

Применение преобразований Уолша и Рида-Маллера для синтеза и тестирования логических схем

10, октябрь 2017

**Бушуев В. В., Иванников П. В., Сосенко А. С.,
Чистяков Р. С., Усанов А. Е.**

УДК: 510

МГТУ им. Н.Э. Баумана, Москва, Россия

vovabush94@mail.ru

ivannikovpv@gmail.com

sosenko1995@gmail.com

romchezz@gmail.com

alexeyusanov@gmail.com

Введение

Рассматриваемые вопросы использования спектральных техник Уолша и применение преобразований Рида-Маллера, являются конструктивными для построения и синтеза логических булевых схем, в том числе и решения вопросов декомпозиции, а также для тестирования оборудования на различных уровнях.

1. Исторический обзор

Первая работа о спектральных техниках была опубликована в октябре 1983 в Бостоне. Работа была посвящена двум основным моментам: приложениям спектральных техник и детектированию ошибок. Она была представлена коллективом из 35 авторов, гражданами 7 стран: США, Канады, Великобритании, ФРГ, Индии, Австралии и Китая.

В работе были освещены следующие моменты:

- применение спектральных техник к синтезу логических схем и компьютерной архитектуры;
- применение спектральных техник для тестирования аппаратной составляющей компьютеров;
- применение спектральных техник для приема и фильтрации цифрового сигнала.

Четыре работы были посвящены тестированию и самотестированию аппаратной составляющей компьютеров и сжатию информации о результатах теста.

Девять документов, представленных на семинаре, были выбраны для публикации в виде отдельных разделов в «Спектральные техники и обнаружение ошибок» Карповского, 1985 года.

В дополнении к этим 10 главам том содержал подборку (около 618) библиографий о приложениях спектральных техник в синтезе логических схем, тестировании и передаче сигнала.

Этот том вместе со старыми книгами Карповского, Хёрста и новой книгой Хёрста, Музио и Миллера представляют наиболее всеобъемлющий материал для изучения вопроса спектральных техник, применимых к синтезу логических схем и тестировании аппаратной составляющей компьютеров.

2. Применение спектральных техник к синтезу логических схем

Рассмотрим обзор некоторых применений спектральных техник (или по-другому преобразования Уолша) для синтеза схем. Эти техники могут использоваться, например, для синтеза схем на транзисторной логике.

Пусть $f = f_i(x_0, \dots, x_{m-1})$, $(i = 0, \dots, k - 1)$ – система булевых функций, которую надо реализовать в виде схемы.

Хорошо известно, что элемент сложения по модулю два (который достаточно легко реализуется в транзисторной логике) в совокупности с элементами И-НЕ, ИЛИ-НЕ создает достаточную базу для реализации функций с наименьшей сложностью.

Рисунки 1, 2 и 3 демонстрируют три разных подхода.

