УДК 621.391: 681.3

В.М. ИЛЮШКО[1], МОХАММЕД ДЖАСИМ МОХАММЕД[1], В.А. КРАСНОБАЕВ[2]

[1]*Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Украина*
[2]*Харьковский национальный технический университет сельского хозяйства, Украина*

ИССЛЕДОВАНИЕ ВЛИЯНИЯ СВОЙСТВ МОДУЛЯРНОЙ АРИФМЕТИКИ НА СТРУКТУРУ И ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ СИСТЕМ ОБРАБОТКИ ИНФОРМАЦИИ РЕАЛЬНОГО ВРЕМЕНИ

В данной статье проводятся теоретические исследования возможности эффективного применения модулярной арифметики (МА) для обработки цифровой информации в реальном времени. Показано влияние основных свойств МА на структуру и принципы функционирования систем обработки цифровой информации реального времени

система обработки информации, модулярная арифметика, цифровая обработка сигналов, поля Галуа, система остаточных классов

Введение

В настоящее время весьма актуальной и до конца нерешенной задачей является задача эффективной цифровой обработки сигналов (ЦОС) в системах обработки информации (СОИ) реального времени. С одной стороны, ЦОС занимает основополагающее место в современных средствах переработки информации в связи с такими ее преимуществами, как высокая точность обработки информации и гибкость. С другой стороны, эффективность ЦОС в большей степени определяется объемом необходимых вычислений, который получается при реализации математических моделей (ММ) процесса ЦОС. Реализация задач цифровой обработки сигналов заключается в синтезе ММ функционирования данной системы и далее ее технической реализации. Практическая реализация задач ЦОС наталкивается на ряд трудностей. Это обусловлено двумя основными факторами: во-первых, нет четкого, единого подхода к синтезу математических моделей систем цифровой обработки сигналов; во-вторых, недостаточная теоретическая и практическая проработка вопросов создания высокопроизводительных и сверхнадежных СОИ, реализующих математические модели систем ЦОС.

Анализ последних исследований и публикаций. В последнее время получают распространение математические модели систем ЦОС, созданные на основе применения абстрактных алгебраических систем, в частности, математические модели, основанные на применении теории полей Галуа [1, 2]. Основные преимущества данных моделей систем ЦОС состоят в следующем:

– такие модели более полно учитывают дискретную структуру представления обрабатываемого цифрового сигнала;

– упрощается аппаратная реализация математических моделей.

Основной недостаток математических моделей систем ЦОС, созданных на основе использования абстрактных алгебраических систем, состоит в необходимости разработки принципиально новой структуры СОИ для эффективной реализации операций конечного поля Галуа или кольца с заданной алгебраической структурой. В связи с этим перечислим ***основные специфические требования и характерные особенности***, предъявляемые к СОИ ЦОС реального времени:

– необходимость обработки большого количества информации в реальном времени, что требует сверх-

высокого быстродействия (высокой пользовательской производительности) решения задач цифровой обработки сигналов, а это, в свою очередь, обуславливает необходимость обеспечения высокой надежности (отказоустойчивости) функционирования и достоверности вычислений;

– универсальность для заданного класса задач ЦОС;

– необходимость оперирования с целыми числами, являющимися элементами поля Галуа GF(M) или конечного кольца вычетов;

– отсутствие привычного физического смысла промежуточных результатов вычислений в конечных полях или кольцах, что одновременно с требованием использования полей Галуа *GF*(M) с большим значением модуля *M*, обуславливает необходимость использования СОИ с сравнительно большой разрядной сеткой;

– глубокая адаптация к классу (типу) решаемых задач систем ЦОС (к типу операций, входящих в реализуемые алгоритмы), что сопровождается необходимостью создания рациональных структуру СОИ, а это, в свою очередь, может оказать существенное влияние на такие характеристики СОИ ЦОС, как производительность, отказоустойчивость, надежность, также на конструкцию отдельных функциональных блоков и узлов, входящих в состав СОИ, и т.д.;

– адаптация к отказам и сбоям;

– для бортовых СОИ (например, для СОИ БПЛА) жесткие требования к массогабаритным характеристикам, потребляемой мощности и т.п.

