С.И. Гуров

СПЕКТРАЛЬНЫЙ R-КОД С ПРОВЕРКАМИ НА ЧЁТНОСТЬ*

Введение. Постановка задачи

Повышение надёжности функционирования интегральных схем (ИС) остаётся актуальной проблемой их синтеза. Важной стороной этой проблемы является устойчивость схем к кратковременным самоустраняемым отказам – *сбоям,* причиной которых является воздействия различных видов помех: радиационных, скачков напряжений питания, деградаций сигналов во времени и др.

Перспективным подходом решения данной проблемы является применение избыточного кодирования информационных потоков ИС [1-3, 7, 8]. При разработке соответствующих аппаратных средств следует учитывать следующие особенности задачи, из которых будут вытекать требования к свойствам выбираемого кода.

1. Прежде всего, как правило, считают, что исходная функциональная схема спроектирована и не подлежит изменению.
2. Проверочные биты вычисляются специальной корректирующей схемой, параллельно и одновременно с информационными, вычисляемыми основной функциональной схемой, в то время как при классическом подходе предполагается кодирование уже имеющегося сообщения.
3. Выигрыш в суммарной площади основной и корректирующей схем при описываемом подходе получается из-за того, что число проверочных разрядов меньше, и обычно – значительно, числа информационных, и методы минимизации позволяют синтезировать корректирующую схему существенно меньшей площади, чем основная.
4. Коды с оптимальными характеристиками избыточности требуют кодирующих и декодирующих устройств повышенной сложности, поэтому при выборе кода необходимо учитывать все факторы, влияющие на сложность реализации схемы.
5. Для комбинационных схем представляется естественным строить корректирующие схемы для также комбинационными, что означает ограничение на реализацию алгоритмов декодирования, заключающееся в отказе от использования последовательностных элементов: сдвиговых регистров, счётчиков и др.
6. Проведённые эксперименты показали, что наиболее вероятный одиночный сбой функционального элемента схемы, как правило, ли-

* Исследование выполнено при финансовой поддержке РФФИ, проект № 16-01-00196

бо маскируется, либо приводит к инвертированию единственного разряда на выходе схемы, т. е. кратные ошибки маловероятны [3].

Для синтеза сбоеустойчивых схем обычно предлагают коды, исправляющую одиночную единичную и обнаруживающие двойную ошибку (SEC / DED[1]). Конкретно, применяют либо модифицированные коды Хэмминга, либо низкоплотностные (LDPC). Отметим, что применение последних упрощает реализацию кодирования и декодирования.

Представляется актуальной разработка альтернативного известным кода для эффективного решения рассматриваемой задачи. В статье предлагается такой новый код.

Коды с проверкой на чётность

При разделимом блоковом кодировании кодовые слова (n, k)-кода имеют длину $n = k + m$, где k – число информационных разрядов, повторяющих символы сообщения, а m - число проверочных разрядов.

Систематическим кодом с проверкой на чётность называется двоичный блоковый код, в котором каждому сообщению $\boldsymbol{u} = (u_1, \dots, u_k)$ сопоставлено кодовое слово $\boldsymbol{v} = (v_1, \dots, v_n)$, определяемое соотношениями

$$v_i = \begin{cases} u_i, & 1 \leqslant i \leqslant k, \\ \sum_{j=1}^{k} u_j \cdot g_{i-k-1,j}, & k+1 \leqslant i \leqslant n, \end{cases} \quad (1)$$

где $\sum$ означает сумму по *mod 2*, а множество двоичных символов $\{g_{i,j}\}$, $0 \leqslant i \leqslant m-1$, $1 \leqslant j \leqslant k$, которое задаёт метод кодирования, фиксировано [4]. Таким образом, мы предполагаем размещение символов сообщения в первых позициях кодового слова.

Общий код с проверкой на чётность определяется соотношением

$$v_i = \sum_{j=1}^{k} u_j \cdot g_{i,j}, \qquad 1 \leqslant i \leqslant n,$$

которое задаёт кодирование общего вида, в т. ч. несистематическое.

Ясно, что все блоковые линейные коды, в том числе исправляющие одну ошибку коды Хемминга, Хсяо и низкоплотностные (LDPC) являются кодами с проверкой на чётность. Заметим, у большинства кодов длина кодовых слов определяется однозначно. Это обстоятельство накладывает существенные ограничения на число информационных разрядов k в кодовом слове. Хотя из (n, k)-циклического кода можно получить $(n-i, k-i)$, $1 \leqslant i < k$ *укороченный код*, для больших значений i такая процедура либо становится слишком трудной, либо требует привлечения достаточно

[1] Single error correction / Double error detection

сложных нетрадиционных подходов [5]. При этом укорачивание кодов Хэмминга проводится элементарно.

Спектральный код на основе функций Радемахера

Опишем новый систематический код с проверками на чётность, имеющий произвольное число k информационных разрядов, определив двоичные символы $\{g_{i,j}\}$ в (1) как набор $q+1$ функций от j. Предположим сначала, что $k = 2^q$, это ограничение потом легко снимается.

