12-2016

Towards an Algebraic Description of Set Arithmetic

Olga Kosheleva
University of Texas at El Paso, olgak@utep.edu

Vladik Kreinovich
University of Texas at El Paso, vladik@utep.edu

Comments:
Technical Report: UTEP-CS-16-90

Towards an Algebraic Description of Set Arithmetic

Olga Kosheleva and Vladik Kreinovich
University of Texas at El Paso
500 W. University, El Paso, TX 79968, USA
olgak@utep.edu, vladik@utep.edu

Abstract

To describe the state of the world, we need to describe the values of all physical quantities. In practice, due to inevitable measurement inaccuracy, we do not know the exact values of these quantities, we only know the sets of possible values for these quantities. On the class of such uncertainty-related sets, we can naturally define arithmetic operations that transform, e.g., uncertainty in a and b into uncertainty with which we know the sum $a + b$.

In many applications, it has been useful to reformulate the problem in purely algebraic terms, i.e., in terms of axioms that the basic operations must satisfy: there are useful applications of groups, rings, fields, etc. From this viewpoint, it is desirable to be able to describe the class of uncertainty-related sets with the corresponding arithmetic operations in algebraic terms. In this paper, we provide such a representation.

Our representation has the same complexity complexity as the usual algebraic description of a field (such as the field of real numbers).

1 Formulation of the Problem

Need for intervals (and more general sets): a brief reminder. To describe the exact state of the world, we need to know the numerical values of the corresponding physical quantities. Some of the quantities can only take values from a given discrete set: e.g., the electric charge must be proportional to the smallest possible charge. However, for most physical quantities, all real numbers are possible values.

In practice, we rarely know the exact value a of a physical characteristic; due to inevitable measurement uncertainty, we only know a *set* of possible values; see, e.g., [5]. In many cases, all we know is the measurement result $\widetilde{a}$ and the upper bound Δ on the absolute value of the measurement error $\widetilde{a} - a$. In this case, all we know about the actual (unknown) value a of this quantity is that it belongs to the *interval* $[\widetilde{a} - \Delta, \widetilde{a} + \Delta]$.

In some cases, the set of possible values of a quantity is more complex than an interval. For example, if we have measured the kinetic energy $m \cdot \frac{v^2}{2}$ of a 1-D particle with some accuracy but we do not know the particle's direction, then the possible values of the velocity v form a union of two disjoint intervals $[-\overline{v}, -\underline{v}] \cup [\underline{v}, \overline{v}]$ for appropriate values $\underline{v}$ and $\overline{v}$.

Algebraic operations on intervals and sets. Once we know the intervals (or, more generally, sets) A and B of possible values of quantities a and b, then we can conclude that the set of possible values of the sum $a + b$ is the set

$$A + B \stackrel{\text{def}}{=} \{a + b : a \in A \,\&\, b \in B\}. \tag{1}$$

Similarly, the sets of possible values of the difference $a - b$ and product take the form

$$A - B \stackrel{\text{def}}{=} \{a - b : a \in A \,\&\, b \in B\}; \tag{2}$$

$$A \cdot B \stackrel{\text{def}}{=} \{a \cdot b : a \in A \,\&\, b \in B\}. \tag{3}$$

For the inverse a^{-1}, the set of possible values exists only when $0 \notin A$:

$$A^{-1} \stackrel{\text{def}}{=} \{a^{-1} : a \in A\}. \tag{4}$$

For the case of intervals, these formulas form *interval arithmetic*; see, e.g., [2, 4]. These operations can be considered for more general sets as well.

It is desirable to have an algebraic description. Often, it is useful to have an algebraic description of a class of mathematical objects. When we know that the properties of this class are described by a few axioms, it is sometimes easier to find a proof based on these axioms. There are many practical examples of such efficiency based on axioms describing groups, rings, fields, etc.; see, e.g., [1].

Formulation of our problem: first approximation. From this viewpoint, it is desirable to come up with an algebraic description of interval (and set) uncertainty.

Let us start with a known algebraic description of real numbers. Most algebraic properties of the set of *real numbers* are captured by describing it as a *field*, i.e., as a set with two constants 0 and 1 and two operations – addition $+$ and multiplication $\cdot$ – which are commutative, associative, distributive, and have the properties that $a + 0 = a$, $a \cdot 1 = a$, and that every non-zero element a has a multiplicative inverse a^{-1}.

