A Full Description of All Commutative Associative Polynomial Operations on Probabilities

Miroslav Svítek[1], Olga Kosheleva[2],
Vladik Kreinovich[2], and Nguyen Hoang Phuong[3]

[1]Czech Technical University in Prague, Prague, Czech Republic
svitek@fd.cvut.cz
[2]University of Texas at El Paso, El Paso, Texas 79968, USA
olgak@utep.edu, vladik@utep.edu
[3]Thang Long University, Hanoi, Vietnam, nhphuong2008@gmail.com

1. Known polynomial operations on probabilities

- Suppose that we have two independent events E_1 and E_2, and we know the probabilities p_1 and p_2 of both events.
- Then the probability that both events occurs is equal to the product $p_1 \cdot p_2$ of these probabilities.
- The corresponding operation $f(p_1, p_2) = p_1 \cdot p_2$ is:
  - commutative, i.e., $f(p_1, p_2) = f(p_2, p_1)$, and
  - associative, i.e., $f(f(p_1, p_2), p_3) = f(p_1, f(p_2, p_3)))$.
- Similarly, for two independent events, the probability that at least one of them will occur is equal to $p_1 + p_2 - p_1 \cdot p_2$.
- The operation $f(p_1, p_2) = p_1 + p_2 - p_1 \cdot p_2$ is also commutative and associative.
- Both operations are also polynomial, in the sense that both functions are polynomials of the two inputs p_1 and p_2.

2. A natural question

- We have listed two examples of commutative associative polynomial operations.
- A natural question is to enumerate all such operations.
- In particular, a natural question is:
  - whether the product is the only possible operation corresponding to "and"
  - or there are other operations of this type that describe the probability of both events happening,
  - e.g., in situations when there is some dependence between the events.
- A similar question can be raised about "or".

3. How natural is this question?

- Commutativity makes sense.
- For example, for "and", $E_1 \,\&\, E_2$ means the same as $E_2 \,\&\, E_1$.
- So it makes sense to require:
  - that our estimate for the probability of $E_1 \,\&\, E_2$ is the same as our estimate for the probability of $E_2 \,\&\, E_1$,
  - i.e., that the corresponding operation is commutative.
- Similarly, since $E_1 \,\&\, (E_2 \,\&\, E_3)$ and $(E_1 \,\&\, E_2) \,\&\, E_3$ mean the same thing, it is reasonable to require associativity.
- Limitation to polynomial operations is motivated by two things.
- First, there is a known mathematical fact that:
  - every continuous function on a bounded domain
  - can be approximation, with any given accuracy, by a polynomial.

4. How natural is this question (cont-d)

- Second, there is a known computational fact that:
  - in a computer, the only directly hardware supported arithmetic operations are addition, subtraction, and multiplication;
  - even division is implemented as a sequence of such operations;
  - to be more precise, the inverse $1/b$ is implemented iteratively, and then a/b is usually implemented as the product $a \cdot (1/b)$.
- So, in effect:
  - whatever we want to compute, be it $\exp(x)$ or $\sin(x)$,
  - what the computer really does is performs a sequence of addition, subtraction, and multiplication operations,
  - i.e., computes a polynomial.

5. What we do in this talk

- We provide a full description of all possible commutative associative polynomial operations.
- We also show that:
  - the only operation of this type that is consistent with the meaning of $E_1 \& E_2$ is $f(p_1, p_2) = p_1 \cdot p_2$, and
  - the only operation of this type that is consistent with the meaning of $E_1 \vee E_2$ is $f(p_1, p_2) = p_1 + p_2 - p_1 \cdot p_2$.

