*УДК 621.391.0319.3*

*Незгазинская Н.В.*
*Незгазинська Н.В.*
*Nezgazinskaja N.V.*

# МЕТОД ПОИСКА ПОРОЖДАЮЩИХ МНОГОЧЛЕНОВ И АНАЛИЗА ХАРАКТЕРИСТИК СВЕРТОЧНЫХ КОДОВ

# МЕТОД ПОШУКУ ПОРОДЖУВАЛЬНИХ БАГОТОЧЛЕНІВ ТА АНАЛІЗУ ХАРАКТЕРИСТИК ЗГОРТКОВИХ КОДІВ

# THE METHOD OF GENERATING POLYNOMIALS SEARCH AND CHARACTERISTICS CONVOLUTIONAL CODES ANALYSIS

***Аннотация.*** *В статье разработан метод поиска порождающих многочленов и анализа характеристик сверточных кодов, основанный на использовании новой концепции «тест-пакета». Метод предназначен для исследования свойств рекурсивных сверточных кодов.*

***Анотація.*** *В статті розроблено метод пошуку породжувальних багаточленів та аналізу характеристик згорткових кодів, базований на використовуванні нової концепції «тест-пакета». Метод призначено для дослідження властивостей рекурсивних згорткових кодів.*

***Summary.*** *In article the search method of generating polynomials and the analysis of characteristics convolutional codes, based on using of new concept of a «test-package», is developed. Method is for research of recursive convolutional codes properties intended.*

Сверточные коды (СК) широко применяются в современных цифровых телекоммуникационных системах для решения проблемы повышения помехоустойчивости при действии различных помех [1 – 4]. Наиболее популярным является сочетание сверточного кодирования с алгоритмом декодирования А. Витерби [5, 6]. При этом типично использование нерекурсивных сверточных кодов (НСК) (генерируемых кодерами без обратной связи). Вместе с тем в последнее время особое внимание обращено на рекурсивные сверточные коды (РСК) ввиду их явного преимущества перед нерекурсивными кодами. Особый интерес к РСК проявляется при реализации турбокодов [5, 7].

Традиционным и широко используемым методом отыскания порождающих многочленов является переборный поиск [4], теория которого в настоящее время для порождающих многочленов СК пока не разработана. А также, в известной нам литературе, отсутствуют справочные сведения о порождающих многочленах РСК. Поэтому цель настоящей работы – разработать метод переборного поиска, предназначенного для поиска рекурсивных порождающих многочленов СК.

**1. Основные параметры рекурсивных сверточных кодов.** На рис. 1 представлена структурная схема кодера РСК (систематический СК со скоростью 1/3), используемого в составе аппаратуры перспективной системы мобильной связи *UMTS* [5].

На рис. 1 прямые связи в схеме кодера показаны сплошными линиями, а обратная связь отмечена штрихами. Анализ показывает, что переход к рекурсивным кодам позволяет существенно упростить реализацию алгоритма Витерби вследствие специфических особенностей РСК (в сравнении с нерекурсивными кодами). Для исследования характеристик РСК мы использовали программы, разработанные в пакете объектно-ориентированного визуального программирования *HP VEE.*

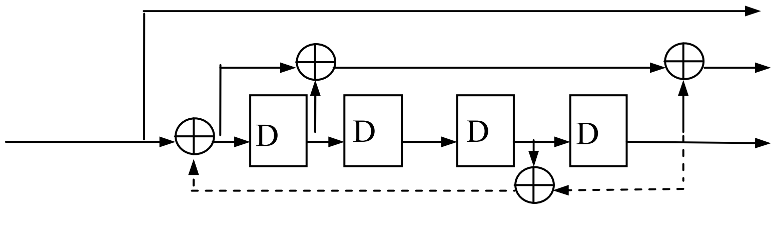


Рисунок 1 – Структура рекурсивного сверточного кодера:
D – элемент задержки на такт; + – сумматор по модулю 2

**2. Спектр расстояний сверточных кодов.** Одной из важных характеристик СК является спектр расстояний, позволяющий призводить сравнение различных кодов по критериям помехоустойчивости, а также оценивать характеристики вновь найденных кодов в сравнении с известными.

