

УДК 004.056

Программный модуль формирования нечетких эталонов в информационной безопасности методом количественного парного сравнения

Автор: С.Д.-О. Агакишиев, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев

Научный руководитель: М.В. Турти, к.т.н., доц., Национальный университет кораблестроения имени адмирала Макарова, г. Николаев

Введение. Информация – это один из самых ценных предметов в современной жизни. Доступ к ней с возникновением глобальных компьютерных сетей стал чрезвычайно простым. В то же время, легкость и скорость такого доступа значительно повысили и угрозу нарушения безопасности данных при отсутствии мер по их защите, а именно – угрозу несанкционированного доступа к информации.

Системы защиты информации являются сложными иерархическими системами, построение, функционирование и анализ эффективности которых предполагают многокритериальное оценивание различных средств в условиях наличия ресурсных ограничений при вероятностном характере влияющих факторов, многие из которых имеют нечеткий характер и подлежат обработке методами нечеткой логики.

Методы, основывающиеся на построении матриц попарных сравнений широко используются для принятия решения относительно выбора одного из альтернативных вариантов по совокупности критериев [1] (метод анализа иерархий), а также для определения функций принадлежности нечетких чисел (НЧ) при наличии условия, для всех точек x_i носителя нечеткого множества (НМ) X сумма функций принадлежности (ФП) равна единице

$$[2, 3]: \forall x_i \in X : \sum_{i=1}^N \mu(x_i) = 1.$$

Целью данной работы является разработка программного модуля формирования нечетких эталонов методом количественного парного сравнения для автоматизированной системы формирования и обработки нечетких эталонов (АСФОНЭ) [4].

Для достижения поставленной цели необходимо решить следующие задачи: проанализировать формы представления входной и выходной информации блока формирования методом количественного парного сравнения в АСФОНЭ, разработать алгоритмы определения ФП по методу количественного парного сравнения и соответствующий

программный модуль; сформулировать практические рекомендации по использованию разработанного модуля.

Основная часть. Метод количественного парного сравнения (МКПС) [2] исходит из того, что для нечеткого множества $\tilde{A}$ из n элементов вида

$$\tilde{A} = \{ \mu_{\tilde{A}}(x_1) / x_1, \mu_{\tilde{A}}(x_2) / x_2, \dots, \mu_{\tilde{A}}(x_n) / x_n \} \quad (1)$$

непрерывным условием для всех элементов множества A является равенство:

$$\sum_{i=1}^n \mu_{\tilde{A}}(x_i) = 1. \quad (2)$$

Степень уверенности эксперта в принадлежности значения x_i нечеткому множеству $\tilde{A}$ определяется с помощью парных сравнений. При этом количество вопросов к эксперту составляет $n(n-1)/2$. В результате опроса каждого эксперта формируется матрица парных сравнений:

$$A = \|a_{ij}\|, \quad (3)$$

где значение a_{ij} выбирается экспертом по шкале Саати [1] как оценка преимущества отнесения к терму элемента x_j по сравнению с x_i , по свойствам $\tilde{A}$.

Для обеспечения согласованности суждений экспертов допускается что $a_{ij} = 1/a_{ji}$. После формирования матрицы A необходимо найти собственный вектор матрицы $w = (w_1, \dots, w_n)$, путем решения уравнения $Aw = \lambda w$, где λ - собственное значение матрицы.

Вычисленные значения, которые составляют собственный вектор, используются как степень принадлежности элементов x множеству $\tilde{A}$:

$$\mu_{\tilde{A}}(x_i) = w_i, i = \overline{1, n}. \quad (4)$$

Если по определению всегда выполняется равенство $Aw = \lambda w$, то найденные значения тем точнее, чем более близко $\lambda_{\max}$ к n . Отклонение $\lambda_{\max}$ от n служит мерой согласованности суждений экспертов, решающих поставленную задачу, то есть используется как мера полезности (правильности) результата.

Для положительной квадратной матрицы $A = \{a_{ij}\}$ правый собственный вектор $y = (y_1, y_2, \dots, y_n)$, соответствующий максимальному собственному значению $\lambda_{\max}$, с точностью до постоянного множителя можно определить по формуле [1]

$$\lim_{k \rightarrow \infty} \frac{A^k e}{e^T A^k e} = c y, \quad (5)$$

где $e = \{1, 1, \dots, 1\}^T$ – единичный вектор;

k – показатель степени, $k = 1, 2, \dots$;

T – знак транспонирования;

c – константа.

Для определения собственного вектора матрицы $A = \{a_{ij}\}$ с заданной точностью ε матрицу $A = \{a_{ij}\}$ возводят в степень k и по формуле (5) рассчитывают y^k (k показывает здесь номер итерации и численно равен степени, в которую возведена матрица $A = \{a_{ij}\}$) и проверяют условие

$$e^T |y^{(k)} - y^{(k-1)}| \leq \varepsilon. \quad (6)$$

Достаточной из практических соображений может считаться [1] $\varepsilon = 0,01$. Максимальное собственное значение тогда может быть рассчитано по формуле

$$\lambda_{\max} = e^T A y^{(k_{\max})}, \quad (7)$$

где $k_{\max}$ – номер итерации, в результате которой получен вектор $y^{(k_{\max})}$, для которого выполняется условие (6).

Как следует из описания метода, определение весовых коэффициентов посредством нахождения вектора матрицы парных сравнений достаточно трудоемкая задача, к тому же в случае увеличения числа сравниваемых величин размерность формируемой матрицы возрастает, что существенным образом затрудняет нахождение ее собственного значения и, соответственно, решение поставленной задачи.

