Труды МАИ. 2026. № 148.
Trudy MAI. 2026. No. 148. (In Russ.)

Научная статья
УДК 621.3.085
URL: https://trudymai.ru/published.php?ID=188279
EDN: https://www.elibrary.ru/MODOWR

ЦИФРОВОЙ ПРЕОБРАЗОВАТЕЛЬ УГЛА ПОВЫШЕННОЙ ИНФОРМАЦИОННОЙ НАДЕЖНОСТИ

В.В. Алексеева✉

Акционерное общество «Научно-Исследовательский Технологический Институт «Авангард», г. Санкт-Петербург, Россия

✉ ladarobotics@gmail.com

Цитирование: Алексеева В.В. Цифровой преобразователь угла повышенной информационной надежности // Труды МАИ. 2026. № 148. URL: https://trudymai.ru/published.php?ID=188279

Аннотация. В статье представлена аналитическая модель цифрового преобразователя угла повышенной информационной надежности, основанная на применении М-последовательностей и циклических кодов Боуза–Чоудхури–Хоквингема с вычислениями в поле Галуа. С помощью предложенного метода решается ключевая задача прецизионной измерительной техники (авиационной и космической) — совмещение высокой помехоустойчивости с минимальными массогабаритными характеристиками. В отличие от кодовых шкал, требующих выделения отдельных дорожек для размещения корректирующих считывающих элементов, использование псевдослучайной кодовой шкалы позволяет интегрировать коррекцию ошибок в существующую структуру шкалы. Ключевым элементом подхода является построение порождающего полинома циклического корректирующего кода в поле Галуа, обеспечивающего оптимальное соотношение избыточности и корректирующей способности. Данная работа является развитием методов кодирования Хэмминга, обеспечивающих исправление однократных ошибок, и расширяет их для коррекции произвольного числа ошибок при минимальном кодовом расстоянии. Результаты моделирования

подтверждают работоспособность модели для 5…16 разрядности включительно, что соответствует периодам М-последовательности в 31…65535 символов.

Ключевые слова: коррекция ошибок; псевдослучайная кодовая шкала; цифровой преобразователь угла; БЧХ коды; поле Галуа; циклические коды; алгоритм Берлекэмпа — Мэсси.

A HIGH-RELIABILITY DIGITAL ANGLE ENCODER

V.V. Alekseeva ✉

Joint-Stock Company «Scientific-Research Technological Institute «Avangard»,

Saint Petersburg, Russiaя

✉ ladarobotics@gmail.com

Citation: Alekseeva V.V. A high-reliability digital angle encoder // Trudy MAI. 2026. No. 148. (In Russ.). URL: https://trudymai.ru/published.php?ID=188279

Abstract. This paper presents an analytical model of a high-information-reliability digital angle encoder with correction of multiple errors based on the theory of M-sequences and Bose–Chaudhuri–Hocquenghem (BCH) cyclic codes. The proposed method solves a key problem in precision measurement technology (aviation and space) — achieving high noise immunity while maintaining minimal size, weight, and structural complexity. In contrast to code scales that require dedicated tracks for redundant or parity sensors, the use of a pseudorandom code scale enables error-correction capability to be embedded directly into the existing scale structure. The core of the approach lies in constructing a generator polynomial of a cyclic code over an extended Galois field, which provides an optimal trade-off between redundancy and error-correcting capacity. This work is a development of Hamming coding methods that provide single-error correction and extend them to correct an arbitrary number of errors with a minimum code distance. The simulation results confirm the model's performance for 5...16-bit data, which corresponds to M-sequence periods of 31...65535 characters.

Keywords: error correction; pseudorandom code scale; digital angle encoder; BCH codes; Galois field; cyclic codes; Berlekamp — Massey algorithm.

Введение

Современные авиационные и космические системы предъявляют повышенные требования к надежности и точности функционирования входящих в их состав компонентов. Особую важность эти параметры приобретают для цифровых преобразователей угла (ЦПУ), или энкодеров, которые играют роль первичных датчиков углового положения в системах управления полетом (Fly-by-Wire), наведения, управления двигателями, механизацией крыла и шасси летательных аппаратов. В таких системах отказ датчика или даже временная ошибка в его показаниях могут привести к катастрофическим последствиям. Энкодеры в этих приложениях должны обеспечивать абсолютное определение положения в условиях экстремальных внешних воздействий: широкого температурного диапазона (от -55°C до +125°C и выше), сильных вибраций, ударных нагрузок, а также воздействия ионизирующего излучения.

Актуальность работы обусловлена тем, что шкалы, выполненные на основе обыкновенного двоичного кода и кода Грея, предполагают выделение отдельной физической дорожки под каждый двоичный разряд. При этом для обеспечения коррекции ошибок необходимы дополнительные проверочные дорожки. В случае кода Хэмминга для исправления одиночных ошибок число проверочных бит r определяется соотношением $2^r \geq m + r + 1$, где m — число информационных бит. Так, для 4 информационных бит требуется 3 проверочных бит, что увеличивает общее число дорожек до 7, а для 8 информационных бит — до 12, и для 16 информационных бит — до 21 дорожки. Как видно из рисунка 1, структура кодовой шкалы для 16-позиционной системы (4 бит) включает 7 кодовых дорожек. Из них 4 дорожки используются в качестве информационных кодовых символов, а 3 служат для коррекции одиночных ошибок [1]. Считывание данных осуществляется четырьмя информационными считывающими элементами (ИСЭ) и тремя корректирующими считывающими элементами (КСЭ), на основе которых получены кодовые комбинации, представленные в таблице 1. При этом биты, считываемые ИСЭ, обозначаются как И1, И2, И3, И4, а биты от КСЭ — как К1, К2, К3. В целом, это приводит к увеличению массогабаритных характеристик, что

противоречит современным требованиям ответственной техники, поскольку каждая дополнительная дорожка увеличивает габариты энкодера.