Анализ методов и алгоритмов решения задач цифровой обработки сигналов посредством СОИ, функционирующих в позиционной системе счисления (ПСС), показал:

– во-первых, возможности позиционных систем счисления для построения СОИ различного назначения практически ограничены;

– во-вторых, на современном уровне развития технологии применение позиционных вычислителей не может полностью обеспечить требований, которые предъявляются к средствам обработки информации [3, 4].

Вследствие этого ***возникает задача*** поиска путей совершенствования СОИ ЦОС на основе использования нетрадиционных систем счисления наиболее адаптивных к классу задач, решаемых системами ЦОС.

Одной из таких систем счисления может служить модулярная арифметика (МА), т.е. непозиционная система счисления в остаточных классах (СОК).

Пусть для области определения E_N цифрового сигнала $x(n)$ рассмотрим абелеву группу

$$H = H_1 \times H_2 ... \times H_n ,$$

где $H -$ циклическая группа порядка

$$[H:1]N = \sum_{i=1}^{n} q_i ;$$

$q_i = m_i^{\alpha i} -$ порядок подгруппы H_i; $\{m_i\} -$ набор простых чисел ($i = \overline{1,n}$) $\alpha_i \in Z$, где $Z -$ кольцо целых чисел.

Произвольный элемент $n \in H$ может быть представлен в виде

$$n = (n_1, n_2, ..., n_i, ..., n_\varsigma), \; n_i \in H_i .$$

В этом случае групповая операция определяется следующим образом:

$$Z = (x \oplus y) = (x_1, x_2, ..., x_n) \oplus (y_1, y_2, ..., y_n) = \\ = ((x_1 \oplus y_1), (x_2 \oplus y_2), ..., (x_n \oplus y_n)),$$

где $x_i \oplus y_i = Z_i (\mathrm{mod} h_i)$, $h_i -$ порядок подгруппы H_{hi}; $x = (x_1, x_2, ..., x_n) \in H$, $x_i = H_i$; $H -$ циклическая неразложимая группа порядка $[H:1] = m_i^{\alpha i} = h_i$ (при $\alpha_i = 1 \to m_i = h_i$).

Рассмотрим общий случай представления групп, когда группа равна прямой сумме подгрупп вида

$$H = H_{h_1} \oplus H_{h_2} \oplus ... \oplus H_{h_n} ,$$

где $[H:1] = \prod_{i=1}^{n} m_i^{\alpha i}$, $h_i -$ порядок подгруппы H_{h_i} для $i = \overline{1,n}$.

Определение 1. Сумма $H_{h_1} \oplus H_{h_2} \oplus ... \oplus H_{h_n}$ называется прямой суммой, если каждое слагаемое имеет нулевое переназначение с суммой остальных, т.е.

$$\left(H_{h_1} + H_{h_2} + ... + H_{h_{i-1}} + H_{h_{i+1}} + ... + H_{h_n}\right) \cap H_{h_n} = 0$$

для $i = \overline{1,n}$.

Определение 2. Примарной циклической группой называется группа вычетов, в общем случае, по модулю m^z, где $m -$ простое число.

Основываясь на известных определениях, покажем справедливость следующего утверждения [1, 3].

Утверждение 1. Всякая конечная абелева группа изоморфна внешней прямой сумме примарных циклических групп.

Правильность утверждения 2 определяется результатами доказательств трех следующих лемм.

Лемма 1. Всякая конечная абелева группа изоморфна прямой сумме циклических подгрупп.

Лемма 2. Всякая циклическая группа изоморфна прямой сумме примарных циклических групп.

Лемма 3. Лемма о транзитивности разложения в прямую сумму.

Пусть $H = H_1 \oplus H_2 \oplus ... \oplus H_n -$ прямая сумма.

