К. т. н. И. В. ИВАНОВА

Россия, г. С.-Петербург, Северо-Западный гос. заочный технический университет
E-mail: rilala_spb@mail.ru

Дата поступления в редакцию
20.05 2005 г.

Оппонент *к. т. н. И. А. КИРЕЕВ*
(ОНАС, г. Одесса)

КЛАССИФИКАЦИЯ И СИНТЕЗ ПОЛИНОМИАЛЬНЫХ КОДЕКОВ В СИСТЕМАХ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ДАННЫХ

Рассматриваются структуры кодеков. Показаны перспективы развития гибридной реализации кодека: временной кодер — гибридный декодер.

Одна из наиболее трудных задач в технике передачи информации — обеспечение достаточной помехоустойчивости. Широкому распространению высокоэффективных помехоустойчивых кодов с обнаружением и исправлением ошибок препятствует сложность практической реализации устройств декодирования.

Различные типы кодов описаны в [1—8], их многообразие отражено на **рис. 1**.

Важным и широко используемым подмножеством кодов Боуза–Чоудхури–Хоквингема (БЧХ) являются коды Рида–Соломона. Это такие коды БЧХ, у которых мультипликативный порядок алфавита символов кодового слова делится на длину кода. Доказано [5], что не существует кода, у которого минимальное расстояние больше, чем у кода Рида–Соломона. Этот факт часто является определяющим для использования кода Рида–Соломона (РС). Коды РС всегда оказываются короче всех других циклических кодов над тем же алфавитом. Коды РС это такие коды БЧХ над полем Галуа $GF(q)$, длина которых n равна q–1. Они не только являются хорошей иллюстрацией кодов БЧХ, но и сами представляют значительный практический и теоретический интерес. На их основе удобно строить другие коды — либо используя только сами коды РС, например отображая их в двоичные, либо используя в каскадных кодах [1].

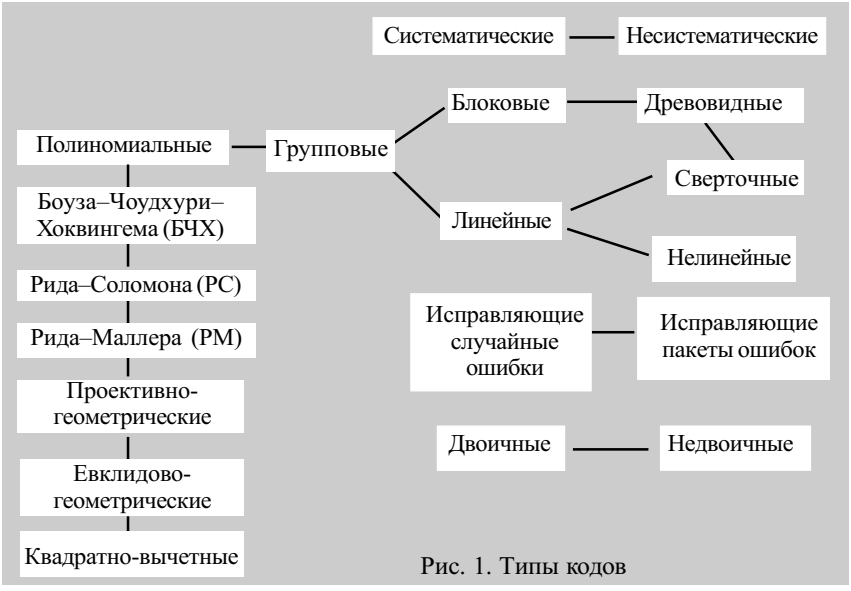


Рис. 1. Типы кодов

Процесс кодирования состоит в том, что наборы k информационных символов отображаются в кодовые последовательности, состоящие из $n>k$ символов. Любое такое отображение будем называть (n, k)-кодом. Кодовое слово (n, k)-кода представляется в виде набора длиной n: (a_0, a_1, …, ..., a_{n-1}) или многочлена

$$f(x)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}.$$

Полиномиальный код можно определить как множество всех многочленов степени, не большей n–1, содержащее в качестве множителя некоторый фиксированный многочлен $g(x)$. Многочлен $g(x)$ называется порождающим многочленом кода.

