УДК 004.312.2; 621.3.049.771.14

С. В. Гаврилов[1], д-р техн. наук, зав. отделом, **С. И. Гуров**[2], канд. физ.-мат. наук, доц., e-mail: sgur@cs.msu.ru,
Т. Д. Жукова[1], инженер-исследователь, **Д. И. Рыжова**[1], мл. науч. сотр., e-mail: ryzhova_d@ippm.ru
[1]Институт проблем проектирования в микроэлектронике РАН, г. Москва
[2]Московский государственный университет имени М. В. Ломоносова

Применение теории кодирования для повышения помехозащищенности комбинационных схем

Исследованы проблемы автоматизации проектирования, направленные на повышение помехозащищенности комбинационных интегральных схем на этапе логического проектирования. Проанализированы различные методы помехоустойчивого кодирования применительно к повышению помехозащищенности комбинационных интегральных схем. Реализованы методы кодирования на основе выбора варианта коммутирования выходов дубликата основной схемы с учетом логических корреляций между выходами схемы. Одним из существенных отличий задачи повышения помехоустойчивости комбинационных схем, по сравнению с кодированием в сетях передачи данных, является дополнительная степень свободы, связанная с реализацией схемы кодирования. Применение методов оптимизации позволяет сокращать размер схемы кодирования, по сравнению с мажоритарным подходом, за счет выбранного порядка коммутаций.

Ключевые слова: *комбинационные схемы, проектирование, помехозащищенность, САПР*

Введение

Среди известных подходов к проектированию помехоустойчивых интегральных схем (ИС) широко используется дублирование с выбором результата по мажоритарному принципу [1]. Однако в последнее время все больший интерес вызывают попытки применения для решения данной задачи методов помехоустойчивого кодирования, которые аналогичны по своей сути подходам к защите от помех потоков информации при ее передаче по линиям связи [2].

Традиционным методом повышения отказоустойчивости при информационных сбоях в каналах связи является помехоустойчивое кодирование. Для парирования информационных сбоев, возникших в результате сбоев аппаратных, возможно использование следующих подходов [3].

1. Аппаратное резервирование с дальнейшим применением мажорирования — процедуры коррекции искаженной в результате сбоя информации путем сравнения результатов, полученных параллельным путем, и выдача на выход наиболее совпадающих результатов.

2. Информационное резервирование с применением результатов теории кодов, обнаруживающих и/или исправляющих ошибки.

Поскольку информационные сбои ИС обычно возникают в результате воздействия заряженных частиц или иных помех, в данном случае как аналоги понятий "отказоустойчивость" и "надежность" используют термины "помехоустойчивость" и "помехозащищенность" (ИС) соответственно.

Одним из существенных отличий задачи кодирования комбинационных схем по сравнению с кодированием в сетях передачи данных является дополнительная степень свободы, связанная с реализацией схемы кодирования, а именно возможность выбора порядка коммутации в целях сокращения аппаратных затрат на схему кодирования. В данной работе предлагается математический аппарат, позволяющий эффективно оценивать потенциальные возможности оптимизации схемы кодирования за счет выбора того или иного порядка коммутации для схемы кодирования.

В качестве математического аппарата для оценки потенциальных возможностей оптимизации схемы кодирования предлагается использовать формализмы для анализа вероятностей и корреляции логических уровней сигналов в комбинационных схемах.

В разд. 1 данной работы представлен анализ существующих подходов к кодированию информации для решения задачи повышения помехозащищенности комбинационных схем, в разд. 2 приведено описание методов помехоустойчивого кодирования для повышения помехозащищенности комбинационных интегральных схем, а также рассмотрены методы построения оптимальных схем комму-

тирования выходов схемы кодирования на основе анализа вероятностей распространения парных корреляций в схеме.

1. Анализ существующих методов блокового кодирования

1.1. Общие положения

Опишем сначала основные положения теории кодов, исправляющих ошибки. Помехоустойчивость кодирования достигается введением избыточности в код. Часто возникновение ошибок может быть описано наиболее простыми моделями со случайным некоррелированным информационным потоком, в котором некоторые биты случайно и независимо друг от друга могут оказаться инвертированными. В случае с передачей информации под влиянием помех такие модели называют *двоичными симметричными каналами*, в которых предполагается, что нет добавлений/стираний битов и замены $0 \to 1$ и $1 \to 0$ равновероятны. При этом могут ставиться задачи автоматического обнаружения и/или исправления ошибок. Отметим, что каждый конкретный корректирующий код не гарантирует исправления любой комбинации ошибок.

