УДК 004.272.26

DOI: 10.21779/2542-0321-2023-38-2-81–89

С.В. Шалагин, Д.Ю. Малькин

Аппаратный модуль для вычисления коэффициентов нелинейной полиномиальной функции над полем Галуа

Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ; Россия, 420111, г. Казань, ул. Карла Маркса, 10; sshalagin@mail.ru, developkin@mail.ru

Аннотация. Предложена конвейерная схема вычисления коэффициентов нелинейной полиномиальной функции над полем Галуа при использовании однотипных блоков на основе задания её значений. Представлена методика подбора коэффициентов данной функции, обеспечивающая снижение сложности ее вычисления за счёт обнуления ее коэффициентов. Коэффициенты ранжированы в зависимости от их вклада в снижение сложности вычисления данной функции за счёт обнуления собственных значений. Получены оценки сложности модуля, реализующего методику, на ПЛИС класса FPGA. Данные оценки позволяют выполнить предварительный анализ затрат аппаратных ресурсов ПЛИС класса FPGA, как существующих, так и перспективных.

Ключевые слова: коэффициенты, нелинейная полиномиальная функция, оценки сложности.

Введение

В настоящее время чрезвычайно актуальна задача вычисления различных отображений в режиме реального времени. Практическое применение данной задачи – бортовые и/или встроенные системы, реализующие различные устройства с высокой степенью надежности в разные периоды времени [1–2]. Высокоскоростная обработка массивов данных обеспечивается аппаратно, при использовании параллельных и/или конвейерных методов обработки [3]. Такие методы требуют применения многопроцессорных вычислительных систем со специализированной архитектурой (МВА СА), отличной от фон-Неймановской [4–6]. В качестве элементов указанных систем выступают ПЛИС класса FPGA [7–8].

В [3; 9–12] показано, что для реализации на МВС СА широкого класса устройств для генерирования и обработки цифровых сигналов применимы программные IP-ядра, реализующие нелинейную полиномиальную функцию (НПФ) над полем Галуа [13]. В [14–15] решена задача минимизации количества коэффициентов нелинейной полиномиальной функции над полем $GF(2^n)$ от одной и двух переменных, но указанная задача не решена для НПФ от большего количества переменных.

В работе предложена структурная схема аппаратного модуля, позволяющего вычислять коэффициенты нелинейной полиномиальной функции над полем Галуа вида $GF(2^2)$. Модуль является масштабируемым в зависимости от количества переменных НПФ. Предложен способ ранжирования для элементарных полиномов [16] в зависимости от степени, в которую возводятся переменные, аргументы НПФ. Данный способ позволяет определить методику подбора неопределённых значений НПФ таким образом, чтобы минимизировать аппаратную сложность вычисления данной НПФ.

Основные понятия и определения

НПФ от m переменных над $GF(2^2)$ (далее – НПФ (m)) определена в виде [12; 17]:

$$g\left(x_1 \quad ... \quad x_m\right) = \sum_{i_1=0}^{3} ... \sum_{i_m=0}^{3} a\left([i_1]...[i_m]\right) x^{i_1} ... x^{i_m}. \qquad (1)$$

Выражение $a\left([i_1]...[i_m]\right) x^{i_1} ... x^{i_m}$ в (1) определим как элементарный полином (ЭлП). Имеют место

Утверждение 1. НПФ (m) вида (1) содержит $C_m^z \cdot 2^{m-z}$ ЭлП, содержащих z множителей-констант $x^{i_j} = 1$, где $i_j = 0$, и $\left(m - z\right)$ множителей, для которых $i_j = \overline{1,2}$, $j \in \left\{1 \quad ... \quad m\right\}$, $z = \overline{0,m}$.

Утверждение 2. НПФ (m) вида (1) содержит $C_m^e \cdot 2^{m-e}$ ЭлП, содержащих e множителей $x^{i_j} \in \left\{0 \quad 1\right\}$ в зависимости от значений входных переменных, где $i_j = 3$, и $\left(m - e\right)$ множителей, для которых $i_j = \overline{1,2}$, $j \in \left\{1 \quad ... \quad m\right\}$, $e = \overline{0,m}$.

