**УДК 519.725, 621.3.049.771.14**

**R-код для синтеза Сбоеустойчивых ИС**

*С.И. Гуров*

*Московский государственный университет имени М.В. Ломоносова*

*sgur@cs.msu.ru*

Важной стороной задачи синтеза интегральных схем (ИС) остаётся проблема устойчивости их к кратковременным самоустраняемым отказам ‑ *сбоям*. Причиной сбоев является воздействия на схему различных видов помех: радиационных, скачков напряжений питания, деградаций сигналов во времени и др.

Перспективным подходом решения данной проблемы является применение избыточного кодирования информационных потоков [1]. При этом подходе 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. 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. 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. Очевидное замечание, что важно заметить и исправить ошибку именно в информационных, а не в проверочных символах, особенно существенно для нашей задачи.

Проведённые эксперименты показали, что наиболее вероятный одиночный сбой функционального элемента схемы, как правило, либо маскируется, либо приводит к инвертированию единственного разряда на выходе схемы, т. е. кратные ошибки маловероятны [2].

**Спектральный код на основе функций Радемахера**

При разделимом блоковом кодировании кодовые слова -кода имеют длину , где – число информационных разрядов, повторяющих символы сообщения, а ‑ число проверочных разрядов. *Систематическим кодом с проверкой на чётность* называется двоичный блоковый код, в котором каждому сообщению сопоставлено кодовое слово , определяемое соотношениями

где означает сумму по *mod 2*, а множество двоичных символов , , , фиксировано [3].

Опишем новый систематический R-код с проверками на чётность, имеющий произвольное число информационных разрядов*.* Предположим сначала, что , это ограничение потом легко снимается.

Для положим

где – значение -й дискретной функции Радемахера на интервале определения в -й точке отсчёта, а  – сигнум-функция. Таким образом, будут получены проверочных разрядов и образован блоковый систематический код длины с проверкой на чётность. Ясно, что порождающая матрица данного кода есть единичная *k*-го порядка матрица с присоединённой справа транспонированной порождающей матрицей кода Рида-Маллера длины первого порядка: .

Покажем, что построенный код способен исправлять ошибку инвертирования некоторого разряда в . Для этого примем ещё одно допущение, что одиночная ошибка может произойти только в информационных битах, т. е. где **–** начальная часть полученного вектора, содержащая информационные разряды, а **‑** вектор ошибки, содержащий не более одной 1.

Вычислим синдромы для вектора : Если , то ошибки, считаем, не произошло. В противном случае вычисляем значения Нетрудно видеть, что для каждой ошибки номер искажённого разряда может быть получен дешифрованием вектора , поскольку инвертирование какого-либо одиночного разряда в приводит к одной из комбинаций вектора и данное отображение биективно. Данное свойство есть следствие того, что совокупность векторов , совпадает со всеми двоичными наборами дины .

Ясно, что вычисление вектора ошибки построенного кода происходит по *укороченной схеме*: входом является синдром ошибки разрядности , а выходом ‑ вектор ошибки разрядности . Построенный спектральный линейный нециклический R-код имеет кодовое расстояние : нулевой вектор и вектор, имеющий 1 только в первом и -м разрядах – его кодовые слова. Но, тем не менее, R-код позволяет исправлять одиночную ошибку в информационных разрядах полученного слова.

**R-код: снятие ограничений**

Ограничение легко снимается: при строим код для как указано выше и отбрасываем последние значений и коэффициентов . В результате получен -код, исправляющий одиночную ошибку в информационных битах. Сравнение R-кода с кодами Хемминга, Сяо LDPC-кодами проводится элементарно.

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 конструктивных методов, выполняют в специальном сбоеустойчивом варианте, и поэтому этот процесс можно считать свободным от ошибок. Платой за такую безошибочность служит увеличение площади корректирующей схемы. Понятно, что общий выигрыш будет лишь в случае, когда площадь корректирующей схемы менее чем в два раза превосходит площадь основной, иначе исправление одиночной ошибки методом тройного резервирования с мажорированием выходов становится более выгодным.

При исправлении одиночной ошибки кодом Хэмминга и LDPC площадь корректирующей схемы может составлять 130% площади основной [4]. 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 проверочных бит, а только единственный -й бит.

**Литература**

1. Хетагуров Я. А., Руднев Ю. П.  Повышение надёжности цифровых устройств методами избыточного кодирования. М.: Энергия, 1974.
2. 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.
3. Галлагер Р.  Теория информации и надёжная связь. – М.: Сов. радио, 1974.
4. Poolakkaparambil M., Mathew J. BCH code based multiple bit error correction in finite field multiplier circuits. ‑ ISQED, 2011, pp. 1‑6.