Ошибки в рассматриваемых кодах исправляются путем решения систем алгебраических уравнений.

Блоковое кодирование состоит в том, что последовательность символов источника сообщений (a_1, a_2,…) разбивается на блоки, например по k символов в каждом:

$$\boldsymbol{a_1}=(a_1, a_2,\ldots, a_k),\ \boldsymbol{a_2}=(a_{k+1}, a_{k+2},\ldots, a_{2k}),\ldots$$

Кодер преобразует каждый входной k-блок $\boldsymbol{a_i}$ в выходной n-блок

$$\boldsymbol{x_i}=x(a_i)=(x_1(a_i),\ldots, x_n(a_i))$$

таким образом, чтобы различным входным блокам соответствовали различные выходные (n=k). Совокупность $\boldsymbol{C}$ всех различных $\boldsymbol{x(a)}$ называется блоковым кодом длины n и мощности $M=q^k$. Скорость кода в q-ичных единицах измерения

$$R=[\log_q M]/n=k/n.$$

Критерием качества кода является кодовое расстояние

$$d(x, y)=|x-y|,$$

определяющее способность кода исправлять ошибки [1—3, 8].

Любое линейное подпространство $\boldsymbol{C}$ можно задать с помощью базиса из k линейно независимых векторов ($1=k=n$), где k называют

размерностью подпространства. *Линейным* (n, k)-кодом называют k-мерное линейное подпространство. Линейный код может быть задан порождающей матрицей кода:

$$G=\begin{bmatrix} g_{11} & g_{12} & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & g_{2n} \\ & & \cdots & \\ g_{k1} & g_{k2} & \cdots & g_{kn} \end{bmatrix}.$$

Тогда кодовый вектор имеет вид

$\boldsymbol{g=aG}$.

Линейный код можно определить как множество решений

$\boldsymbol{gH^T=0}$,

где $\boldsymbol{H}$ — проверочная матрица кода $\boldsymbol{GH^T=0}$.

Современное состояние теории линейных кодов отражено в [1, 5—8]. Совокупность векторов $\boldsymbol{U}=(u_0, u_1,\ldots, u_{n-1})$ образует циклический (n, k)-код, если все соответствующие многочлены $u(x)=u_0+u_1x+\ldots+u_{n-1}x^{n-1}$ содержат в качестве корней $\beta_1, \beta_2,\ldots, \beta_n$.

Пусть $g(x)$ содержит серию последовательных корней $\beta^b, \beta^{b+1}, \beta^{b+\delta-2}$, где β — примитивный корень, т. е. $\beta^n=1$, $\beta^s\neq1$, $s<n$. Код, порождаемый этим многочленом, называется кодом Боуза–Чоудхури–Хоквингема (БЧХ-кодом), для него $k\geq n-m(\delta-1)$ и $d\geq\delta$. Как уже было отмечено, важным частным случаем БЧХ-кодов являются коды Рида–Соломона (РС), которые имеют следующие параметры: $n=q-1$, $k=n-d+1$, $d=\delta$. Таким образом, коды РС являются разделимыми с максимальным расстоянием (достигается равенство $d\leq n-k+1$).

Интерес к этому классу линейных кодов обусловлен вышеуказанными причинами, а также тем, что он используется в конструкциях обобщенных каскадных кодов [9, 10] для исправления многократных пакетов ошибок и имеет эффективный алгебраический метод декодирования.

Известно [9], что код РС над полем $GF(q)$ — это код, состоящий из всех слов $(f_0, f_1,\ldots, f_{n-1})$ длины n, для которых выполняются $d-1$ уравнений

$$\sum_{i=0}^{n-1} f_i\alpha_i^m=0,\ f_{ii}\in GF(q),\ m_0\leq m\leq m_0+d-2, \qquad (1)$$

где m_0 и d — произвольные целые числа (не больше n);
$\alpha_0, \alpha_1,\ldots, \alpha_{n-1}$ — различные ненулевые элементы поля $GF(q)$ (локаторы i-й позиции слова).

