Параллельная передача данных при кодовом уплотнении последовательностей Голда

Д. С. Кукунин

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

kukunin.ds@sut.ru

Аннотация. **Работа демонстрирует возможность применения эквивалентных последовательностей Голда для организации параллельной передачи информации множеству независимых получателей с учетом их анонимности. В отличие от классических кодов Голда, представленные здесь коды могут включать в себя более чем две последовательности максимальной длины. Таким образом, возможности данного подхода возрастают с увеличением числа полиномов деления круга, которые порождают данный вид шумоподобных сигналов.**

Ключевые слова: последовательность максимальной длины; последовательность Голда; поле Галуа; двойственный базис

I. Введение

Основным принципом реализации процедуры кодового уплотнения, как показано в работе [1], является ортогональность. Так, кодовые комбинации $S_i(t)$ и $S_j(t)$, которые планируется без последствий разделять на приеме, в идеале должны удовлетворять условию:

$$\int_T S_i(t)S_j(t)dt = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}, \quad (1)$$

Свойство (1) говорит об отсутствии взаимной корреляции между сигналами $S_i(t)$ и $S_j(t)$ и возможности их использования в качестве расширяющих спектр адресных последовательностей [1–4].

В роли таких сигналов могут выступать ортогональные или квазиортогональные последовательности, например, функции Уолша, последовательности максимальной длины, классические коды Голда или Касами. Так или иначе, кодовое уплотнение на их основе предполагает формирование суммарного многоуровневого сигнала, для которого требуются соответствующие методы модуляции.

Отдельно стоит выделить задачу параллельной передачи данных, где кодовое уплотнение могло бы решить целый ряд важных задач. Так, помимо прямого расширения спектра шумоподобными сигналами [5, 6] появляется реальная возможность одновременной передачи информационных элементов группе получателей в общем частотном и временном диапазоне [6].

Альтернативой многоуровневому сигналу, сформированному ортогональными функциями для организации параллельной передачи данных, мог бы стать двоичный код, использующий наиболее помехоустойчивый метод модуляции, вплоть до ФМ-2. Как показано в данной работе, такой код может быть построен по принципу последовательности Голда.

Работа выполнена в рамках прикладных научных исследований СПБГУТ, регистрационный номер 1023031600087-9 в ЕГИСУ НИОКТР.

II. Эквивалентные коды Голда

Классический код Голда [5] формируется двумя последовательностями максимальной длины одного периода, которые были построены на базе разных минимальных характеристических многочленов вида:

$$P(x) = \sum_{i=0}^{k} p_i x^{k-i} = p_0 x^k + p_1 x^{k-1} + \ \dots \ + p_{k-1}x + p_k, \quad p_i \in GF \quad (2)$$

Схема генератора последовательности Голда может быть реализована на основе двух генераторов рекуррентных последовательностей с вынесенными сумматорами (рис. 1).

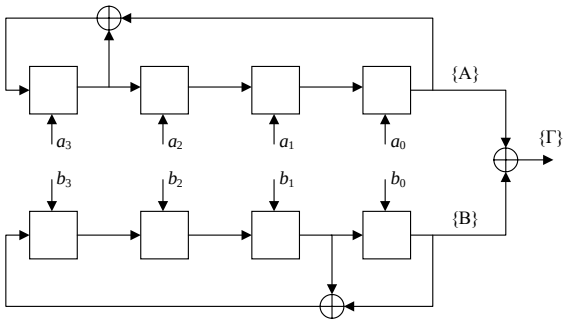

Рис. 1. Генератор последовательности Голда на основе минимальных многочленов x^4+x+1 и x^4+x^3+1

Однако, как было показано в исследованиях [6], возможно построение последовательности, обладающей свойствами кодов Голда, которая будет включать в себя более чем две М-последовательности. Очевидным ограничением при этом является количество многочленов (1) степени k, которые входят в разложение двучлена (x^n–1), где n=2^k–1.

Стоит рассмотреть процедуру построения кода Голда для некоторого значения, например, k=5. В этом случае становится возможным сформировать целых шесть М-последовательностей с периодом n=31 (табл. 1).

