# Discrete Mathematics
# Two useful principles

Saad Mneimneh

## 1 The inclusion-exclusion principle

I have 50 pairs of socks of which 30 are black and 35 are cotton. How many pairs of socks are black and cotton? If I call the set of black socks $A$ and the set of cotton socks $B$, we are looking at $|A \cap B|$. It is not hard to see that:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

because every element that belongs to both $A$ and $B$ is counted twice by $|A|+|B|$, so we subtract the size of the intersection once. Therefore, there are 30+35-50=15 socks that are black and cotton. Note that this assumes that I don't have any red socks for instance. Otherwise, the best claim we can make is that we have at least 15 socks and that black and cotton (because $|A \cup B|$ would be less or equal to 50 and not exactly 50). The formula above represents the simplest form of the inclusion-exclusion principle. We first include the contribution of each set, then we exclude the contribution of their intersection.

Here's another example: at a party of 12 people, each person knows at least $m$ others. How large must $m$ be to guarantee that we can find three people that know each other? Observe that when $m = 6$ there is no such guarantee because it is possible to have two groups of size 6 where knowledge is across groups only. What if $m > 6$? Here's a proof that this is sufficient. Pick any person $p_1$ and let $S_1$ be the set of people known to $p_1$. Now $|S_1| > 6$, so pick a person in $S_1$, say $p_2$, and let $S_2$ be the set of people known to $p_2$. Note that $|S_2| > 6$ also. If we can prove that $S_1 \cap S_2$ is not empty, then we find a person known to $p_1$ and $p_2$ and we are done. Now $|S_1| > 6$, $|S_2| > 6$, and $|S_1 \cup S_2| \leq 12$. Therefore,

$$|S_1 \cap S_2| = |S_1| + |S_2| - |S_1 \cup S_2| > 6 + 6 - 12 = 0$$

## 2 What about more than two sets?

The inclusion-exclusion principle can be generalized to more than two sets. Let's consider the example of three sets $A$, $B$, and $C$. What is $|A \cup B \cup C|$? If we sum $|A| + |B| + |C|$, every element that belongs to two sets has been counted twice. So, we can subtract once those elements by computing $|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C|$. But what if an element belongs to all three sets?

It has been included three times, then excluded three times. We must include it once again. This can be done by adding $|A \cap B \cap C|$. Therefore,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Using a similar argument, one could show that

$$|A \cup B \cup C \cup D| = |A| + |B| + |C| + |D|$$
$$-|A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D|$$
$$+|A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D|$$
$$-|A \cap B \cap C \cap D|$$

and in general,

$$|S_1 \cup S_2 \cup \ldots \cup S_r| = \sum_i |S_i| - \sum_{i<j} |S_i \cap S_j| + \sum_{i<j<k} |S_i \cap S_j \cap S_k| - \ldots + (-1)^{r-1} |S_1 \cap S_2 \cap \ldots \cap S_r|$$

The proof is easy. Consider an element that belongs to $t$ sets. This element will contribute $\left(\begin{array}{c} t \\ 1 \end{array}\right)$ to the first term, $\left(\begin{array}{c} t \\ 2 \end{array}\right)$ to the second term, ..., and $\left(\begin{array}{c} t \\ t \end{array}\right)$ to the $t^{th}$ term. Therefore, the total contribution of each element is:

$$\left(\begin{array}{c} t \\ 1 \end{array}\right) - \left(\begin{array}{c} t \\ 2 \end{array}\right) + \ldots + (-1)^{t-1} \left(\begin{array}{c} t \\ t \end{array}\right)$$
$$= \left(\begin{array}{c} t \\ 0 \end{array}\right) - \left(\begin{array}{c} t \\ 0 \end{array}\right) + \left(\begin{array}{c} t \\ 1 \end{array}\right) - \left(\begin{array}{c} t \\ 2 \end{array}\right) + \ldots + (-1)^{t-1} \left(\begin{array}{c} t \\ t \end{array}\right)$$
$$= \left(\begin{array}{c} t \\ 0 \end{array}\right) - \left[\left(\begin{array}{c} t \\ 0 \end{array}\right) - \left(\begin{array}{c} t \\ 1 \end{array}\right) + \left(\begin{array}{c} t \\ 2 \end{array}\right) - \ldots + (-1)^t \left(\begin{array}{c} t \\ t \end{array}\right)\right]$$
$$= 1 - (1-1)^t$$

The above is 1 when $t > 0$ and 0 when $t = 0$ (the element does not exist).