Тогда

$H = \left(H_1 \oplus ... \oplus H_{i-1}\right) \oplus \left(H_i \oplus ... \oplus H_n\right)$ для $i = \overline{1,n}$,

и если

$$H = H_1 \oplus ... \oplus H_n;$$

$$H_i = H_{i_1} \oplus ... \oplus H_{i_{k_i}}$$

для $i = \overline{1,n}$, то

$$H = H_{11} \oplus ... \oplus H_{1k_1} \oplus H_{21} \oplus ... \oplus$$
$$\oplus H_{2k_2} \oplus ... \oplus H_{n_1} \oplus ... \oplus H_{nk_n},$$

где $H_{ik_i} -$ подмодули.

Исходя из результата утверждения 2, можно доказать следующее научное положение.

Утверждение 2. В случае, если $M = \prod_{i=1}^{n} m_i$ и $HOD(m_i, m_j) = 1$, а $i \neq j$, кольцо Z_M классов вычетов по модулю M изоморфно прямой сумме

$$GF(m_1) + GF(m_2) + ... + GF(m_i) + ... + GF(m_n)$$

конечных полей Галуа вида $\{GF(m_i)\}$, для $i = \overline{1,n}$.

Данный изоморфизм обусловлен также следствием следующего утверждения.

Утверждение 3. Всякая циклическая группа изоморфна или группе целых чисел по сложению или группе вычетов по некоторому модулю M.

Зададим изоморфизм φ между Z_M и прямой суммой $\sum_{i=1}^{n} GF(m_i)$ конечных полей Галуа в виде

$$\varphi : a \to (a_1, a_2, ...a_n),$$

где $a \in Z_M$, $a_i = a(\mathrm{mod} m_i)$, $i = \overline{1,n}$, причем обратное преобразование представим в виде

$$\varphi^{-1} : (a_1, a_2, ...a_n) \to a.$$

Пусть N делит $m_i - 1$ для $i = \overline{1,n}$. Тогда существует примитивный корень ξ_i из единицы $GF(m_i)$. Элемент $\varphi^{-1} : (\xi_1, \xi_2, ..., \xi_n) \to \xi$ соответствует примитивному корню N-й степени из единицы в Z_M. Отсюда следует, что в N точках существует прямое и обратное преобразование над Z_M, т.е.

$$S(a) = \sum_{n=0}^{N-1} x(n) \xi^{-an} \qquad (1)$$

и

$$x(n) = N^{-1} \sum_{a=0}^{N-1} S(a) \xi^{an}. \qquad (2)$$

Применяя преобразование φ, получим следующие соотношения:

$$\varphi[S(a)] = \sum_{n=0}^{K-1} \varphi[x(n)] \varphi\left[\xi^{-an}\right];$$

$$\varphi[x(n)] = N^{-1} \sum_{a=0}^{N-1} \varphi[S(a)] \varphi\left[\xi^{an}\right],$$

т.е.

$$\left(S_1(a), S_2(a), ..., S_n(a)\right) =$$
$$\left(\sum_{n=0}^{N-1} x_1(n) \xi_1^{-an}, \sum_{a=0}^{N-1} x_2(n) \xi_2^{-an}, ..., \sum_{n=0}^{N-1} x_n(n) \xi_n^{-an}\right);$$

$$\left(x_1(n), x_2(n), ..., x_n(n)\right) =$$
$$\left(N^{-1}\sum_{a=0}^{N-1} S_1(a)\xi_1^{an},\ ...\ , N^{-1}\sum_{a=0}^{N-1} S_2(a)\xi_2^{an},\ ...\right.$$
$$\left. ...\ , N^{-1}\sum_{a=0}^{N-1} S_n(a)\xi_n^{an}\right).$$

Приравнивая одноименные координаты заданных векторов, получим:

$$\delta_1(a) = \sum_{n=0}^{N-1} x_1(n)\xi_1^{-an};$$

$$x_1(n) = N^{-1}\sum_{a=0}^{N-1} S_1(a)\xi_1^{an} \left(\mathrm{mod}\, m_1\right),$$