Одним из возможных подходов к решению проблемы является разбиение потока информации на *сообщения* — непересекающиеся блоки фиксированной длины k. Каждый блок можно кодировать независимо от других — *блоковое кодирование* или в зависимости от предыдущих — *сверточное кодирование* [4—6]. В результате вместо сообщений передают *кодовые слова* длины $n > k$ каждое. Естественно требовать построения кода минимальной длины, позволяющего восстановить сообщение, содержащее не более r ошибок (инверсий).

Например, при кодировании каждого k-битного сообщения можно добавить один бит, содержащий 0 или 1, так, чтобы число единиц в коде было четным; полученный код называется *кодом с проверкой на четность*. При таком кодировании обнаруживается искажение любого четного числа символов.

Если кодовое слово длины $n = k + m$ содержит в себе k бит исходного сообщения *(информационные биты)* и дополнительно еще m *проверочных бит*, то говорят о *разделимом блоковом кодировании*. В *неразделимых кодах* выделить информационные и проверочные биты невозможно. Увеличение m ведет, вообще говоря, к увеличению кодового расстояния d и, следовательно, к увеличению числа ошибок, которые может исправить код. Минимальное расстояние d между словами кода называется *кодовым расстоянием*. Известно, что у кода, исправляющего r ошибок, кодовое расстояние должно быть не менее $2r + 1$. Разделимый блоковый код описывают тройкой параметров (n, k, d) или парой (n, k).

Определение кодового расстояния d произвольного кода — сложная задача. Поэтому при создании помехоустойчивых кодов на первый план выходит проблема построения кодов с заданным кодовым расстоянием. Она решается при использовании БЧХ-кодов [7]. Величину $R = k/n$ называют *скоростью*, а $m/n = 1 - R$ — *избыточностью кода*. На сегодняшний день уже построены БЧХ-коды с практически значимыми параметрами.

Блоковое кодирование — это взаимно-однозначное отображение множества сообщений S всех векторов из 2^k во множество кодовых слов C (некоторых векторов из 2^n) — всегда может быть осуществлено с использованием таблицы размера $2^k \times n$. Однако табличное кодирование весьма неэффективно: значения n и k на практике могут достигать десятков и сотен тысяч. Известны две конструкции так называемых *совершенных кодов*, плотно заполняющих шарами радиуса r с центрами в кодовых словах весь куб 2^n: коды Хемминга $(2^q - 1, 2^q - q - 1,3)$, где q — натуральное число, и код Голея (23, 12, 7), исправляющие 1 и 3 ошибки соответственно.

Декодирование состоит в определении сообщения по кодовому слову. Декодирование кодов обычно значительно сложнее кодирования. При передаче по каналу с шумом кодовое слово $v \in 2^n$ превращается в принятое слово $w = v + e$, где e — *вектор ошибок*.

Декодирование (n, k, d)-кода основано на разбиении единичного куба 2^n на k областей, содержащих шары радиуса $r = \left[\frac{d-1}{2}\right]$ с центрами в кодовых словах, в предположении, что при передаче произошло не более r ошибок. Тогда восстановление переданного сообщения v состоит в определении ближайшего к полученному w в метрике Хэмминга, другими словами, в нахождении центра соответствующего шара. Для этого надо перебрать все 2^k строк в таблице $2^k \times n$ кодовых слов. Далее необходимо провести восстановление по словам v исходного сообщения u путем удаления проверочных бит. В общем случае, когда неизвестны их позиции, это потребует использования таблицы размера $2^k \times k$.

Из сказанного следует, что декодирование блокового (n, k)-кода общего вида — очень ресурсоемкий процесс, и поэтому использование таких кодов возможно лишь при небольших значениях n и k. Однако, приняв ряд дополнительных ограничений на множество кодовых слов, можно перейти от экспоненциальных требований по памяти для хранения кода и по сложности алгоритмов кодирования/декодирования к линейным требованиям по n и k. Эти ограничения приводят к использованию блоковых кодов специального вида — групповых, а из групповых кодов — к циклическим.

1.2. Групповые (линейные) коды

Большая часть теории блокового кодирования построена на *линейных кодах*, образующих векторное подпространство координатного пространства 2^n. В линейных кодах сумма по mod2 любых кодовых слов — также кодовое слово. Линейные коды позволяют реализовывать эффективные алгоритмы кодирования/декодирования, и в двоичном случае их называют групповыми, так как они образуют группу относительно операции $\oplus$. Линейные (n, k)-коды могут быть заданы матрицами *порождающей* $G_{n \times k}$ или *проверочной* $H_{m \times n}$. Для них выполняются соотношения $v = Gu$, $Hv = 0$ для любого кодового слова v, и невыполнение последнего равенства свидетельствует о наличии ошибки.

