ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ТЕХНОЛОГИЙ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ И СИГНАЛОВ

УДК 004.9, 004.94, 004.56

МЕТОД ДЕЛЕНИЯ НА ДВОИЧНУЮ ЭКСПОНЕНТУ ДЛЯ ПРЕОБРАЗОВАНИЯ МИНИМАЛЬНО ИЗБЫТОЧНОГО МОДУЛЯРНОГО КОДА В ПОЗИЦИОННЫЙ КОД

Коляда А.А., Кучинский П.В., Червяков Н.И., Чернявский А.Ф., Шабинская Е.В.

Статья посвящена проблематике оптимизации процедур модулярно-позиционного преобразования, основу которых составляет метод деления на двоичную экспоненту. Осуществляемая оптимизация обеспечивает минимизацию суммарных временных затрат при допустимом объеме памяти для таблиц. Это достигается за счет применения минимально избыточного модулярного кодирования, систем счисления с основаниями большой разрядности, а также таблично-сумматорной вычислительной технологии.

Ключевые слова: модулярная система счисления, минимально избыточный модулярный код, позиционный код, кодовое преобразование, деление на двоичную экспоненту.

Введение

В настоящее время арифметика модулярных систем счисления (МСС) – модулярная арифметика (МА) активно применяется в цифровой обработке сигналов, обработке изображений, в спутниковых, сотовых инфокоммуникационных системах, беспроводных сенсорных сетях, множественном доступе с кодовым разделением каналов, облачных вычислениях, в средствах обнаружения и исправления ошибок, контроля отказов и сбойных ситуаций, криптосистемах, других приложениях. Это обусловлено тем, что кодовый параллелилизм модулярных вычислительных структур (МВС) обеспечивает им ряд существенных преимуществ над позиционными структурами. Практическая реализация данных преимуществ в максимальной мере составляет определяющую стратегию всех проводимых разработок по МВС.

Чаще всего модулярные средства обработки информации используются совместно с позиционными. Поэтому эффективность МА-приложений в значительной степени зависит от характеристик сложности и быстродействия применяемых методов и алгоритмов сопряжения разнотипных (по кодовой организации) компонент вычислительных систем, то есть средств позиционно-модулярного интерфейса гибридных систем рассматриваемого класса. Представляемые в настоящей статье исследования относятся к проблематике оптимизации процедур образования кода МСС в позиционный код (ПК). Для решения проставленной задачи применен принцип минимально избыточного модулярного кодирования [1]. Ключевой отличительной особенностью минимально избыточных МСС (МИМСС) является использование так называемых интервально-индексных интегральных характеристик модулярного кода (МК), которые отличаются от известных характеристик – ранга, цифр полиадического кода и других [2-5] предельной простотой базовых расчетных соотношений. Фундаментальные преимущества интервально-индексной технологии синтеза алгоритмов модулярно-позиционного кодового преобразования далее наглядно демонстрируются на примере метода деления на двоичные экспоненты. Особое внимание при этом уделяется оптимизационным аспектам, охватывающим приложения МА на диапазонах больших чисел, и прежде всего криптографические МА-приложения [6-12].

Принцип минимально избыточного модулярного кодирования

Введем обозначения:

- $\lfloor a \rfloor$ и $\lceil a \rceil$ – наибольшее и наименьшее целые числа (ЦЧ) соответственно не большее и не меньшее вещественной величины a;

- $\mathbf{Z}_m = \{0;1 \ldots m-1\}$, $\mathbf{Z}_m^{-} = \{-\lfloor m/2 \rfloor; -\lfloor m/2 \rfloor+1; \ldots \lceil m/2 \rceil-1\}$ – множества вычетов по натуральному модулю m;

- $|A|m$ – элемент кольца $\mathbf{Z}_m$, сравнимый с A (в общем случае рациональным числом) по модулю m;

- $\mathbf{M} = \{m_1; m_2 \ldots m_k\}$ – базис МСС, состоящий из k>1 попарно простых модулей $m_1; m_2 \ldots m_k$.

В МСС с базисом **M** ЦЧ X представляется кодом $(\chi_1;\chi_2 \ldots \chi_k)(\chi_i = |X|_{m_i};\ i = 1,k)$. Максимальная мощность множества $\mathbf{D}_{\text{МСС}}$ чисел X, на

котором отображение $X \to (\chi_1, \chi_2, ..., \chi_k)$ взаимно однозначно составляет $M_k = \prod_{i=1}^{k} m_i$ элементов. В этом случае $\mathbf{D}_{\text{МСС}}$ выполняет роль диапазона МСС. Обычно в качестве диапазона используют $\mathbf{Z}_{M_k}$ или $\mathbf{Z}^{-}_{M_k}$.

Из Китайской теоремы об остатках следует, что ЦЧ $X \in \mathbf{D}_{\text{МСС}}$ может быть получено по своему МК $(\chi_1, \chi_2, ..., \chi_k)$ с помощью равенства

$$X = \sum_{i=1}^{k-1} M_{i,k-1} \left| M^{-1}_{i,k-1} \chi_i \right|_{m_i} + M_{k-1} I(X); \quad (1)$$

где $M_{i,k-1} = M_{k-1} / m_i$; $M_{k-1} = \prod_{j=1}^{k-1} m_j$;

$I(X) = I_k(X)$ – интервальный индекс (ИИ) числа X [1]. Выражение (1) называется интервально-модулярной формой (ИМФ) ЦЧ X.

