Counting

P. Danziger

Given a set S we will use $|S|$ for the number of elements of S.

1 Simple Probability

A random process is a repeatable process (series of events) whose outcome follows a (known) probability distribution.
The sample space, S, is the set of all possible outcomes.
An event is a subset of the sample space. So given a random process with sample space S, an event is a subset $A \subseteq S$.
A trial is a selection from a random process.
Generally we want to find the probability that a given trial will result in one of the members of A. We will make the assumption of equal likelyhood, every outcome within the sample space S is equally likely to occur.
This gives the that the probability of the event A occurring is

$$P(A) = \frac{|A|}{|S|}$$

In this case calculating probabilities becomes a matter of counting the sizes of the relevant sets.
There are two important special cases:

1. $P(S) = 1$
2. $P(\phi) = 0$.

2 Counting

2.1 Intervals

Theorem 1 *Given 2 integers n and m, with $n < m$:*

- *The number of integers from n to m inclusive is $n - m + 1$.*
- *The number of integers from n to m exclusive is $n - m - 1$.*
- *The number of integers from n (exclusive) to m (inclusive)is $n - m$.*

Example 2

1. When we declare an array which will have n elements we say:
   `int a[`n`];`
   which causes the compiler to allocate n blocks of size `int`. When we access the array we do so by indexing with elements from 0 to $n - 1$.

(a) If we choose an element at random from this array, what is the probability that the first element will be chosen?

The sample space is the set of all elements of the array, of which there are n. The event is the single element $\{a[0]\}$, thus $P(\{a[0]\}) = \frac{1}{n}$.

(b) If we choose a random element from this array, what is the probability that either the first or last element will be chosen?

Again the sample space is the set of all elements of the array, of which there are n. The event is now $A = \{a[0], a[n-1]\}$, $|A| = 2$, so $P(A) = \frac{2}{n}$.

2. A publisher advertises a boxed set containing volumes 9 to 16 for only \$10.

   (a) How many volumes are we getting and how much does each one cost?

   We are counting from 9 to 16 inclusive, so there are $16 - 9 + 1 = 8$. Each one costs $\frac{10}{8}$ =\$1.25.

   (b) If we pull a volume at random from the shelf, what is the probability that we get one after volume 12?

   The number of volumes greater than 12 is $16 - 12 = 4$. So $P(x > 12) = \frac{4}{8} = \frac{1}{2}$.

3. How many three digit integers end in a 3?

   We consider the integers from 100 to 999, every 10th one from 103 to 993 (inclusive) ends in a 3. There are $(993 - 103)/10 + 1 = 90$ intervals of ten between 103 and 993 (inclusive), so 90 integers from 100 to 999 end in a 3.

   The probability that a random integer from 100 to 999 ends in 3 is $\frac{90}{999-100+1} = \frac{90}{900} = \frac{1}{10}$.

2.2 The Multiplication Rule

Theorem 3 (Multiplication Rule) *Given Sets $A_1, A_2, \ldots, A_m$ there are $|A_1| \cdot |A_2| \cdot \ldots \cdot |A_m|$ ways to choose one element from each of these sets.*

Example 4

1. How many bit strings of length 4 are there?

   We can view this as choosing from the set $\{0, 1\}$ four times. So, $E_1 = E_2 = E_3 = E_4 = \{0, 1\}$, each of size two, there are thus $2^4 = 16$ bit strings of length 4.

   (a) What is the probability that 0101 is chosen at random?

   $P(x = 0101) = \frac{1}{16}$.

   (b) What is the probability that a randomly chosen 4 bit string contains exactly one 1?

   There are four 4 bit strings which contain exactly one 1.

   $P(x \text{ has one } 1) = \frac{4}{16} = \frac{1}{4}$.

2. A password consists of eight characters made up of the 68 symbols: `[0-9]`, `[A-z]`, `!`, `#`, `$`, `%`, `&`, `*` How many distinct passwords are there?

   $68^8 = 4.5716323965 \times 10^{14}$

(a) What is the probability that a random trial will guess the correct password?
$\approx 2 \times 10^{-15}$

(b) Suppose that we know that a user has only lower case letters in their password, what is the probability that a random trial (consisting of only lower case letters of course) will guess the correct password?
There are now 26 symbols available, so the number of possible passwords is $26^8 \approx 2 \times 10^{11}$, so $P(x = \text{password}) \approx 5 \times 10^{-12}$.

(c) Suppose that we now know that the user has used an English word.
There are roughly 500,000 English words, rising to 10^6 if scientific and technical terms are included. So the number of possible passwords is at most 10^6 and our probability drops to 1 in a million. $P(x = \text{password}) \approx 10^{-6}$.