На практике удобно использовать *систематическое кодирование* [8], при котором k бит сообщения копируются в фиксированные позиции кодового слова, а затем вычисляются остальные $m = n - k$ проверочных битов. Такая возможность основана на том, что порождающая и проверочная матрицы определены с точностью до эквивалентных преобразований столбцов и строк соответственно, что эквивалентно переходу к другому базису пространства кодовых слов C и ортогонального ему $C^{\perp}$. Фиксирование позиций информационных битов задает порождающую и проверочную матрицы однозначно. При этом второй этап декодирования (удаление проверочных битов) становится тривиальным.

Декодирование групповых кодов проводят с использованием *синдромов* — векторов $s = Hw \in 2^m$. Вычисление вектора ошибок e сводится к решению системы линейных алгебраических уравнений (СЛАУ) $He = s$, которое ищут в виде суммы частного $\hat{e}$ решения данной системы и общего Gu решения соответствующей однородной системы $e = \hat{e} + Gu$. После нахождения частного решения $\hat{e}$ все возможные кодовые слова $u_1, ..., u_{2k}$ входного вектора дадут 2^k вариантов вектора $e_i = \hat{e} + Gu_i$. Решение с наименьшим хэмминговым весом дает искомый вектор ошибок.

Для каждого из 2^m синдромов необходимо перебирать 2^k решений очередной СЛАУ, т. е. алгоритм декодирования линейного кода в общем случае имеет экспоненциальную трудоемкость и по памяти, и по числу операций. Получив вектор ошибок e, декодирование осуществляют по правилу $v = w + e$.

Таким образом, кодирование групповыми кодами осуществляется умножением вектора-сообщения на порождающую матрицу. Декодирование также значительно упрощается по сравнению с общим случаем: используются легко вычисляемые синдромы при элементарном этапе удаления проверочных бит в случае систематического кодирования. Однако в общем случае требуется перебрать 2^k решений СЛАУ, т. е. процесс декодирования остается все еще достаточно трудоемким.

Если число единиц во всех комбинациях кода будет постоянным, то такой код будет *кодом с постоянным весом*. Это блочные неразделимые коды. Обнаружение ошибок при таком кодировании сводится к определению веса принятого слова, и если он отличается от заданного, то считается, что произошла ошибка. Код обнаруживает ошибки нечетной кратности и часть ошибок четной кратности. Не обнаруживаются ошибки смещения, при которых несколько единиц превращаются в нули и столько же нулей — в единицы.

1.3. Циклические коды

Циклические коды — подкласс линейных [9]. Код C называется *циклическим (сдвиговым)* (Cyclic Redundancy Code, CRC), если он инвариантен относительно циклических сдвигов, т.е. для любого $0 \leqslant s \leqslant n - 1$ справедливо следующее:

$$(\alpha_0, ..., \alpha_{n-1}) \in C \Rightarrow$$
$$\Rightarrow (\alpha_s, \alpha_{s+1}, ..., \alpha_{n-1}, \alpha_0, ..., \alpha_{s-1}) \in C.$$

В теории конечных полей показывается, что фактор-кольцо многочленов $\mathbb{F}_2[x]/(x^n - 1)$, рассматриваемое как векторное пространство размерности n над полем $\mathbb{F}_2$, имеет базис $\{1, x, ..., x^{n-1}\}$. Если $\varphi(x)$ — неприводимый многочлен из $\mathbb{F}_2[x]$, делящий $x^n - 1$, то порожденный им идеал $(\varphi(x))$ — циклическое подпространство в $\mathbb{F}_2[x]/(x^n - 1)$ и в нем циклический сдвиг равносилен умножению элемента на x. Поэтому для построения циклического кода выбирают степень n, порождающий многочлен кода — некоторый делитель $g(x)$ бинома $x^n - 1$, и в кольце $\mathbb{F}_2[x]/(x^n - 1)$ образуют идеал $(g(x))$. При удачном выборе $g(x)$ коэффициенты многочленов из данного идеала будут давать код с малой избыточностью при большом кодовом расстоянии. Однако известны только несколько конструкций циклических кодов с хорошими параметрами, а в общем случае определение кодового расстояния циклического кода чрезвычайно сложно.