Сведения о спектрах расстояний лучших двоичных нерекурсивных СК опубликованы в многочисленных справочных таблицах кодов [3 – 4]. Эти сведения получены различными авторами в процессе переборного поиска. Известны два метода расчета спектра расстояний:

– аналитический метод порождающих функций,

– вычислительный метод матрицы смежностей, описанный в монографии [2, с. 84 – 85]. Метод предназначен для вычисления членов ряда порождающей функции СК на основе многократного умножения матрицы смежностей диаграммы состояний СК.

Эти методы достаточно громоздки, требуют затрат ручного труда на составление графа диаграммы состояний СК и поэтому трудно применимы на практике. Ниже дано описание простого и легко реализуемого метода для определения спектра расстояний СК, основанного на описанной ниже концепции тест-пакета.

**3. Метод тест-пакета.** Концепция использования тест-пакета базируется на известных положениях теории сверточных кодов. Описанный метод и реализующая его программа [8] подвергались тестированию на примерах ряда кодов, для которых данные спектра расстояний опубликованы в справочных таблицах [2, 4] и могут быть определены аналитически на основе диаграммы состояний или метода порождающих функций [2].

**4. Переборный поиск порождающих многочленов СК.** Как отмечалось во введении, многочлены лучших СК отыскиваются переборным способом. Для организации перебора порождающих многочленов необходимо выполнение ряда условий:

1. Алгоритм перебора должен содержать блок вычисления параметра кода, по которому производится переборный поиск (например, свободное расстояние СК $d_f$).

2. Должен быть сформулирован критерий поиска:

– критерий ($d_f = L$) – равенство расстояния заданной величине $L$;

– критерий ($d_f > L$) – превышение расстоянием заданного порога $L$.

3.Должна быть обеспечена полнота перебора с гарантией отсутствия пропусков.

4. Поскольку многие переборные методы требуют определенных расходов времени на производство вычислений, должны быть предприняты меры по сокращению времени вычислений.

Рассмотрим возможности сокращения объема полного перебора. Если объем алфавита отыскиваемого кода есть $M$ и количество отводов от регистра кодера есть $K$, то количество всех возможных вариантов порождающих многочленов кода есть $N = M^K$ и полный перебор всех $N$ вариантов длинных кодов становится громоздким и может занимать значительное время. Задача сокращения объема в этом случае является родственной известной задаче сокращения объема вычислений при декодировании длинных сверточных кодов. Конструктивное решение такой задачи в теории кодирования найдено в виде алгоритма последовательного декодирования [6]. В то же время алгоритм последовательного декодирования есть вариант известного алгоритма ветвей и границ из теории трудоемкости вычислительных алгоритмов, приспособленного для решения задачи последовательного декодирования СК. Используем идеи метода ветвей и границ. Пусть процесс поиска кода по критерию($d_f > L$) изображается рис. 2. Показаны затраты времени но полный перебор $N$. Искомый код с максимальным свободным расстоянием $d_{f\max}$ (отмечен штриховкой) находится в пределах этого интервала $N$. Обнаружение этого кода возможно на основе последовательного просмотра кодов одного за другим. Процесс просмотра прекращается, когда свободное расстояние кода $d_f$ превысит заранее заданный порог $L$. Затем данные о найденном многочлене кода выводятся на печать. Вообще говоря, время $N_i$ до обнаружения кода с $d_{f\max}$ всегда меньше либо равно времени полного перебора $N$ (искомый код может находиться на правом конце интервала $N$), но некоторые значения $N_i$ могут быть меньше $N$, что позволяет надеяться на то, что в среднем затраты времени на поиск будут меньше $N$, чем и привлекает такой способ организации процесса поиска.