ТАБЛИЦА I. Минимальные многочлены над полем GF(2^5) и их М-последовательности

l	Минимальный полином $P_l(x)$	М-последовательность в канонической форме $\{S\}_l$
1	x^5+x^2+1	1001011001111100011011101010000
2	$x^5+x^4+x^3+x^2+1$	1111101110001010110100001100100
3	x^5+x^3+1	1000010101110110001111100110100
4	$x^5+x^3+x^2+x+1$	1001001100001011010100011101111
5	$x^5+x^4+x^3+x+1$	1110110011100001101010010001011
6	$x^5+x^4+x^2+x+1$	1110100010010101100001110011011

Каждая последовательность максимальной длины, представленная в табл. 1, может иметь n=31 состояние, которое определяется ее начальной фазой, то есть порождающим ее ненулевым вектором поля Галуа GF(2^5) длиной 5 бит. Таким образом, код Голда, построенный как сумма по mod 2 всех шести М-последовательностей, обеспечивает одновременную передачу пяти ненулевых информационных элементов каждому из шести получателей в общем частотном и временном диапазоне. При этом сохраняется анонимность приема, так как любой из шести получателей может не иметь представления о том, какие полиномы $P_l(x)$ используют остальные.

Последовательность Голда может быть построена не только как сумма по mod 2 соответствующих последовательностей максимальной длины из табл. 1, но и на основе общего характеристического многочлена, который определяется произведением всех шести полиномов [6]:

$$\begin{aligned} P(x) &= P_1(x)P_2(x)P_3(x)P_4(x)P_5(x)P_6(x) = \\ &= x^{30}+x^{29}+x^{28}+x^{27}+x^{26}+x^{25}+x^{24}+x^{23}+x^{22}+x^{21}+ \\ &+x^{20}+x^{19}+x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+ \\ &+x^{10}+x^{9}+x^{8}+x^{7}+x^{6}+x^{5}+x^{4}+x^{3}+x^{2}+x+1. \end{aligned} \quad (3)$$

Данный многочлен степени m=30 может быть положен в основу генератора рекуррентной последовательности, способного обеспечить построение кода Голда, для которого справедливо условие, учитывающее коэффициенты p_i многочлена (3):

$$S_i = p_1 S_{i-1} + p_2 S_{i-2} + \ldots + p_{m-1} S_{i-m+1} + p_m S_{i-m}; \quad p_i \in GF(2), \quad (4)$$

где $[i \pmod{(2^k-1)}] \geq m$.

Представление комбинаций кода Голда как рекуррентных последовательностей, удовлетворяющих условию (4) с последующей их обработкой на приеме двойственным базисом поля Галуа, позволяет говорить о новой разновидности последовательностей Голда, которые в литературе получили название эквивалентные [5, 6].

III. Обработка эквивалентных кодов Голда

Многочлен (3) представляет собой произведение шести минимальных многочленов $f_i(x)$ и обеспечивает построение рекуррентной последовательности $\{S\}$, удовлетворяющей условию (4), которая также будет суммой функций след $T(C_i\eta_i^j)$ от элемента поля Галуа $\alpha^i = C_i\eta_i^j$:

$$S_j = \sum_{i=1}^{6} T(C_i \eta_i^j), \quad (5)$$

где η_i – корни соответствующих многочленов $f_i(x)$.

Сама по себе функция след от элемента поля Галуа определяется из выражения [5, 6]:

$$T(\alpha^i) = \sum_{j=0}^{k-1} \left(\alpha^i\right)^{2^j} = \alpha^i + \left(\alpha^i\right)^2 + \left(\alpha^i\right)^{2^2} + \ldots + \left(\alpha^i\right)^{2^{k-1}}.$$

Коэффициенты C_i в (5) также являются элементами поля Галуа GF(2^k), построенного на основании своего $f_i(x)$ степени k. Они вычисляются по любому линейному участку $\{S\}$ длины m [6], в данном случае:

$$C_i = \eta_i^{-\delta} \sum_{j=1}^{m=30} \omega_{ij} S_{\delta+j-1}, \quad i = 1\ldots 6, \quad (6)$$

где δ – расстояние текущего m-элементного участка относительно начала $\{S\}$.