При использовании циклических кодов удобно пользоваться представлением векторов сообщения u и кодового слова v в виде полиномов $u(x)$, $v(x) \in \mathbb{F}_2[x]$:

$$u = [u_0, u_1, ..., u_{k-1}]^{\mathrm{T}} \leftrightarrow$$
$$\leftrightarrow u(x) = u_0 + u_1 x + ... + u_{k-1} x^{k-1},$$

$$v = [v_0, v_1, ..., v_{n-1}]^{\mathrm{T}} \leftrightarrow$$
$$\leftrightarrow v(x) = v_0 + v_1 x + ... + v_{n-1} x^{n-1}.$$

Различают *систематическое* и *несистематическое кодирование* циклическими кодами, которое приводит к разделимому и неразделимому кодированию. Несистематическое кодирование осуществляется путем умножения кодируемого вектора на $g(x) - v(x) = u(x)g(x)$, а систематическое кодирование — "дописыванием" к кодируемому слову остат-

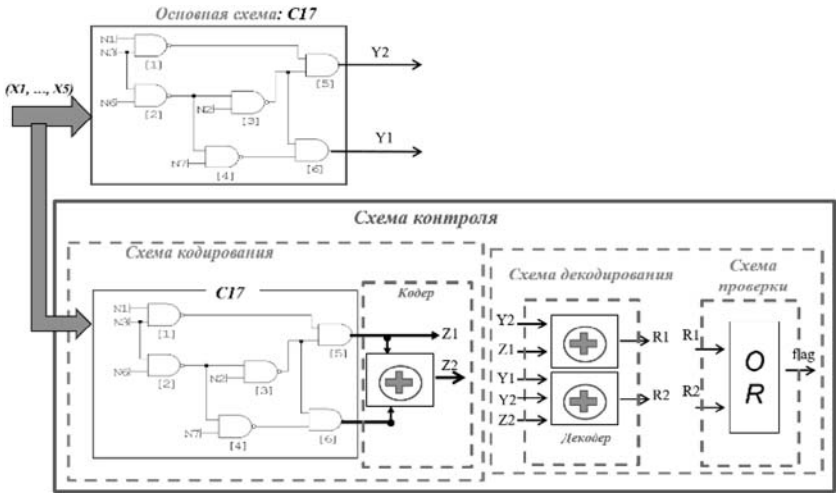
ка от деления $x^{n-k}u(x)$ на $g(x) - v(x) = x^m u(x) + r(x)$, где $r(x) \equiv_{g(x)} x^m u(x)$ (мы рассматриваем простейший вариант систематического кодирования, когда полином $v(x)$ имеет k коэффициентов полинома $u(x)$ в k крайних правых позициях, т. е. при старших степенях x).

Синдромом принятого полинома $w(x)$, закодированного циклическим (n, k)-кодом с порождающим полиномом $g(x)$ (и, возможно, содержащим ошибки), называют остаток $s(x)$ от деления $w(x)$ на $g(x)$: $s(x) \equiv_{g(x)} w(x)$. Ясно, что если $s(x) \equiv 0$, то $w(x)$ — кодовое слово.

Декодирование циклического кода проходит по общей схеме декодирования линейного кода: вычисляется синдром $s(x)$ принятого слова $w(x)$, ищутся решения системы $e(x) = s(x) + g(x)u(x)$ для всех 2^k возможных полиномов $u(x)$ степени $k - 1$, определяется полином ошибок как решение с минимальным числом ненулевых слагаемых и, наконец, восстанавливается переданное сообщение $u(x) = w(x) + e(x)$.

Циклические коды общего вида могут иметь произвольную длину n, но в отличие от линейного кода общего вида его параметры m и, следовательно, $k = n - m$ (число информационных битов) уже не произвольны: $g(x) | (x^n - 1)$. При использовании циклических кодов вместо матричных умножений и решения СЛАУ используются более простые операции умножения и деления с остатком полиномов, легко реализуемые на регистрах сдвига с обратными связями. Однако общий алгоритм декодирования по-прежнему имеет экспоненциальную сложность по k. Существуют и альтернативные методы декодирования циклических кодов общего вида, но и они не имеют удовлетворительных характеристик.

Обнаружение ошибок с помощью циклического кода обеспечивается тем, что в качестве разрешенных комбинаций выбираются такие, которые делятся без остатка на некоторый заранее выбранный порождающий полином. Если принятая комбинация содержит искаженные символы, то такое деление осуществляется с остатком и при этом формируется сигнал, свидетельствующий об ошибке. Большим преимуществом циклических кодов является простота построения кодирующих и декодирующих устройств, которые по своей структуре представляют регистры сдвига с обратными связями.



Предлагаемый подход

2. Применение помехоустойчивого кодирования для повышения помехозащищенности комбинационных интегральных схем

2.1. Предлагаемый метод повышения помехозащищенности

Для повышения помехозащищенности комбинационных схем был выбран метод с применением циклических кодов, который позволяет не только обнаружить наличие ошибок в переданном сообщении, но и исправить определенное число ошибок. Число ошибок, которое можно исправить, определяется свойствами образующего многочлена [10—12]. Данный метод не приводит к неоправданной избыточности, обеспечивает возможность оптимального сочетания требований к минимизации аппаратных затрат и достижение требуемого уровня отказоустойчивости [13, 14]. Схема предлагаемого подхода представлена на рисунке.