Принадлежность кодов РС к классу максимальных кодов следует из свойств его проверочной матрицы:

$$\begin{vmatrix} \alpha_0^{m_0} & \alpha_1^{m_0} & \ldots & \alpha_{n-1}^{m_0} \\ \alpha_0^{m_0+1} & \alpha_1^{m_0+1} & \ldots & \alpha_{n-1}^{m_0+1} \\ & & \ldots & \\ \alpha_0^{m_0+r-1} & \alpha_1^{m_0+r-1} & \ldots & \alpha_{n-1}^{m_0+r-1} \end{vmatrix} = \begin{vmatrix} 1 & 1 & \ldots & \\ \alpha_0 & \alpha_1 & \ldots & \\ & & \ldots & \\ \alpha_0^{r-1} & \alpha_1^{r-1} & \ldots & \end{vmatrix} \cdot \begin{vmatrix} \alpha_0^{m_0} & 0 & \ldots & 0 \\ 0 & \alpha_1^{m_0} & \ldots & 0 \\ & & \ldots & \\ 0 & 0 & \ldots & \alpha_{n-1}^{m_0} \end{vmatrix},$$

где $r=n-k$.

Любые r столбцов матрицы $\boldsymbol{H}$ линейно независимы и образуют матрицу Вандермонда. Отсюда следует, что для любого заданного набора локаторов и любых значений k символов кодового слова система линейных уравнений над $GF(q)$ имеет единственное решение относительно оставшихся $r=n-k$ неизвестных, которое может быть найдено, например, методом Гаусса.

Циклический код РС состоит из всех многочленов степени меньше n над $GF(q)$, корнями которых являются элементы $\{\beta^{m_0+i}\}$, $i=\overline{0,r-1}$, где $\beta\in GF(q)$, $\beta^n=1$ и n кратно $q-1$. Это свойство циклических кодов РС интересно тем, что оно позволяет определить сам код и его декодирование в терминах преобразования Фурье над конечным полем. Выбирая подходящую систему обозначений, можно показать, что вычислительные задачи, составляющие основу приложений методов контроля ошибок, — это те же вычисления сверток, преобразований Фурье и обращений теплицевых систем уравнений, хотя и в другой числовой системе, называемой полем Галуа [11].

Порождающим многочленом (n, k, d)-кода РС называется многочлен степени $(d-1)(\deg(d-1))$;

$$g(x)=(x-\beta^{m_0})(x-\beta^{m_0+1})\ldots(x-\beta^{m_0+d-2}).$$

Проверочным называется многочлен степени k, удовлетворяющий условию

$$h(x)g(x)=0(\mathrm{mod}\ x^n-1).$$

Пусть $(u_0, u_1,\ldots, u_{n-1})$ — принятая последовательность символов на выходе дискретного канала, где $u_i=f_i+e_i$, f_i — символ кодового слова и $e_i\in GF(q)$ — значения ошибок. Обнаружение ошибок состоит в проверке условий (1) для принятого слова. Назовем синдромом вектор $(S_0, S_1,\ldots, S_{d-2})$, где

$$S_j\sum_i u_i\alpha_i^{m_0+j},\ j=\overline{0,d-2}. \qquad (2)$$

Одним из методов декодирования кодов РС является декодирование по максимуму правдоподобия, которое состоит в решении следующей задачи: для заданного u найти слово $f\in C$, максимизирующее условную вероятность $P(u/f)$ [12].

Рассмотрим алгебраический метод декодирования (n, k, d)-кода РС, исправляющего любые комбинации ошибок веса не более $(d-1)/2$. Пользуясь определением синдрома (2), можно построить многочлен

$$S(x)=\sum_{j=0}^{r-1}S_jx^j=\sum_{j=0}^{r-1}x^j\sum_{i=0}^{n-1}e_i\alpha^{m_0+j},$$

где $r=n-k$.