How complex is this description? A natural way to describe the complexity of a general formula is by counting the number of quantifier changes; see, e.g., [6]. The simplest formulas are the ones with no quantifiers at all, such as $0 + 1 = 1$.

Next in complexity are formulas with only universal or only existential quantifiers, such as

$$\forall a \, \forall b \, (a + b = b + a)$$

and

$$\forall a\, \forall b\, \forall c\, (a + (b + c) = (a + b) + c).$$

The class of all formulas described by only universal quantifiers is usually denoted by Π_1. Formulas from this class describe most properties of the field like commutativity, associativity, and distributivity.

The only property that requires more quantifier changes is the property that every non-zero element has an inverse:

$$\forall a\, (a \neq 0 \to \exists b\, (a \cdot b = 1)),$$

or, equivalently,

$$\forall a\, \exists b\, (a \neq 0 \to a \cdot b = 1).$$

The class of all such formulas is denoted by Π_2.

It is desirable to come up with a description of set arithmetic that will have the exact same complexity. Thus, we arrive at the following formulation of the problem.

Final formulation of the problem. It is desirable to come up with a Π_2 description of set arithmetic, i.e., of the class of non-empty subsets of a field which contains all the one-point sets and which is closed under above-defined operations of set addition, set multiplication, and (when applicable) set inverse.

What we do in this paper. In this paper, we present such a description.

In our description, we will use known results. In this description of set arithmetic, we will use the main ideas behind a similar description of interval arithmetic; see, e.g., [3] are references therein.

2 Analysis of the Problem

Let us start with a definition.

Definition 1. *Let F be a field. By a* set arithmetic*, we mean a class C of non-empty subsets of F which contains all one-point sets and which is closed under set addition* (1)*, set subtraction* (2)*, set multiplication* (3)*, and – for sets $A \not\ni 0$ – set inverse* (4)*. On this class, we have elements* 0 $(= \{0\})$*,* 1 $(= \{1\})$*, and operations $A + B$, $A \cdot B$, and A^{-1}.*

How can we characterize one-point sets. Suppose that we have the class of the subsets which is appropriately closed. How can we then select points – i.e., one-point sets? The answer follows from the following simple lemma.

Lemma 1. *For every set arithmetic C, a set $A \in C$ is a one-element set if and only if there exists $A' \in C$ for which $A + A' = 0$.*

Proof. If $A = \{a\}$, then we can take $A' = \{-a\}$. Vice verse, if A is not a one-element set, i.e., if the set A contains two different points $a_1 \neq a_2$, then for

each $a' \in A'$, the set $A + A'$ contains two different elements $a_1 + a'$ and $a_2 + a'$ and thus, the set $A + A'$ cannot be equal to the 1-point set 0 ($= \{0\}$).

How can we describe that a point A belongs to the set B? Such a characterization is also easy to describe:

Lemma 2. *When $A = \{a\}$, then $a \in B$ if and only if the set $B - A$ does not have an inverse.*

Proof. Indeed, $a \in B$ if and only if $0 \in B - a = B - A$, and this is indeed the only condition under which the set $B - A$ does not have an inverse.

Now, we are ready to formulate our main result.

3 Main Result

Notation. Let us denote the condition that the inverse A^{-1} is defined by $D(A^{-1})$.

Proposition. *For a set C with constants 0 and 1, everywhere defined operations $A + B$, $A - B$, $A + B$, and a partially defined operation A^{-1}, the following two statements are equivalent to each other:*

- *elements of the set C can be represented as non-empty subsets of a field with operations $(1) - -(4)$, so that one-point sets are all elements of the class C;*
- *the following Π_2 statements hold:*

$$\forall A\, \forall A'\, \forall B\, \forall B'\, \exists C'\, ((A + A' = 0 \,\&\, B + B' = 0) \to (A + B) + C' = 0). \quad (5)$$

$$\forall A\, \forall A'\, \forall B\, \forall B'\, \exists C'\, ((A + A' = 0 \,\&\, B + B' = 0) \to (A - B) + C' = 0). \quad (6)$$

$$\forall A\, \forall A'\, \forall B\, \forall B'\, \exists C'\, ((A + A' = 0 \,\&\, B + B' = 0) \to (A \cdot B) + C' = 0). \quad (7)$$

