NOTES

The Euler φ-Function and Probability

James Ward

The Euler φ-function, $\varphi(n)$, where n is a positive integer, is defined as the number of positive integers less than n which are coprime to n. $\varphi(n)$ may be evaluated using the formula

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

where $p_1, \ldots, p_k$ are the distinct prime divisors of n, so that $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$. Readers may be interested in the following derivation of this formula, which was presented by Professor E. Eberlein in his lectures on introductory probability and statistics during the Winter Semester of 1980/81 at the University of Freiburg.

Let us consider the sample space $\Omega = \{1, 2, \ldots, n\}$, and the experiment of selecting at random a number from Ω, all numbers being equally likely to be chosen. Denoting by $|X|$ the cardinality of the set X, we have that for any event X (i.e., any subset of Ω), the probability of X is given by $\Pr(X) = |X|/n$. In particular, if A is the event that a number chosen at random from Ω is coprime to n, then $|A| = \varphi(n)$ by definition. On the other hand we have $|A| = n \Pr(A)$. The formula for $\varphi(n)$ will be established by computing $\Pr(A)$.

Writing $A_i = \{ r \in \Omega \mid p_i \text{ divides } r \}$, then it can be seen that

$$A = A_1^c \cap A_2^c \cap \ldots \cap A_k^c \, .$$

Now $|A_i| = n/p_i$, and so $\Pr(A_i) = 1/p_i$ for $1 \leq i \leq k$.

We now show that the events $A_1, \ldots, A_k$ are independent. Independence requires that for every subset $i_1, i_2, \ldots, i_r$ of the index set $1, 2, \ldots, k$, we have

$$\Pr(A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_r}) = \Pr(A_{i_1}) \Pr(A_{i_2}) \cdots \Pr(A_{i_r}) \, .$$

Now

$$\begin{aligned} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_r}| &= \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_r}} \\ = n \frac{1}{p_{i_1}} \frac{1}{p_{i_2}} \cdots \frac{1}{p_{i_r}} &= n \Pr(A_{i_1}) \Pr(A_{i_2}) \cdots \Pr(A_{i_r}) \, , \end{aligned} \tag{1}$$

and also

$$|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_r}| = n \Pr(A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_r}) \, . \tag{2}$$

Together (1) and (2) establish that the events $A_1, \ldots, A_k$ are independent. It follows that the complementary events $A_1^c, \ldots, A_k^c$ are also independent. Therefore

$$\begin{aligned} \Pr(A_1^c \cap A_2^c \cap \ldots \cap A_k^c) &= \Pr(A_1^c) \Pr(A_2^c) \cdots \Pr(A_k^c) \\ &= \prod_{i=1}^{k} (1 - \Pr(A_i)) = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \, . \end{aligned} \tag{3}$$

Since $A = A_1^c \cap A_2^c \cap \ldots \cap A_k^c$ and $\varphi(n) = n \Pr(A)$ we obtain from (3)

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \, .$$

Department of Mathematics,
University College Galway.