

УДК 004.056.53

В.А. Василенко, ст. преподаватель,

Д.В. Степаненко

Севастопольский национальный технический университет

ул. Университетская 33, г. Севастополь, Украина, 99053

E-mail: isd@bios.inf.net

АЛГОРИТМ ОЦЕНКИ ГЛУБИНЫ РАСПРОСТРАНЕНИЯ ОШИБОК В СВЕРТОЧНЫХ ОРТОГОНАЛИЗИРУЕМЫХ КОДАХ

Рассматриваются методы анализа распространения ошибок при декодировании сверточных кодов. Приводится алгоритм определения устойчивости регистра связи и пример его реализации.

При декодировании сверточных кодов часто наблюдается явление распространения ошибок, которое состоит в том, что однажды возникшая ошибка декодирования может привести к возникновению ошибок в последующие моменты времени. В случае сверточных кодов, когда при кодировании каждый информационный символ воздействует на несколько блоков, возникновение одиночной ошибки при декодировании оказывает влияние на декодирование нескольких последующих блоков, а при некоторых неблагоприятных условиях и на бесконечное число блоков. Таким образом, при построении сверточных кодов необходимо стремиться достичь не только высокой корректирующей способности, но и по возможности минимальной глубины распространения ошибок.

Глубина распространения ошибок при декодировании с обратной связью определяется структурой логических схем декодера, и поэтому анализ этой структуры сводится к анализу функционирования регистров сдвига с нелинейной обратной связью (РС с НОС), образующих декодирующие логические схемы. Если шумы превышают корректирующую способность кода и это приводит к появлению ошибки декодирования, то обычно в течение некоторого периода времени ошибок не возникает, декодирующая логическая схема автоматически возвращается в нормальное рабочее состояние и распространение ошибок прекращается. В этом случае глубина распространения ошибок конечна. Если же декодирующая логическая схема в нормальное рабочее состояние не возвращается, то глубина распространения ошибок считается бесконечной. Таким образом, анализ распространения ошибок сводится к анализу работы РС с НОС, когда на их входы подаются нулевые сигналы, т.е. в режиме самоконтроля.

Целью данной статьи является анализ распространения ошибок в сверточных кодах и разработка алгоритмов оценки глубины такого распространения.

Предположим, что есть некоторый регистр сдвига, предназначенный для хранения символов синдрома, и логическая декодирующая схема декодера (рисунок 1).

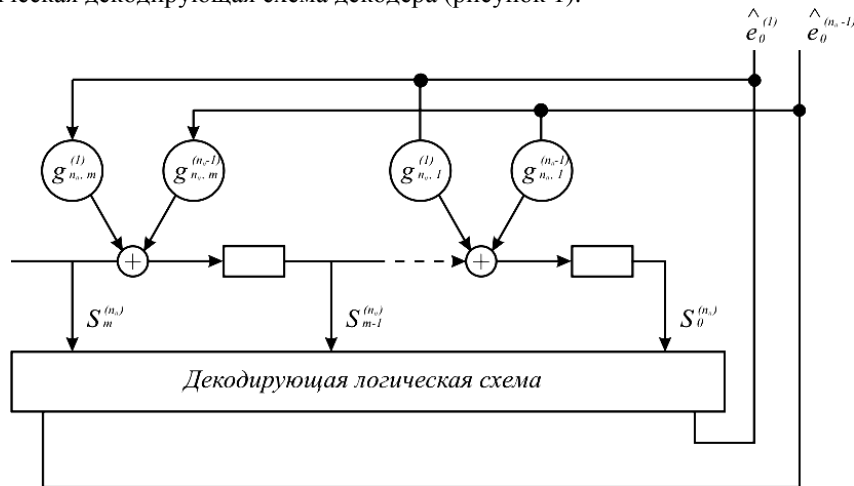


Рисунок 1 — Регистр синдрома и логическая часть декодирующей схемы

В данном случае синдром

$$S^{(n_0)}(D) = S_0^{(n_0)} + S_1^{(n_0)}D + S_2^{(n_0)}D^2 + \dots$$

Вычисляется в декодере согласно правилу

$$S^{(n_0)}(D) = \sum_{j=1}^{n_0-1} G_{(n_0)}^{(j)}(D)E^j(D) - E^{(n_0)}(D)$$

и подается на вход регистра синдрома, показанного на рисунке 1.

