УДК 519.87

Івохін Є.В., д.ф.-м.н, доцент

Про нечітке представлення дійсних чисел у формі триплетів

Київський національний університет імені Тараса Шевченка, м.Київ, пр-т Глушкова, 4д, e-mail: ivohin@univ.kiev.ua

Ivohin E.V., Dr.Sci.

About fuzzy real numbers presentation in triplet form

Taras Shevchenko National University of Kyiv, Kyiv, Glushkova st., 4d, e-mail: ivohin@univ.kiev.ua

В роботі розглянуто алгоритмічний підхід до побудови трикутного представлення нечітких дійсних чисел, що базується на використанні двійкового запису числа за стандартом IEEE754. Розрахунок діапазону представлення та визначення кількості проміжних значень здійснюється на основі обчислення двох простих чисел, найближчих до записаної як ціле число мантиси. У якості прикладу пропонується застосування даного підходу для модифікації базового алгоритму шифрування Меркла-Хелмана, що використовує схему задачі про рюкзак .

Ключові слова: нечітке число, триплет, прості числа, алгоритм шифрування.

The formalization of uncertainty or inaccuracy in the technical processes associated with the use of 'approximate' submission process parameters, which can be carried out using fuzzy representation of real numbers in triplet form. This paper considers an algorithmic approach for constructing triangular fuzzy representation of real numbers, based on the use of binary records by standard IEEE754. Mantissa and characteristics are determined from binary record of a real number. The calculation of the range of fuzzy representation and the determination of intermediate values number is based on calculation of two simple numbers which are closest to recorded as an integer mantissa. The some computational examples are given. This method can be used in the case of absence decision maker subjective representation of fuzziness. As an application example of this approach is proposed the modification of the basic algorithm Merkle-Hellman encryption, which uses a model problem of the knapsack.

Key words: fuzzy numbers, triplets, simple numbers, encryption algorithm.

Статтю представив д.т.н., проф. Волошин О.Ф.

Вступ. При проведенні різних досліджень за умов невизначеності або неточності параметрів важливим завданням є коректно формалізувати процеси, що відбуваються в об'єкті дослідження. Часто формалізація пов’язана з використанням "наближеного" подання параметрів процесів, яке можна провести, наприклад, за допомогою нечіткого представлення довільних чисел.

Проблема представлення нечіткого числа $\widetilde{b}$ у вигляді множини пар

$$\widetilde{b} = \{(b_i, \mu(b_i)) \mid b_i \in [a,c], i \in I, a \le b \le c, \mu(b_i) \in [0,1], i \in I, \mu(b) = 1\}, \quad (1)$$

де $\mu : R \to [0,1]$ - відображення, яке визначає міру належності елемента $x \in R$ нечіткій множині $\widetilde{b}$, передбачає вирішення двох складних задач: визначення діапазону представлення $[a,c]$ нечіткого числа та задання значень функції належності для проміжних величин $b_i \in [a,c], i \in I$. Як правило, вирішення цих задач залежить від суб’єктивних факторів, що може впливати на результати задач дослідження.

В роботі [1] запропоновано застосування спеціальних множин простих чисел для визначення міри належності традиційних нечітких множин. В рамках підходу розглянуто ефективні обчислювальні схеми, які дозволяють отримувати значення функцій належності для елементів нечітких множин, що застосовуються для опису невизначеності параметрів процесу. Основна ідея, що базується на використанні простих чисел, знайшла своє продовження у роботі [2], в якій запропоновано формалізацію нечітких цілих чисел у вигляді (1). Розроблений підхід включає в себе методику обчислення діапазону представлення нечіткого трикутного числа $[a,c]$ та спосіб розрахунку мір належності проміжних значень на основі лінійних функцій

$$\mu_{\tilde{b}}(x) = \frac{x-a}{b-a}, x \in [a,b];$$
$$\mu_{\tilde{b}}(x) = \frac{c-x}{c-b}, x \in [b,c]; \quad (2)$$
$$\mu_{\tilde{b}}(x) = 0, x \notin [a,c].$$

Це дозволило зробити непотрібним суб'єктивне представлення діапазону $[a,c]$ і визначати нові нечіткі поняття, що базуються на використанні цілих чисел.

Однак застосування лише цілих чисел суттєво обмежує сферу використання нечітких величин, обробка яких потрібна в реальних задачах.

В даній роботі пропонується підхід для подання нечітких дійсних чисел, який можна використати при комп'ютерному моделюванні різних процесів з урахуванням нечіткості вхідних даних.

Основний результат. Класичне поняття нечіткої множини (підмножини) заданої універсальної множини X у відповідності до Заде [3] формулюється наступним чином.