## 3 The lazy professor revisited

Assume we want to count the number of ways we can permute tests among students without any student receiving his/her own test. If we number the students and their respective tests from 1 to $n$, then let us call a permutation bad if it assigns test $i$ to student $i$ for some $i$. We will count the number of bad permutations and then subtract that number from $n!$ (the total number of permutations).

Let $S_i$ be the set of permutations that assign test $i$ to student $i$. We want $|S_1 \cup S_2 \cup \ldots \cup S_n|$. Observe that $|S_i| = (n-1)!$. Similarly, $|S_i \cap S_j| = (n-2)!$, $|S_i \cap S_j \cap S_k| = (n-3)!$, etc... So:

$$|S_1 \cup S_2 \cup \ldots \cup S_n| = \left(\begin{array}{c} n \\ 1 \end{array}\right)(n-1)! - \left(\begin{array}{c} n \\ 2 \end{array}\right)(n-2)! + \ldots + (-1)^{n-1}\left(\begin{array}{c} n \\ n \end{array}\right)(n-n)!$$

Expanding, we get:

$$|S_1 \cup S_2 \cup \ldots \cup S_n| = \frac{n!}{1!} - \frac{n!}{2!} + \ldots + (-1)^{n-1}\frac{n!}{n!} = n!\Big[\frac{1}{1!} - \frac{1}{2!} + \ldots + (-1)^{n-1}\frac{1}{n!}\Big]$$

Therefore, the number of good permutations is

$$n!\Big[1 - \Big(\frac{1}{1!} - \frac{1}{2!} + \ldots + (-1)^{n-1}\frac{1}{n!}\Big)\Big] = n!\Big[\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^{n}\frac{1}{n!}\Big]$$

When $n$ is large enough, this is approximately $n!/e$, where $e = 2.71828$. Therefore, if a random permutation is performed, the probability that no student will receive his/her own test is $1/e \approx 37\%$.

# 4 Divisibility

Consider the problem of finding all integers $\leq 1000$ that are divisible by 2 or 3 or 5. Let $S_2$ be the set of integers $\leq 1000$ that are divisible by 2. Define $S_3$ and $S_5$ similarly. Then what we seek is $|S_2 \cup S_3 \cap S_5|$. Now $|S_2| = \lfloor 1000/2 \rfloor = 500$, $|S_3| = \lfloor 1000/3 \rfloor = 333$, and $|S_5| = \lfloor 1000/5 \rfloor = 200$. Since 2 and 3 are both primes, numbers that are divisible by 2 and 3 are exactly the numbers divisible by 6 (we will learn this from number theory). Therefore, $|S_2 \cap S_3| = \lfloor 1000/6 \rfloor = 166$. Similarly, $|S_2 \cap S_5| = \lfloor 1000/10 \rfloor = 100$, $|S_3 \cap S_5| = \lfloor 1000/15 \rfloor = 66$, and $|S_2 \cap S_3 \cap S_5| = \lfloor 1000/30 \rfloor = 33$.

