А. Н. Мальчуков, А. Н. Осокин

Быстрое вычисление контрольной суммы CRC: таблица против матрицы

Контрольная сумма — это некоторое значение, вычисленное для последовательности байт данных с помощью определенного алгоритма, которое используется на приемной стороне для подтверждения корректности полученных данных. В статье рассматривается быстродействующий алгоритм вычисления контрольной суммы, легко реализуемый на комбинационных схемах.

Введение

Первоначально контрольная сумма использовалась в системах с наличием обратной связи (переспроса) для обнаружения ошибок, возникающих в зашумленных каналах связи. Позднее, с развитием криптографических хеш-функций (алгоритмов хеширования), контрольные суммы стали использоваться для подтверждения целостности и подлинности данных. Обычно контрольная сумма посылается (считывается) в конце сообщения:

<блок данных> <контрольная сумма>.

В настоящее время существует множество алгоритмов получения контрольной суммы: сложение байтов, CRC (англ. cyclic redundancy check — избыточный циклический код), MD5, SHA и т. д. CRC традиционно используется в проводных и беспроводных протоколах передачи данных (Ethernet, Bluetooth, ZigBee, CAN, Fibre Channel и т. д.) для контроля целостности управляющих фрагментов или кадров данных. Далее речь пойдет об алгоритмах вычисления контрольных сумм CRC.

«Стандартный» алгоритм

Под «стандартным» алгоритмом подразумевается алгоритм, вычисляющий контрольную сумму CRC побитно, т. е. в каждом такте (итерации) данные последовательно продвигаются в некотором регистре на один бит, и в итоге в этом регистре получают контрольную сумму. Этот алгоритм широко известен [1] по его аппаратной реализации на регистрах с обратной связью (рис. 1).

На рис. 1 схематично показана работа простого алгоритма. Для CRC8 его можно описать следующим образом.

Начало. Регистр (массив) 8 бит содержит нулевое значение, данные поступают в регистр через его младший разряд к старшим, начиная со старшего разряда данных последовательным сдвигом.

Шаг 1. Сдвигаем данные в регистре на один бит от младших к старшему разряду, в младший разряд регистра заносится бит из потока данных.

Шаг 2. Если выдвинутый бит из 8 разряда регистра равен 0, переходим на шаг 4.

Шаг 3. Складываем по модулю два выдвинутый бит с разрядами регистра 1, 2, 3 и результат записываем в соответствующие ячейки регистра, т. е. фактически инвертируем содержимое 1, 2 и 3 разрядов регистра.

Шаг 4. Если еще не все биты поступили в регистр из потока данных, переходим на шаг 1.

Конец. В регистре содержится контрольная сумма CRC8.

При вычислении контрольной суммы CRC8 для последовательности битов данных в конец добавляют 8 нулей. При проверке контрольной суммы через регистр пропускают последовательность битов данных вместе с контрольной суммой в конце. В итоге