а также

$$\delta_2(a) = \sum_{n=0}^{N-1} x_2(n)\xi_2^{-an};$$
$$x_2(n) = N^{-1}\sum_{a=0}^{N-1} S_2(a)\xi_2^{an} \left(\mathrm{mod}\, m_2\right); \quad (3)$$

$$\delta_n(a) = \sum_{n=0}^{N-1} x_n(n)\xi_n^{-an};$$
$$x_n(n) = N^{-1}\sum_{a=0}^{N-1} S_n(a)\xi_n^{an} \left(\mathrm{mod}\, m_n\right). \quad (4)$$

Преобразования (3), (4) могут быть реализованы последовательно за n условных тактов либо параллельно во времени за один условный такт. В этом плане очевидны следующие преимущества от организации такого вида вычислений: значительное сокращение времени реализации совокупности (1) – (4) соотношений за счёт возможности совмещения операции вида (1) и (2) с операцией аналого-цифрового преобразования.

Таким образом, возникает задача синтеза СОИ ЦОС адаптивного к $GF(m_1)+GF(m_2)+...+GF(m_n)$-арифметике.

Теоретически возможность создания такого адаптивного СОИ обусловлена следствием следующей теоремы [1].

Утверждение 4. Пусть Z_M – кольцо классов вычетов по модулю $M = m_1^{\alpha_1} m_2^{\alpha_2} ... m_n^{\alpha_n}$ (m_i – простое число; $i = \overline{1,n}$). Тогда Z_M – изоморфно кольцу $Zm_1^{\alpha_1} + Zm_2^{\alpha_2} + ... + Zm_n^{\alpha_n}$. Элементы этого кольца – n-мерные векторы, арифметические операции над которыми осуществляются покомпонентно. Покажем это.

Пусть отображение

$$f : Z_M \to Z_1^{\alpha_1} + Zm_2^{\alpha_2} + ... + Zm_2^{\alpha_n}$$

определено следующим образом:

$$f(a) = a_1\left(\mathrm{mod}\, m_1^{\alpha_1}\right), a_2\left(\mathrm{mod}\, m_2^{\alpha_2}\right), ..., a_n\left(\mathrm{mod}\, m_n^{\alpha_n}\right). \quad (5)$$

Аргумент a последовательно принимает значение от 0 до $M-1$, при этом, аргумент a_1 принимает значение от 0 до $m_1^{\alpha_1}-1$, а аргумент a_2 принимает значение от 0 до $m_2^{\alpha_1}-1$ и т.д. Так как m_i – простые числа, то вектор (5) в диапазоне [0, M) однозначен, следовательно, отображение f есть биекция. Кроме этого, для всех $a,\ b \in Z_M$ выполняется следующее равенство:

$$f(a+b) = \left((a+b)\mathrm{mod}\, m_1^{\alpha_1}, (a+b)\mathrm{mod}\, m_2^{\alpha_2}, ...,\right.$$
$$(a+b)\mathrm{mod}\, m_n^{\alpha_n}\Big) = \Big(a\left(\mathrm{mod}\, m_1^{\alpha_1}\right), a\left(\mathrm{mod}\, m_2^{\alpha_2}\right), ...,$$
$$a\left(\mathrm{mod}\, m_n^{\alpha_n}\right)\Big) + \Big(b\left(\mathrm{mod}\, m_1^{\alpha_1}\right), b\left(\mathrm{mod}\, m_2^{\alpha_2}\right), ...,$$
$$\left.b\left(\mathrm{mod}\, m_n^{\alpha_n}\right)\right) = f(a)f(b).$$

Аналогично можно показать, что

$$f(ab) = f(a)f(b).$$

Следовательно, при синтезе системы обработки информаци на основе новой машинной модулярной $Zm_1^{\alpha_1} + Zm_2^{\alpha_2} + ... + Zm_n^{\alpha_n}$-арифметики можно получить качественно новые научные и практические результаты в плане улучшения основных тактично-технических характеристик систем обработки информации (производительности, отказоустойчивости, надежности, живучесть, достоверности, а также массогабаритных и энергетических характеристик и т.п.) за счет возможности организации принципиально новой структуры СОИ реального времени и применения новых оригинальных методов и алгоритмов обработки информации, а также реализации нестандартных технических решений отдельных блоков и узлов СОИ ЦОС. Для эффективной реализации математических моделей ЦОС посредством

