Additivity of Probabilities

Math 394

1 Infinity

We cannot "list" or "exhibit" an actual infinite set, but the concept is extremely useful nonetheless. For example, we all agree that it is a good idea to state that "there are infinitely many integers" – even if there is no way we could list them all. A similar, only slightly more sophisticated idea, is "there are infinitely many prime integers.

Proof: We take for granted that any integer can be factored in a product of prime numbers. Assume that there are only n prime numbers, $p_1, p_2, \ldots, p_n$. If so, the integer $p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$, which is different from (and greater than) the primes $p_1, \ldots, p_n$, has none of the listed primes as a factor (if you divide it by, say, p_k, you end up with $\prod_{j=1,\ldots,n, j\neq k} p_j + \frac{1}{p_k}$, which cannot be an integer), so is either a prime itself, or presumes the existence of further primes.

There is another type of infinity that pops up almost inevitably – it occurred, to their great dismay, to Greek philosophers sometime around the 5th Century BCE – is that there is no finite way to get a hold on quantities that, in some sense, have to be "real", like the square root of 2. In fact, it turns out that no root of an integer that is not itself an integer (in the sense that $\sqrt{4} = 2$, and $\sqrt[3]{27} = 3$) is "irrational" – meaning there is no way to represent them exactly as fractions or with a decimal representation that can be described in a finite number of words, as opposed to have to be computed all the way.

Proof Suppose that $\sqrt[n]{m} = \frac{p}{q}$, where $q \neq 1$, and the fraction on the right is reduced to smallest terms, that is p and q have no common prime factor. Then

$$m = \frac{p^n}{q^n}$$

that is

$$p^n = mq^n$$

That means that m is a factor of p^n – but that means it is a factor of p itself. Hence, for some integer s, $p^n = m^n s^n$, and

$$m = \frac{m^n s^n}{q^n}$$

or

$$q^n = m^{n-1} s^n$$

which implies that m^{n-1} is a factor of q^n, and, hence, that m is a factor of q – contradicting our assumption that p and q had no common factor.

The reason that this fact involves an infinity of operations is that we cannot represent a non-rational (*irrational*) number in any finite, explicit way. Stating that $\sqrt{2}$ is the number whose square is 2 is only a tautology. The only way we have been able to make sense of this conundrum (irrational numbers like $\sqrt{2}$ or π, and so on, come up in very practical simple situations) is to define "irrational numbers" as, to express the concept in a hand-waving way, "limits of rational approximate values". That is what the "decimal expansion on $\sqrt{2}$" means: it defines a sequence of *rational* numbers (what you get whenever you stop the expansion at some point) such that if you square them, you get a result that is closer and closer to 2, never quite making it. In other words, very simple and practical problems require us to consider "numbers" that are not quite constructively defined, but are "defined" as "limits" of sequences of "concrete numbers".

There have been attempts to dispose of this pretty abstract concept, but they have not gained too much traction (check out "constructivist mathematics"), because giving up on irrational numbers (and much more, as it turns out) makes our life way much harder (and miserable).

The bottom line of this discussion is that much of mathematics is founded on the concept of *approximating* solutions to problems – and, if need be, *define* objects that can qualify as the target of these approximations. In fact, most of the theory of Partial Differential Equations (to name one of the cornerstones of both pure and applied mathematics) relies on making sense of "solutions" that "exist" only in the sense of having well-defined procedures that "approximate" them.

2 Algebras and $\sigma-$Algebras of Sets

It is clear that there are Boolean algebras of sets, that are not $\sigma-$algebras. For example, the half-open intervals in the real line, of the form $[a, b)$, together with all finite collections of these intervals, form an algebra, but infinite unions and intersections lead to a vastly larger class of subsets (the so-called *Borel sets* of measure theory), which is the $\sigma-$algebra *generated by* the half-open intervals (the smallest $\sigma-$algebra that contains them).

A more familiar algebra that is not a $\sigma-$algebra is given by the collection of intervals (of any kind, even if we can restrict to half-open ones, if we like to narrow the scope) with rational endpoints. The $\sigma-$algebra generated by these intervals is again the Borel $\sigma-$algebra. An interesting way to look at this example, is to notice that in this case we could choose as containing space (the sample space, in our setup) the set of rational numbers $\mathbb{Q}$. However, if we wanted to extend our algebra to a $\sigma-$algebra, we would have to go to a much larger space, namely the set of real numbers. This need to "expand" our space to accommodate all the countable unions and intersections that we could build reappears in other important situations, as when one tries to define a useful probability model where the sample set is a set of functions, and we begin with functions that are too smooth.

3 Additivity and Countable Additivity of Probabilities

Of course, if we are given only an algebra of events, countable additivity ($\sigma-$additivity) cannot hold for a probability function, since it will not be even defined on most countable unions or intersections (which are not events). However, there may be some countable unions or intersections, that happen to be events in the algebra, and for these sets $\sigma-$additivity may or may not hold.

An important theorem states that if a probability function is countably additive when the countable union or intersection is an event, then if one constructs the $\sigma-$algebra generated by our original algebra (that is, if one looks at the smallest $\sigma-$algebra that contains our algebra, and we have noticed that in some cases this will force us to enlarge the sample space), there is a unique probability function defined on this $\sigma-$algebra that is $\sigma-$additive, and coincides with our original probability on events that belong to the algebra we started with. The prime example would be one of the algebras we mentioned in the previous sections, with, for example, the sample space chosen as the interval $[0, 1]$, and the probability of any interval with endpoints a and b defined as $b - a$. The construction of the $\sigma-$additive extension to the Borel $\sigma-$algebra is extremely non trivial, and the result is *Lebesgue measure*.

However, not every additive probability is $\sigma-$additive on countable unions or intersections that belong to an algebra. Thus, even if we then extend our collection of events to a $\sigma-$algebra, we would not obtain a countably additive probability. A classic example is the following:

Example: Let Ω be a countable set. Consider the algebra consisting of subsets that are finite, and their complements. For example, you can think of the natural numbers as an example. Define a probability by

$$P\left[A\right] = \begin{cases} 0 & \text{if } A \text{ is finite} \\ 1 & \text{if } \bar{A}\text{is finite} \end{cases}$$

($\bar{A}$ is the complement of A, $\Omega \setminus A$). This is a fairly trivial model, but all finite axioms are satisfied. P is not countably additive, since any infinite set has probability 1, but is the countable union of its points, all of which have probability 0.

Note: If Ω is uncountable, the counterexample above does not work, since complements of finite sets are now uncountable, and thus are not a countable union of sets of probability 0!