УДК 004.272.2

Параллельные вычисления в кольце гауссовых чисел над полем Галуа $GF(p)$

В.М. Амербаев, А.Л. Стемпковский, Р.А. Соловьев

Институт проблем проектирования в микроэлектронике РАН, turbo@ippm.ru

***Аннотация* — В статье рассматриваются методы "глубокого распараллеливания" вычислений над комплекснозначными операндами. В качестве модели вычислений выбрано кольцо гауссовых чисел над полем Галуа $GF(p)$. Элементы кольца имеют строение комплексных чисел с действительной и мнимой частями из конечного поля $GF(p)$. Разработанные методы глубокого распараллеливания распространяются на вычисления в традиционном кольце целых комплексных чисел.**

***Ключевые слова* — поле Галуа, гауссовы числа, кольцо гауссовых чисел, вычеты целых комплексных чисел по комплексному модулю.**

I. Введение. Постановка задачи

Вычислительные процессы обработки планарной информации, включая спектральный анализ многомерных сигналов, сопряжены с вычислениями в комплексной плоскости. В связи с этим возникает проблема ускорения подобного рода вычислений. В качестве прототипа объекта распараллеливания в статье рассматриваются операции на множестве "обобщенных комплексных чисел": $G_p = \{z | z = x + jy,$ где $x, y \in GF(p), j^2 = -1\}$ [4]. Здесь x, y элементы поля Галуа $GF(p)$. G_p наделяется структурой кольца, если операции $\pm,\times$ над элементами G_p определять по аналогии с операциями над комплексными числами:

$\forall z_1, z_2 \in G_p,$ где $z_1 = x_1 + jy_1, z_2 = x_2 + jy_2$

$z_1 \pm z_2 = (x_1 \pm x_2) + j(y_1 \pm y_2);$

$z_1 \times z_2 = (x_1 \cdot x_2 - y_1 \cdot y_2) + j(x_1 \cdot y_2 - x_2 \cdot y_1)$

при этом в роли операций $\pm,\times$ над компонентами комплекснозначных операндов z_1, z_2 выступают аддитивные и мультипликативные операции поля $GF(p)$, а не соответствующие операции поля $\mathbb{R}$. Элементы из G_p будем называть гауссовыми числами над полем Галуа $GF(p)$.

Ставится задача распараллелить арифметические операции кольца G_p . Традиционный подход к решению этой задачи состоит в параллельной реализации операций над действительной и мнимой частями операндов. Нас будет интересовать возможность более глубокого распараллеливания за счет перехода к более низкому уровню вычислений.

В связи с этим напомним исходные положения алгебры вычетов целых комплексных чисел по комплексным модулям, впервые исследованных великим математиком К.Ф. Гауссом [1].

Пусть w – фиксированное целое комплексное число $w = a + bj \in \mathbb{CZ}$ с нормой $p = a^2 + b^2$. Пусть $z = x + yj$ – произвольное целое комплексное число.

Рассмотрим отношение $\frac{z}{w} = \frac{z \cdot \bar{w}}{p} = \frac{|z \cdot \bar{w}|_p}{p} + \left\lfloor \frac{z \cdot \bar{w}}{p} \right\rfloor$.

Здесь символом $|u|_p$ обозначен вычет целого комплексного числа u по модулю натурального числа p.

Отсюда

$$z = \frac{|z \cdot \bar{w}|_p \cdot w}{p} + \left\lfloor \frac{z \cdot \bar{w}}{p} \right\rfloor \cdot w \qquad (1)$$

Поскольку числа $z, w, \left\lfloor \frac{z \cdot \bar{w}}{p} \right\rfloor$ являются целыми комплексными числами, то первое слагаемое разложения (1) также является целым. Обозначим его символом:

$$\langle z |_w = \frac{|z \cdot \bar{w}|_p \cdot w}{p} \qquad (2)$$

Разложение (1) представляет собой аналог теоремы Евклида в кольце целых комплексных чисел $\mathbb{CZ}$. При этом число $\left\lfloor \frac{z \cdot \bar{w}}{p} \right\rfloor$ служит неполным частным, а $\langle z |_w$ – остатком от деления числа z на число w. К.Ф. Гаусс в работе [1] число $\langle z |_w$ называет вычетом числа z по комплексному модулю w, а совокупность $\mathbb{CZ}_w$ всех возможных вычетов чисел из $\mathbb{CZ}$ - полной системой вычетов по $mod\, w$. Исходя из тождества (1) доказываются свойства вычетов: $\forall z_1, z_2 \in \mathbb{CZ}$ справедливы равенства:

$$\langle z_1 \pm z_2 |_w = \langle \langle z_1 |_w \pm \langle z_2 |_w |_w \qquad (3)$$

$$\langle z_1 \cdot z_2 |_w = \langle \langle z_1 |_w \cdot \langle z_2 |_w |_w \qquad (4)$$

Тождества (3) и (4) позволяют доказать, что множество $\mathbb{CZ}_w$ является кольцом.

В соответствие с определением вычета (2), кольцо $\mathbb{CZ}_w$ изоморфно кольцу $\mathbb{CZ}_p$, поскольку:

$$|(z_1 \pm z_2) \cdot \bar{w}|_p = \left| \left(|z_1|_p \pm |z_2|_p \right)_p \right) \cdot \bar{w} \Big|_p; \qquad (5)$$

$$|(z_1 \cdot z_2) \cdot \bar{w}|_p = \left| \left(|z_1|_p \cdot |z_2|_p \right)_p \right) \cdot \bar{w} \Big|_p. \qquad (6)$$

Аналогичные утверждения справедливы и для модуля $\overline{w} = a - bj$, сопряженного модулю $w = a + bj$. Соответственно, соотношения (1)-(6) перепишутся посредством замены в них модуля w на модуль $\overline{w}$.

Тем самым, при условии $(a, b) = 1$ кольцо $\mathbb{CZ}_{\|w\|}$ где $\|w\| = a^2 + b^2$, в силу китайской теоремы об остатках [1] изоморфно прямому произведению колец $\mathbb{CZ}_w \times \mathbb{CZ}_{\overline{w}}$.

II. Кольцо гауссовых чисел над простым полем $GF(p)$

Мультипликативная структура кольца G_p зависит от того, какому из двух нижеследующих ограничений удовлетворяет простое число $p: p \equiv 3(mod\ 4)$ или $p \equiv 1(mod\ 4)$. В первом случае G_p – поле порядка p^2 [2,3] и здесь распараллеливание арифметических операций реализуется традиционным путем – посредством параллельной обработки действительных и мнимых частей операндов. Во втором случае G_p – кольцо с делителями нуля [4,5] и здесь открывается возможность низкоуровнего распараллеливания арифметических операций в G_p. Такую возможность предоставляет теорема Гаусса об изоморфизме [1]. Остановимся на этих вопросах подробнее. Рассмотрим кольцо целых комплексных чисел $\mathbb{CZ}$:

$$\mathbb{CZ} = \{z | z = x + jy, \text{где } x, y \in \mathbb{Z}, j^2 = -1\}.$$

В соответствии с теоремой Евклида [3], для любого натурального числа p $(p \neq 1)$ кольцо $\mathbb{CZ}$ гомоморфно отображается в кольцо вычетов по $mod\ p$:

$$\mathbb{CZ}_p = \{z | z = x + jy, \text{где } x, y \in \mathbb{Z}_p, j^2 = -1\}.$$

Так как при простом p: $\mathbb{Z}_p = GF(p)$, то кольцо $\mathbb{CZ}_p$ изоморфно кольцу G_p. Это позволяет интерпретировать все операции кольца гауссовых чисел G_p над полем $GF(p)$ в терминах теории сравнения целых комплексных чисел по комплексным модулям. Известно, что если простое число p удовлетворяет условию $p \equiv 1(mod\ 4)$, то число p представимо в виде суммы квадратов: $\exists a, b \in \mathbb{Z}: p = a^2 + b^2, (a, b) = 1$. Тем самым простое натуральное число p перестает быть простым в кольце целых комплексных чисел $\mathbb{CZ}$, так как $p = (a + jb)(a - jb)$. Поскольку при этом a и b взаимно простые, то и числа $a + jb$ и $a - jb$ взаимно простые. Следовательно, в рассматриваемом случае и при простом p, согласно китайской теореме об остатках, кольцо $\mathbb{CZ}_p$ изоморфно прямому произведению колец вычетов $\mathbb{CZ}_w \times \mathbb{CZ}_{\overline{w}}$ кольца $\mathbb{CZ}$ по комплексным модулям $w = a + jb$ и $\overline{w} = a - jb$, соответственно. Этот факт лежит в основе более глубокого распараллеливания операций кольца G_p. Заметим, что для случая кольца целых комплексных чисел $\mathbb{CZ}$ он использован в работах [4,5].

