

Информатика, вычислительная техника и управление

УДК 004.315

DOI: 10.30987/article_5c8b5ceb59c001.39557524

А.А. Кожевников

СИНТЕЗ ТОНАЛЬНЫХ УСТРОЙСТВ ДЛЯ УМНОЖЕНИЯ ПО МОДУЛЮ

Приведен анализ арифметических устройств, осуществляющих операции над дискретными состояниями фаз синусоидального тока. Рассмотрена реализация ряда алгоритмов умножения в системе

остаточных классов на основе таких вычислительных структур.

Ключевые слова: арифметические устройства, система остаточных классов, СОК.

А.А. Kozhevnikov

ТОНЕ DEVICE SYNTHESIS FOR MODULE MULTIPLICATION

The application of the systems of residual classes (SRC) allows carrying out arithmetic operations of addition and multiplication more efficiently which are basic in DSP at the expense of small digit capacity of deductions. An additional growth of an operating speed gives a transition from a digital processing to a tone one, that is, to number encoding in the SRC by discrete phases of tone signals of one frequency. The application of an instrumentation framework on the superconductor basis shows an outlook of the special processor formation on the basis of principles marked earlier with the productivity of a subtherahertz order. If a mathematical expression for a signal processing is rigidly specified and contains a constant k which does not need to vary, then in the special processor structure a tone multiplication of a number by a constant through

a module may be carried out as a serial addition of an operand with itself. If a special processor work needs sometimes a program reconstruction of system constant parameters, then it is possible to carry out on the basis of other multiplication device by a constant. A tone multiplication of two numbers by a module is formed through a simplest algorithm consisting in a serial addition through a module of the first operand with itself and a choice of the result required through the second operand. The multiplication fulfillment through a module in a tone form in different versions is possible that enables unique possibilities of signal processing on the basis of the well-known DSP methods with an operation speed which is a record for these algorithms.

Key words: arithmetic devices, system of residual classes, SRC.

Введение

Развитие измерительной техники до уровня работы с сигналами порядка 100 ГГц [1] требует соответствующих возможностей от спецпроцессоров, позволяющих удешевить и уменьшить габариты конечного продукта за счет применения обработки информации вычислительными методами. Широкое использование цифровой электроники в аналогичных системах здесь же наталкивается на специфику рассматриваемой области измеряемых частот, естественно связанной с быстродействием. Выходом может стать активное внедрение системы остаточных классов (СОК) [2], позволяющей за счет малоразрядности вычетов более эффективно осуществлять арифметические операции сложения и умножения, которые являются основными в ЦОС [3]. Дополнительный рост быстро-

действия дает переход от цифровой обработки к тональной [4], т.е. кодированию чисел в СОК дискретными фазами гармонических сигналов одной частоты. Применение приборной базы на основе сверхпроводников [5] проявляет перспективу построения спецпроцессоров на основе обозначенных ранее принципов с производительностью субтерагерцового порядка. Проецирование наработанных алгоритмов ЦОС в СОК на структуры с дискретно-фазированным представлением чисел требует в первую очередь проработки вопросов функционирования устройств для сложения (вычитания) и умножения по модулю. Если первое достаточно просто и рассмотрено ранее [4], то второе несколько сложнее и является предметом данного исследования.

Основные алгоритмы цифровых устройств

Прежде чем перейти к тональным вычислительным операциям, рассмотрим цифровые алгоритмы. Как и сложение, умножение в СОК выполняется в параллельных трактах по соответствующим модулям без перекрестного обмена информацией между ними [2]. Реализация вычислений в кольце вычетов с гораздо меньшей по сравнению с позиционными числами разрядностью порождает более эффективные алгоритмы как в быстродействии, так и объеме оборудования. В качестве аппаратной основы могут использоваться несколько различных устройств: двоичные позиционные сумматоры, унитарные таблицы и кольцевые сдвиговые регистры [6; 7].

Самый простой вариант бинарных вычислений сводится к преобразованию операндов в унарный код, с дальнейшей выборкой правильного ответа на пересечении выбранных сигнальных линий через логический элемент И, с последующей дешифровкой результата. В силу коммутативности модулярных операций возможно сокращение аппаратных затрат [8].