(d) In fact an educated person only knows about 20,000 words and will only use about 2,000 different words in regular conversion. Given that the user just thought of a word, the probability of getting a correct guess skyrockets.

3. Suppose that we have a set of m nested `for` loops:

$$
\begin{array}{l}
\text{for}(i_1 = 0;\ i_1 < n_1;\ i_1\texttt{++}) \\
\quad \text{for}(i_2 = 0;\ i_2 < n_2;\ i_2\texttt{++}) \\
\qquad \ddots \\
\qquad\quad \text{for}(i_m = 0;\ i_m < n_m;\ i_m\texttt{++})
\end{array}
$$

How many iterations are there in total?

For each choice of the n_1 values of i_1 we choose each of the n_2 values for i_2 ... for each of which we choose the n_m possible values of i_m. Thus there are $n_1 \cdot n_2 \dots n_m$ iterations in total.

Suppose that there is a bug and that errors are equally likely at any level of the iteration.

(a) What is the probability that the bug is in the last iteration?
The program is in the last iteration n_m times. Thus $P = \dfrac{n_m}{n_1 \cdot n_2 \dots n_m} = \dfrac{1}{n_1 \cdot n_2 \dots n_{m-1}}$.

Warning Note that the multiplication rule assumes that the sets are independent, meaning that the choice from the first set does not effect the choice from the second and so on.

Example 5

1. If in the above example the counters depended on the previous one the multiplication rule would not apply.

$$
\begin{array}{l}
\text{for}(i_1 = 0;\ i_1 < n_1;\ i_1 \mathrel{\texttt{+=}} 2) \\
\quad \text{for}(i_2 = i_1 + 1;\ i_2 < n_2;\ i_2\texttt{++}) \\
\qquad \ddots \\
\qquad\quad \text{for}(i_m = 0;\ i_m < n_m - i_2;\ i_m\texttt{++})
\end{array}
$$

2. Suppose we wish to enumerate the number of options the user has in a menu system. Generally the number of options available in the second step will depend on the first option chosen.

   E_1 ={ File, Edit }
   E_{File} ={ New, Load, Save, Print }
   E_{Edit} ={ Cut, Copy, Paste }

   Number of options is 7.

2.3 The Disjoint Addition Rule

Theorem 6 (Disjoint Addition Rule) *Given m* **disjoint** *Sets $A_1, A_2, \ldots, A_m$ then*

$$|A_1 \cup A_2 \cup \ldots \cup A_m| = |A_1| + |A_2| + \ldots + |A_m| .$$

Example 7

1. In a collection of movies there are 10 horror films, 4 comedies and 5 cartoon classics. How many ways are there to chose 2 movies from different categories?

   There are 40 ways to choose a horror and a comedy.
   There are 50 ways to choose a horror and a cartoon.
   There are 20 ways to choose a comedy and a cartoon.

   Thus in total there are $40 + 50 + 20 = 110$ ways to choose.

   (a) Given the information above, what is the probability that we get a horror film and a comedy?

   There are 40 ways to choose a horror and a comedy out of a total of 110, so $P(H\&C) = \frac{40}{110} = \frac{4}{11} \approx 0.3636$

2. How many integers between 0 and 1000 have exactly one digit equal to 3.

   We break this problem down into 3 easier problems:
   How many one digit integers have exactly one digit equal to 3. (A_1)
   How many two digit integers have exactly one digit equal to 3. (A_2)
   How many three digit integers have exactly one digit equal to 3. (A_3)

   The first case is obviously $|A_1| = 1$.

   For the second case: if the second digit is a 3 we have 8 choices for the first (not 0 or 3). If the first digit is a 3 we have 9 choices for the second. Thus $|A_2| = 8 + 9 = 17$.

   Finally for the third case: if the first digit is a 3 there are 9×9 choices for the other two. Now suppose that the first digit is not 0 or 3 (8 possibilities), if the second is a three there are 9 choices for the third; similarly if the third is a three there are 9 choices for the second digit. Thus $|A_3| = 9 \times 9 + 8 \times 9 \times 2 = 81 + 72 \times 2 = 225$

   So the total number is $|A_1| + |A_2| + |A_3| = 1 + 17 + 225 = 243$.

(a) Suppose that a PIN is an integer between 0 and 1000, what is the probability that a random guess will reveal a PIN?
$P(x = \text{PIN}) = \frac{1}{1000}$.

(b) If we observe that the PIN includes exactly one 3, what is the probability that a random guess will reveal a PIN?
$P(x = \text{PIN}) = \frac{1}{243} \approx 0.0041152263374$

(c) What is the probability that a random integer between 0 and 1000 will contain exactly one 3?
$P(3 \in x) = \frac{243}{1000} = 0.243 \approx \frac{1}{4}$.