6. Definitions and Proposition 1

- *By an* operation, *we means a function* $f(a, b)$ *from pairs of real numbers to real numbers.*
- *We say that an operation* $f(a, b)$ *is* commutative *if* $f(a, b) = f(b, a)$ *for all* a *and* b.
- *We say that an operation* $f(a, b)$ *is* associative *if* $f(f(a, b), c) = f(a, f(b, c))$ *for all* a, b, *and* c.
- *We say that an operation* $f(a, b)$ *is* polynomial *if the function* $f(a, b)$ *is a polynomial.*
- **Proposition 1.** *For every operation* $f(a, b)$, *the following two conditions are equivalent to each other:*
  - *the operation* $f(a, b)$ *is commutative, associative, and polynomial;*
  - $f(a, b) = c_0 + c_1 \cdot (a + b) + c_2 \cdot a \cdot b$, *where* $c_1^2 = c_1 + c_0 \cdot c_2$.

7. Discission

- We are interested in probabilities.
- So, we may want to limit ourselves to operations for which the value $f(a, b)$ is always in the interval $[0, 1]$.
- Such operations are described by the following inequalities.

8. Proposition 2

- *For every commutative associative polynomial operation* $f(a,b) = c_0 + c_1 \cdot (a+b) + c_2 \cdot a \cdot b$, *the following two conditions are equivalent:*
  - *the value* $f(a,b)$ *is always located in the interval* $[0,1]$*;*
  - *the following inequalities are satisfied:*

$$0 \le c_0 \le 1, \quad 0 \le c_0 + c_1 \le 1, \quad 0 \le c_0 + 2c_1 + c_2 \le 1.$$

9. Definitions and Proposition 3

- *We say that an operation* $f(a,b)$ represents "and" *if:*
  - *for every two values* $p_1, p_2 \in [0,1]$
  - *there exists a probability distribution and two events* E_1 *and* E_2 *for which* $\mathrm{Prob}(E_1) = p_1$, $\mathrm{Prob}(E_2) = p_2$, *and*

$$\mathrm{Prob}(E_1 \,\&\, E_2) = f(p_1, p_2).$$

- **Proposition 3.** *The only commutative associative polynomial operations that represents "and" is* $f(a,b) = a \cdot b$.

10. Definitions and Proposition 4

- *We say that an operation* $f(a, b)$ represents "or" *if:*
  - *for every two values* $p_1, p_2 \in [0, 1]$
  - *there exists a probability distribution and two events* E_1 *and* E_2 *for which* $\text{Prob}(E_1) = p_1$, $\text{Prob}(E_2) = p_2$, *and*

$$\text{Prob}(E_1 \vee E_2) = f(p_1, p_2).$$

- **Proposition 4.** *The only commutative associative polynomial operations that represents "or" is* $f(a, b) = a + b - a \cdot b$.
- Of course, not all commutative associative polynomial operations represent "and" or "or".
- Another example of such an operation is $f(a, b) = a + b - 2a \cdot b$.
- This operation represents "exclusive or", i.e., the probability that exactly one of these events will happen.

11. Proof of Proposition 1

- It is easy to check that:
  - every operation of the type $f(a,b) = c_0 + c_1 \cdot (a+b) + c_2 \cdot a \cdot b$, where $c_1^2 = c_1 + c_0 \cdot c_2$,
  - is commutative, associative, and polynomial.
- Vice versa, let $f(a,b)$ be a commutative and associative polynomial operation.
- Let us prove that this operation has the desired type.
- Let us first prove that:
  - in each monomial $c \cdot a^n \cdot b^m$ of the polynomial $f(a,b)$,
  - the powers n and m cannot exceed 1,
  - i.e., the expression $f(a,b)$ must be linear in each of its variables.
- Indeed, let us take a monomial with the highest possible degree n of the variable a.

12. Proof of Proposition 1 (cont-d)

- This means that:
  - in the polynomial $f(a, b)$, there is a term $k(b) \cdot a^n$ proportional to a^n,
  - for some coefficient of proportionality $k(b)$ depending on b.
- Similarly, in the expression $f(f(a, b), c)$:
  - there is a term equal to $k(c) \cdot (f(a, b))^n$,
  - i.e., the term equal to $k(c) \cdot (k(b) \cdot a^n + \ldots)^n$.
- If we open parentheses, we will see that one of the resulting terms is equal to $k(c) \cdot (k(b) \cdot a^n)^n = k(c) \cdot (k(b))^n \cdot a^{n^2}$.
- Thus, the expression $f(f(a, b), c)$ has a term proportional to a^{n^2}.
- On the other hand, in the expression $f(a, f(b, c))$:
  - the highest power of a is in the term $k(f(b, c)) \cdot a^n$,
  - i.e., the highest power of a is n.