$$\forall A\, \forall A'\, \exists C'\, ((A + A' = 0 \,\&\, D(A^{-1})) \to A^{-1} + C' = 0). \quad (8)$$

$$\forall A\, \forall A'\, \forall B\, \forall B'\, ((A + A' = 0 \,\&\, B + B' = 0) \to A + B = B + A). \quad (9)$$

$$\forall A\, \forall A'\, \forall B\, \forall B'\, ((A + A' = 0 \,\&\, B + B' = 0) \to A \cdot B = B \cdot A). \quad (10)$$

$$\forall A\, \forall A'\, \forall B\, \forall B'\, \forall C\, \forall C'\, ((A + A' = 0 \,\&\, B + B' = 0 \,\&\, C + C' = 0) \to A + (B + C) = (A + B) + C). \quad (11)$$

$$\forall A\, \forall A'\, \forall B\, \forall B'\, \forall C\, \forall C'\, ((A + A' = 0 \,\&\, B + B' = 0 \,\&\, C + C' = 0) \to A \cdot (B \cdot C) = (A \cdot B) \cdot C). \quad (12)$$

$$\forall A\, \forall A'\, \forall B\, \forall B'\, \forall C\, \forall C'\, ((A + A' = 0 \,\&\, B + B' = 0 \,\&\, C + C' = 0) \to A \cdot (B + C) = A \cdot B + A \cdot C). \quad (13)$$

$$\forall A\, \forall A'\, \forall B\, \forall B'\, \forall C\, \forall C'\, ((A + A' = 0 \,\&\, B + B' = 0 \,\&\, C + C' = 0) \to$$

$$(A + B = C \leftrightarrow C - A = B)). \tag{14}$$

$$\forall A\, \forall A'\, ((A + A' = 0\, \&\, A \neq 0) \rightarrow D(A^{-1})). \tag{15}$$

$$\forall A\, \forall A'\, \forall A_1\, \forall B\, \forall B'\, \forall B_1\, ((A + A' = 0\, \&\, B + B' = 0\, \&$$
$$D((A_1 - A)^{-1})\, \&\, D((B_1 - B)^{-1})) \rightarrow D((A_1 + B_1) - (A + B))^{-1})). \tag{16}$$

$$\forall A\, \forall A'\, \forall A_1\, \forall B\, \forall B'\, \forall B_1\, ((A + A' = 0\, \&\, B + B' = 0\, \&$$
$$D((A_1 - A)^{-1})\, \&\, D((B_1 - B)^{-1})) \rightarrow D((A_1 - B_1) - (A - B))^{-1})). \tag{17}$$

$$\forall A\, \forall A'\, \forall A_1\, \forall B\, \forall B'\, \forall B_1\, ((A + A' = 0\, \&\, B + B' = 0\, \&$$
$$D((A_1 - A)^{-1})\, \&\, D((B_1 - B)^{-1})) \rightarrow D((A_1 \cdot B_1) - (A \cdot B))^{-1})). \tag{18}$$

$$\forall A\, \forall A'\, \forall A_1\, ((A + A' = 0\, \&\ D((A_1 - A)^{-1})\, \&\, D(A_1^{-1})) \rightarrow$$
$$(D(A^{-1})\, \&\, D(A_1^{-1} - A^{-1}))). \tag{19}$$

$$\forall A_1\, \forall B_1\, \forall C\, \forall C'\, (C + C' = 0\, \&\, D((A_1 + B_1) - C)^{-1})) \rightarrow$$
$$\exists A\, \exists A'\, \exists B\, \exists B'\, (A + A' = 0\, \&\, B + B' = 0\, \&\, C = A + B)). \tag{20}$$

$$\forall A_1\, \forall B_1\, \forall C\, \forall C'\, (C + C' = 0\, \&\, D((A_1 - B_1) - C)^{-1})) \rightarrow$$
$$\exists A\, \exists A'\, \exists B\, \exists B'\, (A + A' = 0\, \&\, B + B' = 0\, \&\, C = A - B)). \tag{21}$$

$$\forall A_1\, \forall B_1\, \forall C\, \forall C'\, (C + C' = 0\, \&\, D((A_1 \cdot B_1) - C)^{-1})) \rightarrow$$
$$\exists A\, \exists A'\, \exists B\, \exists B'\, (A + A' = 0\, \&\, B + B' = 0\, \&\, C = A \cdot B)). \tag{22}$$

