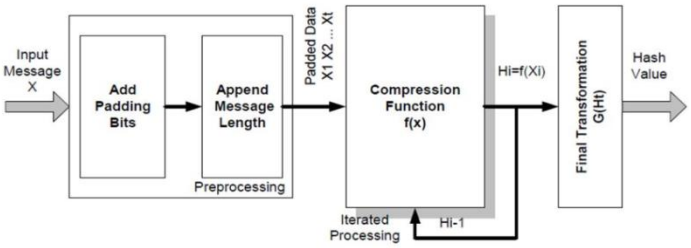

Рисунок 1 –Общая модель хэш-функции.

Процедура разделена на предварительную обработку, сжатие и окончательное преобразование. Предварительная обработка в основном добавляет необходимое количество битов к входному сообщению, чтобы сформировать заполненный блок данных заданной длины. Дополненные данные делятся на t блоков одинаковой длины. Каждый блок X_i служит входом для функции сжатия h, которая каждый раз вычисляет новое преобразованное сообщение данных H_i, как функцию предыдущего H_{i-1} и входного X_i. После определенного количества циклов обработки данные окончательно модифицируются в результате окончательного преобразования. Таким образом генерируется хэш-значение (дайджест сообщения), соответствующее входному сообщению x. Предложенная архитектура гарантирует высокий уровень безопасности во всех приложениях, требующих аутентификации сообщения, посредством создания кода аутентификации сообщения. Уровень безопасности и преимущества хэш-функции SHA-2, на которой основана предложенная архитектура, обеспечивают высокий уровень безопасности. При реализации этой схемы аутентификации Хэш-функция SHA-2 представляет собой криптографические алгоритмы, которые принимают в качестве входных данных сообщение произвольной длины, и которые возвращают дайджест (или хэш-значение) фиксированной длины (от 160 до 512 бит в большинстве приложений). Хэш-функции используются во множестве протоколов, будь то для цифровых подписей на высокопроизводительных серверах или для аутентификации встроенных систем

Список использованных источников:

1. Качинский, М. В. Конвейерный процессор хэш-функции SHA-256 / М. В. Качинский, А. В. Станкевич // Информационные технологии и системы 2018 (ИТС 2018) = Information Technologies and Systems 2018 (ITS 2018) : материалы международной научной конференции, Минск, 25 октября 2018 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2018. – С. 158 - 159.

2. Качинский, М. В. Высокопроизводительная реализация криптографической хэш-функции SHA-256 на базе FPGA / М. В. Качинский, А. В. Станкевич // Технические средства защиты информации : тезисы докладов XVI Белорусско-российской научно – технической конференции, Минск, 5 июня 2018 г. – Минск: БГУИР, 2017. – С. 47.

3. Xiao-yang Zeng, Shi-tingLu, "A core-based multi-function security processor with GALS Wrapper",Solid-State and Integrated-Circuit Technology 2008. ICSICT 2008. 9th International Conference on, pp. 1839-1842, 2008.

ЛОГИЧЕСКАЯ ОПТИМИЗАЦИЯ НЕПОЛНОСТЬЮ ОПРЕДЕЛЁННЫХ ФУНКЦИЙ

Грицовец А.О.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бибило П.Н. – д.т.н., профессор

С каждым днём задачи проектирования цифровой аппаратуры становятся более объёмными, а требования к электронным вычислительным средствам по габаритам и затраченным ресурсам становятся всё жёсткими. Многие функциональные блоки управляющих и вычислительных устройств описываются булевыми функциями, поэтому оптимизация различных форм представлений систем булевых функций по-прежнему остается актуальной задачей.

На сегодняшний день многие задачи требуют большей производительности при меньших затратах при производстве электронных вычислительных средств. Производители стараются найти наилучшее решение при проектировании устройств. Для выполнения этой задачи часто прибегают к логической оптимизации булевых функций, которые являются математическими моделями функционирования многовыходных комбинационных схем.

Один из подходов к оптимизации булевых функций – аппарат диаграмм двоичного выбора [1-5]. Диаграммы двоичного выбора – компактная форма представления булевых функций в виде ациклического графа, которая соответствует многоуровневому представлению на базе разложения Шеннона. В начале логической оптимизации булевых функций на основе диаграмм двоичного выбора

требуется выбрать последовательность переменных, по которой ведётся многоуровневое разложение Шеннона. На следующем этапе строится диаграмма двоичного выбора по заданной перестановке переменных. Далее происходит поиск одинаковых поддеревьев в дереве (графе представления системы функций). Одинаковые поддеревья удаляются и заменяются уже найденным аналогичным поддеревом, тем самым удаляются лишние узлы, и сложность представления функций уменьшается.