новой $\sum_{i=1}^{n} Zm_i^{\alpha_i}$ -арифметики, определенной над конечными полями и кольцами, необходимо, чтобы посредством СОИ можно было бы эффективно реализовать арифметические операции заданных алгебраических структур. Реализация арифметических операций конечного поля Галуа $GF(M)$ сводится к реализации. модульных операций параллельно над каждым из n конечных полей $GF\left(m_i^{\alpha_1}\right)$, $i=\overline{1,n}$. В этом аспекте известный математический аппарат теории чисел, служащий основой для создания кодов в СОК, будет "адаптивен" (приспособлен) к классу целочисленных задач СОИ реального времени.

Действительно, пусть для $\chi-$ преобразований, определенных над конечным полем или кольцом, необходимо получить нужный порядок первообразного элемента [1, 3]. Для этого необходимо выбрать соответствующее конечное поле или кольцо, т.е. выбрать соответствующее значение модуля M. При этом M должно быть либо простым, либо разлагаться на простые сомножители.

Пусть $M=\prod_{i=1}^{n} m_i, HOD(m_i,m_j)=1$ для $i\neq j$, $\alpha_i=1$, $(i=\overline{1,n})$; тогда вычисления по модулю M, т.е. в поле $GF(M)$, заменяются параллельными вычислениями одновременно по n основаниям (модулям) m_i, т.е. параллельно в n полях Галуа $\sum_{i=1}^{n} GF(m_i)$. В этом случае СОИ должно весьма эффективно реализовать целочисленные модульные операции над $\sum_{i=1}^{n} GF(m_i)$-арифметикой, а это возможно только при применении МА, т.е. СОК.

Цель статьи – провести теоретические исследования возможности использования модулярной арифметики для построения систем обработки дискретной информации, функционирующих в реальном времени. Основная задача, которая ставится в данной статье – это показать тесную связь между принципами построения абстрактных алгебраических систем на основе применения полей Галуа *GF*(*M*) и принципами переработки информации в СОК как для вещественной, так и для гиперкомплексной числовых областей.

Основные материалы исследований

Предварительные исследования показали, что использования кодов МА дает возможность эффективно реализовать математические модели СОИ, определенные над конечными полями или кольцами в вещественной области.

В случае если M – простое число, то набор $\{m_i\}$ оснований СОК должен обеспечить выполнение следующего требования:

$$M \le \prod_{i=1}^{n} m_i .$$

Рассмотрим пример реализации СОИ задач ЦОС, в частности, задачи определения свертки цифровых сигналов $x_1(n'),x_2(n')$ посредством применения преобразований Фурье-Галуа, определенных над прямыми суммами полей Галуа $\sum_{i=1}^{n} GF(m_i)$ на основе использования СОК, заданной набором оснований $\{m_i\}$. В этом случае значения соответствующих сигналов $x_1(n'),x_2(n')$ представляются в виде остатков от последовательного деления их на набор взаимно попарно простых чисел $\{m_i\}$:.

$$x_1(n')=(x_{11}(n')\bmod m_1, x_{12}(n')\bmod m_2,...); \quad (6)$$

$$x_1(n')=(x_{21}(n')\bmod m_1, x_{21}(n')\bmod m_2,...). \quad (7)$$

В соответствии с алгоритмами реализации арифметических операций в СОК соответствующие компоненты $x_{1i}(n')\bmod m_i$ и $x_{2i}(n')\bmod m_i$ векторов (6) и (7) обрабатывается в канале по модулю m_i СОИ независимо от других компонент и параллельно во времени. В этом случае разрядность

$$r_{mi}=\left[\log_2(m_i-1)\right]+1$$

канала обработки информации по основанию m_i системы обработки информации будет меньше разрядности $r_M = [\log_2(M-1)]+1$ СОИ, обрабатывающего информацию в конечном поле Галуа $GF(M)$ по модулю $M = \prod_{i=1}^{n} m_i$.