Степень экономии можно оценить аналитически. Пусть в каждом из моментов «испытания кода» условие ($d_f > L$) выполняется с вероятностью $p_i$. Считая события выполнения неравенства ($d_f > L$) равновероятными ($p_i$ = const), определим среднюю длину интервала до момента отыскания оптимального кода. Из рис. 2 следует, что до момента обнаружения (отмечен штриховкой) с вероятностью $p_i$ происходят моменты «необнаружения» с вероятностью $(1 - p_i)$. Нетрудно показать, что вероятность пакета событий длиной $N_i$, начинающегося от начала эксперимента ($i$ = 0) и оканчивающегося обнаружением в момент $N_i$ при значениях $p_i \approx 1$ равна $P_{N_i} = (1 - p_i)^{(N_i - 1)} p_i \approx p_i$,

а средние затраты времени на обнаружение оптимального кода определяются усреднением

$$N_{cp} \approx \sum_{i=0}^{N} p_i N_i = p_i \sum_{i=0}^{N} i = p_i \sum_{i=0}^{N} i = p_i \frac{N(N-1)}{2}$$ и для $p_i = 1/N$ имеем $N_{cp} = (N - 1)/2$.

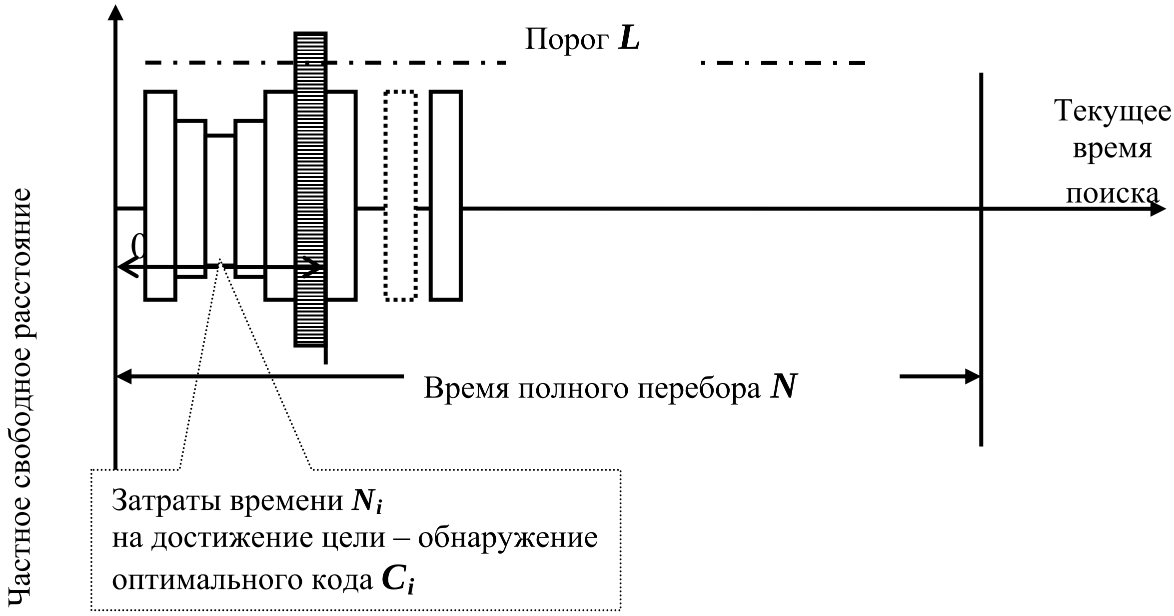


Рисунок 2 –Иллюстрация процесса переборного поиска

Тогда выигрыш от сокращения времени поиска кода в среднем составит

$$E = N / N_{cp} = 2N / (N - 1).$$

При больших значениях $N$ средний выигрыш равен $E = N/N_{cp} = 2$, т. е. среднее время поиска вдвое меньше максимального времени.

