УДК 621.391.833

А.В. Дикарев

Государственный университет телекоммуникаций, Киев

КОДЫ НА ОСНОВЕ ДВОИЧНЫХ КОЛЕЦ

В статье предлагается ошибкообнаруживающий код на основе двоичных колец абелевых групп и рассматриваются его характеристики.

Ключевые слова: *код, кольцо, матрица, сдвиг, инвариантность.*

Исходный алгоритм. Имеется множество 2^N числовых векторов. Элементами их могут быть целые, действительные, десятичные, двоичные, шестнадцатиричные, знаковые и беззнаковые числа только одного типа. Для векторов двоичных чисел, количество бит находится в пределах m=0..N, образуя на элементах векторов C_N^m сочетаний. Суммарное число сочетаний составляет 2^N.

Выполним следующие операции:

- выберем вектор с m двоичными элементами, который в тексте именуется как исходная сдвиговая цифровая последовательность (ИСЦП);

- посредством циклического сдвига вправо на один символ создадим N-1 новых N-мерных вектров-цифровых последовательностей, разместив их в виде квадратной матрицы размером N*N. Как будет ясно из дальнейшего, согласно [1], каждая такая матрица является кольцом с двоичными символами из абелевой группы 2^N двоичных векторов, из которой можно выделить $(2^N / N^2)/2$ подобных матриц-колец;

- используя одну из логических операций xor, or или and (далее в тексте применяется только операция xor), выполним построчное векторное произведение первой строки матрицы с остальными N-1 строками, второй строки с остальными N-2 строками и т. д. вплоть до предпоследней и последней N-1 и N строк;

- после каждой такой операции с двумя строками кольца проверяется и суммируется количество несовпадений в получаемом результате единиц и нулей. Количество несовпадений для любых двух строк записывается целым положительным числом в последовательность-строку.

Результаты векторного произведения с участием первой строки образуют последовательность целых десятичных чисел или вектор длиной N-1 знаков, второй строки соответственно последовательность N-2 знаков и т. д. вплоть до одного единственного числа. Если эти последовательности расположить построчно одну под другой, получим треугольную квадратную матрицу размерностью (N-1)*(N-1). Назовём отдельные элементы полученной матрицы показателями сдвига (ПС). Описанные здесь операции для двух векторов длиной N=9 и N=6 совместно со своими матрицами показателей сдвига представлены на рис. 1. С учётом возможностей практического применения колец сформулируем следующие определения используемых в тексте понятий.

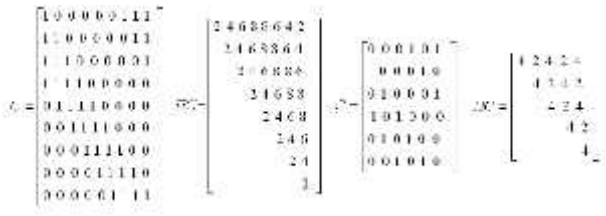

Рис. 1. Кольца сдвиговых последовательностей и соответствующие им показатели сдвига

Используемые понятия. Сдвиговая цифровая последовательность (СЦП)-вектор длиной N элементов с данными любого типа, которые затем подвергаются круговому сдвигу N раз [2] до получения исходной СЦП.

Исходная сдвиговая цифровая последовательность (ИСЦП)-первоначальный вектор длиною N элементов из их множества 2^N, подвергающийся затем круговому сдвигу N-1 раз.

Показатель сдвига (ПС). Целое десятичное число ненулевых элементов после векторного преобразования двух строк кольца одной из логических операций and, or, xor .

Сдвиговый показатель различия (СПР)-матрица размером (N-1)*(N-1) либо вектор длиной (N-1), элементами которых являются число несовпадений на любом месте n, n=1..N, элементов двух строк

кольца после их векторного преобразования одной из выбранных логических операций and, or, xor.

Символ модуляции – принятый в теории передачи дискретной информации по широкочастотным радиоканалам термин, описывающий некоторым количеством двоичных нулей и единиц одну из множества используемых в данной радиотехнологии комбинацию фаз, амплитуд и частот несущей частоты [3].

Код, кодовое слово, кодовая последовательность – представленные двоичными символами отдельные единицы сообщения, например, буквы латинского алфавита ACSII-символы.