Утверждение 3. Количество ЭлП, включенных в НПФ (m) вида (1) и содержащих m множителей $x^{i_j} \in \left\{\xi \quad \xi^2\right\}$, где $i_j = \overline{1,2}$, $j \in \left\{1 \quad ... \quad m\right\}$, равно 2^m.

На основе утверждений 1, 2 и 3 сформулировано

Утверждение 4. Количество ЭлП, включенных в НПФ (m) вида (1) и содержащих z множителей-констант $x^{i_j} = 1$, где $i_j = 0$, e множителей $x^{i_j} \in \left\{0 \quad 1\right\}$ в зависимости от значений входных переменных, где $i_j = 3$ и $\left(m - z - e\right)$ множителей, для которых $i_j = \overline{1,2}$, $j \in \left\{1 \quad ... \quad m\right\}$, $0 \le \left(z + e\right) \le m$, равно $Q(w,e,z) = C_m^z \cdot C_{m-z}^e \cdot 2^{m-z-e}$.

Согласно [9; 11], чем меньше множителей, отличных от единицы, присутствует в ЭлП, тем меньше ресурсов требуется для его вычисления. Определим ранги ЭлП в зависимости от степеней $\left(i_1 ... i_m\right)$, в которые возводятся соответствующие переменные – аргументы НПФ (m). Больше всего аппаратных ресурсов для вычисления требуют ЭлП, для которых $i_j = \overline{1,2}$; затем – такие ЭлП, для которых $i_j = 3$, и не требуют ресурсов ЭлП, для которых $i_j = 0$, $j \in \left\{1 \quad ... \quad m\right\}$. Ранг ЭлП определяется тремя величинами, определёнными согласно утверждению 4: $\left(w \;\; e \;\; z\right)$, где $w = m - z - e$. Справедливо

Утверждение 5. Ранг ЭлП при заданных значениях $\left(w \;\; e \;\; z\right)$ определяется согласно значению величины w (чем больше значение – тем выше ранг), а при равных значениях w – по значению величины e.

Схема вычисления НПФ (m) на основе однотипных блоков

Предложенная схема (далее – Схема) служит для вычисления коэффициентов НПФ вида (1) при заданных её значениях. Схема структурно включает в свой состав

однотипные блоки (ОдБ), определённые согласно [12]. На вход ОдБ подаются значения НПФ от одной переменной, определённой над $GF(2^2)$ и представленной в виде вектора

$$F[*]=\begin{pmatrix} f(0) & f(1) & f(\xi) & f(\xi^2)\end{pmatrix}^T. \quad (2)$$

С выхода ОдБ снимаются коэффициенты НПФ (1), которая реализует функцию, заданную согласно (2). Вектор коэффициентов, элементы которого определены над $GF(2^2)$, вычисляется согласно уравнению

$$a[*]=\begin{pmatrix} a_0 & a_1 & a_2 & a_3\end{pmatrix}^T = C^{-1}\cdot F[*]. \quad (3)$$

Матрица $C^{-1}=\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & \xi^2 & \xi\\ 0 & 1 & \xi & \xi^2\\ 1 & 1 & 1 & 1\end{pmatrix}$.