Другие подходы основаны на идее максимально свести умножение к промежуточному сложению и вычитанию. В первую очередь таковым является метод,

получаемый из квадратов суммы и разности:

$$a \cdot b = \frac{1}{4} [(a + b)^2 - (a - b)^2].$$

Особенности данного алгоритма - необходимость возведения в квадрат и деление на четыре в СОК - приводят к повышенным аппаратным затратам, но в ряде случаев такой подход видится наиболее приемлемым.

Одним из столпов модулярной арифметики является теория индексов [2], представляющая из себя некоторый аналог логарифмических вычислений. Здесь каждому вычету γ по модулю m в заданной СОК ставится в соответствие уникальный индекс $\text{ind } \gamma$. При выполнении операции умножения сначала определяются индексы для каждого из операндов, затем производится их сложение, после чего происходит обратное преобразование через нахождение антииндекса.

Даже краткий обзор подходов к бинарному умножению на основе цифровых устройств показывает широкий выбор инструментов для решения аналогичной задачи в тональной форме. Тем не менее оперирование аналоговым сигналом имеет свои преимущества и недостатки, раскрыть которые в полной мере применительно к рассмотренным алгоритмам в рамках одной статьи невозможно.

Тональное умножение числа по модулю на константу

Если математическое выражение для обработки сигнала жестко задано и содержит константу k , которая не требует изменения, то в структуре спецпроцессора соответствующая операция может быть отображена в виде последовательного сложения операнда с самим собой (рис. 1а) [9].

На синхронизирующий вход поступает сигнал $S_0 = \sin(\omega t)$, а на информационные гармоника $S_i = \sin(\omega t + 2\pi \cdot \gamma_i / m)$, где $i = \overline{1, k}$, $\gamma_i \in [0, m - 1]$, m - модуль СОК. Процесс сложения двух вычетов γ как результат манипуляции с дискретными значениями фаз (СФ) изложен в [4]. Последовательная работа блоков СФ приводит к формирова-

нию на выходе устройства итоговой гармоники $S_{\text{рез}} = \sin[\omega t + 2\pi \cdot \sum_{i=1}^k \gamma_i / m]$.

Для операции умножения на константу данное выражение принимает вид $S_{\text{рез}} = \sin[\omega t + 2\pi \cdot k \cdot \gamma / m]$.

Если работа спецпроцессора иногда требует программной перестройки постоянных параметров системы, то это возможно осуществить на основе другого устройства умножения на константу (рис. 1б) [10]. Рассмотрим операцию умножения двух чисел $\Gamma = A \times B$, где B представлено в виде полинома: $B = \beta_k \cdot 2^{g-1} + \dots + \beta_2 \cdot 2^1 + \beta_1$. Здесь g - максимальное количество двоичных разрядов $\beta_j \in [0; 1]$ ($j = \overline{1, g}$), применяемое