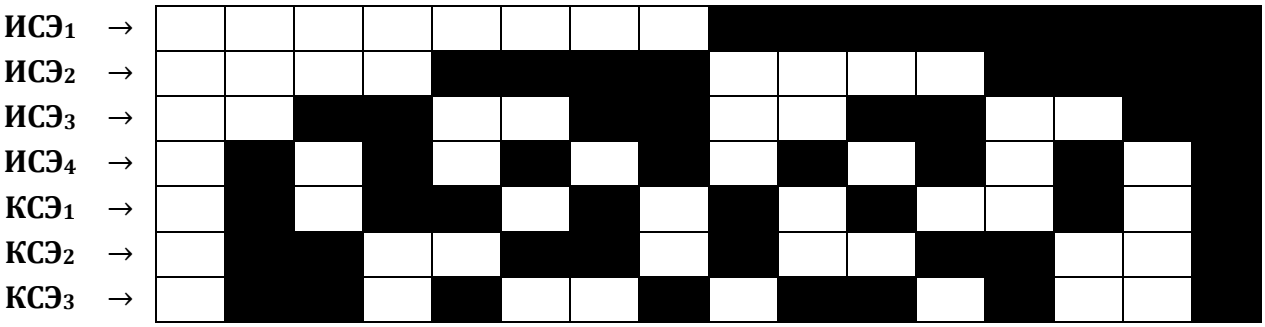

Рисунок 1 — Структура многодорожечной кодовой шкалы на основе кода Хэмминга. Черные участки соответствуют активным (единичным) символам кода, белые — пассивным (нулевым)

Таблица 1

Кодовые комбинации многодорожечной шкалы на основе кода Хэмминга

Поз. шкалы	И1	И2	И3	И4	К1	К2	К3
0	0	0	0	0	0	0	0
1	0	0	0	1	1	1	1
2	0	0	1	0	0	1	1
3	0	0	1	1	1	0	0
4	0	1	0	0	1	0	1
5	0	1	0	1	0	1	0
6	0	1	1	0	1	1	0
7	0	1	1	1	0	0	1
8	1	0	0	0	1	1	0
9	1	0	0	1	0	0	1
10	1	0	1	0	1	0	1
11	1	0	1	1	0	1	0
12	1	1	0	0	0	1	1
13	1	1	0	1	1	0	0
14	1	1	1	0	0	0	0
15	1	1	1	1	1	1	1

При эксплуатации авиационно-космических аппаратов классические подходы к коррекции ошибок считывания демонстрируют недостаточную эффективность. Воздействие ионизующего излучения и тяжелых заряженных частиц высоких энергий способно вызывать множественные ошибки в соседних или произвольно распределенных битах считываемого кода. Это превышает корректирующие возможности кодов Хэмминга, которые гарантируют исправление лишь одиночных сбоев [2, 3]. Например, пролет

высокоэнергетической частицы через область считывания может привести к одновременному искажению трех и более смежных битов, что повлечет за собой возникновение критической погрешности измерения углового положения или отказ системы управления [4].

Применение радиационно-стойкой элементной базы не решает проблему надежности оптических энкодеров, поскольку ионизирующее воздействие непосредственно затрагивает физическую кодовую шкалу и оптоэлектронные компоненты. Оптический тракт принципиально не поддается экранированию без блокировки полезного светового сигнала. Вызванная внешним воздействием деградация материала кодовой шкалы (наведенное поглощение в стеклах и снижение контраста [5]), радиационное старение излучателя (падение мощности светодиодов [6]), а также радиационные дефекты решетки в фотоприемниках, вызывающие отклонения чувствительности и рост темновых токов [7], — все это приводит к тому, что на вычислительный узел поступают уже искаженные первичные данные. Предлагаемая архитектура с несколькими фазово-сдвинутыми считывающими элементами и мажоритарным голосованием позволяет преодолеть данное ограничение. За счет пространственно-фазовой избыточности система отбраковывает недостоверные отсчеты, вызванные локальными сбоями в любом из элементов оптического тракта, и восстанавливает корректное значение угла.

Зарубежные производители, такие как Renishaw с серией энкодеров RESOLUTE, уже предлагают решения с расширенным температурным диапазоном и возможностью коррекции множественных ошибок с помощью многоуровневого подхода [8]. В связи с этим актуальной задачей является разработка отечественных ЦПУ повышенной информационной надежности, способных функционировать в условиях целевых применений. Одним из наиболее перспективных направлений является применение псевдослучайных кодовых шкал (ПСКШ) на основе М-последовательностей в сочетании с циклическими кодами и вычислениями в поле Галуа. В отличие от рассмотренных выше многодорожечных решений, структура ПСКШ реализуется на одной физической

дорожке (см. рисунок 2). Соответствующие кодовые комбинации для данной структуры представлены в таблице 2.

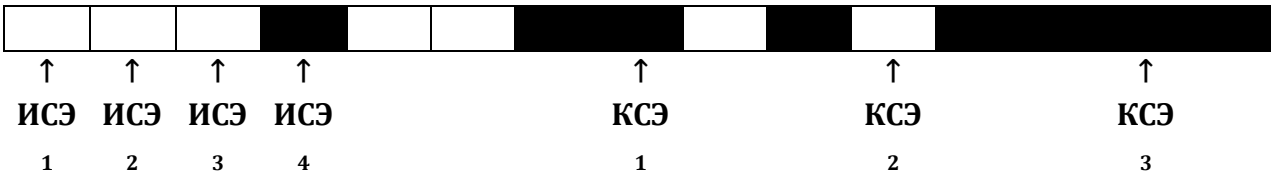

Рисунок 2 — Схема размещения считывающих элементов на однодорожечной псевдослучайной кодовой шкале: ИСЭ — информационные считывающие элементы, КСЭ — корректирующие считывающие элементы

