A Realistic (Non-Associative) Logic And a Possible Explanations of 7 ± 2 Law

Raúl Trejo[1,2], Vladik Kreinovich[1], I. R. Goodman[3], Jesus Martinez[1], and Reginaldo Gonzalez[1]

[1]Department of Computer Science
University of Texas, El Paso, TX 79968, USA
contact email vladik@cs.utep.edu
[2]Sistemas de Informacion
Division de Ingeneria y Ciencias
ITESM (Instituto Technológico de Monterrey)
Campus Estadoy de México
Apdo. Postal 2, Modulo de Servicio Postal
Atizapan, Mexico 52926
rtrejo@campus.cem.itesm.mx
[3]Code D42215
Space & Naval Warfare Systems Center
San Diego, CA 92152, USA
goodman@spawar.navy.mil

Abstract

When we know the subjective probabilities (degrees of belief) p_1 and p_2 of two statements S_1 and S_2, and we have no information about the relationship between these statements, then the probability of $S_1 \,\&\, S_2$ can take any value from the interval $[\max(p_1 + p_2 - 1, 0), \min(p_1, p_2)]$. If we must select a single number from this interval, the natural idea is to take its midpoint. The corresponding "and" operation $p_1 \,\&\, p_2 \stackrel{\rm def}{=} (1/2) \cdot (\max(p_1+p_2-1, 0)+\min(p_1, p_2))$ is not associative. However, since the largest possible non-associativity degree $|(a \,\&\, b) \,\&\, c - a \,\&\, (b \,\&\, c)|$ is equal to $1/9$, this non-associativity is negligible if the realistic "granular" degree of belief have granules of width $\geq 1/9$. This may explain why humans are most comfortable with ≤ 9 items to choose from (the famous "7 plus minus 2" law).
We also show that the use of interval computations can simplify the (rather complicated) proofs.

1 In Expert Systems, We Need Estimates for the Degree of Certainty of $S_1 \,\&\, S_2$ and $S_1 \vee S_2$

In many areas (medicine, geophysics, military decision-making, etc.), top quality experts make good decisions, but they cannot handle all situations. It is therefore desirable to incorporate their knowledge into a decision-making computer system.

Experts describe their knowledge by statements $S_1, \ldots, S_n$ (e.g., by if-then rules). Experts are often not 100% sure about these statements S_i; this uncertainty is described by the *subjective probabilities* p_i (degrees of belief, etc.) which experts assign to their statements. The conclusion C of an expert system normally depends on several statements S_i. For example, if we can deduce C either from S_2 and S_3, or from S_4, then the validity of C is equivalent to the validity of a Boolean combination $(S_2 \,\&\, S_3) \vee S_4$. So, to estimate the reliability $p(C)$ of the conclusion, we must estimate the probability of Boolean combinations. In this paper, we consider the simplest possible Boolean combinations are $S_1 \,\&\, S_2$ and $S_1 \vee S_2$.

In general, the probability $p(S_1 \,\&\, S_2)$ of a Boolean combination can take different values depending on whether S_1 and S_2 are independent or correlated. So, to get the precise estimates of probabilities of all possible conclusions, we must know not only the probabilities $p(S_i)$ of individual statements, but also the probabilities of all possible Boolean combinations. To get all such probabilities, it is sufficient to describe 2^n probabilities of the combinations $E_1^{\varepsilon_1} \,\&\, \ldots \,\&\, E_n^{\varepsilon_n}$, where $\varepsilon_i \in \{+, -\}$, E^+ means E, and E^- means $\neg E$. The only condition on these probabilities is that their sum should add up to 1, so we need to describe $2^n - 1$ different values. A typical knowledge base may contain hundreds of statements; in this case, the value $2^n - 1$ is astronomically large. We cannot ask experts about all 2^n such combinations, so in many cases, we must estimate $p(S_1 \,\&\, S_2)$ or $p(S_1 \vee S_2)$ based only on the values $p_1 = p(S_1)$ and $p_2 = p(S_2)$.

2 Interval Estimates Are Possible, But Sometimes, Numerical Estimates Are Needed

It is known that for given $p_1 = p(S_1)$ and $p_2 = p(S_2)$:

- possible values of $p(S_1 \,\&\, S_2)$ form an interval $\mathbf{p} = [p^-, p^+]$, where $p^- = \max(p_1 + p_2 - 1, 0)$ and $p^+ = \min(p_1, p_2)$; and
- possible values of $p(S_1 \vee S_2)$ form an interval $\mathbf{p} = [p^-, p^+]$, where $p^- = \max(p_1, p_2)$ and $p^+ = \min(p_1 + p_2, 1)$

(see, e.g., a survey [22] and references therein).

So, in principle, we can use such interval estimates and get an interval $\mathbf{p}(C)$ of possible values of $p(C)$. Sometimes, this idea leads to meaningful estimates, but often, it leads to a useless $\mathbf{p}(C) = [0,1]$ [22, 23]. In such situations, it is reasonable, instead of using the entire interval $\mathbf{p}$, to select a point within this interval as a reasonable estimate for $p(S_1 \,\&\, S_2)$ (or, correspondingly, for $p(S_1 \vee S_2)$).

3 Natural Idea: Selecting a Midpoint as the Desired Estimate

Since the only information we have, say, about the unknown probability $p(S_1 \,\&\, S_2)$ is that it belongs to the interval $[p^-, p^+]$, it is natural to select a *midpoint* of this interval as the desired estimate. In other words, if we know the probabilities p_1 and p_2 of the statements S_1 and S_2, then, as estimates for $p(S_1 \,\&\, S_2)$ and $p(S_1 \vee S_2)$, we can take the values $p_1 \,\&\, p_2$ and $p_1 \vee p_2$, where

$$p_1 \,\&\, p_2 \stackrel{\rm def}{=} \frac{1}{2} \cdot \max(p_1 + p_2 - 1, 0) + \frac{1}{2} \cdot \min(p_1, p_2); \qquad (1)$$

$$p_1 \vee p_2 \stackrel{\rm def}{=} \frac{1}{2} \cdot \max(p_1, p_2) + \frac{1}{2} \cdot \min(p_1 + p_2, 1). \qquad (2)$$

This midpoint selection is not only natural from a common sense viewpoint; it also has a deeper justification. Namely, in accordance of our above discussion, for $n = 2$ statements S_1 and S_2, to describe the probabilities of all possible Boolean combinations, we need to describe $2^2 = 4$ probabilities $x_1 = p(S_1 \,\&\, S_2)$, $x_2 = p(S_1 \,\&\, \neg S_2)$, $x_3 = p(\neg S_1 \,\&\, S_2)$, and $x_4 = p(\neg S_1 \,\&\, \neg S_2)$; these probabilities should add up to 1: $x_1 + x_2 + x_3 + x_4 = 1$. Thus, each probability distribution can be represented as a point $(x_1, \ldots, x_4)$ in a 3-D simplex $\mathcal{S} = \{(x_1, x_2, x_3, x_4) \,|\, x_i \geq 0 \,\&\, x_1 + \ldots + x_4 = 1\}$. We know the values of $p_1 = p(S_1) = x_1 + x_2$ and $p_2 = p(S_2) = x_1 + x_3$, and we are interested in the values of $p(S_1 \,\&\, S_2) = x_1$ and $p(S_1 \vee S_2) = x_1 + x_2 + x_3$. It is natural to assume that *a priori*, all probability distributions (i.e., all points in a simplex $\mathcal{S}$) are "equally possible", i.e., that there is a uniform distribution ("second-order probability") on this set of probability distributions. Then, as a natural estimate for the probability $p(S_1 \,\&\, S_2)$ of $S_1 \,\&\, S_2$, we can take the conditional mathematical expectation of this probability under the condition that the values $p(S_1) = p_1$ and $p(S_2) = p_2$:

$$E(p(S_1 \,\&\, S_2) \,|\, p(S_1) = p_1 \,\&\, p(S_2) = p_2) = P(x_1 \,|\, x_1 + x_2 = p_1 \,\&\, x_1 + x_3 = p_2).$$

(This idea was proposed and described in [1, 6, 7, 8, 9]; see also [2].)

From the geometric viewpoint, the two conditions $x_1 + x_2 = p_1$ and $x_1 + x_3 = p_2$ select a straight line segment within the simplex $\mathcal{S}$, a segment which can be parameterized by $x_1 \in [p^-, p^+] = [\max(p_1 + p_2 - 1, 0), \min(p_1, p_2)]$; then, $x_2 = p_1 - x_1$, $x_3 = p_2 - x_1$, and $x_4 = 1 - (x_1 + x_2 + x_3)$. Since we start with a uniform distribution on $\mathcal{S}$, the conditional probability distribution on this segment is uniform, i.e., x_1 is uniformly distributed on the interval $[p^-, p^+]$. Thus, the conditional mathematical expectation of x_1 with respect to this distribution is equal to $(p^- + p^+)/2$, i.e., to the midpoint of this interval. Similarly, for an "or" operation, we can conclude that

$$E(p(S_1 \vee S_2) \,|\, p(S_1) = p_1 \,\&\, p(S_2) = p_2) = \frac{1}{2} \cdot \max(p_1, p_2) + \frac{1}{2} \cdot \min(p_1 + p_2, 1).$$

4 Problem: Midpoint Operations Are Not Associative

Any "and" operation $p_1 \,\&\, p_2$ enables us to produce an estimate for $P(S_1 \,\&\, S_2)$ provided that we know estimates p_1 for $p(S_1)$ and p_2 for $p(S_2)$. If we are interested in estimating the degree of belief in a conjunction of three statements $S_1 \,\&\, S_2 \,\&\, S_3$, then we can use the same operation twice:

- first, we apply the "and" operation to p_1 and p_2 and get an estimate $p_1 \,\&\, p_2$ for the probability of $S_1 \,\&\, S_2$;
- then, we apply the "and" operation to this estimate $p_1 \,\&\, p_2$ and p_3, and get an estimate $(p_1 \,\&\, p_2) \,\&\, p_3$ for the probability of $(S_1 \,\&\, S_2) \,\&\, S_3$.

Alternatively, we can get start by combining S_2 and S_3, and get an estimate $p_1 \,\&\, (p_2 \,\&\, p_3)$ for the same probability $p(S_1 \,\&\, S_2 \,\&\, S_3)$. Intuitively, we would expect these two estimates to coincide: $(p_1 \,\&\, p_2) \,\&\, p_3 = p_1 \,\&\, (p_2 \,\&\, p_3)$, i.e., in algebraic terms, we expect the operation $\&$ to be associative. Unfortunately, midpoint operations are *not* associative [2]: e.g., $(0.4 \,\&\, 0.6) \,\&\, 0.8 = 0.2 \,\&\, 0.8 = 0.1$, while $0.4 \,\&\, (0.6 \,\&\, 0.8) = 0.4 \,\&\, 0.5 = 0.2 \neq 0.1$.

By itself, a small non-associativity may not be so bad:

- associativity comes from the requirement that our reasoning be rational, while
- it is well known that our actual handling of uncertainty is not exactly following rationality requirements; see, e.g., [29].

So, it is desirable to find out how non-associative can these operations be.

5 How Non-Associative Are Natural (Midpoint) Operations? Main Results and Their Psychological Interpretation

We know that the midpoint operations are non-associative, i.e., that sometimes, $(a \,\&\, b) \,\&\, c \neq a \,\&\, (b \,\&\, c)$. We want to know how big can the difference $(a \,\&\, b) \,\&\, c - a \,\&\, (b \,\&\, c)$ can be.

