УДК 681.3

О.Г. СТАРУСЕВ, канд. техн. наук, НТУ "ХПИ" (г. Харьков)

ВЫБОР ИНСТРУМЕНТАРИЯ ДЛЯ ФОРМАЛЬНОЙ СПЕЦИФИКАЦИИ ИНФОРМАЦИОННЫХ СИТЕМ В НОТАЦИИ Z

У статті наведений огляд програмних засобів, що підтримують метод формальної специфікації – Z, розглянуті основні властивості та характеристики програмного інструментарію, наведені рекомендації щодо вибору того чи іншого програмного засобу.

In this article the review of program tools for support of language of the formal specification Z is resulted. In addition, the basic criteria of choice and functionality of the considered software are considered. In the article the recommendations on the choice of the most comfortable program instrument are given.

Постановка проблемы. Нотация Z – это набор правил для представления формального математического описания информационных систем на основе W-логики. Нотация Z основана на модели, т.е. является поведенческим описанием системы. Модель может быть представлена в виде последовательности состояний, т.е. набора переменных состояния и операций, которые могут изменять эти состояния. Ядро нотации содержит достаточно большой набор абстрактных типов данных и операций для работы с ними. Этот вид моделирования приводит к использованию императивных процедурных языков программирования, предлагающих большую коллекцию типов данных и действий над ними. Кроме того, от Z-модели возможен переход к языкам объектно-ориентированного программирования (ООП). При этом переменные состояния могут быть интерпретированы как атрибуты объектов, а операции – как методы. В описании нотации Z также приведены возможности использования такого правила ООП как наследование. Выбор стиля работы с моделью – функционального или объектно-ориентированного существенно зависит от задач, а также от предпочтений разработчиков.

Метод Z не является полноправным методом, а всего лишь нотацией, и поддерживается многими другими подходами к формальной спецификации. Текст, написанный при помощи нотации Z, позволяет задать поведение системы. Нотация Z не является выполняемой, т.е. текст не может быть откомпилирован или интерпретирован в исполняемый код. С ее помощью можно описать систему и доказать ее непротиворечивость, что особенно важно при построении критичных систем. На сегодняшний день описание моделей и доказательства противоречивости производится при помощи программного инструментария. Необходимо рассмотреть задачу выбора такого инструментария.

Анализ литературы. Стоит отметить, что, к сожалению, отечественной литературы по нотации Z не существует. Основная информация доступна в виде печатных изданий Оксфордского и Кембриджского университетов, а также ряда других университетов и научных центров Великобритании [1–3]. Одним из комитетов ISO был предложен первичный вариант (draft) стандарта на нотацию Z [4], который обсуждается и сейчас. Вопросы выбора и применения программного инструментария в существующей литературе практически не освещены.

Целью этой статьи является выбор программного инструментария для поддержки работы с моделями, описанными при помощи нотации Z.

Выбор инструментария, поддерживающего нотацию Z. Наиболее широко используемыми средствами программной поддержки нотации Z являются ProofPower, Zola, Zeus и CADiZ. Прежде чем перейти к рассмотрению возможностей этих средств необходимо определится с критериями выбора. Все используемые критерии можно разделить на две группы: основные и дополнительные. К основным критериям относятся:

- возможности записи и чтения спецификации;
- возможность доказательства свойств спецификации;
- генерацию программного кода из созданной спецификации.

В качестве дополнительных критериев используем следующее:

- поддержка математического инструментария;
- поддержка больших спецификаций;
- открытость и интероперабельность;
- цену инструментария.

Весь рассматриваемый программный инструментарий является коммерческим и распространяются согласно ряду предлагаемых лицензий (коммерческая, академическая и временная).

ProofPower. Инструмент предназначен для доказательств теорем и подготовки документов. Использует подход HOL (High Ordered Language), который реализован на языке Poly/ML под управлением SunOS (Sunview).

Константы и синтаксические категории (инфиксные отношения, функции и родовые понятия) операторов объявляются на верхнем уровне и при помощи специальной функции П заставляют схему выполнять предикаты-выражения. Схема задается в виде документа LATEX. Инструмент позволяет также производить проверку корректности вводимых выражений.

Поддержка доказательств для Z достигается путем семантического включения языка Z в HOL, таким образом, что термы Z представляются в виде термов HOL [5]. Хотя, в принципе, можно использовать только язык Z без HOL.

Zola. Средство создания, поддержки и проверки Z спецификаций. Разработано компанией Imperial Software Technology (Кембридж,

Великобритания). Функционирует под управлением SunOS 4 и SunView.

Zola предлагает два режима создания спецификаций: синтаксически зависимый и ASCII парсер. Первый режим полезен при изучении синтаксиса Z, а второй является более быстрым при вводе спецификаций.

В Zola представлено подмножество Z, расширенное за счет добавления средств доказательств теорем. Наиболее существенным недостатком Zola (характерным для большинства Z средств) является то, что по соглашению схема S подразумевает неявную схему ΔS, если она не определена явным образом. При помощи дельта-оператора определяется неявная форма, а явная форма использует большую греческую Δ как часть имени схемы, что вносит определенную путаницу в определения.

