МАТЕМАТИКА

Сергей Арнольдович ИНЮТИН —
проректор по научной работе
Сургутского государственного
педагогического института,
доктор технических наук, профессор

Помехозащитные модулярные кодовые конструкции квадратичного диапазона

УДК 621.26

АННОТАЦИЯ. Введены помехозащитные модулярные кодовые конструкции квадратичного диапазона. Исследованы соотношения между метриками в линейном пространстве векторов с модулярными компонентами для различных методов кодирования и декодирования.

The author introduces the constructions of the modular error protection codes with square computer diapason and researches the ratio between the metrics of the code space for the coding and correction algorithms.

Контроль процессов хранения, передачи и обработки дискретной информации является актуальной проблемой для алгоритмически сложных распределенных вычислений, в частности при больших и сверхбольших диапазонах изменения компьютерных переменных, находящих широкое применение в современной вычислительной практике [1]. Для таких задач отсутствует наглядность результатов вычислений и только контроль позволяет оценить достоверность результата вычислений. Для контроля процесса и результатов вычислений в сверхбольших компьютерных диапазонах необходимы средства верификации или подтверждения правильности выполнения вычислительного процесса на промежуточных этапах, что позволяет гарантировать правильность окончательного результата [2]. Сквозной контроль всего вычислительного процесса обеспечить алгоритмически достаточно сложно, поэтому необходим контроль его отдельных этапов, на которых должны быть сосредоточены основные объемы модульных «быстрых» и параллельных вычислений на основе кольцевых операций [3].

Помехозащитные арифметические модулярные коды относятся к одному из двух известных классов арифметических помехозащитных кодов, и являются мощным средством контроля вычислительного процесса без дублирования [4,5].

Для уменьшения алгоритмической сложности кодовых и контрольных процедур модулярный помехозащитный код должен удовлетворять ряду требования:

— быть регулярным, т. е. контрольные компоненты кодовых векторов должны обрабатываться по тем же самым алгоритмам, что и информационные;

— информационные и контрольные компоненты должны быть равноправны относительно арифметических алгоритмов, поддерживающих вычислительный процесс и процедуры кодирования – декодирования: обнаружения и коррекции ошибок;

— из-за большого количества оснований модулярной системы для сверхбольших диапазонов алгоритмы кодирования –декодирования не должны быть полно переборными (с экспоненциальной сложностью), т.е. должны использовать операционные ресурсы или линейные таблицы;

— алгоритмы кодирования – декодирования должны базироваться на алгоритмах вычисления позиционных характеристик для модулярной величины, использующихся для выполнения немодульных операций;

— алгоритмы декодирования должны быть синдромные.

Аналогично классической теории алгебраического кодирования введем ряд понятий, связывающих модулярные системы счисления и помехозащитные коды.

Определение.

$[0, P^2)$ — информационный диапазон модулярного помехозащитного кода;

$[0, E^2) = [0, P^2H^2)$ — избыточный диапазон блокового модулярного помехозащитного кода;

$H^2 = E^2/P^2$ — множитель избыточного диапазона модулярного помехозащитного кода;

n — количество информационных компонент модулярного вектора;

k — количество контрольных компонент модулярного вектора;

$n+k$ — блоковая длина модулярного помехозащитного кода.

Подчеркнув связь с модулярной системой и добавив в обозначение количество оснований, обозначим модулярный помехозащитный код MC(E2, n+k),.

В выше указанном смысле модулярная система квадратичного диапазона MC(P2) –есть модулярный помехозащитный безизбыточный код MC(P2, n).

Модулярный код MC(E2, n+k) обладает следующими свойствами.

1. MC(E2, n+k) –линейный код.

Действительно: $vA + uB = D \in C$, где A, B(mod E2) — модулярные вектора, принадлежащие коду C.

2. Модулярный код — систематический, так как информационная часть кодового вектора отделена от контрольной.

3. Помехозащитный модулярный код – арифметический, т. к. является алгебраическим кольцом, что позволяет контролировать все основные кольцевые операции, а также множество машинных или программно эмулируемых операций на их основе.

