УДК 004.05+004.415.5

В.Л. ПЕТРИК

Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Украина

ЭКСПЕРТИЗА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ДЕСКРИПТОРНОГО СЕМАНТИЧЕСКОГО ПРОСТРАНСТВА

Показаны проблемы экспертизы, основанной на оценке семантической корректности программного обеспечения информационно-управляющих систем, обусловленные значительной ресурсоемкостью. Предложен метод эффективного представления семантической информации, основанный на использовании сжимающего семантического отображения семантического пространства в упорядоченное множество семантических дескрипторов. Исследованы свойства дескрипторного семантического пространства. Показана возможность использования семантических дескрипторов для вычисления физической размерности результата. Определена аксиоматика дескрипторной алгебры, использование которой позволяет снизить вычислительные ресурсы, необходимые для формального доказательства семантической корректности программного обеспечения информационно-управляющих систем.

семантический вектор, сжимающее семантическое отображение, семантический дескриптор, дескрипторное семантическое пространство, дескрипторная алгебра

Введение

В современных информационно-управляющих системах до 80% функций реализовано программно. Это порождает высокую сложность программного обеспечения (ПО) и требует применения специальных методов обеспечения надежности. Важную роль играет независимая верификация при экспертизе ПО сертификационными центрами (СЦ). Значительные объемы и сложность ПО, а также ограниченность ресурсов требуют использования СЦ формальных методов оценки корректности ПО для областей критического применения, например, авиационно-космической отрасли или атомной энергетики.

Постановка задачи. Известен метод оценки надежности ПО, основанный на анализе преобразований размерностей [1, 2], позволяющий идентифицировать значительную часть программных дефектов определенных классов. Существенным недостатком метода является значительная трудоемкость, связанная с подготовкой ПО к экспертизе и обусловленная необходимостью указания для каждой переменной ее физической размерности – семантики.

Представление семантической информации в виде семантических векторов (СВ) приводит к многократному увеличению объема исходных данных, необходимых для проведения экспертизы, по сравнению с обычным тестированием. Так использование системы СИ увеличивает общий объем дополнительных данных и операций, связанных с контролем семантической корректности, на порядок по сравнению с обычным тестированием.

Таким образом, существует проблема реализации контроля семантической корректности программного обеспечения в условиях ресурсных ограничений.

Одно из возможных решений заключается в разработке и использовании компактного представления семантической информации. Необходимо доказать существование специального сжимающего семантического отображения (ССО), исследовать его свойства, а также свойства самих объектов – носителей семантической информации и определить алгебраические свойства операций над ними. Рассмотрению перечисленных выше вопросов и посвящена данная работа.

Возможность существования отображения

Докажем возможность построения ССО *n*-мерного семантического пространства (СП) на упорядоченное множество скалярных числовых элементов, называемых далее семантическими дескрипторами (СД):

$$S : P \to D, \qquad (1)$$

где S – ССО, P – СП, $D = \{D_i\}$ – упорядоченное множество СД.

Пусть СП P представлено декартовым произведением: $X_1 \times X_2 \times ... \times X_n = Q$, тогда

$$S : \{X_1 \times X_2 \times ... \times X_n\} \to \{D_i\},$$

где $X_1, X_2, ..., X_n$ – основные единицы выбранной системы единиц (СЕ) [3].

Взаимнооднозначное отображение S множества $\{Q_i\}$ во множество $\{D_i\}$ сопоставляет каждому элементу $x \in Q$ элемент $S(x) \in D$ – СД, который является значением отображения S на элемент x. Необходимым условием существования ССО является эквивалентность множеств элементов СП и семантических дескрипторов.

Свойства сжимающего семантического отображения

Одна из задач данной работы – разработка и исследование свойств биективного отображения S, обеспечивающего такое взаимно однозначное соответствие элементов множеств Q и D, что каждому элементу множества Q отвечает один и только один элемент множества D, и наоборот. Напомним, что отображение S является биекцией, если оно одновременно является сюръекцией и инъекцией [3, 4]. Таким образом, искомое отображение S должно быть сюръективным и инъективным.

Искомое отображение S есть сюръекция, так как $S(Q)=D$.

Для любых двух различимых элементов x_1 и x_2 из Q их образы $d_1=S(x_1)$, $d_2=S(x_2)$ должны быть также различны, поэтому S является инъекцией, т.е.:

$$\forall\ x_1 \neq x_2 \text{ и } x_1, x_2 \in Q\ \exists\ d_1=S(x_1),\ d_2=S(x_2),\ d_1 \neq d_2.$$

Отображение S множества Q во множество D однозначно должно определяться множеством $\{(x,S(x)\rangle \in Q \text{x} D\ |x \in Q\}$ $S{:}Q \to D$. Это множество и будет отображением S.