Zola содержит модуль тактического доказательства теорем (tactical theorem prover), который базируется на W-логике. Тактика включает в себя такие подходы как SEQ (последовательности) и CHOICE (альтернативы). Доказательства сохраняются как часть состояний схемы.

Система позволяет подключать внешние приложения за счет детально описанной спецификации и прозрачной структуры схем.

CADiZ. Средство для синтаксического анализа и проверки Z схем. Предложено York Software Engineering и функционирует под управлением большинства клонов Unix и на платформе Windows.

Средство не является интерактивным и требует создания входного файла со спецификацией в LATEX или troff. Основной целью инструмента является представление иерархии доказательств при помощи правил W-логики [5]. На сегодняшний день средства тактического доказательства теорем заявлены, но не разработаны (планируется на ближайший год). CADiZ используется для работы со схемами малого и среднего размера (до 200 страниц).

Zeus. Небольшое интерактивное средства для создания спецификаций и доказательства теорем непротиворечивости. Zeus является перспективным проектом, который разрабатывается университетом Вирджинии (США). Основной целью проекта является разработка инструмента для промышленного использования метода формальной спецификации Z. Инструментарий функционирует под управлением большинства клонов ОС UNIX и на платформе Windows. Может быть использован совместно с инструментом Z/EVES (компания Ora, Канада).

Основным отличием является достаточно удобная интерактивная среда с дружественным интерфейсом. Кроме того, средство обладает удобным синтаксическим анализатором и может работать с малыми и средними спецификациями. Пример рабочего экрана приведен на рисунке.

Выводы. Основным преимуществом использования метода формальной спецификации является возможность выявления противоречий в системных требованиях. Метод формальной спецификации Z представляется наиболее перспективным для этих целей.

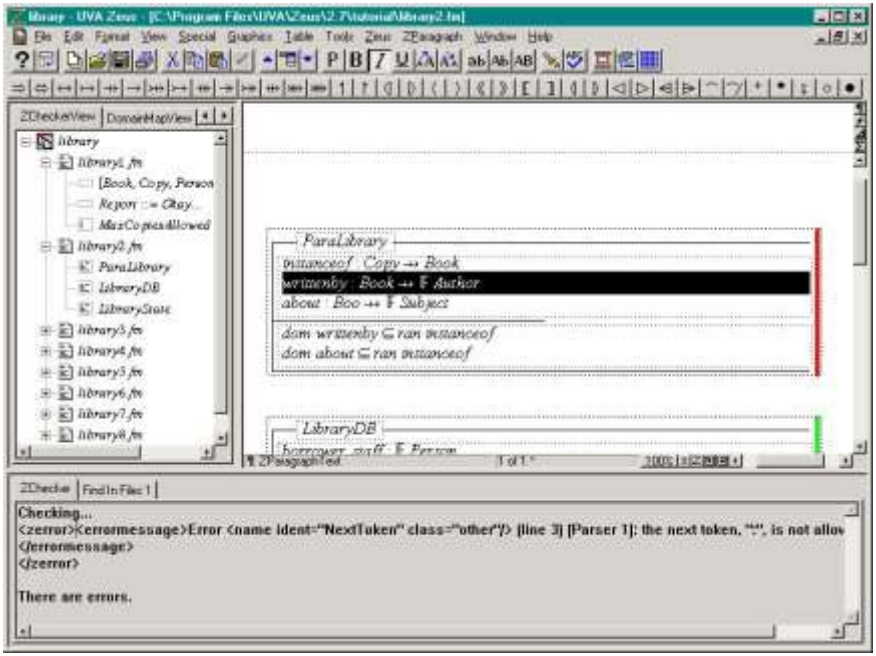

Рис. Рабочий экран инструмента Zeus

Наиболее перспективным из рассмотренных выше средств является ProofPower, который предполагает не только использование языка Z, но и объединяет в себе возможности представления формальных схем с возможностью доказательств теорем высших порядков при помощи подхода HOL. При этом может быть использован как коммерческий инструментарий (ProofPower), так и средства, входящие в репозиторий HOL88 [6].

В дальнейшем необходимо провести проверку правильности работы данного инструментария на больших спецификациях (более 400 страниц) со сложными семантическими правилами.

Список литературы: 1. *Spivey J.M.* The Z Notation: A reference manual. – Prentice Hall International Series of Computer Science, 1992. – 150 p. **2.** *Bowen J.P., Hall J.A.* Z User Workshop. – Cambridge, Springer-Verlag, 1994. – 320 p. **3.** *Woodcock J.C.P., Davies J.* Using Z: Specification, Proof, Refinement. – London, Prentice-Hall, 1996. – 407 p. **4.** *ISO/IEC 13568:2002* Information technology – Z formal specification notation – Syntax, type system and semantic. – 2002. – 189 p. **5.** *Gordon M.J., Bowen J.P.* Z and HOL // Z Users Workshop. – Cambridge. – 1994. – P. 141 – 166. **6.** *Gordon M.J., Melham T.* Introduction to HOL: A theorem proving environment for higher order logic. – NY: Cambridge, 1993. – 472 p.

Поступила в редакцию 24.09.2004