Таблица 2

Кодовые комбинации однодорожечной псевдослучайной кодовой шкалы

Поз. шкалы	**И1**	**И2**	**И3**	**И4**	**К1**	**К2**	**К3**
0	0	0	0	1	1	0	1
1	0	0	1	0	0	1	1
2	0	1	0	0	1	1	0
3	1	0	0	1	0	1	0
4	0	0	1	1	1	1	0
5	0	1	1	0	1	0	1
6	1	1	0	1	1	0	0
7	1	0	1	0	1	0	0
8	0	1	0	1	0	1	1
9	1	0	1	1	0	0	1
10	0	1	1	1	0	0	0
11	1	1	1	1	1	1	1
12	1	1	1	0	0	1	0
13	1	1	0	0	0	0	1
14	1	0	0	0	1	1	1

Целью исследования является разработка аналитической модели цифровых преобразователей угла повышенной информационной надежности на основе теории М-последовательностей и циклических кодов БЧХ (Боуза-Чоудхури-Хоквингема) с вычислениями в поле Галуа [9–12]. Предлагаемый подход позволяет гибко настраивать систему на требуемый уровень помехоустойчивости для коррекции до t ошибок при минимальном кодовом расстоянии $d = 2t + 1$ для однодорожечной псевдослучайной кодовой шкалы (ПСКШ).

Математическая модель системы

Рассмотрим модель системы считывания информации с ПСКШ на основе М-последовательности. Пусть поле Галуа GF(2^m) порождается примитивным полиномом степени m. Длина периода М-последовательности $N = 2^m - 1$. Символы этой последовательности удовлетворяют рекуррентному соотношению [13, 14]:

$$a_i = \sum_{j=1}^{m} h_j a_{i-j} \pmod 2, \quad 0 < i < m, \qquad (1)$$

где $h_i \in \{0, 1\}$ — коэффициенты примитивного полинома $h(x) = x^m + h_{m-1}x^{m-1} + \cdots + h_1 x + 1$. В таблице 3 представлены полиномы $h(x)$ до $m = 16$ включительно, используемые для генерации М-последовательностей [15, 16].

Таблица 3

Примитивные полиномы степени m

m	$h(x)$	N	m	$h(x)$	N
1	$x + 1$	1	9	$x^9 + x^4 + 1$	511
2	$x^2 + x + 1$	3	10	$x^{10} + x^3 + 1$	1023
3	$x^3 + x + 1$	7	11	$x^{11} + x^2 + 1$	2047
4	$x^4 + x + 1$	15	12	$x^{12} + x^6 + x^4 + x + 1$	4095
5	$x^5 + x^2 + 1$	31	13	$x^{13} + x^4 + x^3 + x + 1$	8191
6	$x^6 + x + 1$	63	14	$x^{14} + x^{10} + x^6 + x + 1$	16383
7	$x^7 + x^3 + 1$	127	15	$x^{15} + x + 1$	32767
8	$x^8 + x^4 + x^3 + x^2 + 1$	255	16	$x^{16} + x^{12} + x^3 + x + 1$	65535

Построение циклического кода для коррекции ошибок. Для обеспечения коррекции числа t ошибок используется циклический код с минимальным расстоянием $d = 2t + 1$. Порождающий полином $g(x)$ строится как наименьшее общее кратное (НОК) минимальных полиномов $m_i(x)$ для примитивного элемента $\alpha^i \in$ GF(2^m), где $i = (1,..., 2t)$ [5, 9–12]:

$$g(x) = \text{НОК}\{m_1(x), m_2(x),..., m_{2t}(x)\}. \qquad (2)$$

Важно отметить, что минимальные полиномы $m_i(x) = m_j(x)$, если i и j принадлежат одному циклотомическому классу по модулю $N = 2^m - 1$. Таким образом, в произведении (2) достаточно учитывать минимальные полиномы

только для нечетных i или других представителей каждого циклотомического класса.

Размещение считывающих элементов

Для обнаружения и исправления ошибок требуется получить m информационных и r проверочных бит, где степень порождающего полинома $g(x)$ определяет число r. Общее число бит равно $n = m + r$.

Размещение информационных считывающих элементов (ИСЭ) и корректирующих считывающих элементов (КСЭ) определяется структурой образующей матрицы кода. Позиции ИСЭ соответствуют m информационным битам и обозначаются как И1, И2, …, Иm; позиции КСЭ соответствуют r проверочным битам и обозначаются как К1, К2, …, Кr.

Пусть G — образующая матрица циклического кода вида

$G = [I|F]$, (3)

где I — единичная матрица размерности $m \times m$, а F — матрица размерности $m \times (n - m)$. Позиции считывающих элементов (СЭ) определяются как множество индексов P, соответствующих ненулевым элементам в строках матрицы G. Формально это можно выразить следующим образом:

$P = \{i \mid G(i, j) \neq 0$ для некоторого $j\}$, где $0 \leq P \leq N - 1$.

Более подробно алгоритм размещения информационных и корректирующих считывающих элементов (СЭ) рассмотрен в отечественной и зарубежной литературе [1, 17–19].

Процесс кодирования

Пусть $u = (u_0, u_1, \ldots, u_{m-1})$ — информационное слово, а $u(x) = u_0 + u_1 x + \ldots + u_{m-1} x^{m-1}$ — соответствующий полином.

1. Полином $u(x)$ умножается на x^r, где r – число проверочных бит.

2. Вычисляется остаток от деления произведения $u(x) \times x^r$ на порождающий полином $g(x)$:

$r(x) = u(x) \times x^r \bmod g(x)$.

3. Формируется кодовое слово (полином) вида:

$c(x) = u(x) \times x^r + r(x)$,

где коэффициенты полинома $c(x)$ представляют собой биты, которые должны быть считаны в соответствующих позициях шкалы.

Процесс декодирования и коррекции ошибок. Пусть при считывании получено кодовое слово $r(x) = c(x) + e(x)$, где $c(x)$ — переданное кодовое слово, а $e(x)$ — полином ошибок, содержащий t ошибочных символов.