При $|\mathbf{D}_{\text{МСС}}| = M_k$ МСС с базисом $\mathbf{M}$ является неизбыточной. Между тем использование в системах счисления кодовой избыточности, как правило, позволяет существенно улучшить их арифметические и иные свойства [1; 7-9]. Так называемое минимально избыточное модулярное кодирование: $\mathbf{D}_{\text{МИМСС}} \to \mathbf{Z}_{m_1} \times \mathbf{Z}_{m_2} \times ... \times \mathbf{Z}_{m_k}$ предусматривает применение диапазона $\mathbf{D}_{\text{МИМСС}}$, мощность которого меньше мощности диапазона $\mathbf{D}_{\text{МСС}}$ неизбыточной (классической) МСС с базисом $\mathbf{M}$. Сущность реализуемого принципа раскрывает нижеследующее утверждение.

Теорема 1. О минимальной избыточном модулярном кодировании. Для того, чтобы в МСС с попарно простыми основаниями $m_1; m_2 \ldots m_k$ ИИ $I(X) = I_k(X)$ каждого элемента $X = (\chi_1, \chi_2, ..., \chi_k)$ диапазона $\mathbf{Z}^{-}_{2M} = \{-M, -M+1 \ ... \ M-1\}$, где $M = m_0 M_{k-1}$; m_0 – вспомогательный модуль, полностью определялся компьютерным ИИ – вычетом $\hat{I}_k(X) = |I(X)|_{m_k}$, необходимо и достаточно, чтобы k-ое основание удовлетворяло условию: $m_k \geq 2m_0 + k - 2$ $(m_0 \geq k - 2)$. При этом для $I(X)$ верны расчетные соотношения:

$$I(X) = \begin{cases} \hat{I}_k(X), & \text{если } \hat{I}_k(X) < m_0; \\ \hat{I}_k(X) - m_k, & \text{если } \hat{I}_k(X) \geq m_0; \end{cases} \quad (2)$$

$$\hat{I}(X) = \hat{I}_k(X) = \left| \sum_{i=1}^{k} R_{i,k}(\chi_i) \right|_{m_k}; \quad (3)$$

$$R_{i,k}(\chi_i) = \left| -m_i^{-1} \left| M^{-1}_{i,k-1} \chi_i \right|_{m_i} \right|_{m_k} \quad (i \neq k),$$

$$R_{k,k}(\chi_k) = \left| M^{-}_{k-1} \chi_k \right|_{m_k}. \quad (4)$$

Переход от МСС с базисом $\mathbf{M}$ и $\mathbf{Z}^{-}_{M_k}$ к МИМСС с тем же базисом и диапазоном $\mathbf{Z}^{-}_{2M}$ предельно упрощает базовой интегральной характеристики модулярного кода (ИХМК) – ИИ $I(X)$ согласно (2)-(4)). Это приводит к адекватной оптимизации и немодульных процедур, базирующихся на ИМФ (1). Количество необходимых таблиц и модульных операций для таких процедур при расчете базовых ИХМК сокращается в $k/2$ раз [1-2]. С увеличением мощности рабочего диапазона МИМСС получаемый выигрыш становится особенно значимым.

Формализация метода деления на двоичную экспоненту для преобразования минимально избыточного модулярного кода в ПК

Пусть в МИМСС с базисом $\mathbf{M}$ и диапазоном $\mathbf{Z}^{-}_{2M}$ задано число $X = (\chi_1; \chi_2 \ \ldots \ \chi_k)$ и пусть требуется получить его представление в ПСС с основанием r – дополнительный r-ичный код $(x_{n-1} x_{n-2} \ldots x_0)_r$ ($x_j \in \mathbf{Z}_r$ $(j = \overline{0, n-1})$) длины n. Необходимым условием корректности преобразования $(\chi_1, \chi_2, \ldots, \chi_k) \to (x_{n-1} x_{n-2} \ldots x_0)_r$ является включение диапазона $\mathbf{Z}^{-}_{2M}$ МИМСС в диапазон

$$\mathbf{Z}^{-}_{r^n} = \left\{ -\left\lfloor \frac{1}{2} r^n \right\rfloor; -\left\lfloor \frac{1}{2} r^n \right\rfloor + 1; \ldots \left\lceil \frac{1}{2} r^n \right\rceil - 1 \right\} \quad \text{ПСС.}$$

Из отношения $\mathbf{Z}^{-}_{2M} \subseteq \mathbf{Z}^{-}_{r^n}$ вытекает неравенство $2M \leq r^n$. Следовательно, дополнительный r-ичный ПК должен иметь длину $(n \geq \lceil \log_r (2M_k) \rceil)$ цифр.

