | 5,32876E + 14 | 7 | 86619909787 | 2,73569E + 20 |
| 139 | 7 | 1,00254E + 15 | 8 | 1,62965E + 11 | 5,99257E + 20 |
| 353 | 6 | 1,93485E + 15 | 9 | 3,14514E + 11 | 9,26844E + 20 |

Маючи всі дані для обчислення кількості елементів помножувача, можна вивести загальну формулу:

$$X = (M \cdot r) \cdot X_{\text{ADD}} + ((M-1) \cdot r) \cdot X_{\text{ADD}} + \\ + ((M-1) \cdot r) \cdot X_{\text{MUX}} + ((2 \cdot r) X_{\text{ADD}} + \\ + (2 \cdot r) \cdot X_{\text{MUX}}) \cdot (M-1)^2.$$

Маючи значення $X_{\text{ADD}}$ та $X_{\text{MUX}}$, кількість елементів $X$ можна визначити як

$$X = M \cdot r(r + 1 + 8N_{\text{MUX}}) - r(1 + 8N_{\text{MUX}}) + \\ + (2r^2 + 16rN_{\text{MUX}})(M-1)^2.$$

Підставивши нове значення $X$ у формулу (1), отримаємо наступні значення структурної складності. У табл. 4–6 наведено обчислення структурної складності для полів з приблизно однаковою кількістю елементів.

Як видно з обчислень, структурна складність залежить від порядку поля Галуа. При використанні полів з приблизно однаковою кількістю елементів структурна складність зменшується, коли розрядність поля дорівнює кількості бітів у порядку поля. Тобто для полів $GF(p^m)$ з табл. 4 найменшою буде структурна складність за розрядності поля 3, тобто коли $p = 5$, $m = 4$. Для полів $GF(p^m)$ із табл. 5 – за розрядності поля 6, тобто коли $p = 61$, $m = 6$, та для полів $GF(p^m)$, із табл. 6 – за розрядності поля 7, тобто коли $p = 139$, $m = 7$.

**Висновки**

У роботі запропоновано метод обчислення структурної складності для помножувача Мастровіто у полях $GF(p^m)$. Структурна складність обчислювалась об'єднанням VHDL- та SH-моделей в одну VHDL-SH-модель. Під час дослідження було встановленно, що структурна складність помножувача залежить від розрядності поля $GF(p^m)$, у якому здійснюються обчислення.

У роботі обчислено структурну складність помножувача Мастровіто у полях $GF(p^m)$ з приблизно однаковою кількістю елементів. При обчисленні структурної складності без урахування внутрішніх елементів структурна складність помножувача зменшується, коли збільшується різниця між розрядністю поля та кількістю бітів у порядку поля. При врахуванні внутрішніх елементів структурна складність зменшується, коли розрядність поля дорівнює кількості бітів у порядку поля.

Використання цього методу дає можливість розроблювати помножувачі в полях Галуа $GF(p^m)$ з великим порядком. Це буде предметом подальших досліджень.

### Список літератури

1. *Глухов В.С., Глухова О.В.* Результати оцінки структурної складності помножувачів елементів полів Галуа // Вісник НУ “Львівська політехніка” “Комп’ютерні системи та мережі”. – 2013. – № 773. – С. 27–32.
2. *Шологон Ю.З.* Оцінювання структурної складності помножувачів полів Галуа на основі елементарних перетворювачів // Вісник НУ “Львівська політехніка” “Комп’ютерні системи та мережі”. – 2014. – № 806. – С. 290–296.
3. *Черкаський М. В., Мурад Хусейн Халіл.* Універсальна SH-модель // Вісник НУ “Львівська політехніка” “Комп’ютерні системи та мережі”. – 2004. – № 523. – С. 150–154.
4. *Шологон О.З.* Обчислення структурної складності помножувачів у поліноміальному базисі елементів полів Галуа GF(2^m) // Вісник НУ “Львівська політехніка” “Комп’ютерні системи та мережі”. – 2014. – № 806. – С. 284–289.
5. *Bahram Rashidi, Sayed Masoud Sayedi, Reza Rezaeian Farashahi.* Efficient implementation of bit-parallel fault tolerant polynomial basis multiplication and squaring over GF(2m) // IET Computers & Digital Techniques. – 2016. – **10**, № 1. – P. 18–29.
6. *Low* complexity polynomial expansion detector with deterministic equivalents of the moments of channel gram matrix for massive MIMO uplink / Anan Lu, Xiqi Gao, Yahong Rosa Zheng, Chengshan Xiao // IEEE Trans. Commun. – 2016. – **64**, № 2. – P. 586–600.
7. *Yin Li, Gong-liang Chen, Xiaoning Xie.* Low complexity bit-parallel GF(2m) multiplier for all-one polynomials // J. Cryptography. – 2012. – P. 410–415.
8. *Shelly S., Chacko B.T.* Fault detection multipliers in polynomial and normal basis // Int. J. Comp. Applications. – 2010. – **1**, № 5. – P. 102–106.
9. *Kitsos P., Theodoridis G., Koufopavlou O.G.* An efficient reconfigurable multiplier architecture for Galois field GF(2m) // Microelectronics J. – 2003. – **34**, № 10. – P. 975–980.
10. *Al-Rabadi A., Perkowski M.A.* Multiple-valued galois field S/D trees for GFSOP minimization and their complexity // Proc. 31st IEEE Int. Symp. Multiple-Valued Logic, May 22–24, 2001. – P. 159–166.