Для кодирования сообщений применяется операция умножения на образующий многочлен, при этом вектор исходного сообщения $a_{k-1}, ..., a_0$ представляется в виде многочлена $a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_0$, где k — длина сообщения. Для декодирования сообщения используется операция деления переданного сообщения на образующий многочлен. Остаток от деления принятого слова на образующий многочлен называется синдромом. Если ошибок в переданном сообщении нет, то синдром равен нулю. Вектор ошибок можно найти по вычисленному синдрому.

В задаче передачи сообщений для реализации операций умножения и деления многочленов используют сдвиговые регистры, так как сигнал передается в виде последовательности нулей и единиц. В случае комбинационных схем сигналы на выходы приходят параллельно, поэтому здесь необходимо использовать в качестве схем кодирования и декодирования логические схемы.

Принципиальное отличие задачи кодирования данных для передачи через канал связи от задачи повышения помехоустойчивости комбинационных схем состоит в следующем. Так как в задаче повышения помехоустойчивости сама комбинационная схема подвержена ошибкам, схема кодирования реализу-

ется за счет дублирования исходной схемы с последующей оптимизацией совместно со схемой кодирования. Для синтеза схемы кодирования используется операция умножения многочлена выходного сообщения комбинационной схемы $a_{k-1}x^{k-1} + \ldots + a_0$ на образующий многочлен $g^r(x)$, где r — степень образующего многочлена.

Ключевая проблема задачи передачи сообщений — минимизация площади или размера схем кодирования и декодирования. Одним из путей оптимизации схемы является построение логических функций на основе применения аппарата BDD. Предлагаемое при этом использование синтеза булевых функций в конечных полях Галуа на основе редуцированных диаграмм двоичных решений (ROBDD) позволяет снять существующее в настоящее время ограничение на размерность проектируемых комбинационных схем (число входов и выходов). Использование предлагаемой методики обеспечивает управляемость и предсказуемость процесса проектирования схем при достижении оптимального сочетания заданных требований по отказоустойчивости и минимизации структурных затрат. Критерием оценки площади при применении BDD может служить число вершин графа BDD. Оценку задержек можно рассчитать исходя из длины цепи от входа до выхода при предположении мультиплексорной реализации BDD.

Проведенные исследования показали, что на качество результата в терминах занимаемой площади существенное влияние оказывает не только переупорядочение входов, как в случае стандартной BDD, но и порядок коммутации выходов в схеме кодирования.

Полный перебор различных вариантов коммутаций требует анализа $k!$ вариантов и, следовательно, невозможен для большого числа выходов k. Выбор вариантов коммутаций будет более эффективен, если заранее оценить потенциальные возможности оптимизации схемы кодирования до проведения самого процесса создания и оптимизации схемы.

Для выбора оптимального варианта коммутации предлагается использовать оценочную функцию, вычисленную на основе расчета взаимных корреляций между выходами [15]. Примеры синтеза схемы контроля на основе предложенного подхода были приведены ранее в работах [10—14]. Наибольший эффект от оптимизации схемы кодирования достигается при условии вхождения в одну формулу схемы кодирования выходов схемы, имеющих взаимные корреляции. Для всех выходов дублирующей схемы применяют предложенные методы анализа логических корреляций в цифровой схеме для получения оценочных функций.

Используя полученные оценочные функции, выбирают порядок коммутации выходов дублирующей схемы на основе анализа вероятностей распространения парных корреляций.

2.2. Методы построения оптимальных схем коммутирования входов схемы кодирования с учетом логики работы основной схемы

За счет учета дискретных корреляций можно сократить размер схемы кодирования. Однако дискретные корреляции не описывают полную картину возможных корреляций сигналов в схеме. Для полного учета парных корреляций в качестве альтернативы предлагается модифицировать аппарат анализа парных корреляций сигналов, который использовался при оптимизации мощности и анализе стрессовых состояний транзисторов [16].

Пусть каждый сигнал a в комбинационной схеме (либо первичный вход, либо выход любого вентиля) характеризуется с помощью величины $p(a = v)$, равной отношению времени нахождения сигнала в состоянии $(a = v)$ к общему времени моделирования. Для описания корреляции между двумя сигналами введем коэффициент корреляции сигналов по аналогии с работой [17]:

$$SC_{ij}^{ab} = \frac{p(a = i \;\&\; b = j)}{p(a = i)p(b = j)},\ i, j = 0, 1. \qquad (1)$$

Для выбора оптимального варианта коммутации предлагается использовать оценочную функцию, которая вычисляется согласно следующей формуле:

$$f(a, b) = \begin{cases} SC, & SC \leqslant 1; \\ 1/SC, & SC > 1. \end{cases}$$

Наибольшего эффекта оптимизации можно добиться, сопоставляя минимум оценочной функции с парами связанных сигналов в кодере.