Ключевым этапом в оптимизации является поиск одинаковых поддеревьев. Он начинается с листьев и продолжается до тех пор, пока не обнаружится, что одинаковых поддеревьев в дереве больше нет. Также важным этапом оптимизации булевых функций с помощью диаграмм двоичного выбора является выбор порядка переменных, по которым ведется разложение Шеннона. От этого выбора зависит количество одинаковых поддеревьев, а, следовательно, и степень оптимизации. Хорошей эвристикой при выборе перестановки переменных является порядок, в котором сначала идут наиболее часто встречающееся переменные, а в конце - наименее встречающиеся в исходной системе дизъюнктивных нормальных форм (ДНФ), задающей исходную систему либо уже полученные подфункции. Этот подход прост в реализации и даёт хорошие результаты, так как существует большая вероятность обнаружения «больших» одинаковых поддеревьев, и это позволяет упростить граф.

Зачастую встречаются ситуации, когда используются неполностью определённые булевы функции. Неполностью определённые функции, или частичные функции, - это функции, значения которых не определены на некоторых наборах значений переменных, на данных наборах значения функций при оптимизации заменяются определенными (0,1). При логической оптимизации неполностью определённых функций при помощи диаграмм двоичного выбора алгоритмы выбора перестановки и построения диаграммы аналогичны. Однако при поиске одинаковых поддеревьев неопределённые листовые значения следует дополнять до значений 0 или 1, чтобы получилось наибольшее число одинаковых поддеревьев. Таким образом, общий алгоритм логической оптимизации неполностью определённых функций начинается с этапа выбора порядка переменных разложения. Далее идёт этап разложения по выбранной перестановке переменных. На третьем этапе производится анализ всего дерева и дополнение неопределённых листьев до значения 0 или 1. На заключительном этапе производится поиск одинаковых поддеревьев и удаление избыточностей.

Список использованных источников:

1. Карпов, Ю. Верификация параллельных и распределённых программных систем /Ю. Карпов. - СПб: «БХВ-Петербург», 2010 – 560 с.
2. Бибило, П. Н. Применение диаграмм двоичного выбора при синтезе логических схем /П. Н. Бибило. – Минск: «Беларуская навука», 2014 – 231с..
3. Бибило, П. Н. Логическое проектирование дискретных устройств с использованием продукционно-фреймовой модели представления знаний /П. Н. Бибило, В. Н. Романов – Минск.: «Беларуская Навука», 2011. - 279 с.
4. Бибило, П. Н. Минимизации многоуровневых представлений систем булевых функций на основе разложения Шеннона / П. Н. Бибило, Ю. Ю. Ланкевич // Информатика, 2017 – № 2. – С. 45- 57.
5. Бибило П. Н. Алгоритм построения диаграммы двоичного выбора для системы полностью определённых булевых функций / П. Н. Бибило, П. В. Леончик - // Управляющие системы и машины. - 2009. - № 6. – С. 42 – 49.

ИССЛЕДОВАНИЕ КРИТЕРИЕВ ОЦЕНКИ КОРРЕКТНОСТИ ПРОИЗНОШЕНИЯ ФРАЗ ДЛЯ СИСТЕМЫ ИСПРАВЛЕНИЯ РЕЧЕВЫХ ДЕФЕКТОВ

Демидович В.С.

Белорусский государственный университет информатики и радиоэлектроники
Г. Минск, Республика Беларусь

Лихачев Д.С. – к.т.н., доцент

Речь человека имеет огромное количество характеристик таких как темп речи, громкость, высота голоса, интонация, тембр и др. Эти характеристики делают речь каждого человека уникальной и неповторимой, что в свою очередь усложняет ее анализ.

В данной статье описан метод, позволяющий определить правильность произношения фразы или слова, основываясь на *DTW-алгоритме* с использованием мел-кепстральных коэффициентов. Данные коэффициенты, расположенные на мел-шкале, позволяют выделить наиболее значимые для восприятия человеком частоты.