Theorem 1. $\max\limits_{a,b,c} |(a \,\&\, b) \,\&\, c - a \,\&\, (b \,\&\, c)| = 1/9.$

Theorem 2. $\max\limits_{a,b,c} |(a \vee b) \vee c - a \vee (b \vee c)| = 1/9.$

(For readers' convenience, all the proofs are placed in the last section.)

Human experts do not use all the numbers from the interval $[0, 1]$ to describe their possible degrees of belief; they use a few words like "very probable", "mildly probable", etc. Each of words is a "granule" covering the entire sub-interval of values. Since the largest possible non-associativity degree $|(a \,\&\, b) \,\&\, c - a \,\&\, (b \,\&\, c)|$ is equal to $1/9$, this non-associativity is negligible if the corresponding realistic "granular" degree of belief have granules of width $\geq 1/9$. One can fit no more than 9 granules of such width in the interval $[0, 1]$. This may explain why humans are most comfortable with ≤ 9 items to choose from – the famous "7 plus minus 2" law; see, e.g., [19, 20].

This general psychological law has also been confirmed in our specific area of formalizing expert knowledge: namely, in [5], it was shown that this law explains why in intelligent control, experts normally use ≤ 9 different degrees (such as "small", "medium", etc.) to describe the value of each characteristic.

6 Pessimism-Optimism As an Alternative to Midpoint

For each interval $[p^-, p^+]$, the lower endpoint p^- is the most pessimistic estimate, while the upper bound p^+ is the most optimistic one. Selecting as midpoint means selecting an average of the pessimistic and an optimistic estimates. Alternatively, we can use *Hurwicz* pessimism-optimism criterion (originally proposed in [11]): namely, we choose a real number $\alpha \in [0, 1]$, and select a value $p = \alpha \cdot p^- + (1 - \alpha) \cdot p^+$. This selection can be justified by the requirement that the corresponding mapping from intervals to points should not depend neither on the units in which we measure u (i.e., be *scale-invariant*), nor on the choice of the starting point (i.e., be *shift-invariant*).

Definition. *By a choice function, we mean a function s that maps every interval $[u^-, u^+]$ into a point from that interval, and that has the following properties for every interval and for every c and $\lambda > 0$:*

- $s([u^- + c, u^+ + c]) = s([u^-, u^+]) + c$ *(shift-invariance);*
- $s([\lambda \cdot u^-, \lambda \cdot u^+]) = \lambda \cdot s([u^-, u^+])$ *(unit-invariance).*

Proposition. [21] *Every choice function has the form*

$$s([u^-, u^+]) = \alpha \cdot u^- + (1 - \alpha) \cdot u^+.$$

Hurwicz's pessimism-optimism criterion has been successfully used in areas ranging from submarine detection [3, 4, 24, 25, 26] to petroleum engineering [28]; see also [12, 13, 14, 18, 27]. (In [31, 32], this approach is applied to second-order probabilities.)

With this approach, we get the following formulas which generalize (1) and (2):

$$p_1 \,\&\, p_2 \stackrel{\text{def}}{=} \alpha \cdot \max(p_1 + p_2 - 1, 0) + (1 - \alpha) \cdot \min(p_1, p_2); \tag{3}$$

$$p_1 \vee p_2 \stackrel{\text{def}}{=} \alpha \cdot \max(p_1, p_2) + (1 - \alpha) \cdot \min(p_1 + p_2, 1). \tag{4}$$

These operations (3) and (4) have the following easy-to-prove properties:

- they are *commutative*: $a \,\&\, b = b \,\&\, a$ and $a \vee b = b \vee a$;
- they are *monotonic* in the sense that if $a \le a'$ and $b \le b'$, then $a \,\&\, b \le a' \,\&\, b'$ and $a \vee b \le a' \vee b'$;
- for classical truth values $a, b \in \{0, 1\}$, these operations coincide with the corresponding operations of classical two-valued (Boolean) logic;
- the "and"-operation (3) is a convex combination of two t-norms for both of which $a * b \le a$, hence $a \,\&\, b \le a$ for all a and b; similarly, $a \le a \vee b$ for all a and b.

For these new operations, the largest possible degrees of non-associativity are equal to the following values:

Theorem 3. $\max\limits_{a,b,c} |(a \,\&\, b) \,\&\, c - a \,\&\, (b \,\&\, c)| = \dfrac{\alpha \cdot (1 - \alpha)}{2 + \alpha \cdot (1 - \alpha)}.$

Theorem 4. $\max\limits_{a,b,c} |(a \vee b) \vee c - a \vee (b \vee c)| = \dfrac{\alpha \cdot (1 - \alpha)}{2 + \alpha \cdot (1 - \alpha)}.$

7 These Operations Are Semi-Associative

It turns out that in proving Theorems 1–4, it is useful to take into consideration that although the new operations $\&$ and $\vee$ are *not* associative, i.e., the values $(a \,\&\, b) \,\&\, c$ and $a \,\&\, (b \,\&\, c)$ are not always equal, these operations are *semi-associative* in the sense that instead of *equality*, we have *one-sided inequality*. To be more precise, the following result is true:

Definition 1. *We say that a commutative operation $*$ is semi-associative if $a \le b \le c$ implies that $a * (b * c) \ge b * (a * c) \ge c * (a * b)$.*

Theorem 5. *For every $\alpha \in (0, 1)$, both operations (3) and (4) are semi-associative.*

8 Proofs

8.1 General comment

One can easily see that the operation (2) is *dual* to the operation (1) in the sense that $a \vee b = 1 - (1-a) \,\&\, (1-b)$. Similarly, for every $\alpha \in (0,1)$, the operation (4) corresponding to this α is dual to the operation (3) corresponding to $\alpha' = 1 - \alpha$, and vice versa. Because of this duality, we can easily deduce Theorem 2 from Theorem 1, Theorem 4 from Theorem 3, and the "or" part of Theorem 5 from its "and" part. Thus, it is sufficient to prove Theorem 1, Theorem 3, and the "and" part of Theorem 5.

Of these three results, Theorem 1 is a particular case of Theorem 1 which corresponds to $\alpha = 0.5$; thus, it is sufficient to prove Theorem 3 and the "and" part of Theorem 5. Since, as we have mentioned, Theorem 5 is used in the proof of Theorem 3, we will start by proving Theorem 5.

To make it easier to follow these proofs, the reader is welcome to use the fact that the traditional fuzzy logic operation $\min(a,b)$ corresponds to $\alpha = 0$ and $1 - \alpha = 1$; to make this following even easier, we introduce a new variable $\beta = 1 - \alpha$; then, $\alpha = 1 - \beta$.

8.2 Proof of Theorem 5

8.2.1 General Idea of the Proof

Let us assume that a, b, and c are three real numbers for which $a \le b \le c$. For these real numbers, we want to prove the inequalities between the three terms $a \,\&\, (b \,\&\, c)$, $b \,\&\, (a \,\&\, c)$, and $c \,\&\, (a \,\&\, b)$. Each of these terms describes the order in which we apply an "and" operation & to these three numbers: e.g., $a \,\&\, (b \,\&\, c)$ means that we first apply this operation to b and c, and then combine the result with a. To simplify notations, we will denote each of these three terms by the number which is the last to be combined; to be more precise, we will use the notations $t_a \stackrel{\text{def}}{=} a \,\&\, (b \,\&\, c)$, $t_b \stackrel{\text{def}}{=} b \,\&\, (a \,\&\, c)$, and $t_c \stackrel{\text{def}}{=} c \,\&\, (a \,\&\, b)$:

The formulas for $a \,\&\, b$, $a \,\&\, c$, and $b \,\&\, c$ depend on the relation between, correspondingly, $a+b$, $a+c$, $b+c$, and the number 1. Since we assumed that $a \le b \le c$, we have $a+b \le a+c \le b+c$. Thus, there are exactly four possible locations of number 1 in relation to these three sums:

I. the number 1 can be larger than the largest of these three sums; in this case, all three sums are ≤ 1, i.e.,

$$a + b \le a + c \le b + c \le 1;$$

II. the number 1 can be between $a+c$ and $b+c$; in this case,

$$a + b \le a + c \le 1 < b + c;$$

III. the number 1 can be between $a + b$ and $a + c$; in this case,

$$a + b \le 1 < a + c \le b + c;$$

IV. the number 1 can be smaller than the smallest of these three sums; in this case, all three sums are > 1, i.e.,

$$1 < a + b \le a + c \le b + c.$$

Let us consider these four cases one by one.

8.2.2 Case I

In this case, $a + b \le a + c \le b + c \le 1$, so $a + b \le 1$ and $b + c \le 1$. Hence, $b \,\&\, c = \beta \cdot b$, $a \,\&\, c = \beta \cdot a$, and $a \,\&\, b = \beta \cdot a$. Let us find the values of all three terms t_a, t_b, and t_c:

t_c: Since $a \,\&\, b \le a$ (by the properties of the new operation), and $a \le c$ (by our assumption), we conclude that $a \,\&\, b \le c$. Also, $(a \,\&\, b) + c = \beta \cdot a + c \le a + c \le 1$, so

$$(a \,\&\, b) \,\&\, c = \beta \cdot (a \,\&\, b) = \beta \cdot (\beta \cdot a) = \beta^2 \cdot a.$$

t_b: Similarly, $(a \,\&\, c) \le a \le b$, and $(a \,\&\, c) + b = \beta \cdot a + b \le a + b \le 1$, so

$$(a \,\&\, c) \,\&\, b = \beta \cdot (a \,\&\, c) = \beta \cdot (\beta \cdot a) = \beta^2 \cdot a.$$

t_a: Finally, $(b \,\&\, c) + a = \beta \cdot b + a \le a + b \le 1$, so

$$(b \,\&\, c) \,\&\, a = \beta \cdot \min(\beta \cdot b, a) = \min(\beta^2 \cdot b, \beta \cdot a).$$

Now we are ready to prove the desired inequalities:

$t_c \le t_b$: We have shown even that $t_b = (a \,\&\, c) \,\&\, b = (a \,\&\, b) \,\&\, c = t_c$.

$t_b \le t_a$: Since $b \ge a$, we have $\beta^2 \cdot b \ge \beta^2 \cdot a$; clearly, since $\beta < 1$, we have $\beta > \beta^2$, hence $\beta \cdot a \ge \beta^2 \cdot a$. Hence, $\min(\beta^2 \cdot b, \beta \cdot a) \ge \beta^2 \cdot a$.

Thus, for Case I, the inequalities are proven.