Очевидно, что совокупность остатков $\{x_{1i}(n') \bmod m_i\}$ по модулю m_i образует конечное поле Галуа $GF(m_i)$, а совокупность остатков по каждому из n полей для $i = \overline{1,n}$ можно отождествить с прямой суммой полей Галуа $\sum_{i=1}^{n} GF(m_i)$.

Результат модульной операции необходимо преобразовать в исходное поле Галуа $GF(M)$, т.е. в позиционную систему счисления. Эта процедура при необходимости (например, в бортовых СОИ БПЛА) может быть эффективно реализована одновременно с процедурой цифро-аналогового преобразования [4]. Отметим, что в большинстве случаев при необходимости процедура преобразования сигнала из позиционной двоичной системы счисления в СОК может быть легко совмещена с операцией аналог-код.

Рассмотренный принцип реализации арифметических операций в поле $GF(M)$, посредством реализации этих операций одновременно в n полях Галуа $GF(m_i)$ для $i = \overline{1,n}$, нетрудно распространить и на гиперкомплексную числовую область, в частности, простое поле Галуа $GF(M)$ может быть расширено до конечного поля комплексных чисел $Z[i]$.

Воспользуемся результатами "китайской" теоремы об остатках для определения χ – преобразований над прямой суммой комплексных полей $GF\left(m_i^{(2)}\right)$ [1, 5].

Утверждение 6. Для любых взаимно простых дивизоров (идеалов) $A_i (i = \overline{1,n})$ и для любых элементов α_i кольца J существует такой элемент $\beta \in J$, что

$$\beta = \alpha_1 (\bmod A_1); \beta = \alpha_2 (\bmod A_2); \ldots, \beta = \alpha_n (\bmod A_n).$$

Пусть Z_M – кольцо классов вычетов по модулю $M = \prod_{i=1}^{n} m_i$ (m_i простое число) и пусть $Z_M[i]$ – конечное поле комплексных чисел по модулю простого числа M, тогда справедливо следующее утверждение.

Утверждение 7. Кольцо, $Z_M[i]$ изоморфно прямой сумме комплексных полей Галуа $\sum_{i=1}^{n} GF\left(m_i^{(2)}\right)$, т.е.

$$Z_M[i] \approx GF\left(m_1^{(2)}\right) + GF\left(m_2^{(2)}\right) + \ldots + GF\left(m_n^{(n)}\right),$$

при условии, если полином x^2+1 является неприводимым над каждым из полей $GF\left(m_i^{(2)}\right)$.

Покажем это [1, 6]. Пусть комплексное число $A = \alpha_1 + i\alpha_2 \in Z_M[i]$.

Определим следующее отображение:

$$f : \alpha_1 + \alpha_2 \to ((\alpha_{11} + \alpha_{21}) \bmod m_1, \ldots, (\alpha_n + \alpha_n) \bmod m_n).$$

Так как полином x^2+1 неприводим над каждым из n показателей $GF\left(m_i^{(2)}\right)$, то произвольный остаток $(\alpha_{1j} + i\alpha_{2j}) \bmod m_j$ принадлежит полю $GF\left(m_i^{(2)}\right)$ для всех $j = \overline{1,n}$. Таким образом, f является отображением кольца $Z_M[i]$ в прямую сумму полей $GF\left(m_i^{(2)}\right)$, т.е.

$$f : Z_M[i] \to GF\left(m_1^{(2)}\right) + GF\left(m_2^{(2)}\right) + \ldots + GF\left(m_n^{(2)}\right).$$