При исправлении случайных ошибок с помощью порогового декодирования логическая декодирующая схема в момент времени t по исправленному синдрому, символы которого получаются из

символов синдрома $S_0^{(n_0)}, S_1^{(n_0)}, \dots, S_m^{(n_0)}$ вычитанием информационных шумовых сигналов, возникающих до момента O , формирует оценки $e_0, \dots, e_0$ значений шумовых символов в момент времени O . Используемый при этом исправленный синдром имеет вид:

$$\delta(m) = [\delta_0(m), \delta_1(m), \dots, \delta_n(m)].$$

Внутреннее состояние декодирующей логической схемы (рисунок 1) определяется состояниями $(m+1)$ ячеек регистра сдвига. Если после момента возникновения ошибки декодирования в течение m последующих моментов времени декодирование происходит правильно, то влияние этой ошибки декодирования исчезает и схема оказывается в нормальном рабочем состоянии. Следовательно, необходимым условием возникновения бесконечного распространения ошибок является возникновение после каждой ошибки декодирования в течение m последующих моментов времени новой ошибки декодирования. Простейший нелинейный регистр сдвига показан на рисунке 2.

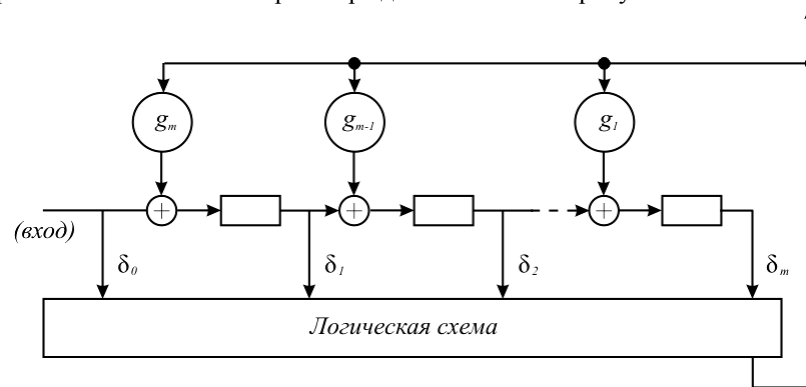


Рисунок 2 — Нелинейный регистр сдвига

На вход регистра с НОС (рисунок 2) подается последовательность из одних нулей, т.е. в режиме самоконтроля. Пусть $\delta = (\delta_0, \delta_1, \dots, \delta_m)$ — внутреннее состояние РС и O — вектор, все компоненты которого равны нулю. Если обозначить через T оператор следующего состояния, то функционирование схемы можно описать следующим образом:

$$T\delta = F(\delta).$$

Здесь F — некая векторная функция ($F(0) = 0$). Вектор $T\delta$ представляет собой состояние нелинейного регистра сдвига после однократного сдвига, а $T^N\delta$ — после N последовательных сдвигов. Из того, что $F(0) = 0$, следует, что $TO = 0$, т.е. O — равновесное состояние РС с НОС.

Известно, что если для каждого состояния δ существует такое N , что $T^N\delta = O$, то РС с НОС считается устойчивым, в противном случае — неустойчивым.

Для самоортогональных кодов существуют простые достаточные условия устойчивости, которые оказываются полезными и на практике.

Для произвольных кодов таких критериев не существует. Можно при анализе РС с НОС воспользоваться либо методом Ляпунова, либо Робинсона.

Если вес внутреннего состояния РС с НОС обозначить через $W(\delta)$, то необходимое условие устойчивости пороговой кодирующей схемы состоит в следующем.

Если каждый шаг декодирования, при котором значение оценки шумового сигнала равно 1, приводит к уменьшению веса внутреннего состояния ($W(T\delta) \leq W(\delta)$), то декодирующая логическая схема является устойчивой.

По Ляпунову РС с НОС является устойчивым, если при сдвиге любое его ненулевое внутреннее состояние переходит в состояние O и неустойчивым, если при сдвиге никакое состояние, кроме нулевого, не переходит в состояние O . Однако, в действительности часть ненулевых состояний при сдвиге переходит в состояние O , но существуют также так называемые неопределенные состояния, которые при сдвиге в состояние O не переходят. Предлагаемый алгоритм определения устойчивости касается случая неопределенности состояний. Он может быть записан следующим образом.