8.2.3 Case II

In this case, $a + b \le a + c \le 1$, so $a \,\&\, c = \beta \cdot a$ and $a \,\&\, b = \beta \cdot a$. On the other hand, since $b + c \ge 1$ and $b \le c$, we have $b \,\&\, c = \beta \cdot b + (1 - \beta) \cdot (b + c - 1) \ge \beta \cdot b$. Let us find the values of the three terms t_a, t_b, and t_c:

t_c: Here, $(a \,\&\, b) \le a \le c$ and $(a \,\&\, b) + c = \beta \cdot a + c \le a + c \le 1$, so

$$(a \,\&\, b) \,\&\, c = \beta \cdot (a \,\&\, b) = \beta^2 \cdot a.$$

t_b: Similarly, $(a \,\&\, c) \le a \le b$ and $(a \,\&\, c) + b = \beta \cdot a + b \le a + b \le 1$, so

$$(a \,\&\, c) \,\&\, b = \beta \cdot (a \,\&\, c) = \beta^2 \cdot a.$$

t_a: Finally, since $b \,\&\, c \ge \beta \cdot b$, and & is a monotonic operation, we can conclude that $(b \,\&\, c) \,\&\, a \ge (\beta \cdot b) \,\&\, a$. We have $\beta \cdot b + a \le a + b \le 1$, so

$$(\beta \cdot b) \,\&\, a = \beta \cdot \min(\beta \cdot b, a) = \min(\beta^2 \cdot b, \beta \cdot a)$$

and

$$(b \,\&\, c) \,\&\, a \ge (\beta \cdot b) \,\&\, a = \min(\beta^2 \cdot b, \beta \cdot a).$$

Now we are ready to prove the desired inequalities:

$t_c \le t_b$: We have shown that $(a \,\&\, c) \,\&\, b = (a \,\&\, b) \,\&\, c$.

$t_b \le t_a$: In proving Case I, we have already shown that $\min(\beta^2 \cdot b, \beta \cdot a) \ge \beta^2 \cdot a$, hence $t_a \ge \min(\beta^2 \cdot b, \beta \cdot a) \ge \beta^2 \cdot a = t_b$ and $t_b \le t_a$.

Thus, for Case II, the inequalities are proven as well.

8.2.4 Case III

Here, $a + b \le 1$, so $a \,\&\, b = \beta \cdot a$. Since $a + c \ge 1$ and $b + c \ge 1$, we have

$$a \,\&\, c = \beta \cdot a + (1 - \beta) \cdot (a + c - 1) =$$

$$\beta \cdot a + (1 - \beta) \cdot a + (1 - \beta) \cdot c - (1 - \beta) = a + (1 - \beta) \cdot c - (1 - \beta)$$

and similarly, $b \,\&\, c = b + (1 - \beta) \cdot c - (1 - \beta)$. Let us find the values of the three terms t_a, t_b, and t_c:

t_c: Here, $(a \,\&\, b) \,\&\, c = (\beta \cdot a) \,\&\, c$. Since $a \le c$, we have $\beta \cdot a \le c$. Hence, the expression for this term depends on whether $\beta \cdot a + c \le 1$ or $\beta \cdot a + c > 1$:

a) If $\beta \cdot a + c \le 1$, then $(a \,\&\, b) \,\&\, c = (\beta \cdot a) \,\&\, c = \beta^2 \cdot a$.

b) If $\beta \cdot a + c > 1$, then $(a \,\&\, b) \,\&\, c = (\beta \cdot a) \,\&\, c = \beta \cdot a + (1 - \beta) \cdot c - (1 - \beta)$.

t_b: We have $a \,\&\, c \le a \le b$ and $(a \,\&\, c) + b \le a + b \le 1$, hence

$$(a \,\&\, c) \,\&\, b = \beta \cdot (a \,\&\, c) = \beta \cdot a + \beta \cdot (1 - \beta) \cdot c - \beta \cdot (1 - \beta).$$

t_a: Finally, since $b \,\&\, c \le b$, we have $(b \,\&\, c) + a \le b + a \le 1$. Therefore, the expression for this third term depends on whether $b \,\&\, c = b + (1 - \beta) \cdot c - (1 - \beta) \le a$ or $b + (1 - \beta) \cdot c - (1 - \beta) > a$:

a) If $b + (1-\beta)\cdot c - (1-\beta) \le a$, then

$$(b \,\&\, c) \,\&\, a = \beta \cdot (b \,\&\, c) = \beta \cdot b + \beta \cdot (1-\beta) \cdot c - \beta \cdot (1-\beta).$$

b) If $b + (1-\beta)\cdot c - (1-\beta) > a$, then $(b \,\&\, c) \,\&\, a = \beta \cdot a$.

Let us now prove the inequalities.

$t_c \le t_b$: First, we will prove that $(a \,\&\, b) \,\&\, c \le (a \,\&\, c) \,\&\, b$. We will prove this inequality for both possible expression for $(a \,\&\, b) \,\&\, c$:

a) If $\beta \cdot a + c \le 1$, then $(a \,\&\, b) \,\&\, c = \beta^2 \cdot a$. On the other hand, $(a \,\&\, c) \,\&\, b = \beta \cdot (a \,\&\, c)$ and since

$$a \,\&\, c = \beta \cdot a + (1-\beta) \cdot (a + c - 1) \ge \beta \cdot a,$$

and $\beta \ge \beta^2$, we conclude that

$$(a \,\&\, c) \,\&\, b = \beta \cdot (a \,\&\, c) \ge \beta \cdot a \ge \beta^2 \cdot a = (a \,\&\, b) \,\&\, c.$$

b) If $\beta \cdot a + c > 1$, then

$$(a \,\&\, b) \,\&\, c = (\beta \cdot a) \,\&\, c = \beta \cdot a + (1-\beta) \cdot c - (1-\beta) =$$

$$\beta \cdot a - (1-\beta) \cdot (1-c).$$

On the other hand,

$$(a \,\&\, c) \,\&\, b = \beta \cdot a + \beta \cdot (1-\beta) \cdot c - \beta \cdot (1-\beta) = \beta \cdot a - \beta \cdot (1-\beta) \cdot (1-c).$$

Since $0 < \beta < 1$, we have $\beta \cdot (1-\beta) \cdot c \le (1-\beta) \cdot c$. Thus,

$$\beta \cdot a - (1-\beta) \cdot (1-c) \le \beta \cdot a - \beta \cdot (1-\beta) \cdot (1-c),$$

i.e., $(a \,\&\, b) \,\&\, c \le (a \,\&\, c) \,\&\, b$.

So, this inequality is proven for both cases.

$t_b \le t_a$: Let us now prove the second inequality $(a \,\&\, c) \,\&\, b \le (b \,\&\, c) \,\&\, a$. To prove this inequality, we will also consider two possible expressions for $(b \,\&\, c) \,\&\, a$:

a) If $b \,\&\, c = b + (1-\beta) \cdot c - (1-\beta) \le a$, then

$$(b \,\&\, c) \,\&\, a = \beta \cdot (b \,\&\, c) = \beta \cdot b + \beta \cdot (1-\beta) \cdot c - \beta \cdot (1-\beta).$$

Since $b \ge a$, we have

$$(b \,\&\, c) \,\&\, a = \beta \cdot b + \beta \cdot (1-\beta) \cdot c - \beta \cdot (1-\beta) \ge$$

$$\beta \cdot a + \beta \cdot (1-\beta) \cdot c - \beta \cdot (1-\beta) = (a \,\&\, c) \,\&\, b.$$

b) If $b \,\&\, c = b + (1-\beta)\cdot c - (1-\beta) > a$, then $(b \,\&\, c) \,\&\, a = \beta \cdot a$, and

$$(a \,\&\, c) \,\&\, b = \beta \cdot a + \beta \cdot (1-\beta) \cdot c - \beta \cdot (1-\beta) =$$

$$\beta \cdot a - \beta \cdot (1-\beta) \cdot (1-c).$$

Since $c \le 1$, we have

$$(b \,\&\, c) \,\&\, a = \beta \cdot a \ge \beta \cdot a - \beta \cdot (1-\beta) \cdot (1-c) = (a \,\&\, c) \,\&\, b.$$

So, this inequality is also proven for both possible cases.

8.2.5 Case IV

In this case, all three sums $a+b$, $a+c$, and $b+c$ are greater than 1, so $a \,\&\, b = a+(1-\beta)\cdot b-(1-\beta)$, $a \,\&\, c = a+(1-\beta)\cdot c-(1-\beta)$, and $b \,\&\, c = b+(1-\beta)\cdot c-(1-\beta)$. Before we start computing the values of the terms t_a, t_b, and t_c, we want to make some preliminary analysis:

- The value of $t_a = (b \,\&\, c) \,\&\, a$ depends on whether $(b \,\&\, c) + a \le 1$, i.e., whether $b + (1-\beta)\cdot c - (1-\beta) + a \le 1$. If we move terms which do not contain a, b, or c to the right hand-side, and rearrange terms which do contain a, b, or c, in alphabetic order, we get an equivalent inequality $a + b + (1-\beta)\cdot c \le 2-\beta$.
- Similarly, the value of $t_b = (a \,\&\, c) \,\&\, b$ depends on whether $(a \,\&\, c) + b \le 1$, i.e., whether $a + (1-\beta)\cdot c - (1-\beta) + b \le 1$, which is also equivalent to the same inequality $a + b + (1-\beta)\cdot c \le 2-\beta$.
- Finally, the value of $t_c = (a \,\&\, b) \,\&\, c$ depends on whether $(a \,\&\, b) + c \le 1$, i.e., whether $a + (1-\beta)\cdot b - (1-\beta) + c \le 1$, which is equivalent to the inequality $a + (1-\beta)\cdot b + c \le 2-\beta$.

So, to find the expressions for t_a, t_b, and t_c, we must know where $2-\beta$ stands in comparison with $a+b+(1-\beta)\cdot c$ and $a+(1-\beta)\cdot b+c$. Since $b \le c$, we have $\beta \cdot b \le \beta \cdot c$, hence

$$a+b+(1-\beta)\cdot c = (a+b+c) - \beta\cdot c \le (a+b+c) - \beta \cdot b = a+(1-\beta)\cdot b + c.$$

Due to this inequality, we have exactly three possibilities:

A. the number $2-\beta$ can be larger than the largest of the above two expressions; in this case, both expressions are $\le 2-\beta$, i.e.,

$$a+b+(1-\beta)\cdot c \le a+(1-\beta)\cdot b+c \le 2-\beta;$$

B. the number $2-\beta$ is in between the above two expressions; in this case,

$$a+b+(1-\beta)\cdot c \le 2-\beta < a+(1-\beta)\cdot b+c;$$

C. the number $2-\beta$ is smaller than the smallest of the above two expressions; in this case, both expressions are $\ge 2-\beta$, i.e.,

$$2-\beta < a+b+(1-\beta)\cdot c \le a+(1-\beta)\cdot b+c.$$

We will prove the inequalities by analyzing these three cases one by one.