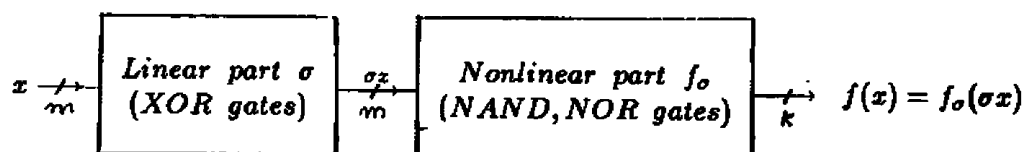


Рис. 1. Последовательная линеаризация

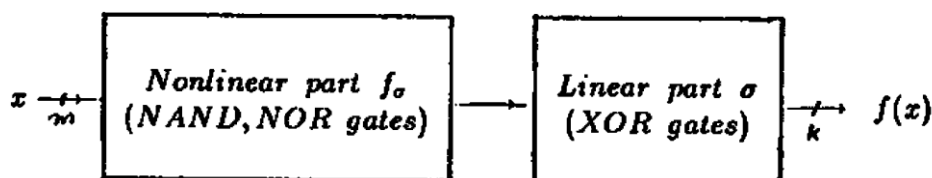


Рис. 2. Последовательная линеаризация

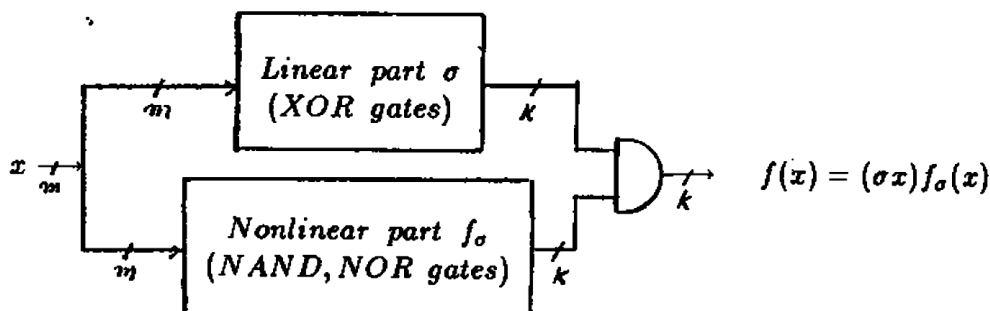


Рис. 3. Параллельная линеаризация

Для оценки критерия сложности нелинейной части можно рассмотреть следующее выражение

$$L(f) = \sum_{i=0}^{k-1} \sum_{d(X,Y)=1} f_i(X)f_i(Y), \quad (1)$$

где $d(X, Y)$ – расстояние Хэмминга между двоичными m -мерными векторами X и Y .

Подтверждение выбора именно этого критерия могут быть найдены в [1, 2]. Проблема минимизации сложности нелинейной части преобразования, представленного на рисунке 1 известна как проблема линеаризации системы булевых функций [2-4].

Известно, что преобразования на рисунках 2 и 3 для большинства случаев не приводили к существенному снижению числа элементов.

Решение проблемы линеаризации в соответствии с критерием, введенным выше основывается на автокорреляционной функции, которая может быть определена как

$$B(\tau) = \sum_{i=0}^{k-1} \sum_X f_i(X)f_i(X \oplus \tau). \quad (2)$$

Пусть M – набор всех двоичных невырожденных матриц размера $m \times m$, $T \in M$ и $t_0, \dots, t_{m-1}$ – набор столбцов матрицы T , то есть $T = (t_0, \dots, t_{m-1})$. Положим

$$B(T) = \sum_{j=0}^{m-1} B(t_j). \quad (3)$$

Тогда, согласно [2], $\sigma \in M$ минимизирует сложность $L(f_\sigma)$ нелинейной части на рисунке 1, если она является обратной к матрице $\bar{T}$, где

$$\max_{T \in M} B(T) = B(\bar{T}). \quad (4)$$

Обобщение этого алгоритма для линеаризации системы булевых функций может быть найдено в [3, 4].

Для вычисления автокорреляционной функции мы используем преобразование Винера-Хинчина.

Вычисление $\bar{T} \in M$, удовлетворяющей (4), очень трудоемко. Для его упрощения используем следующее наблюдение.

Обозначим за $\rho(m)$ вероятность того, что случайно выбранная двоичная матрица $T = (t_{ij})$ размерности $(m \times m)$ будет невырожденной. Очевидно, что

$$\rho(m) = \frac{\prod_{i=0}^{m-1} (2^m - 2^i)}{\prod_{i=0}^{m-1} (2^m - i)}$$

и

$$\lim_{m \rightarrow \infty} \rho(m) = \rho = 0.288788.$$

В результате видно, что примерно одна из четырех выбранных случайно таких матриц будет невырожденная.

Следует подчеркнуть, что такой подход, основанный на линеаризации, может быть менее эффективным для реализации нелинейной части при помощи ПЛИС, так как это потребует увеличения количества элементов для линейной части.

3. Преобразования Рида-Маллера и его применение к тестированию аппаратной составляющей компьютеров.

Тестирование при помощи коэффициентов Уолша было исследовано в [5]. Достаточно хороший обзор спектральных техник для тестирования представлен в [1].

Для преобразования Уолша каждый спектральный коэффициент зависит от значения функции от m аргументов или в итоге от 2^m входных векторов. Это приводит к двум ключевым недостаткам тестирования, основанного на преобразовании Уолша. Во-первых, требуется 2^m шагов, также как и для полного перебора. Во-вторых, так как каждый спектральный коэффициент m -битный вектор, тестирование требует дополнительного m -битного счетчика.