Синдромы S_j для двоичного БЧХ-кода определяются как значения принятого полинома в корнях порождающего полинома:

$$S_j = r(\alpha^j) = \sum_{i=1}^{t} X_i^j, \quad j = 1, 2, \ldots, 2t, \tag{3}$$

где $X_i = \alpha^{\varphi_i}$ — локатор -й ошибки, а и φ_i — ее позиция в кодовом слове.

На основе свойств полинома-локатора ошибок уравнение (3) можно упростить до вида:

$$S_{t+j} + \sigma_1 S_{t+j-1} + \cdots + \sigma_t S_j = 0, \tag{4}$$

где $\sigma_1, \ldots, \sigma_t$ — коэффициенты полинома-локатора ошибок $\sigma(x)$.

Алгоритм Берлекэмпа — Мэсси итеративно вычисляет коэффициенты полинома-локатора минимальной степени $\sigma^{(i)}(x)$. Этот полином определяет линейный рекуррентный регистр сдвига (ЛРРС / РСЛОС), генерирующий ограниченную последовательность синдромов $S_1, S_2, \ldots, S_{2t}$ [9–12, 20, 21]:

$\sigma^{(i)}(x) = 1 + \sigma_1^{(i)} x + \ldots + \sigma_t^{(i)} x^t$, (5)

где t — текущая оценка числа ошибок на -шаге, $i \in [1, 2t]$.

Расхождение (несовместимость) информации определено выражением:

$$\Delta_i = S_i + \sum_{j=1}^{L} \sigma_j^{(i-1)} S_{i-j}$$

Здесь $\sigma_j^{(i-1)}$ — коэффициент при x^j в $\sigma^{(i)}(x)$. Все операции выполняются в поле GF(2^m).

В цикле итераций (для i от 1 до $2t$) возможен один из двух случаев:

1. Если $\Delta_i = 0$, то уравнение (4) разрешимо с равенством:

- $\sigma^{(i)}(x) = \sigma^{(i-1)}(x)$,
- $\rho^{(i)}(x) = x \times \rho^{(i-1)}(x)$ (корректирующий полином),

- $t = t$ (остается неизменным).

2. Если $\Delta_i \neq 0$, то на следующей ($i = i + 1$) итерации:

- $\sigma^{(i)}(x) = \sigma^{(i-1)}(x) + \Delta_i \times \Delta_\varepsilon^{-1} \times x^{(i-\varepsilon)} \times \rho^{(\varepsilon)}(x)$, где ε — предыдущая итерация с ненулевым расхождением Δ_ε ,
- $\rho^{(i)}(x) = x \times \rho^{(i-1)}(x)$ (сдвиг).

Итеративное вычисление полинома-локатора ошибок $\sigma^{(i)}(x)$ продолжается до достижения числа $2t = i$, когда происходит изменение:

- $t = i - t$ (обновление числа ошибок),
- $\Delta_{i-1} = \Delta_i$,
- $\rho^{(i)}(x) = x \times \rho^{(\varepsilon)}(x)$.

Начальными условиями алгоритма являются:

$\sigma^{(0)}(x) = \rho^{(0)}(x) = \Delta_0 = 1,\ i = t = 0.$ (6)

Если элемент α^i является корнем полинома-локатора $\sigma(\alpha^i) = 0$, то локатор ошибки $X = \alpha^i$, а позиция ошибки:

$\varphi = (-\log_\alpha X) \bmod N = (-i \times \log_\alpha \alpha) \bmod N = -i \bmod N.$ (7)

Ошибки исправляются путем инвертирования битов в найденных позициях φ искаженного кодового слова $r(x)$. После из восстановленного слова $c'(x)$ извлекаются коэффициенты, соответствующие позициям исходного информационного слова $u(x)$.

Алгоритм построения системы с коррекцией произвольного числа ошибок содержит следующие шаги:

1. **Инициализация системы:**

- Определяется степень расширения поля m.
- Выбирается примитивный полином $h(x)$ степени m, порождающий поле GF(2^m).
- Строится М-последовательность длины $N = 2^m - 1$.
- Задается число исправляемых ошибок t.
- Рассчитывается минимальное кодовое расстояние $d = 2t + 1$.

2. **Построение циклического кода:**

- Находится минимальные полиномы $m_i(x)$ для элементов α^i при $i = 1, 2,..., 2t$, где α — примитивный элемент поля GF(2^m).
- С помощью выражения (2) вычисляется порождающий полином $g(x)$ как НОК этих минимальных полиномов.
- Проверяется деление $g(x)$ на $x^N - 1$ без остатка.

3. **Формирование структуры считывающих элементов:**

- В соответствии с образующей матрицей G вида (3) определяется число m позиций информационных считывающих элементов (ИСЭ) и r позиций корректирующих считывающих элементов (КСЭ).

4. **Кодирование информационных слов:**

- Для каждого информационного слова $u(x)$ длины m формируется кодовое слово:

$c(x) = u(x) \times x^r + (u(x) \times x^r \bmod g(x))$.

- Каждой позиции P шкалы длины N сопоставляется кодовое слово.

5. **Декодирование и коррекция ошибок:**

- Для принятого слова $r(x)$ с числом t произвольных ошибок вычисляются синдромы $S_j = r(\alpha^j),\ j = 1, 2,..., 2t$.
- С помощью выражений (4) и (5) определяется полином-локатор ошибок $\sigma(x)$.
- Находятся корни полинома-локатора $\sigma(x)$: $\sigma(\alpha^i) = 0$ путем перебора минимальных элементов $\alpha^i \in$ GF(2^m).
- С помощью выражения (7) определяются позиции φ числа t ошибок.
- Инвертируются биты в найденных позициях $\varphi \in P$ кодового слова r.
- Извлекается исходное кодовое слово c' и информационное кодовое слово u'.