Коэффициенты НПФ (*m*), заданной множеством значений при определенных наборах входных переменных, могут быть вычислены при использовании $m\cdot 4^{m-1}$ ОдБ. Вычисление обосновано путем представления (1) в виде рекурсивной формулы [9]: $g\begin{pmatrix} x_1 & \dots & x_m\end{pmatrix}=\sum_{i_1=0}^{3} g_{i_1}\begin{pmatrix} x_2 & \dots & x_m\end{pmatrix}x^{i_1}$. На входы первой группы из 4^{m-1} ОдБ подаются значения НПФ (*m*), которые она принимает при заданных значениях переменных на входе: $F[*][i_2]...[i_m]$, $i_j=\overline{0,3}$, $j=\overline{2,m}$. С выходов указанных блоков снимаются соответствующие вектора промежуточных коэффициентов первого уровня (ПрК1), полученных согласно (3): $a^{(1)}[*][i_2]...[i_m]$, $i_j=\overline{0,3}$, $j=\overline{2,m}$. На входы второй группы из 4^{m-1} ОдБ подаются следующие значения ПрК1: $a^{(1)}[i_1][*][i_3]...[i_m]$, а с выходов снимаются вектора ПрК2: $a^{(2)}[i_1][*][i_3]...[i_m]$, $i_j=\overline{0,3}$, $j=1,\overline{3,m}$. В общем случае на входы *d*-той группы из 4^{m-1} ОдБ, $d=\overline{2,(m-1)}$ подаются следующие значения ПрК $(d-1)$: $a^{(d-1)}[i_1]...[i_{d-1}][*][i_{d+1}]...[i_m]$, а с выходов снимаются вектора ПрК*d*: $a^{(d)}[i_1]...[i_{d-1}][*][i_{d+1}]...[i_m]$, $i_j=\overline{0,3}$, $j=\overline{1,(d-1)},\overline{(d+1),m}$. На входы *m*-той группы из 4^{m-1} ОдБ подаются следующие значения ПрК$(m-1)$: $a^{(m-1)}[i_1]...[i_{m-1}][*]$, а с выходов снимаются вектора ПрК*m*: $a^{(m)}[i_1]...[i_{m-1}][*]$, $i_j=\overline{0,3}$, $j=\overline{1,(m-1)}$.

Замечание 1. Множество векторов $a^{(m)}[i_1]...[i_{m-1}][*]$ образует матрицу коэффициентов НПФ (*m*) вида (1) – $a([i_1]...[i_m])$, $i_j=\overline{0,3}$, $j=\overline{1,(m-1)}$.

Замечание 2. Множество векторов $a^{(m)}[i_1]...[i_{m-1}][*]$ вычисляется путём конвейерного вычисления векторов ПрКd, $a^{(d)}[i_1]...[i_{d-1}][*][i_{d+1}]...[i_m]$, $i_j = \overline{0,3}$, $j = \overline{1,(d-1)}, \overline{(d+1),m}$, с сохранением промежуточных результатов.

На основе замечаний 1 и 2 и вышеизложенного сформулировано

Утверждение 6. Для конвейерного вычисления матрицы коэффициентов НПФ (m) вида (1) – $a([i_1]...[i_m])$, на основе матрицы её значений $F[i_1]...[i_m]$, $i_j = \overline{0,3}$, $j = \overline{1,m}$ требуется $m \cdot 4^{m-1}$ однотипных блоков, заданных согласно (3), по 4^{m-1} на каждой из m ступеней конвейера, а также m регистров на $2m$ двоичных разрядов, по одному после каждой ступени конвейера.

Методика подбора неопределённых значений НПФ (m)

Пусть для НПФ (m) вида (1) определены не все 4^m значений: x из них остаются неопределенными, причём $x \le 4^m/2$. Тогда всевозможные значения элементов матрицы $F[i_1]...[i_m]$, $i_j = \overline{0,3}$, $j = \overline{1,m}$, принадлежащих множеству неопределённых значений X, $|X| = x$, определяются методом перебора при использовании инкрементного двоичного счетчика на $2x$ разрядов.

Предложена методика подбора неопределённых значений НПФ (m) вида (1) в зависимости от ранга ЭлП, для которых при определении элементов множества X коэффициент $a([i_1]...[i_m])$ будет равен нулю. Методика включает пять этапов.

Этап 1. Задание элементов НПФ (m) вида (1) $F[i_1]...[i_m] \notin X$.

Этап 2. Задание всевозможных наборов значений элементов $F[i_1]...[i_m] \in X$ в количестве 2^{2x}. При заданных значениях элементов матрицы $F[i_1]...[i_m] \in X$ выполняем этапы 2.1 и 2.2. Этап 2.1. Вычисление $a([i_1]...[i_m])$ для НПФ (m) вида (1) при использовании аппаратного модуля. Этап 2.2. Определение количества ЭлП с рангами $(m \quad 0 \quad 0)$, $(m-1 \quad 1 \quad 0)$, $(m-1 \quad 0 \quad 1)$ и т. д., для которых $a([i_1]...[i_m]) = 0$ – нулевых ЭлП.

