

Linear Fuzzy Integers and Bezout's Identity

Frank Rogers

Department of Mathematics, University of West Alabama Livingston
Alabama 35470, USA
Email: [fr Rogers \[AT\] uwa.edu](mailto:fr Rogers [AT] uwa.edu)

ABSTRACT---- *Fuzzy arithmetic is a powerful tool to solve engineering problems with uncertain parameters. In doing so, the uncertain parameters in the model equations are expressed by fuzzy numbers, and the problem is solved by using fuzzy arithmetic to carry out the mathematical operations in a generalized form. Diophantine equations have played an important role in many applications of optimization and decision making problems. This work considers the solution of Diophantine equations and Bezout's Identity with Linear Fuzzy Integer coefficients. Overestimation is also addressed.*

Keywords--- Linear fuzzy real number, Liner fuzzy integers, Diophantine Equations, Number Theory

1 INTRODUCTION

Computing, finance, and rocket science are only a few areas that rely heavily on mathematical computations. With these computations several types of errors may occur. Uncertainty, rounding, and approximation errors are only a few. Scientists have used interval arithmetic and fuzzy set theory to deal with these errors. Diophantine equations are used in factorization strategies in the RSA algorithm, optimization and control design to name only a few applications. In this paper we will present a set of numbers that has both properties of real numbers and of interval numbers. The hybrid set of numbers are denoted as Linear Fuzzy Real numbers (LFR). Then we will briefly present the set of Linear Fuzzy Integers (LFZ). This set is a subset of LFR. The properties of LFZ will allow us to solve a fuzzy unit Diophantine equation using the Euclidean Algorithm.

Fuzzy sets were initially introduced by Bellman and Zadeh [1]. This concept was then adopted to mathematical programming by Tanaka *et al.* [10]. Fuzzy linear programming problem with fuzzy coefficients was formulated by Negoita [6]. Zimmerman [11] presented a fuzzy approach to multi-objective linear programming problems. Dubois and Prade [2] studied linear fuzzy constraints. Tankaka and Asai [9] proposed a formulation of fuzzy linear programming with fuzzy constraints and gave a method for its solution. Neggers and Kim researched fuzzy posets [4] and created Linear Fuzzy Real numbers [5]. Linear Fuzzy Real numbers were used by Monk [3] and Prevo [7] in the study of fuzzy random variables. Linear Fuzzy Real numbers were also used to optimize the primal problems of linear programs with fuzzy constraints[8].

The set of LFR is a set that shows true intermediate properties which are unique to the set and not to those of either the real numbers or the "general" fuzzy numbers. Because of the unique properties of LFR and thus LFZ, we can solve Fuzzy Diophantine equations using the Euclidean Algorithm. The paper is outlined as follows. Operations on LFR are considered in Section 2. In Section 3, an introduction of the LFZ, a method of solution to a Diophantine Equation and examples. In Section 4, applications and future research are considered.

2 LINEAR FUZZY REAL NUMBERS

Considering the real numbers R , one way to associate a fuzzy number with a fuzzy subset of real numbers is as a function $\mu : R \rightarrow [0,1]$, where the value $\mu(x)$ is to represent a degree of belonging to the subset of R . The Linear Fuzzy Real numbers as described by Neggers and Kim [5, 3] is a triple of real numbers (a,b,c) where $a \leq b \leq c$ of real numbers, See Fig. 1, such that:

1. $\mu(x) = 1$ if $x = b$;
2. $\mu(x) = 0$ if $x \leq a$ or $x \geq c$;
3. $\mu(x) = (x - a)/(b - a)$ if $a < x < b$;
4. $\mu(x) = (c - x)/(c - b)$ if $b < x < c$.