Пример реализации системы

Для наглядности принято значение разрядности системы $m = 5$ и $t = 2$, минимальное кодовое расстояние $d = 5$. Из таблицы 1 выбран примитивный полином $h(x) = x^5 + x^2 + 1$. Длина периода М-последовательности $N = 2^5 - 1 =$

31. Символы последовательности $a = (0000100101100111110001101110101)$ были получены с помощью рекуррентного соотношения (1).

Последовательное считывание кодовой шкалы с помощью информационных (ИСЭ) и корректирующих (КСЭ) считывающих элементов позволяет выделить 31 уникальную кодовую комбинацию, соответствующую 31 позиции ПСКШ энкодера. Эти комбинации, образующие циклический корректирующий код, приведены в таблице 4 [22].

Таблица 4

Кодовые слова БЧХ-кода длиной 15 бит для 31-позиционной ПСКШ

И1	**И2**	**И3**	**И4**	**И5**	**К1**	**К2**	**К3**	**К4**	**К5**	**К6**	**К7**	**К8**	**К9**	**К10**
0	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**1**
0	0	0	1	0	0	1	1	0	1	1	1	0	1	1
0	0	1	0	0	1	1	0	1	1	1	0	1	1	0
0	1	0	0	1	1	0	1	1	1	0	1	1	0	0
1	0	0	1	0	1	0	1	0	1	1	0	0	0	1
0	0	1	0	1	0	0	0	0	0	1	1	1	1	1
0	1	0	1	1	1	1	0	1	0	1	0	1	1	1
1	0	1	1	0	0	1	1	1	0	0	0	1	1	1
0	1	1	0	0	1	0	1	1	1	1	0	0	1	1
1	1	0	0	1	0	1	1	1	1	0	0	1	1	0
1	0	0	1	1	0	1	1	1	0	1	1	0	0	0
0	0	1	1	1	0	1	1	0	1	0	0	1	0	0
0	1	1	1	1	0	0	0	0	1	0	0	0	0	1
1	1	1	1	1	1	1	0	0	1	0	1	0	1	1
1	1	1	1	0	0	0	0	1	0	0	0	0	1	0
1	1	1	0	0	0	1	1	1	1	1	1	0	0	1
1	1	0	0	0	1	0	1	0	0	0	1	1	1	1
1	0	0	0	1	0	0	0	1	1	0	0	0	1	1
0	0	0	1	1	1	0	1	1	0	1	0	0	1	0
0	0	1	1	0	1	0	1	1	0	0	1	1	0	1
0	1	1	0	1	0	1	1	0	0	1	1	0	1	0
1	1	0	1	1	0	0	0	1	0	1	1	1	0	1
1	0	1	1	1	1	0	1	0	1	0	1	1	1	0
0	1	1	1	0	1	1	0	1	0	0	1	0	0	0
1	1	1	0	1	1	0	1	0	0	1	0	0	0	0
1	1	0	1	0	1	1	0	0	1	1	0	1	0	0
1	0	1	0	1	1	1	0	0	0	1	0	1	0	1
0	1	0	1	0	0	0	0	0	1	1	1	1	1	0
1	0	1	0	0	0	0	0	1	1	1	1	1	0	0
0	1	0	0	0	0	1	1	0	0	0	0	1	0	1
1	0	0	0	0	1	1	0	0	0	0	1	0	1	0

Порождающий полином формируется в виде наименьшего общего кратного минимальных полиномов для корней $\alpha^1, \alpha^2, \alpha^3, \alpha^4$, где α — минимальный элемент поля GF(2^5), порожденного примитивным полиномом $h(x)$.

Минимальные полиномы для циклотомических классов:

- Для {1, 2, 4, 8, 16}: $m_1(x) = x^5 + x^2 + 1$.
- Для {3, 6, 12, 24, 17}: $m_3(x) = x^5 + x^4 + x^3 + x^2 + 1$.

Порождающий полином вида (2):

$$g(x) = m_1(x) \times m_3(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1.$$

Степень $g(x)$ равна 10, что составляет число корректирующих считывающих элементов $r = 10$. Число значащих членов полинома $g(x)$, равное семи, говорит о соблюдении минимального кодового расстояния $d \geq 5$ для исправления 2-х ошибок.

Пусть были считаны информационные биты [0, 0, 0, 0, 1], тогда информационный полином имеет следующий вид:

$u(x) = 1 \times x^0 = 1$.

Чтобы освободить место для числа r проверочных битов, умножаем информационный полином на моном x^r:

$u(x) \times x^r = 1 \times x^{10} = x^{10}$.

Вычисляем остаток $r(x) = u(x) \times x^r \bmod g(x)$ в GF(2):

$r(x) = x^{10} \bmod g(x) = x^9 + x^8 + x^6 + x^5 + x^3 + 1$.

Кодовое слово: $c(x) = x^{10} + r(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^3 + 1$.

В битовом представлении $c = [0, 0, 0, 0, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1]$, где первые 5 позиций кодовой шкалы заняли информационные биты, тогда как оставшиеся 10 позиций — проверочные биты.

Предположим, что при считывании произошло две ошибки в позициях 1 и 6. Тогда искаженное кодовое слово $r = [0, \mathbf{1}, 0, 0, 1, 1, \mathbf{0}, 0, 1, 1, 0, 1, 0, 0, 1]$. Запишем искаженный принятый полином $r(x)$ через полином ошибок $e(x)$:

$r(x) = c(x) + e(x) = c(x) + x^1 + x^6$.

Вычислим синдромы с помощью выражения (3):

- $S_1 = r(\alpha^1) = \alpha^1 + \alpha^6$.

- $S_2 = r(\alpha^2) = \alpha^2 + \alpha^{12}$.
- $S_3 = r(\alpha^3) = \alpha^3 + \alpha^{18}$.
- $S_4 = r(\alpha^4) = \alpha^4 + \alpha^{24}$.

Для поля GF(2^5), $\alpha^5 + \alpha^2 + 1 = 0$, можно вычислить конкретные численные значения синдромов (см. таблица 5).