Означення 1. [3] Нечіткою множиною $\widetilde{A}$ універсальної множини X, називають сукупність пар $\widetilde{A}=\{(\mu_{\widetilde{A}}(x),x)\}$, де $\mu_{\widetilde{A}}(x): X\to[0,1]$ – відображення множини X в одиничний відрізок [0,1], яке називається функцією належності нечіткій множині.

Інтерпретацією ступеня належності $\mu_{\widetilde{A}}(x)$ є суб'єктивна міра відповідності елемента $x\in X$ поняттю, сенс якого формалізується нечіткою множиною $\widetilde{A}$.

Визначимо в якості універсальної множини X простір над полем дійсних чисел R, т.е. $X=R$. У цьому випадку розглядаються нечіткі величини, а при розв'язанні прикладних задач для формалізації нечіткості використовують інші означення нечітких величин, що еквівалентні класичному означенню 1.

Означення 2. [4] Нечітким трикутним числом $\widetilde{b}$ називають впорядковану трійку чисел *(a, b, c)*, $a\le b\le c$, для якої функція належності $\mu_{\widetilde{b}}(x)$ має вигляд (2).

Нечітке трикутне число $\widetilde{b}$, задане у вигляді трійки *(a, b, c)*, іноді називають триплетом, при чому, для довільного числа $x\in[a,b]$ справедливе представлення $x=a+\lambda(b-a),$ а для довільного $x\in[b,c]$ - $x=c-\lambda(c-b),$ де $0\le\lambda\le1$ - заданий рівень міри належності числа x нечіткій множині $\widetilde{b}$. Нечітке трикутне число виду *(a, b, b)*, яке називається лівим нечітким трикутним числом, визначається функцією належності

$$\mu_{\widetilde{b}}(x)=0, x<a;\ \ \mu_{\widetilde{b}}(x)=\frac{x-a}{b-a}, x\in[a,b];$$
$$\mu_{\widetilde{b}}(x)=1, x>b, \qquad (3)$$

а нечітке трикутне число виду *(b, b, c)*, яке називається правим нечітким трикутним числом, - функцією належності

$$\mu_{\widetilde{b}}(x)=1, x<b;\ \ \mu_{\widetilde{b}}(x)=\frac{c-x}{c-b}, x\in[b,c];$$
$$\mu_{\widetilde{b}}(x)=0, x>c. \qquad (4)$$

Використаємо прості числа для комп'ютерного моделювання нечітких дійсних чисел, базуючись на представленні довільних дійсних чисел у форматі IEEE 754 [5].

Припустимо, що для подання дійсних чисел використовуються n-байтні двійкові представлення. Це означає, що будь-яке дійсне число $x\in R$ може бути подане у двійковому вигляді

$$x=\left[\underset{1\,bit}{s}\,|\,\underset{p\,bit}{characteristic}\,|\,\underset{q\,bit}{mantissa}\right], \qquad (5)$$

де $s=\begin{cases}0, x\ge0\\1, x<0\end{cases}$ - знак числа x, $characteristic=k+BIAS$ - зміщений порядок, k - порядок числа x за основою 2 (степінь, до якої необхідно піднести число 2, щоб виконувалась умова $m=|x|*2^k\in[1,2)$), $BIAS>0$ - деяка константа, величина якої обчислюється за формулою $BIAS=2^{p-1}-1$ [5], $mantissa=m-1$ - мантиса числа x без уявної одиниці, p та q - відповідно кількості розрядів для представлення характеристики та мантиси числа x, $(p+q+1)/8=n$.

Зауважимо, що у представленні (5) характеристика та мантиса визначаються полями двійкових цифр, які є записами деяких цілих чисел. Використаємо поняття нечіткого цілого числа для знаходження діапазону представлення нечіткого трикутного дійсного числа.

Означення 3. Нечітким цілим числом $\widetilde{v}$ будемо називати впорядковану трійку чисел *(u, v, w)*, $u\le v\le w$, $u,v,w\in Z$, де

$$u=\begin{cases}P_{-1}(v), v\ge0,\\-P_1(-v), v<0,\end{cases}\quad w=\begin{cases}P_1(v), v\ge0,\\-P_{-1}(-v), v<0,\end{cases} \qquad (6)$$

а $P_1(\cdot), P_{-1}(\cdot)$ - наступне та попереднє прості числа відносно v, $v\ge0$, та $-v$, $v<0$.

Іншими словами, довільне нечітке ціле число $\widetilde{v}$ може бути представлене у вигляді триплету, ліве (u) та праве (w) значення якого подаються найближчими простими числами.

