Петербург, 2000. – 320 с.: ил. 3. Молдовян Н. А. Проблематика и методы криптографии. – СПб.: издательствр СпбГУ. – 1998.

УДК 004.56.021.2: 510.22 (043.2)

КЛАССИФИКАЦИЯ НЕЧЕТКИХ ЧИСЕЛ ДЛЯ РАЦИОНАЛЬНОГО ПРИМЕНЕНИЯ В МЕТОДАХ И МОДЕЛЯХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Александр Корченко, Виктория Рындюк, Евгения Пацира

Национальный авиационный университет

Аннотация: **Предлагается классификация нечетких чисел для использования их в системах защиты информации.**

Summary: **The paper suggests a classification of fuzzy numbers for their using in information protection systems.**

Ключевые слова: **Нечеткие множества, нечеткие числа.**

I Введение

В области информационной безопасности существует множество задач [1–3], решение которых основано на методах и моделях теории нечетких множеств [4, 5], где, в частности, осуществляется обработка различных типов нечетких чисел (НЧ). Например, нечеткая логика применяется для измерения потенциальных потерь при анализе степени риска [6], при разработке методов принятия решений и оценки уровня защищенности компьютерных систем [7] и др.

II Постановка задачи

Исследуя известные методы выполнения операций с НЧ [8–15], приходим к выводу, что существует множество различных подходов к выполнению нечетких арифметических операций (НАО), каждый из которых рассчитан на определенный класс НЧ. К примеру, матричный метод с выбором строки и столбца с максимальным элементом, описанный в [9], пригоден для дискретных унимодальных НЧ. Метод выполнения монотонных операций над НЧ [11] рассчитан на непрерывные выпуклые НЧ. В последнее время появилось несколько новых методов выполнения НАО, но авторы не всегда однозначно определяют, какие же НЧ наиболее целесообразно и допустимо использовать. Такое положение во многом связано с тем, что в отечественной и зарубежной литературе до сих пор нет наиболее полной классификации НЧ, которые используются при выполнении НАО и, как следствие, область применения указанных методов была недостаточно определена. Учитывая указанные недостатки, в данной работе предлагается классификация НЧ, которые наиболее часто используются при решении разного рода прикладных задач, основанных на выполнении НАО.

III Основная часть

Многолетний опыт работы авторов в этом направлении показал, что классификацию НЧ лучше всего осуществлять по следующим признакам: по нормальности, модальности, выпуклости, непрерывности и параметричности. Раскроем сущность указанных признаков.

По нормальности НЧ можно разделить на нормальные и субнормальные.

Нормальные. НЧ $\underset{\sim}{X}$ на действительной прямой называется нормальным, если $\exists \mu_{\underset{\sim}{X}}(x_i) = 1$, $(i = \overline{1, n})$ [8, 11, 16], т. е. верхняя граница значений его функции принадлежности (ФП) равна единице. Пример нормальных НЧ приведен на рис. 1.

Субнормальные. НЧ субнормально, если верхняя граница значений его ФП меньше единицы [11, 12, 15], т. е. $\max \mu_{\underset{\sim}{X}}(x) < 1$, где

$$\max \mu_{\underset{\sim}{X}}(x) = \bigvee_{i=1}^{n} \mu_{\underset{\sim}{X}}(x_i) < 1. \quad (1)$$

На рис. 1,а показан пример такого НЧ. Для приведения субнормального НЧ

$$\underset{\sim}{X}_{c} = \left\{\mu_{\underset{\sim}{X}_c}(x_1)/x_1,\ldots,\mu_{\underset{\sim}{X}_c}(x_n)/x_n\right\} = \bigcup_{i=1}^{n}\{\mu_{\underset{\sim}{X}_c}(x_i)/x_i\} \tag{2}$$

к нормальной форме $\underset{\sim}{X}_{н}$ используется следующее выражение [19]:

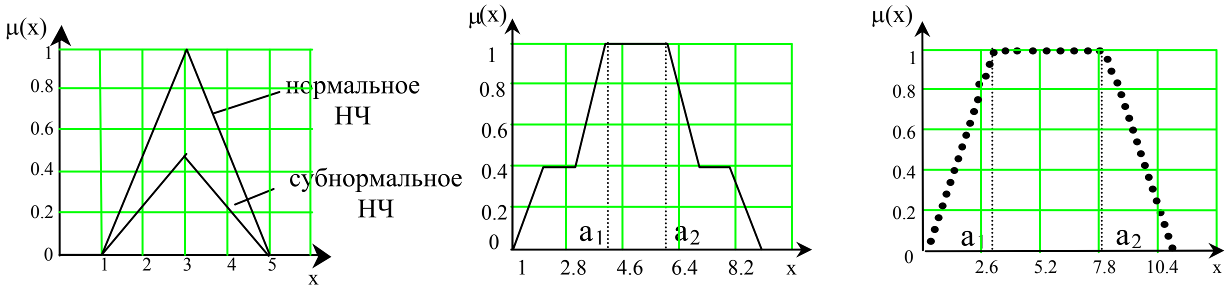
$$\underset{\sim}{X}_{н} = \bigcup_{i=1}^{n}\{(\mu_{\underset{\sim}{X}_c}(x_i) : \max \mu_{\underset{\sim}{X}_c}(x_i))/x_i\}\,. \tag{3}$$

Так, на рис. 1,а представлены НЧ до и после нормализации.

По модальности *НЧ можно разделить на унимодальные, толерантные и полимодальные.*

Унимодальные. НЧ унимодально, если оно имеет только один компонент, у которого ФП максимальна, например, равна единице, т. е. $\exists!\mu(z_M) = \bigvee_{k=1}^{n}\mu(z_k) = 1$, где n – количество компонент НЧ [8, 12]. Пример нормального унимодального НЧ приведен на рис. 1,а.

Толерантные. Толерантными называются НЧ, у которых модальные значения ФП принимают форму плато [17], и в этих случаях говорят о модальной зоне НЧ, которая в случае полной неопределенности, когда $\mu(x) \equiv \text{const}$, $\forall x \in \{x\}$, распространяется на всю шкалу $\{x\} \in \mathbf{R}$. На рис. 1,б и в модальная зона НЧ представлена интервалом $[a_1, a_2]$, причем a_1, a_2 называют еще границами интервала толерантности НЧ.



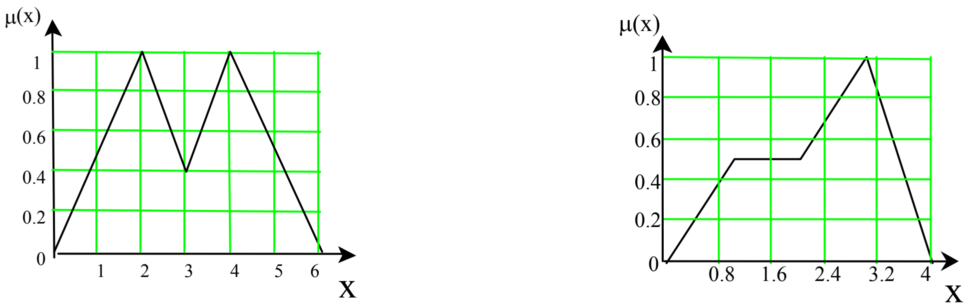
а) б) в)

Рисунок 1 – Примеры а – нормального и субнормального, б и в – толерантных НЧ

Полимодальные. НЧ $\underset{\sim}{Q}$ называется полимодальным, если существует конечное множество выпуклых нечетких подмножеств $\{\underset{\sim}{X}_i \mid i \in I\}$ с полунепрерывными сверху ФП, таких, что $\underset{\sim}{Q}$ есть объединение [18] унимодальных НЧ $\underset{\sim}{X}_i$ с одинаковыми модами в смысле выражения

$$\forall x\text{:}\ \mu_{\underset{\sim}{Q}}(x) = \mu_{\bigcup \underset{\sim}{X}_i}(x) = \bigcup_{i=1}^{n}\{\mu_{\underset{\sim}{X}_i}(x)\}\,. \tag{4}$$

Пример полимодального НЧ представлен на рис. 2,а.