Поскольку компьютерная позиционная арифметика ЦЧ, в частности в персональных ЭВМ, фактически представляет собой арифметику по модулям вида 2^b (b = 8; 16; 32; 64), то в качестве основания базовой ПСС целесообразно использовать $r \in \{2^8, 2^{16}, 2^{32}, 2^{64}\}$. Нетрудно видеть, что вычисление выражений вида (1) с использованием (2)-(4) по указанным модулям r в рамках применяемой таблично-сумматорной технологии осуществляется весьма просто.

Благодаря реализационным преимуществам ИМФ (1) и отмеченному обстоятельству преобразование МИМК в ПК эффективно может быть выполнено методом деления на двоичную экспоненту – основание r ПСС. Представляемый метод преобразования кода МИМСС в дополнительный r-ичный ПК базируется на операционном кортеже рекурсивного типа:

$$\langle X_0 = X,\ x_0 = |X_0|_r;\ X_1 = \lfloor X/r \rfloor,\ x_1 = |X_1|_r;$$
$$X_2 = \lfloor X_1/r \rfloor;\ x_2 = |X_2|_r\ \ldots\ X_{n-1} = \lfloor X_{n-2}/r \rfloor;\quad (5)$$
$$x_{n-1} = |X_{n-1}|_r \rangle .$$

На j-ой итерации процесса реализации (5) сначала формируется минимально избыточный модулярный код (МИМК) $(\chi_1^{(j)}, \chi_2^{(j)}, \ldots, \chi_k^{(j)})$ ЦЧ X_j, а затем находится цифра x_j его дополнительного r-ичного ПК путем расширения полученного МИМК на модуль r согласно правилу

$$x_j = |X_j|_r = \Big| \sum_{i=1}^{k-1} |M_{i,k-1}| M_{i,k-1}^{-1} \chi_i^{(j)} \Big|_{m_i} |_r + \\ + |M_{k-1} I(X_j)|_r |_r \ (j = \overline{0,\ n-1}). \quad (6)$$

Что касается числа X_j, то в соответствии с (5) для цифр его МИМК верна формула

$$\chi_i^{(j)} = \left| \left\lfloor \frac{X_{j-1}}{r} \right\rfloor \right|_{m_i} =$$
$$= \begin{cases} \chi_i \ \text{ при } j = 0; \\ \big| |\chi_i^{(j-1)} - x_{j-1}|_{m_i} \cdot |r^{-1}|_{m_i} \big|_{m_i} \ \text{ при } j = \overline{1,\ n-1}; \end{cases} \quad (7)$$
$$(i = \overline{1,\ k}).$$

Конкретный выбор способа компьютерной реализации расчетных соотношений (6)-(7) рассматриваемого метода кодового преобразования в первую очередь определяется величиной основания r ПСС. Если $r = 2^8$ или $r = 2^{16}$, то вычисление выражений (6) с использованием (7) в рамках таблично-сумматорной технологии, предполагающей ограничение модулей m_i МИМСС порогом m_max = 2^{16} ($m_i < 2^{16}$ $(i = \overline{1,\ k})$), наиболее просто и эффективно осуществляется с помощью таблиц TMpl_i модульного умножения на константы $C_i = |r^{-1}|_{m_i}$ и таблиц TE_i расширения МК. Необходимые таблицы генерируются по правилам:

$$\mathrm{TMpl}\_i[\chi] = |C_i \chi|_{m_i} \ (\chi = \overline{0, m_i - 1};\ i = \overline{1,\ k});\quad (8)$$

$$\mathrm{TE}\_i[\chi] = |M_{i,k-1}|M_{i,k-1}^{-1}\chi|_{m_i}|_r;$$
$$(\chi = \overline{0, m_i - 1};\ i = \overline{1, k-1}), \quad (9)$$

$$\mathrm{TE}\_k[\chi] =$$
$$= \begin{cases} |M_{k-1}\chi|_r \ \text{ при } \chi = \overline{0,\ m_0 - 1}; \\ |M_{k-1}(\chi - m_k)|_r \ \text{ при } \chi = \overline{m_0,\ m_k - 1}. \end{cases} \quad (10)$$

Расчетное соотношение (10) базируется на формуле (2) для ИИ ЦЧ в МИМСС. Аргументом таблицы TE_k при фиксированном j служит компьютерный ИИ $\chi = \hat{I}(X_j)$ числа X_j – см. (6). Для вычисления $\hat{I}(X_j)$ воспользуемся таблицами ИИ – TII_i, в которых хранятся наборы вычетов вида (4) согласно правилу

$$\mathrm{TII}\_i[\chi] = R_{i,k}(\chi)\ (\chi = \overline{0, m_i - 1};\ i = \overline{1,\ k}). \quad (11)$$

С учетом (11) из (3)-(4) для компьютерного ИИ $\hat{I}_k(X_j)$ следует расчетное соотношение

$$\hat{I}_k(X_j) = \left| \sum_{i=1}^{k} \mathrm{TII}\_i[\chi_i^{(j)}] \right|_{m_k}. \quad (12)$$

Таблично-сумматорная технология предполагает получение модульных сумм (12) аккумулятивно-табличным методом [10]. Это требует использования еще двух таблиц:

$$\mathrm{TRes}\_\mathrm{UP}k[x] = |2^{16}x|_{m_k}\ (x = \overline{0,\ 2^{16} - 1}),$$
$$\mathrm{TRes}k[x] = |x|_{m_k}\ (x = \overline{0,\ 2^{16} + m_k - 2}) \quad (13)$$

для приведения ЦЧ к остаткам по модулю m_k.