В целях устранения экспоненциальной сложности алгоритма можно воспользоваться предположением о том, что существенны только парные корреляции. Иначе говоря, будем пренебрегать корреляцией любых двух сигналов к третьему и т.д. В этом случае вероятность сложного события может быть приближенно вычислена по формуле

$$p\left(\prod_{k=1}^{n}(a_k = i_k)\right) = \prod_{k=1}^{n} p(a_k = i_k) \prod_{1 \leqslant k < l \leqslant n} SC_{i_k i_l}^{a_k a_l}. \qquad (2)$$

Поскольку

$$p(a = i \;\&\; b = j) = p(a = i/b = j)p(b = j) = \\ = p(b = j/a = i)p(a = i),$$

где $p(X/Y)$ обозначает вероятность события X при условии Y, то

$$SC_{ij}^{ab} = \frac{p(a = i/b = j)}{p(a = i)} = \frac{p(b = j/a = i)}{p(b = j)}.$$

Следовательно, мы имеем следующие соотношения для четырех коэффициентов SC_{ab}:

$$\sum_{i=0,1} SC_{ij}^{ab} p(a=i) = 1;$$

$$\sum_{j=0,1} SC_{ij}^{ab} p(b=j) = 1;\ j = 0,1,\ i = 0,1. \qquad (3)$$

Матрица системы (3) имеет ранг 3, поэтому, зная SC_{00}^{ab}, можно вычислить три других коэффициента по следующим формулам:

$$SC_{01}^{ab} = \frac{1 - SC_{00}^{ab} p_b}{1 - p_b},\ SC_{10}^{ab} = \frac{1 - SC_{00}^{ab} p_a}{1 - p_a},$$

$$SC_{11}^{ab} = \frac{1 - SC_{10}^{ab} p_b}{1 - p_b}. \qquad (4)$$

При вычислении длительности нуля для выхода вентиля должны быть известны вероятности нулевого значения сигналов для всех входов вентиля и коэффициенты SC для всех пар входов вентиля. Все возможные входные векторы вентиля могут быть разделены на два множества:

1) V_0 — множество входных векторов вентиля, для которых выход вентиля равен 0;

2) V_1 — множество входных векторов вентиля, для которых выход вентиля равен 1.

Для сложного совместного события, обеспечивающего значение на выходе, равное нулю ($y = 0$), можно записать:

$$(y=0) = \sum_{I \in V_0} \prod_{k=1}^{n} (x_k = i_k), \qquad (5)$$

где n — число входов вентиля; x_k — сигналы на входах вентиля (переменные); $I = (i_1, ..., i_n)$ — входной вектор вентиля. Векторы под дизъюнкцией в выражении (5) являются взаимно исключающими, поэтому

$$p(y=0) = \sum_{I \in V_0} p\left(\prod_{k=1}^{n} (x_k = i_k) \right).$$

Используя (2) и пренебрегая корреляциями более высоких порядков, получаем следующую формулу для расчета времени нахождения транзистора в стрессовом состоянии:

$$p(y=0) = \sum_{I \in V_0} \prod_{k=1}^{n} \left(p(x_k = i_k) \prod_{k < l \leqslant n} SC_{i_k i_l}^{x_k x_l} \right).$$

Для корректной обработки каждого вентиля также необходимо распространять по схеме коэффициенты корреляции SC. Пусть z — любой сигнал с известной вероятностью и известными SC с каждым входом вентиля. Необходимо решить задачу распространения SC сигнала z с входов вентиля на его выход. В соответствии с определением (1) можно записать

$$SC_{00}^{zy} = \frac{p(z=0\ \&\ y=0)}{p(z=0)p(y=0)}.$$

Рассматривая ($z = 0$ & $y = 0$) как сложное событие и вычисляя его вероятность, получаем следующую формулу для распространения SC через вентиль:

$$SC_{00}^{zy} = \frac{\sum_{I \in V_0} \prod_{k=1}^{n} \left(p(x_k = i_k) SC_{0 i_k}^{z x_k} \prod_{k < l \leqslant n} SC_{i_k i_l}^{x_k x_l} \right)}{p(y=0)}.$$

Остальные коэффициенты SC могут быть вычислены по формулам (4).

Формула учета парных корреляций для выбора варианта коммутации может быть модифицирована следующим образом:

$$S^*(a, b) = \sum_{v_a = 0,1} \sum_{v_b = 0,1} p(a = v_a\ \&\ b = v_b) =$$

$$= \sum_{v_a = 0,1} \sum_{v_b = 0,1} p(a = v_a) p(b = v_b) SC_{v_a v_b}^{ab}.$$

В результате применения предложенных методов получены результаты, которые показывают выигрыш порядка 10 % (в единичных случаях около 58 %) по площади для схем из набора ISCAS85 при построении схемы кодирования на основе полинома второй ($x^2 + x + 1$) и третьей степени ($x^3 + x + 1$) по сравнению с мажорированием.