8.2.6 Case IV, Subcase A

In this case, $a+b+(1-\beta)\cdot c \le a+(1-\beta)\cdot b+c \le 2-\beta$, hence, $(a\,\&\,b)+c \le 1$, $(a\,\&\,c)+b \le 1$, and $(b\,\&\,c)+a \le 1$.

t_c: Since $a\,\&\,b \le a$ (by the properties of the new operation), and $a \le c$ (by our assumption), we conclude that $a\,\&\,b \le c$. Since $(a\,\&\,b)+c \le 1$, we conclude that

$$(a\,\&\,b)\,\&\,c = \beta\cdot(a\,\&\,b) = \beta\cdot a+\beta\cdot(1-\beta)\cdot b-\beta\cdot(1-\beta).$$

t_b: Since $a\,\&\,c \le a \le b$, and $(a\,\&\,c)+b \le 1$, we have

$$(a\,\&\,c)\,\&\,b = \beta\cdot(a\,\&\,c) = \beta\cdot a+\beta\cdot(1-\beta)\cdot c-\beta\cdot(1-\beta).$$

t_a: Since $(b\,\&\,c)+a \le 1$, we have

$$(b\,\&\,c)\,\&\,a = \beta\cdot\min(b\,\&\,c,a) = \beta\cdot\min(b+(1-\beta)\cdot c-(1-\beta),a).$$

Let us now prove the desired inequalities:

$t_c \le t_b$: Since $b \le c$, we have

$$(a\,\&\,b)\,\&\,c = \beta\cdot a+\beta\cdot(1-\beta)\cdot b-\beta\cdot(1-\beta) \le$$

$$\beta\cdot a+\beta\cdot(1-\beta)\cdot c-\beta\cdot(1-\beta) = (a\,\&\,c)\,\&\,b.$$

$t_b \le t_a$: By the properties of the operation &, we have $a\,\&\,c \le a$; also, from $a \le b$ and monotonicity of &, we conclude that $a\,\&\,c \le b\,\&\,c$. Since $a\,\&\,c$ does not exceed the two numbers a and $b\,\&\,c$, it therefore cannot exceed the smallest of these two numbers, i.e., $a\,\&\,b \le \min(b,\&\,c),a)$. Multiplying both sides of this inequality by β, we conclude that

$$\beta\cdot(a\,\&\,c) \le \beta\cdot\min(b\,\&\,c,a),$$

hence

$$(a\,\&\,c)\,\&\,b = \beta\cdot(a\,\&\,c) \le \beta\cdot\min(b\,\&\,c,a) = (b\,\&\,c)\,\&\,a.$$

8.2.7 Case IV, Subcase B

In this case, $a+b+(1-\beta)\cdot c \le 2-\beta < a+(1-\beta)\cdot b+c$, hence, $(a \,\&\, b)+c > 1$, $(a \,\&\, c)+b \le 1$, and $(b \,\&\, c)+a \le 1$.

t_c: Since $a \,\&\, b \le a \le c$ and $(a \,\&\, b)+c > 1$, we conclude that

$$(a \,\&\, b) \,\&\, c = (a \,\&\, b) + (1-\beta)\cdot c - (1-\beta) =$$

$$a + (1-\beta)\cdot b + (1-\beta)\cdot c - 2\cdot(1-\beta).$$

t_b: Since $a \,\&\, c \le a \le b$, and $(a \,\&\, c)+b \le 1$, we have

$$(a \,\&\, c) \,\&\, b = \beta\cdot(a \,\&\, c) = \beta\cdot a + \beta\cdot(1-\beta)\cdot c - \beta\cdot(1-\beta).$$

t_a: Since $(b \,\&\, c)+a \le 1$, we have

$$(b \,\&\, c) \,\&\, a = \beta\cdot\min(b \,\&\, c, a) = \beta\cdot\min(b+(1-\beta)\cdot c-(1-\beta), a).$$

Let us now prove the desired inequalities:

$t_c \le t_b$: Indeed,

$$t_c - t_b = (a + (1-\beta)\cdot b + (1-\beta)\cdot c - 2\cdot(1-\beta)) -$$

$$(\beta\cdot a + \beta\cdot(1-\beta)\cdot c - \beta\cdot(1-\beta)) =$$

$$(1-\beta)\cdot a + (1-\beta)\cdot b + (1-\beta)^2\cdot c - (2-\beta)\cdot(1-\beta) =$$

$$(1-\beta)\cdot(a + b + (1-\beta)\cdot c - (2-\beta)).$$

We know that $\beta < 1$, so $1-\beta > 0$. Also, in this case IV.B, we have $a+b+(1-\beta)\cdot c-(2-\beta) \le 0$; hence, $t_c - t_b \le 0$, i.e., $t_c \le t_b$.

$t_b \le t_a$: This inequality is proven exactly as in the case IV.A.

8.2.8 Case IV, Subcase C

In this case, $2-\beta < a+b+(1-\beta)\cdot c \le a+(1-\beta)\cdot b+c$, hence, $(a \,\&\, b)+c > 1$, $(a \,\&\, c)+b > 1$, and $(b \,\&\, c)+a > 1$.

t_c: Since $a \,\&\, b \le a \le c$ and $(a \,\&\, b)+c > 1$, we conclude that

$$(a \,\&\, b) \,\&\, c = (a \,\&\, b) + (1-\beta)\cdot c - (1-\beta) =$$

$$a + (1-\beta)\cdot b + (1-\beta)\cdot c - 2\cdot(1-\beta).$$

t_b: Since $a \,\&\, c \le a \le b$ and $(a \,\&\, c)+b > 1$, we conclude that

$$(a \,\&\, c) \,\&\, b = (a \,\&\, c) + (1-\beta)\cdot b - (1-\beta) =$$

$$a + (1-\beta)\cdot b + (1-\beta)\cdot c - 2\cdot(1-\beta).$$

t_a: Since $(b \,\&\, c) + a > 1$, the expression for t_a depends on whether $b \,\&\, c \le a$, i.e., on whether $b + (1-\beta) \cdot c - (1-\beta) \le a$:

a) If $b \,\&\, c = b + (1-\beta) \cdot c - (1-\beta) \le a$, then

$$(b \,\&\, c) \,\&\, a = (b \,\&\, c) + (1-\beta) \cdot a - (1-\beta) =$$

$$(1-\beta) \cdot a + b + (1-\beta) \cdot c - 2 \cdot (1-\beta).$$

b) If $b \,\&\, c = b + (1-\beta) \cdot c - (1-\beta) > a$, then

$$(b \,\&\, c) \,\&\, a = a + (1-\beta) \cdot (b \,\&\, c) - (1-\beta) =$$

$$a + (1-\beta) \cdot b + (1-\beta)^2 \cdot c - (1-\beta)^2 - (1-\beta).$$

Let us now prove the desired inequalities:

$t_c \le t_b$: Indeed, in this case, $t_b = t_c$.

$t_b \le t_a$: We will prove that this inequality holds in both cases a) and b):

a) In this case,

$$t_a - t_b = ((1-\beta)c \cdot a + b + (1-\beta) \cdot c - 2 \cdot (1-\beta)) -$$

$$(a + (1-\beta) \cdot b + (1-\beta) \cdot c - 2 \cdot (1-\beta)) =$$

$$-\beta \cdot a + \beta \cdot b = \beta \cdot (b - a) \ge 0,$$

so $t_a \ge t_b$.

b) In this case,

$$t_a - t_b = (a + (1-\beta) \cdot b + (1-\beta)^2 \cdot c - (1-\beta)^2 - (1-\beta)) -$$

$$(a + (1-\beta) \cdot b + (1-\beta) \cdot c - 2 \cdot (1-\beta)) =$$

$$-\beta \cdot (1-\beta) \cdot c + \beta \cdot (1-\beta) = \beta \cdot (1-\beta) \cdot (1-c) \ge 0,$$

so also $t_a \ge t_b$.

The theorem is proven.

8.3 Proof of Theorem 3

8.3.1 General Idea of the Proof

We want to prove that the maximum (over all real numbers a, b, and c) of the absolute value $|(a \,\&\, b) \,\&\, c - a \,\&\, (b \,\&\, c)|$ of the difference $(a \,\&\, b) \,\&\, c - a \,\&\, (b \,\&\, c)$ between different "and"-combinations of these numbers, is equal to

$$M \stackrel{\text{def}}{=} \frac{\alpha \cdot (1-\alpha)}{2 + \alpha \cdot (1-\alpha)} = \frac{\beta \cdot (1-\beta)}{2 + \beta \cdot (1-\beta)}.$$

From Theorem 5, we know that for arbitrary three numbers, the possible combinations always appear in a certain order: namely, if we order the original numbers in the increasing order $a \le b \le c$, then we have

$$t_a = a \,\&\, (b \,\&\, c) \ge t_b = b \,\&\, (a \,\&\, c) \ge t_c = c \,\&\, (a \,\&\, b).$$

Thus, the largest possible difference between the possible "and"-combinations is equal to

$$t_a - t_c = a \,\&\, (b \,\&\, c) - c \,\&\, (a \,\&\, b).$$

Thus, to prove Theorem 3, it is sufficient to prove that the maximum of the difference $t_c - t_a$ over all possible values $a \le b \le c$ is equal to M.

The fact that the difference $t_a - t_c$ can take the value M can be easily shown by the following example:

$$a_0 \stackrel{\text{def}}{=} \frac{1}{2+\beta\cdot(1-\beta)}; \quad b_0 \stackrel{\text{def}}{=} 1 - a_0 = \frac{1+\beta\cdot(1-\beta)}{2+\beta\cdot(1-\beta)};$$

$$c_0 \stackrel{\text{def}}{=} 1 - \beta\cdot a_0 = \frac{2-\beta^2}{2+\beta\cdot(1-\beta)}.$$

(In particular, for $\alpha = 0.5$ and $\beta = 1 - \alpha = 0.5$, we have $M = 1/9$ and

$$a_0 = \frac{4}{9}; \quad b_0 = \frac{5}{9}; \quad c_0 = \frac{7}{9}.\Big)$$

Let us show that for these values, $t_a - t_c = M$. Indeed, here, $a_0 < 0.5$ hence $b_1 = 1 - a_0 > 0.5$, so $a_0 < b_0$. Also, since $\beta < 1$, we have $c_0 = 1 - \beta\cdot a_0 > b_0 = 1 - a_0$, so $a_0 < b_0 < c_0$.

Since $a_0 + b_0 = 1$, and $a_0 < b_0 < c_0$, we have $a_0 + c_0 > 1$ and $b_0 + c_0 > 1$. Thus, $a_0 \,\&\, b_0 = \beta\cdot a_0$ and

$$b_0 \,\&\, c_0 = b_0 + (1-\beta)\cdot c_0 - (1-\beta) = 1 - a_0 + (1-\beta)\cdot(1-\beta\cdot a_0) - (1-\beta) =$$

$$1 - a_0 + (1-\beta) - \beta\cdot(1-\beta)\cdot a_0 - (1-\beta) = 1 - a_0 - \beta\cdot(1-\beta)\cdot a_0 - (1-\beta) =$$

$$1 - \frac{1+\beta\cdot(1-\beta)}{2+\beta\cdot(1-\beta)} = \frac{1}{2+\beta\cdot(1-\beta)} = a_0.$$

Now we can compute the values t_a and t_c and the difference between them:

t_c: Here, $a_0 \,\&\, c_0 \le a_0 \le b_0$. Since $(a_0 \,\&\, b_0) = \beta\cdot a_0$, we have $(a_0 \,\&\, b_0) + c_0 = \beta\cdot a_0 + c_0 = 1$, so

$$t_c = (a_0 \,\&\, b_0) \,\&\, c_0 = \beta\cdot(a_0 \,\&\, b_0) = \beta^2\cdot a_0.$$

t_a: Here, $(b_0 \,\&\, c_0) = a_0$, so $a_0 \le b_0 \,\&\, c_0$, and $(b_0 \,\&\, c_0) + a_0 = 2a_0 < 1$, hence

$$t_a = a_0 \,\&\, (b_0 \,\&\, c_0) = \beta\cdot a_0.$$

Hence,

$$t_a - t_c = \beta \cdot a_0 - \beta^2 \cdot a_0 = \beta \cdot (1-\beta) \cdot a_0 = \frac{\beta \cdot (1-\beta)}{2 + \beta \cdot (1-\beta)} = M.$$

To complete the proof, it is therefore sufficient to prove that the difference $t_a - t_c$ cannot exceed M. We will prove this by reduction to a contradiction by assuming that $t_a - t_c > M$ and by getting a contradiction. This contradiction will be different for the four cases I–IV considered in the proof of Theorem 5.

