УДК 681.325

А. А. КОЛЯДА

ИНТЕРВАЛЬНО-МОДУЛЯРНЫЕ КОДЫ С ИСПРАВЛЕНИЕМ ОШИБОК

В теории кодирования разработан широкий набор алгебраических кодов, предназначенных для обнаружения и исправления ошибок при хранении и передаче информации [1. С. 163—382]. Для контроля вычислительных устройств такие коды не пригодны [2. С. 107—108]. Среди позиционных арифметических кодов наибольшую известность получили AN коды и так называемые остаточные коды [3]. Идеи, положенные в основу этих кодов, нашли дальнейшее развитие в рамках системы остаточных классов (СОК) [4—6]. Алгоритмы декодирования кодов СОК, как правило, базируются на процедурах формирования интегральных характеристик кодов, наиболее трудоемких операциях модулярной арифметики. Это приводит к усложнению и снижению быстродействия декодирующей аппаратуры (см., например, [7]). В данной работе предпринимается попытка устранить отмеченный недостаток кодов СОК путем некоторой их модификации.

Рассмотрим систему модулей $m_1, m_2, \ldots, m_k, q_1, \ldots, q_n$, удовлетворяющую условиям: $(m_i, m_j)=1$, $i\neq j$; $i, j=1, 2, \ldots, k$; $(q_s, q_l)=1$, $s\neq l$; $s, l=1, 2, \ldots, n$; $(m_i, q_l)=1$, $i=1, 2, \ldots, k-1$; $l=1, 2, \ldots, n$;

$$m_k \geqslant 2p+k-2, \tag{1}$$

где n, k, p — фиксированные натуральные числа ($n \geqslant 1$, $k \geqslant 2$, $p \geqslant 1$); и пусть: $V_i = \{0, 1, \ldots, m_i-1\}$, $i=1, 2, \ldots, k$; $W_l = \{0, 1, \ldots, q_l-1\}$, $l=1, 2, \ldots, n$; $V = V_1 \times V_2 \times \ldots \times \underset{k-1}{V_k} \times W_1 \times \ldots \times W_n$; $D(p) = \{-pM, -pM+1, \ldots, pM-1\}$, $M = \prod_{i=1} m_i$. Тогда отображение $f: D(p) \to V$, ставящее в соответствие числу $A \in D(p)$ слово $a = f(A) = (\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \overline{I}_a, \beta_1, \ldots, \beta_n) \in V$, в котором $\alpha_i = |AM_i^{-1}|_{m_i}$ ($i=1, 2, \ldots, k-1$), $\beta_l = |A|_{q_l}$ ($l=1, 2, \ldots, n$), а $\overline{I}_a$ выбирается так, чтобы выполнялось равенство

$$A = \sum_{i=1}^{k-1} M_i \alpha_i + I_a M, \tag{2}$$

где

$$I_a = \begin{cases} \overline{I}_a, & \text{если } 0 \leqslant \overline{I}_a < p, \\ \overline{I}_a - m_k, & \text{если } p \leqslant \overline{I}_a < m_k; \end{cases} \tag{3}$$

$M_i = M/m_i$, через $|X|_d$ обозначается наименьший неотрицательный вычет по модулю d, сравнимый с величиной X; определяет некоторый код $C \subseteq V$, который назовем интервально-модулярным кодом с информаци-

онными модулями $m_1, m_2, \ldots, m_k$ и контрольными модулями $q_1, q_2, \ldots, q_n$ (ИМ код).

Как известно, корректирующие возможности кодов с исправлением ошибок зависят от значения их кодового расстояния [1. С. 26 — 28]. Для задания на множестве V метрики определим в нем операцию сложения следующим образом. Суммой двух слов $a_1 = (\alpha_1^{(1)}, \alpha_2^{(1)}, \ldots, \alpha_{k-1}^{(1)}, \bar{I}_{a_1}, \beta_1^{(1)}, \ldots, \beta_n^{(1)})$ и $a_2 = (\alpha_1^{(2)}, \alpha_2^{(2)}, \ldots, \alpha_{k-1}^{(2)}, \bar{I}_{a_2}, \beta_1^{(2)}, \ldots, \beta_n^{(2)})$ из V назовем слово $a_3 = (\alpha_1^{(3)}, \alpha_2^{(3)}, \ldots, \alpha_{k-1}^{(3)}, \bar{I}_{a_3}, \beta_1^{(3)}, \ldots, \beta_n^{(3)}) \in V$ такое, что $\alpha_i^{(3)} = |\alpha_i^{(1)} + \alpha_i^{(2)}|_{m_i}$ $(i = 1, 2, \ldots, k-1)$; $\beta_l^{(3)} = |\beta_l^{(1)} + \beta_l^{(2)}|_{q_l}$ $(l = 1, 2, \ldots, n)$ и