Производя некоторые преобразования [7], приходят к уравнению, которое обычно называют ключевым уравнением:

$$S(x)\sigma(x)\equiv\omega(x)(\mathrm{mod}\ x^r),$$

где $\sigma(x)$ — многочлен локаторов ошибок; $\deg\sigma(x)$, если $t<r$;
$\omega(x)$ — многочлен значений ошибок; $\deg\omega(x)<\deg\sigma(x)$.

Решение ключевого уравнения можно искать с помощью алгоритмов Евклида или Берлекэмпа–Месси. Алгоритм Евклида для произвольной пары (a, b) целых чисел (или многочленов) дает решение уравнения

$$aQ+bP=d,$$

где d — наибольший общий делитель (НОД) пары (a, b) [7].

На практике для решения ключевого уравнения обычно используется алгоритм Берлекэмпа–Месси, который синтезирует минимальный регистр с обрат-

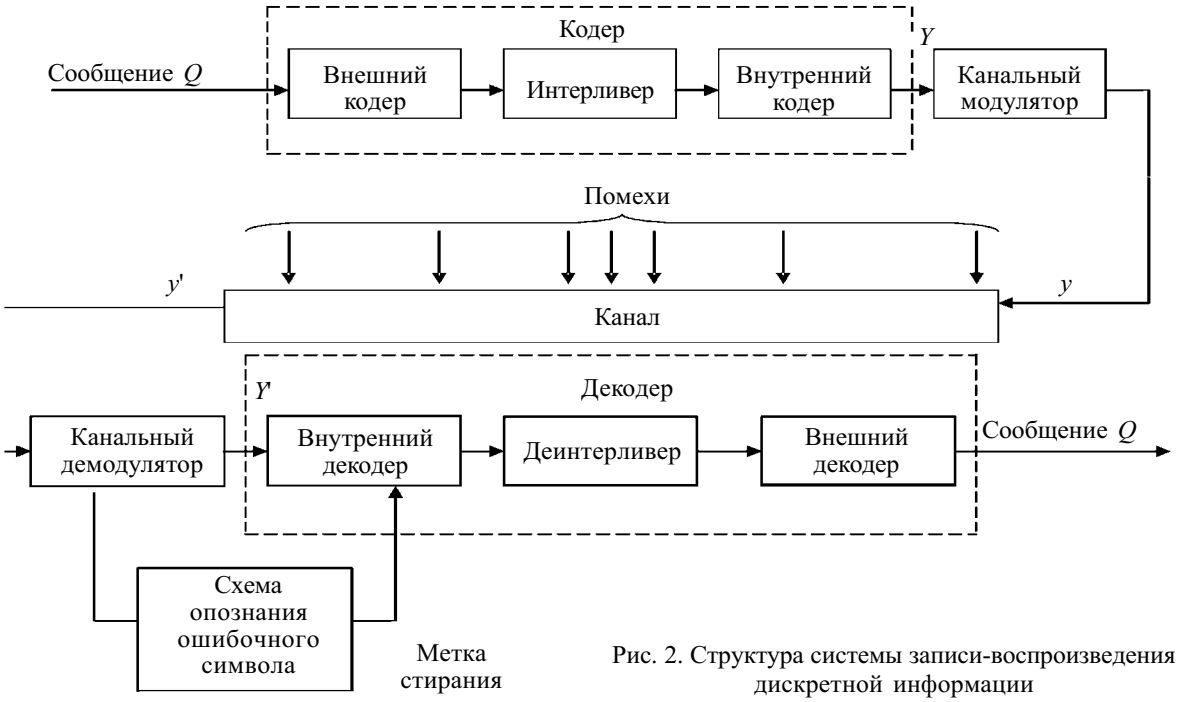


Рис. 2. Структура системы записи-воспроизведения дискретной информации

ной связью, порождающий заданную последовательность символов [3].