для реализации константы В. Если целый остаток числа А по модулю m есть α_m , а

результат умножения по модулю m - это γ_m , то

$$\gamma_m = \alpha_m \cdot \sum_{j=1}^g (\beta_j \cdot 2^{j-1}) \bmod m.$$

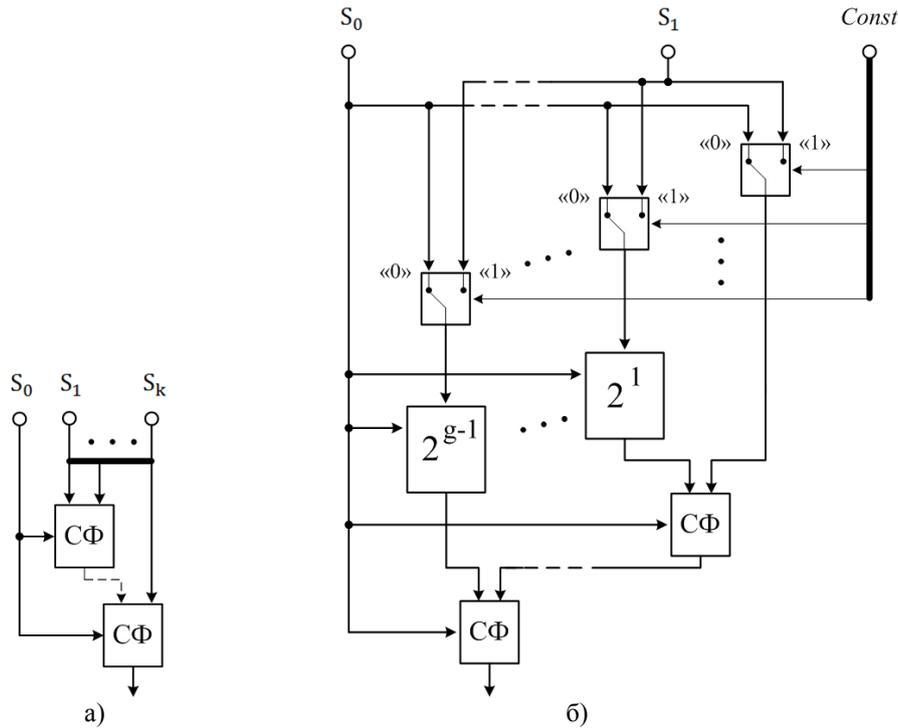


Рис. 1. Устройство умножения на константу: а - на основе последовательного сложения двух операндов; б - на основе умножения на два

Для реализации алгоритма вычислений на дискретных блоках полученное выражение примет следующий вид:

$$\gamma_m = (\alpha_m \cdot \beta_k \cdot 2^{k-1} \bmod m + \dots + \alpha_m \cdot \beta_2 \cdot 2^1 \bmod m + \alpha_m \cdot \beta_1 \bmod m) \bmod m$$

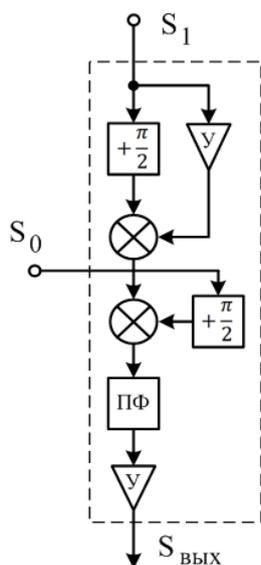


Рис. 2. Арифметический вентиль умножения на два

На синхронизирующий вход поступает сигнал $S_0 = \sin(\omega t)$, на информационный - гармоника $S_1 = \sin(\omega t + \alpha_m \cdot 2\pi/m)$, а константа представлена двоичным кодом, который замыкает соответствующие ключи, пропуская дальше S_0 или S_1 . Для умножения вычета α_m на два в дискретно-фазированной форме используется вентиль (рис. 2). Гармоника S_1 увеличивает фазу на $\pi/2$, а в параллельной линии - амплитуду в два раза, после чего оба сигнала поступают на входы первого смесителя, где реализуется известное тригонометрическое выражение:

$$\sin(2 \cdot \varphi) = 2 \cdot \sin(\varphi) \cdot \cos(\varphi).$$

Полученная промежуточная гармоника удвоенной частоты $S_{пр} = \sin[2\omega t + 2\alpha_m \cdot 2\pi/m]$ перемножается на втором смесителе с синхронизирующей гармоникой S_0 , фаза которой увеличена на $\pi/2$ (т.е. $S_0 = \cos[\omega t]$). При этом, согласно тригонометрическому выражению

$\sin(\varphi_1) \cdot \cos(\varphi_2) = \frac{1}{2} [\sin(\varphi_1 - \varphi_2) + \sin(\varphi_1 + \varphi_2)]$,
 после полосовой фильтрации более низкочастотной составляющей и усиления формируется результат в виде гармоники с единичной амплитудой и искомой результирующей фазой

Тональное умножение двух чисел по модулю

Данная арифметическая операция формируется простейшим алгоритмом, заключающимся в последовательном сложении по модулю первого операнда с самим собой и выборе нужного результата через второй операнд (рис. 3).