For a real number c , we let $\epsilon(c) = \mu$ with associated triple (c, c, c) . Then μ is a linear fuzzy real number with $\mu(c) = 1$ and $\mu(x) = 0$ otherwise. As a linear fuzzy real number we consider $\epsilon(c) = \mu$ to represent the real number c itself. Thus by this interpretation we note that the set R of all real numbers is a subset of the set containing the linear fuzzy real numbers. The set of the linear fuzzy real numbers is a hybrid set showing intermediate properties,

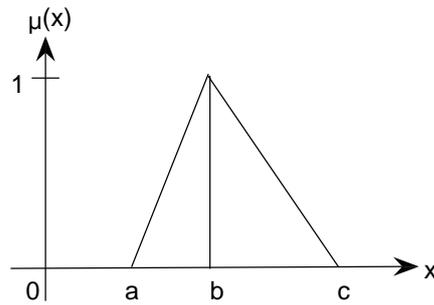


Fig. 1. Linear Fuzzy Real number $\mu(a, b, c)$

which are unique to the set and not those of either the real numbers or the “general” fuzzy numbers.

Let $LFR = \{\mu : R \rightarrow [0, 1] \mid \mu \text{ is a linear fuzzy real number}\}$. Each μ has a set of descriptive parameters. The base is defined as the triple (a, b, c) that occurs in the definition of a linear fuzzy real number. Thus one may write an element of LFR as $\mu = \mu(a, b, c)$.

2.1 Addition and Subtraction

Given the linear fuzzy real numbers $\mu_1 = \mu(a_1, b_1, c_1)$ and $\mu_2 = \mu(a_2, b_2, c_2)$,

$\mu_1 + \mu_2$ is defined by

$$\mu_1 + \mu_2 = \mu(a_1 + a_2, b_1 + b_2, c_1 + c_2).$$

This operation is not the usual definition of addition of functions. It is also clear that $\mu + \epsilon(0) = \mu$ for all $\mu \in LFR$. For subtraction, we have

$$\mu_1 - \mu_2 = \mu(a_1 - c_2, b_1 - b_2, c_1 - a_2).$$

2.2 Law of trichotomy

A linear fuzzy real number $\mu(a, b, c)$ is defined to be positive if $a > 0$, negative if $c < 0$, and zeroic if $a \leq 0$ and $c \geq 0$. The following properties also hold:

1. If μ is positive, then $-\mu$ is negative;
2. If μ is negative, then $-\mu$ is positive;
3. If μ is zeroic, then $-\mu$ is also zeroic;
4. If μ_1 and μ_2 are positive, then so is $\mu_1 + \mu_2$;
5. If μ_1 and μ_2 are negative, then so is $\mu_1 + \mu_2$;
6. If μ_1 and μ_2 are zeroic, then so is $\mu_1 + \mu_2$;
7. For any μ , $\mu - \mu$ is zeroic.

2.3 Multiplication and Division

Given the linear fuzzy real numbers $\mu_1 = \mu(a_1, b_1, c_1)$ and $\mu_2 = \mu(a_2, b_2, c_2)$,

$\mu_1 \cdot \mu_2$ is defined by

$$\mu_1 \cdot \mu_2 = \mu(\min\{a_1 a_2, a_1 c_2, a_2 c_1, c_1 c_2\}, b_1 b_2, \max\{a_1 a_2, a_1 c_2, a_2 c_1, c_1 c_2\}).$$

Given the linear fuzzy real numbers $\mu_1 = \mu(a_1, b_1, c_1)$ and $\mu_2 = \mu(a_2, b_2, c_2)$, $\frac{\mu_1}{\mu_2}$ is defined by

$$\frac{\mu_1}{\mu_2} = \mu_1 \cdot \frac{1}{\mu_2}$$

where $\frac{1}{\mu_2} = \mu(\min\{\frac{1}{a_2}, \frac{1}{b_2}, \frac{1}{c_2}\}, \text{median}\{\frac{1}{a_2}, \frac{1}{b_2}, \frac{1}{c_2}\}, \max\{\frac{1}{a_2}, \frac{1}{b_2}, \frac{1}{c_2}\})$.