Таблично-сумматорная алгоритмизация схемы деления на двоичную экспоненту для преобразования МИМК в ПК

Из изложенных базовых положений метода деления на двоичную экспоненту и принципов его компьютерной реализации вытекает нижеследующий алгоритм преобразования кода МИМСС в ПК.

Параметры алгоритма: модули $m_1, m_2, \ldots, m_k$ МИМСС, выбираемые из множества простых чисел промежутка $(2^{15}; 2^{16})$ с минимизацией k [10], и основание $r = 2^b$ (b=16 бит) используемой ПСС.

Входные данные алгоритма: МИМК $(\chi_1; \chi_2; \ldots \chi_k)$ произвольного элемента X диапазона $\mathbf{Z}_{2M}^-$.

Выходные данные: дополнительный r-ичный код $(x_{n-1}x_{n-2}\ldots x_0)_r$ длины $n = \lceil \log_r(2M) \rceil$ ЦЧ X.

Предварительно получаемые данные: константы $C_i = |r^{-1}|_{m_i}$ $(i = \overline{1,k})$, а также таблицы TMpl_i, TE_i, TII_i $(i = \overline{1,k})$, TRes_UPk и TRes$k$ – см. (8)-(11) и (13).

Тело алгоритма модулярно-позиционного кодового преобразования по методу деления на основание ПСС с применением таблиц расширения МИМК.

МП_Д.1. Положить

$$X_0 = (\chi_1^{(0)}, \chi_2^{(0)}, ..., \chi_k^{(0)}) = (\chi_1, \chi_2, ..., \chi_k).$$

МП_Д.2. Порядковому номеру очередной цифры дополнительного *r*-ичного кода ЦЧ *X* присвоить начальное значение *j* = 0.

МП_Д.3. В соответствии с (6) с помощью таблиц (9), (10) расширить МК $(\chi_1^{(j)}, \chi_2^{(j)}, ..., \chi_k^{(j)})$ числа X_j (см. (5), (7)) на основание *r* ПСС, выполняя операции:

МП_Д.3а. Применяя таблицы (11), вычислить входящую в расчетное соотношение (12) сумму $s = \sum_{i=1}^{k} \text{TII}\_i[\chi_i^{(j)}]$.

МП_Д.3б. Получить компьютерный ИИ ЦЧ X_j, приводя *s* к остатку по модулю m_k согласно правилу

$$\hat{I}(X_j) = |s|_{m_k} = \text{TRes}k[s^{(0)} + \text{TRes\_UP}k[s^{(1)}]] \quad (s^{(0)} = s \wedge (2^{16} - 1),\ s^{(1)} = s >> 16).$$

МП_Д.3в. Вычислить *j*-ую цифру дополнительного *r*-ичного ПК входного числа:

$$x_j = |\sum_{i=1}^{k-1} \text{TE}\_i[\chi_i^{(j)}] + \text{TE}\_k[\hat{I}(X_j)]|_r. \quad (14)$$

МП_Д.4. По достижении равенства $j = n - 1$ завершить работу алгоритма.

МП_Д.5. Инкрементировать переменную *j* ($j = j + 1$).

МП_Д.6. Следуя (7), сформировать МИМК $(\chi_1^{(j)}, \chi_2^{(j)}, ..., \chi_k^{(j)})$ числа $X_j = \lfloor X_{j-1} / r \rfloor$, реализуя для всех $i = \overline{1,k}$ операционную последовательность:

МП_Д.6а. Найти $\chi = \chi_i^{(j-1)} - x_{j-1}$.

МП_Д.6б. Если $\chi < 0$, то положить $\chi = \chi + m_i$. В противном случае – перейти к МП_Д.6г.

МП_Д.6в. При $\chi < 0$ текущее значение переменной χ нарастить на m_i ($\chi = \chi + m_i$).

МП_Д.6г. Из таблицы TMpl_*i* (см. (8)) по адресу χ искомое значение *i*-ой цифры МК числа X_j: $\chi_i^{(j)} = \text{TMpl}\_i[\chi]$.

МП_Д.7. Перейти к МП_Д.3.

Для временных затрат на выполнение в ПЭВМ модулярно-позиционного кодового преобразования с помощью процедуры МП_Д.1–МП_Д.7 справедлива оценка:

$$t_{\text{МП\_Д.ПЭВМ}}(k,n) = 2(2kn - k - n)t_{\text{сл}} + (k(n-1) + 5n)t_{\text{ч}}, \quad (15)$$

где $t_{\text{сл}}$ и $t_{\text{ч}}$ – длительности операций сложения и чтения двухбайтового слова из таблицы соответственно.