13. Proof of Proposition 1 (cont-d)

- Since the operation is associative, we must have

$$f(f(a,b),c) = f(a,f(b,c)).$$

- Thus, the term proportional to a^{n^2} in the left-hand side of this equality must be present in its right-hand side as well.
- But in the right-hand side, the highest degree of a is a^n.
- Thus, we must have $n^2 \leq n$.
- Dividing both sides of this inequality by n, we indeed get $n \leq 1$.
- For each of the two variables, we have two options: the degree of this variable is either 0 or 1.
- By combining two possible options for each of the two variables a and b, we have four possible combinations.

14. Proof of Proposition 1 (cont-d)

- So, the general polynomial of this type is a linear combination of four terms corresponding to four possible combinations:

$$f(a,b) = c_0 + c_1 \cdot a + c_b \cdot b + c_2 \cdot a \cdot b \text{ for some coefficients } c_i.$$

- Since the operation is commutative, we can conclude that $c_b = c_1$.
- So $f(a,b) = c_0 + c_1 \cdot (a+b) + c_2 \cdot a \cdot b$.
- Let us now check when this operation is associative.
- For this operation, we have

$$f(f(a,b),c) = c_0 + c_1 \cdot (f(a,b) + c) + c_2 \cdot f(a,b) \cdot c.$$

- Substituting the expression for $f(a,b)$ into this formula, we conclude that

$$f(f(a,b),c) = c_0 + c_1 \cdot (c_0 + c_1 \cdot (a+b) + c_2 \cdot a \cdot b + c) +$$
$$c_2 \cdot (c_0 + c_1 \cdot (a+b) + c_2 \cdot a \cdot b) \cdot c.$$

15. Proof of Proposition 1 (cont-d)

- If we open parentheses, we get

$$f(f(a,b),c) = c_0 + c_0 \cdot c_1 + c_1^2 \cdot a + c_1^2 \cdot b + c_1 \cdot c + c_2 \cdot c_0 +$$
$$c_1 \cdot c_2 \cdot a \cdot c + c_1 \cdot c_2 \cdot b \cdot c + c_2^2 \cdot a \cdot b \cdot c.$$

- By combining coefficients at the same monomial, we get

$$f(f(a,b),c) = (c_0 + c_0 \cdot c_1) + c_1^2 \cdot a + c_1^2 \cdot b + (c_1 + c_0 \cdot c_2) \cdot c +$$
$$c_1 \cdot c_2 \cdot a \cdot b + c_1 \cdot c_2 \cdot a \cdot c + c_1 \cdot c_2 \cdot b \cdot c + c_2^2 \cdot a \cdot b \cdot c.$$

- Due to commutativity, we have $f(a, f(b,c)) = f(f(c,b),a)$.
- So, to get the expression for $f(a, f(b,c))$, it is sufficient to swap a and c in the above formula.
- Thus:

$$f(a, f(b,c)) = (c_0 + c_0 \cdot c_1) + (c_1 + c_0 \cdot c_2) \cdot a + c_1^2 \cdot b + c_1^2 \cdot c +$$
$$c_1 \cdot c_2 \cdot a \cdot b + c_1 \cdot c_2 \cdot a \cdot c + c_1 \cdot c_2 \cdot b \cdot c + c_2^2 \cdot a \cdot b \cdot c.$$

16. Proof of Proposition 1 (cont-d)

- Associativity means that these two expressions must be equal.
- The only coefficients that are different in these expressions are coefficients at a and c.
- Thus, for the operation to be associative, it is necessary and sufficient:
  - that these two coefficients be equal,
  - i.e., that we have $c_1^2 = c_1 + c_0 \cdot c_2$.
- The proposition is proven.