Этап 3. На основе выполнения этапов 2, 2.1 и 2.2 для всех наборов значений $F[i_1]...[i_m] \in X$ выбираем такое, для которого количество нулевых ЭлП с рангом $(m \quad 0 \quad 0)$ будет максимальным; в случае, когда существует два и более наборов значений $F[i_1]...[i_m] \in X$, имеющих равное количество нулевых ЭлП с рангом $(m \quad 0 \quad 0)$, выбор делаем на основе максимального количества нулевых ЭлП с рангом $(m-1 \quad 1 \quad 0)$ и т. д.

Предложенная методика позволяет осуществить подбор неопределённых значений НПФ (m) таким образом, чтобы минимизировать процесс её вычисления согласно формуле (1). Минимизация достигается путём обнуления коэффициентов при ЭлП максимальных рангов. Согласно данной методике на вход Схемы подаются значения НПФ(m), а с её выхода снимаются коэффициенты НПФ (m), заданной согласно (1).

Сложность реализации аппаратного модуля на ПЛИС/FPGA

ПЛИС класса FPGA включает в свой состав табличные генераторы заданных булевых функций от четырёх переменных – ГФ(4) [7; 8]. Оценим сложность реализации на ПЛИС/FPGA аппаратного модуля (далее – Модуля), реализующего как Схему, так и методику подбора неопределённых значений НПФ (m) при использовании конвейерных вычислений. По формуле (3) реализация ОдБ сводится к вычислению системы уравнений вида: $a_0 = f(0)$, $a_1 = f(1) + \xi^2 f(\xi) + \xi f(\xi^2)$, $a_2 = f(1) + \xi f(\xi) + \xi^2 f(\xi^2)$, $a_3 = f(0) + f(1) + f(\xi) + f(\xi^2)$.

Согласно [18] вычисление переменных a_1 и a_2 требует по 4 ГФ (4) соответственно, а переменной a_3 – 2 ГФ (4). Для вычисления a_0 ГФ (4) не требуются. Справедливо

Утверждение 7. Реализация ОдБ на ПЛИС/FPGA, включающего в свой состав ГФ (4), требует 6 ГФ (4).

Время задержки функционирования конвейерной реализации Модуля определяется временем задержки каждой из m ступеней конвейера, реализующего вычисление коэффициентов НПФ(m) вида (1). Блоки ввода-вывода (БВВ) ПЛИС/FPGA позволяют ввести $4^m - x$ значений НПФ (m), которые поступают в $2(4^m - x)$-разрядный двоичный регистр. Остальные x значений НПФ (m) доопределяются путем последовательного перебора всевозможных значений при использовании $2x$-разрядного инкрементного двоичного счетчика, установленного в нулевое значение на этапе инициализации Модуля. Ввод значений в зависимости от их количества может осуществляться либо параллельно, либо последовательно, либо параллельно-последовательно. В первом случае количество БВВ, сконфигурированных как входы, будет равно $2(4^m - x)$, и заполнение регистра происходит за один такт. Во втором случае требуется один БВВ, а заполнение происходит за $2(4^m - x)$ тактов. В третьем случае количество БВВ определяем произвольно как In. Количество тактов, требуемых для ввода значений НПФ (m) внутрь микросхемы ПЛИС/FPGA, равно $\left]2(4^m - x)/In\right[$. Квадратные скобки вида $\left]\ \right[$ обозначают округление значения, обрамлённого ими, до ближайшего большего целого.

Для вывода 4^m значений коэффициентов НПФ (m) вида (1), вычисленных при использовании Модуля, а также доопределённых значений указанной НПФ (m), произвольно определим Out БВВ. Доопределённые значения получаются путём сохранения содержимого $2x$-разрядного счетчика, уменьшенного на m, что требует блока вычитания константы m, включающего $2x$ разряда. В этом случае количество тактов, требуемых для вывода коэффициентов и доопределённых значений, будет равно $\left]2 \cdot 4^m/Out\right[+ \left]2x/Out\right[$.