$$|S_2 \cup S_3 \cup S_5| = 500 + 333 + 200 - 166 - 100 - 66 + 33 = 734$$

# 5 Euler's totient function

Euler asked the following question (it looks like he has been really busy): How many integers $\leq n$ are relatively prime with $n$? Let us consider the example of $n = 60$. If an integer is relatively prime with 60, then it cannot share any prime factor with 60. So let us count the opposite. In other words, how many integers $\leq 60$ share a prime factor with 60? We can write 60 as a product of primes $2^3 \cdot 3 \cdot 5$. Any integer $\leq 60$ that has 2, 3, or 5 as a prime factor is a candidate. How many integers are there? Let $S_2$ be the set of integers $\leq 60$ that has 2 as a prime factor. Define $S_3$ and $S_5$ similarly. We want $|S_2 \cup S_3 \cup S_5|$.

$$|S_2 \cup S_3 \cup S_5| = |S_2| + |S_3| + |S_5| - |S_2 \cap S_3| - |S_2 \cap S_5| - |S_3 \cap S_5| + |S_2 \cap S_3 \cap S_5|$$

Obviously, $|S_2| = 60/2$, $|S_3| = 60/3$, $S_5 = 60/5$. Similarly, $|S_2 \cap S_3| = 60/(2 \cdot 3)$; this is true because both 2 and 3 are primes. If we continue this way, we find that:

$$|S_2 \cup S_3 \cup S_5| = \frac{60}{2} + \frac{60}{3} + \frac{60}{5} - \frac{60}{2 \cdot 3} - \frac{60}{2 \cdot 5} - \frac{60}{3 \cdot 5} + \frac{60}{2 \cdot 3 \cdot 5} = 44$$

Therefore, the number of integers $\leq 60$ that are relatively prime with 60 is $60 - 44 = 16$. In general, if $n$ has the prime factors $p_1, p_2, \ldots, p_r$, then

$$\begin{aligned} \phi(n) &= n - \Big[\sum_i \frac{n}{p_i} - \sum_{i<j} \frac{n}{p_i p_j} + \sum_{i<j<k} \frac{n}{p_i p_j p_k} - \ldots + (-1)^{r-1} \frac{n}{p_1 \ldots p_r}\Big] \\ &= n - \sum_i \frac{n}{p_i} + \sum_{i<j} \frac{n}{p_i p_j} - \sum_{i<j<k} \frac{n}{p_i p_j p_k} + \ldots + (-1)^r \frac{n}{p_1 \ldots p_r} \end{aligned}$$

It is not hard to verify that the above is equal to:

$$\phi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \ldots \Big(1 - \frac{1}{p_r}\Big)$$

because every combination of the prime factors in the denominator (including the empty one) appears with the appropriate sign.

# 6 Counting passwords

A good password must include at least one digit, at least one lower case letter, and at least one upper case letter. How many good passwords of length $n \geq 3$ are there? A password is bad if it fails any of the three criteria above. But it is easy to count passwords that fail a given criteria. For instance, the number of password that do not contain a any digit is $52^n$ because each character of the password can be any of $\{a, \ldots z, A, \ldots, Z\}$. By inclusion-exclusion it should be feasible to count all bad passwords. Then we subtract that number from $62^n$, which is the total number of passwords (where any every character can be any of $\{0, \ldots, 9, a, \ldots z, A, \ldots, Z\}$. Let us define $S_0$ to be the set of all passwords with no digits, $S_a$ with no lower case letters, and $S_A$ with no upper case letters. Then $|S_0| = 52^n$, $|S_a| = 36^n$, $|S_A| = 36^n$, $|S_0 \cap S_a| = 26^n$, $|S_0 \cap S_A| = 26^n$, $|S_a \cap S_A| = 10^n$, and $|S_0 \cap S_a \cap S_A| = 0$. Therefore, the number of good passwords is

$$62^n - (52^n + 36^n + 36^n - 26^n - 26^n - 10^n + 0)$$

Observe that when we replace $n$ by 3 in the above expression, we get $40560 = 10 \times 26 \times 26 \times 3!$ (why?). Could we have done the following: choose three characters from $n$ with order, make them a digit, a lower case letter, and an upper case letter respectively, then choose the rest of the characters in $62^{n-3}$ ways? This would give

$$\frac{n!}{(n-3)!} \times 10 \times 26 \times 26 \times 62^{n-3}$$

which works when $n = 3$.

