3 April 2019

Random Walk Algorithms: Lecture 2

David A. Meyer

In which we digress to discuss the non-primality of 1, thereby reviewing complex numbers, and then introduce some basic notions of probability.

Digression

The question which arose as we constructed an algorithm for primality testing in the previous lecture, namely whether or not 1 is a prime number, is interesting both historically and mathematically [1,2]: According to Sir Thomas Heath, for the ancient Greeks, 1 was a *unit*, not a number [3, p.69], and *a fortiori*, not a prime number. This conception held for almost two millennia, but by the time Simon Stevin's 1585 treatise on decimal notation and arithmetic, *De Thiende*, was translated into English in 1608, many accepted "The sixt Definition. A Whole number is either a unitie, or a compounded multitude of unities." [4, p.A3v]. Once 1 was a number, it could be considered a prime number, and for the next few hundred years, some mathematicians did so (Christian Goldbach being a famous example [5]), while others did not (Carl Friedrich Gauß counted 168 primes less than 1000 [6]).

In fact, it was Gauß in his second paper on quartic reciprocity [7] who introduced what we now call the Gaussian integers—complex numbers of the form $a+bi$, $a,b \in \mathbb{Z}$—and the modern ideas which led to 1 again being considered a unit, still a number, but not a prime number: Recall that a commutative *ring* like the integers has two operations, addition and multiplication. A *unit* in a ring has a multiplicative inverse in the ring (so for $\mathbb{Z}$, 1 and -1 are the only units). Two important features of prime numbers are that they are, in modern terminology:

1. *irreducible*: not the product of two non-units;
2. *prime*: $a|bc \Rightarrow a|b$ or $a|c$.

For *integral domains* (commutative rings in which the product of non-zero elements is non-zero), prime implies irreducible. The converse, is not always true, however; only for *unique factorization domains* (every element has a unique factorization as a product of irreducible elements, as integers do, by the Fundamental Theorem of Arithmetic) does irreducible imply prime. The following example is *not* a unique factorization domain:

Example. Consider the set of quadratic integers $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$. The norm on $\mathbb{C}$ defines a norm on $\mathbb{Z}[\sqrt{-5}]$:

$$\|a + b\sqrt{-5}\| = \sqrt{(a+ib\sqrt{5})(a-ib\sqrt{5})} = \sqrt{a^2+5b^2}.$$

Notice that since $a,b \in \mathbb{Z}$, the possible values for the norm of an element in $\mathbb{Z}[\sqrt{-5}]$ are rather sparse: $\{0,1,2,\sqrt{5},\sqrt{6},3,\ldots\}$. Recall that the norm of complez numbers satisfies

$\|wz\| = \|w\| \cdot \|z\|$. We can use this property to see that 1 and -1 are the only units in $\mathbb{Z}[\sqrt{-5}]$, since they are the only elements with norm 1, and there are no fractional norm values. Thus $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible, since again by the paucity of norm values, it cannot be the product of two non-units. But 2 is not prime since $2|6 = (1+\sqrt{-5})(1-\sqrt{-5})$, each of these factors has norm $\sqrt{6}$, and $\sqrt{6}/2$ is not a norm value, so 2 does not divide either of them.

Probability

When we flip a coin, we describe the process as "it lands head up with probability p", where if $p = 1/2$ we say it is a fair coin. In principle, if we knew the initial position, velocity, angular velocity, mass, position of landing surface, elastic properties of the coin and the surface, gravitational field, air resistance, *etc.*, we could compute how the coin would land. In practice, we cannot know all these details, so we summarize our *ignorance* by saying that the coin will land head up with *probability* p, *i.e.*, a fraction p of the time.

Definition. The set of *outcomes* or *sample space* is written Ω. (For a coin flip, $\Omega = \{\text{head}, \text{tail}\}$, which we will sometimes abbreviate $\{\text{H}, \text{T}\}$.) We will consider cases where Ω is countable. An *event* is a subset of Ω.

