

А. С. Ионисян (Ставрополь, СКФУ). **VHDL-библиотека базовых операций арифметики системы остаточных классов.**

Одним из современных способов представления чисел и выполнения операций над ними является система остаточных классов (СОК), в которой каждое число задается набором остатков от деления на набор взаимно простых чисел-оснований. СОК образует конечное кольцо относительно операций сложения и умножения. Операции деления и сравнения чисел в данной алгебре считаются трудновыполнимыми. Перспективным направлением исследований СОК является реализация арифметических операций на аппаратном уровне в виде прошивок FPGA-микросхем.

Автором создана на языке VHDL библиотека взаимосвязанных модулей, реализующая арифметические, логические и конверсионные операции над целыми неотрицательными числами, выраженными в двоичной системе счисления и в СОК. За счет выявления связей между операциями, использования единых структур данных и устранения излишнего дублирования получилось оптимизировать объем исходного кода библиотеки и сделать его простым для понимания сути работы расчетных алгоритмов, практически без ущерба по скорости работы. Задачи создания топологии, существенно превышающей по скорости работы, или более оптимальной по числу используемых транзисторов относительно уже имеющихся выдающихся частных результатов не ставилось.

В основу работы были положены алгоритмы и методы, описанные автором в [1]. В качестве оснований СОК можно использовать любой кортеж из простых 8-битных чисел. Операции сравнения и деления чисел реализованы путем перехода к так называемой обобщенной позиционной системе счисления (mixed radix system — в англоязычной литературе).

Использование данной библиотеки в рабочих проектах исследователей СОК позволит ускорить их работу, уменьшит количество ошибок реализации низкоуровневых алгоритмов и даст возможность сконцентрироваться на решении более высокоуровневых задач компьютерной алгебры.

СПИСОК ЛИТЕРАТУРЫ

1. *Ионисян А. С.* Алгоритмы и методы модулярной арифметики на основе интервальных характеристик чисел. — Параллельная компьютерная алгебра и ее приложения в новых инфокоммуникационных системах: Первая международная конференция, сборник научных трудов, 20–24 октября 2014 г. Ставрополь: Фабула, 2014, с. 206–214.