8.3.2 Case I

In this case, as we have shown in the proof of Theorem 5, $t_a = \min(\beta^2 \cdot b, \beta \cdot a)$ and $t_c = \beta^2 \cdot a$. Thus, from the assumption that $t_a - t_c > M$, we can conclude that $\beta^2 \cdot \beta - \beta^2 \cdot a > M$ and that $\beta \cdot a - \beta^2 \cdot a > M$.

The second of these inequalities is equivalent to $\beta \cdot (1-\beta) \cdot a > M$, i.e., to

$$a > \frac{M}{\beta \cdot (1-\beta)}.$$

By definition of M, we have

$$\frac{M}{\beta \cdot (1-\beta)} = \frac{1}{2 + \beta \cdot (1-\beta)} = a_0,$$

so this inequality leads to

$$a > a_0 = \frac{1}{2 + \beta \cdot (1-\beta).} \tag{5}$$

The first inequality $\beta^2 \cdot b - \beta^2 \cdot a = \beta^2 \cdot (b-a) > M$ is equivalent to

$$b - a > \frac{M}{\beta^2} = \frac{1-\beta}{\beta \cdot (2 + \beta \cdot (1-\beta))}. \tag{6}$$

From (5) and (6), we conclude that

$$a + b = (b-a) + 2a > \frac{1-\beta}{\beta \cdot (2 + \beta \cdot (1-\beta))} + \frac{2}{2 + \beta \cdot (1-\beta)} =$$

$$\frac{2\beta + (1-\beta)}{\beta \cdot (2 + \beta \cdot (1-\beta))} = \frac{1+\beta}{\beta \cdot (2 + \beta \cdot (1-\beta))}.$$

Since in Case I, $a + b \le 1$, we conclude that

$$\frac{1+\beta}{\beta \cdot (2 + \beta \cdot (1-\beta))} < 1,$$

i.e., that

$$1 + \beta < \beta \cdot (2 + \beta \cdot (1 - \beta)) = 2\beta + \beta^2 - \beta^3.$$

If we move β to the right-hand side and β^3 to the left-hand side, we get a simpler equivalent inequality

$$1 + \beta^3 < \beta + \beta^2.$$

This inequality can be further simplified if we divide its both sides by $1+\beta > 0$, resulting in the following:

$$1 - \beta + \beta^2 < \beta.$$

If we move β from the right-hand side to the left, we get $1-2\beta+\beta^2 = (1-\beta)^2 < 0$, which is impossible.

The contradiction shows that in Case I, we cannot have $t_a - t_c > M$.

8.3.3 Case II

In this case, as we have shown, $t_c = \beta^2 \cdot a$. To get the desired contradiction, we must deduce the expression for $t_a = (b \,\&\, c) \,\&\, a$. Here, $b \,\&\, c = b + (1 - \beta) \cdot c - (1 - \beta)$. From $b \,\&\, c \le b$, we can conclude that $(b \,\&\, c) + a \le b + a \le 1$, so

$$t_a = \beta \cdot \min(b \,\&\, c, a) = \beta \cdot \min(b + (1 - \beta) \cdot c - (1 - \beta), a).$$

Thus, from the assumption that $t_a - t_c > M$, we can conclude that

$$\beta \cdot (b + (1 - \beta) \cdot c - (1 - \beta)) - \beta^2 \cdot a > M \tag{7}$$

and

$$\beta \cdot a - \beta \cdot a^2 > M. \tag{8}$$

From (8), similarly to Case I, we can conclude that $a > a_0$. Since in Case II, we have $a+c \le 1$, we conclude that $c \le 1-a$; due to $a > a_0$, we have $1-a < 1-a_0$ and therefore,

$$c < 1 - a_0 = b_0 = \frac{1 + \beta \cdot (1 - \beta)}{2 + \beta \cdot (1 - \beta)}.$$

From $b \le c$, we can now deduce that $b < b_0$.

From the inequality (7), by dividing its both sides by β, we conclude that

$$b + (1 - \beta) \cdot c - (1 - \beta) - \beta \cdot a > \frac{M}{\beta} = \frac{1 - \beta}{2 + \beta \cdot (1 - \beta)}. \tag{9}$$

On the other hand, since $b < b_0$, $c < b_0$, and $a > a_0$, we conclude that

$$b + (1 - \beta) \cdot c - (1 - \beta) - \beta \cdot a < b_0 + (1 - \beta) \cdot b_0 - (1 - \beta) - \beta \cdot a_0.$$

Substituting $b_0 = 1 - a_0$ into this inequality, we get

$$b + (1 - \beta) \cdot c - (1 - \beta) - \beta \cdot a < 1 - a_0 + (1 - \beta) \cdot (1 - a_0) - (1 - \beta) - \beta \cdot a_0.$$

Combining together terms which contain a_0 and terms which do not contain a_0, and substituting the expression for a_0, we conclude that

$$b+(1-\beta)\cdot c-(1-\beta)-\beta\cdot a < (1+1-\beta-1+\beta)+a_0\cdot(-1-1+\beta-\beta) = 1-2a_0 =$$

$$1-\frac{2}{2+\beta\cdot(1-\beta)} = \frac{\beta\cdot(1-\beta)}{2+\beta\cdot(1-\beta)}. \tag{10}$$

Comparing (9) and (10), we conclude that

$$\frac{1-\beta}{2+\beta\cdot(1-\beta)} < b+(1-\beta)\cdot c-(1-\beta)-\beta\cdot a < \frac{\beta\cdot(1-\beta)}{2+\beta\cdot(1-\beta)},$$

hence

$$\frac{1-\beta}{2+\beta\cdot(1-\beta)} < \frac{\beta\cdot(1-\beta)}{2+\beta\cdot(1-\beta)}.$$

Multiplying both sides by the common denominator and dividing both sides by the common factor $1-\beta$ of both numerators, we conclude that $\beta > 1$, which contradicts to our assumption that $\beta < 1$.

The contradiction shows that in Case II, we cannot have $t_a - t_c > M$.

8.3.4 Case III

In this case, as we have shown in the proof of Theorem 5, $(b\,\&\,c)+a \le 1$, hence

$$t_a = (b\,\&\,c)\,\&\,a = \beta\cdot\min(b\,\&\,c, a) = \beta\cdot\min(b+(1-\beta)\cdot c-(1-\beta), a).$$

For t_c, we had two possible expressions:

a) If $\beta\cdot a + c \le 1$, then $(a\,\&\,b)\,\&\,c = \beta^2\cdot a$.

b) If $\beta\cdot a + c > 1$, then $(a\,\&\,b)\,\&\,c = \beta\cdot a+(1-\beta)\cdot c-(1-\beta)$.

Let us show that in both cases, the assumption $t_a - t_c > M$ leads to a contradiction.

8.3.5 Case III, Subcase a)

In this case, from $t_a - t_c = t_a - \beta^2\cdot a > M$, we can conclude that $\beta\cdot a - \beta^2\cdot a > M$ – from which, as we have shown in Case II, we can deduce $a > a_0$ – and that

$$\beta\cdot b+\beta\cdot(1-\beta)\cdot c-\beta\cdot(1-\beta)-\beta^2\cdot a > M.$$

Dividing both sides of this inequality by β, and taking into consideration that $M = \beta\cdot(1-\beta)\cdot a_0$, we conclude that

$$b+(1-\beta)\cdot c-(1-\beta)-\beta\cdot a > (1-\beta)\cdot a_0. \tag{11}$$

Since in Case III, $a + b \le 1$, we conclude that $b \le 1 - a$, so from $a > a_0$, we can deduce that $b \le 1 - a < 1 - a_0 = b_0$.

In subcase a), we have $\beta \cdot a + c \le 1$, hence $c \le 1 - \beta \cdot a$. So, from $a > a_0$, we can deduce that $c \le 1 - \beta \cdot a < 1 - \beta \cdot a_0 = c_0$. So, $a > a_0$, $b < b_0$, and $c < c_0$. Hence,

$$\beta \cdot b + \beta \cdot (1-\beta) \cdot c - \beta \cdot (1-\beta) - \beta^2 \cdot a < \beta \cdot b_0 + \beta \cdot (1-\beta) \cdot c_0 - \beta \cdot (1-\beta) - \beta^2 \cdot a_0.$$

Substituting into this inequality the expressions $b_0 = 1 - a_0$ and $c_0 = 1 - \beta \cdot a_0$, and combining terms together with a_0 and without a_0, we get

$$b + (1-\beta) \cdot c - (1-\beta) - \beta \cdot a < b_0 + (1-\beta) \cdot c_0 - (1-\beta) - \beta \cdot a_0 =$$

$$(1 - a_0) + (1-\beta) \cdot (1 - \beta \cdot a_0) - (1-\beta) - \beta \cdot a_0 =$$

$$(1 + 1 - \beta - 1 + \beta) + a_0 \cdot (-1 - \beta \cdot (1-\beta) - \beta) = 1 + a_0 \cdot (-1 - 2\beta + \beta^2). \quad (12)$$

From (11) and (12), we can conclude that

$$(1-\beta) \cdot a_0 < b + (1-\beta) \cdot c - (1-\beta) - \beta \cdot a < 1 + a_0 \cdot (-1 - 2\beta + \beta^2);$$

hence,

$$(1-\beta) \cdot a_0 < 1 + a_0 \cdot (-1 - 2\beta + \beta^2).$$

Moving terms containing a_0 to the left-hand side, we conclude that

$$a_0 \cdot (1 - \beta + 1 + 2\beta - \beta^2) < 1,$$

i.e.,

$$a_0 \cdot (2 + \beta \cdot (1-\beta)) < 1. \quad (13)$$

We know that

$$a_0 = \frac{1}{2 + \beta \cdot (1-\beta)},$$

so (13) leads to $1 < 1$ – a contradiction.

8.3.6 Case III, Subcase b)

In this case, from $t_a - t_c = t_a - (\beta \cdot a + (1-\beta) \cdot c - (1-\beta)) > M$, and from the fact that t_a is the minimum of two expressions:

$$t_a = \min(\beta \cdot b + \beta \cdot (1-\beta) \cdot c - \beta \cdot (1-\beta), \beta \cdot a),$$

we can conclude that the following two inequalities hold:

$$\beta \cdot b + \beta \cdot (1-\beta) \cdot c - \beta \cdot (1-\beta) - (\beta \cdot a + (1-\beta) \cdot c - (1-\beta)) > M; \quad (14)$$

$$\beta \cdot a - (\beta \cdot a + (1-\beta) \cdot c - (1-\beta)) > M. \quad (15)$$

The inequality (15) leads to

$$-(1-\beta)\cdot c+(1-\beta)>M.$$

Dividing both sides of this inequality by $1-\beta$ and taking into consideration that $M=\beta\cdot(1-\beta)\cdot a_0$, we conclude that $-c+1>\beta\cdot a_0$, i.e., that $c<1-\beta\cdot a_0$. Since c_0 was defined as $1-\beta\cdot a_0$, we conclude that $c<c_0$.

Subcase b) corresponds to the inequality $\beta\cdot a+c>1$, so $\beta\cdot a>1-c$; since $c<c_0$, we have $\beta\cdot a>1-c>1-c_0=\beta\cdot a_0$, hence $a>a_0$.

In Case III, $a+b\le 1$, so $b\le 1-a$, hence $b\le 1-a<1-a_0=b_0$. So, $a>a_0$, $b<b_0$, and $c<c_0$.