а) б)

Рисунок 2 – Примеры а – полимодального и б – унимодального НЧ

По выпуклости НЧ разделим на выпуклые и невыпуклые.

Выпуклые. НЧ $\underset{\sim}{X}$ называют выпуклым, если для его произвольных точек u, y, z $\in$R при условии $u \le y \le z$ соблюдается неравенство [11, 16] $\mu_{\underset{\sim}{X}}(y) \ge \min(\mu_{\underset{\sim}{X}}(u),\ \mu_{\underset{\sim}{X}}(z))$. Примеры выпуклых НЧ приведены на рис. 1 и 2,б.

Невыпуклые. НЧ называют невыпуклым, если оно не удовлетворяет вышеописанному свойству выпуклости. Пример невыпуклого полимодального НЧ можно увидеть на рис. 2,а.

По непрерывности **НЧ делят на дискретные и непрерывные.**

Дискретные. Если множество X области определения НЧ $\underset{\sim}{X}_i$, где X $\in$ **R**, конечно или счетно, то НЧ $\underset{\sim}{X}_i$ называются дискретными [8, 15].

Непрерывные. Непрерывное НЧ – это переменная, которая принимает все числовые значения, т. е. все значения, заключенные между некоторыми границами [20]. В [15] она определена как $|X| = |R|$, где X – множество области определения НЧ. Примеры дискретных и непрерывных НЧ приведены соответственно на рис. 1,в и рис. 1,а, б, 2.

По параметричности **НЧ разделяют на параметрические и непараметрические.**

Параметрические. Параметрическим (или числом L-R типа) называют НЧ, которое описывается несколькими параметрами $a < b_1 \le b_2 < c$, являющимися его границами, и двумя функциями, определяющими форму его ФП [16, 19]. ФП такого НЧ выражается следующей формулой:

$$\mu_X(x) = \begin{cases} L\left(\dfrac{b_1 - x}{b_1 - a}\right), & x \in [a, b_1]; \\ 1, & x \in [b_1, b_2]; \\ R\left(\dfrac{x - b_2}{c - b_2}\right), & x \in [b_2, c], \end{cases} \tag{5}$$

где L(x), R(x) – функции (невозрастающие на множестве неотрицательных действительных чисел), удовлетворяющие свойствам: L(–x) = L(x), R(–x)= R(x), L(0) = R(0) = 1. На рис. 3 представлены основные виды параметрических НЧ, приведенных в [16].