# 7 How many solutions?

How many solutions are there to the following system?

$$x_1 + \ldots + x_n = k$$

$$\forall i, a < x_i < b$$

where $k$, $a$, and $b$ are all integers.

We know how to handle the lower bound. Since each $x_i \geq a+1$, we can rewrite the equation as:

$$x_1 + \ldots + x_n = k - n(a+1)$$

$$\forall i, 0 \leq x_i < b - a - 1$$

The number of solutions ignoring the upper bound is $\left( \begin{array}{c} k-na-1 \\ n-1 \end{array} \right)$. From this number, we need to subtract the solutions in which some $x_i \geq b-a-1$. Using the inclusion-exclusion principle, this is:

$$\left( \begin{array}{c} k-na-1 \\ n-1 \end{array} \right) - \left( \begin{array}{c} n \\ 1 \end{array} \right) \left( \begin{array}{c} k-na-1-(b-a-1) \\ n-1 \end{array} \right) + \left( \begin{array}{c} n \\ 2 \end{array} \right) \left( \begin{array}{c} k-na-1-2(b-a-1) \\ n-1 \end{array} \right) - \ldots$$

$$= \sum_{i=0}^{n} (-1)^i \left( \begin{array}{c} n \\ i \end{array} \right) \left( \begin{array}{c} k-na-1-i(b-a-1) \\ n-1 \end{array} \right)$$

where we define $\left( \begin{array}{c} x \\ n-1 \end{array} \right) = 0$ if $x < n-1$.

# 8 The pigeonhole principle revisited

The generalized pigeonhole principle states that if $m$ objects are to be placed in $n$ boxes, at least one box will contain at least

$$\left\lfloor \frac{m-1}{n} \right\rfloor + 1$$

objects, where $\lfloor x \rfloor$ is the largest integer less than or equal to $x$ (similarly, $\lceil x \rceil$ is the smallest integer greater than or equal to $x$, question: is $\lfloor x \rfloor + 1 = \lceil x \rceil$?). When $m = n+1$, the above evaluates to 2 giving the standard pigeonhole principle. The proof of the pigeonhole principle is again by contradiction. Assume every box has at most $\lfloor \frac{m-1}{n} \rfloor$ objects. Then the total number of objects is at most $\lfloor \frac{m-1}{n} \rfloor n \leq \frac{m-1}{n} n = m - 1$, a contradiction.

Although the pigeonhole principle is stated as such, when $m$ and $n$ are both positive integers, $\lfloor \frac{m-1}{n} \rfloor + 1 = \lceil \frac{m}{n} \rceil$. Therefore, one interpretation of the pigeonhole principle is the following. To minimize the occupancy of every box, the best strategy is to evenly distribute $m$ among the $n$ boxes. If $m$ is fluid, then each box will contain exactly an amount of fluid equal to $m/n$. The pigeonhole principle cannot claim an occupancy that exceeds that. But since $m$ does not represent a fluid amount, the formula is adjusted to $\lceil\frac{m}{n}\rceil$. In fact, the same proof by contradiction can be constructed for $\lceil\frac{m}{n}\rceil$.

An example of applying the pigeonhole principle is the following: we shoot 10 bullets on a $3 \times 3$ square target. Prove that two bullets are within a distance of 1.5 from each other. We can divide the square into 9 unit squares (the boxes). Since we have 10 bullets, two of them must land in the same box. The distance between two points in the unit square is at most that of a diagonal, which is $\sqrt{2} < 1.5$.

Another example is the following: at least 4 of any set of 44 people are born in the same month! This is equivalent to "placing" 44 people in 12 boxes (each month is a box). One box will contain at least $\lfloor\frac{44-1}{12}\rfloor + 1 = 4$ people.