III. Параллельные вычисления над G_p

Параллельные вычисления над G_p $(p \equiv 1\ mod\ 4)$ базируются на нижеследующей теореме.

Теорема Гаусса (об изоморфизме). Если целое комплексное число $w = A + jB$ удовлетворяет условию $(A, B) = 1$, то кольцо вычетов $\mathbb{CZ}_w$ кольца целых комплексных чисел $\mathbb{CZ}$ по комплексному модулю w изоморфно кольцу вычетов $\mathbb{Z}_p$ целых действительных чисел $\mathbb{Z}$ по модулю p, где $p = A^2 + B^2$.

Доказательство: Пусть $n + jm$ – некоторое целое комплексное число. Вычислим произведение:

$$w \cdot (n + jm) = (An - Bm) + j(Am + Bn) \qquad (7)$$

Так как $(A, B) = 1$, то уравнение $Am + Bn = 1$ разрешимо в целых числах [7]. Пусть m_0 и n_0 некоторое его решение, т.е.

$$Am_0 + Bn_0 = 1 \qquad (8)$$

Преобразуем (7) к виду $j = (Bm_0 - An_0) + (n_0 + jm_0)w$. Поскольку $p = w \cdot \overline{w}$, то последнее равенство можно переписать так:

$$j = |Bm_0 - An_0|_p + (q_0\overline{w} + n_0 + jm_0)w \qquad (9)$$

где $q_0 = \left\lfloor \frac{Bm_0 - An_0}{p} \right\rfloor$, а выражением $|Bm_0 - An_0|_p$ обозначен наименьший неотрицательный вычет целого действительного числа $Bm_0 - An_0$ по модулю p.

Согласно (1) $z = \langle z|_w + q \cdot w$, где $q = \left\lfloor \frac{z}{w} \right\rfloor$. Используя (9) получим, что для любого $(x + jy) \in \mathbb{CZ}$ справедливо:

$$\langle x + jy|_w \equiv |x + q^+ y|_p (mod\ w) \qquad (10)$$

где

$$q^+ = |Bm_0 - An_0|_p \qquad (11)$$

Из сравнения (10) следует, что форма $|x + q^+ y|_p$ пробегает полную систему наименьших неотрицательных чисел по модулю p, когда форма $\langle x + jy|_w$ пробегает полную систему вычетов целых комплексных чисел по комплексному модулю w. Указанное соответствие устанавливает изоморфизм кольца вычетов кольца $\mathbb{CZ}$ по комплексному модулю $w = a + bj$ кольцу вычетов $\mathbb{Z}_p$ кольца целых действительных чисел $\mathbb{Z}$ по модулю p. Величина q^+, определяемая формулой (11) названа в [4,5] коэффициентом изоморфизма Гаусса по модулю w. Из (10) следует, что $(q^+)^2 \equiv -1(mod\ p)$.

Следуя аналогичным рассуждениям можно показать, что для сопряженного модуля $\overline{w} = A - Bj$ коэффициент изоморфизма q^- принимает вид $q^- = |An_0 - Bm_0|_p = |-q^+|_p$. При этом кольцо вычетов $\mathbb{CZ}_{\overline{w}}$ также изоморфно кольцу $\mathbb{Z}_p$.