### References

1. V. Glukhov and A. Glukhov, “The results of evaluation of structural complexity multipliers elements of Galois fields”, *Visnyk NU “L'vivs'ka Politekhnika” “Komp"yuterni Systemy ta Merezhi”*, no. 773, pp. 27–32, 2013 (in Ukrainian).
2. Y. Sholohon, “Evaluation of structural complexity Galois field multipliers based on the elementary transducers”, *Visnyk NU “L'vivs'ka Politekhnika” “Komp"yuterni Systemy ta Merezhi”*, no. 806, pp. 150–154, 2014 (in Ukrainian).
3. M. Cherkaskyy and Mourad Houssein Khalil, “Universal SH-model”, *Visnyk NU “L'vivs'ka Politekhnika” “Komp"yuterni Systemy ta Merezhi”*, no. 523, pp. 150–154, 2004 (in Ukrainian).
4. O. Sholohon, “Structural complexity of Galois field GF(2m) elements multipliers in polynomial basis calculation”, *Visnyk NU “L'vivs'ka Politekhnika” “Komp"yuterni Systemy ta Merezhi”*, no. 806, pp. 284–289, 2014 (in Ukrainian).
5. Bahram Rashidi *et al.*, “Efficient implementation of bit-parallel fault tolerant polynomial basis multiplication and squaring over GF(2 m )”, *IET Computers & Digital Techniques*, vol. 10, no. 1, pp. 18–29, 2016. doi:10.1049/iet-cdt.2015.0020
6. Anan Lu *et al.*, “Low complexity polynomial expansion detector with deterministic equivalents of the moments of channel gram matrix for massive MIMO uplink”, *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 586–600, 2016. doi: 10.1109/TCOMM.2015.2506700
7. Yin Li *et al.*, “Low complexity bit-parallel GF(2m) multiplier for all-one polynomials”, *J. Cryptography*, pp. 410–415, 2012.
8. S. Shelly and B.T. Chacko, “Fault detection multipliers in polynomial and normal basis”, *Int. J. Com. Applications*, vol. 1, no. 5, pp. 102–106, 2010. doi: 10.5120/114-229
9. P. Kitsos *et al.*, “An efficient reconfigurable multiplier architecture for Galois field GF(2m)”, *Microelectronics J.*, vol. 34, no. 10, pp. 975–980, 2003. doi: 10.1016/S0026-2692(03)00172-1
10. A. Al-Rabadi and M.A. Perkowski, “Multiple-valued galois field S/D trees for GFSOP minimization and their complexity”, in *Proc. 31st IEEE Int. Symposium on Multiple-Valued Logic*, 2010, pp. 159–166. doi: 10.1109/ISMVL.2001.924567


О.З. Шологон, Ю.З. Шологон

## МЕТОД ОЦІНЮВАННЯ СТРУКТУРНОЇ СКЛАДНОСТІ ПОМНОЖУВАЧА МАСТРОВІТО У $GF(p^m)$ З УРАХУВАННЯМ ВНУТРІШНІХ ЕЛЕМЕНТІВ

**Проблематика.** В помножувачах, у яких використовуються поля Галуа $GF(p^m)$ з великим порядком, апаратна складність дає змогу проводити реалізації на кристалі програмованої логічної інтегральної схеми, однак велика структурна складність перешкоджає це зробити. Тому важливо провести дослідження в полях Галуа $GF(p^m)$ для визначення поля, у якому структурна складність буде найменшою.