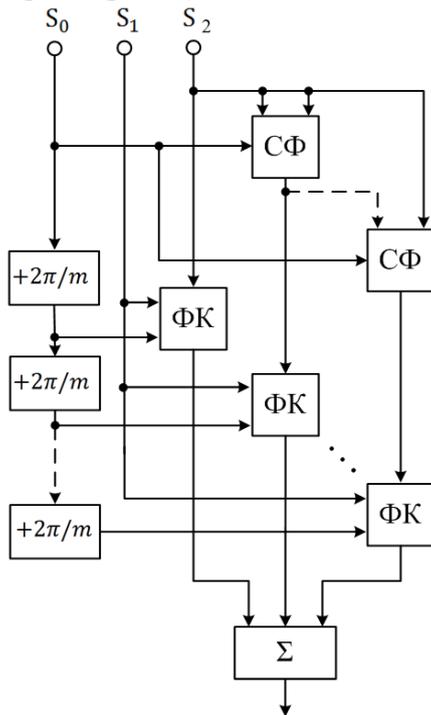


Рис. 3. Тональное умножение двух операндов по модулю

Работа начинается с подачи на входы устройства гармоник одной частоты:

- синхронизирующий: $S_0 = \sin(\omega t)$;
- первый операнд:
 $S_1 = \sin(\omega t + 2\pi \cdot \gamma_a / m)$;

$$(\gamma_a \cdot \gamma_b) \bmod m = \left[\left(\frac{\gamma_a + \gamma_b}{2} \right)^2 \bmod m - \left(\frac{\gamma_a - \gamma_b}{2} \right)^2 \bmod m \right] \bmod m.$$

Вычисления в рамках данного выражения удобно осуществлять в двоичном коде без ограничения на разрядность результатов промежуточных операций. Поскольку в дискретно-фазированной форме адекватно только модулярное представление, то результат суммы и разности [4] в некоторых случаях вызовет появление

$$S_{\text{ВЫХ}} = \sin[\omega t + 2\alpha_m \cdot 2\pi/m].$$

Требуемая степень двойки набирается последовательным умножением на два необходимое количество раз. Последнее действие сложения всех разрядов происходит попарно на блоках СФ.

- второй операнд:

$$S_2 = \sin(\omega t + 2\pi \cdot \gamma_b / m),$$

где γ_a и γ_b - вычеты по модулю m , над которыми осуществляется операция умножения. Второй операнд претерпевает $m-1$ операций сложения по модулю, в результате чего на выходах блоков СФ формируются сигналы:

$$S_{\text{СФ.1}} = \sin(\omega t + 2\pi \cdot 2 \cdot \gamma_b / m);$$

$$S_{\text{СФ.2}} = \sin(\omega t + 2\pi \cdot 3 \cdot \gamma_b / m);$$

...

$$S_{\text{СФ.m-1}} = \sin(\omega t).$$

Гармоники с выходов фазовращателей на фиксированное значение $2\pi/m$ сравниваются фазированными ключами (ФК) [11] со значением первого операнда. Если наблюдается равенство, то на один из входов результирующего сумматора мощности проходит сигнал от соответствующего блока СФ или значение второго операнда (если $\gamma_a = 1$). Складываясь с нулевыми уровнями от других ключей, на выходе устройства формируется результат:

$$S_{\Sigma} = \sin[\omega t + 2\pi \cdot (\gamma_a \cdot \gamma_b) \bmod m / m].$$

Существуют и другие подходы к реализации искомой арифметической операции. Как известно, квадраты суммы и разности, при вычитании второго из первого, позволяют представить умножение двух чисел по модулю в виде

ошибки. Рассмотрим пример. Пусть $m=7$, $\gamma_a=3$ и $\gamma_b=5$, тогда

$$(\gamma_a + \gamma_b) \bmod m = (3 + 5) \bmod 7 = 1;$$

$$\left(\frac{\gamma_a + \gamma_b}{2} \right)^2 \bmod m = 0.25;$$

$$(\gamma_a - \gamma_b) \bmod m = (3 - 5) \bmod 7 = 5;$$

$$\left(\frac{\gamma_a - \gamma_b}{2}\right)^2 \bmod m = 4.25.$$

Итого:

$$(0.25 - 4.25) \bmod 7 = 3, \text{ при этом}$$

$$(\gamma_a \cdot \gamma_b) \bmod m = (3 \cdot 5) \bmod 7 = 1.$$

Ошибка.