Для $k = 2^q, 1 \leqslant j \leqslant k$ положим

$$g_{0,j} \equiv 1, \;\; g_{1,j} = 1 \Leftrightarrow j = 2^{q-1}+1, 2^{q-1}+2, \dots, k,$$

$g_{i,j}$ – функция с периодом длины 2^{q-i+1} из подряд идущих 2^{q-i} нулей и такого же количества единиц, $2 \leqslant i \leqslant q$.

Ясно, что данные функции могут быть получены линейными преобразованиями аргумента и значений функций Радемахера [9]. Таким образом, будут получены $m = q+1$ проверочных разрядов и образован блоковый систематический код длины $n = 2^q + q + 1$ с проверкой на чётность. Система функций Радемахера используется для построения функций Уолша, по которым, как по базису, осуществляют спектральное разложение кусочно-постоянных булевых функций. В силу этого полученный код предлагается называть *R-спектральным*.

Ясно, что порождающая матрица G_R данного кода есть единичная k-го порядка матрица I_k с присоединённой справа транспонированной порождающей матрицей $G_{RM}(k,1)$ кода Рида-Маллера длины 2^k первого порядка: $G_R = [\, I_k \mid G_{RM}^T(k,1) \,]$. Также G_R может быть получена из кода Макдональда (дуального к расширенному коду Хэмминга).

Покажем, что построенный код способен исправлять ошибку инвертирования некоторого разряда в $\boldsymbol{u}$. Для этого примем ещё одно допущение, что одиночная ошибка может произойти только в информационных битах, т. е. $\boldsymbol{w'} = (w_1, \dots, w_k) = \boldsymbol{u} + \boldsymbol{e}, \;\; \boldsymbol{e} = (e_1, \dots, e_k)$, где $\boldsymbol{w'}$ – начальная часть полученного вектора, содержащая информационные разряды, а $\boldsymbol{e}$ - вектор ошибки, содержащий не более двух 1. Это ограничение мы далее обойдём.

Вычислим синдромы $s_0, \dots, s_q$ для вектора $\boldsymbol{w'}$:

$$s_i = \sum_{j=1}^{k} w_j \cdot g_{i,j}\,, \qquad 0 \leqslant i \leqslant q$$

и значения $r_i = w_{k+i} + s_i, \;\; i = 1, \dots, q$. Если $s_0 = 1$, то произошла одиночная ошибка, и, как нетрудно видеть, номер искажённого разряда может быть получен дешифрованием вектора $\boldsymbol{r} = (r_1, \dots, r_q)$, поскольку инвертирование какого-либо одиночного разряда в $\boldsymbol{u}$ приводит к одной из 2^k ком-

бинаций вектора $\boldsymbol{r}$ и данное отображение биективно. Данное свойство есть следствие того, что совокупность векторов $(g_{1,j}, \dots, g_{q,j})$, $j = \overline{1, 2^q}$ совпадает со всеми двоичными наборами дины q. Ясно, что вычисление вектора ошибки происходит по *упрощённой схеме*: входом является синдром ошибки разрядности $n - k - 1$, а выходом - вектор ошибки разрядности k.

При $s_0 = 0$, то если $\boldsymbol{r}$ – нулевой вектор, то ошибки нет, и произошли две ошибки, иначе.

Построенный спектральный линейный нециклический R-код имеет кодовое расстояние $d = 2$: нулевой вектор и вектор, имеющий 1 только в первом и $(k + 1)$-м разрядах – его кодовые слова. Но, тем не менее, R-код позволяет исправлять одиночную ошибку в информационных разрядах полученного слова.

Рассмотрим пример с $q = 3$. Значения коэффициентов $g_{i,j}$, $0 \leqslant i \leqslant 3$, $1 \leqslant j \leqslant 8$ представлены ниже в таблице, являющейся порождающей матрицей РМ-кода первого порядка длины 8:

$g_{0,j}$	1	1	1	1	1	1	1	1
$g_{1,j}$	0	0	0	0	1	1	1	1
$g_{2,j}$	0	0	1	1	0	0	1	1
$g_{3,j}$	0	1	0	1	0	1	0	1
Позиции информационных разрядов, j	1	2	3	4	5	6	7	8

Мы видим, что значения вектора $(g_{1,j}, g_{2,j}, g_{3,j})$ есть двоичный код числа $j - 1$. Значения проверочных $v_9, \dots, v_{12}$ разрядов для $\boldsymbol{u} = (u_1, \dots, u_8)$ будут определяться соотношениями

$$v_9 = u_1 + u_2 + u_3 + u_4 + u_5 + u_6 + u_7 + u_8,$$
$$v_{10} = u_5 + u_6 + u_6 + u_8,$$
$$v_{11} = u_3 + u_4 + u_7 + u_8,$$
$$v_{12} = u_2 + u_4 + u_6 + u_8.$$

Если ошибка произошла, например, в 5-м разряде, то $r_1 = 1$, $r_2 = r_3 = 0$, при ошибке в 8-м разряде будем иметь $r_1 = r_2 = r_3 = 1$ и т. д., т. е. для определения разряда, в котором произошла ошибка, может использоваться стандартная схема дешифратора.

