О ВОЗМОЖНОСТИ ИТЕРАЦИИ СВЕРТОЧНЫХ КОДОВ И КОДОВ В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ

С. Н. Терентьев, В. С. Скляров
Харьков

За последнее время появилось много работ [1—5], свидетельствующих о большом интересе к использованию хороших арифметических свойств чисел, представляемых в системе остаточных классов (СОК).

Главное преимущество СОК состоит в том, что при умножении, сложении и вычитании цифра любого результанта зависит лишь от соответствующих цифр операндов. Это свойство исключает переносы в трех перечисленных арифметических операциях, устраняет необходимость получения частных произведений при умножении и открывает большие возможности при построении новой машинной арифметики, позволяющей увеличить быстродействие цифровых вычислительных машин до миллиона операций в секунду. Задача кодирования чисел в остатках признана важной не только для выполнения внутримашинных операций, но и для передачи информации по каналам связи [5].

Требование высокой достоверности, предъявляемое к получаемой по каналу связи информации при возрастающем объеме ее потоков, выдвигает задачу отыскания эффективных методов построения систем связи. Одним из методов передачи информации в позиционных системах счисления является метод последовательного кодирования и декодирования длинного ограниченного множества [6, 8, 11].

Авторы настоящей статьи пытаются выявить возможность итерации класса кодов в остатках и вероятностно-последовательного кодирования по алгоритму, предложенному Д. Возенкрафтом [6], для обеспечения эффективного обмена по каналам связи между ЦВМ непозиционного класса.

Учитывая, что представление чисел в СОК мало известно широкому читателю, для удобства дальнейшего изложения кратко рассмотрим построение кода в остатках. Код в остатках, соответствующий некоторому натуральному числу, образуется из наименьших неотрицательных вычетов этого числа относительно выбранной системы оснований.

Если $p_1, p_2, \ldots, p_k$ — целые числа, называемые основаниями, то цифрой i-го разряда α_i числа N будет наименьший положительный остаток от деления N на основание p_i

$$\alpha_i = N - \left[\frac{N}{p_i}\right] p_i. \qquad (1)$$

$$(i = 1, 2, \ldots, k)$$

Знаком [ ] обозначена целая часть результата деления N на p_i.

Чтобы обеспечить единственность представления в диапазоне $0 \div P-1$ ($P = p_1 p_2 p_3 \ldots p_k$) данного N числа p_i, системы оснований должны быть взаимно-простыми.

Основная особенность рассматриваемой системы и ее отличие от позиционных систем счисления состоит в том, что операции сложения и умножения производятся над соответствующими цифрами разрядов, отдельно по каждому разряду и независимо один от другого.

Пусть $A = (\alpha_1, \alpha_2, \ldots \alpha_k)$ и $B = (\beta_1, \beta_2, \ldots \beta_k)$ — два числа, представленных остатками α_i и β_i по основаниям p_i. Тогда, если $A + B$ и AB не выходят из диапазона $0 \div P - 1$, справедливы равенства

$$A + B = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_k + \beta_k); \quad (2)$$
$$AB = (\alpha_1\beta_1, \alpha_2\beta_2, \ldots, \alpha_k\beta_k).$$

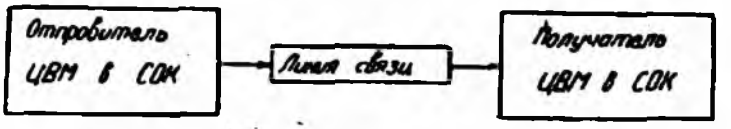

Рис. 1.

Немаловажной особенностью рассматриваемой системы кодирования является ее некоторая избыточность по сравнению с позиционной двоичной системой. Эту избыточность тривиально можно оценить отношением числа избыточных двоичных разрядов, требуемых для представления наибольшего по данной системе оснований однозначно представимого числа N^* в остатках к числу разрядов, необходимых для записи этого же числа в двоичной системе счисления. Например, для системы оснований $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ и $p_4 = 7$ диапазон однозначно представимых чисел $0 \div 209$. Для записи числа $209 = (1, 2, 4, 6) \pmod{2, 3, 5, 7}$ в СОК требуется $n_1 = 9$ разрядов, в то время как для перевода десятичного числа 209 в двоичное требуется $n_2 = 8$ двоичных разрядов. Таким образом, избыточность данной системы оснований

$$r = \frac{n_1 - n_2}{n_2} = 0{,}125.$$

Очевидно, что в зависимости от выбранной системы оснований эта избыточность будет меняться.

