Метод случайных булевых производных в оценке комбинационных схем

Савкин Леонид Васильевич

Соискатель

Московский авиационный институт, Москва, Россия

E-mail: android4.1@mail.ru

Одним из важнейших этапов проектирования любых дискретных цифровых устройств является оценка их комбинационных схем на наличие внутренних логико-арифметических коллизий. Комбинационные схемы, как правило, в процессе верификации проекта рассматриваются в виде соответствующих орграфов $G(W, R)$, где W - множество функциональных вершин орграфа, реализующих одну из базовых логико-арифметических операций комбинационной схемы, а R - множество дуг орграфа, описывающих направленные связи между его функциональными вершинами.

Ввиду высокой степени сложности современных цифровых устройств, орграфы $G(W, R)$ часто представляют собой графы больших размерностей. Для структурной и функциональной оценки таких графов довольно широкую популярность получили рандомные методы идентификации внутренних логико-арифметических коллизий [1], которые в ряде случаев сводятся к прямой оценке булевых функций, реализуемых той или иной случайной выборкой k фрагментов (подграфов) исходного орграфа $G(W, R)$.

В данной работе предлагается метод оценки комбинационных схем, основанный на оценке значений не булевых функций, а их производных. При этом данный метод также предполагает использование случайной (рандомной) выборки фрагментов орграфа, соответствующего рассматриваемой комбинационной схеме.

Пусть фрагменту $G_1(W, R) \subset G(W, R)$ исследуемого орграфа $G(W, R)$ соответствует функция $f_1(x) = f_1(x_1, x_2, ..., x_n)$. Булеву производную функции $f_1(x)$ по двоичной переменной x_i запишем в виде

$$\frac{df_1(x_i)}{dx_i} \equiv f_1(x_1, x_2, ..., x_i, ..., x_n) \oplus f_1(x_1, x_2, ..., \bar{x}_i, ..., x_n), \qquad (1)$$

где $\bar{x}_i$ - инверсное значение двоичной переменной x_i.

В соответствии с общим определением булевой производной [2], выражение (1) позволяет найти такие значения переменных $x_1, x_2, ..., x_n$ (все кроме x_i), при которых изменение значения x_i будет приводить к изменению значения функции $f_1(x)$. При этом не существенным является то, каким образом меняется значение $f_1(x)$: с 0 на 1, или с 1 на 0. Поэтому, выражение (1) очень часто записывают в сокращенной форме

$$\frac{df_1(x_i)}{dx_i} \equiv f_1(x_i = 0) \oplus f_1(\bar{x}_i = 1) \equiv f_1(x_i = 1) \oplus f_1(\bar{x}_i = 0), \qquad (2)$$

что совершенно равнозначно, поскольку полностью удовлетворяет общему определению булевой производной.

Введем индикаторную функцию $\mathcal{Q}_1$, позволяющую однозначно зафиксировать логико-арифметическую коллизию на орграфе $G_1(W, R)$ по изменению значения переменной x_i, и запишем ее как

$$\mathcal{Q}_1 = x_i \times \frac{df_1(x_i)}{dx_i} = 0 \Leftrightarrow \bar{\mathcal{Q}}_1 = \bar{x}_i \times \frac{df_1(x_i)}{dx_i} = 1, \qquad (3)$$

для случая без коллизий на i - ой входной двоичной переменной фрагмента $G_1(W, R)$. В случае регистрации логико-арифметической коллизии на фрагменте $G_1(W, R)$, будем иметь соответствующие обратные значения индикаторной функции

$$\mathcal{Q}_1 = x_i \times \frac{df_1(x_i)}{dx_i} = 1 \Leftrightarrow \bar{\mathcal{Q}}_1 = \bar{x}_i \times \frac{df_1(x_i)}{dx_i} = 0. \qquad (4)$$

Таким образом, процедуру *положительной* оценки комбинационной схемы по методу случайных булевых производных можно представить в виде формального выражения

$$Rand(H, < G_1, G_2, ..., G_k >) \Rightarrow \mathcal{Q}_j = 0, j = \overline{1, k}, \qquad (5)$$

где H - параметр рандомизации, задающий особенности случайных проверок булевых производных на равенство их нулю в j - м фрагменте орграфа $< G_1, G_2, ..., G_j >$ - набор орграфов, образующих случаюную выборку k; Q_j - индикаторная функция j - го фрагмента орграфа $G(W, R)$.

Литература

1. Кнут Дональд Э. Глава 3. Случайные числа // Искусство программирования, 3-е изд. М.: Вильямс, 2000.
2. Шевелев Ю. П. Дискретная математика. Ч.1: Теория множеств. Булева алгебра (Автоматизированная технология обучения «Символ»), Томск: Изд-во ТУСУР, 2003.