2.4 Functions on LFR

Given a function $f: R \rightarrow R$ and $\mu(a, b, c) \in LFR$, $f^*(\mu) : LFR \rightarrow LFR$ is defined as

$$f^*(\mu) = \mu(a^*, b^*, c^*),$$

where $a^* = \min\{f(a), f(b), f(c)\}, b^* = \text{median}\{f(a), f(b), f(c)\}, c^* = \max\{f(a),$

$f(b), f(c)\}$. If $a = b$ or $b = c$, then $a^* = b^*$ or $b^* = c^*$. Therefore if $a = b = c$ then it follows that $a^* = b^* = c^*$, i.e., $f^*(\epsilon(b)) = \epsilon(f(b))$. Hence f^* is an extension of the function f .

2.5 Ordering Properties

Given $\mu_1, \mu_2 \in LFR$, $\mu_1 \leq \mu_2$ provided that $a_1 \leq a_2, b_1 \leq b_2, c_1 \leq c_2$. If $\epsilon(0) \leq \mu(a, b, c)$, then $0 \leq a \leq b \leq c$, hence μ is a non-negative linear fuzzy real number. Therefore if μ is non-negative and zeroic, then $a = 0$ precisely. If $\{\mu_i\}_{i \in I}$ is a collection of linear fuzzy real numbers which is bounded above by a linear fuzzy real number μ where $\mu_i = \mu(a_i, b_i, c_i) \leq \mu = \mu(a, b, c)$, it follows that $\{a_i\}_{i \in I}, \{b_i\}_{i \in I}$, and $\{c_i\}_{i \in I}$ are collections of real numbers bounded above by a, b , and c , respectively. By the completeness of R there exist real numbers $\sup(a_i), \sup(b_i)$, and $\sup(c_i)$. Suppose that $\sup(a_i) > \sup(b_i)$, then if $2\epsilon = \sup(a_i) - \sup(b_i) > 0$, there is an a_j such that $a_j > \sup(a_i) - \epsilon > \sup(b_i) \geq b_j$, which leads to a contradiction. Therefore, $\sup(a_i) \leq \sup(b_i)$ and by a similar argument, $\sup(b_i) \leq \sup(c_i)$. It follows that $\sup(a_i) \leq \sup(b_i) \leq \sup(c_i)$ and thus $\mu(\sup(a_i), \sup(b_i), \sup(c_i))$ is a linear fuzzy real number. Now suppose that $\mu < \mu(\sup(a_i), \sup(b_i), \sup(c_i))$. Then $\mu = \mu(a, b, c)$ with $a \leq \sup(a_i), b \leq \sup(b_i)$, and $c \leq \sup(c_i)$ where at least one of these is a strict inequality. Given without loss of generality that $a < \sup(a_i)$, there is an index k such that $a_k > a$ so that it is not the case that $\mu_k \leq \mu$ and thus μ is not an upper bound for the collection $\{\mu_i\}_{i \in I}$. If μ is such an upper bound, then $a \geq a_i$ implies $a \geq \sup(a_i), b \geq \sup(b_i)$, and $c \geq \sup(c_i)$, so that $\mu(\sup(a_i), \sup(b_i), \sup(c_i))$ is the least upper bound. Therefore, (LFR, \leq) is a complete ordered set. However, it is not linearly ordered. If we let $\mu_1 = \mu(3, 4, 5)$ and let $\mu_2 = \mu(a, 5, 6)$ and state that $a < 3$, then it is not true that $\mu_1 \leq \mu_2$ nor is it true that $\mu_1 \geq \mu_2$. Therefore, μ_1 and μ_2 are incomparable in this order.

2.6 Linear equations on LFR

Before discussing the Diophantine equation, we must discuss linear equations in the LFR system. A linear equation over LFR is an equation of the form

$$\mu_1 \cdot \mu_x + \mu_2 = \mu_3 \cdot \mu_x + \mu_4,$$

where the μ_i are LFR 's for $i = 1, 2, 3, 4$ and μ_x is an unknown LFR with a triple of unknown real numbers (α, β, γ) . The solution set of the general linear equation can be roughly classified as

1. empty set,
2. singleton set,
3. not a singleton set but a bounded set:
 $\beta_1 \leq \alpha \leq \beta \leq \gamma \leq \beta_2$ for $\beta_1, \beta_2 \in R,$,
4. an unbounded set but not all LFR 's are included,
5. all possible LFR 's are included.