17. Proof of Proposition 2

- The function $f(a, b)$ is linear in terms of each of its variables.
- For a linear function, the smallest and the largest values on each interval are obtained on the endpoints of the corresponding interval.
- Thus:
  - to check that the smallest value of this function when $a, b \in [0, 1]$ is at least 0 and the largest value is at most 1,
  - it is sufficient to check these inequalities for the four possible combinations of the endpoints,
  - i.e., for situations in which a is equal to 0 or 1 and b is equal to 0 or 1.
- For these values, the double inequality $0 \leq f(a, b) \leq 1$ takes the desired form.
- The proposition is proven.

18. Proof of Proposition 3

- Since $E_1 \,\&\, E_2$ implies E_1 and E_2, we always have

$$\text{Prob}(E_1 \,\&\, E_2) \le \text{Prob}(E_1).$$

- In particular, when $\text{Prob}(E_1) = 0$, we should have $\text{Prob}(E_1 \,\&\, E_2) = 0$.
- Thus, we must have $f(0, p_2) = 0$ for all p_2.
- Substituting the general expression $f(a, b) = c_0 + c_1 \cdot (a + b) + c_2 \cdot a \cdot b$ into this formula, we conclude that $c_0 + c_1 \cdot p_2 = 0$ for all p_2.
- Thus, we must have $c_0 = c_1 = 0$, and $f(a, b) = c_2 \cdot a \cdot b$.
- On the other hand:
  - when the both events E_1 and E_2 occur with probability 1,
  - this means that the event $E_1 \,\&\, E_2$ should also occur with probability 1.
- So, we should have $f(1, 1) = 1$.

19. Proof of Proposition 3 (cont-d)

- Substituting $f(a, b) = c_2 \cdot a \cdot b$ into this formula, we conclude that $c_1 = 1$.
- So indeed $f(a, b) = a \cdot b$.
- The proposition is proven.

20. Proof of Proposition 4

- Since E_1 implies $E_1 \vee E_2$, we always have $\text{Prob}(E_1) \le \text{Prob}(E_1 \vee E_2)$.
- In particular, when $\text{Prob}(E_1) = 1$, we should have $\text{Prob}(E_1 \vee E_2) = 1$.
- Thus, we must have $f(1, p_2) = 1$ for all p_2.
- Substituting the general expression $f(a, b) = c_0 + c_1 \cdot (a + b) + c_2 \cdot a \cdot b$ into this formula, we conclude that

$$c_0 + c_1 \cdot (p_2 + 1) + c_2 \cdot p_2 = (c_0 + c_1) + (c_1 + c_2) \cdot p_2 = 1 \text{ for all } p_2.$$

- Thus, we must have $c_0 + c_1 = 1$ and $c_1 + c_2 = 0$.
- So, $c_2 = -c_1$ and $c_0 = 1 - c_1$, so

$$f(a, b) = (1 - c_1) + c_1 \cdot (a + b) - c_1 \cdot a \cdot b.$$

- On the other hand, when the event E_1 has zero probability, then the probabilities of E_2 and $E_1 \vee E_2$ should be the same.
- So, we must have $f(0, p_2) = p_2$ for all p_2.

21. Proof of Proposition 4 (cont-d)

- Substituting $f(a,b) = (1-c_1) + c_1 \cdot (a+b) - c_1 \cdot a \cdot b$ into this formula, we conclude that $1 - c_1 + c_1 \cdot p_2 = p_2$ for all p_2.
- Thus, we must have $c_1 = 1$, i.e., indeed $f(a,b) = a + b - a \cdot b$.
- The proposition is proven.

22. Acknowledgments

This work was supported in part by:

- National Science Foundation grants 1623190, HRD-1834620, HRD-2034030, and EAR-2225395;
- AT&T Fellowship in Information Technology;
- program of the development of the Scientific-Educational Mathematical Center of Volga Federal District No. 075-02-2020-1478, and
- a grant from the Hungarian National Research, Development and Innovation Office (NRDI).