Блок информации – некоторое постоянное число нулей и единиц, на которые делится цифровой поток (контент) видео, аудио либо иной двоичной информации в основном для применения ошибкообнаруживающего либо исправляющего ошибки кода [4].

Кольцо – квадратная матрица размером N*N числовых или двоичных элементов, строки которой получаются посредством сдвига (N-1) раз на один элемент вправо выбранной из множества 2^N двоичных векторов исходной сдвиговой последовательности.

Основные свойства сдвиговых цифровых последовательностей

Основные свойства СЦП удобно продемонстрировать на конкретных примерах.

1) Свойства инвариантности.

- Инвариантность значений ПС всех строк кольца и соответствие их СПР первой строки с уменьшением числа элементов каждой следующей строки на один элемент. Благодаря этому свойству вместо треугольных матриц СПР, показанных на рис. 1, можно в дальнейшем ограничиваться лишь их первой строкой.

- Инвариантность СПР циклического сдвига ИСЦП относительно типа данных, в частности, двоичных и десятичных. На рис. 2 показаны векторы, получающиеся циклическим сдвигом вправо двух последовательностей A и B длиною N=7 двоичных и целых десятичных чисел со знаком A=[1 1 1 0 0 0 1], B=[12 -4 9 0 0 0 1].

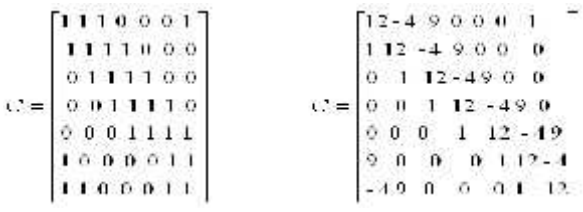

Рис. 2. Инвариантность ПС различного типа данных сдвиговых последовательностей одинаковой структуры для которых СПР=[2 4 6 6 4 2]

Применение к этим последовательностям логической операции xor ко всем по порядку строкам матриц A и B (рис. 1) даёт одинаковый по значениям элементов вектор показателей сдвига СПР=[2 4 6 6 4 2]. Длина вектора СПР равна N-1.

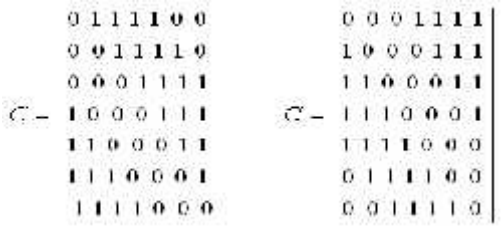

Рис. 3. Инвариантность СПР относительно любой строки кольца

- Инвариантность СПР инверсии элементов исходного кольца. На рис. 4 два кольца с прямыми и инвертированными значениями элементов дают одинаковый вектор СПР=[2 4 6 6 6 4 2].

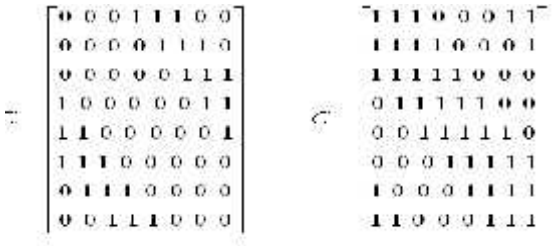

Рис. 4. Инвариантность инверсии символов исходной ИСЦП относительно СПР; в обоих случаях получается одинаковый СПР=[2 4 6 6 6 4 2]

- Одна единица на любом месте в строке ИСЦП произвольной длины всегда даёт одинаковую числовую последовательность СПР (при использовании операции xor), состоящую из одних единиц, что для различных длин N показано в таблице 1.

Таблица 1

N	Исходная последовательность	Последовательность ПС
9.	1 0 0 0 0 0 0 0 0 0	2 2 2 2 2 2 2 2
7.	0 0 0 1 0 0 0	2 2 2 2 2 2
5.	0 1 0 0 0	2 2 2 2

2) Другие свойства. Из других свойств колец следует отметить, что каждому кольцу соответствует

свой уникальный вектор СПР, отличающийся от всех остальных либо значением своих элементов, либо их расположением, либо тем и другим.