Заключение

В работе выполнен анализ существующих методов кодирования для решения задачи повышения помехозащищенности комбинационных схем. Предложен подход к оптимизации схем кодирования за счет выбора варианта коммутирования выходов дубликата основной схемы на основе результатов анализа вероятностей логических корреляций. Применение разработанных методов на основе выбора порядка коммутаций позволяет добиться минимизации размера схемы кодирования примерно на 10 % по сравнению с мажоритарным подходом.

Список литературы

1. **Черкесов Г. Н.** Надежность аппаратно-программных комплексов: учеб. пособие. СПб.: Питер, 2004. 479 с.
2. **Морелос-Сарагоса Р.** Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / пер. с англ. В. Б. Афанасьева. М.: Техносфера, 2006. 320 с.
3. **Матвеевский В. Р.** Надежность технических систем: учеб. пособие. М.: Изд. МИЭМ, 2002. 113 с.
4. **Вернер М.** Основы кодирования: учебник для вузов. М.: Техносфера, 2004. 288 с.
5. **Блейхут Р.** Теория и практика кодов, контролирующих ошибки. М.: Книга по требованию, 2013. 566 с.
6. **Van Lint J. H.** Introduction to Coding Theory. Springer Science & Business Media, 2012. 234 p.

7. **Poolakkaparambil M., Mathew J.** BCH Code Based Multiple Bit Error Correction in Finite Field Multiplier Circuits // ISQED, 2011. P. 1—6.
8. **MacWilliams F. J., Sloane N. J. A.** The Theory of Error—Correcting Codes. North—Holland Publishing Company, 1977. 762 p.
9. **Касами Т., Токура Н., Ивадари Е.** Теория кодирования / пер. с яп. А. В. Кузнецова. М.: Мир, 1978. 576 с.
10. **Гаврилов С. В., Иванова Г. А., Рыжова Д. И., Соловьев А. Н., Стемпковский А. Л.** Методы синтеза помехозащищенных комбинационных блоков // Информационные технологии. 2015. Т. 21, № 11. С. 821—826.
11. **Гаврилов С. В., Иванова Г. А., Рыжова Д. И., Стемпковский А. Л.** Методы повышения надежности комбинационных микроэлектронных схем на основе мультиинтервального анализа быстродействия // Системы высокой доступности. 2015. № 4. С. 69—76.
12. **Соловьев А. Н., Стемпковский А. Л.** Методы повышения отказоустойчивости работы устройства управления микросистемы за счет введения структурной избыточности // Информационные технологии. 2014. № 10. С. 17—22.
13. **Гаврилов С. В., Иванова Г. А., Соловьев А. Н., Стемпковский А. Л.** Оптимизация схем кодирования на основе выбора варианта коммутаций с учетом логических корреляций между выходами комбинационной схемы // Известия ЮФУ. Технические науки. 2015. № 6 (167), С. 255—262.
14. **Гаврилов С. В., Иванова Г. А., Соловьев А. Н., Щелоков А. Н.** Учет логических корреляций между выходами комбинационной схемы при коммутации с входами схемы кодирования // Труды Международного конгресса по интеллектуальным системам и информационным технологиям — 2015, IS & IT'15. С. 192—197.
15. **Гаврилов С. В.** Методы анализа логических корреляций для САПР цифровых КМОП СБИС. М.: Техносфера, 2011. 136 с.
16. **Стемпковский А. Л., Глебов А. Л., Гаврилов С. В., Гудкова О. Н.** Вероятности напряженного состояния транзисторов для временного анализа с учетом электротемпературной нестабильности // Информационные технологии. 2009. № 7. С. 32—38.
17. **Marculescu R., Marculescu D., Pedram M.** Switching Activity Analysis Considering Spatiotemporal Correlations // Proc. ICCAD-1994. P. 294—299.

S. V. Gavrilov[1], DSc, Head of Department, **S. I. Gurov**[2], PhD, Assistant Professor,
T. D. Zhukova[1], Research Engineer, **D. I. Ryzhova**[1], Junior Research Scientist, ryzhova_d@ippm.ru
[1]Institute for Design Problems in Microelectronics of Russian Academy of Sciences (IPPM RAS)
[2]Lomonosov Moscow State University

Application of Coding Theory to Improve the Noise Immunity of Combinational Circuits

The work is devoted to solving problems of design automation to improve the noise immunity of combinational integrated circuits at the logical level design. The different methods of error-correcting coding for improving noise immunity of combinational integrated circuits are analyzed. The coding methods with a selection of duplicate circuit outputs commutation based on the logical correlations between the circuit outputs are implemented. One of the significant difference of the noise immunity of combinational circuits, in comparison with coding in data networks, is an additional degree of freedom associated with the implementation of the coding scheme. The application of effective optimization methods reduces the size of coding circuit by selection of the commutation order, compared to the majority approach.