Объем памяти для таблиц, используемых в алгоритме МП_Д.1–МП_Д.7, не превышает

$$M_{\text{Т.МП\_Д}}(k) = \frac{3}{8}(k+1) \text{ Мб}. \quad (16)$$

Предположим, что полумощность *M* диапазона МИМСС удовлетворяет условию $M > 2^{1024}$. В этом случае минимальное число *k* оснований базиса **M** принимает значение *k* = 65 [10]. Согласно теореме $1\ 2m_0 \le m_k - k + 2$. Поэтому ввиду $m_i < r$ ($i = \overline{1,k}$) неравенство $2M < r^n$, обеспечивающее минимум разности $r^n - 2M$, достигается при $n \le k$. Пусть $n = k = 65$, тогда оценочные выражения (15)-(16) в случае $t_{сл}$ = 2 нс, $t_ч$ = 1,14 нс дают: $t_{\text{МП\_Д.ПЭВМ}}(65,65)$ = 38392,9 нс, $M_{\text{Т.МП\_Д}}$ = 24,75 Мб.

Приведем оценки (15)-(16) для еще одной конфигурации алгоритма МП_Д.1 – МП_Д.7, которая определяется условием $M > 2^{2462}$. Отвечающая данному равенству МИМСС имеет *k* = 155 оснований; и при *n* = *k* = 155, $t_{сл}$ = 2 нс, $t_ч$ = 1,14 нс искомые значения характеристик (15)-(16) составляют: $t_{\text{МП\_Д.ПЭВМ}}(155,155)$ = 219055,3 нс, $M_{\text{Т.МП\_Д}}$ = 59,5 Мб.

Пусть теперь $r \in \{2^{32}, 2^{64}\}$. Так как в этом случае цифры *r*-ичного ПК $(x_{n-1}x_{n-2}...x_0)_r$ достаточно велики, то при реализации (7) они должны быть преобразованы в остатки по модулям m_i. Для выполнения операции $x_{j-1} \to |x_{j-1}|_{m_i}$ воспользуемся представлением ЦЧ $x_{j-1} \in \mathbf{Z}_r$ в ПСС с основанием $\tilde{r} = 2^{\tilde{b}}$ ($\tilde{b} = 16$ бит):

$$x_{j-1} = (x_{j-1}^{(\tilde{n}-1)}\ x_{j-1}^{(\tilde{n}-2)}...x_{j-1}^{(0)})_{\tilde{r}} = \sum_{l=0}^{\tilde{n}-1} x_{j-1}^{(l)} \tilde{r}^l = x_{j-1}^{(0)} + \tilde{r}(x_{j-1}^{(1)} + \tilde{r}(...\tilde{r}(x_{j-1}^{(\tilde{n}-2)} + \tilde{r}(x_{i-1}^{(\tilde{n}-1)}))...)) \quad (17)$$

$(\tilde{n} = b/\tilde{b};\ x_{j-1}^{(l)} \in \mathbf{Z}_{\tilde{r}})$.

Вычисление выражений вида (17) по модулям m_i весьма просто осуществляется с помощью таблиц

$$\text{TRes\_UP}i[x] = |\tilde{r}x|_{m_i},\ \text{TRes}i[x] = |x|_{m_i} \quad (x = \overline{0, \tilde{r} + m_i - 2});\ i = \overline{1,k}). \quad (18)$$

Искомое расчетное соотношение для остатков $\chi_i^{(j-1)} = |\, x_{j-1} \,|_{m_i}$, базирующееся на (17)-(18), имеет вид

$$\chi_i^{(j-1)} = \begin{cases} \mathrm{TRes}i[x_{j-1}^{(0)} + \mathrm{TRes\_UP}i[x_{j-1}^{(1)}]], & \text{если } r = 2^{32}, \\ \mathrm{TRes}i[x_{j-1}^{(0)} + \mathrm{TRes\_UP}i[x_{j-1}^{(1)} + \mathrm{TRes\_UP}i[x_{j-1}^{(2)} + \\ + \mathrm{TRes\_UP}i[x_{j-1}^{(3)}]]]], & \text{если } r = 2^{64}, \end{cases} \quad (19)$$

$$(i = \overline{1,k}).$$

Поскольку с увеличением разрядности p основания r используемой ПСС длина n кода $(x_{n-1}x_{n-2}\ldots x_0)_r$ уменьшается, причем достигаемое за счет этого сокращение временных затрат на преобразование МИМК в ПК при достаточно большом r становится более значимым, чем их возрастание, обусловленное выполнением операций (19), то с точки зрения проблемы повышения скорости процедур модулярно-позиционного кодового преобразования рассматриваемого класса весьма эффективным является совместное использование таблиц TE_i ($i = \overline{1,k}$) расширения кода и ПСС с большими основаниями.

Модификация алгоритма преобразования МИМК в ПК, реализующая обозначенную концепцию, заключается в нижеследующем.

Параметры алгоритма: модули $m_1, m_2, \ldots, m_k$ базовой МИМСС, основание $r=2^b$ ($b \in \{32, 64\}$) используемой ПСС и основание $\tilde{r} = 2^{\tilde{b}}$ ($\tilde{b} = 16$ бит) ПСС для представления цифр дополнительного r-ичного ПК.

Входные данные алгоритма: МИМК ($\chi_1; \chi_2; \ldots \chi_k$) ЦЧ X из диапазона $\mathbf{Z}_{2M}^{-}$.