Необходимо обеспечить взаимнооднозначное соответствие между множествами Q и D. Для этого множества Q и D должны быть эквивалентными. Множество элементов Q счетно, т.к. его элементы можно биективно сопоставить с натуральными числами, т.е. элементы Q можно занумеровать. Множество D также счетно. Два конечных множества эквивалентны тогда и только тогда, когда число элементов у них одинаково.

Множество СД D является частично упорядоченным множеством. Действительно, пусть φ – некоторое бинарное отношение во множестве D, определяемое некоторым множеством $R_\varphi \subset D \times D$.

Отношение φ является частичной упорядоченностью, так как оно удовлетворяет условиям:

1) рефлексивности: $a \varphi a$;
2) транзитивности: если $a \varphi b$, $b \varphi c$, то $a \varphi c$;
3) антисимметричности: если $a \varphi b$ и $b \varphi a$, то $a = b$.

Запись $d_1 \le d_2$ означает, что пара $(d_1,d_2) \in R_\varphi$, при этом d_1 не превосходит d_2 или d_1 подчинен d_2.

Отображение S сохраняет порядок. Действительно, пусть Q и D – два частично упорядоченных множества, и пусть S есть отображение Q в D. Отображение S сохраняет порядок, т.к. из $a \le b$, где $a,b \in Q$ следует, что $S(a) \le S(b)$ в D.

Отображение S – изоморфизм частично упорядоченных множеств Q и D, т.к. оно биективно, а соотношение $S(a) \le S(b)$ выполняется в том и только в том случае, когда $a \le b$. Таким образом, множества Q и D являются изоморфными между собой. Отношение изоморфизма S между частично упорядоченными множествами является отношением эквивалентности (оно симметрично, транзитивно и рефлексивно).

Отображение S СП Q будем называть сжимающим семантическим отображением или сжатием, если существует такое число $\alpha < 1$, что для любых двух элементов $x,y \in Q$ выполняется неравенство $\rho(Ax,Ay) \le \alpha\rho(x,y)$.

Рассмотрим ССО S, задаваемое уравнением

$$d = \sum_{j=1}^{n} a_j x_j + b, \qquad (2)$$

где n – количество основных единиц СЕ;

x_j – степени основных единиц СЕ;

b – коэффициент сдвига ССО.

Найдем условие, при котором ССО будет сжатием. Для n-мерного евклидового пространства метрика определяется следующим образом:

$$\rho(x,y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}\ .$$

На основании неравенства Коши-Буняковского имеем

$$\rho^2(y',y'') = \left(\sum_j a_j (x_j' - x_j'')\right)^2 \le \left(\sum_j a_j^2\right)\rho\ .$$

Отсюда условие сжимаемости

$$\sum_j a_j^2 \le \alpha \le 1\ . \qquad (3)$$

Найдем ССО в виде (2).

Предположим, что существуют $L_{\max j}$ – граничное максимальное по модулю значение j-й координаты СВ, соответствующей одной из основных единиц выбранной системы; $L_{\min j} \ne 0$ – граничное минимальное по модулю значение j-й координаты СВ. Тогда координаты элементов, принадлежащих ограниченной области СП, могут быть определены как:

$$x_j \in [-L_{\max j;}\ -L_{\min j}] \cup 0 \cup [L_{\min j}; L_{\max j}]\ . \quad (4)$$

На основании того, что СД для безразмерной переменной $d = S(0) = 0$, имеем $b = 0$ для (2).

Далее будем искать сжимающее семантическое отображение в виде:

$$d = \sum_{j=1}^{n} a_j x_j\ . \qquad (5)$$

Сформулируем необходимое условие (НУ) изоморфизма ССО для положительных x:

$$\forall j = \overline{1,n}\ \ a_j \cdot L_{\min j} > \sum_{i=j+1}^{n} a_i \cdot L_{\max i}\ . \qquad (6)$$

В случае, когда x может принимать как положительные, так и отрицательные значения, необходимо выполнение более сильного НУ изоморфизма:

$$\forall j = \overline{1,n}\ \ a_j \cdot L_{\min j+1} > \sum_{i=j+2}^{n} a_i \cdot L_{\max i}\ . \qquad (7)$$

Полагаем, что $\sum_j a_j^2 \le 1$

и $\forall j = \overline{1,n}\ \ a_j > 0$.