Keywords: *combinational circuits, design, noise tolerance, CAD*

References

1. **Cherkesov G. N.** *Nadezhnost' apparatno-programmnyh kompleksov,* uchebnoe posobie, Saint Petersburg: Piter, 2004, 479 p.
2. **Morelos-Saragosa R.** *Iskusstvo pomehoustojchivogo kodirovanija. Metody, algoritmy, primenenie*, per. s angl. V. B. Afanas'eva, Moscow: Tehnosfera, 2006, 320 p.
3. **Matveevskij V. R.** *Nadezhnost' tehnicheskih system, uchebnoe posobie*, Moscow, Moskovskij gosudarstvennyj institut jelektroniki i matematiki, Moscow, 2002, 113 p.
4. **Verner M.** *Osnovy kodirovanija, uchebnik dlja VUZov*, Moscow, Tehnosfera, 2004, 288 p.
5. **Blejhut R.** *Teorija i praktika kodov, kontrolirujushhih oshibki*, Moscow, Kniga po trebovaniju, 2013, 566 p.
6. **Lint J. H.** *Introduction to Coding Theory*, Springer Science & Business Media, 2012, 234 p.
7. **Poolakkaparambil M., Mathew J.** BCH Code Based Multiple Bit Error Correction in Finite Field Multiplier Circuits, *Proceedings of the 12th International Symposium on Quality Electronic Design (ISQED 2011)*, pp. 1—6.
8. **MacWilliams F. J., Sloane N. J.A.** The Theory of Error-Correcting Codes, North—Holland Publishing Company, 1977, 762 p.
9. **Kasami T., Tokura N., Ivadari E.** Teorija kodirovanija, per. s jap. A. V. Kuznecova, Moscow, Mir, 1978, 576 p.
10. **Gavrilov S. V., Ivanova G. A., Ryzhova D. I., Solov'ev A. N., Stempkovskij A. L.** Metody sinteza pomehozashhishhennyh kombinacionnyh blokov, *Informacionnye tehnologii*, 2015, vol. 21, no. 11, pp. 821—826.
11. **Gavrilov S. V., Ivanova G. A., Ryzhova D. I., Stempkovskij A. L.** Metody povyshenija nadezhnosti kombinacionnyh mikrojelektronnyh shem na osnove mul'tiinterval'nogo analiza bystrodejstvija, *Sistemy vysokoj dostupnosti*, 2015, no. 4, pp. 69—76.
12. **Solov'ev A. N., Stempkovskij A. L.** Metody povyshenija otkazoustojchivosti raboty ustrojstva upravlenija mikrosistemy za schet vvedenija strukturnoj izbytochnosti, *Informacionnye tehnologii*, 2014, no. 10, pp. 17—22.
13. **Gavrilov S. V., Ivanova G. A., Solov'ev A. N., Stempkovskij A. L.** Optimizacija shem kodirovanija na osnove vybora varianta kommutacij s uchetom logicheskih korreljacij mezhdu vyhodami kombinacionnoj shemy, *Izvestija JuFU. Tehnicheskie nauki*, 2015, no. 6 (167), pp. 255—262.
14. **Gavrilov S. V., Ivanova G. A., Solov'ev A. N., Shhelokov A. N.** Uchet logicheskih korreljacij mezhdu vyhodami kombinacionnoj shemy pri kommutacii s vhodami shemy kodirovanija, *Trudy Mezhdunarodnogo kongressa po intellektual'nym sistemam i informacionnym tehnologijam*, "IS & IT'15", 2015, pp. 192—197.
15. **Gavrilov S. V.** *Metody analiza logicheskih korreljacij dlja SAPR cifrovyh KMOP SBIS*, Moscow, Tehnosfera, 2011, 136 p.
16. **Stempkovskij A. L., Glebov A. L., Gavrilov S. V., Gudkova O. N.** Verojatnosti naprjazhennogo sostojanija tranzistorov dlja vremennogo analiza s uchetom jelektrotemperaturnoj nestabil'nosti, *Informacionnye tehnologii*, 2009, no. 7, pp. 32—38.
17. **Marculescu R., Marculescu D., Pedram M.** Switching Activity Analysis Considering Spatiotemporal Correlations, *Proceedings of the International Conference on Computer-Aided Design*, 1994, pp. 294—299.