Модуль включает в себя блок анализа нулевых коэффициентов. Для его реализации требуется идентификация наличия нулевых коэффициентов для ЭлП максимальных рангов, наибольшее количество которых не будет превышать максимального значения y. Блок анализа включает в себя:

- y ГФ (4), каждый из которых реализует функцию конъюнкции с инверсными входами;

- l схем сумматоров однобитных чисел [19], на R_a входов каждый (обозначим как Сум (R_a)), $a=\overline{1,l}$;
- l двоичных регистров, на r_a разрядов каждый: $r_a=\left]\log_2\left(R_a\right)\right[$, $a=\overline{1,l}$;
- компаратор на $\widehat{r}$ двоичных разрядов, $\widehat{r}=\sum_{a=1}^{l} r_a$;
- блок вычитания константы m на $2x$ разрядов;
- регистр на $2x$ двоичных разрядов.

Функции конъюнкции с инверсными входами служат для идентификации нулевых значений коэффициентов при ЭлП ранга $R_1\left(m\ \ 0\ \ 0\right)$, $R_2\left(m-1\ \ 1\ \ 0\right)$, …, $R_l\left(w_l\ \ \ e_l\ \ \ z_l\right)$, при этом $y=\sum_{R_1,\ldots,R_l} Q(w,e,z)$. Определим $R_a=Q(w_a,e_a,z_a)$, $a=\overline{1,l}$. Блок анализа функционирует следующим образом. На этапе инициализации $2x$- и r_a-разрядные регистры обнуляются, $a=\overline{1,l}$. На этапе анализа, начиная с m-того такта, производится сравнение содержимого r_a-разрядных регистров и значений, снимаемых с выходов Сум (R_a), $a=\overline{1,l}$. При этом двоичные значения, снимаемые с r_1-разрядных регистров и с выходов Сум (R_1), подаются на старшие разряды компаратора; на следующие разряды подаются значения, снимаемые с r_2-разрядных регистров и с выходов Сум (R_2) и т. д. На младшие разряды компаратора подаются значения, снимаемые с r_l-разрядных регистров и с выходов Сум (R_l). Если двоичное значение, образуемое выходами Сум (R_1), Сум (R_2), …, Сум (R_l), будет больше, чем значение, образуемое двоичными числами, занесёнными в регистры разрядности r_1, r_2, …, r_l, то значения с выходов Сум (R_a) заносятся в соответствующие регистры разрядности r_a, $a=\overline{1,l}$; кроме того, в $2x$-разрядный регистр заносится разность, снимаемая с блока вычитания. Что касается блока вычитания, то на вход уменьшаемого подается значение, снимаемое с $2x$-разрядного двоичного счётчика, а на вход вычитаемого – константа m.

Обозначим $t_{ББВ}$, $t_{ОдБ}$, $t_{Вч}$, $t_{\&}$, $t_{стр}$, t_D и t_{Ct} как времена задержек БВВ, ОдБ, блока вычитания константы m на $2x$ разрядов, блока вычисления конъюнкции, компаратора на $\widehat{r}$ двоичных разрядов, $\widehat{r}=\sum_{a=1}^{l} r_a$, загрузки в D-триггер значения на его входе и максимальное время срабатывания (изменения значения) счетчика соответственно. Согласно утверждениям 6 и 7, а также на основе вышеизложенного, для Модуля, вычисляющего коэффициенты (1) при заданных значениях НПФ (m) и реализованного на ПЛИС/FPGA при использовании конвейерной схемы на m ступеней, имеют место

Утверждение 8. Для реализации Модуля требуется не более $6m\cdot 4^{m-1}+y$ ГФ (4), $2m\cdot 4^m+\widehat{r}+2x$ D-триггеров, двоичный инкрементный счётчик, блок вычитания кон-

станты m на $2x$ разрядов, l Сум (R_a), $a = \overline{1, l}$, компаратор на $\widehat{r}$ двоичных разрядов, $\widehat{r} = \sum_{a=1}^{l} r_a$, а также $In + Out$ БВВ.

Утверждение 9. Оценки времени инициализации, задержки вычисления коэффициентов НПФ (m) вида (1) и вывода полученных коэффициентов для Модуля равны соответственно

$$T_{INIT} = \left(t_{БВВ} + t_D\right) \cdot \left]2\left(4^m - x\right)\right/ In\left[, \tag{4}$$

$$T = \max\left(t_{ОдБ}, t_{Вч}, \left(t_{\&} + t_{стр}\right)\right) + \max\left(t_D, t_{Ct}\right) \text{ и} \tag{5}$$

$$T_{Out} \geq t_{БВВ} \cdot \left(\right]2 \cdot 4^m / Out\left[+ \right]2x / Out\left[\right). \tag{6}$$

Утверждение 8 определяет оценки аппаратных затрат однотипных элементов ПЛИС класса FPGA, требуемых для реализации Модуля с параллельным выводом. Верхняя оценка количества ГФ(4) при росте числа переменных НПФ (m) вида (1) растет экспоненциально и имеет порядок $\mathrm{O}\left(m \cdot 4^m\right)$. Количество D-триггеров также растет экспоненциально и имеет порядок $\mathrm{O}\left(4^m\right)$.