R-код: снятие ограничений, применение для синтеза сбоеустойчивых схем

Ограничение $k = 2^q$ легко снимается: при $2^{q-1} < k \leqslant 2^q$ строим код для q как указано выше и отбрасываем последние $2^q - k$ значений $\boldsymbol{v}$ и коэффициентов $g_{i,j}$. В результате получен $(\lceil \log k \rceil + 1 + k, k)$-код, исправляющий одиночную ошибку в информационных битах.

Кодирование и декодирование R-кодов и кодов Хемминга проходит по общей схеме. В неукороченном случае и при небольшом укорочении R-код уступает коду Хемминга по избыточности на пренебрежимо малую величину, а при большом укорочении эти коды могут иметь и одинаковую избыточность. R-коды, очевидно, экономнее многомерных итеративных кодов и LDPC-кодов: параметры последних для случая исправления одиночной ошибки приведены в [6].

Можно легко избавиться от последнего и, казалось бы, существенного ограничения на одиночную ошибку – предположения о её появлении лишь в информационных битах. Для этого достаточно удвоить в кодовом слове символ v_{k+1}, лишь незначительно увеличив избыточность кода и сложность декодирования. Этого, однако, можно не делать при использовании R-кодов для решения рассматриваемой задачи.

Для исключения появления ошибки уже в процессе проверки и исправления выходного вектора в ИС (проблема «сторожа над сторожем»), корректирующую схему, с помощью специальных схемотехнических и технологических методов, выполняют в специальном сбоеустойчивом варианте, и поэтому этот процесс можно считать свободным от ошибок. Платой за такую безошибочность служит увеличение площади корректирующей схемы.

При исправлении одиночной ошибки кодом Хэмминга и LDPC площадь корректирующей схемы может составлять *130%* площади основной [8]. Обоснованно предположить, что использование предлагаемых R-кодов позволит существенно улучшить данный результат, поскольку схемотехнической защитой можно будет обеспечивать функциональные элементы корректирующей схемы, вычисляющие не все m проверочных бит, а только единственный $(k+1)$-й бит.

Также давно известно [1], что общая сложность корректирующей схемы при реализации метода избыточного кодирования зависит, первую очередь, от сложности определения синдрома, вычисление которого у которого у R-кода не представляет трудностей: проверочная матрица имеет меньшее число единиц и вычисления производятся по укороченной схеме.

При использовании корректирующих кодов важно заметить и исправить ошибку именно в информационных, а не в проверочных символах. Это очевидное замечание, а также особенности применения избыточного кодирования в задаче синтеза сбоеустойчивых схем позволяет ожидать, что применение R-кода окажется весьма эффективным.

Структура R-кода позволяет предполагать возможность для них эффективных мажоритарных методов декодирования, а также конструирования кодов, исправляющих более одной ошибки и построенных на той же идее.

Автор благодарит зав. отделом ИППМ РАН С. В. Гаврилова за полезные консультации.

Литература

1. *Коц Ч.* Коды с исправлением ошибок и их реализация в цифровых системах / В кн.: Методы введения избыточности для вычислительных систем / Под ред. В. С. Пугачева. – М.: Сов. радио, 1966. С. 179-229.
2. *Хетагуров Я.А., Руднев Ю.П.* Повышение надёжности цифровых устройств методами избыточного кодирования. М.: Энергия, 1974.
3. *Гаврилов С.В., Гуров С.И., Жукова Т.Д., Рыжова Д.И., Тельпухов Д.В.* Методы повышения сбоеустойчивости комбинационных ИМС методами избыточного кодирования // Прикладная математика и информатика. № 53. М.: МАКС Пресс, 2016. С. 93-102.
4. *Галлагер Р.* Теория информации и надёжная связь. – М.: Сов. радио, 1974.
5. *Вернер М.* Основы кодирования. – М.: Техносфера, 2004.
6. Кодирование информации (двоичные коды). Справочник / Под ред. проф. Н.Т. Березнюка. - Харьков: Вища школа, 1978.
7. *Poolakkaparambil M., Mathew J.* BCH code based multiple bit error correction in finite field multiplier circuits. - ISQED, 2011, pp. 1-6.
8. *Mahesh Poolakkaparambil, Jimson Mathew and Abusaleh Jabir.* Multiple Bit Error Tolerant Galois Field Architectures Over $GF(2^m)$ // Electronics, 2012, **1**, pp. 3-22.
9. *Беспалов М.С., Скляренко В.А.* Функции Уолша и их приложения Учебное пособие. - Владим. гос. ун-т. имени Александра Григорьевича и Николая Григорьевича Столетовых - Владимир: Изд-во ВлГУ, 2012.