While making the pigeonhole argument is typically trivial, modeling the problem is such as way that the pigeonhole principle becomes applicable is the hard part. Sometimes it is really not obvious! Let's take a simplified version of the Dirichlet approximation theorem. For any real number $\alpha$ and any integer $n$, there exist integers $p$ and $1 \leq q \leq n$ such that

$$|q\alpha - p| \leq \frac{1}{n}$$

Here's a proof using the pigeonhole principle: consider the following $n+1$ numbers:

$$\beta_1 = \alpha - \lfloor\alpha\rfloor$$
$$\beta_2 = 2\alpha - \lfloor 2\alpha\rfloor$$
$$\vdots$$
$$\beta_{n+1} = (n+1)\alpha - \lfloor(n+1)\alpha\rfloor$$

By definition of $\lfloor\ \rfloor$, we have $0 \leq \beta_i < 1$ for $i = 1, \ldots n+1$. Divide the interval $[0, 1]$ into $n$ "boxes" of equal size. Two of the above $n+1$ numbers must end up in the same box. Therefore, for some $i > j$

$$|\beta_i - \beta_j| = |(i-j)\alpha - (\lfloor i\alpha\rfloor - \lfloor j\alpha\rfloor| \leq \frac{1}{n}$$

Finally, set $q = i - j$ and $p = \lfloor i\alpha\rfloor - \lfloor j\alpha\rfloor$. Note that $1 \leq q \leq n$ and $p \geq 0$.

The following are two problems by Erdös: Given the set $S = \{1, 2, \ldots, 2n\}$, pick $n+1$ numbers in $S$. Then,

- two must be consecutive
- two must be such that one divides the other

Both can be proved using the pigeonhole principle. To prove the first, construct the following $n$ "boxes": $\{1, 2\}, \{3, 4\}, \ldots, \{2n-1, 2n\}$. Now imagine that to pick a number you must place a ball in the appropriate box. Two of the $n+1$ balls must fall in the same box and, therefore, two numbers must be consecutive. To prove the second, construct the following $n$ "boxes":

$$\{1,2,4,\ldots\}$$
$$\{3,6,12,\ldots\}$$
$$\{5,10,20,\ldots\}$$
$$\vdots$$
$$\{2n-1\}$$

In other words, for every odd number $i \in S$, construct a subset of $S$

$$S_i = \{x | x \in S \text{ and } x = i \cdot 2^k, k = 0,1,2,\ldots\}$$

Every number in $S$ must belong to one of these subsets because every number can be written as an odd number multiplied by a power of 2 (if we keep dividing it by 2 we eventually reach an odd number). Here's an example when $n = 5$, i.e. $S = \{1,2,3,4,5,6,7,8,9,10\}$.

$$S_1 = \{1,2,4,8\}$$
$$S_3 = \{3,6\}$$
$$S_5 = \{5,10\}$$
$$S_7 = \{7\}$$
$$S_9 = \{9\}$$

Again, two of the $n+1$ numbers must fall in the same box and hence one of them can be written as $i \cdot 2^k$ and the other as $i \cdot 2^{k'}$. Therefore, one must divide the other.

Here's a final example (also by Erdös) before we move to another section on the application of the pigeonhole principle: Consider a sequence of any $n^2+1$ different numbers $a_1, a_2, \ldots a_{n^2+1}$. There is a monotonous subsequence of $n+1$ numbers, where monotonous means either increasing or decreasing. Here's an example when $n = 2$:

$$10 \quad 4 \quad 13 \quad 8 \quad 21$$

There is obviously an increasing sequence of length $n+1 = 3$. How to prove this for any $n$? Let $t_i$ be the length of the largest increasing sequence starting at $a_i$. The $t_i$'s are shown for the above sequence:

$$10 \quad 4 \quad 13 \quad 8 \quad 21$$
$$3 \quad 3 \quad 2 \quad 2 \quad 1$$

If there is an increasing sequence of length $n+1$, we are done. Otherwise, $t_i \leq n$ for all $i$. Therefore, by the pigeonhole principle there must be

$$\left\lfloor \frac{(n^2+1)-1}{n} \right\rfloor + 1 = n+1$$

$t_i$'s that have the same value. We claim that the corresponding $a_i$'s form a decreasing sequence. Take any two of these, say $a_i$ and $a_j$ with $i < j$. If $a_i < a_j$, then $t_i \geq t_j + 1$, a contradiction since $t_i = t_j$. Therefore, $a_i > a_j$.