The inequality (14) leads to

$$\beta\cdot b-(1-\beta)^2\cdot c-\beta\cdot a+(1-\beta)^2>M. \tag{16}$$

If we replace, in (16), c by a smaller value $1-\beta\cdot a$, we get a valid inequality

$$\beta\cdot b-(1-\beta)^2\cdot(1-\beta\cdot a)-\beta\cdot a+(1-\beta)^2=$$

$$\beta\cdot b-(1-\beta)^2+\beta\cdot(1-\beta)^2\cdot a-\beta\cdot a+(1-\beta)^2=\beta\cdot b-\beta^2\cdot(2-\beta)\cdot a>M,$$

i.e.,

$$\beta\cdot b-\beta^2\cdot(2-\beta)\cdot a>M.$$

Dividing both sides of the resulting inequality by β and taking into consideration that $M=\beta\cdot(1-\beta)\cdot a_0$, we conclude that

$$b-(2\beta-\beta^2)\cdot a>(1-\beta)\cdot a_0. \tag{17}$$

On the other hand, since $b<b_0=1-a_0$ and $a>a_0$, we conclude that

$$b-(2\beta-\beta^2)\cdot a<b_0-(2\beta-\beta^2)\cdot a_0=$$

$$1-a_0-(2\beta-\beta^2)\cdot a_0=1+(\beta^2-2\beta-1)\cdot a_0. \tag{18}$$

By definition of a_0, we have $1=(1+\beta\cdot(1-\beta))\cdot a_0$, hence

$$1+(\beta^2-2\beta-1)\cdot a_0=(2+\beta-\beta^2)\cdot a_0+(\beta^2-2\beta-1)\cdot a_0=(1-\beta)\cdot a_0,$$

so (18) implies that

$$b-(2\beta-\beta^2)\cdot a<(1-\beta)\cdot a_0.$$

This inequality contradicts to the previously proven inequality (17).

8.3.7 Case IV, Subcase A

Case IV means that

$$a + b > 1, \tag{19}$$

and therefore, that

$$a + c > 1 \tag{20}$$

and

$$b + c > 1. \tag{21}$$

Subcase A means that

$$a + (1 - \beta) \cdot b + c \le 2 - \beta. \tag{22}$$

In the proof of Theorem 5, we have shown that in Case IV, Subcase A,

$$t_c = \beta \cdot a + \beta \cdot (1 - \beta) \cdot b - \beta \cdot (1 - \beta), \tag{23}$$

and that t_a is the minimum of two expressions:

$$t_a = \min(\beta \cdot b + \beta \cdot (1 - \beta) \cdot c - \beta \cdot (1 - \beta), \beta \cdot a). \tag{24}$$

Thus, the inequality $t_a - t_c > M$ is equivalent to the following two inequalities:

$$\beta \cdot b + \beta \cdot (1 - \beta) \cdot c - \beta \cdot (1 - \beta) - (\beta \cdot a + \beta \cdot (1 - \beta) \cdot b - \beta \cdot (1 - \beta)) > M; \tag{25}$$

$$\beta \cdot a - (\beta \cdot a + \beta \cdot (1 - \beta) \cdot b - \beta \cdot (1 - \beta)) > M. \tag{26}$$

The inequality (26) leads to

$$-\beta \cdot (1 - \beta) \cdot b + \beta \cdot (1 - \beta) > M.$$

Dividing both sides of this inequality by $\beta \cdot (1 - \beta)$ and taking into consideration that $M = \beta \cdot (1 - \beta) \cdot a_0$, we conclude that $-b + 1 > a_0$, i.e., that $b < 1 - a_0 = b_0$ and $b < b_0$.

Since in Case IV, $a + b > 1$, we conclude that $a > 1 - b$, and since $b < b_0$, we have $a > 1 - b > 1 - b_0 = a_0$, i.e., $a > a_0$.

Subtracting (19) from (22), we conclude that $-\beta \cdot b + c \le 1 - \beta$. Moving the term $-\beta \cdot b$ to the right-hand side, we get $c \le 1 - \beta + \beta \cdot b$. We have already shown that $b < b_0$, hence $c \le 1 - \beta + \beta \cdot b < 1 - \beta + \beta \cdot b_0$. By definition of b_0 as $1 - a_0$, we get $c < 1 - \beta + \beta \cdot b_0 = 1 - \beta \cdot a_0$. The right-hand side of this equality is exactly the definition of c_0, so we conclude that

$$c < c_0. \tag{27}$$

Now, the inequality (25) leads to

$$-\beta \cdot a + \beta^2 \cdot b + \beta \cdot (1 - \beta) \cdot c > M.$$

Dividing both sides of this inequality by β and taking into consideration that $M = \beta \cdot (1-\beta) \cdot a_0$, we get

$$-a + \beta \cdot b + (1-\beta) \cdot c > (1-\beta) \cdot a_0.$$

Moving all the terms except for the term proportional to c to the right-hand side, we get

$$(1-\beta) \cdot c > a - \beta \cdot b + (1-\beta) \cdot a_0. \tag{28}$$

We know that $a > a_0$ and that $b < b_0 = 1 - a_0$. Therefore, from (28), we can conclude that

$$(1-\beta) \cdot c > a_0 - \beta \cdot (1-a_0) + (1-\beta) \cdot a_0 = (1+\beta+1-\beta) \cdot a_0 - \beta = 2a_0 - \beta. \tag{29}$$

From the definition of a_0 as

$$a_0 = \frac{1}{2 + \beta \cdot (1-\beta)},$$

we conclude that

$$2a_0 - \beta = \frac{2}{2 + \beta \cdot (1-\beta)} - \beta = \frac{2 - 2\beta - \beta^2 \cdot (1-\beta)}{2 + \beta \cdot (1-\beta)} = \frac{(1-\beta) \cdot (2-\beta^2)}{2 + \beta \cdot (1-\beta)}.$$

From the definition of c_0, we can now conclude that $2a_0 - \beta = (1-\beta) \cdot c_0$. Thus, the inequality (29) is equivalent to $(1-\beta) \cdot c > (1-\beta) \cdot c_0$, i.e., to $c > c_0$, which contradicts to (27).

8.3.8 Case IV, Subcase B

Case IV means the inequalities (19), (20), and (21) are all true, and Subcase B means that

$$a + b + (1-\beta) \cdot c \le 2 - \beta \tag{29a}$$

and

$$a + (1-\beta) \cdot b + c > 2 - \beta. \tag{29b}$$

In the proof of Theorem 5, we have shown that in Case IV, Subcase B,

$$t_c = a + (1-\beta) \cdot b + (1-\beta) \cdot c - 2 \cdot (1-\beta),$$

and that t_a is the minimum of two expressions:

$$t_a = \min(\beta \cdot b + \beta \cdot (1-\beta) \cdot c - \beta \cdot (1-\beta), \beta \cdot a).$$

Thus, the inequality $t_a - t_c > M$ is equivalent to the following two inequalities:

$$\beta \cdot b + \beta \cdot (1-\beta) \cdot c - \beta \cdot (1-\beta) - a - (1-\beta) \cdot b - (1-\beta) \cdot c + 2 \cdot (1-\beta) > M; \tag{30}$$

$$\beta \cdot a - a - (1-\beta) \cdot b - (1-\beta) \cdot c + 2 \cdot (1-\beta) > M. \tag{31}$$

By combining together terms proportional to a, we can simplify the inequality (31) into the following equivalent form:

$$-(1-\beta) \cdot a - (1-\beta) \cdot b - (1-\beta) \cdot c + 2 \cdot (1-\beta) > M.$$

Dividing both sides of this inequality by $1-\beta$ and taking into consideration that $M = \beta \cdot (1-\beta) \cdot a_0$, we get $-a - b - c + 2 > \beta \cdot a_0$. Moving terms a, b, and c to the right-hand side and $\beta \cdot a_0$ to the left-hand side, we get

$$a + b + c < 2 - \beta \cdot a_0. \tag{32}$$

Subtracting (19) from (31), we conclude that $c < 1 - \beta \cdot a_0$, i.e., by definition of c_0, that $c < c_0$.

Subtracting (29b) from (32), we get $\beta \cdot b < \beta - \beta \cdot a_0 = \beta \cdot (1 - a_0)$. By definition of b_0 as $1 - a_0$, we thus get $\beta \cdot b < \beta \cdot b_0$, hence $b < b_0$.

From $a + b > 1$, we can now conclude that $a > 1 - b$ and since $b < b_0$, that $a > 1 - b > 1 - b_0$, hence (by definition of $b_0 = 1 - a_0$), that $a > a_0$.

From (30), we conclude that

$$-a + (2\beta - 1) \cdot b - (1-\beta)^2 \cdot c + (2-\beta) \cdot (1-\beta) > M,$$

i.e., that

$$a < (2\beta - 1) \cdot b - (1-\beta)^2 \cdot c + (2-\beta) \cdot (1-\beta) - M. \tag{33}$$

On the other hand, from (29b), it follows that

$$a > -(1-\beta) \cdot b - c + (2-\beta). \tag{34}$$

The lower bound for a coming from the inequality (34) should be smaller than the upper bound for a which comes from the inequality (33), i.e., we should have

$$-(1-\beta) \cdot b - c + (2-\beta) < (2\beta - 1) \cdot b - (1-\beta)^2 \cdot c + (2-\beta) \cdot (1-\beta) - M.$$

Moving the terms containing b and c to the right-hand side and all the other terms to the left-hand side, we conclude that

$$(2-\beta) \cdot \beta + M < \beta \cdot b + \beta \cdot (2-\beta) \cdot c. \tag{35}$$

Dividing both sides of this inequality by β and taking into consideration that $M = \beta \cdot (1-\beta) \cdot a_0$, we conclude that

$$b + (2-\beta) \cdot c > 2 - \beta + (1-\beta) \cdot a_0. \tag{36}$$

On the other hand, we have already proven that $b > b_0 = 1 - a_0$ and $c < c_0 = 1 - \beta \cdot a_0$, hence

$$b + (2-\beta)\cdot c < b_0 + (2-\beta)\cdot c_0 = 1 - a_0 + (2-\beta)\cdot(1-\beta\cdot a_0) =$$

$$(1+2-\beta) + (-1-2\beta+\beta^2)\cdot a_0 = (3-\beta) + (-1-2\beta+\beta^2)\cdot a_0. \quad (37)$$

The lower bound for $b + (2-\beta)\cdot c$ coming from the inequality (36) should be smaller than the upper bound for this quantity which comes from the inequality (37), i.e., we should have

$$(2-\beta) + (1-\beta)\cdot a_0 < (3-\beta) + (-1-2\beta+\beta^2)\cdot a_0.$$

Moving all the terms proportional to a_0 to the left-hand side and all other terms to the right-hand side, we conclude that

$$(2+\beta-\beta^2)\cdot a_0 < 1. \quad (38)$$

However, by the definition of a_0, $(2+\beta-\beta^2)\cdot a_0 = 1$, which contradicts to (38).