Definition. For countable Ω, a *discrete probability distribution* is a map $\Pr : \Omega \to \mathbb{R}_{\geq 0}$, with the property that

$$\sum_{\omega \in \Omega} \Pr(\omega) = 1.$$

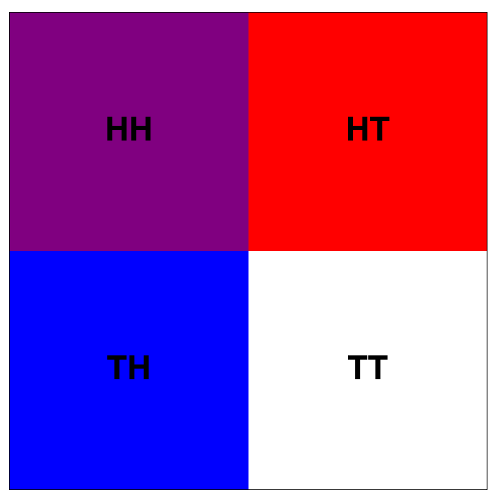
This map extends to events:

$$\Pr(A) = \sum_{\omega \in A} \Pr(\omega).$$

Example. For the coin flip we discussed above, $\Pr(\text{head}) = p$; $\Pr(\text{tail}) = 1 - p$. Now suppose we flip a coin twice. Then $\Omega = \{\text{HH}, \text{HT}, \text{TH}, \text{TT}\}$. A general probability distribution on Ω is defined by four nonnegative real numbers: $\Pr(\text{HH})$, $\Pr(\text{HT})$, $\Pr(\text{TH})$ and $\Pr(\text{TT})$, summing to 1. Let

$$\begin{aligned} A &= \{\text{HH}, \text{HT}\} \\ B &= \{\text{HH}, \text{TH}\}, \end{aligned}$$

i.e., A is the event that the first flip is head up and B is the event that the second flip is head up.



Definition. The *conditional probability* of event B, *given* event A, is

$$\Pr(B \mid A) = \frac{\Pr(A \cap B)}{\Pr(A)},$$

which is the relative fraction of B within A.

Definition. Events A and B are *independent* if $\Pr(B \mid A) = \Pr(B)$, or equivalently, using the definition of conditional probability above, if $\Pr(A \cap B) = \Pr(A)\Pr(B)$.

Example. If events A and B in the example above are independent, then $\Pr(\mathrm{HH}) = p$, $\Pr(\mathrm{HT}) = p(1-p) = \Pr(\mathrm{TH})$, and $\Pr(\mathrm{TT}) = (1-p)^2$.

References

[1] C. K. Caldwell and Y. Xiong, "What is the smallest prime?", *Journal of Integer Sequences* **15** (2012) Article 12.9.7.

[2] E. Lamb, "Why isn't 1 a prime number? And how long has it been a number?", Roots of Unity blog, *Scientific American* (2 April 2019); `https://blogs.scientificamerican.com/roots-of-unity/why-isnt-1-a-prime-number/`.

[3] T. Heath, *A History of Greek Mathematics, Vol. 1. From Thales to Euclid* (Oxford: Clarendon Press 1921).

[4] S. Stevin, *Disme: The Art of Tenths, or, Decimall Arithmetike, Teaching how to performe all Computations whatsoever, by whole Numbers without Fractions, by the foure Principles of Common Arithmeticke: namely, Addition, Substraction, Multiplication, and Division*, published in English with some additions by R. Norton (London: S. Stafford 1608).

[5] C. Goldbach, "*Lettre XLIII à Euler*" (7 June 1742) in P.-H. Fuss, ed., *Correspondance Mathématique et Physique de Quelques Célèbres Géomètres du XVIIIème Siècle, Tome I* (St. Pétersbourg: L'Académie Impériale des Sciences 1843) 125-129.

[6] C. F. Gauß, "*Tafel der Frequenz der Primzahlen*", in *Werke, Band II* (Göttingen: Königlichen Gesellschaft der Wissenschaften 1876) 435-443.

[7] C. F. Gauß, "*Theoria residuorum biquadraticorum. Commentatio secunda*", *Commentationes societatis regiae scientiarum Gottingensis recentiores* **VII** (1832) in *Werke, Band II* (Göttingen: Königlichen Gesellschaft der Wissenschaften 1876) 93-148.