Таблица 5

Значения степеней примитивного элемента α в поле Галуа GF(2^5)

α^i	Значения	α^i	Значения	α^i	Значения
α^5	$\alpha^2 + 1$	α^{14}	$\alpha^4 + \alpha^3 + \alpha^2 + 1$	α^{23}	$\alpha^3 + \alpha^2 + \alpha + 1$
α^6	$\alpha^3 + \alpha$	α^{15}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$	α^{24}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha$
α^7	$\alpha^4 + \alpha^2$	α^{16}	$\alpha^4 + \alpha^3 + \alpha + 1$	α^{25}	$\alpha^4 + \alpha^3 + 1$
α^8	$\alpha^3 + \alpha^2 + 1$	α^{17}	$\alpha^4 + \alpha + 1$	α^{26}	$\alpha^4 + \alpha^2 + \alpha + 1$
α^9	$\alpha^4 + \alpha^3 + \alpha$	α^{18}	$\alpha + 1$	α^{27}	$\alpha^3 + \alpha + 1$
α^{10}	$\alpha^4 + 1$	α^{19}	$\alpha^2 + \alpha$	α^{28}	$\alpha^4 + \alpha^2 + \alpha$
α^{11}	$\alpha^2 + \alpha + 1$	α^{20}	$\alpha^3 + \alpha^2$	α^{29}	$\alpha^3 + 1$
α^{12}	$\alpha^3 + \alpha^2 + \alpha$	α^{21}	$\alpha^4 + \alpha^3$	α^{30}	$\alpha^4 + \alpha$
α^{13}	$\alpha^4 + \alpha^3 + \alpha^2$	α^{22}	$\alpha^4 + \alpha^2 + 1$	α^{31}	1

Подставляя значения из таблицы 5:

- $S_1 = \alpha + (\alpha^3 + \alpha) = \alpha^3$.
- $S_2 = \alpha^2 + (\alpha^3 + \alpha^2 + \alpha) = \alpha^3 + \alpha$.
- $S_3 = \alpha^3 + (\alpha + 1) = \alpha^3 + \alpha + 1$.
- $S_4 = \alpha^4 + (\alpha^4 + \alpha^3 + \alpha^2 + \alpha) = \alpha^3 + \alpha^2 + \alpha$.

Алгоритм Берлекэмпа — Мэсси итеративно строит полином-локатор ошибок $\sigma^{(i)}(x)$, который должен удовлетворять уравнению (5). Начальные условия ($i = 0$) согласно выражению (6):

- $\sigma^{(0)}(x) = \rho^{(0)}(x) = \Delta_0 = 1$,
- $i = t = 0$.

Итерация 1 ($i = 1$): расхождение $\Delta_1 = S_1 = \alpha^3 \neq 0$. Так как условие $2t = 0 < 1$ – истинно для $\Delta_0 \neq 0$, обновляем:

- $t = i - t = 1 - 0 = 1$,
- $\rho^{(1)}(x) = \sigma^{(0)}(x)/\Delta_0 = 1$,

- $\sigma^{(1)}(x) = 1 + \alpha^3 x$ (коэффициенты: $[0, \alpha^3]$).

Итерация 2 ($i = 2$): вычисляем значение $\Delta_2 = S_2 + S_1 \times \sigma_1^{(1)}(x) = (\alpha^3 + \alpha) + \alpha^3(\alpha^3)$, где $\alpha^3(\alpha^3) = \alpha^6 = \alpha^3 + \alpha$ (см. таблица 5). После подстановки $\Delta_2 = (\alpha^3 + \alpha) + (\alpha^3 + \alpha) = 0$.

Поскольку $\Delta_2 = 0$, то уравнение (4) выполняется без изменения:

- $\sigma^{(2)}(x) = \sigma^{(1)}(x) = 1 + \alpha^3 x$,
- $\rho^{(2)}(x) = x \times \rho^{(1)}(x) = x$,
- $t = 1$ (число ошибок не меняется).

Итерация 3 ($i = 3$): вычисляем расхождение $\Delta_3 = S_3 + S_2 \times \sigma_1^{(2)}(x) = (\alpha^3 + \alpha + 1) + (\alpha^3 + \alpha) \times \alpha^3 = (\alpha^3 + \alpha + 1) + (\alpha^6 + \alpha^4)$, где $\alpha^6 = \alpha^3 + \alpha$. Складываем члены по модулю два: $\Delta_3 = \alpha^3 + \alpha + 1 + \alpha^3 + \alpha + \alpha^4 = \alpha^4 + 1$ (из табл. 5: $\alpha^{10} = \alpha^4 + 1$).

Т.к. $2t = 2 < 1$ – истинно для $\Delta_3 \neq 0$:

- $t = 3 - 1 = 2$.
- $\rho^{(3)}(x) = x \times \rho^{(2)}(x) = x \times x = x^2$,
- $\sigma^{(3)}(x) = \sigma^{(2)}(x) + \Delta_3 \times \Delta_1^{-1} \times x^{(3-1)} \times \rho^{(1)}(x)$,
- $\Delta_3 \times \Delta_1^{-1} = \alpha^{10} \times \alpha^{-3} = \alpha^7$,
- $\sigma^{(3)}(x) = 1 + \alpha^3 x + \alpha^7 x^2$, коэффициенты: $[0, \alpha^3, \alpha^7]$.

Итерация 4 ($i = 4$): расхождение $\Delta_4 = S_4 + S_3 \times \sigma_1^{(3)}(x) + S_2 \times \sigma_2^{(3)}(x)$, где коэффициент при x: $\sigma_1^{(3)}(x) = \alpha^3$, при x^2 $\sigma_2^{(3)}(x) = \alpha^7$.