Определение. Модулярный помехозащитный код для модулярной системы $MC(E^2)$ *с* $n+k$ — основаниями — есть подмножество C в множестве модулярных векторов с $n+k$ модулярными компонентами такое, что существует биективное отображение множества C на множество модулярных векторов из $MC(P^2)$ с n — основаниями.

Для модулярных помехозащитных кодов введем ряд расстояний между модулярными векторами, учитывающих специфический модульный тип ошибки в ка-

нале. Известен способ ввода расстояния — метрики на множестве n- мерных векторов через их скалярное произведение.

Определение. Первое скалярное произведение двух модулярных величин — векторов $A, B(mod\ P^2)$ из МС(P^2) — есть:

$$s_1 = \sum_{i=1}^{n} a_i \cdot b_i = (A, B)$$

Замечание. $s_1 \le n \cdot (p_i^2 - 1)^2$

Определение. Второе скалярное произведение двух модулярных величин — векторов $A, B(mod\ P^2)$ из МС(P2) — есть:

$$s_2 = \sum_{i=1}^{n} |a_i|_{p_i^2} \cdot |b_i|_{p_i^2}$$

Замечание 1. $s_2 \le n \cdot (p_i^2 - 1)^2$

Замечание 2. $s_2 = \sum_{i=1}^{n} |a_i|^2_{p_i^2}$ при $A=B(mod\ P^2)$

Введем два типа расстояний на множестве модулярных векторов, связанных со скалярными произведениями.

Определение. Евклидово расстояние между двумя модулярными величинами — векторами $A, B(mod\ P^2)$ из МС(P^2) — есть число:

$$\varepsilon(A,B) = \sqrt{\sum_{i=1}^{n} (a_i - b_i)^2} = \sqrt{(A-B, A-B)}$$

Определение. Модулярное расстояние между двумя модулярными величинами — векторами $A, B(mod\ P^2)$ из МС(P2) — есть число:

$$l(A,B) = \sqrt{\sum_{i=1}^{n} |a_i - b_i|^2_{p_i^2}} = \sqrt{(|A-B|_{p_i^2}, |A-B|_{p_i^2})}$$

Евклидово расстояние есть метрика, т. к. не отличается от соответствующей математической конструкции в евклидовом пространстве векторов с целочисленными компонентами из Z. Для модулярного расстояния справедлива следующая.

Теорема Т-1. Модулярное расстояние является метрикой.

Доказательство.

Используя арифметическое значение квадратного корня, по определению получим:

1. $l(A,B) \ge 0$.

2. $l(A,B) = 0$, если $A=B(mod\ P^2)$.

3. $l(A,B) = l(B,A)$.

4. Рассмотрим неравенство треугольника. Действительно, выполняется:

$$|x_i - y_i|_{p_i^2} = ||x_i - z_i|_{p_i^2} + |z_i - y_i|_{p_i^2}|_{p_i^2} = |x_i - z_i|_{p_i^2} + |z_i - y_i|_{p_i^2} - 0|p_i^2.$$

Следовательно:

$$|x_i - z_i|_{p_i^2} + |z_i - y_i|_{p_i^2} \ge |x_i - y_i|_{p_i^2}.$$

Возведем обе части неравенства в квадрат и просуммируем.

$$\sum_{i=1}^{n} (|x_i - z_i|^2_{p_i^2} + 2|x_i - z_i|_{p_i^2} |z_i - y_i|_{p_i^2} + |x_i - y_i|^2_{p_i^2}) \ge \sum_{i=1}^{n} |x_i - y_i|^2_{p_i^2}.$$

Используя неравенство Коши — Буняковского, которое для соотношений по модулям имеет вид:

$$\sum_{i=1}^{n}(|x_i - z_i|_{p_i^2}|z_i - y_i|_{p_i^2}) \geq \sqrt{\sum_{i=1}^{n}|x_i - z_i|^2_{p_i^2}}\sqrt{\sum_{i=1}^{n}|z_i - y_i|^2_{p_i^2}},$$

окончательно получим:

$$\sqrt{\sum_{i=1}^{n}|x_i - z_i|^2_{p_i^2}} + \sqrt{\sum_{i=1}^{n}|z_i - y_i|^2_{p_i^2}} \geq \sqrt{\sum_{i=1}^{n}|x_i - y_i|^2_{p_i^2}}.$$

Теорема Т-2. Первое и второе скалярные произведения определяют метрики, но не нормы.