Остается вопрос о выборе порога $L$. Используя известное положение о том, что для любых распределений случайной величины максимальное значение всегда больше среднего, можно рекомендовать в качестве порога $L$ выбирать среднее значение искомого расстояния, выполнив для его определения «прогон» всего вычислительного процесса на длине интервала $N$, но без фиксации порождающих многочленов, что занимает значительно меньшее время. Приведенные оценки остаются справедливыми и для случая поиска кодов с заданной величиной расстояния по критерию ($d_f = L$).

Описанный алгоритм поиска отображается структурой, представленной на рис. 3.

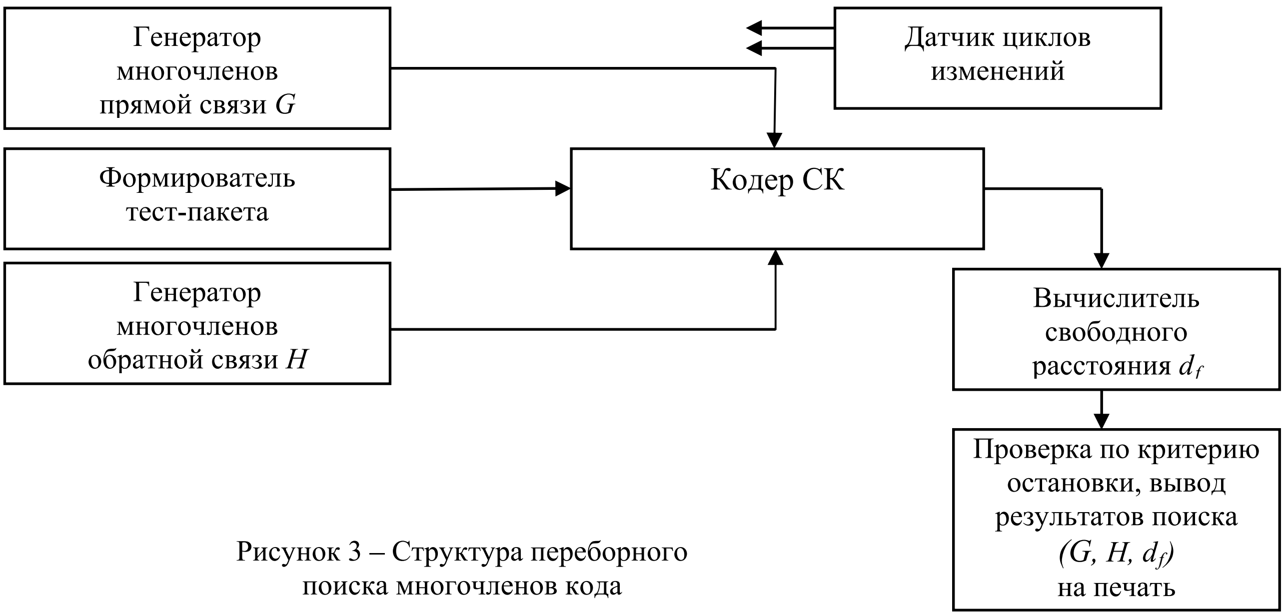


Рисунок 3 – Структура переборного поиска многочленов кода

При поиске кодов по критериям($d_f > L$) и ($d_f = L$) для определения величины свободного расстояния $d_f$ используется описанный выше метод тест-пакета. Генераторы многочленов прямой связи $G$ и многочленов обратной связи $H$ вырабатывают в начале каждого тест-пакета многочлены, выбираемые случайным образом из полных множеств этих многочленов объема $N = M^K$.

После остановки вычислительного процесса по выбранному критерию результаты поиска ($G, H, d_f$) выводятся на печать.

**5. Нерекурсивный и рекурсивные сверточные коды.** Эффективность и работоспособность разработанного метода подтверждаются результатами переборного поиска многочленов. Результаты поиска использованы для синтеза структур РСК, что позволило сравнить найденные рекурсивные коды с лучшими известными нерекурсивными (стандартными) СК, сведения о которых опубликованы в справочных таблицах [2, 3, 4]. Наибольший интерес представляет сравнение с нерекурсивным кодом со скоростью $R = 1/2$ и порождающим многочленом (133, 171), который был найден Р. Оденвальдером (R.Odenwalder) на заре эры активного освоения техники сверточного кодирования. Этот код вошел во многие стандарты спутниковой и космической связи [3, 4] и получил статус Planetary Standard Code (стандартный код для планетных исследований), и в настоящее время широко используется во многих телекоммуникационных системах. Западными компаниями выпускается ИМС кодека этого кода. Результаты такого сравнения приведены в табл.1.