Обобщенная структура системы записи-воспроизведения цифровой информации (на диске, полупроводниковом запоминающем устройстве) приведена на **рис. 2**. Кодер преобразует сообщение Q в кодовое слово V, которое подвергается канальной модуляции. В системах записи-воспроизведения цифровой информации модулятор представляет собой логическую комбинационную схему, задача которой — преобразование кодовых символов.

Декодер исправляет стирания и ошибки, если их число не нарушает условия

$$d \geq 2\tau+\nu+1,$$

где d — кодовое расстояние кода;
τ — число стираний;
ν — число ошибок.

Повысить кодовое расстояние d кода можно при каскадировании. Кодер и декодер на рис. 2 изображены двухкаскадными [9, 10, 13].

В качестве кодов в обоих каскадах целесообразно использовать коды Рида–Соломона над полем $GF(2^r)$.

Как отмечалось выше, кодировать и декодировать РС-коды над бесконечными полями можно во временной и в частотной областях. Сказанное справедливо и для конечных полей.

Обобщенные структуры кодеров и декодеров изображены на **рис. 3**—**6**.

Кодирование во временной области осуществляется с помощью порождающей матрицы или порождающего полинома. В этом случае кодирование может быть как несистематическим, так и систематическим. В частотной области кодирование всегда несистематическое.

Особенность временного декодера (рис. 4) — раздельное вычисление позиций и величин ошибок. Для этого приходится решать: а) степенное уравнение локаторов; б) систему линейных уравнений относительно величин стираний (после того как найдены позиции ошибок, последние переходят в разряд стираний).

Частотное декодирование (рис. 5) не требует решения указанных уравнений, т. к. позволяет непосредственно найти спектр E конфигурации ошибок, вычисляемый как продолжение синдрома (ганкелевой матрицы). Недостаток данной структуры — невозможность косвенного контроля выделенного сообщения Q, т. к. ошибка в блоке преобразования Фурье–Мэттсона–Соломона (ФМС) не может быть обнаружена и исправлена без повторных ФМС-преобразований аналогичными блоками.

Гибридная структура на рис. 6 согласуется с временным кодером. Рекуррентное продолжение характерно для частотного декодирования. Далее осуществляется обратное ФМС-преобразование синдрома

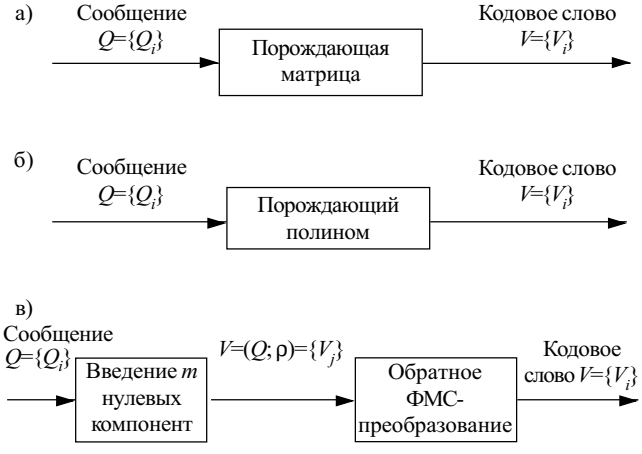


Рис. 3. Обобщенные структуры кодеров РС-кодеров: во временной области — линейного (*а*) и циклического (*б*); в частотной области — *в*;
$i=1, 2, ..., k$; $j=1, 2, ..., n=k+m$; $\rho=(0...0)m$ нулей

