

порядка. Они являются арифметическими законами теории. В построенной теории выводимы многие истинные формулы. Например, формула $\exists z((x+z)=y \wedge \neg(z=0))$ истинна и выводима. Она представляет предикат $x < y$. Примеры истинных, но невыводимых в арифметике первого порядка формул привести довольно сложно. Тем не менее такие формулы существуют, т. е. арифметика первого порядка — неполная теория, как это следует из теоремы Гёделя о неполноте. Эта теория также неразрешима, а множество истинных в ней формул не является даже рекурсивно перечислимым. Арифметика первого порядка без операции умножения (арифметика Пресбургера) является уже разрешимой теорией, хотя и со сложным алгоритмом разрешимости (см. § 5.4).

Пример 2.5. Расширением элементарной арифметики является арифметика с одномерными массивами чисел. Язык этой арифметики *Ar1m* был описан в примере 2.3 как двухсортный язык. В дополнение к нелогическим аксиомам арифметики первого порядка (без массивов) для рассматриваемой теории необходимо добавить еще две нелогические аксиомы, определяющие операции доступа к элементу массива и обновления элемента массива:

А.М1. $(x=y) \Rightarrow \text{upd}(M, x, e)[y] = e;$

А.М2. $\neg(x=y) \Rightarrow \text{upd}(M, x, e)[y] = M[y].$

Полученная теория сложнее элементарной арифметики. Пример выводимой в ней формулы: $\text{upd}(\text{upd}(M, x, e), x, i)[x] = i$. Эта теория так же, как и элементарная арифметика, конечно, неразрешима и неполна. Оказывается, что неразрешима даже арифметика Пресбургера с массивами.

Примерами разрешимых теорий нечисловой природы являются элементарная геометрия на плоскости, теория линейного порядка.

2.3. ЛОГИЧЕСКИЙ ЯЗЫК СПЕЦИФИКАЦИИ СВОЙСТВ ПРОГРАММ

Для записи утверждений о свойствах и отношениях переменных программы будем в дальнейшем использовать формальный логический язык спецификации. Важнейшими качествами этого языка для задач верификации программ являются:

выразительная способность, т. е. возможность формально выражать широкий класс утверждений о свойствах и отношениях программных переменных;

дедуктивная способность, т. е. возможность формально доказывать истинность утверждений, выражимых в языке.

Следует иметь в виду, что оба эти качества формального языка спецификации не могут быть безграничны в своем приближении к естественному языку и к неформальным способам рассуждений. Для любого достаточно богатого формального логического языка существуют как невыразимые утверждения естественного языка, так и недоказуемые (но истинные) формальные утверждения.

С практической точки зрения логический язык спецификации свойств программ должен обладать следующими свойствами.