Доказательство.

В евклидовом пространстве норма определяется

$$h(A) = \sqrt{(A, A)} = \sqrt{\sum_{i=1}^{n}|a_i|^2_{p_i^2}}$$

Для нормы должна выполняться, кроме ранее рассмотренных свойств, также следующая аксиома. Для любого целого числа $e \in Z$:

$h(e \cdot A) = |e| \cdot h(A)$

Выполняется отображение:

$$e \cdot A(\mathrm{mod}\, P^2) \leftrightarrow |ea_i|_{p_i^2}\ (\mathrm{mod}\, p_i^2)$$

и выполняется неравенство:

$$|ea_i|_{p_i^2} \leq e \cdot |a_i|_{p_i^2},$$

то может выполняться неравенство:

$h(e \cdot A) \leq |e| \cdot h(A)$.

Третья аксиома нормы не выполняется, теорема доказана.

Определение. Одномодульная ошибка в модулярном векторе есть произвольное искажение одной компоненты модулярного представления числовой величины в МС(Р2) (одной парной компоненты модулярного вектора).

Определение. Аддитивная модульная ошибка (одиночная) – есть число, модульная сумма которого и вычета некоторой величины по данному основанию из МС(Р2), приводит к произвольному искажению исходной модулярной величины.

Определение. Многократная модульная ошибка в модулярном векторе есть произвольное искажение некоторого множества компонент модулярного вектора.

Выше введенные расстояния – метрики не в полной мере соответствуют модели модульной ошибки канала для модулярного помехозащитного кода.

Формализуем понятие ошибки в модулярном коде и введем остаточное расстояние – аналог расстояния Хэмминга для модулярных кодов.

Определение. Остаточный вес модулярного вектора $A\,(mod\ P^2)$ есть количество ненулевых вычетов модулярного вектора.

Определение. Остаточное расстояние $d(A,B)$ между двумя модулярными векторами $A\,(mod\ P^2)$, $B\,(mod\ P^2)$ — есть остаточный вес модульной разности двух модулярных векторов.

$$d(A,B) = \sum_{i=1}^{n}\delta\left(|a_i - b_i|_{p_i^2}\right),$$

где $\delta\left(|a_i - b_i|_{p_i^2}\right) = \begin{cases} 1, \text{ при } a_i \neq b_i \\ 0, \text{ при } a_i = b_i \end{cases}$

Остаточное расстояние метрика, т. к. для него выполняются аксиомы:

1. $d(A,B) \geq 0$,
2. $d(A,) = d(B,A)$,
3. $d(A,B) \leq d(A,C) + d(C,B)$.

Определение. Остаточное кодовое расстояние dC — есть наименьшее из остаточных расстояний между любыми парами кодовых векторов.

Остаточное кодовое расстояние совпадает с минимальным остаточным весом ненулевых кодовых векторов, так как модулярный код линейный:

$d_C = min\ w(A),\ A \in C,\ A \neq 0.$

Для безизбыточного модулярного кода: $d_C = min\ w(A) = 1.$

Определение. Шар остаточного радиуса r в пространстве модулярных векторов есть множество:

$$S_A^r = \{B(\mathrm{mod}\, E^2) \mid \quad d(A,B) \leq r\},$$

где $A\,(mod\ E^2)$ — модулярная величина — центр шара.

При r=1 определяются шары для одиночных модульных ошибок.

По аналогии сформулируем ряд теорем — утверждений, позволяющих установить границы для обнаруживающих и корректирующих способностей модулярных кодов.