Коэффициенты двойственного базиса ω_{ij} в формуле (6) также являются элементами поля Галуа GF(2^k) и определяются выражением [6]:

$$\omega_{i\rho} = \frac{\sum_{l=0}^{m-\rho} p_{m-\rho-l} (\eta_i)^l}{P'(\eta_i)}, \quad \rho = 1, 2, \ldots, m. \quad (7)$$

где $P'(\eta_i)$ – значение производной многочлена (3) в точке, соответствующей примитивному элементу η_i соответствующего поля GF(2^k). В данном примере коэффициенты двойственного базиса будут иметь вид (табл. 2).

ТАБЛИЦА II. Коэффициенты двойственного базиса

Базисные коэф-ты λ_i, i=1…30	*Получатели* 1	2	3	4	5	6
	$P_1(x)$	$P_2(x)$	$P_3(x)$	$P_4(x)$	$P_5(x)$	$P_6(x)$
λ_1	η^{18}	η^{20}	η^{14}	η^{12}	η^{13}	η^{19}
λ_2	η^{4}	η^{8}	η^{27}	η^{23}	η^{25}	η^{6}
λ_3	η^{27}	η^{24}	η^{3}	η^{6}	η^{21}	η^{9}
λ_4	η^{7}	η^{15}	η^{22}	η^{14}	η^{18}	η^{11}
λ_5	η^{29}	η^{4}	η^{30}	η^{24}	η^{3}	η^{25}
λ_6	η^{22}	η^{16}	η^{5}	η^{11}	η^{10}	η^{17}
λ_7	η^{16}	η^{23}	η^{10}	η^{3}	η^{30}	η^{27}
λ_8	η^{13}	η^{29}	η^{12}	η^{27}	η^{4}	η^{21}
λ_9	η^{8}	η^{25}	η^{16}	η^{30}	η^{17}	η^{7}
λ_{10}	η^{26}	η^{7}	η^{28}	η^{16}	η^{5}	η^{18}
λ_{11}	η^{9}	η^{2}	η^{13}	η^{20}	η^{29}	η^{24}
λ_{12}	η^{12}	1	η^{9}	η^{21}	η^{19}	η^{2}
λ_{13}	η^{2}	η^{5}	η^{18}	η^{15}	η^{20}	1
λ_{14}	1	η^{14}	η^{19}	η^{5}	η^{28}	η^{22}
λ_{15}	η^{10}	η^{11}	η^{8}	η^{7}	η^{23}	η^{26}
λ_{16}	η^{25}	η^{26}	η^{23}	η^{22}	η^{7}	η^{10}
λ_{17}	η^{14}	η^{28}	η^{2}	η^{19}	η^{11}	η^{5}
λ_{18}	η^{15}	η^{18}	1	η^{28}	η^{2}	η^{13}
λ_{19}	η^{24}	η^{12}	η^{21}	η^{2}	1	η^{14}
λ_{20}	η^{20}	η^{13}	η^{24}	1	η^{9}	η^{4}
λ_{21}	η^{5}	η^{17}	η^{7}	η^{26}	η^{15}	η^{28}
λ_{22}	η^{17}	η^{3}	η^{25}	η^{8}	η^{26}	η^{16}
λ_{23}	η^{21}	η^{6}	η^{20}	η^{4}	η^{12}	η^{29}
λ_{24}	η^{23}	η^{30}	η^{17}	η^{10}	η^{6}	η^{3}
λ_{25}	η^{28}	η^{22}	η^{11}	η^{17}	η^{16}	η^{23}
λ_{26}	η^{3}	η^{9}	η^{4}	η^{29}	η^{8}	η^{30}
λ_{27}	η^{11}	η^{19}	η^{26}	η^{18}	η^{22}	η^{15}
λ_{28}	η^{30}	η^{27}	η^{6}	η^{9}	η^{24}	η^{12}
λ_{29}	η^{6}	η^{10}	η^{29}	η^{25}	η^{27}	η^{8}
λ_{30}	η^{19}	η^{21}	η^{15}	η^{13}	η^{14}	η^{20}

Применяя формулу (6) с учетом значений (7) из табл. 2, не составляет труда определить начальные фазы М-последовательностей, входящих в состав кода Голда.

Для примера организуем одновременную передачу данных нескольким получателям, при этом информация будет определять начальную фазу адресной

последовательности, которая должна быть детектирована на приеме в соответствующем канале (табл. 3).