**Мета досліження.** Розробити метод оцінювання структурної складності помножувача Масторовіто у $GF(p^m)$ з урахуванням внутрішніх елементів.

**Методика реалізації.** Структурна складність помножувача Масторвіто в полях Галуа визначається за допомогою об'єднання VHDL- та SH-моделей в одну VHDL-SH-модель. Для визначення поля з найменшою структурною складністю аналізуються розширені поля Галуа $GF(p^m)$ з приблизно однаковою кількістю елементів.

**Результати дослідження.** Визначено залежність структурної складності від розрядності поля. Наведено обчислення структурної складності для полів Галуа $GF(p^m)$ з урахуванням внутрішніх елементів.

**Висновки.** Запропоновано метод обчислення структурної складності для помножувача Мастровіто в полях $GF(p^m)$. Структурна складність обчислювалась об'єднанням VHDL- і SH-моделей в одну VHDL-SH-модель. Встановлено, що структурна складність помножувача залежить від розрядності поля $GF(p^m)$, у якому здійснюються обчислення. Обчислено структурну складність помножувача Мастровіто в полях $GF(p^m)$ з приблизно однаковою кількістю елементів: $p^m \approx 625$, $p^m \approx 78502725751$, $p^m \approx 1,93485E+15$. При обчисленні структурної складності без урахування внутрішніх елементів структурна складність помножувача зменшується, коли збільшується різниця між розрядністю поля та кількістю бітів у порядку поля. При врахуванні внутрішніх елементів структурна складність зменшується, коли розрядність поля дорівнює кількості бітів у порядку поля. Використання цього методу дає можливість розроблювати помножувачі у полях Галуа $GF(p^m)$ з великим порядком.

**Ключові слова:** поля Галуа $GF(p^m)$; VHDL-SH-модель; помножувач Масторвіто; структурна складність.

О.З. Шологон, Ю.З. Шологон

МЕТОД ОЦЕНКИ СТРУКТУРНОЙ СЛОЖНОСТИ УМНОЖИТЕЛЯ МАСТРОВИТО В $GF(p^m)$ С УЧЕТОМ ВНУТРЕННИХ ЭЛЕМЕНТОВ

**Проблематика.** В умножителях, в которых используются поля Галуа $GF(p^m)$ с большим порядком, аппаратная сложность позволяет проводить реализации на кристалле программируемой логической интегральной схемы, однако большая структурная сложность препятствует это сделать. Поэтому важно провести исследования в полях Галуа $GF(p^m)$ для определения поля, в котором структурная сложность будет наименьшей.

**Цель исследования.** Разработать метод оценки структурной сложности умножителя Масторовито в $GF(p^m)$ с учетом внутренних элементов.

**Методика реализации.** Структурная сложность умножителя Масторвито в полях Галуа определяется с помощью объединения VHDL- и SH-моделей в одну VHDL-SH-модель. Для определения поля с наименьшей структурной сложностью анализируются расширенные поля Галуа $GF(p^m)$ с примерно одинаковым количеством элементов.

**Результаты исследования.** Определена зависимость структурной сложности умножителя Масторвито в полях $GF(p^m)$ от количества битов в разрядности поля. Приведены расчеты структурной сложности умножителя Масторвито для полей Галуа $GF(p^m)$ с учетом внутренних элементов.

**Выводы.** Предложен метод расчета структурной сложности для умножителя Мастровито в полях $GF(p^m)$. Структурная сложность рассчитывалась путем объединения VHDL- и SH-моделей в одну VHDL-SH-модель. Установлено, что структурная сложность умножителя зависит от разрядности поля $GF(p^m)$, в котором осуществляются вычисления. Рассчитана структурная сложность умножителя Мастровито в полях $GF(p^m)$ с примерно одинаковым количеством элементов, где $p^m \approx 625$, $p^m \approx 78502725751$, $p^m \approx 1,93485E+15$. При расчете структурной сложности без учета внутренних элементов структурная сложность умножителя меньше, когда увеличивается разница между разрядностью поля и количеством битов в порядке поля. При расчете структурной сложности с учетом внутренних элементов структурная сложность меньше, когда разрядность поля равна количеству бит в порядке поля. Использование данного метода позволяет разрабатывать умножители в полях Галуа $GF(p^m)$ с большим порядком.

**Ключевые слова:** поля Галуа $GF(p^m)$; VHDL-SH-модель; умножитель Масторвито; структурная сложность.

Рекомендована Радою
факультету прикладної математики
НТУУ "КПІ ім. І. Сікорського"

Надійшла до редакції
12 жовтня 2016 року