A solution set that is bounded but not a singleton would imply that μ_x is not equal to the solution set in a crisp sense. Solving these equations through traditional means can be a daunting task. If we define a relation $\mu_1 \equiv \mu_2 \pmod{\theta}$ iff $\mu_1 - \mu_2$ is zeroic, then $\mu(a, b, c) \equiv \epsilon(b) \pmod{\theta}$ since $\mu(a, b, c) - \epsilon(b) = \mu(a - b, 0, c - b)$. Therefore if we define $[\mu_1] = \{\mu_2 | \mu_2 \equiv \mu_1 \pmod{\theta}\}$, then $[\mu(a, b, c)] = [\epsilon(b)]$. Furthermore, in order that $\epsilon(a) \equiv \epsilon(b) \pmod{\theta}$, we must have $\epsilon(a) - \epsilon(b) = \epsilon(a - b)$ zeroic, which can only happen if $a = b$. Hence, we have a mapping $\Phi : \mu \rightarrow [\mu]$ with the property that if we compose this with the mapping $b \rightarrow \epsilon(b)$ then we obtain the sequence $R \xrightarrow{\epsilon} LFR \xrightarrow{\Phi} LFR/Z$, where Z is the set of zeroic elements of LFR , whence LFR/Z is seen to be isomorphic to itself. If $\iota : Z \rightarrow LFR$ is the inclusion mapping, then we obtain a further diagram:

$$Z \xrightarrow{\sigma} LFR \xrightarrow{\varphi} LFR/Z \xrightarrow{\epsilon} LFR.$$

Thus $[\mu * \mu^{-1}] = [\mu] * [\mu^{-1}] = \epsilon(1)$, i.e., $[\mu]$ has a multiplicative inverse in LFR/Z . The properties of LFR/Z allow one to solve for the solution of fuzzy linear equations using the inverse order of operations.

3 LINEAR EQUATIONS AND DIOPHANTINE LINEAR EQUATIONS

As stated earlier, a linear equation in LFR is an equation of the form $\mu_1 * \mu_x + \mu_2 = \mu_3 * \mu_x + \mu_4$, where μ_1, μ_2, μ_3 and μ_4 are LFR's and $\mu_x = \mu(x, y, z)$ is an unknown LFR. The Linear Fuzzy Real Diophantine problem requires that the solution μ_x as well as μ_1, μ_2, μ_3 and μ_4 be elements such that $\mu_i = \mu(a_i, b_i, c_i)$ implies that $a_i, b_i, c_i \in Z$ for $i = 1, 2, 3, 4$. Thus $\mu(a, b, c) \in LFZ$ is an integral LFR and behaves much like Z in R . The mapping

$$Z \xrightarrow{\sigma} LFZ \xrightarrow{\varphi} LFZ/Z \xrightarrow{\epsilon} LFZ$$

where Z is the set of Zeroic elements and LFZ is the set of Linear Fuzzy Integers yields the same properties of the mapping of LFR/Z .

3.1 Crisp Greatest Common Divisor and it's applications

It has been shown by Neggers [7] that arithmetic operations upon elements of LFR increase the area of $\mu(a_i, b_i, c_i)$. This is also known as overestimation. It is a phenomenon typical of fuzzy operations. The overestimation effect is responsible for a more or less large discrepancy between the arithmetical solution of a problem and the calculated one. In an effort to avoid this, a combination of LFZ/Z unique properties and a re-imagining of the problem is implemented in some cases. In particular we use $\epsilon(b_i)$ in place of $\mu_i = \mu(a_i, b_i, c_i)$ for certain operations and we rewrite certain problems in a *calculation friendly* way to reduce overestimation.