$$\bar{I}_{a_3} = \left|\bar{I}_{a_1} + \bar{I}_{a_2} + \sum_{i=1}^{k-1} \left[\frac{\alpha_i^{(1)} + \alpha_i^{(2)}}{m_i}\right]\right|_{m_k},$$

где квадратные скобки употребляются для обозначения целой части чисел.

Легко проверить, что относительно введенной операции множество V является абелевой группой: нулевым элементом является слово $0 = (0, 0, \ldots, 0)$, а противоположным по отношению к слову $a = (\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \bar{I}_a, \beta_1, \ldots, \beta_n)$ будет слово

$$-a = (|-\alpha_1|_{m_1}, |-\alpha_2|_{m_2}, \ldots, |-\alpha_{k-1}|_{m_{k-1}}, |-I_a - n_a|_{m_k}, |-\beta_1|_{q_1}, \ldots, |-\beta_n|_{q_n}), \tag{4}$$

где n_a — число ненулевых символов в последовательности $\alpha_1, \alpha_2, \ldots, \alpha_{k-1}$.

Для разности слов a_1 и a_2 справедлива формула

$$a_1 - a_2 = (|\alpha_1^{(1)} - \alpha_1^{(2)}|_{m_1}, |\alpha_2^{(1)} - \alpha_2^{(2)}|_{m_2}, \ldots, |\alpha_{k-1}^{(1)} - \alpha_{k-1}^{(2)}|_{m_{k-1}}, \tag{5}$$

$$\left|\bar{I}_{a_1} - \bar{I}_{a_2} + \sum_{i=1}^{k-1} \left[\frac{\alpha_1^{(1)} - \alpha_2^{(2)}}{m_i}\right]\right|_{m_k}, |\beta_1^{(1)} - \beta_1^{(2)}|_{q_1}, \ldots, |\beta_n^{(1)} - \beta_n^{(2)}|_{q_n}).$$

Назовем весом $W(a)$ слова $a \in V$ число его ненулевых символов и определим расстояние между элементами a_1 и a_2 из V по формуле

$$d(a_1, a_2) = \max\{W(a_1 - a_2), W(a_2 - a_1)\}. \tag{6}$$

Нетрудно убедиться в том, что функция $d(a_1, a_2)$ удовлетворяют аксиомам расстояния.

Лемма. Если хотя бы один из первых k символов слова $a = (\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \bar{I}_a, \beta_1, \ldots, \beta_n) \in V$ не равен нулю, то множество $\{\bar{I}_a, \bar{I}_{-a}\}$, ($-a$ — элемент, противоположный по отношению к a) содержит ненулевой символ.

Доказательство. Пусть a — слово, удовлетворяющее условию леммы. Предположим, что $I_a = 0$. Тогда число n_a ненулевых символов в последовательности $\alpha_1, \alpha_2, \ldots, \alpha_{k-1}$ положительно и, согласно формулам (1) и (4), имеем $\bar{I}_{-a} = |-n_a|_{m_k} > 0$, что и доказывает лемму.

Теорема 1. Если контрольные модули ИМ кода таковы, что $Q > 2p$, $\left(Q = \prod_{l=1}^{n} q_l\right)$, то для кодового расстояния $d(C)$ $(d(C) = \min\{d(a_1, a_2)\}$ кода C имеет место формула

$$d(C) = n + k - \max\{S = j_0 + l_0 \mid 0 < \prod_{j=1}^{j_0} m_{ij} \prod_{l=1}^{l_0} q_{k_l} \leqslant 2pM, \tag{7}$$

где максимум берется по упорядоченным по возрастанию наборам индексов $(i_1, i_2, \ldots, i_{j_0}) \subseteq \{1, 2, \ldots, k-1\}$ и $(k_1, k_2, \ldots, k_{l_0}) \subseteq \{1, 2, \ldots, n\}$.