1. Пусть C_0 — множество, включающее только состояние O .
2. Пусть есть некоторая функция $D(\delta)$, которая принимает два значения $D(0) = 0$, если $\delta \in C$ (C — произвольное множество векторов) и $D(\delta) = 1$, если $D(\delta) \in \bar{C}$. Если $D_0(\delta)$ — функция такая, что $D_0(\delta) = 0$ и

$D_0(\delta)=1$ при всех $\delta \neq 0$ тогда РС с НОС будет неустойчивым если $\Delta D_0=0$ (ΔD — изменение $D(\delta)$ при изменении состояния δ при сдвиге) при всех δ и устойчивым, если $\Delta D_0=1$ при всех $\delta \neq 0$.

3. Пусть S_1 — множество таких δ , что $D_0(\delta)=1$, и пусть $C_1 = C_0 \cup S_1$. Состояния, принадлежащие S_1 , обладают тем свойством, что при сдвиге они переходят в состояние O . Если $\overline{C}$ является пустым множеством, то рассматриваемая схема устойчива, а если $S_1 \neq \emptyset$ то неустойчивая. Если ни одного из этих условий не выполняется, то переходим к следующему шагу.

4. Определим функцию $D_1(\delta)$ ($D_1(\delta)=0$, если $\delta_1 \in C_1$ и $D_1(\delta)=1$, если $\delta_1 \in \overline{C_1}$).

5. Пусть S_2 — множество всех состояний δ , для которых $\Delta D_1(\delta)=1$ и пусть $C_2 = C_1 \cup S_2$. К S_2 относятся те состояния, которые переходят в состояние O в результате двух сдвигов.

6. Этот процесс будем продолжать до тех пор, пока одно из множеств $\overline{C_M}$ или S_M не окажется пустым. Если $\overline{C_M} = \emptyset$ то схема является устойчивой. Если $S_M \neq \emptyset$, то существует некоторое не нулевое состояние, которое никогда в состояние O не переходит, это означает неустойчивость исследуемой схемы.

Для примера воспользуемся предложенным алгоритмом для определения устойчивости декодирующей логической схемы (рисунок 3). В целях упрощения внутреннее состояние этого регистра будем представлять в десятичной записи, а именно, состоянию $\delta = (\delta_0, \delta_1, \delta_2, \delta_3, \delta_4, \delta_5)$ сопоставим десятичное число $\delta_1 + \delta_2 \cdot 2 + \delta_3 \cdot 2^2 + \delta_4 \cdot 2^3 + \delta_5 \cdot 2^4$ ($\delta_0 = 0$). Состояния ячеек регистра, которые могут принимать значения 0 и 1, обозначим через X .

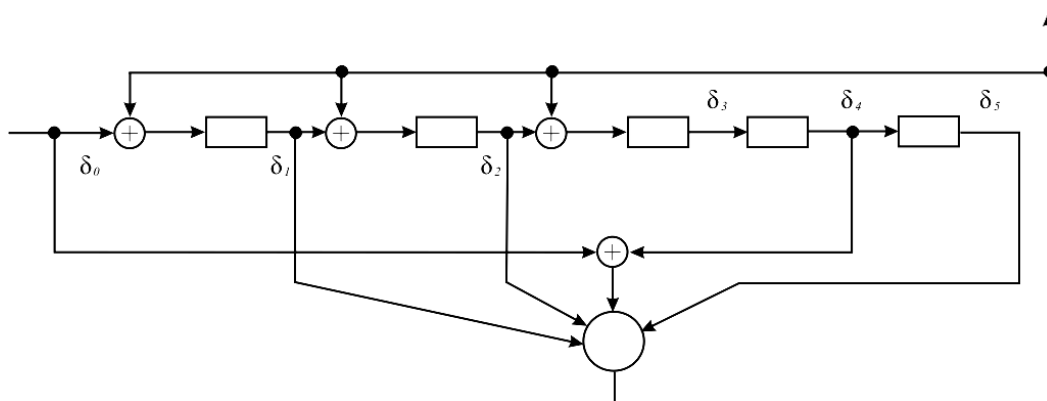


Рисунок 3 — Регистр синдрома (12, 6) кода

Воспользуемся вышеописанным алгоритмом. Тогда получаем следующее:

1. При однократном сдвиге только состояние $\delta = (0,0,0,0,1)$ (десятичное представление числа 16) переходит в состояние O .