1. Если во всех шарах радиуса l содержится лишь по одному кодовому вектору – центру шара, то модульные ошибки кратности — l обнаруживаются и корректируются модулярным помехозащитным кодом.

2. Если в шарах радиуса l+1, в отличии от шаров радиуса l, содержится более одного кодового вектора, то модульные ошибки кратности l+1 в общем случае не обнаруживаются.

3. Если шары радиуса [l / 2] не пересекаются и содержат не более одного кодового вектора, то модульные ошибки кратности [l / 2] можно корректировать, в частности полнопереборными методами.

4. Модулярные помехозащитные коды не являются совершенными, для них не выполняется условие плотной упаковки [5]. По этой причине модулярный код, построенный для обнаружения ошибок кратности l, обнаруживает часть ошибок большей кратности.

Определение. Модулярный помехозащитный код, построенный методом вложенных модулярных диапазонов, – есть множество $n+k$ -компонентных модулярных величин, заданных в МС(E^2, n+k), таких, что их числовое значение не превышает максимум информационного диапазона: $A \in [0, P^2) \subset [0, E^2)$.

Метод вложенных диапазонов является не единственным, но наиболее естественным, основным методом построения помехозащитного модулярного кода, для него выполняется следующая теорема.

Теорема Т-3. Для модулярной величины $A\,(mod\ E^2)$, A-P или A<P^2 модулярная величина $B\,(mod\ E^2)$, содержащая одномодульную ошибку по основанию p^2_i имеет вид:

$$B = A + N_i \cdot E^2 / p_i^2 (\mathrm{mod}\, E^2),$$

где $N_i(\mathrm{mod}\, E^2 / p_i^2)$ — модулярная величина, зависящая от значения модульной ошибки по основанию p^2_i.

Доказательство.

Пусть исходная модулярная величина $A\,(mod\ E^2)$, A-P или A<P^2 задана в МС(E^2, n+k) . Только вычет по основанию p^2_i содержит аддитивную модульную

ошибку, следовательно, величина $B(mod\ E^2)$ с одномодульной ошибкой $vi\ (mod\ p^2_i)$ имеет вид:

$$B = A + N_i \cdot E^2 / p_i^2 (\mathrm{mod}\, E^2),$$

где $N_i \cdot E^2 / p_i^2 (\mathrm{mod}\, E^2) \leftrightarrow v_i (\mathrm{mod}\, p_i^2)$,

$$1 \le N_i < p_i^2,$$

$$v_i = d_i + l_i p_i \ (\mathrm{mod}\, p_i^2),$$

$$A(\mathrm{mod}\, E^2) \leftrightarrow a_i + k_i p_i (\mathrm{mod}\, p_i^2),$$

$$B(\mathrm{mod}\, E^2) = |\, a_i + d_i \,|_{p_i^2} + (k_i + l_i + [(a_i + d_i) / p_i])\, p_i (\mathrm{mod}\, p_i^2).$$

Следствие С-1. Ошибки типа d_i Ќ 0, l_iЌ 0 и d_i Ќ 0, l_i= 0 не разделимы. Действительно:

$$N_i \cdot E^2 / p_i^2 (\mathrm{mod}\, E^2) \leftrightarrow v_i (\mathrm{mod}\, p_i^2),$$

$$v_i = d_i < p_i,$$

$$B(\mathrm{mod}\, E^2) = |\, a_i + d_i \,|_{p_i^2} + (k_i + [(a_i + d_i) / p_i])\, p_i (\mathrm{mod}\, p_i^2).$$

Следствие С-2. Ошибки типа d_i Ќ 0, l_iЌ 0 и d_i = 0, l_iЌ 0 разделимы. Действительно:

$$A + N_i \cdot E^2 / p_i \ (\mathrm{mod}\, E^2) = A + N_i \cdot E^2 / p_i^2 (\mathrm{mod}\, E^2),$$

$$N_i \cdot E^2 / p_i^2 (\mathrm{mod}\, E^2) \leftrightarrow v_i = l_i p_i (\mathrm{mod}\, p_i^2),$$

$$B(\mathrm{mod}\, E^2) = |\, a_i \,|_{p_i^2} + (k_i + l_i) p_i (\mathrm{mod}\, p_i^2).$$

Коррекция одномодульных ошибок в модулярном коде возможна, если для любой комбинации пар оснований и величин ошибок модулярные величины, содержащие эти ошибки, не равны между собой. Следующие теоремы устанавливают условия, при которых возможны обнаружение и коррекция ошибок модулярным кодом.