Инициализация Модуля производится за время, определённое согласно (4). Формула (5) в утверждении 9 позволяет определить частоту подачи различных вариантов значений НПФ (m) на вход Модуля в зависимости от максимального значения времени задержки либо ОдБ, либо блока вычитания константы m, либо суммы $\left(t_{\&} + t_{стр}\right)$, сложенного с максимальным временем, либо загрузки значений в D-триггер, либо срабатывания счетчика. Результаты оказываются на выходе Модуля спустя m тактов с момента подачи исходных данных на его вход. Затем на каждом такте происходит анализ количества нулевых коэффициентов при ЭлП максимальных рангов. Выполнение конвейерного вычисления всевозможных значений коэффициентов НПФ(m) вида (1) производится за $\left(2^{2x} + m\right)$ тактов. Затем производится вывод коэффициентов НПФ (m) и её доопределённых значений за время, определённое согласно формуле (6).

Заключение

Предложена масштабируемая структурная Схема для вычисления коэффициентов нелинейной полиномиальной функции над полем Галуа вида $GF(2^2)$ на основе задания её значений. Схема реализуема при использовании однотипных блоков, количество которых варьируется определённым образом в зависимости от количества переменных НПФ (m). Показано, что Схема предполагает возможность конвейерной реализации. На основе данной Схемы предложена методика подбора неопределённых значений НПФ(m) таким образом, чтобы обнулить её коэффициенты при элементарных полиномах максимальных рангов. Получены оценки аппаратной сложности и времени задержки функционирования Модуля, позволяющего реализовать методику подбора неопределённых значений НПФ (m), на основе предложенной конвейерной Схемы. Время задержки функционирования включает три этапа: инициализацию Модуля, подбор коэффициентов с их обнулением при элементарных полиномах максимальных рангов и вывод полученных коэффициентов вместе с подобранными доопределёнными значениями НПФ (m).

Полученные оценки сложности реализации Схемы и Модуля являются универсальными и могут быть адаптированы к различным семействам ПЛИС класса FPGA, как к уже существующим, так и к перспективным.

Литература

1. Высокопроизводительные реконфигурируемые вычислительные системы / *А.И. Дордопуло, И.А. Каляев, И.И. Левин и др.* // Суперкомпьютеры. 2010. № 3 (3). – С. 44–48.

2. Развитие отечественных многокристальных реконфигурируемых вычислительных систем: от воздушного к жидкостному охлаждению / *И.А. Каляев, А.И. Дордопуло, И.И. Левин, А.М. Федоров* // Труды СПИИРАН. 2017. № 1 (50). – С. 5–31.

3. *Захаров В.М., Шалагин С.В*. Распределенное вычисление нелинейных многочленов над полем Галуа в архитектуре FPGA // Вестник Технологического университета. 2018. Т. 21, № 11. – С. 146–149.

4. *Воеводин В.В., Воеводин Вл.В*. Параллельные вычисления. – СПб.: БХВ-Петербург, 2002. – 600 с.

5. *Rakhmatullin A.K., Gibadullin R.F*. Synthesis and Analysis of Elementary Algorithms for a Differential Neural Computer // Lobachevskii J. Math. 2022. № 43. – Pp. 473–483 https://doi.org/10.1134/S1995080222050225

6. *Cherny S.N., Gibadullin R.F*. The Recognition of Handwritten Digits Using Neural Network Technology // International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). – Sochi, 2022. – Pp. 965–970.