Доказательство. Пусть a_1 и a_2 — кодовые слова, причем $a_1 \neq a_2$ и пусть A_1 и A_2 — соответствующие им числа из $D(p)$ (см. форму-

лу (2)). Тогда из формул (2), (5), (6) и доказанной леммы следует, что $d(a_1, a_2)=n+k-S_0$, где S_0 — количество модулей ИМ кода, исключая m_k, которым кратно число $|A_1-A_2|$. Теперь видим справедливость формулы (7), если учесть, что $|A_1-A_2|\in[1, 2pM]\subseteq[1, MQ]$.

Из теоремы 1 и общей теории кодирования [5, 6] вытекает следующая.

Теорема 2. Корректирующий ИМ код, для которого $n=1$, $q_1>m_i$ (для всех $i=1, 2, \ldots, k$); $n=2$, $q_l>m_i$ (для всех $i=1, 2, \ldots, k$ и $l=1, 2$), обнаруживает (исправляет) любую аддитивную ошибку веса 1.

Рассмотрим ИМ код, для которого $n=2$ и

$$q_l>m_i \quad (i=1, 2, \ldots, k; \ l=1, 2). \tag{8}$$

Предположим, что в результате обработки числовой информации слово $a=(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, I_a, \beta_1, \beta_2)\in V$, в котором один из символов может быть искаженным. Приводимая ниже процедура декодирования слова a позволяет обнаружить и исправить любые такие искажения.

1. Вычислим величины

$$S_l=\Big|\beta_l+\sum_{i=1}^{k-1}|M_i\alpha_i|_{q_l}+|I_aM|_{q_l}\Big|_{q_l}, \quad l=1, 2. \tag{9}$$

где I_a определяется по формуле (3).

Если $S=(S_1, S_2)=(0, 0)$, то декодируемое слово, очевидно, является кодовым. С другой стороны, если a содержит ошибку, то благодаря условию (8) это неизбежно приведет к отличию от нуля, по меньшей мере, одной из компонент величины S. Таким образом, S представляет собой синдром рассматриваемого кода.

2. Если одна из компонент синдрома (например, S_1) не равна нулю, а другая (S_2) равна нулю, то контрольный символ β_1 искажен и, согласно (9), истинное значение его β_1' восстанавливается по формуле

$$\beta_1'=\Big|\sum_{i=1}^{k-1}M_i\alpha_i+I_aM\Big|_{q_1}=|\beta_1-S_1|_{q_1}.$$

3. Случай $S_1\neq 0$, $S_2\neq 0$ соответствует искажению одного из информационных символов. Для локализации и исправления такой ошибки достаточно:

а) для каждого $j=1, 2, \ldots, k$ в формуле (2) заменить j-й символ a на неизвестное X_j и затем найти его по контрольным модулям, используя формулы (2) и (9):

$$|X_j|_{q_l}=\Big|M_j^{-1}\Big(\beta_l-\sum_{i=1}^{k=1}M_i\alpha_i-I_aM\Big)\Big|_{q_l}=|M_j^{-1}S_l+\alpha_j|_{q_l}$$

$$(j=1, 2, \ldots, k-1; \ l=1, 2),$$

$$|X_k|_{q_l}=\Big|M^{-1}\Big(\beta_l-\sum_{i=1}^{k-1}M_i\alpha_i\Big)\Big|_{q_l}=|M^{-1}S_l+I_a|_{q_l}; \ l=1, 2;$$

б) если для некоторого $j_0\in\{1, 2, \ldots, k-1\}$ выполняется $|X_{j_0}|_{q_1}=|X_{j_0}|_{q_2}=\alpha_{j_0}'$, причем $0\leqslant\alpha_{j_0}'<m_{j_0}$, то заключаем, что искажен символ слова a с номером j_0 и правильным его значением является вычет α_{j_0}'. Аналогично, если величины I_1' и I_2', определяемые соответственно вычетами $|X_k|_{q_1}$ и $|X_k|_{q_2}$ по формулам вида (3), совпадают, причем находятся в интервале $[-p-k+2, p)$, то принимаем, что искажен k-й символ слова a и его истинным значением будет $|I_1'|_{m_k}$.