Практического применение. Для блоков длиной N элементов число колец с учётом инварианта инверсии составляет $(2^N / N^2)/2$. Пусть количество кодовых слов контента равно 32, например, алфавит кириллицы. Для кодирования кириллицы можно выбрать восьмисимвольные кольца с последующим использованием всех строк его матрицы. Потребуется всего 4 кольца из общего числа их $2^8/2 = 128$. Можно также для каждой буквы выбрать отдельное кольцо и тогда их потребуется 32. Если в результате искажения ошибками в канале связи кода любой буквы алфавита с равной вероятностью может появиться любая из 128 возможных двоичных комбинаций, то в обоих случаях вероятность необнаружения искажённой буквы составит $p_8 = (4*N)/(2^N/2) = 4*8)/(2^8/2) = 32/128 = 0.25$. С увеличением N вероятность p_i быстро уменьшается. Так для N=11 $p_{11} = 0.03$, а для N=20 всего $p_{20} = 1.907*10^{-4}$ Таким образом, кольца могут быть использованы как квазибезизбыточный код с обнаружением ошибок. Проверка может осуществляться с прямыми и инверсными двоичными кольцами. Такие кольца удобно использовать в префиксах пакетов и фреймов видеоконтента [4, 5]. В широкочастотных радиотехнологиях при использовании шумоподобных сигналов двоичные кольца могут найти применение для расширения спектра полезных сигналов аналогично кодам Баркера [6].

Заключение

Благодаря своим уникальным свойствам, проявляющимися в рассмотренных инвариантах, на основании двоичных колец могут быть сконструированы квазибезизбыточные коды с обнаружением и исправлением ошибок, а также широкочастотные шумоподобные сигналы, сходные с кодами Баркера.

Список литературы

1. *Бронштейн И.Н. Справочник по математике для инженеров и учащихся втузов / И.Н. Бронштейн, К.А. Семендяев //М.:Наука, 1980,- 718 с.*
2. *Лео Скэнлон. Персональные ЭВМ IBM PC и XT. Программирование на языке ассемблера/ Лео Скэнлон // М.:Радио и связь, 1991,- 336 с.*
3. *Серов А.В. Эфирное цифровое телевидение DVB-T/H / Серов А.В. //СПб: БХВ-Петербург, 2010.-464 с.*
4. *Смирнов А.В. Цифровое телевидение: от теории к практике /Смирнов А.В., Пескин А.Е. //М.: Горячая линия-Телеком, 2005,-352 с.*
5. *Мешковский К.А. Кодирование в технике святи / Мешковский К.А., Кириллов Н.Е.//М.: Связь, 1966,-320 с.*
6. *Олійник В.Ф. Системи та мережі цифрового радіозв'язку: інженерно-технічний довідник / Олійник В.Ф., Сайко В.Г., Булгач С.В., Кривуца В.Г. // Ніжин: вид-во "Аспект-Поліграф", 2011. - 612 с.*

Поступила в редколлегию 14.10.2013

Рецензент: д-р техн. наук, проф. А.В. Дробик, Государственный университет телекоммуникаций, Киев.

КОДИ НА БАЗІ ДВІЙКОВИХ КІЛЕЦЬ

О.В. Дікарєв

*У роботі розглядаються властивості кілець абельових груп, що отримуються завдяки циклічному зсуву будь-якого з 2^N числових векторів N разів. Кожне кільце являє собою квадратну матрицю розміром N*N, яка окремими рядками піддається векторному перетворенню однією з логічних операцій xor, or, and і результуючий вектор перевіряється на кількість незбігаючих елементів. Отриманий чисельний вектор може використовуватись як перевірочна комбінація квазібеззбиткового коду.*

Ключові слова: *код, кільце, матриця, зсув, інваріантність.*

CODES ON THE BASIS OF BINARY RINGS

A.V. Dikarev

*In work properties of rings the groups of Abel which are turning out as a result of cyclic shift of any of 2^N of numerical vectors N of time are considered. The ring representing a square matrix in the size N*N, then lines is exposed to vector of result transformation of one of logic operations xor, or, and and the vector of result is checked on number of incoincident elements. Obtained the numerical vector can be used as a verifying combination of codes which have no verifying symbols.*

Keywords: *codes, a ring, a matrix, shift, invariancy.*