Розглянемо довільне дійсне число b. Припустимо, що мантиса числа b дорівнює m, порядок числа за основою 2 рівний k. Представимо нечітке дійсне число $\widetilde{b}$ у вигляді трійки *(a, b, c)*, де діапазон представлення $[a,c]$

визначається за допомогою дійсних чисел a та c, які можна отримані, виходячи з формату (5). Для цього визначимо нечітке ціле число $\tilde{m}$ у вигляді впорядкованої трійки цілих чисел (m_a, m, m_c), де m_a та m_c обчислюються за формулами (6). Розглядаючи далі величини m_a та m_c як мантиси деяких дійсних чисел заданого порядку k за основою 2 обчислимо два числа a та c, що визначатимуть діапазон представлення $[a,c]$.

Значення m_a та m_c дозволяють також визначити кількість проміжних чисел $b_i \in [a,c]$, $i \in I$, що використовуються для формалізації нечіткого дійсного числа $\tilde{b}$. Множина індексів у цьому випадку задається діапазоном $I = \overline{0, m_c - m_a}$, а величини мір належності проміжних значень визначаються на основі лінійних функцій (2).

Таким чином, двійкове представлення чисел у форматі (5) дозволяє досить конструктивно визначати нечіткі дійсні числа. Однак, є випадок, що потребує більш детальної уваги. Якщо число b є степенем числа 2 зі знаком плюс або мінус, то мантиса у представленні (5) для такого числа дорівнює 0. У цьому випадку нечітке представлення дійсного числа у вигляді трійки чисел *(a, b, c)* може бути записане як ліве нечітке трикутне число (a,b,b) для від'ємного b, або як праве нечітке трикутне число (b,b,c) для додатного b.

При цьому необхідно звернути увагу на одну важливу деталь. Відомо, що обчислення простих чисел з великими номерами відносно довільного $z \geq 0$ є досить ресурсоємким процесом. В той же час, знаходження найближчих простих чисел $P_1(z)$ та $P_{-1}(z)$ для довільного $z \geq 0$ відбувається дуже швидко і не вимагає суттєвих обчислювальних витрат.

Для демонстрації методики представлення нечітких дійсних чисел у вигляді трійок $\tilde{b} = \{(a,b,c)\}$ з лінійною функцією належності (2) розглянемо два дійсних числа 10567.18 та -0.63147. У цьому випадку з точністю 10 знаків після коми маємо відповідно:

$$\tilde{10567.18} = (10567.1748046875, 10567.18, 10567.2138671875),\ m = 2432184,$$
$$m_a = 2432179,\ m_c = 2432219;$$

$$\tilde{-0.63147} = (-0.6314701438, -0.63147, -0.6314679980),\ m = 2205701,$$
$$m_a = 2205667,\ m_c = 2205703.$$

В якості практичного застосування введеного представлення нечіткого дійсного числа можна навести різні приклади. Серед них, однак, особливо хотілося б відзначити один, в якому безпосередньо використовується нечітке подання довільного числа.

Розглянемо алгоритм для узагальненого шифрування з відкритим та закритим ключами на основі алгоритму рюкзака, розроблений Ральфом Мерклом та Мартином Хелманом [6]. Основна ідея даного алгоритму полягає у створенні закритого ключа, який є перетвореною послідовністю ваг задачі про рюкзак спеціального вигляду, побудові на його основі відкритого ключа $K = \{r_j, j = \overline{1,n}\}$ та проведенні процесу шифрування довільної вхідної інформації. Не заглиблюючись у подробиці, відмітимо, що перетворення закритого ключа у відкритий проводиться за допомогою двох взаємно простих чисел M та N та нескладних математичних операцій з ними. В якості суттєвого покращення криптостійкості базового алгоритму Меркла-Хелмана є модифікація, у якій відкритий ключ доповнюєтьсяи двома довільними цілими значеннями k та l, $k \leq l$, $k = 0,1,2,...$, $l = 1,2,3,...$, за якими з послідовності простих чисел визначаються величини $s = P_k(z)$, $t = P_l(z)$ для деякого числа $z \geq 0$. За допомогою значень s та t можна змінити ваги відкритого ключа та величини N та M, наприклад, за наступною схемою:

- для чисел M та N, які є взаємно простими числами, обчислюються числа $P_s(M)$ та $P_t(N)$ відповідно, де $s = P_k(z)$, $t = P_l(z)$;

- для цілих чисел $r_j \in K, j = \overline{1,n}$, які входять до ключа K, обчислюються величини $u_j = P_s(r_j) - r_j$ та $v_j = P_t(r_j)$, $j = \overline{1,n}$, $s = P_k(z)$, $t = P_l(z)$;

- формується вектор пар елементів $\overline{K} = \{(u_1, v_1), ..., (u_n, v_n)\}$, який буде новим значенням відкритого ключа *K.* Величини $P_s(M)$, $P_t(N)$ та вектор $\overline{K}$ передаються отримувачу повідомлення разом з зашифрованим за допомогою елементів v_j, $j = \overline{1,n}$, повідомленням.