Описанный алгоритм декодирования может быть выполнен за $2+$ $+]\log_2 k[$ модульных операций [8].

Исследования показали, что в интервально-модулярных системах счисления операция расширения кода выполняется значительно проще,

чем в СОК. Это позволяет использовать для корректирующих ИМ кодов предельно простые проверочные соотношения и алгоритмы декодирования.

Список литературы

1. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. М., 1978.
2. Журавлев Ю. П., Котелюк Л. А., Циклинский Н. И. Надежность и контроль ЭВМ. М., 1978.
3. Дадаев Ю. Г. Теория арифметических кодов. М., 1981.
4. Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. М., 1968.
5. Торгашев В. А. Система остаточных классов и надежность ЦВМ. М., 1973.
6. Mandelbaum D. M. // IEEE Trans. Inform. Theory. 1976. V. 23. N. 1. P. 85.
7. Краснобаев В. А., Давыдов И. Б. Устройство для обнаружения ошибок в системе остаточных классов СОК: А. с. 1013957 СССР // БИ 1983. № 15.
8. Коляда А. А. Устройство для исправления ошибок в непозиционном коде: А. с. 1136165 СССР // БИ 1985. № 3.

Поступила в редакцию 10.03.86.

УДК 519.234.8

Т. Н. ДЫЛЬКО

ВЫБОР КОЭФФИЦИЕНТОВ СТАТИСТИКИ ДЛЯ ПРОВЕРКИ ГИПОТЕЗЫ ОДИНАКОВОЙ РАСПРЕДЕЛЕННОСТИ В ЗАДАЧАХ АНАЛИЗА ДИХОТОМИЧЕСКОЙ ИНФОРМАЦИИ

1. При формировании группы экспертов по принципу согласованности мнений [1] возникает задача проверки гипотезы о равенстве распределений.

Например, группа экспертов проводит классификацию изделий в N классов (изделия 1-го сорта, 2-го и т. д.) при m-кратной экспертизе, причем классификация проводится независимо между экспертами и между экспертизами. Ответы j-го эксперта можно описывать набором независимых случайных величин следующим образом: $\alpha_{ts}^j = 1$ с вероятностью P_{ts}^j, если при s-й экспертизе изделие отнесено в t-й класс и $\alpha_{ts}^j = 0$ с вероятностью $1 - P_{ts}^j$ в противном случае.

Случайные величины $\{\alpha_{ts}^j,\ t = 1, \ldots, N;\ s = 1, \ldots, m\}$ при сделанных предположениях независимы в совокупности и представляют собой конечную последовательность независимых испытаний Бернулли, т. е. образуют люсиан [2].

В соответствии с методом, предложенным в [1] и подробно изложенным в [2], строится критерий для проверки гипотезы одинаковой распределенности, основанный на расстоянии между люсианами и содержащий некоторые коэффициенты. Возникает вопрос: каким условиям должны удовлетворять эти коэффициенты, чтобы функция распределения статистики была близка к предельной функции распределения (в пределах заданной точности)?

2. **Математическая постановка задачи.** Рассматривается последовательность n люсианов A_j, $j = 1, \ldots, n$, $A_j = \{\alpha_{11}^j, \ldots, \alpha_{N1}^j, \alpha_{12}^j, \ldots, \alpha_{N2}^j, \ldots, \alpha_{1m}^j, \ldots, \alpha_{Nm}^j\}$, $N \geqslant 2$, где α_{ts}^j определены в п. 1. Проверяется гипотеза

$$H_0 : P_{ts}^j = P_{ts},\ t = 1, \ldots, N,\ s = 1, \ldots, m \text{ для любого } j. \qquad (1)$$

(В рассмотренном выше примере это соответствует согласованности мнений экспертов, т. е. тому, что вероятность классификации изделия в один класс одинакова для всех экспертов). Рассматривается асимпто-