Таблица 1 – Результаты переборного поиска РСК

| Номер кода № | Длина регистра $K$ | Тип кода | Порождающие многочлены | Свободное расстояние $d_f$ | Средне расстояние $d_{ср}$ | Показатель сложности S | АЭВК, дБ |
|---|---|---|---|---|---|---|---|
| 1 | 6 | РСК | {(16),(20)//16} | 10 | 14,8 | 64 | 6,02 |
| 2 | 7 | НСК | (133,171) | 10 | 12,4 | 128 | 6,02 |
| 3 | 6 | РСК | {(11),(12)//14} | 12 | 15,2 | 64 | 7,78 |

Принято следующее сокращенное обозначение РСК со скоростью $R= 1/n$: $\{(G_1), (G_2), (G_n)//H\}$, в котором многочлены прямых связей $(G_1)$, $(G_2)$, $(G_n)$ и многочлен обратной связи $H$ представлены в восьмеричной форме записи**.** Приведенные данные подтверждают перспективность применения рекурсивных кодов. Найден РСК {(16), (20)//16} (код № 1, показатель сложности S = 64)), который обеспечивает величину свободного расстояния $d_f = 10$, сопоставимую с расстоянием стандартного НСК (код № 2 с показателем сложности S = 128), но при меньшей длине кодирующего регистра. Показатель сложности декодирования РСК вдвое меньше (S = 64). Более того, удалось отыскать короткий РСК с большим свободным расстоянием(код № 3). В табл.1 указано также значение АЭВК (дБ) – асимптотический энергетический выигрыш при использовании кодирования.

Таким образом, разработан простой и легко реализуемый метод переборного поиска порождающих многочленов сверточных кодов. Применение метода и реализующих его программ в пакете *HP VEE* позволило отыскать короткие РСК с характеристиками лучшими, нежели характеристики стандартного нерекурсивного СК.

***Литература***

1. Помехоустойчивость и эффективность передачи информации / [Фалько А.И., Панфилов И.П., Банкет В.Л., Иващенко П.В.]; под ред. А.Г. Зюко. – М.: Радио и связь, 1985.– 272 с.
2. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение / Скляр Б.; пер. с англ. – М.: Изд. дом «Вильямс», 2003. – 1004 с.
3. *Банкет В.Л.* Цифровые методы в спутниковой связи: учебн. пособие / В.Л. Банкет, В.М. Дорофеев – М.: Радио и связь, 1988. 240с.
4. *Berrou C.* The Ten-Year-Old Turbo Codes are Entering into Service / *Berrou C.* // Communicatios Magazine. – 2001. – Vol. 41. – No8. – P.110 – 116.
5. *Valenti M. C.* The UMTS Turbo Code and Efficient Decoder Implementation Suitable for Software-defined Radios / M. C. Valenti, and J. Sun // International Iournal of Wireless Information Networks – 2001. – Vol. 8. – No4. – P. 203 – 215.
6. *Возенкрафт Дж*. Теоретические основы техники связи / Дж. Возенкрафт, И. Джекобс. – М.: Мир, 1969. – 640 с.
7. Сучасні телекомунікації: мережі, технології , економіка, управління, регулювання / [Довгий С.О., Савченко О.Я., Воробієнко П.П. та ін.]; за ред. С. О. Довгого. – К.: Укр. Видавн. Центр. – 2002. – 520 с.
8. *Банкет В.Л.* Метод синтеза рекурсивных сверточных кодов / В.Л. Банкет, Н.В. Незгазинская // Цифрові технології; – 2009. – № 5.