3. Variable length passwords. Above we required passwords to be 8 characters, but most systems allow for variable length passwords. How many passwords of length 6 to 8 made up of the 68 symbols `[0-9]`, `[A-z]`, `!`, `#`, `$`, `%`, `&`, `*` are there?

A_1 = passwords of length 6, $|A_1| = 68^6 = 98867482624 \approx 10^{10}$
A_2 = passwords of length 7, $|A_2| = 68^7 \approx 6.7229888184 \times 10^{12}$
A_3 = passwords of length 6, $|A_3| = 68^8 \approx 4.5716323965 \times 10^{14}$

$|A_1| + |A_2| + |A_3| \approx 4.6398509595 \times 10^{14}$.

(a) Suppose that we know that a user has only a 6 digit password, what is the probability that a random guess will find the correct password?
$P(x = \text{password}) = \frac{1}{98867482624}$

(b) What is the probability that a randomly generated password will contain 7 characters?
$P(x = 7 \text{ character password}) = \frac{68^7}{4.63985 \times 10^{14}} \approx 0.147$.

Note that almost all passwords in this set have length 8.

Theorem 8 (Contained Subtraction Rule) *Given two sets A and B with $B \subseteq A$, then $|A - B| = |A| - |B|$.*

Example 9
How many of the password above do not have length 7?
Total - those of length 7 $= 4.6398509595 \times 10^{14} - 6.7229888184 \times 10^{12} = 4.5726210713 \times 10^{14}$
The Contained Subtraction Rule has an important corollary

Corollary 10 *Given an event A from a sample space S $P(A^c) = 1 - P(A)$.*

Example 11
What is the probability that a random number from 0 to 1000 does not contain exactly one 3?
From the above 243 integers from 0 to 1000 contain a 3. Thus $P((3 \in x)^c) = 1 - P(3 \in x) = 1 - 0.243 = 0.757$

2.4 Inclusion Exclusion

Theorem 12 (Inclusion Exclusion) *Given two sets A and B, $|A \cup B| = |A| + |B| - |A \cap B|$*

Note that the addition rule is a direct corollary of this Theorem.

Example 13

1. How many integers from 1 to 1000 are divisible by either 3 or 5.

   The number of integers from 1 to 1000 divisible by 3 is $\lfloor \frac{1000}{3} \rfloor = 333$.

   The number of integers from 1 to 1000 divisible by 5 is $\lfloor \frac{1000}{5} \rfloor = 200$.

   An integer is divisible by both 3 and 5 if and only if it is divisible by 15 (note that this is only true because $\gcd(3,5) = 1$). The number of integers from 1 to 1000 divisible by 15 is $\lfloor \frac{1000}{15} \rfloor = 66$.

   Thus the number of integers from 1 to 1000 divisible by either 3 or 5 is $333 + 200 - 66 = 467$.

   (a) What is the probability that a randomly chosen integer is divisible by either 3 or 5?
   $P((3 \mid x) \vee (5 \mid x)) = \frac{467}{1000} = 0.467$.

   (b) What is the probability that a randomly chosen integer is divisible by neither 3 nor 5?
   $P(\sim((3 \mid x) \vee (5 \mid x))) = 1 - 0.467 = 0.533$.

2. How many integers from 1 to 1000 are divisible by either 6 or 10.

   The number of integers from 1 to 1000 divisible by 6 is $\lfloor \frac{1000}{6} \rfloor = 166$.

   The number of integers from 1 to 1000 divisible by 10 is $\lfloor \frac{1000}{10} \rfloor = 100$.

   $\gcd(6,10) = 2$, so of the 166 integers divisible by 6, they will also be divisible by 10 if they are also divisible by $\frac{10}{\gcd(6,10)} = 5$.

   So an integer is divisble by both 5 and 6 if and only if it is divisible by 30. $\lfloor \frac{1000}{30} \rfloor = 33$.

   (Note that 30 is the lcm (least common multiple) of 6 and 10)

   Thus the number of integers from 1 to 1000 divisible by either 6 or 10 is $166 + 100 - 33 = 233$.

   (a) What is the probability that a randomly chosen integer is divisible by either 6 or 10?
   $P((x \mid 6) \vee (x \mid 10)) = \frac{233}{1000} = 0.233$.

   (b) What is the probability that a randomly chosen integer is divisible by neither 6 nor 10?
   $P(\sim((x \mid 6) \vee (x \mid 10))) = 1 - 0.233 = 0.767$.

Theorem 14 (3-way Inclusion Exclusion) *Given 3 sets A, B and C,* $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$