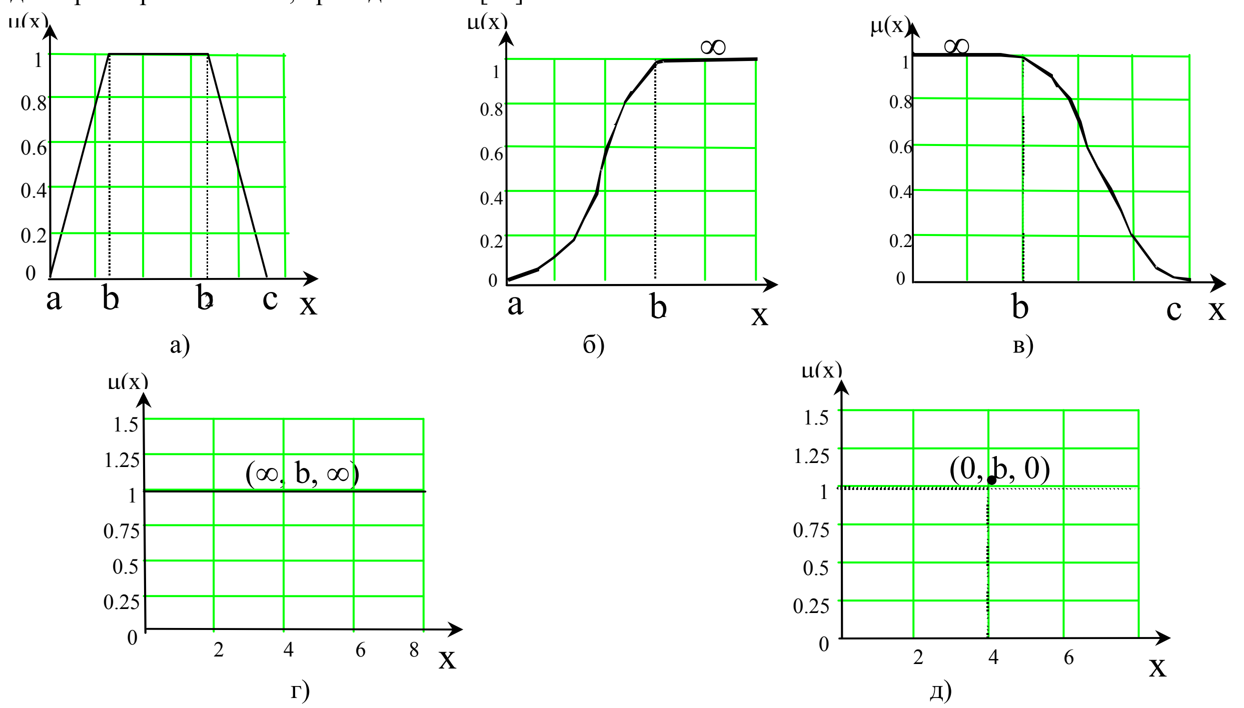


Рисунок 3 – Основные виды параметрических НЧ

Так, на рис. 3а, б, в, г и д НЧ $\underset{\sim}{X}_1$, $\underset{\sim}{X}_2$, $\underset{\sim}{X}_3$, $\underset{\sim}{X}_4$, $\underset{\sim}{X}_5$ определяются соответственно параметрами (a, b_1, b_2, c), (a, b_1, ∞), где b_2=c=∞, (∞, b_2, c) , где a, b_1=∞, (∞, b, ∞), где $\mu_X(x) = \mathrm{const}\ \forall x \in R$, и (0, b, 0), где b_1=b_2=b, a=c=0, или что эквивалентно записи $\underset{\sim}{X}_1$= (a, b_1, b_2, c)$_{LR}$, $\underset{\sim}{X}_2$= (a, b_1, ∞)$_{LR}$, $\underset{\sim}{X}_3$= (∞, b_2, c)$_{LR}$, $\underset{\sim}{X}_4$ = (∞, b, ∞)$_{LR}$ и $\underset{\sim}{X}_5$ = (0, b, 0)$_{LR}$ соответственно. Параметрическое НЧ также представлено на рис. 1,а (нормальное НЧ).

Непараметрические. НЧ, не соответствующие описанию параметрических чисел, называются непараметрическими. Такие числа показаны на рис. 1,а (субнормальное НЧ), 1,б и в, 2. Т. о., пользуясь приведенной классификацией, представленное на рис. 2,б НЧ можно определить как нормальное унимодальное выпуклое непрерывное непараметрическое, а, например, НЧ, обработка которых описана в работе [1] – как нормальные выпуклые унимодальные дискретные непараметрические .

IV Выводы

Итак, согласно данной классификации, НЧ, используемые в теории и практике нечетких множеств, можно разделить на определенные группы. Такое разделение позволяет однозначно и наиболее полно учитывать особенности НЧ (которые могут формироваться различными методами) для рационального выбора методов последующей их обработки [21] при решении задач в области защиты информации.