Если не ограничивать сумму и разность величинами, не превышающими значения $m-1$, то будет наблюдаться следующий результат:

$$\gamma_a + \gamma_b = 3 + 5 = 8;$$

$$\left(\frac{\gamma_a + \gamma_b}{2}\right)^2 \bmod m = (16) \bmod 7 = 2;$$

$$\gamma_a - \gamma_b = 3 - 5 = -2;$$

$$\left(\frac{\gamma_a - \gamma_b}{2}\right)^2 \bmod m = (1) \bmod 7 = 1.$$

Заключение

Осуществление операции умножения по модулю в тональной форме в различных вариантах возможно, что открывает уникальные возможности обработки сиг-

Итого: $(2 - 1) \bmod 7 = 1$, при этом

$$(\gamma_a \cdot \gamma_b) \bmod m = (3 \cdot 5) \bmod 7 = 1.$$

Верно.

Следовательно, рассмотренный алгоритм, по крайней мере в представленной форме, не годится для реализации на основе дискретно-фазированного представления чисел.

Теория синтеза аппаратных средств в системе остаточных классов знает примеры эффективного сопряжения ряда арифметических операций в составе единого универсального устройства. Образец тонального табличного вычислителя подробно рассмотрен в [12].

налов на основе известных методов ЦОС с рекордным для данных алгоритмов быстродействием.

СПИСОК ЛИТЕРАТУРЫ

1. Дьяконов, В. Sensation 2015: Teledyne LeCroy освоила выпуск первого в мире 100-ГГц осциллографа реального времени! / В. Дьяконов // Компоненты и технологии. – 2015. – № 3. – С. 16-22.
2. Акушский, И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М.: Сов. радио, 1968. – 440 с.
3. Галанина, Н.А. Анализ эффективности синтеза устройств вычислительной техники для непозиционной цифровой обработки сигналов / Н.А. Галанина, Н.Н. Иванова // Кибернетика и программирование. – 2015. – № 3. – С. 1-6.
4. Кожевников, А.А. Арифметические вентили модулярных спецпроцессоров / А.А. Кожевников // Приборы и системы. Управление, контроль, диагностика. – 2018. – № 2. – С. 46-51.
5. Шитов, С.В. Малошумящий СИС смеситель на частоту 1 ТГц с двойной дипольной антенной / С.В. Шитов [и др.] // ЖТФ. – 2002. – № 9. – С. 87-92.
6. Ирхин, В.П. Табличная реализация цифровых фильтров в модулярной арифметике / В.П. Ирхин, Л.А. Овчаренко // Информационные технологии. – 2005. – № 10. – С. 13-20.
7. Мельник, В.А. Информационная избыточность в узлах непозиционного спецвычислителя для телекоммуникационных устройств / В.А. Мельник, Р.В. Кузьменко, В.П. Ирхин // Вестник Воронежского института МВД России. – 2015. – № 2. – С. 149-155.
8. Ирхин, В.П. Расширение функциональных возможностей вычислителей в телекоммуникационных устройствах / В.П. Ирхин, В.А. Мельник, Д.С. Шведов // Вестник Воронежского института ФСИН России. – 2016. – № 1. – С. 21-26.
9. Пат. 2653312 РФ, МПК (2006.01) G06F 7/72. Устройство для сложения k чисел по модулю m / А.А. Кожевников [и др.]. – Заявл. 24.05.17; опубл. 07.05.18.
10. Пат. 2653310 РФ, МПК (2006.01) G06F 7/72. Устройство для умножения числа по модулю на константу / А.А. Кожевников [и др.]. – Заявл. 24.05.17; опубл. 07.05.18.
11. Пат. 2659866 РФ, МПК (2006.01) G01R 25/00, G01R 29/02, H03K 17/00. Фазированный ключ по модулю m / А.А. Кожевников [и др.]. – Заявл. 24.05.17; опубл. 04.07.18.
12. Пат. 2656992 РФ, МПК (2006.01) G06F 7/72. Арифметическое устройство по модулю m / А.А. Кожевников [и др.]. – Заявл. 24.05.17; опубл. 07.06.18.
1. Diyakonov, V. Sensation 2015: Teledyne LeCroy mastered manufacturing online oscilloscope – world first! / V. Diyakonov // *Components and Technologies*. – 2015. – No.3. – pp. 16-22.