Вывод: Поскольку $(A, B) = 1$, то в силу китайской теоремы об остатках согласно теореме Гаусса каждый элемент $z = x + jy$ из G_p однозначно кодируется парой $(\langle z|_w, \langle z|_{\overline{w}})$ или (v, v'), где

$$v = |x + q^+ y|_p,\ v' = |x + q^- y|_p \qquad (12)$$

При этом $\forall z_1, z_2 \in G_p$:

$$\langle z_1 \pm z_2|_p \leftrightarrow \left(|v_1 \pm v_2|_p, |\,v'_1 \pm\, v'_2|_p\right) \quad (13)$$

$$\langle z_1 \cdot z_2|_p \leftrightarrow \left(|v_1 \cdot v_2|_p, |\,v'_1 \cdot\, v'_2|_p\right) \quad (14)$$

Обратное преобразование, восстанавливающее $z = x + jy \in \mathbb{CZ}_p$ по паре (v, v'), согласно (12) имеет вид:

$$x = \left|\frac{q^- v - q^+ v'}{q^- - q^+}\right|_p = \left|\frac{v+v'}{2}\right|_p \quad (15)$$

$$y = \left|\frac{v-v'}{q^+ - q^-}\right|_p = \left|\frac{v-v'}{2q^+}\right|_p \quad (16)$$

Итак, совокупность всех пар (v, v') образует кольцо с операциями сложения, вычитания, умножения, реализуемыми параллельным сложением, вычитанием и умножением компонент пар по модулю p, изоморфное G_p - кольцу гауссовых чисел над полем $GF(p)$. Обозначим это кольцо символом $\mathbb{Z}_p \times \mathbb{Z}_p$, и назовем его кольцом парных вычетов.

Описанную схему, в отличие от традиционного распараллеливания, будем называть низкоуровневым или более глубоким распараллеливанием.

Замечание 1: Следует отметить, что теорема Гаусса, вообще говоря, не требует простоты p - квадрата нормы комплексного числа w. Этот факт используется в [4,5] при построении на основе теоремы Гаусса об изоморфизме модулярной арифметики в кольце $\mathbb{CZ}_{p_1 p_2 \dots p_n}$, где p_i – не обязательно простые числа вида $p_i \equiv 1(mod\ 4)$.

Благодаря этому существенно упрощается реализация мультипликативных операций комплексных чисел, не усложняя при этом реализацию аддитивных операций.

Замечание 2: При фиксированной норме p комплексного модуля w $(p = a^2 + b^2)$ сам модуль w может выступать в роли любого из следующих целых комплексных чисел $\pm a \pm bj, \pm b \pm aj$. Эта вариативность выбора модулей w может использоваться при построении различных цифровых преобразователей со скрытыми параметрами, связанных с обработкой многомерных сигналов [6], защитой от помех в вычислительных каналах и защитой от несанкционированного доступа.

IV. Численный пример низкоуровнего параллельного умножения и сложения в поле гауссовых чисел G_p над полем $GF(p)$

Сначала выберем простое число p, удовлетворяющее условию $p \equiv 1(mod\ 4)$. Пусть $p = 97 = 24 \cdot 4 + 1$. Далее выберем некоторое комплексное число w, норма которого будет равна p. Пусть $w = 9 + 4j$, т.е. $A = 9, B = 4$. $9^2 + 4^2 = 97 = p$. Предположим, что нам требуется умножить и сложить два комплексных числа $z_1 = 2 + j$ и $z_2 = 3 + 2j$ по модулю 97.

Прямое преобразование:

Шаг 1: Находим произвольное решение уравнения (8) $Am_0 + Bn_0 = 1$ в целых числах.

$$9m_0 + 4n_0 = 1 \rightarrow m_0 = \frac{1 - 4n_0}{9} \rightarrow\ n_0 = -2, m_0 = 1$$

Шаг 2: Находим коэффициент $q^+ = |Bm_0 - An_0|_p$ по формуле (11).

$$q^+ = |4m_0 - 9n_0|_{97} = 22 \rightarrow q^- = |-22|_{97} = |97 - 22|_{97} = 75$$

Шаг 3: Находим пару (v, v') для обоих чисел z_1 и z_2 по формулам (12).

$$v_1 = |x_1 + q^+ y_1|_p = |2 + 22 \cdot 1|_{97} = 24$$

$$v'_1 = |x_1 + q^- y_1|_p = |2 + 75 \cdot 1|_{97} = 77$$

$$v_2 = |x_2 + q^+ y_2|_p = |3 + 22 \cdot 2|_{97} = 47$$

$$v'_2 = |x_2 + q^- y_2|_p = |3 + 75 \cdot 2|_{97} = 56$$

Сложение:

Используем формулу (13):

$$\langle z_1 \pm z_2|_p \leftrightarrow \left(|v_1 \pm v_2|_p, |\,v'_1 \pm\, v'_2|_p\right) = (|24 + 47|_{97}, |77 + 56|_{97}) = (71,36)$$

Умножение:

Используем формулу (14):

$$\langle z_1 \cdot z_2|_p \leftrightarrow \left(|v_1 \cdot v_2|_p, |\,v'_1 \cdot\, v'_2|_p\right) = (|24 \cdot 47|_{97}, |77 \cdot 56|_{97}) = (61,44)$$

Обратное преобразование:

Чтобы по заданной паре (v, v') восстановить число $z = x + jy \in \mathbb{CZ}_p$, необходимо воспользоваться формулами (15 и 16). Отметим, что операция деления, которая встречается в формулах, является операцией обратной умножению и выполняется в целых числах. То есть, чтобы найти x в выражении $\left|\frac{1}{a}\right|_p = x$, треубется решить уравнение $|a \cdot x|_p = 1$.

$$(v, v') = (71,36) \rightarrow$$

$$x = \left|\frac{v + v'}{2}\right|_p = \left|\frac{71 + 36}{2}\right|_{97} = \left|\frac{10}{2}\right|_{97} = 5$$

$$y = \left|\frac{v - v'}{2q^+}\right|_p = \left|\frac{71 - 36}{2 \cdot 22}\right|_{97} = \left|35 \cdot \left|\frac{1}{44}\right|_{97}\right|_{97} = |35 \cdot 86|_{97} = 3$$

$$(v, v') = (61,44) \rightarrow$$

$$x = \left|\frac{v + v'}{2}\right|_p = \left|\frac{61 + 44}{2}\right|_{97} = \left|\frac{8}{2}\right|_{97} = 4$$

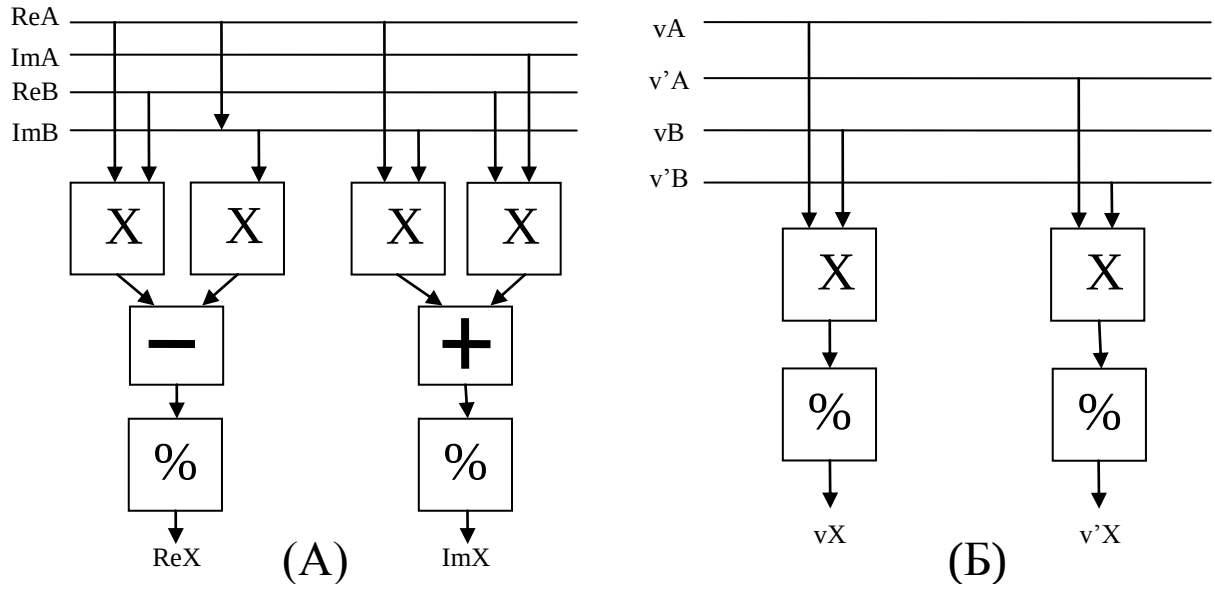

Рис. 1. (А) – традиционный комплексный модулярный умножитель, (Б) –умножитель в кольце G_p. X – блок умножения, - – блок сложения, % - блок вычисления остатка по модулю