Теорема Т-4. Модулярный помехозащитный код МС(E², n+2) для упорядоченной модулярной системы корректирует одномодульные ошибки при избыточном диапазоне: $H^2 > p_{n+1}^2 \cdot p_{n+2}^2$.

Доказательство.

От противного. Пусть одномодульные ошибки не корректируются. Следовательно, для модулярных величин $A, B(mod\ E^2)$ выполняется равенство в Z:

$$A + N_i \cdot E^2 / p_i^2 (\mathrm{mod}\, E^2) = B + N_j \cdot E^2 / p_j^2 (\mathrm{mod}\, E^2),$$

$$|A - B| = |(N_i \cdot p_j^2 - N_j \cdot p_i^2) \cdot E^2 / (p_i^2 p_j^2) (\mathrm{mod}\, E^2),$$

Для левой части последнего равенства справедливо при $A, B(mod\ E^2) < P^2$:

$$0 \le |A - B| \le P^2 - 1.$$

Правая часть последнего равенства в условиях теоремы больше P^2 $\forall i,j$=1jn+2 .

Следствие С-1. При *Ni, NjЌ0, (pi, pj)*=1

$$\min |(N_j p_i^2 - N_i p_j^2)| = (p_i + p_j)\,|\, p_i - p_j \,| > \max\{p_i, p_j\}$$

Более точное условие для коррекции одномодульных ошибок

$$H^2 \ge p_i^2 p_j^2$$

Следствие С-2. При $A, B(mod\ E^2) < P$ для левой части последнего равенства выполняется: $0 \trianglelefteq A - B \trianglelefteq P - 1$.

Правая часть последнего равенства будет не меньше Р при $E^2 = P^2$, т. е. для без избыточного кода МС(Р2, n).

Следствие С-3. С учетом результата из С-1 данной теоремы справедливо утверждение: часть многомодульных ошибок будет обнаруживаться данным модулярным кодом.

Теорема Т-5. Для квадратичной формы $\Delta = |(N_j p_i^2 - N_i p_j^2)|$, описывающей одномодульные ошибки, при ненулевых коэффициентах существует точная нижняя грань: $\min \Delta = 2p_j - 1$

i, j

Доказательство.

Интерес представляет случай ненулевых модульных ошибок в модулярной величине: $N_i N_j \neq 0$.

Пусть $p_j > p_i$, $p_i = p_j - 1$

$N_i = p_i^2 - 1$, $N_j = p_j^2 - 1$,

тогда выполняются следующие соотношения:

$$(p_j^2 - 1)p_i^2 - (p_i^2 - 1)p_j^2 = (p_j^2 - 1)(p_j - 1)^2 - ((p_j - 1)^2 - 1)p_j^2 =$$

$$= (p_j - 1)^2 p_j^2 - (p_j - 1)^2 - (p_j - 1)^2 p_j^2 + p_j^2 = -p_j^2 + 2p_j - 1 + p_j^2 =$$

$$= 2p_j - 1.$$

Различные методы построения помехозащитных модулярных кодов исследовал В.А. Торгашев [7]. AN коды – введены Ю. Г. Дадаевым [6], их аналоги для модулярных систем, а также слабо — арифметические модулярные коды, исследованы автором [8].

Алгоритмы декодирования быть совмещены с алгоритмами вычисления позиционных характеристик (ПХ), используемых для выполнения немодульных операций, таким образом, чтобы:

— при вычислении ПХ для определения знака или переполнения одновременно обнаруживались модульные ошибки;

— при обнаружении ошибок дополнительно выполнялись процедуры их коррекции.