Выходные данные: дополнительный r-ичный код $(x_{n-1}x_{n-2}\ldots x_0)_r$ длины $n = \lceil \log_r(2M) \rceil$ числа X.

Предварительно получаемые данные: таблицы TMpl_i, TE_i, TII_i, TRes_UPi и TRes$i$ ($i = \overline{1,k}$), формируемые согласно (8)-(11) и (18).

Тело алгоритма модулярно-позиционного кодового преобразования с применением таблиц расширения МИМК на модули r разрядностью b=32, 64 бита.

_МП_Д.1. Положить

$$X_0 = (\chi_1^{(0)}; \chi_2^{(0)} \ \ldots \ \chi_k^{(0)}) = (\chi_1; \chi_2 \ \ldots \ \chi_k).$$

_МП_Д.2. Порядковому номеру очередной цифры ПК числа X присвоить начальное значение: j=0.

_МП_Д.3. С помощью соотношения (6) и таблиц (9), (10) расширить МИМК $(\chi_1^{(j)}; \chi_2^{(j)} \ \ldots \ \chi_k^{(j)})$ числа Xj (см. (5), (7)) на основание r ПСС, выполняя операции:

_МП_Д.3а. Применяя таблицы (11) и (18), вычислить компьютерный ИИ $\hat{I}(X_j)$ ЦЧ X_j, определяемый по расчетному соотношению (12), согласно схеме:

$$\left\langle s = \sum_{i=1}^{k} \mathrm{TII\_}i[\chi_i^{(j)}];\ s^{(0)} = s \wedge (\tilde{r} - 1),\ s^{(1)} = s >> \tilde{b};\right.$$
$$\left. \hat{I}(X_j) = |\, s \,|_{m_k} = \mathrm{TRes}k[s^{(0)} + \mathrm{TRes\_UP}k[s^{(1)}]] \right\rangle.$$

_МП_Д.3б. Найти j-ую цифру ПК $(x_{n-1}x_{n-2}\ldots x_0)_r$ исходного ЦЧ X по правилу:

$$x_j = |\sum_{i=1}^{k-1} \mathrm{TE\_}i[\chi_i^{(j)}] + \mathrm{TE\_}k[\hat{I}(X_j)]|_r.$$

_МП_Д.4. При j=n–1 завершить работу алгоритма.

_МП_Д.5. Переменную j увеличить на 1 (j=j+1).

_МП_Д.6. Согласно (7) сформировать МИМК $(\chi_1^{(j)}, \chi_2^{(j)}, \ldots, \chi_k^{(j)})$ числа $X_j = \lfloor X_{j-1} / r \rfloor$, реализуя для $i = \overline{1,k}$ действия:

_МП_Д.6а. По формуле (19) выполнить преобразование $x_{j-1} \to (\chi_i^{(j-1)})$.

_МП_Д.6б. Найти $\chi = \chi_i^{(j-1)} - \tilde{\chi}_i^{(j-1)}$.

_МП_Д.6в. Если $\chi < 0$, то положить $\chi = \chi + m_i$.

_МП_Д.6г. Получить искомое значение i-ой цифры МИМК числа X_j: $\chi_i^{(j)} = \mathrm{TMpl\_}i[\chi]$.

_МП_Д.7. Перейти к шагу _МП_Д.3.

При реализации на ПЭВМ алгоритм _МП_Д.1–_МП_Д.7 требует временных затрат

$$t_{\_\mathrm{МП\_Д.ПЭВМ}}(k,n,b) = n(kt_{\mathrm{сл}} + 4t_{\mathrm{ч}} + 2\frac{b}{\tilde{b}}t_{\mathrm{ч}} + t_{\mathrm{сл}}(b) + (k-2)\max\{\frac{b}{\tilde{b}}t_{\mathrm{ч}}, t_{\mathrm{сл}}(b)\}) + k(n-1)(t_{\mathrm{ПО}}(b) + 2t_{\mathrm{сл}} + t_{\mathrm{ч}}), \quad (20)$$

где $t_{ч}$– время чтения двухбайтового слова из таблицы; $t_{\mathrm{сл}}(b)$ – время сложения двух b-битовых ЦЧ; $t_{\mathrm{сл}} = t_{\mathrm{сл}}$ (32); $t_{\mathrm{ПО}}(b)$ – длительность операции приведения к остатку цифры r-ичного ПК по модулю m_i ($i = \overline{1,k}$) МИМСС. Из (19) следует, что

$$t_{\mathrm{ПО}}(b) = \begin{cases} t_{\mathrm{сл}} + 2t_{\mathrm{ч}} & \text{при } b = 32 \text{ бита}, \\ 3t_{\mathrm{сл}} + 4t_{\mathrm{ч}} & \text{при } b = 64 \text{ бита}. \end{cases} \quad (21)$$

Быстродействие современных схем сложения несущественно зависит от разрядности b. С учетом этого положим $t_{\mathrm{сл}}(b) = t_{\mathrm{сл}}$.