Пусть $A = \alpha_1 + i\alpha_2$, $B = \beta_1 + i\beta_2 \in Z_M[i]$, тогда:

$$\begin{aligned} f(A+B) &= f((\alpha_1+\beta_1) + i(\alpha_2+\beta_2)) = \\ &= ([(\alpha_1+\beta_1) + i(\alpha_2+\beta_2)]) \bmod m_1, \ldots \\ &[(\alpha_1+\beta_1) + i(\alpha_2+\beta_2)] \bmod m_2, \ldots, \\ &[(\alpha_1+\beta_1) + i(\alpha_2+\beta_2)] \bmod m_1, \ldots, \\ &[(\alpha_1+\beta_1) + i(\alpha_2+\beta_2)] \bmod m_n) = \\ &= ((\alpha_1 + i\alpha_2) \bmod m_1 + (\beta_1 + i\beta_2) \bmod m_1); \end{aligned}$$

$$(\alpha_1 + i\alpha_2)\bmod m_2 + (\beta_1 + i\beta_2)\bmod m_2),...$$
$$(\alpha_1 + i\alpha_2)\bmod m_i + (\beta_1 + i\beta_2)\bmod m_i),...$$
$$(\alpha_1 + i\alpha_2)\bmod m_n + (\beta_1 + i\beta_2)\bmod m_n) =$$
$$= [((\alpha_1 + i\alpha_2)\bmod m_1 + (\alpha_1 + i\alpha_2)\bmod m_2,...,$$
$$...,(\alpha_1 + i\alpha_2)\bmod m_i,...,$$
$$..,(\alpha_1 + i\alpha_2)\bmod m_n + (\beta_1 + i\beta_2)\bmod m_1,$$
$$(\beta_1 + i\beta_2)\bmod m_2,...,(\beta_1 + i\beta_2)\bmod m_i,...,$$
$$...,(\beta_1 + i\beta_2)\bmod m_n)] = f(A) + f(B).$$

Нетрудно показать, что $f(AB) = f(A)\cdot f(B)$, т.е. заданное отображение f является гомоморфным. В [1, 7] показано, что если ограничить отображение f только на одну из частей (реальную или мнимую) комплексного числа, то оно перейдет в изоморфизм, связывающий класс вычетов Z_M и прямую сумму

$$GF(m_1) + GF(m_2) + \ldots + GF(m_i) + \ldots + GF(m_n).$$

Данный факт свидетельствует о том, что отображение f является изоморфизмом.

Вышеизложенное подтверждает вывод об эффективности применения модулярной $\sum_{i=1}^{n} GF(m_i)$ – арифметики (использования в качестве системы счисления СОИ системы остаточных классов) для реализации ММ ЦОС в комплексной области [8].

По аналогии с χ – преобразованиями [1], определенными над конечным полем комплексных чисел, определяются преобразования над алгебраическими структурами более высоких порядков (гиперкомплексные числовые системы), в частности, над конечным кольцом кватернионов $Z_M^{(K)}$. Преимущества такого подхода состоят, в первую очередь, в отсутствии шума округления и в сохранении ассоциативного и коммутативного законов при выполнении модульных операций, что позволяет весьма действенно использовать математический аппарат МА.

Данное обстоятельство обеспечивает возможность эффективной реализации СОИ в СОК ММ ЦОС в алгебраической числовой структуре заданного порядка.

Построение ММ ЦОС, определенных над конечными полями и кольцами произвольной размерности, является новым, но весьма перспективным направлением в теории обработки цифровых сигналов. Однако без средств эффективной реализации таких ММ ЦОС не удается полностью использовать преимущества такого подхода.

Принципиально реализация ММ ЦОС может быть осуществлена на современных СОИ, функционирующих в ПСС. Однако такая реализация моделей не будет соответствовать степени эффективности использования нового подхода к построению моделей ЦОС на основе использования конечных алгебраических структур, так как вычислительные средства ПСС, в общем случае, не адаптивны к классу задач ЦОС (трудность реализации арифметических операций в конечных полях и кольцах, необходимость использования больших разрядных сеток и прочее, снижает технико-экономические показатели СОИ).

