On formally proved programs for arithmetic of natural numbers in binary representation

S.D. Meshveliani (Ailamazyan Program Systems Institute of RAS, Pereslavl-Zalessky)
E-mail address: mechvel@botik.ru

It is described an experience in developing proved programs for arithmetic of binary represented natural numbers. The programs are provided with formal machine-checked proofs for certain basic properties of such arithmetic. It is used the Agda language (having pure functionality, rich type system, "lazy" computation model, and *dependent types*). The arithmetic is done by usual naive algorithms operating with bit lists. Constructing full formal proofs for these algorithms occurs not so simple as it seems at first sight. The programs constitute the Binary library (http://www.botik.ru/pub/local/Mechveliani/binNat/3.1/) that improves and completes the Bin part of the Standard library lib-0.15 for Agda.

A. Alekseyev provided a similar library for binary arithmetic for Agda in 2013 (https://github.com/Rotsor/BinDivMod). This library presents the program code, there are no explanations about this code. The two libraries are developed independently and their proof parts are built in a different way. In this talk there is described the approach of the Binary library.

О формальных доказательствах для программ арифметики натуральных чисел в двоичном представлении

С.Д. Мешвелиани (Институт программных систем им. А.К. Айламазяна РАН, Переславль-Залесский)
E-mail address: mechvel@botik.ru

Обсуждается опыт программирования арифметики натуральных чисел в двоичной записи. Программа содержит формальные машинно-проверяемые доказательства некоторых основных свойств такой арифметики. Используется язык программирования Agda (чисто функциональный, с богатой системой типов и *зависимыми типами*). Рассматриваются обычные алгоритмы «в столбик», обрабатывающие списки битов. Задача составления полных формальных доказательств для этих алгоритмов оказывается не такой простой, как может показаться. Программы составляют библиотеку Binary (http://www.botik.ru/pub/local/Mechveliani/binNat/3.1/), которая исправляет и дополняет часть Bin стандартной библиотеки lib-0.15 Агды.

А. Алексеев опубликовал подобную библиотеку для языка Agda в 2013-м году (https://github.com/Rotsor/BinDivMod). Эта библиотека состоит из программного кода, без каких-либо объяснительных материалов по разработке. Две эти библиотеки разработаны независимо, доказательства в их программах устроены по-разному. В данном докладе объясняются принципы построения библиотеки Binary.