- $\Delta_4 = \alpha^3 + \alpha^2 + \alpha + (\alpha^3 + \alpha + 1) \times \alpha^3 + (\alpha^3 + \alpha) \times \alpha^7$,
- $(\alpha^3 + \alpha + 1) \times \alpha^3 = \alpha^6 + \alpha^4 + \alpha^3 = [\alpha^6 = \alpha^3 + \alpha] = \alpha^4 + \alpha$,
- $(\alpha^3 + \alpha) \times \alpha^7 = \alpha^{10} + \alpha^8 = [\alpha^8 = \alpha^3 + \alpha^2 + 1] = \alpha^4 + \alpha^3 + \alpha^2$,
- $\Delta_4 = \alpha^3 + \alpha^2 + \alpha + \alpha^4 + \alpha + \alpha^4 + \alpha^3 + \alpha^2 = 0$.

Поскольку $\Delta_4 = 0$ и $2t = i = 4$, вычислим:

- $\rho^{(4)}(x) = x \times \rho^{(3)}(x) = x \times (x^2) = x^3$,
- t не меняется ($t = 2$).

Итоговый полином-локатор ошибок:

$$\sigma(x) = 1 + \alpha^3 x + \alpha^7 x^2. \qquad (8)$$

Чтобы найти корни $w_t = \alpha^i$, оцениваем $\sigma(\alpha^i) = 0$, где $\alpha^i \in \mathrm{GF}(2^5)$. Подставим корни в уравнение (8):

- Для $w_1 = \alpha^{25}$: $\alpha^7(\alpha^{25})^2 + \alpha^3 \times \alpha^{25} + 1 = [\alpha^{25\times 2} \bmod N = \alpha^{19}] = \alpha^{19+7} + \alpha^{25+3} + 1 = \alpha^{26} + \alpha^{28} + 1 = [\alpha^{26} = \alpha^4 + \alpha^2 + \alpha + 1,\ \alpha^{28} = \alpha^4 + \alpha^2 + \alpha$ (см. таблица 5)$] = 0$ (все члены сокращаются по модулю 2).
- Для $w_2 = \alpha^{30}$: $\alpha^7(\alpha^{30})^2 + \alpha^3 \times \alpha^{30} + 1 = (\alpha^{67} + \alpha^{33} + 1) \bmod N = \alpha^5 + \alpha^2 + 1 = [\alpha^5 = \alpha^2 + 1$ (см. таблица 5)$] = 0$.

С помощью выражения (7) запишем:

- Для $w_1 = \alpha^{25}$: $\varphi_1 = -25 \bmod 31 = 6$,
- Для $w_2 = \alpha^{30}$: $\varphi_2 = -30 \bmod 31 = 1$.

Позиции ошибок $\varphi_1 = 1$ и $\varphi_2 = 6$ на шкале соответствуют исходным данным о внесенных ошибках. Инвертируем биты в найденных позициях и получаем исходное кодовое слово:

$c' = [0, \mathbf{0}, 0, 0, 1, 1, \mathbf{1}, 0, 1, 1, 0, 1, 0, 0, 1]$,

где биты на позициях 0…4 шкалы формируют информационное кодовое слово:

$u' = [0, 0, 0, 0, 1]$.

Анализ и сопоставление с известными результатами

Проведем сравнение предложенного подхода с известными решениями для 5-разрядного цифрового преобразователя угла на основе псевдослучайной кодовой шкалы (длина информационного слова $m = 5, N = 31$ положение кодовой шкалы).

Как отмечалось ранее, метод на основе кода Хэмминга обеспечивает исправление только одиночных ошибок ($t = 1$) при кодовом расстоянии $d = 3$. Несмотря на то, что применение однодорожечной ПСКШ позволяет уменьшить массогабаритные характеристики за счет использования единственной дорожки, помехоустойчивость такой системы остается сравнительно низкой и не защищает от множественных искажений данных.

В качестве альтернативы часто рассматривается тройное модульное резервирование (TMR) каналов считывания. Данный метод позволяет маскировать сбои длиной до 5 бит ($t \leq 5$) в одном из трех каналов посредством мажоритарного голосования. Однако TMR остается уязвимым к коррелированным сбоям, затрагивающим все три дорожки одновременно. Кроме того, TMR сопряжен с высокой аппаратной избыточностью (до 200%), что делает его нецелесообразным для систем с жесткими массогабаритными ограничениями.

В недавнем патенте [23] предложено решение, обеспечивающее исправление четырехкратных ошибок ($t = 4$) за счет введения дополнительных корректирующих считывающих элементов. Формируемый циклический код содержит $m = 5$ информационных и $r = 15$ корректирующих бит и обладает минимальным кодовым расстоянием $d = 9$.

Разработанный метод на основе БЧХ-кода позволяет гибко настраивать корректирующую способность: для поля GF(2^m) и примитивного элемента α можно построить циклический код, исправляющий t ошибок, где t выбирается в зависимости от требований к надежности и допустимой аппаратной сложности.

Для укороченного кода с параметрами (25, 5, 11) теоретически достижимо исправление до

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{11-1}{2} \right\rfloor = 5$$

ошибок. Однако практическая реализация соответствующего декодера требует вычисления $2t = 10$ синдромов и построения полинома-локатора ошибок 5-й степени. Сложность алгоритма Берлекэмпа — Мэсси составляет $O(t^2)$ операций в поле Галуа, а поиск корней полинома локатора — $O(n \cdot t)$, что приводит к существенному росту аппаратной сложности и увеличению времени задержки сигнала при реализации на ПЛИС [24]. Поэтому в качестве примера выбран режим $t = 2$, позволяющий наглядно проиллюстрировать работоспособность подхода.

Верификация предложенной модели выполнена в специализированном консольном приложении на языке Python с использованием библиотек NumPy и galois. Программный комплекс обеспечивает генерацию псевдослучайных

кодовых шкал на основе М-последовательностей, синтез циклических БЧХ-кодов, а также моделирование процессов кодирования, декодирования и коррекции ошибок.