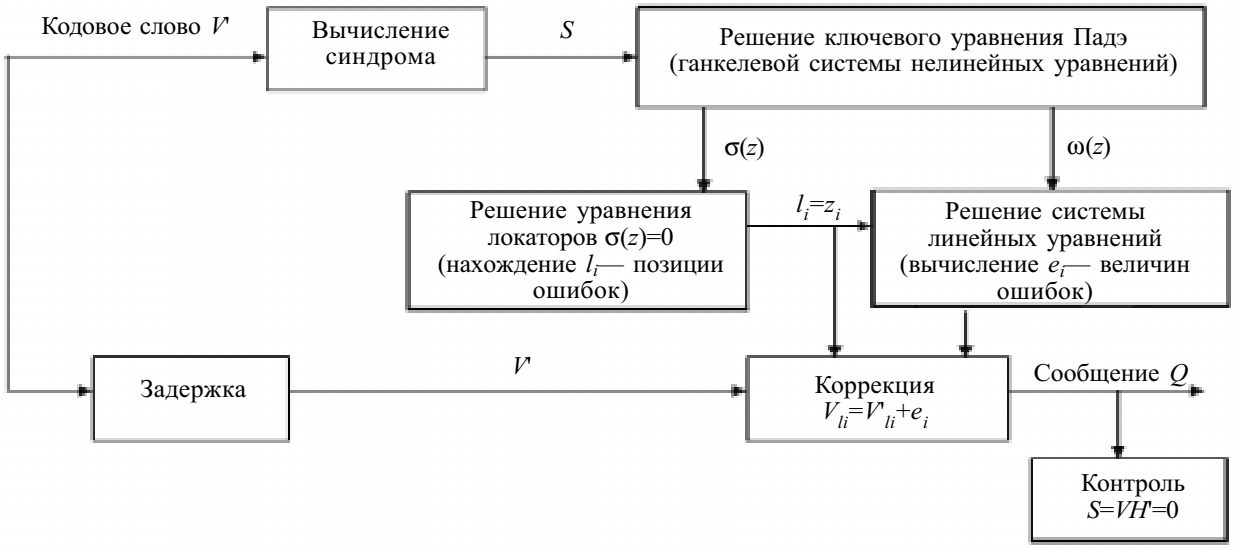


Рис. 4. Временная структура декодеров:

$S=(S_0, S_1, ..., S_{m-1})$; $C=(C_0, C_1, ..., C_k, ..., C_{n-1})$; $E=(E_0, E_1, ..., E_k, ..., E_{n-1})$; $C_k=S_0=E_k$, $C_{k+1}=S_1=E_{k+1}$, ..., $C_{n-1}=S_{m-1}=E_{n-1}$

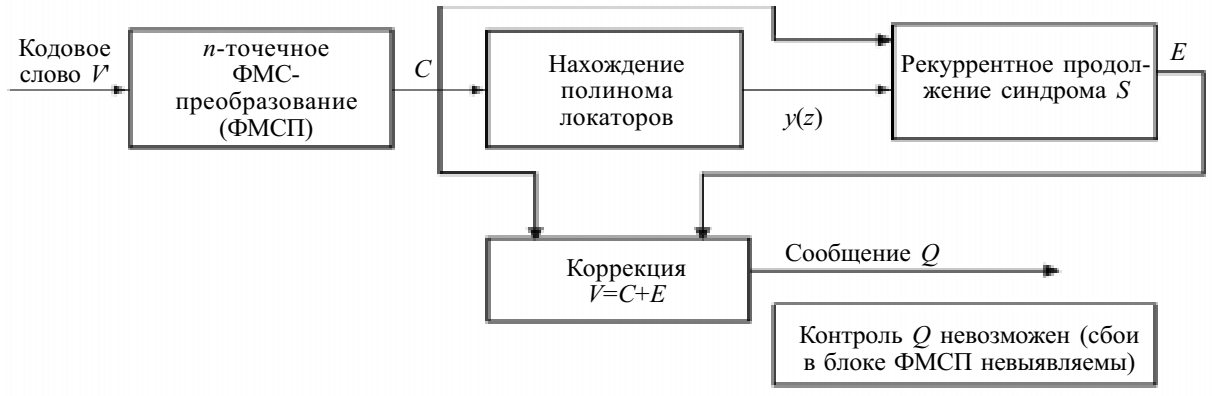


Рис. 5. Структурная схема частотного декодирования:

$S=(S_0, S_1, ..., S_{m-1})$; $C=(C_0, C_1, ..., C_k, ..., C_{n-1})$; $E=(E_0, E_1, ..., E_k, ..., E_{n-1})$; $C_k=S_0=E_k$, $C_{k+1}=S_1=E_{k+1}$, ..., $C_{n-1}=S_{m-1}=E_{n-1}$

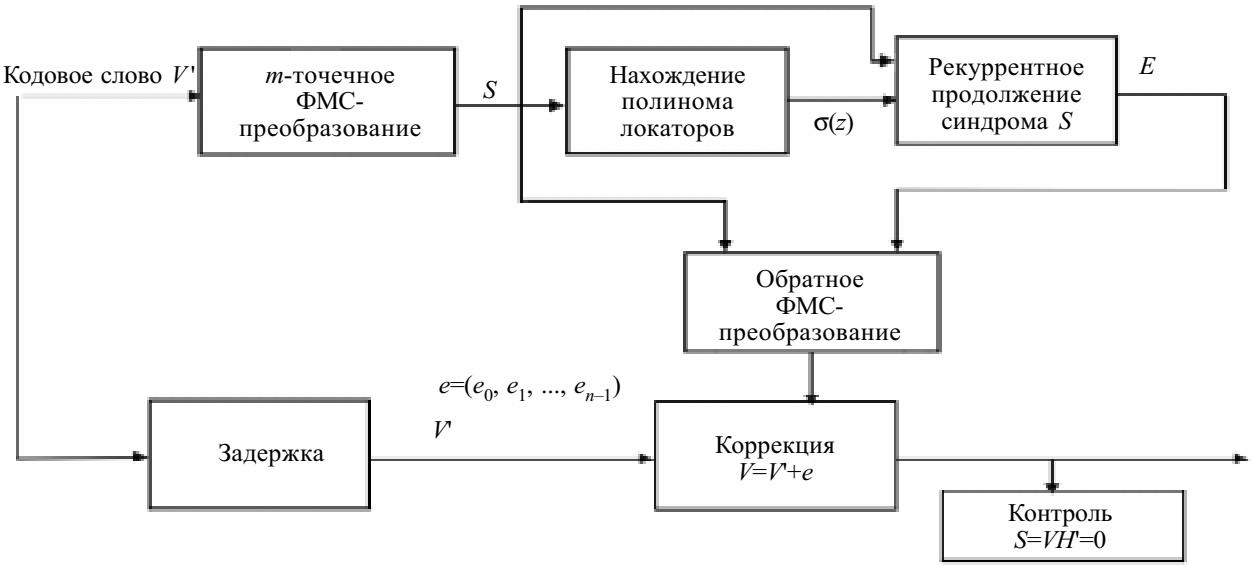


Рис. 6. Гибридная (частотно-временная) структура декодеров:

$S=(S_0, S_1, ..., S_{m-1})$; $C=(C_0, C_1, ..., C_k, ..., C_{n-1})$; $E=(E_0, E_1, ..., E_k, ..., E_{n-1})$; $C_k=S_0=E_k$, $C_{k+1}=S_1=E_{k+1}$, ..., $C_{n-1}=S_{m-1}=E_{n-1}$

S, удлиненного его продолжением *C*, что дает временной вектор *e* ошибок.

Исследования [5—7, 11] показали, что наиболее перспективна именно смешанная реализация кодека: временной кодер — гибридный декодер; причем для прямого и обратного ФМС-преобразования могут быть использованы быстрые алгоритмы.

***

Упрощение схемной реализации позволяет широко использовать высокоэффективные помехоустойчивые коды с обнаружением и исправлением ошибок. Внедрение таких устройств приведет к повышению вероятности обнаружения ошибок в системах автоматизированной обработки данных.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки.— М.: Связь, 1979.

2. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки.— М.: Мир, 1976.

3. Берлекэмп Э. Алгебраическая теория кодирования.— М.: Мир, 1971.

4. Блох Э. Л., Зяблов В. В. Обобщенные каскадные коды: алгебраическая теория и сложность реализации.— М.: Связь, 1976.