Литература: 1. Корченко А. Г., Черныш Л. Г. Организация моделей систем оценки уровня защищенности с использованием нечетких множеств // Моделювання та інформаційні технології: Зб. наук. пр. ІПМЕ НАН України. Випуск 1. – Львів: Вид-во “Світ“. – 1999. – С. 66 – 73. 2. Корченко А. Г., Черныш Л. Г. Оценка безопасности компьютерных систем на базе методов и моделей нечетких множеств // Защита информации: Сб. науч. тр. – К: КМУГА. – 1998. – С. 14–18. 3. Корченко А. Г., Щербина В. П., Черныш Л. Г. Логико-лингвистический подход в задачах оценки уровня безопасности информации в компьютерных системах // Збірник наукових праць ІПМЕ НАН України. Випуск 10. – Львів: НВМ ПТ УАД.– 2000.– С. 41–46. 4. Заде Л. А. Понятие лингвистической переменной и его применение к принятию приближенных решений. – М.: Мир, 1976. – 166 с. 5. Кофман А. Введение в теорию нечетких множеств. – М.: Радио и связь, 1982. – 432 с. 6. Стенг Д., Мун С. Секреты безопасности сетей. – К.: Диалектика, 1995. – 544 с. 7. Герасименко В. А., Малюк А. А. Основы защиты информации. – М.: МИФИ (МГТУ), 1997. – 537 с. 8. А. Н. Борисов, А. В. Алексеев, Г. В. Меркурьева и др. Обработка нечеткой информации в системах принятия решений. – М.: Радио и связь, 1989. – 304 с. 9. Минаев Ю. Н. К вопросу анализа и выбора показателей надежности программного обеспечения вычислительных систем. / Кибернетика и системный анализ, 1992, № 2. – С. 46–60. 10. Алтунин А. Е., Семухин М. В. Модели и алгоритмы принятия решений в нечетких условиях: Монография. Тюмень: Издательство Тюменского государственного университета, 2000. 352 с. 11. Борисов А. Н., Крумберг О. А., Федоров И. П. Принятие решений на основе нечетких моделей. Примеры использования. Рига: Зинатне, 1990 г. 12. Корченко А. Г. Методы и аппаратные средства реализации нечетких операций // Автоматизированные системы обработки информации: Сб. науч. трудов. – К.: КМУГА, 1996. – С. 17–25. 13. Корченко А. Г. Нечеткие арифметические операции с линейной аппроксимацией по локальным максимумам // Зб. наук. пр. ІПМЕ НАН України. Випуск 4. – Львів: Вид-во “Світ“ при Львівському університеті, 1998. – С. 3–6. 14. Ротштейн А. П., Штовба С. Д. Нечеткая надежность алгоритмических процессов. – Винница: Континент – ПРИМ, 1997. – 142 с. 15. Модели принятия решений на основе лингвистической переменной. / А. Н. Борисов, А. В. Алексеев, О. А. Крумберг и др. – Рига: Зинатне, 1982. – 256 с. 16. Нечеткие множества в моделях управления и искусственного интеллекта / Под ред. Д. А. Поспелова. – М.: Наука. Гл. ред. Физ.-мат. лит., 1986. – 312 с. 17. Шошин П. Б. Размытые числа как средство описания субъективных величин // Статистические методы анализа экспертных оценок. – М.: Наука, 1977. – с. 234–250. 18. Дюбуа Д., Прад А. Теория возможностей. Приложения к представлению знаний в информатике: Пер. с фр. – М.: Радио и связь, 1990. – 228 с. 19. Корнеев В. В., Гареев А. Ф., Васютин С. В., Райх В. В. Базы данных. Интеллектуальная обработка информации. – М.: Издатель Молгачева С. В., Издательство Нолидж, 2001. – 496 с. 20. Картавов С. А. Математические термины: Справ.-библиогр. Словарь. – К.: Выща шк. Головное изд-во, 1988 – 295 с. 21. Корченко А. Г., Рындюк В. А., Пацира Е. В. Анализ методов выполнения нечетких операций для использования в системах защиты информации // Матеріали IV Міжнародн. науково-технічної конф. “АВІА-2002”. – Том 1. – К.: НАУ, 2002.