As a result of this we will define the Crisp GCD of LFZ , $CGCD$, as $d = \epsilon(b)$ such that $d \mid \mu_i = \mu(a_i, b_i, c_i)$ $i = 1, 2, 3, 4, 5 \dots$ and if there is an element $w \geq d$ and $w \mid \mu_i = \mu(a_i, b_i, c_i)$ $i = 1, 2, 3, 4, 5 \dots$ then $d = w$. The $CGCD$ will essentially be the GCD of $\epsilon(b_i)$ for a given set of LFZ numbers. Note that for $d \mid \mu(a_i, b_i, c_i)$ where a, b, c , and $d > 0$ in LFZ , yields $\mu\left(\text{floor}\left(\frac{a_i}{d}\right), \frac{b_i}{d}, \text{floor}\left(\frac{c_i}{d}\right)\right)$, as expected in integer division.

Proposition 3.1: If d divides μ_a and μ_b then d divides $\mu_a * \mu_x + \mu_b * \mu_y$ for all LFZ

Proof: If d divides μ_a then $\mu_a = \mu_m * d$, likewise for μ_b . Then it follows that

$$\mu_a * \mu_x + \mu_b * \mu_y = \mu_m * d * \mu_x + \mu_n * d * \mu_y. \text{ Thus } d \text{ divides } \mu_a * \mu_x + \mu_b * \mu_y \text{ for all } LFZ.$$

□

Proposition 3.2 Let μ_a and μ_b be LFZ (not both zeroic) with $CGCD$ d . Then an LFZ μ_c has the form $\mu_a * \mu_x + \mu_b * \mu_y$ for some $\mu_x, \mu_y \in LFZ$ iff μ_c is a multiple of d .

Proof: If $\mu_c = \mu_a * \mu_x + \mu_b * \mu_y$ where $\mu_x, \mu_y \in LFZ$ then since d divides μ_a and μ_b , Proposition 3.1 implies that d divides μ_c .

□

Proposition 3.2 implies that $\mu_c = \mu_a * \mu_x + \mu_b * \mu_y$ has a Linear Fuzzy Integer solution if and only if $d \mid \mu_c$.

3.2 Fuzzy Linear Diophantine Equation and Bezout's Identity

The Fuzzy Diophantine equation are equations of one or more variables, for which we seek integer solutions. One of the simplest of these is the Fuzzy Linear Diophantine equation $\mu_c = \mu_a * \mu_x + \mu_b * \mu_y$. Derived from this is Bezout's identity $d = \mu_a * \mu_x + \mu_b * \mu_y$. In fact, dividing by d , and defining $\frac{\mu_a}{d} = \mu_\alpha$ and $\frac{\mu_b}{d} = \mu_\beta$ produces the equation $\epsilon(1) = \mu_\alpha * \mu_x + \mu_\beta * \mu_y$. It follows that a fuzzy solution to $\epsilon(1) = \mu_\alpha * \mu_x + \mu_\beta * \mu_y$ is

$$\mu_x = \epsilon(x)_0 + \mu_y t \text{ and } \mu_y = \epsilon(y)_0 - \mu_x t.$$

3.3 Examples of the Application of the Euclidean Algorithm on Unit Fuzzy Linear Diophantine Problems

The following examples illustrate the application of the Euclidean Algorithm to a Fuzzy Linear Diophantine Problem.

Example 3.1

Solve $\mu(51,52,53)*\mu_x + \mu(55,56,57)*\mu_y = 4$, where $d = 4$, thus dividing by 4 we have $\mu_\alpha * \mu_x + \mu_\beta * \mu_y = \epsilon(1)$.

To reduce overestimation when evaluating the solution, we will use $\mu_\alpha * \mu_x \div \mu_y + \mu_\beta = \mu_\theta$. This is a product of dividing the unit Diophantine equation by μ_y where μ_θ is a zeroic value.

After dividing by 4 we have

$\mu(12,13,13)*\mu_x + \mu(13,14,14)*\mu_y = 1$, note that the LFZ $\mu(a,b,b)$ or $\mu(b,b,c)$ is a right triangular fuzzy number or LFZ.