$$\forall A_1\ \forall C\, \forall C'\, (C + C' = 0\, \&\, D(A_1^{-1} - C)^{-1})) \rightarrow$$
$$\exists A\, \exists A'\, (A + A' = 0\, \&\, C = A^{-1})). \tag{23}$$

$$\forall A\, \forall B\, (A \neq B \rightarrow \exists C\, \exists C'\, (C + C' = 0\, \&$$
$$((D((A - C)^{-1})\, \&\, \neg D((B - C)^{-1}) \vee (\neg D((A - C)^{-1})\, \&\, D((B - C)^{-1}))). \tag{24}$$

$$\forall A\, (A + 0 = A). \tag{25}$$

$$\forall A\, (A \cdot 1 = A). \tag{26}$$

Proof. If C is the class of subsets of a field F, then properties (5)-(8) means that when applied to 1-point sets (elements), arithmetic operations lead to 1-point sets. The properties (9)-(13) means that for elements, addition and multiplication are commutative, associative, and distributive. The property (14) means that for one-point elements, subtraction is defined in terms of addition, and the property (15) means that every one-element set different from 0 has an inverse.

The property (16) means that if $a \in A_1$ and $b \in B_1$, then $a+b \in A_1+B_1$. The properties (17)-(19) describe similar properties for subtraction, multiplication, and inverse.

The property (20) means that if an element c belongs to $A_1 + B_1$, then it can be represented as $a + b$ for some elements $a \in A_1$ and $b \in B_1$. The properties (21)-(23) mean the same for other arithmetic operations.

The property (24) means that if two objects are different, this means that there is a point that belongs to only one of them.

Finally, (25) and (26) are the usual properties of 0 and 1.

Vice versa, let us assume that we have a class C with constants 0 and 1 and with operations $A + B$, $A \cdot B$, and A^{-1} that satisfy the properties (5)-(24).

Let F denote the set of all the objects A for which $A + A' = 0$ for some A'. Then, due to the properties (5)-(8), the set F is closed under the arithmetic operations. The properties (9)-(13) imply that on the set F, addition and multiplication are commutative, associative, and distributive. The property (14) implies that on the set F, subtraction is defined in terms of addition, and the property (15) implies that every one-element set different from 0 has an inverse. The properties (25) and (26) are usual properties of 0 and 1. Thus, the set F is a field.

To every element $A \in C$, we can then assign the set of all the elements B for which $D((A - B)^{-1})$. Due to the property (24), different elements from C correspond to different sets.

The properties (16)-(19) imply that for each arithmetic operation $\odot$, if $a \in A_1$ and $b \in B_1$, then $a \odot b \in A_1 \odot B_1$. The properties (20)-(23) imply that, vice versa, that if an element c belongs to $A_1 \odot B_1$, then it can be represented as $a \odot b$ for some elements $a \in A_1$ and $b \in B_1$. Thus, the set corresponding to $A \odot B$ is indeed the set of all possible values $a \odot b$ where $a \in A$ and $b \in B$.

The proposition is proven.

Acknowledgments

This work was supported by the National Science Foundation grants HRD-0734825 and HRD-1242122 (Cyber-ShARE Center of Excellence) and DUE-0926721, and by an award "UTEP and Prudential Actuarial Science Academy and Pipeline Initiative" from Prudential Foundation.

The authors are thankful to all the participants of SCAN'2016 for valuable discussions.

References

[1] D. W. Hardy, F. Richman, and C. L. Walker, *Applied Algebra: Codes, Ciphers and Discrete Algorithms*, CRC Press, Boca Raton, Florida, 2009.

[2] L. Jaulin, M. Kiefer, O. Dicrit, and E. Walter, *Applied Interval Analysis*, Springer, London, 2001.

[3] S. Markov, "On the algebra of intervals", *Reliable Computing*, 2016, Vol. 21, pp. 80–108.

[4] R. E. Moore, R. B. Kearfott, and M. J. Cloud, *Introduction to Interval Analysis*, SIAM, Philadelphia, 2009.

[5] S. G. Rabinovich, *Measurement Errors and Uncertainty: Theory and Practice*, Springer Verlag, Berlin, 2005.

[6] H. Straubing, *Finite Automata, Formal Logic, and Circuit Complexity*, Springer Verlag, New York, 2013.