Г. Л. Гарнер исследовал арифметические свойства остаточных чисел, чтобы получить коды с исправлением ошибок для вычислительных машин.

В данной статье получение корректирующих кодов в СОК рассматриваться не будет. Однако будем полагать, что принципиально такие коды возможны, и при обмене данными по каналу связи между ЦВМ, работающими в СОК (рис. 1), отправитель и получатель оперируют информацией, избыточность которой определяется корректирующей способностью, необходимой для исправления ошибок при внутримашинных операциях.

Естественно, что в линиях связи ошибки имеют более сложную статистическую структуру, чем ошибки, возникающие в ЦВМ, и код, с успехом применяемый для исправления ошибок, возникающих внутри машины, не всегда может обеспечить требуемую достоверность информации, получаемой по каналу связи. Поэтому в канале связи должно производиться дополнительное кодирование (рис. 2).

С целью повышения скорости передачи информации между абонентами, соединенными каналом, пропускная способность которого медленно меняется во времени, предлагается использовать дополнительно кодер-декодер, работающий по алгоритму, предложенному Д. Возенкрафтом. В этом

случае в канале связи имеет место код, представляющий итерацию сверточного кода и кода в остатках.

Чтобы понять особенности декодирования итерационного кода, кратко остановимся на алгоритме последовательного декодирования. Древовидная структура сверточных кодов, применяемых Возенкрафтом, дает возможность сосредоточить усилия при декодировании не на выборе наиболее вероятной последовательности $\bar{s}_t$ из совокупности $|S| = 2^{n_t R_t}$, возможных на входе декодера, а на исключении всех маловероятных последовательностей $\bar{s}_t$, ввиду того, что большинство случайно выбранных из совокупности $|S|$ сообщений будет в значительной мере отличаться от полученного сообщения $\bar{y}$.



Рис. 2.

Эта процедура не является идеальной (не обеспечивает максимума правдоподобия), но она вносит упрощение в декодирование, не влияя на экспоненту усредненной по ансамблю сверточных кодов вероятности ошибки

$$\overline{Pr(\epsilon)} \leqslant A \cdot 2^{-n_t E_1(R)}, \qquad (3)$$

где A — медленно меняющаяся функция n_t;

$E_1(R)$ — функция только скорости $R = \frac{k}{n}$ и пропускной способности C.

«Маловероятная» последовательность определяется Возенкрафтом как последовательность, отличающаяся от принятого кодового слова $\bar{y}$ длины n в k_n или более символах. В двоичном симметричном канале (ДСК) без памяти исключающая функция k_n определена для заданной вероятности перехода p_0 и заданной длины кодового ограничения n_t из условия

$$\Pr[d_0(n) > k_n] \leqslant 2^{-K}, \qquad (4)$$

где K — некоторая положительная константа, называемая «вероятностным критерием»;

$d_0(n)$ — действительное число единиц в векторе ошибки $\bar{e}$ длины n.

Сверточный кодер на передающей стороне в соответствии с выбранной порождающей $\bar{g}$ формирует (n, k)-код типа свертки. Выход кодирующего устройства зависит от последнего поступившего на его вход информационного символа и от $(k-1)$ предшествующих ему символов. Схема канонического сверточного кодера со связями, соответствующими порождающей, равной 111011001011001 $\left(\text{для } R_t = \frac{1}{3}\right)$, приведена на рис. 3.

Последовательный декодер содержит точную копию устройства сверточного кодирования и производит выбор пути по разветвлениям кодового дерева. Он вырабатывает гипотетическую последовательность $\bar{s}_i$ и сравнивает ее с соответствующей последовательностью $\bar{r}_t = \bar{s}_t \oplus \bar{e}$ та-

кой же длины. Если на длине $L = k$ выполняется условие $d_0(L) < k_n(I)$, то самый «старый» символ m_s^* последовательности $\overline{s_i^*}$ считается декодированным по данному критерию I, после чего «расширением» устройство приступает к декодированию следующего информационного символа m_{s+1}^*. Если же при попытке «расширением» декодировать символ m_{s+1}^* хеммингово расстояние между $\overline{s_{i+1}^*}$ и $\overline{r_{i+1}}$ удовлетворяет неравенству

$$d_0(L) > k_n(I), \tag{5}$$

то декодер переходит в режим поиска. Упрощенная диаграмма цикла управления поиском в устройстве *SECO* [11] для $k = 60$ изображена на рис. 4.