8.3.9 Case IV, Subcase C

Case IV means the inequalities (19), (20), and (21) are all true, and Subcase C means that

$$a + b + (1-\beta)\cdot c > 2-\beta. \quad (39)$$

In the proof of Theorem 5, we have shown that in Case IV, Subcase C,

$$t_c = a + (1-\beta)\cdot b + (1-\beta)\cdot c - 2\cdot(1-\beta)$$

and

$$t_a = \beta\cdot\min(b\,\&\,c, a) + (1-\beta)\cdot((b\,\&\,c) + a - 1) =$$

$$\min(b\,\&\,c, +(1-\beta)\cdot a - (1-\beta), a + (1-\beta)\cdot(b\,\&\,c) - (1-\beta)) =$$

$$\min((1-\beta)\cdot a + b + (1-\beta)\cdot c - 2\cdot(1-\beta), a + (1-\beta)\cdot b + (1-\beta)^2\cdot c - (1-\beta)^2 - (1-\beta)).$$

Thus, the inequality $t_a - t_c > M$ leads to the following two inequalities:

$$(1-\beta)\cdot a + b + (1-\beta)\cdot c - 2\cdot(1-\beta) -$$

$$a - (1-\beta)\cdot b - (1-\beta)\cdot c + 2\cdot(1-\beta) > M; \quad (40)$$

$$a + (1-\beta)\cdot b + (1-\beta)^2\cdot c - (1-\beta)^2 - (1-\beta) -$$

$$a - (1-\beta)\cdot b - (1-\beta)\cdot c + 2\cdot(1-\beta) > M. \quad (41)$$

The inequality (41) is equivalent to

$$-\beta\cdot(1-\beta)\cdot c + \beta\cdot(1-\beta) > M.$$

Dividing both sides of this inequality by β and taking into consideration that $M = \beta \cdot (1-\beta) \cdot a_0$, we conclude that $-c+1 > a_0$, i.e., that $c < 1 - a_0$. By definition of b_0, this means that $c < b_0$.

Since $b \le c$, from $c > b_0$, we can also conclude that $b > b_0$.

From $a + b > 1$ (inequality (19)), we conclude that $a > 1 - b$. Since $b < b_0 = 1 - a_0$, we thus conclude that $a > 1 - b_0 = 1 - (1 - a_0) = a_0$, i.e., that $a > a_0$.

The inequality (40) leads to

$$-\beta \cdot a + \beta \cdot b > M.$$

Dividing both sides of this inequality by $\beta \cdot (1-\beta)$, we conclude that $b - a > (1-\beta) \cdot a_0$, i.e., that

$$a < b - (1-\beta) \cdot a_0.$$

Since we have shown that $b < b_0 = 1 - a_0$, we can therefore conclude that

$$a < 1 - a_0 - (1-\beta) \cdot a_0,$$

i.e.,

$$a < 1 - (2-\beta) \cdot a_0. \tag{42}$$

On the other hand, from (39), we conclude that

$$a > -b - (1-\beta) \cdot c + (2-\beta).$$

Since we have proven that $b < b_0 = 1 - a_0$ and $c < b_0 = 1 - a_0$, we can conclude that

$$a > -b_0 - (1-\beta) \cdot b_0 + (2-\beta) =$$
$$-(2-\beta) \cdot b_0 + (2-\beta) = (2-\beta) \cdot (1-b_0) = (2-\beta) \cdot a_0,$$

i.e.,

$$a > (2-\beta) \cdot a_0. \tag{43}$$

The lower bound for a coming from the inequality (43) should be smaller than the upper bound for a which comes from the inequality (42), i.e., we should have

$$(2-\beta) \cdot a_0 < 1 - (2-\beta) \cdot a_0.$$

Moving the negative term to the right-hand side, we get

$$(4 - 2\beta) \cdot a_0 < 1.$$

Multiplying both sides of this inequality by $2 + \beta - \beta^2$ and taking into consideration that (by definition of a_0) $(2 + \beta - \beta^2) \cdot a_0 = 1$, we conclude that $4 - 2\beta < 2 + \beta - \beta^2$. By moving all the terms to the left-hand side, we get the equivalent inequality $\beta^2 - 3\beta + 2 < 0$, i.e.,

$$(\beta - 1) \cdot (\beta - 2) < 0. \tag{44}$$

Since $\beta < 1$, we have $\beta - 1 < 0$ and $\beta - 2 < 0$, hence $(\beta - 1) \cdot (\beta - 2) > 0$ – a contradiction.

8.3.10 Conclusion

So, in all cases, the assumption that $|(a \,\&\, b) \,\&\, c - a \,\&\, (b \,\&\, c)| > M$ leads to a contradiction. Thus, the theorem is proven.

9 For Midpoint Operations, the Proof Can Be Simplified If We Use Interval Computations

9.1 What Are Interval Computations

For $\alpha = 0.5$, we can simplify this proof by using *interval computations* (see, e.g., [10, 15, 16, 30]). Namely, our goal is to find the maximum of the function $|(a \,\&\, b) \,\&\, c - a \,\&\, (b \,\&\, c)|$ when $a \in [0,1]$, $b \in [0,1]$, and $c \in [0,1]$. We know that the minimum of this function is 0: it is attained, e.g., if $a = b = c = 0$. Thus, what we are looking for is the *range* of the above function of three real variables.

Interval computations is a technique which allows us, given a function $y = f(x_1, \ldots, x_n)$ of several real variables and a "box" $B = \mathbf{x}_1 \times \ldots \times \mathbf{x}_n$, where $\mathbf{x}_i = [x_i^-, x_i^+]$, to compute either the range of the given function on the given box:

$$\mathbf{y} = f(\mathbf{x}_1, \ldots, \mathbf{x}_n = \{f(x_1, \ldots, x_n) \,|\, x_1 \in [x_1^-, x_1^+], \ldots, x_n \in [x_n^-, x_n^+]\},$$

or an interval $\mathbf{Y}$ which is guaranteed to contain the desired range, i.e., for which $\mathbf{y} \subseteq \mathbf{Y}$ (We cannot always compute the *exact* range because computing this exact range is intractable even for quadratic functions $f(x_1, \ldots, x_n)$: see, e.g., [17].)

This technique is based on the fact that in the computer, the computation of a function f consists of several elementary steps. For example, a compiler will translate the computation of the midpoint "and" operation

$$f(p_1, p_2) = \frac{1}{2} \cdot \max(p_1 + p_2 - 1, 0) + \frac{1}{2} \cdot \min(p_1, p_2)$$

into the following sequence of elementary steps (r_1, r_2, etc. denote the preliminary computation results):

- first, we compute $r_1 := p_1 + p_2$;
- then, we compute $r_2 := r_1 - 1$;
- compute $r_3 := \min(r_2, 0)$;
- compute $r_4 := (1/2) \cdot r_3$;
- compute $r_5 := \min(p_1, p_2)$;
- compute $r_6 := (1/2) \cdot r_5$;

- finally, compute the result as $y := r_4 + r_6$.

In this example, we have two input variables $x_1 = p_1$ and $x_2 = p_2$. In general, for each input variable x_i, we know the interval $\mathbf{x}_i = [x_1^-, x_1^+]$ of possible values. For each elementary step $h(a, b)$, if we know the intervals $\mathbf{a} = [a^-, a^+]$ and $\mathbf{b} = [b^-, b^+]$ of possible values for each of the input, then we can compute the interval $h(\mathbf{a}, \mathbf{b})$ of possible values of the results:

- $[a^-, a^+] + [b^-, b^+] = [a^- + b^-, a^+ + b^+]$;
- $[a^-, a^+] - [b^-, b^+] = [a^- - b^+, a^+ - b^-]$;
- $[a^-, a^+] \cdot [b^-, b^+] = [c^-, c^+]$, where:
  - $c^{=} \min(a^- \cdot b^-, a^- \cdot b^+, a^+ \cdot b^-, a^+ \cdot b^+,$
  - $c^+ = \max(a^- \cdot b^-, a^- \cdot b^+, a^+ \cdot b^-, a^+ \cdot b^+)$;
- $\min([a^-, a^+], [b^-, b^+]) = [\min(a^-, b^-), \min(a^+, b^+)]$;
- $\max([a^-, a^+], [b^-, b^+]) = [\max(a^-, b^-), \max(a^+, b^+)]$.

These formulas are called formulas of *interval arithmetic.*

So, to find an interval that contains the desired range, we follow the original algorithm step-by-step, on each step replacing the original elementary operation with real numbers by the corresponding operation of interval arithmetic.

In particular, if we want to know the range of the values of the function $f(p_1, p_2) = p_1 \& p_2$ when $p_1 \in \mathbf{p}_1$ and $p_2 \in \mathbf{p}_2$, we do the following:

- first, we compute $\mathbf{r}_1 := \mathbf{p}_1 + \mathbf{p}_2$;
- then, we compute $\mathbf{r}_2 := \mathbf{r}_1 - [1, 1]$;
- compute $\mathbf{r}_3 := \min(\mathbf{r}_2, [0, 0])$;
- compute $\mathbf{r}_4 := [0.5, 0.5] \cdot \mathbf{r}_3$;
- compute $\mathbf{r}_5 := \min(\mathbf{p}_1, \mathbf{p}_2)$;
- compute $\mathbf{r}_6 := [0.5, 0.5] \cdot \mathbf{r}_5$;
- finally, compute the result as $\mathbf{Y} := \mathbf{r}_4 + \mathbf{r}_6$.

It is easy to prove (by induction) that at any given moment of time, the result of this procedure is guaranteed to contain the result of the interval of possible values of the corresponding quantity.

It is also easy to show that this "naive" interval computation procedure sometimes overestimates. For example, for a function $f(x_1) = x_1 \cdot (1 - x_1)$ on the interval $[0, 1]$, the computational procedure consists of the following two steps:

- $r_1 := 1 - x_1$;
- $y := x_1 \cdot r_1$,

so we get the following estimate:

- $\mathbf{r}_1 := [1,1] - \mathbf{x}_1 = [1,1] - [0,1] = [1-1, 1-0] = [0,1]$;
- $\mathbf{Y} := \mathbf{x}_1 \cdot \mathbf{r}_1 = [0,1] \cdot [0,1] = [\min(0 \cdot 0, 0 \cdot 1, 1 \cdot 0, 1 \cdot 1), \max(0 \cdot 0, 0 \cdot 1, 1 \cdot 0, 1 \cdot 1)] = [0,1]$,

while the actual range is $\mathbf{y} = [0, 0.25] \subset \mathbf{Y} = [0,1]$.

To decrease the overestimation, we can use the following methodology of interval computations: we divide each interval $\mathbf{x}_i$ into several sub-intervals, thus dividing the original box into many sub-boxes; then, we estimate the range of the function over each of the subintervals, and then take the union of the resulting ranges as an estimate for the range over the whole original box.

If we are interested not only in the actual value of the maximum, but if we also want to know where exactly this maximum is attained, then we can use this sub-boxes as follows: if we have two subboxes B_1 and B_2 with range estimates $[m_1, M_1]$ and $[m_2, M_2]$, and $M_1 < m_2$, then we are guaranteed that an arbitrary value $f(x_1, \ldots, x_n)$ for $(x_1, \ldots, x_n)$ from the first subbox is smaller than every value from the second subbox. Thus, we can safely claim that the (global) maximum of the given function cannot be attained in the first subbox – hence, this first subbox can be safely removed from the list of possible location of the global maximum.

We used this idea to simplify our proof.

9.2 How We Used Interval Computations to Simplify the Proof for Midpoint Operation

In our proof, we considered four different cases I, II, III, and IV, which depended on the relation between 1 and the sums $a+b$, $a+c$, and $b+c$. In the above proof, for each of these four cases, we showed that the value of the desired function cannot exceed the bound described by the theorem (for $\alpha = \beta = 0.5$, this upper bound is $M = 1/9$).