2. Akushsky, I.Ya. Machine arithmetic in residual classes / I.Ya. Akushsky, D.I. Yuditsky. – M.: *Sov. Radio*, 1968. – pp. 440.
3. Galanina, N.A. Efficiency analysis of computer engineering synthesis for non-positional digital processing of signals / N.A. Galanina, N.N. Ivanova // *Cybernetics and Programming*. – 2015. – No.3. – pp. 1-6.
4. Kozhevnikov, A.A. Arithmetic valves of modular special processors / A.A. Kozhevnikov // *Devices and Systems. Management, Control, Diagnostics*. – 2018. – No.2. – pp. 46-51.
5. Shitov, S.V. Noise-reduced SIS mixer for frequency 1THZ with double dipolar antenna / S.V. Shitov [et al.] // *ZhTF*. – 2002. – No.9. – pp. 87-92.
6. Irkhin, V.P. Tabular realization of digital filters in modular arithmetic // V.P. Irkhin, L.A. Ovcharenko // *Information Technologies*. – 2005. – No.10. – pp. 13-20.
7. Melnik, V.A. Information redundancy in units of non-positional special calculator for telecommunication devices / V.A. Melnik, R.V. Kuzmenko, V.P. Irkhin // *Bulletin of Voronezh Institute of Russian MIA*. – 2015. – No.2. – pp. 149-155.
8. Irkhin, V.P. Calculator functional potentiality expansion on telecommunication devices / V.P. Irkhin, V.A. Melnik, D.S. Shvedov // *Bulletin of Voronezh Institute of Federal Penitentiary Service of Russia*. – 2016. – No.1. – pp. 21-26.
9. Pat. 2653312 RF, IPC (2006.01) G06F 7/72. Device for k Numbers Addition through m Module / A.A. Kozhevnikov [et al.]. – appl. 24.05.17; pub. 07.05.18.
10. Pat. 2653310 RF, IPC (2006.01) G06F 7/72. Device for Number Multiplication by Constant through Module / A.A. Kozhevnikov [et al.]. – appl. 24.05.17; pub. 07.05.18.
11. Pat. 2659866 RF, IPC (2006.01) G01R 25/00, G01R 29/02, H03K 17/00. Phased Key through m Module / A.A. Kozhevnikov [et al.]. – appl. 24.05.17; pub. 04.07.18.
12. Pat. 2656992 RF, IPC (2006.01) G06F 7/72. Arithmetic Device through m Module / A.A. Kozhevnikov [et al.]. appl. 24.05.17; pub. 07.06.18.

Статья поступила в редакцию 15.01.18.

*Рецензент: д.т.н., доцент Воронежского института ФСИИ России
Ирхин В.П.*

Статья принята к публикации 25.12.18.

Сведения об авторах:

Кожевников Алексей Александрович, к.физ.-мат.н., доцент кафедры социально-гуманитарных, естественно-научных и общепрофессиональных

Kozhevnikov Alexey Alexandrovich, Can. Phys-Math., Assistant Prof. of the Dep. of Social-Humanities, Natural and General Professional Subjects,

дисциплин филиала Ростовского государственного университета путей сообщения в г. Воронеже, тел. 8-909-211-0674, e-mail: akozhev@yandex.ru.

Voronezh Branch of Rostov State University of Communications in Voronezh, e-mail: akozhev@yandex.ru.