2. При однократном сдвиге в состояние 16 переходит лишь состояние вида $\delta = (0,0,0,1,X)$, т.е. состояния 8 и 24.

3. При однократном сдвиге в состояние 8 или 24 переходят лишь состояния вида $\delta = (0,0,1X,X)$, т.е. состояния 4, 20, 12 и 28.

4. При однократном сдвиге в состояния 4, 20, 12 и 28 переходят лишь состояния вида $\delta = (0,1,X,1,0)$ и $\delta = (0,1,X,0,0)$, т.е. состояния 2, 18, 10, 6, 22, 24. Продолжая этот процесс, построим таблицу и найдем, что $S_9 = \emptyset$. Это означает, что рассматриваемая система неустойчива.

Таблица 1 — Алгоритм анализа глубины ошибок

j	S_j	Число элементов $\overline{C_j}$	$P_j(S)$
1	16	30	$\delta_5(\delta_4+1)(\delta_3+1)(\delta_2+1)(\delta_1+1)$
2	8, 24	28	$\delta_4(\delta_3+1)(\delta_2+1)(\delta_1+1)$
3	4, 20, 12, 28	24	$\delta_3(\delta_2+1)(\delta_1+1)$
4	2, 18, 10, 6, 22, 14	18	$(\delta_4\delta_5+1)\delta_2(\delta_1+1)$

5	1, 17, 9, 5, 21, 3, 7	11	$\delta_1[(\delta_2 + 1)(\delta_3 + 1)\delta_4(\delta_5 + 1) + \delta_2(\delta_4 + 1)(\delta_5 + 1) + (\delta_2 + 1)(\delta_4 + 1)]$
6	25, 17, 11, 27, 23	6	$\delta_1[\delta_2(\delta_3 + 1)\delta_4 + \delta_2 + \delta_3(\delta_4 + 1)\delta_5 + \delta_2\delta_5(\delta_3 + 1)(\delta_4 + 1) + \delta_4\delta_5(\delta_3 + 1)(\delta_2 + 1)]$
7	26, 30, 15, 31	2	$\delta_4\delta_2[\delta_5(\delta_1 + 1) + \delta_3\delta_1]$
8	13	1	$\delta_1(\delta_2 + 1)\delta_4\delta_3(\delta_5)$
9	0	1	неустойчива

Однако вывод о неустойчивости схемы (рисунок 3) не означает, что она имеет бесконечную глубину распространения ошибок. Из всех внутренних состояний РС с НОС с распространением ошибок связаны лишь так называемые достижимые состояния, т.е. те состояния, в которых регистр может оказаться при возможных синдромах на его входе. Если РС с НОС является устойчивым по отношению к входному воздействию, то глубина распространения ошибок бесконечной быть не может.

В результате исследований получили методику анализа глубины распространения ошибок при кодировании сверточными кодами с использованием РС с НОС, что позволяет более эффективно выбирать технические средства для подобных кодов.

Дальнейшие пути исследования в этом направлении предполагают автоматизацию и оптимизацию алгоритмов кодирования и декодирования на основе мгновенных оценок шумового сигнала.

Библиографический список

1. Анин Б.Ю. Защита компьютерной информации / Б.Ю. Анин. — СПб.: Изд-во «БХВ — Санкт Петербург», 2000. — 384 с.
2. Василенко В.А. Организация потоковых шифров на базе регистров с обратной связью по переносу / В.А. Василенко, В.В. Кудрявченко // Вестник Сев.ГТУ. Сер. Физика и математика: сб. научн. тр. — Севастополь, 2006. — Вып. 74. — С. 96 — 100.
3. Коробейников А.Г. Математические основы криптологии: учеб. пособие / А.Г. Коробейников, Ю.А. Гатчин. — СПб.: ГУ ИТМО, 2004. — 106 с.

Поступила в редакцию 28.03.2008 г.