7. FPGA Leadership across Multiple Process Nodes / Advanced Micro Devices, Inc. 2023. – URL: https://www.xilinx.com/products/silicon-devices/fpga.html

8. ПЛИС Altera. ООО «Электроника-РА». 2014–2021. – Режим доступа: https://el-ra.ru/mikroskhemy/plis-cpld/plis-altera/

9. *Шалагин С.В*. Реализация цифровых устройств в архитектуре ПЛИС/FPGA при использовании распределенных вычислений в полях Галуа. – Казань: Казанский государственный технический университет им. А.Н. Туполева, 2016. – 228 с.

10. *Шалагин С.В., Глазков И.Д*. Сложность реализации нелинейных полиномов на массивах ПЛИС класса FPGA // Вестник Дагестанского государственного университета. Сер. 1: Естественные науки. 2021. Т. 36, вып. 2. – С. 31–38.

11. *Shalagin S.V*. Computing a group of polynomials over a galois field in fpga architecture // Mathematics. 2021. Vol. 9, no. 24.

12. *Захаров В.М., Шалагин С.В., Эминов Б.Ф*. Автоматные марковские модели над конечным полем. – Казань: Специализированный фонд управления целевым капиталом для развития Казанского национального исследовательского технического университета им. А.Н. Туполева – КАИ, 2022. – 328 с.

13. *Лидл Р., Нидеррайтер Г*. Конечные поля: в 2 т. – М.: Мир, 1988.

14. *Николаев А.Г., Нурутдинов Ш.Р*. Полиномиальные модели конечных детерминированных автоматов над полем GF(2^p) // Вестник Удмуртского университета. Математика. 2007. № 1. – С. 83–98.

15. *Нурутдинов Ш.Р., Шалагин С.В*. Минимизация количества элементов однородной вычислительной структуры // Исследования по информатике. – Казань: Отечество, 2000. № 2. – С. 117–124.

16. *Захаров В.М., Шалагин С.В*. Параллельные марковские модели над полем $GF(2^n)$ // Высокопроизводительные параллельные вычисления на кластерных системах:

сб. тр. Восьмой Межд. конф. – Казань: Изд-во КГТУ им. А.Н. Туполева, 2008. – С. 155–160.

17. *Нурутдинов Ш.Р*. Однородные вычислительные структуры над конечным полем // Исслед. по прикл. матем. 1990. Вып. 17. – С. 105–114. – Режим доступа: https://www.mathnet.ru/links/ dc80eb51f8613447aaf96e2049fa0578/kuipm55.pdf

18. *Шалагин С.В.* Сложность вычисления нелинейной полиномиальной функции над полем Галуа вида GF(2^k) в базисе булевых функций от 2k переменных // Дискретные модели в теории управляющих систем: IX Международная конференция (г. Москва, 20–22 мая 2015 г.) / отв. ред. В.Б. Алексеев, Д.С. Романов, Б.Р. Данилов. – М.: МАКС Пресс, 2015. – С. 264–266.

19. *Гашков С.Б*. Сложение однобитных чисел. Треугольник Паскаля, салфетка Серпинского и теорема Куммера. – М.: МЦНМО, 2014. – 40 с. – Режим доступа: https://mccme.ru/free-books/mmmf-lectures/book.38.pdf

Поступила в редакцию 2 марта 2023 г.

UDC 004.272.26

DOI: 10.21779/2542-0321-2023-38-2-81–89

Hardware Module for Calculating Coefficients of Nonlinear Polynomial Function Over Galois Field

S.V. Shalagin, D.Ju. Mal`kin

Kazan National Research Technical University named after A.N. Tupolev – KAI; Russia, 420111, Kazan, Karl Marks st., 10; sshalagin@mail.ru, developkin@mail.ru

Abstract. A conveyor scheme for calculating the coefficients of nonlinear polynomial function over Galois field using the same type of blocks based on setting its values is proposed. The method of selecting the coefficients of this function, which reduces the complexity of its calculation by zeroing its coefficients is presented. The coefficients are ranked depending on their contribution to reducing the complexity of calculating this function by zeroing the eigenvalues. Estimates of the complexity of the module implementing the technique on FPGA-class are obtained. These estimates allow us to perform a preliminary analysis of the costs of FPGA-class hardware resources, both existing and prospective.

Keywords: coefficients, nonlinear polynomial function, complexity estimates.

Received 2 March 2023