Сжимающее семантическое отображение и свойства семантических дескрипторов

Реализация ССО в условиях ограниченных вычислительных ресурсов требует ограничения мощности множества элементов СП. Анализ физических размерностей для нескольких систем единиц позволил определить диапазоны модулей степеней основных единиц, представленные в табл.1.

Таблица 1

Диапазоны модулей степеней основных единиц

Система единиц	$L_{\min j}$	$L_{\max j}$
СИ	1	7
СГС	½	3
МКГСС	1	6

Ввиду того, что СИ обеспечивает наибольшую достоверность экспертизы ПО ИУС [5], ограничимся исследованием возможности построения ССО для СИ. Согласно [6] примем порядок основных единиц, приведенный в табл. 2.

Таблица 2

Порядок основных единиц ССО

№	Величина	Размерность	Наименование основной единицы	
			Наименование	Обозначение
1	Длина	*L*	метр	м
2	Масса	*M*	килограмм	кг
3	Время	*T*	секунда	с
4	Сила электрического тока	*I*	Ампер	А
5	Термодинамическая температура	Θ	Кельвин	К
6	Сила света	*J*	кандела	Кд
7	Количество вещества	–	моль	Моль
8	Плоский угол	–	радиан	Рад
9	Телесный угол	–	стерадиан	Ср

Таблица 3

Коэффициенты ССО и структура СД

№ Разряда	Основная единица	Степень основной единицы		Порядок разряда	Коэффициенты ССО a_j
		x_j	размерность		
0	Знаковый разряд			1	
1	Длина [м]	4	$м^4$	1/2	1/8
2		2	$м^2$	1/4	
3		1	$м^1$	1/8	
4	Разделительный			1/16	
5	Масса [кг]	4	$кг^4$	1/32	1/128
6		2	$кг^2$	1/64	
7		1	$кг^1$	1/128	
8	Разделительный			1/256	
9	Время [сек]	4	$сек^4$	1/512	1/2048
10		2	$сек^2$	1/1024	
11		1	$сек^1$	1/2048	
12	Разделительный			1/4096	
13	Сила электрического тока [А]	4	$а^4$	1/8192	1/32768
14		2	$а^2$	1/16384	
15		1	$а^1$	1/32768	

На основании:

– НУ изоморфизма ССО;

– выбранного порядка основных единиц, приведенного в табл. 2;

– диапазона модулей степеней основных единиц, приведенного в табл. 1, определим значения коэффициентов ССО a_j.

Значения искомых коэффициентов будем искать в двоичной форме.

Старший, знаковый разряд, – нулевой. Значения каждого из последующих разрядов в два раза меньше предыдущего. Коэффициенты ССО, а также характеристики разрядов СД, представлены в табл. 3, при построении которой подразумевалось на основании табл. 1, что максимальное значение степеней каждой из основных единиц ограничено семью, что обусловило выделение трех двоичных разрядов.

Согласно принятым допущениям «длина», измеряемая в [м], представляется единицей в третьем разряде СД, остальные разряды имеют нулевые значения. «Площадь», измеряемая в [$м^2$], имеет единицу во втором разряде, остальные разряды – нулевые. «Объем», измеряемый в [$м^3$], имеет только во втором и третьем разрядах СД единицу. Аналогично представляются размерности остальных физических единиц {время}, {масса} и т.п. В последней колонке табл. 3 приведены коэффициенты ССО, значения которых совпадают с минимальным порядком разряда соответствующей основной единицы, который содержится в предпоследней колонке. Значение СД определяются суммой произведений степеней порядков разрядов на соответствующие коэффициенты a_j ССО. Например, СД «длины» имеет значение 1/8, СД «объема» 3/8. Введение «разделительных» раз-

рядов обусловлено необходимостью обеспечения изоморфизма ССО как для положительных, так и для отрицательных степеней размерностей основных единиц.

Предложенное ССО позволяет находить СД функций по СД ее аргументов. При этом СД частного определяется как разность СД делимого и делителя, а СД произведения – как сумма СД сомножителей. СД функции возведения в целую степень определяется как произведение СД аргумента на константу – показатель степени.

Свойства дескрипторного семантического пространства

Множество СД D обладает метрикой, определяющей расстояние $\rho(x,y)$ между любыми элементами x и y из D в соответствии с аксиомами:

1) $\rho(x,y) = 0$, если $x = y$;
2) $\rho(x,y) = \rho(y,x)$; (8)
3) $\rho(x,z) \le \rho(x,y) + \rho(y,z)$.

Множество СД D является метрическим пространством, которое далее будем называть дескрипторным семантическим пространством (ДСП).