$y = \left|\frac{v-v'}{2q^+}\right|_p = \left|\frac{61-44}{2\cdot 22}\right|_{97} = \left|17 \cdot \left|\frac{1}{44}\right|_{97}\right|_{97} = |17 \cdot 86|_{97} = 7$

Проверка корректности преобразования:

Проверим, что найденные результаты сложения $(5 + 3j)$ и умножения $(4 + 7j)$ корректны.

$$|z_1 + z_2|_p = |2 + j + 3 + 2j|_{97} = 5 + 3j$$

$$|z_1 \cdot z_2|_p = |(2 + j) \cdot (3 + 2j)|_{97} = |6 - 2 + 3j + 4j|_{97} = 4 + 7j$$

V. Сравнительный анализ эффективности аппаратной реализации вычислений в кольце гауссовых чисел над полем Галуа $GF(p)$

Для построения модели устройства выбран маршрут проектирования цифровых ИС на основе библиотек стандартных ячеек. В маршруте используется: поведенческое описание устройства на языке Verilog HDL; средства логического синтеза Synopsys Design Compiler; средства статического временного анализа Synopsys Prime Time; библиотека стандартных ячеек Nangate Open Cell Library с проектными нормами 45нм.

В данной работе были созданы модели как традиционного модулярного комплексного умножителя, так и умножителя в кольце гауссовых чисел над полем Галуа. Анализ характеристик этих двух моделей позволяет получить сравнительную оценку эффективности аппаратной реализации предложенного подхода.

Структурные схемы разработанных устройств приведены на рисунке 1.

Из приведенных структурных схем видно, что схема «Б» содержит вдвое меньше блоков умножения, чем схема «А», и не содержит блоков сложения и вычитания, что даст при аппаратной реализации схемы «Б» значительный выигрыш по площади, занимаемой на кристалле. С точки зрения быстродействия анализ схем, также показывает некоторое преимущество варианта «Б» за счет отсутствия блоков сложения/вычитания и вызванного этим уменьшения на одну позицию разрядности входных данных блока вычисления остатка по модулю.

В соответствие с предложенными структурными схемами были разработаны RTL-описания комплексных модулярных умножителей и умножителей в кольце Гауссовых чисел над полями Галуа для всех простых оснований вида $p \equiv 1(mod\ 4)$ в диапазоне от 5 до 300.

В результате логического синтеза в базисе библиотеки стандартных ячеек и статического временного анализа были получены значения суммарных площадей ячеек и задержек сигналов на критических путях.

Литература

[1] Гаусс К.Ф., Труды по теории чисел / общ.ред. ак. И.М. Виноградова / М.: Изд. АНСССР, 1959.

[2] Лидл Р., Пильц Г., Прикладная абстрактная алгебра / Пер. с англ. Коряков И.О. Екатеринбург: Изд. Уральского университета, 1996. 744 с.

[3] Ноден П., Китте К. Алгебраическая алгоритмика (перевод с французского Соколова В.А. под ред. Казарика Л.С.) . М.: Изд. «Наука». 1984. 183 с.

[4] Акушский И.Я., Амербаев В.М., Пак И.Т. Основы машинной арифметики комплексных чисел. Алма-Ата.: Изд. «Наука». 1970. 247 с.

[5] Амербаев В.М., Пак И.Т. Параллельные вычисления в комплексной плоскости. Алма-Ата.: Изд. «Наука». 1984. 183 с.

[6] Чобану М. Многомерные многоскоростные системы обработки сигналов. М.: Техносфера. 2009. 480 с.

[7] Виноградов И.М. Основы теории чисел. 1965. 180 с.