Using the Euclidean algorithm on the numerical values, 13 and 14 we find that $\epsilon(x)_0 = -1$ and $\epsilon(y)_0 = 1$. Thus for $\mu_x = \epsilon(x)_0 + \mu_x t$ and $\mu_y = \epsilon(y)_0 - \mu_x t$, we have

$$\mu_x = \mu(12,13,13) \text{ and } \mu_y = \mu(-12,-12,-11)$$

Now, we check our solution, when $t=1$ using the aforementioned equation $\mu_\alpha * \mu_x \div \mu_y + \mu_\beta$

$$\text{We have } \mu(12,13,13) * \mu(12,13,13) \div \mu(-12,-12,-11) + \mu(13,14,14) = \mu(-2,0,2).$$

Example 3.2

Solve $\mu(7919,7920,7921)*\mu_x + \mu(4535,4536,4537)*\mu_y = 72$, where $d = 72$, thus dividing by 72 we have $\mu_\alpha * \mu_x + \mu_\beta * \mu_y = \epsilon(1)$.

After dividing by 72 we have

$$\mu(109,110,110)*\mu_x + \mu(62,63,63)*\mu_y = 1.$$

Using the Euclidean algorithm on 110 and 63 we find that $\epsilon(x)_0 = -4$ and $\epsilon(y)_0 = 7$. Thus for $\mu_x = \epsilon(x)_0 + \mu_x t$ and $\mu_y = \epsilon(y)_0 - \mu_x t$, we have

$$\mu_x = \mu(58,59,59) \text{ and } \mu_y = \mu(-103,-103,-102)$$

Setting $t=1$, for $\mu_\alpha * \mu_x \div \mu_y + \mu_\beta$

$$\text{We have } \mu(7919,7920,7921) * \mu(58,59,59) \div \mu(-103,-103,-102) + \mu(4535,4536,4537) = \mu(-1,0,2).$$

Thus in both examples, μ_x and μ_y are viable solutions.

4 CONCLUSION

From our examples, it is clear that we can find a crisp solution by projecting to the middle, $\mu(a,b,c) \rightarrow \epsilon(b)$. At the same time the method outlined produces a fuzzy solution in the form of an LFZ expression, which can be used directly as a fuzzy value or a fuzzy interval. In the future, LFZ may be applied to not just Linear Fuzzy Diophantine equations of two variables, but of three or more. LFZ may also provide useful insight in Simultaneous Linear Fuzzy Diophantine Equations as well as Fuzzy Number Theory.

5 REFERENCES

- [1] R.E. Bellman, L.A. Zadeh, Decision making in a fuzzy environment, *Management Science*, **17** (1970), B141–B164.
- [2] D. Dubois, H. Prade, System of linear fuzzy constraints, *Fuzzy Sets and Systems*, **13** (1982), 1–10.
- [3] B. Monk, *A Proposed Theory of Fuzzy Random Variables*, Dissertation, University of Alabama, 2001.
- [4] J. Neggers, H. Kim, Fuzzy posets on sets, *Fuzzy sets and systems*, **17** (2001), 391–402.
- [5] J. Neggers, H. Kim, *On Linear Fuzzy Real Numbers*, Manuscript for book under development, 2007.
- [6] C.V. Negoita, *Fuzziness in management*, OPSA/TIMS, Miami, 1970.
- [7] R. Prevo, *Entropies of families of fuzzy random variables: an introduction to an in-depth exploration of several classes of important examples*, Dissertation, University of Alabama, 2002.

- [8] F. Rogers, J. Neggers, Y. Jun. Method for Optimizing Linear Problems with Fuzzy Constraints. *International Mathematical Forum*, **3** (2008), 1141-1155.
- [9] H. Tanaka, K. Asai, Fuzzy linear programming problems with fuzzy numbers, *Fuzzy sets and Systems*, **13** (1984), 1–10.
- [10] H. Tanaka, T. Okuda and K. Asai, On fuzzy mathematical programming, *J. Cybernetics*, **3** (1984), 37–46.
- [11] H.J. Zimmermann, Fuzzy mathematical programming, *Comput. Ops. Res.*, **10** (1983), 291–298.