ДСП D является линейным (векторным), т.к. оно удовлетворяет следующим условиям:

I. Для любых двух СД d_i, $d_j \in D$ однозначно определен третий элемент – СД $d_k \in D$, соответствующий их сумме, обозначаемой $d_i + d_j$, причем выполняются законы:

1) $d_i + d_j = d_j + d_i$ (коммутативность сложения СД);
2) $d_i + (d_j + d_к) = (d_i + d_j) + d_к$ (ассоциативность сложения СД);
3) в D существует нулевой СД d_0, соответствующий безразмерной единице, такой, что $d_i + d_0 = d_i$ для всех $d_i \in D$;
4) для каждого СД $d_i \in D$ существует противоположный СД $(-d_i)$, такой, что $d_i + (-d_i) = 0$.

II. Для любого числа α и любого СД $d_i \in D$ определен СД $\alpha d_i \in D$, причем:

1) $\alpha(\beta d_i) = (\alpha\beta) d_i$;
2) $1 d_i = d_i$; (9)
3) $(\alpha + \beta) d_i = \alpha d_i + \beta d_i$;
4) $\alpha(d_i + d_j) = \alpha d_i + \alpha d_j$.

ДСП D является алгеброй, т.к. в нем определена алгебраическая операция умножения СД с аксиомами:

1) $(d_i d_j)\, d_к = d_i\, (d_j d_к)$; (10)
2) $d_i\, (d_j + d_к) = d_i\, d_j + d_i\, d_к$; $(d_j + d_к)\, d_i = d_j d_i + d_к d_i$;
3) $\alpha\, (d_i d_j) = (\alpha d_i)\, d_j = d_i\, (\alpha d_j)$.

Так как операция умножения коммутативна, т.е. выполняется аксиома: $d_i d_j = d_j d_i$, то дескрипторная алгебра (алгебра ДСП) является коммутативной алгеброй.

ДСП D является нормированным, т.к. в нем определена норма p, удовлетворяющая условиям:

1) $p(d_i) = 0$ только если $d_i = d_0$, где d_0 – нулевой СД.

   Роль нулевого СД в ДСП D играет элемент, имеющий координату 0;
2) $p(\alpha d_i) = |\alpha| p(d_i)$ для всех α, где α – число;
3) $p(d_i) \ge 0$ при $d_i \ne d_0$; (11)
4) $p(d_i + d_j) \le p(d_i) + p(d_j)$, $d_i, d_j \in D$.

ДСП является нормированным и метрическим, т.к. $\rho(d_i,d_j) = \| d_i - d_j \|$.

Дескрипторное семантическое нормированное пространство D является нормированной алгеброй, т.к. в нем выполняются две аксиомы:

1) $\|e\| = 1$;
2) $\| d_i\, d_j \| \le \|d_i\| \, \|d_j\|$.

Дескрипторная алгебра

Линейность ДСП позволяет контролировать семантическую корректность ПО ИУС благодаря свойствам операций, приведенным в табл. 4, в кото-

рой приняты следующие обозначения: L, R – левый и правый операнды, $d(L)$, $d(R)$ – их СД.

Таблица 4

Аксиоматика дескрипторной алгебры

№	Операция	Обозначение	Условие корректности	Дескриптор результата
1	Сложение	$L+R$	$d(L)=d(R)$	$d(L)$
2	Вычитание	$L–R$	$d(L)=d(R)$	$d(L)$
3	Умножение	$L\cdot R$	Отсутствует	$d(L)+d(R)$
4	Деление	L/R	Отсутствует	$d(L)–d(R)$
5	Возведение в степень	L^R	$d(R)=0$	$d(L)*R$
6	Сравнение	$L>R$, $L<R$, $L=R$	$d(L)=d(R)$	Отсутствует
7	Присваивание	$L=R$	$d(L)=d(R)$	$d(L)$

Значение СД результата корректного выполнения операций сложения, вычитания, сравнения, присваивания совпадает со значением СД любого из операндов. Несовпадение значений СД операндов перечисленных операций свидетельствует о некорректности операций и, соответственно, о программном дефекте. При выполнении операций умножения условие корректности не проверяется, а СД результата определяется как сумма СД множителей. При выполнении операции деления условие корректности также не проверяется, однако СД результата является разностью значений СД делимого и делителя. При возведении в степень условием корректности является нулевое значение СД правого операнда – безразмерность показателя степени, а СД результата корректного возведения в степень определяется как произведение СД основания на показатель степени.

При выполнении операций над СД, ввиду представления семантической информации в виде дроби, возможно накопление ошибки из-за конечной точности как хранения данных, так вычислений. Это влечет необходимость дополнительной корректировки СД результата. В связи с дискретностью допустимых значений СД, кратных порядку минимального разряда старшей основной единицы, который является своеобразным дескрипторным квантом, может возникнуть необходимость восстановления значений СД до ближайшего целочисленного количества квантов.