Як вже було сказано вище, обчислення простих чисел, суттєво віддалених від заданого $z \geq 0$, вимагає певного часу, що сповільнює процеси шифрування та розшифрування

повідомлень. Наведений у статті спосіб нечіткого представлення дійсних чисел у формі триплетів дозволяє спростити схему модифікації алгоритму Меркла-Хелмана без зміни рівня його захищеності.

Припустимо, що задано довільне число $z \geq 0$. Використовуючи його нечітке подання можна отримати три цілих числа – два взаємно простих $P_1(x)$ та $P_{-1}(x)$, де x - зміщений порядок у двійковому представленні числа z, та число m, яке є мантисою числа z.

Використовуючи в якості чисел N та M відповідно $P_1(x)$ та $P_{-1}(x)$, можна записати схему модифікації у наступному вигляді:

- з допомогою чисел $M = P_{-1}(x)$ та $N = P_1(x)$, які є взаємно простими числами, обчислюються значення елементів відкритого ключа $r_j \in K, j = \overline{1,n}$;

- отримані значення збільшуються на m: обчислюються величини $u_j = r_j + m$, $j = \overline{1,n}$;

- формується вектор значень елементів $\overline{K} = \{u_1, ..., u_n\}$, який буде новим значенням відкритого ключа *K*.

При цьому для параметризації цього алгоритму шифрування необхідно визначення лише початкового числа $z \geq 0$. Його двійкове представлення дозволяє отримати числа N, M та m для створення/модифікації відкритого ключа і проведення шифрування/розшифрування вхідних повідомлень.

Висновки. Запропонований підхід дає можливість моделювати нечітке подання довільного числа, не визначаючи діапазону представлення. Дане нечітке представлення враховує точність і величину дійсного числа, з урахуванням чого формується множина проміжних значень, що використовуються для формалізації нечіткого дійсного числа. Чисельні експерименти дозволяють говорити про конструктивність і ефективність розглянутого алгоритму.

На завершення варто зазначити, що у випадках, коли діапазон на основі представлення не задовольняє дослідника, можна використати суб'єктивне визначення трикутного вигляду нечіткого дійсного числа.

Список використаних джерел

1. *Івохін Є.В.* Про застосування спеціальних множин простих чисел для визначення міри належності нечітких множин/ Є.В.Івохін// Журнал обчислювальної та прикл. математики. – 2013. – №4. – С.11-18.
2. *Івохін Є.В.* Про застосування простих чисел для визначення міри належності нечітких цілих чисел/ Є.В.Івохін // Журнал обчислювальної та прикл. математики. – 2014. – №1. – С.1-8.
3. *Zadeh L. A.* Fuzzy sets // Inf. Contr. – 1965. – 8. – P. 338-353.
4. *Bablu Jana, Tapan Kumar Roy.* Multi-Objective Fuzzy Linear Programming and Its Application in Transportation Model/ Bablu Jana, Tapan Kumar Roy.// Tamsui Oxford Journal of Mathematical Sciences. – 2005. – 21(2). – P.243-268.
5. Стандарт *IEEE 754* представлення чисел з плаваючою крапкою [Електронний ресурс]. Режим доступу: http://www.h-schmidt.net/FloatConverter/IEEE754.html
6. *Merkle R.* Hiding information and signatures in trapdoor knapsacks/ R.Merkle, M. Hellman //IEEE Trans. Inform. Theory. – 1978. – 24(5). – P.525-530.

References

1. IVOHIN E. (2013) *On the application of specific sets of simple numbers to determine the membership measure of fuzzy sets*. Journ.Comp.&Appl.Math. 4. p.11-18.
2. IVOHIN E. (2014) *On the application of simple numbers to determine the membership measure of fuzzy integers*. Journ.Comp.&Appl.Math. 1. p.31-38.
3. ZADEH L. (1965) *Fuzzy sets*. Inf. Contr. 8. p. 338-353.
4. BABLU J. AND TAPAN K. R. (2005) *Multi-Objective Fuzzy Linear Programming and Its Application in Transportation Model.* Tamsui Oxford Journal of Mathematical Sciences. 21(2). p.243-268.
5. IEEE 754 of floating point representation [Online]. Available from: http://www.h-schmidt.net/FloatConverter/IEEE754.html
6. MERKLE R., HELLMAN M. (1978). *Hiding information and signatures in trapdoor knapsacks.* IEEE Trans. Information Theory. 24(5). p.525-530.

Надійшла до редколегії 15.05.2014