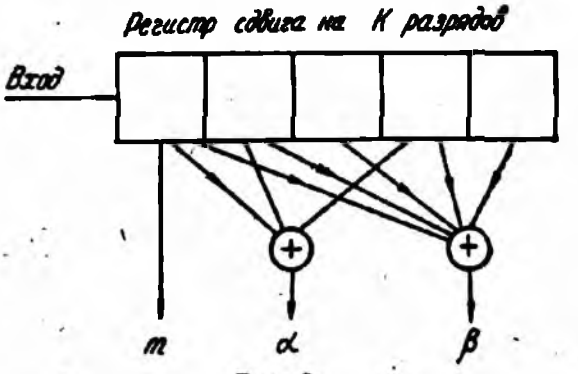

Рис. 3.

Из логической структуры операции поиска следует, что при большом количестве ошибок в канале связи ветвь, предполагаемая верной по критерию I, может уточняться до длины $L = 1$, после чего номер критерия увеличивается на единицу и поиск правильной ветви возобновляется. С увеличением I возрастает длительность процесса поиска, поскольку мы требуем уменьшения вероятности выполнения события $d_0(L) > k(I + \tau)$.

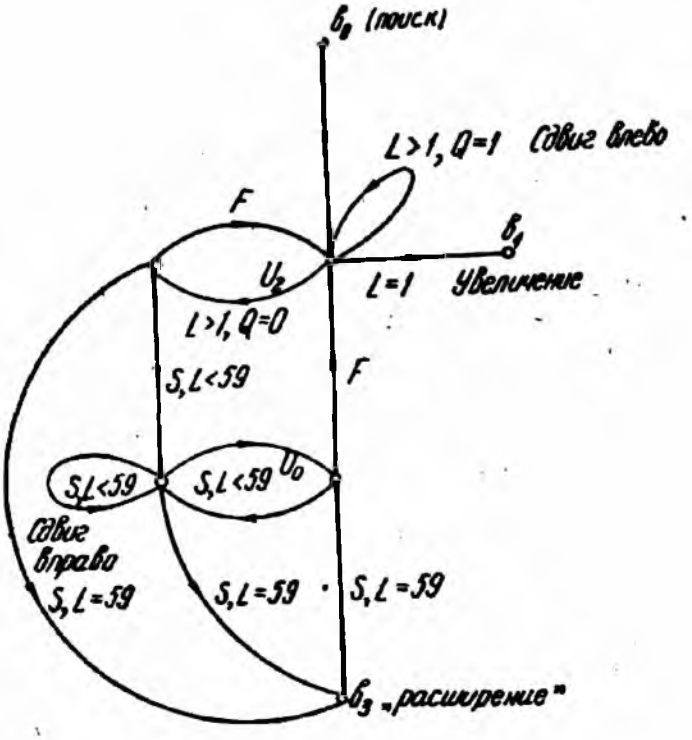

Рис. 4.

Несмотря на то, что вероятность первой ошибки определяется экспонентой выражения (3), ошибка все же может произойти и привести декодер к режиму поиска, характеризуемому вспышкой вычислений.

Резкий рост требуемого объема вычислений, возникающий при приближении R_t к $R_{вых}$ означает, что окончательные ограничения на скорость передачи данных накладываются рабочей скоростью декодирующей вычислительной машины [6].

В предположении, что код СОК позволяет исправить любые одиночные (по одному основанию) ошибки, проанализируем структуру устройства для декодирования итерационного кода (рис. 5). На передающей стороне кодирование информации осуществляется сверточным кодером, ничем не отличающимся от кодера, изображенного на рис. 3. На приемной стороне информация из линии связи поступает на линейный буфер декодера. Порождение гипотетической последовательности производится с задержкой на k тактов, необходимых для выделения кода СОК на первую проверку.