Пусть b = 32 бита, а мощность диапазона $\mathbf{Z}_{2M}^{-}$ МИМСС удовлетворяет условию $2M > 2\cdot 2^{1024}$. В этом случае k = 65, n = 33 и оценка (20) с учетом (21) при $t_{сл}$ = 2 нс, $t_{ц}$ = 1,14 нс принимает значение $t_{\_МП\_Д.ПЭВМ}(65,33,32) = 28990{,}68$ нс. В случае, когда b = 64 бита, $2M > 2^{1025}$, длина r-ичного ПК составляет 17 цифр и $t_{\_МП\_Д.ПЭВМ}(65,17,64) = 236883$ нс. Если мощность диапазона МИМСС удовлетворяет условию $2M > 2\cdot 2^{2462}$, которому отвечает k = 155, то при b = 32 бита длина r-ичного ПК составляет n = 77 цифр и $t_{\_МП\_Д.ПЭВМ}(155,77,32) = 162554{,}52$ нс. В случае, когда b = 64 бита, код ПСС с основанием $r = 2^{64}$ имеет длину n = 39 цифр и $t_{\_МП\_Д.ПЭВМ}(155,39,64) = 132384{,}04$ нс.

Объем табличной памяти для алгоритма _МП_Д_1–_МП_Д_7 не превышает

$$M_{\text{Т.\_МП\_Д}}(k,b) = k\cdot 2^{17}(6+b/16) \text{ байт.} \quad (22)$$

Для пар $\langle k,b\rangle = \langle 65,32\rangle$; $\langle 65,64\rangle$; $\langle 155,32\rangle$; $\langle 155,64\rangle$ оценка (3.61) принимает значения:

$$M_{\text{Т.\_МП\_Д}}(65,32) = 65 \text{ Мб};$$

$$M_{\text{Т.\_МП\_Д}}(65,64) = 81{,}25 \text{ Мб};$$

$$M_{\text{Т.\_МП\_Д}}(155,32) = 155 \text{ Мб};$$

$$M_{\text{Т.\_МП\_Д}}(155,64) = 193{,}75 \text{ Мб}.$$

Приведенные оценочные данные по производительности и суммарному объему табличной памяти для приведенных конфигураций алгоритмов преобразования МИМК в ПК по методу деления на основание r ПСС позволяют заключить, что с ростом r четко просматривается тенденция к увеличению скорости осуществляемого преобразования. При рассматриваемых значениях параметров k и b ($k\in\{65, 155\}$, $b\in\{16, 32, 64\}$) характер и уровень достигаемого повышения производительности наглядно иллюстрируют коэффициенты:

$$t_{\text{МП\_Д.ПЭВМ}}(65,65,16)/t_{\_\text{МП\_Д.ПЭВМ}}(65,33,32) = 1{,}3;$$

$$t_{\text{МП\_Д.ПЭВМ}}(65,65,16)/t_{\_\text{МП\_Д.ПЭВМ}}(65,17,64) = 1{,}6;$$

$$t_{\text{МП\_Д.ПЭВМ}}(155,155,16)/t_{\_\text{МП\_Д.ПЭВМ}}(155,77,32) = 1{,}35;$$

$$t_{\text{МП\_Д.ПЭВМ}}(155,155,16)/t_{\_\text{МП\_Д.ПЭВМ}}(155,39,64) = 1{,}7.$$

Благодаря возможности применения принципа обобществления таблиц при формировании базового КТ системы, что допускает использование одних и тех же таблиц разными немодульными процедурами, сопровождаемое отмеченный рост быстродействия алгоритмов модулярно-позиционного кодового преобразования, увеличение объема необходимой табличной памяти фактически оказывается несущественным и для МА-приложений вполне приемлемо.

Заключение

Наиболее значимые результаты представленной разработки по оптимизации методологических и алгоритмических средств модулярно-позиционного кодового преобразования кратко можно охарактеризовать следующим образом.

1. Проведена математическая формализация метода деления ЦЧ в МСС на двоичную экспоненту, который положен в основу процедур модулярно-позиционного кодового преобразования. Главной отличительной особенностью реализуемого подхода при синтезе процедур исследуемого класса является применение минимально избыточного модулярного кодирования. Это позволяет сократить объем табличной памяти и временные затраты, приходящиеся на вычисление базовых интегральных характеристик МК в $k/2$ раз.

2. Синтезированы два новых алгоритма модулярно-позиционного кодового преобразования. Один из них ориентирован на ПСС с основанием $r = 2^{16}$, а другой – на ПСС с основаниями $r = 2^{32}$ и 2^{64}. Алгоритм с $r = 2^{16}$ прост в реализации, но формирует ПК максимальной длины. С увеличением r количество цифр ПК уменьшается. При этом, однако, в реализуемом вычислительном процессе на каждой итерации выполняется операция приведения последней полученной цифры ПК к остаткам по модулям МСС, что снижает производительность соответствующего алгоритма.

3. Исследована эффективность компьютерной реализации рекурсивной схемы деления на основание ПСС в рамках двух стратегий, первая из которых предполагает расширение МК преимущественно с помощью системных средств, а вторая с использованием таблиц расширения. Анализ разработанных конфигураций процедур преобразования МИМК в ПК с точки зрения проблемы повышения производительности при установленном верхнем пороге для размера табличной памяти показывает, что оптимальный результат достигается в случае совместного применения таблиц расширения и ПСС с большими основаниями r. При $r = 264$ получаемый выигрыш в быстродействии (в сравнении $r = 2^{16}, 2^{32}$) является (1,3-1,7)-кратным.