Спектральные техники тестирования при помощи преобразования Уолша были изменены с целью уменьшить временные затраты. Этот подход более известен как тестирование путем линейной проверки. Тестирование линейной проверкой эффективно используется для тестирования на уровне кристалла, для тестирования микроконтроллера, для тестирования памяти и для тестирования аппаратных компонентов при выполнении числовых расчетов. Модификация тестирования линейной проверкой обычно используется для самотестирования многопроцессорных систем, выполняющих вычисления сложных функций.

Рассмотрим спектральный подход для тестирования, который приводит к сокращению времени тестирования и аппаратных накладных расходов, необходимых для тестирования. Этот подход основан на преобразовании Рида-Маллера (РМ), которое определено ниже. Для этого подхода каждый спектральный коэффициент $\bar{f}(W)$ зависит только от $2^{|W|}$ значений функции $f(X)$ ($|W|$ это вес вектора W) в добавок к тому, что $\bar{f}(W) \in \{0, 1\}$ для каждого W .

Таким образом, проверка $\bar{f}(W)$ требует использования $2^{|W|}$ входных данных и соответствующий проверке результат будет иметь лишь один бит информации. Очевидно, что этой однобитной структуры будет достаточно для определения с высокой вероятностью ошибки типа «залипания» (постоянно 0 или постоянно 1).

Рассмотрим некоторые основные результаты, связанные с тестированием путем проверки коэффициентов Рида-Маллера.

Преобразование Рида-Маллера $f \rightarrow \bar{f}$ можно определить следующим образом. Пусть $X = (x_0, \dots, x_{m-1})$, $W = (w_0, \dots, w_{m-1})$, $(x_i, w_j \in \{0, 1\})$, и

$$R_X(W) = \prod_{i=0}^{m-1} x_i^{w_i},$$

где $(0^0 = 1)$.

Тогда

$$\bar{f}(W) = \bigoplus_{X=0}^N R_W(X) f(X) = \bigoplus_{X \subseteq W} f(X),$$

$$f(X) = \bigoplus_{W=0}^N R_X(W) \bar{f}(W) = \bigoplus_{W \subseteq X} \bar{f}(W),$$

где $\oplus$ – операция сложения по модулю 2, $N = 2^m - 1$, $X \subseteq W$, если $x_i \leq w_i$ для всех $i = 0, 1, \dots, m - 1$.

Вычисление $\bar{f}(W)$ для всех W требует $m2^{m-1}$ элементов $\oplus$. Существует также быстрое преобразование Рида-Маллера.

Преобразования Рида-Маллера широко распространены в синтезе схем и кодах, исправляющих ошибки. Отметим, что преобразования, описанные выше очень похожи на формулы обобщения Мёбиуса, хорошо известные в теории чисел.

Заключение

Преобразования Рида-Маллера имеют множество свойств, некоторые из которых очень похожи на свойства преобразования Уолша.

Использование спектральных техник Уолша и преобразований Рида-Маллера решают большой спектр проблем связанных с синтезом логических схем, тестированием и передачей сигнала.

Список литературы

- [1]. M. Karpovsky. Spectral Techniques and fault detection. *Academic Press*. 1985. 597 p.
- [2]. M. Karpovsky. Finite Orthogonal Series in Analysis and Design of Digital Devices. *John Wiley*. 1976. 251 p.
- [3]. M. Karpovsky. Harmonic analysis over finite commutative groups in linearization problem for system of logical functions. // *Information and control*. 1977. Vol. 33. Is. 2. Pp. 142-165. DOI: [https://doi.org/10.1016/S0019-9958\(77\)90546-0](https://doi.org/10.1016/S0019-9958(77)90546-0)
- [4]. C. Moraga. Comments on a method of Karpovsky. // *Information and control*. 1978. Vol. 39. Is. 3. Pp. 243-246. DOI: [https://doi.org/10.1016/S0019-9958\(78\)90599-5](https://doi.org/10.1016/S0019-9958(78)90599-5)
- [5]. A.K. Susskind. Testing by verifying Walsh coefficients. // *IEEE Transactions on Computers*. 1983. Vol. 32. No. 02. Pp. 198-201.