5. Блейхут Р. Теория и практика кодов, контролирующих ошибки.— М.: Мир, 1986.

6. Кларк Дж., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи.— М.: Радио и связь, 1987.

7. Габидулин Э. М., Афанасьев В. Б. Кодирование в радиоэлектронике.— М.: Радио и связь, 1986.

8. Теория кодирования / Т. Касами, Н. Токура, Е. Ивадари, Я. Инагаки.— М.: Мир, 1978.

9. Форни Д. Каскадные коды.— М.: Мир, 1970.

10. Блох Э. Л., Зяблов В. В. Линейные каскадные коды.— М.: Наука, 1982.

11. Блейхут Р. Э. Алгебраические поля, обработка сигналов, контроль ошибок // ТИИЭР.— 1985.— Т. 73, № 5.— С. 30—53.

12. Евсеев Г. С. К вопросу о сложности декодирования линейных кодов / Тр. V Междунар. симп. по теории информ. Ч. I.— Москва—Тбилиси.— 1979.— С. 139—141.

13. Морелос–Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение.— М.: Техносфера, 2005.

НОВЫЕ КНИГИ

НОВЫЕ КНИГИ

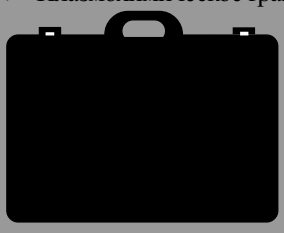
Денисенко А. Н. Сигналы. Теоретическая радиотехника. (Справочное пособие.)— М.: Горячая линия–Телеком, 2005.— 704 с.

В достаточно сжатой и приемлемой для инженерной и исследовательской практики форме обобщены и достаточно полно изложены методы анализа детерминированных сигналов (часть 1) и случайных сигналов и шумов (часть 2), используемые в теоретической радиотехнике. В каждом разделе теоретическая часть заканчивается расчетными выражениями и примерами расчета по ним.

Для инженеров и исследователей, работающих в области радиотехники, преподавателей, студентов старших курсов радиотехнических факультетов вузов, аспирантов.

в портфеле редакции в портфеле редакции в портфеле редакции в портфеле редакции

- Сетевая система контроля технологического процесса выращивания полупроводниковых кристаллов и тонких пленок. (Украина, г. Черновцы)
- Некоторые вопросы проектирования микросхем широкополосных усилителей. (Украина, г. Киев)
- Моделирование амплитудно-частотных характеристик электромеханических фильтров с использованием метода электромеханических аналогий. (Украина, г. Алчевск)
- Установка для регенерации сорбентов в электромагнитном поле. (Украина, г. Харьков)
- Состояние и перспективы развития метода ионно-плазменного, магнетронного распыления материалов в вакууме применительно к микро- и наноэлектронике. (Грузия, г. Тбилиси)
- Методы синдромного декодирования кодов Рида–Соломона, основанные на вычислениях особых продолжений ганкелевых матриц. (Россия, г. Санкт-Петербург)
- Экспериментально-расчетная методика определения характеристик встречнообратновключенных переходов. (Узбекистан, г. Ташкент)
- Использование термозащитных пленочных покрытий на основе AlN в электронной технике. (Россия, г. Москва, г. Пермь)
- Зависимость свойств толстопленочных терморезисторов от состава базовой шпинели. (Украина, г. Львов, г. Дрогобыч)
- Плазмохимическое травление эпитаксиальных структур нитрида галлия. (Украина, г. Киев; Россия, г. Москва)



- Проектирование трансформаторов для балансных кольцевых смесителей. (Украина, г. Киев)
- Измерение толщины покрытий с помощью емкостных датчиков. (Россия, г. Рыбинск)
- Принципиально новая технология изготовления элементов узлов систем связи и навигации. (Украина, г. Днепропетровск)
- Широкополосные трансформаторы для интегральных схем в технологии LTCC. (Украина, г. Киев)

в портфеле редакции в портфеле редакции в портфеле редакции в портфеле редакции