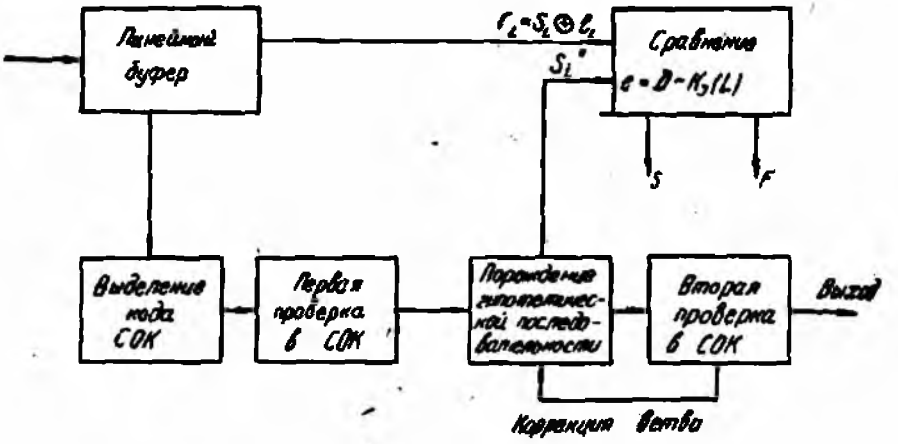

Рис. 5.

Информация, скорректированная первой проверкой в СОК, поступает на кодер декодера, порождающий гипотетическую последовательность. Дальнейший алгоритм декодирования ничем не отличается от описанного выше алгоритма последовательного декодирования. После того как будет декодировано $n_t R_t$ символов, т. е. с выхода последовательного декодера получим декодированный блок СОК, производим вторую проверку в СОК, аналогичную первой, с той лишь разницей, что информация, поступающая на вторую проверку, имеет вероятность ошибки, определяемую выражением (3). Предположим, что кодирование ведется так, что длина кодовых ограничений $n_t R_t \approx 100$ и $\Pr(\varepsilon) \leqslant 10^{-13}$, тогда блок СОК перед второй проверкой будет поражен одной ошибкой с вероятностью примерно 10^{-11}.

Считая ошибки независимыми, оценим вероятность ошибки в блоке длиной $n_t R_t$ после исправления одиночной ошибки второй проверкой в СОК

$$\Pr^*(\varepsilon) \approx C_{100}^2 \Pr^2(\varepsilon') q^{98} \approx 5 \cdot 10^{-19}.$$

После коррекции ветви второй проверкой декодер производит последовательное декодирование следующего блока СОК. Таким образом, вторая проверка в СОК резко уменьшает вероятность возврата с поиском для уточнения декодированного участка ветви, или, другими словами, применение второй проверки в СОК позволяет резко увеличить скорость декодирования, что в конечном итоге увеличивает скорость передачи данных R_t.

ЛИТЕРАТУРА

1. И. Я. Акушский. Арифметические операции в системе остаточных классов. «Вопросы радиоэлектроники», вып. 3, серия VII, 1960.

2. И. М. Виноградов. Основы теории чисел. Гостехиздат, 1953.

3. H. L. Garner. Error checking and the structure of binary addition, Ph. D. Diss. Univ. Michigan, Ann. Arbor, Mich. 1958.

4. H. L. Garner. The residue number system, IRE Trans. an Electronic Comput., EC — 8 (1959), June.

5. А. Свобода. Система счисления остаточных классов. «Кибернетический сборник». Изд-во «Мир», 1964, № 8.

6. Р. Фано. Передача информации. Статистическая теория связи. Изд-во «Мир», 1963.

7. Д. Возенкрафт, В. Рейффен. Последовательное декодирование. Изд-во иностр. лит-ры, 1963.

8. Р. Фано. Эвристическое обсуждение вероятностного декодирования. Сб. «Теория кодирования». Изд-во «Мир», 1964.

9. М. С. Пинскер. О сложности декодирования. «Проблемы передачи информации», т. 1, вып. 1, 1965.

10. У. Питерсон. Коды, исправляющие ошибки. Изд-во «Мир», 1964.

11. Перри. Д. Возенкрафт. *SECO* — саморегулирующееся кодирующее-декодирующее устройство с исправлением ошибок. «Зарубежная радиотехника», 1964. № 9.