В разработанном программном модуле формирование матрицы парных сравнений осуществляется по следующим правилам

$$a_{ij} = \begin{cases} 1 & \text{при } i = j; \\ \frac{1}{a_{ji}} & \text{при } i \neq j \text{ и } i > j; \\ \frac{a_{ji}}{a_{ij}} & \text{при } i \neq j \text{ и } i < j, \end{cases} \quad (8)$$

Тогда матрица $A = \{a_{ij}\}$ является транзитивно согласованной и имеет вид

$$A = \left\{ \begin{array}{cccccc} 1 & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ \frac{1}{a_{12}} & 1 & \dots & a_{2j} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \frac{1}{a_{1j}} & \frac{1}{a_{2j}} & \dots & 1 & \dots & a_{jn} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \frac{1}{a_{1n}} & \frac{1}{a_{2n}} & \dots & \frac{1}{a_{jn}} & \dots & 1 \end{array} \right\} = \left\{ \begin{array}{cccccc} 1 & a_{12} & a_{13} & \dots & a_{1j} & \dots & a_{1n} \\ \frac{1}{a_{12}} & 1 & \frac{a_{13}}{a_{12}} & \dots & \frac{a_{1j}}{a_{12}} & \dots & \frac{a_{1n}}{a_{12}} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \frac{1}{a_{1j}} & \frac{a_{12}}{a_{1j}} & \frac{a_{13}}{a_{1j}} & \dots & 1 & \dots & \frac{a_{1n}}{a_{1j}} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \frac{1}{a_{1n}} & \frac{a_{12}}{a_{1n}} & \frac{a_{13}}{a_{1n}} & \dots & \frac{a_{1j}}{a_{1n}} & \dots & 1 \end{array} \right\}.$$

Задачей экспертов является введение элементов первой строки матрицы $A = \{a_{ij}\}$, которые усредняются в соответствии с весовыми коэффициентами экспертов.

Выводы. Как показал проведенный анализ, метод количественного парного сравнения является достаточно сложными для реализации, поскольку предполагают определение собственного вектора матрицы, определяемого при программной реализации итерационной процедурой.

Специфика ФП по теории ОНЛ позволяет описывать функции принадлежности отдельных термов координаты соответствующего числа-терма и его соседей слева и справа на универсуме. Для лингвистической переменной в целом достаточно задать координаты всех чисел термов (опорных точек) на универсуме и граничных точек. Методы КПС и КПСК в классическом варианте не гарантируют отсутствие зон толерантности в ФП, поэтому они непригодны для создания НЕ в соответствии с теорией ОНЛ.

Примененная для программной реализации модификация метода количественных попарных сравнений, состоящая в формировании матрицы попарных сравнений по определенным правилам позволяет получить ряд преимуществ по сравнению с методами КПС и КПСК:

- сокращается время работы эксперта, поскольку экспертом заполняется только первая строка матрицы попарных сравнений;
- сокращается объем вводимых данных, поскольку количество вопросов, на которые отвечает эксперт равно $n-1$ по сравнению с $\frac{n(n-2)}{2}$ для немодифицированного метода (при $n \rightarrow \infty$ количество вводимых данных сокращается в $\frac{n}{2}$ раза);
- матрица попарных сравнений является согласованной и не подлежит проверке на согласованность при помощи вспомогательных таблиц, которые необходимо хранить в памяти системы, т.е. экономится машинное время и ресурсы;
- процедура определения собственного вектора матрицы попарных сравнений

существенно упрощается и не является итерационной;

– процедуры определения ФП при формировании матрицы попарных сравнений по правилам (4.5) методом количественных попарных сравнений и методом попарных сравнений с извлечением квадратного корня совпадают, т.е. программной реализации подлежит один метод.

Недостатком примененной модификации метода попарных сравнений является отсутствие возможности оценивать квалификацию эксперта по согласованности заполненной им матрице попарных сравнений. Однако, при наличии группы экспертов, имеющих собственные весовые коэффициенты, данный недостаток нивелируется путем взвешивания элементов первых строк матриц попарных сравнений, полученных различными экспертами, и формирования интегральных взвешенных оценок каждого элемента, используемых в дальнейшем для расчета остальных элементов матрицы попарных сравнений.

Разработанная программа может работать в составе АСФОНЭ или использоваться как отдельный модуль для обработки нечетких эталонов, может встраиваться как модуль системы распознавания образов или системы принятия решений в информационной безопасности и других отраслях.

Программный модуль может использоваться также в учебном процессе на лабораторных и практических работах, проводимых при преподавании дисциплин, связанных с искусственным интеллектом (п.1.2 ПЗ)

Функции принадлежности, формируемые данным программным модулем, могут использоваться при моделировании процессов информационной борьбы и мониторинге атак.

Список литературы:

1. Катренко А.В. Системний аналіз об'єктів і процесів комп'ютеризації: Навчальний посібник.- Львів: «Новий світ-2000», 2003. – 424 с.

2. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: “МК-Пресс”, 2006. – 320 с.

3. Домарев В.В., Камлов Ю.О. Проблеми моделювання процесів інформаційної боротьби //Інформаційні технології та безпека. Збірник наукових праць. – Київ: Ін-т реєстрації інформації, 2003. – Вип.4. -С.40-56.

4. Мігунов В.О., Турти М.В. Розробка програмного засобу обробки нечітких еталонів //Матеріали II Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». – Миколаїв: НУК, 2012/ – С.142-147.

5. Турти М.В. Теорія однозначних нечітких систем та нейронні мережі: Монографія. Частина 1.- Миколаїв: Вид-во Європейський університет, Миколаївська філія, 2007. – 140 с.