# 9 The birthday paradox

The pigeonhole principle tells us that in a group of 367 people there must be at least two with the same birthday (there are only 366 possible birthdays). But much less is required to guarantee this with a high probability. Let's generalize the setting. Given that we choose $k$ elements from a set of size $n$ (ordered selection), what is the probability that all elements are distinct? Well, there are $n!/(n-k)!$ ways of ending up with distinct elements among the total number of possibilities $n^k$ (ordered selection with repetition).

$$p = \frac{n!}{(n-k)!n^k} = \frac{n(n-1)\dots(n-k+1)}{n^k}$$

$$\ln p = \ln\frac{n-1}{n} + \ln\frac{n-2}{n} + \dots + \frac{n-k+1}{n}$$

It is known that $\ln x \leq x - 1$ and, therefore,

$$\ln\frac{n-i}{n} \leq \frac{n-i}{n} - 1 = \frac{n-i-n}{n} = -\frac{i}{n}$$

$$\ln p \leq -\frac{1}{n} - \frac{2}{n} - \dots - \frac{k-1}{n} = -\frac{k(k-1)}{2n}$$

$$p \leq e^{-\frac{k(k-1)}{2n}}$$

Applying this to our birthday problem, in a group of 50 people, the probability that no two will have the same birthday is at most

$$e^{-\frac{50(50-1)}{2\times 366}} < 0.036$$

This means more than 96% chance of finding two people with the same birthday.

# 10 Simplified Ramsey theory (also pigeonhole)

I will start this section by a famous example. In a group of six people there are three mutual friends or three mutual strangers. The proof of this is by pigeonhole and goes as follows: consider person 1. The other five fall into one of two "boxes" (sets):

$$F = \{\text{friends of person 1}\}$$

$$S = \{\text{strangers to person 1}\}$$

By pigeonhole, one of the above sets must have at least

$$\left\lfloor\frac{5-1}{2}\right\rfloor + 1 = 3$$

people. If $|F| \geq 3$, then either we have three mutual strangers in $F$, or there is a pair of friends. Grouping the pair of friends in $F$ with person 1 gives three mutual friends. Similarly, if $|S| \geq 3$, then either we have three mutual friends in $S$, or there is a pair of strangers. Grouping the pair of strangers in $S$ with person 1 gives three mutual strangers.

Let $N(a, b)$ be the number of people required to find $a$ mutual friends or $b$ mutual strangers. We can show that $N(a, b) \leq N(a-1, b) + N(a, b-1)$. Before we do this, let's consider a variant of the pigeonhole principle: If $m_1 + m_2 + \ldots + m_n - n + 1$ objects are placed in $n$ boxes, then the first box will contain at least $m_1$ objects, or the second box will contain at least $m_2$ objects, ..., or the $n^{\text{th}}$ box will contain at least $m_n$ objects. This can be easily shown by contradiction: If box $i$ contains at most $m_i - 1$ objects, then the total number of objects is at most $m_1 + m_2 + \ldots + m_n - n$, a contradiction.

Now back to $N(a, b)$. Given a set of $N(a-1, b) + N(a, b-1)$ people, consider person 1. Divide the other $N(a-1, b) + N(a, b-1) - 1 = N(a-1, b) + N(a, b-1) - 2 + 1$ people into $F$ and $S$ as before. Either $|F| \geq N(a-1, b)$ or $|S| \geq N(a, b-1)$.