Литература

1. Коляда А.А., Пак И.Т. Модулярные структуры конвейерной обработки цифровой информации. Мн.: Университетское, 1992. – 256 с.

2. Коляда А.А., Чернявский А.Ф. Интегрально-характеристическая база модулярных систем счисления // Информатика. №1, 2013. – С. 106-119.
3. Червяков Н.И., Лавриненко А.Н. Исследования немодульных операций в системе остаточных классов // Научные ведомости БелГУ. Сер.: История. Политология. Экономика. Информатика. Вып. 21/1, №1 (120), 2012. – С. 110-121.
4. Siewobr H., Gbolade K.A. Modulo operation free reverse conversion in the {22n+1–1, 22n, 22n–1} moduli set // Int. J. of Computer Applications. Vol. 85, N1, 2014. – P. 11-14.
5. Исупов К.С. Алгоритм вычисления интервально-позиционной характеристики для выполнения немодульных операций в системах остаточных классов // Вестник ЮжУрГУ. Сер.: Компьютерные технологии, управление, радиоэлектроника. Вып. 1, Т.14, 2014. – С. 89-97.
6. Инютин С.А. Основы модулярной алгоритмики. Ханты-Мансийск: Полиграфист, 2009. – 347 с.
7. Чернявский А.Ф., Коляда А.А., Коляда Н.А. и др. Умножение по большим модулям методом Монтгомери с применением минимально избыточной модулярной арифметики // Нейрокомпьютеры: разработка, применение. № 9, 2010. – С. 3-8.
8. Коляда А.А., Чернявский А.Ф. Умножение по большим модулям с использованием минимально избыточной модулярной схемы Монтгомери // Информатика. №3, 2010. –С. 31-48.
9. Каленик А.Н., Коляда А.А., Коляда Н.А., Чернявский А.Ф., Шабинская Е.В. Умножение и возведение в степень по большим модулям с использованием минимально избыточной модулярной арифметики // Информационные технологии. №4, 2012. – С. 37-44.
10. Каленик А.Н., Коляда А.А., Коляда Н.А., Протько Т.Г., Шабинская Е.В. Компьютерно-арифметическая и реализационная база быстрых процедур умножения по большим модулям на основе модифицированной модулярной схемы Монтгомери // Электроника инфо. №7, 2012. – С. 114-118.
11. Червяков Н.И., Евдокимов А.А., Галушкин А.И. и др. Применение искусственных нейронных сетей и системы остаточных классов в криптографии. М.: Физматлит, 2012. – 280 с.
12. Tao Wu, Shoguo Li, Litian Liu. Improved RNS Montgomery modular multiplication with residue recovery // Proc. Int. Cons. on Soft. Computing Techniques and Engineering Application Advances in Intelligence Systems and Computing. Vol. 250, 2014. – P. 233-245.

BINARY EXPONENT DIVISION METHOD FOR CONVERSION OF THE MINIMALLY REDUNDANT MODULAR CODE TO THE POSITIONAL CODE

A.A. Kolyada, N.I. Chervyakov, P.V. Kuchynski, A.F. Chernyavsky, E.V. Shabinskaya

The paper is dedicated to the optimization procedures of the modular-positional conversion, which are based on the binary exponent division method. The optimization provides mi-nimization of summary time spent and applying of accessible memory for tables. It is achieved by using of minimally redundant modular coding, and number systems with large bit radix, as well as the table-summatory technology of calculation.

Keywords: *modular number system, minimally redundant modular code, positional code, code conversion, binary exponent division.*

Коляда Андрей Алексеевич, д.ф.-м.н., доцент, гл.н.с. Лаборатории специализированных вычислительных систем (СВС) НИИ Прикладных физических проблем (ПФП) им. А.Н. Севченко Белорусского государственного университета (БГУ), г. Минск. Тел. 8-10-375-17-212-47-45; 8-10-375-17-271-96-09. E-mail: razan@tut.by

Кучинский Петр Васильевич, д.ф.-м.н., доцент, директор НИИ ПФП им. А.Н. Севченко БГУ. Тел. 8-10-375-17-212-48-16. E-mail: niipfp@bsu.by

Червяков Николай Иванович, д.т.н., профессор, Заслуженный деятель науки и техники РФ, заведующий Кафедрой прикладной математики и математического моделирования Северо-Кавказского федерального университета, г. Ставрополь. Тел. (8-865) 275-35-64. E-mail: k-fmf-primath@stavsu.ru

Чернявский Александр Федорович, д.т.н., профессор, действительный член НАН Республики Беларусь, заведующий отделом информатики НИИ ПФП им. А.Н. Севченко БГУ. Тел. 8-10-375-17-278-58-26; 8-10-375-17-334-53-35. E-mail: niipfp@bsu.by

Шабинская Елена Владимировна, к.т.н., с.н.с. Лаборатории СВС НИИ ПФП им. А.Н. Севченко БГУ. Тел. 8-10-375-17-212-47-45; 8-10-375-17-271-83-21. E-mail: shabinskaya@rambler.ru