ТАБЛИЦА III. ПЕРЕДАЧА ДАННЫХ ПО ТРЕМ КАНАЛАМ

Канал i	Данные (элемент поля η^j)	Адресная последовательность $\{S\}_i$
1	(00011) = η^{15}	00110111010100001001011001111110
2	(11000) = η^{7}	11000101011010000110010011111101
3	(10010) = η^{24}	01101001000010101111011000111110
4	(00000) = NULL	–
5	(00000) = NULL	–
6	(00000) = NULL	–

Таким образом, в состав последовательности Голда войдут только три адресные комбинации, которые соответствуют первым трем активным каналам:

$$\{\Gamma\} = (100110110011001000011110111111 01).$$

Используя коэффициенты двойственного базиса λ_i из табл. 3, произведем обработку начального 30-элементного участка $\{\Gamma\}$. Для этого достаточно будет вычислить сумму следующего набора коэффициентов: λ_1, λ_4, λ_5, λ_7, λ_8, λ_{11}, λ_{12}, λ_{15}, λ_{20}, λ_{21}, λ_{22}, λ_{23}, λ_{25}, λ_{26}, λ_{27}, λ_{28}, λ_{29} для каждого из каналов:

Канал 1:

$$\eta^{18}+\eta^{7}+\eta^{29}+\eta^{16}+\eta^{13}+\eta^{9}+\eta^{12}+\eta^{10}+\eta^{20}$$
$$+\eta^{5}+\eta^{17}+\eta^{21}+\eta^{28}+\eta^{3}+\eta^{11}+\eta^{30}+\eta^{6}=\eta^{15},$$
$$\eta\in GF(2^5),\ P_1(x)=x^5+x^2+1;$$

Канал 2:

$$\eta^{20}+\eta^{15}+\eta^{4}+\eta^{23}+\eta^{29}+\eta^{2}+1+\eta^{11}+\eta^{13}+$$
$$+\eta^{17}+\eta^{3}+\eta^{6}+\eta^{22}+\eta^{9}+\eta^{19}+\eta^{27}+\eta^{10}=\eta^{7},$$
$$\eta\in GF(2^5),\ P_2(x)=x^5+x^4+x^3+x^2+1;$$

Канал 3:

$$\eta^{14}+\eta^{22}+\eta^{30}+\eta^{10}+\eta^{12}+\eta^{13}+\eta^{9}+\eta^{8}+\eta^{24}+$$
$$+\eta^{7}+\eta^{25}+\eta^{20}+\eta^{11}+\eta^{4}+\eta^{26}+\eta^{6}+\eta^{29}=\eta^{24},$$
$$\eta\in GF(2^5),\ P_3(x)=x^5+x^3+1;$$

Канал 4:

$$\eta^{12}+\eta^{14}+\eta^{24}+\eta^{3}+\eta^{27}+\eta^{20}+\eta^{21}+\eta^{7}+1+\eta^{26}+$$
$$+\eta^{8}+\eta^{4}+\eta^{17}+\eta^{29}+\eta^{18}+\eta^{9}+\eta^{25}=\text{NULL},$$
$$\eta\in GF(2^5),\ P_4(x)=x^5+x^3+x^2+x+1;$$

Канал 5:

$$\eta^{13}+\eta^{18}+\eta^{3}+\eta^{30}+\eta^{4}+\eta^{29}+\eta^{19}+\eta^{23}+\eta^{9}+\eta^{15}+$$
$$+\eta^{26}+\eta^{12}+\eta^{16}+\eta^{8}+\eta^{22}+\eta^{24}+\eta^{27}=\text{NULL},$$
$$\eta\in GF(2^5),\ P_5(x)=x^5+x^4+x^3+x+1;$$

Канал 6:

$$\eta^{19}+\eta^{11}+\eta^{25}+\eta^{27}+\eta^{21}+\eta^{24}+\eta^{2}+\eta^{26}+\eta^{4}+$$
$$+\eta^{28}+\eta^{16}+\eta^{29}+\eta^{23}+\eta^{30}+\eta^{15}+\eta^{12}+\eta^{8}=\text{NULL},$$
$$\eta\in GF(2^5),\ P_6(x)=x^5+x^4+x^2+x+1.$$

Обработка m-элементного участка показывает, что информация присутствует в первых трех каналах, а в остальных констатируется ее отсутствие. Полученные при этом значения начальных фаз, как и ожидалось, совпадают со значениями из табл. 3.