Заключение

В работе представлена аналитическая модель цифрового преобразователя угла повышенной информационной надежности, основанная на применении М-последовательностей и циклических кодов Боуза–Чоудхури–Хоквингема с вычислениями в поле Галуа. Модель обеспечивает гибкую настройку уровня помехоустойчивости без увеличения массогабаритных характеристик благодаря встраиванию корректирующих функций непосредственно в структуру однодорожечной псевдослучайной кодовой шкалы. Результаты моделирования подтверждают корректность работы модели для разрядностей энкодера 5…16 бит, что соответствует периодам М-последовательности в 31…65535 символов.

Предложенная модель может быть реализована на программируемых логических интегральных схемах (ПЛИС) в системах управления, где критически важны массогабаритные характеристики и высокая отказоустойчивость.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Conflict of interest

The author declares no conflict of interest.

Список источников

1. Ozhiganov A.A., Tarasyuk M.V. The use of error-correcting codes in displacement transducers with combinatorial scales // Measurement Techniques. 2016.Vol. 59, no 1. P. 16–20.

2. Ozhiganov A.A., The use of hamming codes in digital angle converters based on pseudo-random code scales // Measurement Techniques. 2015. Vol. 58, no. 5. P. 28–32.

3. Богданов Д.С., Богданова И.А., Волныкин А.Н. Радиационная стойкость радиоэлектронного устройства в условиях космического пространства // Вестник РГРТУ. 2019. № 70.

4. Renishaw. RESOLUTE Absolute Encoder System: Technical Manual. 2020.

5. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки / пер. с англ. М.: Мир, 1976. 594 с.

6. Блейхут Р. Теория и практика кодов, контролирующих ошибки / пер. с англ. М.: Мир, 1986. 576 с.

7. Ожиганов А.А., Псевдослучайные кодовые шкалы // Изв. вузов. Приборостроение. 1987. Т. 30, № 2. С. 40–43.

8. Golomb S.W. Shift register sequences. Aegean Park Press, 1982. 247 p.

9. Massey J.L. Shift-Register Synthesis and BCH Decoding // IEEE Transactions on Information Theory. 1969. Vol. 15, iss. 1. P. 122–127.

10. Макуильямс Ф.Д., Слоан Н.Д. Псевдослучайные последовательности и таблицы // ТИИЭР. 1976. Т. 64, № 12. С. 80–95.

11. Ожиганов А.А. Алгоритм размещения считывающих элементов на псевдослучайной кодовой шкале // Изв. вузов СССР. Приборостроение, 1994. Т. 37, № 2. С. 22–27.

12. Bose R.C., Ray-Chaudhuri D.K. On a class of error-correcting binary group codes // Information and Control. 1960. Vol. 3, no. 1, P. 68–79.

13. Error correction for algebraic block codes: patent US Patent 4633470 / Welch L.R., Berlekamp E.R. Filed 27.09.1986. 17 p.

14. Псевдослучайная кодовая шкала: патент RU 2777832 C1 / Ожиганов А.А., Пребыткин П.А.; патентообладатель Открытое акционерное общество «Авангард» Заявка 2022103349, дата подачи заявки 09.02.2022; опубл. 11.08.2022, Бюл. № 23. 13 с.

References

1. Ozhiganov A.A., Tarasyuk M.V. The use of error-correcting codes in displacement transducers with combinatorial scales. *Measurement Techniques*, 2016.vol. 59. no 1. pp. 16–20.

2. Ozhiganov A.A., The Use of Hamming Codes in Digital Angle Converters Based on Pseudo-Random Code Scales. *Measurement Techniques,* 2015. vol. 58, no. 5. pp. 28–32.

3. Bogdanov D.S., Bogdanova I.A., Volnykin A.N. *Vestnik RGRTU*, 2019, no. 70.

4. Renishaw. *RESOLUTE Absolute Encoder System*. Technical Manual, 2020.

5. Peterson W., Weldon E.J., Jr. *Error-Correcting Codes*. MIT Press, 1972. xi, 560p.
6. Blahut R.E. *Theory and Practice of Error Control Codes,* Reading, Mass., etc., 1984.
7. Ozhiganov A.A. *Izv. vuzov. Priborostroenie*, 1987, vol. 30, no 2. pp. 40–43.
8. Golomb S.W. *Shift register sequences*. Aegean Park Press, 1982. 247 p.
9. Massey J.L. Shift-Register Synthesis and BCH Decoding. *IEEE Transactions on Information Theory*, 1969, vol. 15, iss. 1. pp. 122–127.
10. McWilliams F.D., Sloan N.D. *TIIEHR,* 1976, vol. 64, iss. 12. pp. 80–95.
11. Ozhiganov A.A. *Izv. vuzov SSSR. Priborostroenie*, 1994, vol. 37, no. 2, pp. 22–27.
12. Bose R.C., Ray-Chaudhuri D.K. On a class of error-correcting binary group codes. *Information and Control*, 1960, vol. 3, no. 1, pp. 68–79.
13. Welch L.R., Berlekamp E.R. *Error correction for algebraic block codes:* patent US Patent 4633470. Filed 27.09.1986. 17 p.
14. Ozhiganov A.A., Prebytkin P.A. *Pseudo-random code scale*. Patent RU 2777832. Date of publication 11.08.2022. Bull. no. 23. 13 p.

Информация об авторах

Влада Вадимовна Алексеева, инженер-программист, лаборатория цифровых преобразователей угла, АО «НИТИ «Авангард», Санкт-Петербург, Россия; e-mail: ladarobotics@gmail.com

Information about the authors

Vlada V. Alekseeva, Software engineer, Digital Angle Converters Laboratory, JSC «SRTI «Avangard», Saint Petersburg, Russia; e-mail: ladarobotics@gmail.com

Получено 12 января 2026 ● Принято к публикации 27 мая 2026 ● Опубликовано 25 июня 2026
Received 12 January 2026 ● Accepted 27 May 2026 ● Published 25 June 2026