Использование СД позволяет доказывать семантическую корректность ПО ИУС посредством решения только одной алгебраической системы линейных уравнений. Например, корректность оператора, вычисляющего путь, пройденный телом за время t, находящимся первоначально на расстоянии S_0, движущимся со скорость V и ускорением a:

$$S = S_0 + V \cdot t + a \cdot t \cdot t / 2,$$

сводится к доказательству непротиворечивости системы уравнений и тождеств, построенных на основе аксиоматики дескрипторной алгебры:

$$\begin{cases} d_S = d_{S0}; \\ d_S = d_V + d_t; \\ d_S = d_a + 2d_t, \end{cases}$$

где $d_S, d_{S0}, d_V, d_t, d_a$ – СД пройденного пути, первоначального расстояния, начальной скорости, времени и ускорения.

Преимущества семантических дескрипторов

Использование СД для контроля семантической корректности возможно в двух вариантах. Первый предусматривает непосредственную интерпретацию операций посредством переопределения программных типов данных или статического анализа программного кода. Второй заключается в генерации в процессе статического анализа программного кода системы линейных алгебраических уравнений и последующем доказательстве ее совместности. В каждом из вариантов применение СД обеспечивает следующие преимущества по сравнению с СВ:

– уменьшение дополнительных объемов ОЗУ, необходимых для хранения семантической инфор-

мации. Так СВ для системы СИ представляет собой упорядоченное множество из девяти чисел, а СД для любой СЕ – только одно число;

– уменьшение количества дополнительных операций для проверки условия семантической корректности и вычисления СД результата. При работе с СВ требуется производить операции над всеми девятью координатами, а при работе с СД – только над одним числом;

– применение СД для алгебраического контроля семантической корректности ПО, основывающегося на решении системы линейных алгебраических уравнений (или доказательстве их непротиворечивости), построенных на основе условий семантической корректности дескрипторной алгебры, требует решения только одной системы уравнений, а использование СВ для системы СИ требует доказательства непротиворечивости девяти систем уравнений.

Таким образом, применение СД снижает дополнительные ресурсные потребности для экспертизы ПО ИУС примерно в 10 раз.

Заключение

В работе показаны проблемы экспертизы, основанной на оценке семантической корректности ПО ИУС, обусловленные значительной ресурсоемкостью. Предложен метод эффективного представления семантической информации, основанный на использовании сжимающего семантического отображения. Доказана возможность построения сжимающего отображения ограниченной области семантического пространства в упорядоченное множество семантических дескрипторов. Сформулированы необходимые условия изоморфизма. Исследованы свойства разработанного отображения. Показана возможность использования семантических дескрипторов для вычисления физической размерности результата. Исследованы свойства дескрипторного семантического пространства. Определена аксиоматика дескрипторной алгебры, использование которой позволяет снизить на порядок уровень вычислительной мощности, необходимой для формального доказательства семантической корректности ПО ИУС, как в режиме интерпретации кода, так и посредством применения алгебраических методов.

Дальнейшие исследования целесообразно выполнять в направлении исследования алгебраических методов восстановления семантической информации, а также возможности использования целочисленных семантических дескрипторов.

Литература

1. Харченко В.С., Манжос Ю.С., Петрик В.Л. Статистический анализ программного обеспечения системы управления космическим аппаратом и оценка проверяющей способности семантического контроля // Технология приборостроения. – 2002. – № 2. – С. 52-59.

2. Манжос Ю.С. Оценка эффективности независимой верификации программного обеспечения // Авиационно-космическая техника и технология. – 2004. – № 7. – С. 210-214.

3. Колмогоров А.Н., Фомин С.В. Элементы теории функций и функционального анализа: учебник для вузов. – М.: Наука, 1989. – 624 с.

4. Канторович Л.В., Акилов Г.П. Функциональный анализ. – М.: Наука, 1977. – 744 с.

5. Конорев Б.М., Петрик В.Л. Обоснование выбора системы физических единиц для формальной верификации программного обеспечения // Открытые информационные и компьютерные интегрированные технологии. – 2006. – № 33. – С. 116-120.

6. Яворский Б. М., Детлаф А. А. Справочник по физике. – М.: Наука, 1979. – 944 с.

Поступила в редакцию 25.04.2007

Рецензент: д-р техн. наук, проф. В.М. Вартанян, Национальный аэрокосмический университет им. Н.Е. Жуковского "ХАИ", Харьков.