Следует отметить, что в данном примере были использованы минимальные многочлены степени k=5, которых насчитывается всего шесть. Они обеспечивают увеличение базы сигнала в 6 раз с учетом передачи 5 бит информации каждому из получателей. В случае с k=7 таких многочленов будет уже 18, а при k=11 их количество возрастет до 186. Эти же значения определят степень увеличения базы сигнала при расширении спектра прямой последовательностью.

Расширение набора минимальных многочленов возможно также за счет использования рекуррентных последовательностей, построенных на основе полей с двойным расширением [7]. Такие последовательности могут быть эффективно декодированы двойственным базисом поля Галуа в соответствии с теми же принципами, что и представленные в настоящей работе эквивалентные коды Голда [8].

IV. ЗАКЛЮЧЕНИЕ

Предложенный метод кодового уплотнения, как видно, обеспечивает параллельную передачу информации на основе эквивалентных кодов Голда, которые могут иметь в своем составе более двух последовательностей максимальной длины.

Действительно, отличительной особенностью эквивалентных кодов Голда является их способность сочетать в себе произвольное число М-последовательностей от разных характеристических полиномов, а в случае использования полей Галуа с двойным расширением количество таких полиномов значительно возрастает, что в перспективе повышает степень анонимности получателей информации. Приведенный в работе пример показывает процедуру кодового уплотнения и прием данных в системе, использующей шесть минимальных многочленов.

Выделение информации, содержащейся в начальных фазах М-последовательностей, обеспечивается не за счет вычисления скалярного произведения, как это реализовано в случае с классическими ортогональными кодами, а посредством обработки линейных рекуррентных участков принятой последовательности двойственным базисом поля Галуа.

Последовательности максимальной длины формируют общий сигнал не как линейную сумму, а по mod 2. Полученный при этом код Голда будет иметь единичную максимальную амплитуду сигнала, что в дальнейшем позволит применить к нему фазовую модуляцию ФМ-2 с целью достижения наилучшей степени помехоустойчивости.

Очевидным недостатком предложенного метода кодового уплотнения является то, что принцип сопоставления информационным элементам векторов поля Галуа делает невозможным передачу нулевого вектора. Приведенный в работе пример наглядно демонстрирует регистрацию нулевого вектора в случае отсутствия информации в канале. Таким образом, показано, что нулевой вектор не должен использоваться для передачи данных.

Список литературы

[1] Кукунин Д.С., Березкин А.А., Киричек Р.В. Использование фантомных каналов в качестве катализаторов усиления ортогональных свойств М-последовательностей в системе с кодовым разделением каналов // Труды Научно-исследовательского института радио. 2022. №1. С.37-47.

[2] Бабков В.Ю., Никитин А.Н., Осенний К.Н., Сиверс М.А. Системы связи с кодовым разделением каналов. Санкт-Петербург: ТРМАDA. 2003. 239 с.

[3] Бобровский В.И. Многопользовательское детектирование: монография. Ульяновск: Вектор-С. 2007. 348 с.

[4] Никитин Г.И. Применение функций Уолша в сотовых системах связи с кодовым разделением каналов: учебное пособие. Санкт-Петербург: ГУАП. 2003. 86 с.

[5] Когновицкий О.С. Двойственный базис и его применение в телекоммуникациях: монография. Санкт-Петербург: Линk, 2009.

[6] Кукунин Д.С., Когновицкий О.С., Березкин А.А., Киричек Р.В. Перспективы использования рекуррентных последовательностей в современной телекоммуникационной среде: монография. Санкт-Петербург: СПбГУТ, 2023. 289 с.

[7] Когновицкий О.С., Кукунин Д.С. Рекуррентные последовательности максимальной длины над полем Галуа с двойным расширением // Электросвязь. 2023. №6. с. 77-83.

[8] Когновицкий О.С., Кукунин Д.С. Применение двойственного базиса для обработки М-последовательностей над полем с двойным расширением // Электросвязь. 2023. №10. с. 26-34.