To check whether the corresponding four parts of the proof are really necessary, we divided each original interval $[0,1]$ into 100 subintervals of length 0.01: $[0, 0.01]$, $[0.01, 0.02]$, etc. As a result of this subdivision, we get $100 \times 100 \times 1000 = 10^6$ sub-boxes. (At first, we started with dividing each interval $[0,1]$ into 10 subintervals, but this did not lead to any simplification of the proof.) For each of these subboxes, we applied the naive interval computations technique to estimate the range $[m_i, M_i]$ of the desired function $|(a \,\&\, b) \,\&\, c - a \,\&\, (b \,\&\, c)|$ on this subbox. Then, we eliminated all subboxes for which $M_i < 1/9$. (Thus, if a subbox has been discarded, this means that for each combination (a, b, c) from this subbox, the value of the desired function is $< 1/9$.)

As a result, out of the original million subboxes, we were left with only 80 possible locations of the global maximum. These subboxes were located in the following places:

- For b, the only possible subintervals turned out to be are $[0.54, 0.55]$, $[0.55, 0.56]$, $[0.56, 0.57]$, and $[0.57, 0.58]$, i.e., we can conclude that $b \in [0.54, 0.58]$.
- For a, the possible subintervals are:
  - either from the interval $a \in [0.43, 0.46]$, in which case $c \in [0.75, 0.79]$;
  - or from the interval $a \in [0.75, 0.79]$, in which case $c \in [0.43, 0.46]$.

If we sort these values in the increasing order, then we conclude that for the sorted variables, $a \in [0.43, 0.46]$, $b \in [0.54, 0.58]$, and $c \in [0.75, 0.79]$.

Since $a \in [0.43, 0.46]$ and $c \in [0.75, 0.79]$, the sum $a + c$ is guaranteed to belong to the interval $[0.43, 0.46] + [0.75, 0.79] = [1.18, 1.25]$, i.e., is guaranteed to be larger than 1. Thus, if for some values a, b, and c, we have $a + c < 1$, then we already know that for these values, the desired function cannot take a value $> 1/9$ (since this triple (a, b, c) belongs to the discarded subboxes, for which we have already shown that the value of the function is $< 1/9$).

To check that the desired function cannot take the values $> 1/9$, it is sufficient only to check 80 remaining subboxes. Since for these remaining subboxes, $a + c > 1$, there is no need to consider Cases I and II for which $a + c \leq 1$. So, we only have to prove the result for Cases III and IV.

Interval computations not only reduces the number of cases in half, it also simplified the proof of at least one of the cases – Case IV. Indeed, in the above proof, to prove the theorem for Case IV, we separately considered three subcases (A, B, and C) which correspond to the possible relation between $2 - \beta$ $(= 1.5$ for midpoint operations) and the expressions $a + (1 - \beta) \cdot b + c$ $(= a + 0.5 \cdot b + c)$ and $a + b + (1 - \beta) \cdot c$ $(= a + b + 0.5 \cdot c)$. By using the above-described guaranteed intervals, we can eliminate the need to consider some of these subcases in our proof. Indeed, within the above interval bounds for a, b, and c, the upper bound for $a + b + (1 - \beta) \cdot c = 1 + b + 0.5 \cdot c$ is equal to $0.46 + 0.58 + 0.5 \cdot 0.79 = 1.435 < 1.5$. Thus, to check that the value of the desired function cannot exceed $1/9$, we only need to consider cases when $a + b + 0.5 \cdot c < 1.5$. Thus, we can dismiss Subcase C when this inequality is not satisfied, and only consider Subcases A and B in our proof.

Thus, for the midpoint operations, the use of interval computations indeed eliminates more than half of the cases and thus, simplifies the proof. (We expect the same simplification to occur for other operations as well, when $\alpha \neq 0.5$.)

A further simplification emerges from observing that for each subcase, the problem of maximizing the difference $t_a - t_c$ is a problem of optimizing a linear function under constraints which are linear inequalities; in other words, this problem is a *linear programming* problem. It is known that for such problems, the optimum is always attained at one of the vertices. Each vertex can be obtained as follows: if we have n variables, then we need to select n inequalities, make them equalities, solve the corresponding system of n linear equations with n unknowns, and check that the remaining inequalities are still satisfied. This checking can be done automatically. Then, all we have to do is compute the values of the optimized function at different vertices and make sure that all these values do not exceed our bound M.

Acknowledgments

This work was supported in part by NASA under cooperative agreement NCC5-209, by NSF grants No. DUE-9750858 and CDA-9522207, by the United Space Alliance, grant No. NAS 9-20000 (PWO C0C67713A6), by the Future Aerospace Science and Technology Program (FAST) Center for Structural Integrity of Aerospace Systems, effort sponsored by the Air Force Office of Scientific Research, Air Force Materiel Command, USAF, under grant number F49620-95-1-0518, and by the National Security Agency under Grant No. MDA904-98-1-0561.

The authors are very thankful to H. T. Nguyen for helpful discussions, to J. Schubert for useful references, and to participants of the 2000 International Conference of the North American Fuzzy Information Society (NAFIPS), especially to T. Whalen, for useful comments.

References

[1] D. Bamber, "Entailment with near surety of scaled assertions of high conditional probability", *Journal of Philosophical Logic*, 2000 (to appear).

[2] A. D. C. Bennett, J. B. Paris, and A. Vencovská, "A new criterion for comparing fuzzy logics for uncertain reasoning", *Journal of Logic, Language, and Information*, 2000, Vol. 9, pp. 31–63.

[3] U. Bergsten and J. Schubert, "Dempster's rule for evidence ordered in a complete directed acyclic graph", *Int. J. Approx. Reasoning* 1993, Vol. 9, No. 1, pp. 37–73.

[4] U. Bergsten, J. Schubert, and P. Swennson, "Applying Data Mining and Machine Learning Techniques to Submarine Intelligence Analysis", *Proc. Third Int. Conf. on Knowledge Discovery and Data Mining (KDD'97)*, Newport Beach, August 14–17, 1997, AAAI Press, 1997, pp. 127–130.

[5] L. Godo, R. Lopez de Mantaras, C. Sierra, and A. Verdaguer, "MILORD: The Architecture and management of Linguistically expressed Uncertainty", *International Journal of Intelligent Systems*, 1989, Vol. 4, pp. 471–501.

[6] I. R. Goodman, "A decision aid for nodes in Command & Control Systems based on cognitive probability logic", *Proceedings of the 1999 Command & Control Research and Technology Symposium*, US Naval War College, Newport, RI, June 29–July 1, 1999, pp. 898–941.

[7] I. R. Goodman and H. T. Nguyen, "Amas' high probability and combination of information in the context of product probability conditional event algebra", *Proceedings of Fusion'98*, Las Vegas, NV, July 6–8, 1998, Vol. 1, pp. 1–8.

[8] I. R. Goodman and H. T. Nguyen, "Computational aspects of quantitative second order probability logic and fuzzy if-then rules: Part I, Basic representations as integrals", *Proceedings of the Joint Conferences in Information Sciences JCIS'2000*, Atlantic City, NJ, February 27–March 3, 2000, Vol. I, pp. 64–67.

[9] I. R. Goodman and H. T. Nguyen, "Probability updating using second-order probabilities and conditional event algebra", *Information Sciences*, 2000 (to appear).

[10] R. Hammer *et al.*, *Numerical Toolbox for Verified Computing I*, Springer-Verlag, 1993.

[11] L. Hurwicz, *A criterion for decision-making under uncertainty*, Technical Report 355, Cowles Commission, 1952.

[12] J. Y. Jaffray, "Linear utility theory for belief functions", *Op. Res. Letters*, 1989, Vol. 8, pp. 107–112.

[13] J. Y. Jaffray, "Linear utility theory and belief functions: a discussion", In: A. Chickan (ed.), *Proc. of FUR IV Conference*, Dordrecht, Kluwer, 1991.

[14] J. Y. Jaffray, "Dynamic decision making with belief functions", In: R. R. Yager, J. Kacprzyk, and M. Pedrizzi (Eds.), *Advances in the Dempster-Shafer Theory of Evidence*, Wiley, N.Y., 1994, pp. 331–352.

[15] R. B. Kearfott, *Rigorous global search: continuous problems*, Kluwer, Dordrecht, 1996.

[16] R. B. Kearfott and V. Kreinovich (eds.), *Applications of Interval Computations*, Kluwer, Dordrecht, 1996.

[17] V. Kreinovich, A. Lakeyev, J. Rohn, and P. Kahl, *Computational complexity and feasibility of data processing and interval computations*, Kluwer, Dordrecht, 1998.

[18] S. A. Lesh, *An evidential theory approach to judgment-based decision making*, Ph.D. Thesis, Department of Forestry and Environmental Studies, Duke University, Durham, NC, 1986.

[19] G. A. Miller, "The magical number seven plus or minus two: some limits on our capacity for processing information", *Psychological Review*, 1956, Vol. 63, pp. 81–97.

[20] P. M. Milner, *Physiological psychology,* Holt, NY, 1970.

[21] H. T. Nguyen and V. Kreinovich, "Nested Intervals and Sets: Concepts, Relations to Fuzzy Sets, and Applications", In: R. B. Kearfott and V. Kreinovich (eds.), *Applications of Interval Computations*, Kluwer, Dordrecht, 1996, pp. 245–290.

[22] H. T. Nguyen, V. Kreinovich, and Q. Zuo, "Interval-valued degrees of belief: applications of interval computations to expert systems and intelligent control", *International Journal of Uncertainty, Fuzziness, and Knowledge-Based Systems (IJUFKS)*, 1997, Vol. 5, No. 3, pp. 317–358.

[23] N. J. Nilsson, "Probabilistic logic", *Artificial Intelligence*, 1996, Vol. 28, pp. 71–87.

[24] J. Schubert, "On nonspecific evidence", *Int. J. Intell. Syst.*, 1993, Vol. 8, No. 6, pp. 711–725.

[25] J. Schubert, *Cluster-based specification techniques in Dempster-Shafer theory for an evidential intelligence analysis of multiple target tracks*, Ph.D. Dissertation, Royal Institute of Technology, Department of Numerical Analysis and Computer Science, Stockholm, Sweden, 1994.

[26] J. Schubert, *Specifying nonspecific evidence*, *Int. J. Intelligent Systems*, 1996, Vol. 11, No. 8, pp. 525–563.

[27] T. M. Strat, "Decision analysis using belief model", *Int. J. Approx. Reasoning*, 1990, Vol. 4, No. 5/6, pp. 391–417.

[28] T. M. Strat, "Decision analysis using belief functions", In: R. R. Yager, J. Kacprzyk, and M. Pedrizzi (Eds.), *Advances in the Dempster-Shafer Theory of Evidence*, Wiley, N.Y., 1994, pp. 275–310.

[29] P. Suppes, D. M. Krantz, R. D. Luce, and A. Tversky, *Foundations of measurement*, Vol. I-III, Academic Press, San Diego, CA, 1989.

[30] Website on interval computations: http://www.cs.utep.edu/interval-comp.

[31] T. Whalen and C. Brönn, "Hurwicz and regret criteria extended to decisions with ordinal probabilities", *Proc. of 1990 North Amer. Fuzzy Inform. Proc. Soc. Conference*, pp. 219–222.

[32] T. Whalen, "Interval probabilities induced by decision problems", In: R. R. Yager, J. Kacprzyk, and M. Pedrizzi (Eds.), *Advances in the Dempster-Shafer Theory of Evidence*, Wiley, N.Y., 1994, pp. 353–374.