If $|F| \geq N(a-1, b)$ then we find $a-1$ mutual friends or $b$ mutual strangers. If it's $b$ mutual strangers we are done. If it's $a-1$ mutual friends, adding person 1 results in $a$ mutual friends. The case for $|S| \geq N(a, b-1)$ can be argued similarly.

Finally, observe that $N(a, 2) = a$ and that $N(a, b) = N(b, a)$. Therefore, $N(a, b)$ is finite for all $a, b \geq 2$. In particular, $N(a, a)$ is finite for all $a \geq 2$.

Imagine a complete graph (all edges are present) where the edges are colored either blue or red. For a given $a$, Ramsey's theory tells us that any such graph, if large enough, must either contain a set of $a$ vertices where every pair is connected by a blue edge, or a set of $a$ vertices where every pair is connected by a red edge. In other words, the graph must contain a "homogeneous" set of $a$ vertices. **This result can be generalized to any number of colors**. Can you use this result to prove a weaker version of the monotonous subsequence result, i.e. that given a large enough sequence of different numbers, there must be a large enough increasing or decreasing subsequence?

# 11 Program termination by Ramsey

Consider the following program in pseudocode where $x = \{...\}$ assigns $x$ a value from the set, and $(x, y) = (..., ...)$ simultaneously assigns $x$ and $y$ their values:

```
(x,y,z)=({1,...,n},{1,...,n},{1,...,n})
while x>0 and y>0 and z>0
  control={1,2,3}
  if control==1 then
    (x,y,z)=(x+1,y-1,z-1)
  else
  if control==2 then
    (x,y,z)=(x-1,y+1,z-1)
  else
    (z,y,z)=(x-1,y-1,z+1)
```

It is typical to prove that a program terminates by finding a quantity that is always decreasing. In the above program, obviously $x+y+z$ decreases by 1 after every iteration. Therefore, one of $x$, $y$, or $z$ will eventually reach zero and the program will terminate. However, it is not always possible to find a decreasing quantity, like in the following program:

```
(x,y,z)=({1,...,n},{1,...,n},{1,...,n})
while x>0 and y>0 and z>0
  control={1,2}
  if control==1 then
    x={x,...,n}
    y={y,...,n}
    z=z-1
  else
    y={y,...,n}
    x=x-1
```

Let $x_i$ be the value of $x$ in iteration $i$. For every pair of iterations $i < j$, we can show that either $x_j < x_i$ or $z_j < z_i$: If between iterations $i$ and $j$ we ever have control=1 then $z$ will decrease. If we only have control=2 then $x$ will decrease. Now assume that the program runs for $I$ iterations. Construct a graph with $I$ vertices where each vertex represents an iteration. Make edge $(i,j)$ blue if $x_j < x_i$ and edge $(i,j)$ red if $z_j < z_i$. By Ramsey's theory, there is a large set of vertices (iterations) that are homogeneous (either all connected by blue or all connected by red). If the color is blue (or red), then $x$ (or $z$) is decreasing in these iterations. Since $x \leq n$ (and $z \leq n$) at all times, there must be a choice of $I$ that will make $x$ (or $z$) go to zero. The program cannot run for more than $I$ iterations.

Another way to prove the termination of this program is by constructing a partial order relation. Consider the following relation on the tuples of the form $(z_i, x_i, y_i)$, where $z_i, x_i, y_i$ are the values of the variable in iteration $i$.

$$(z_i, x_i, y_i) \prec (z_j, x_j, y_j) \Leftrightarrow (z_i < z_j) \vee (z_i = z_j \wedge x_i < x_j)$$

It is easy to verify that $\prec$ is a partial order relation (simply verify anti-symmetry and transitivity). Further more, $(z_{i+1}, x_{i+1}, y_{i+1}) \prec (z_i, x_i, y_i)$ (either $z$ decreases or $x$ decreases and $z$ remains the same). This means some veriable ($x$ or $z$) will reach zero.