Для этого введем следующую конструкцию модулярных диапазонов:

[0, P^2) — рабочий мультипликативный диапазон,

$D^2 = p^2_0$ — множитель расширения на диапазон со знаком и аддитивным переполнением. Минимальное значение $D^2 = p^2_0 = 2 \cdot 2$. Причем:

$$p_0^2 < p_1^2 < p_2^2 < p_3^2 .... < p_n^2 < p_{n+1}^2 < p_{n+2}^2 .$$

$H^2 = p^2_{n+1} \cdot p^2_{n+2}$ — множитель расширения на диапазон с контролем: обнаружением и коррекцией одномодульных ошибок.

Выполняются условия:

$[A / D^2] \in [0, 2P^2)$ — модулярная величина имеет положительное значение;

$[A / D^2] \in [E^2 - 2P^2, E^2)$ — модулярная величина имеет отрицательное значение;

$[A / D^2] \in [2P^2, E^2 - 2P^2)$ — модулярная величина содержит модульные ошибки.

Целесообразен выбор D2=p20 < p1, тогда знак и обнаружение одномодульных ошибок для модулярной величины определяется значениями одной компоненты, меньшей максимума типового машинного диапазона [9, 10].

ЛИТЕРАТУРА

1. Ноден П. и др. Алгебраическая алгоритмика. М.: Мир, 1999. 720 с.
2. Инютин С. А. Основы многоразрядной алгоритмики. Сургут: Изд-во РИЦ, 2002. 137 с.
3. Амербаев В. М. Теоретические основы машинной арифметики. Алма-Ата: Наука, 1976. 320 с.
4. Инютин С. А. Модулярные вычисления в сверхбольших компьютерных диапазонах // Известия вузов. Электроника. 2001. № 6. С. 34–39.
5. Касами Т. и др. Теория кодирования. М.: Мир, 1978. 576 с.
6. Дадаев Ю. Г. Теория арифметических кодов. М.: Радио и связь, 1981. 272 с.
7. Торгашев В. А. Система остаточных классов и надежность ЦВМ. М.: Советское радио, 1973. 120 с.
8. Инютин С. А. Декодирование слабо-арифметических кодов СОК на многозначных структурах // Многозначные элементы, системы, структуры: Сб. ст. / ИПМЭ. Киев: Наукова-Думка, 1983. С. 28–34.
9. Инютин С. А. Компьютерная модулярная алгебра квадратичного диапазона и область ее приложения // Вестник Тюменского госуниверситета. 2001. № 2. С. 141–148.
10. Инютин С. А. Вычислительные задачи большой алгоритмической сложности и модулярная арифметика // Вестник Тюменского госуниверситета. 2002. № 3. С. 3–9.

Игорь Николаевич ГЛУХИХ —
проректор по информационным технологиям ТюмГУ,
доктор технических наук, доцент

Событийно-ориентированное представление объектов в условиях неопределенности координат событий и отношений между ними

УДК 007:681.3.06

АННОТАЦИЯ. В рамках объектно-ориентированного подхода рассмотрен способ формального представления объектов на основе представления мультивекторов событий и их преобразований. Предложено обобщение на случай неопределенности координат событий.

Object-oriented approach and the method of objects presentations are considered. The method is based on the events multivectors and their transformations. The fuzzy coordinate generalization of events multivectors and transformations is offered.

Модель предметной области (ПО) является важным компонентом прикладных интеллектуальных систем (интеллектуальных САПР, учебно-исследовательских систем и тренажеров, систем поддержки принятия решений), который представляет собой совокупность знаний об объектах данной ПО, их параметрах, состояниях, особенностях поведения и отношений между ними. При объектно-ориентированном моделировании предметной области она представляется в виде модели некоторого виртуального мира, включающего в себя единообразные по описанию объекты различной сложности — от наиболее сложного объекта «моделируемый мир» до простых неделимых объектов — компонентов этого мира [1]. При этом можно выделить два уровня моделирования и два вида моделей, отличающихся по уровню формализации.