СТРУКТУРЫ СУММАТОРОВ ПО МОДУЛЮ 2^N+1 ДЛЯ УСТРОЙСТВ ТЕОРЕТИКО-ЧИСЛОВЫХ ПРЕОБРАЗОВАНИЙ

Лунин Д.А.

Национальный технический университет "Харьковский политехнический институт", г. Харьков

Арифметика остаточных классов нашла большое применение в многочисленных теоретико-числовых преобразованиях (ТЧП), которые широко используются для вычислений сверток, корреляций, в криптографии и моделях отказоустойчивых цифровых систем.

В частности, арифметика по модулю 2^n +1 находится в центре внимания многих последних исследовательских работ, потому что этот модуль является частью хорошо известного тройного набора модулей {2^n-1, 2^n, 2^n +1}, который широко используется для общего и специального представления системы остаточных классов.

Для ускорения операции сложения по модулю 2^n +1 следует свести к минимуму время вычисления переноса. Одно из решений состоит в использовании сумматоров CLA (Carry Look-Ahead – опережающий перенос).Пусть $A = a_{n-1}a_{n-2}\ldots a_1a_0$ и $B = b_{n-1}b_{n-2}\ldots b_1b_0$ – два n-битовых числа, $S = s_{n-1}s_{n-2}\ldots s_1s_0$ – их сумма. Для описания задачи вычисления переноса обычно используются две переменные: переменная генерирования переноса: $g_i = a_i \times b_i$; переменная распространения переноса : $p_i = a_i + b_i$.

Вычисление переносов в различных реализациях CLA выполняется при помощи рекурсивной формулы $c_i = g_i + p_i \times C_{i-1}$; сумма бит будет равна $s_i = h_i \oplus q_{i-1}$, где $h_i = a_i \oplus b_i$ является полусуммой.

Определяя знак операции ○ как оператор, который связывает образованные и переданные пары, можно вычислить новую пару в соответствии с уравнением: $(g_x, p_x) \circ (g_y, p_y) = (g_x + p_x g_x, p_x p_y)$

Рисунок 1. Блок-схема сумматора CLA

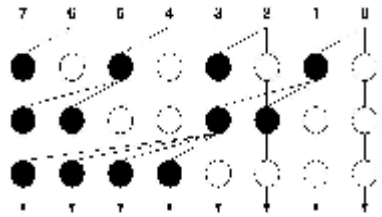

Рисунок 2. Схема параллельного переноса Скланского