Требования реализации арифметических операций в конечных полях Галуа *GF*(*M*), в конечных полях целых комплексных чисел $Z_M^{(C)}$, а также в конечных кольцах различных структур (например, $Z_M, Z_M^{(C)}$ и т.п.) сводятся к возможности эффективной реализации модульных арифметических операций. Вследствие этого очевидно, что основой операционного устройства (ОУ) СОИ в СОК будет являться канал обработки информации по модулю m_i, а ОУ будет представлять собой совокупность из *n* каналов обработки информации по соответствующим модулям $\{m_i\}$, для $i = \overline{1,n}$, реализующее алгоритмы цифровой обработки сигналов посредством модулярной $GF(m_i) + GF(m_2) + ... + GF(m_n)$ -арифметики. При этом структура СОИ полностью соответствует принципу образования СОК, т.е. структура как ОУ, так и СОИ, будет реализована, исходя из

основных свойств системы остаточных классов [9 – 11]. Этим и определяется высокая степень адаптации структуры СОИ в СОК к классу решаемых задач реализации ММ цифровой обработки сигналов.

Кроме этого СОК присущи особенности, выявленные для рассматриваемых математических моделей систем цифровой обработки сигналов: кодирование элементов рассмотренных алгебраических структур (вычетов по произвольному модулю m_i СОК) осуществляется в целых неотрицательных числах (0, 1, 2, …, $m_i - 1$), а также отсутствие привычного физического смысла результатов вычислений в конечных полях и кольцах (невозможность оценки величины операнда в СОК по его аналитическому представлению). Данное обстоятельство еще раз подчеркивает адаптивность математического аппарата СОК к классу задач (типу операций) систем цифровой обработки сигналов.

Выводы

Таким образом, использование свойств модулярной арифметики (непозиционной системы в остаточных классах) позволяет синтезировать систему обработки информации, удовлетворяющую основным требованиям по эффективной реализации систем ЦОС, определенных в конечных полях и кольцах. Высокая адаптивность структуры СОИ в СОК к моделям систем ЦОС позволит получить качественно новые результаты, имеющие важное теоретическое и практическое значение для решения проблемы создания цифровых аппаратных средств реализации ММ.

Литература

1. Абстрактные алгебраические системы и цифровая обработка сигналов / Л.В. Вариченко, В.Г. Лабунец, М.А. Раков. – К.: Наук. думка, 1986. – 248 с.

2. Маклеллан Дж., Рейдер Ч.М. Применение теории чисел в цифровой обработке сигналов. – М.: Радио и связь, 1983. – 264 с.

3. Скорняков Л.А. Элементы алгебры. – М.: Наука, 1981. – 175 с.

4. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Сов. радио, 1968. – 440 с.

5. Виноградов И.М. Основы теории чисел. – М.: Наука, 1981. – 175 с.

6. Акушский И.Я., Амербаев В.М., Пак И.Т. Основы машинной арифметики комплексных чисел. – Алма-Ата: Наука, 1970. – 248 с.

7. Кантор И.Л., Солодовников А.С. Гиперкомплексные числа. – М.: Наука, 1973. – 144 с.

8. А.с. 1166098 СССР. Устройство для умножения в системе остаточных классов / В.А. Краснобаев – Бюл. изобретений,1985. – № 25.

9. Жихарев В.Я., Илюшко Я.В., Краснобаев В.А. Влияние системы счисления на надежность ЭВМ // Радіоелектронні і комп'ютерні системи. – Х.: НАУ „ХАІ". – 2004. – № 1 (5). – С. 98 – 104.

10. Краснобаєв В.А., Ілюшко Я.В. Метод та обчислювальна система обробки інформації, що представлена у системі залишкових класів // Системи обробки інформації. – Х.: НАНУ ПАНМ, ХВУ. – 2004. – Вип. 7 (35). – С. 106 – 111.

11. Краснобаев В.А., Илюшко Я.В. Методы обработки информации в системе остаточных классов // Радіоелектронні і комп'ютерні системи. – Х.: НАУ „ХАІ". – 2004. – № 2 (6). – С. 101 – 109.

Поступила в редакцию 21.03.05

Рецензент: д-р техн. наук, проф. И.А. Фурман, Харьковский национальный технический университет сельского хозяйства, Харьков.