1 The division rule

In how many ways can we place two *identical* rooks on an 8 by 8 chessboard so that they occupy different rows and different columns?

Let's first count the number of configurations for two *different* rooks. Each configuration can then be represented by a sequence (r_1r, r_1c, r_2r, r_2c) indicating the row and column of the first and second rook, respectively. By the generalized product rule, the set of configurations $C_{\text{different}}$ has size

$$|C_{\text{different}}| = 8 \cdot 8 \cdot 7 \cdot 7 = (8 \cdot 7)^2.$$

Now let $C_{\text{identical}}$ be the set of configurations when the two rooks are identical. We won't count the number of elements of $C_{\text{identical}}$ directly but take advantage of what we know already. Each configuration in $C_{\text{identical}}$ can be naturally represented by a *pair* of sequences in $C_{\text{different}}$. For example, the configuration in $C_{\text{identical}}$ in which one rook is at position $(1, 1)$ and the second one is at $(2, 3)$ is represented by the pair of sequences $(1, 1, 2, 3)$ and $(2, 3, 1, 1)$ in $C_{\text{different}}$.

Since each element in $C_{\text{identical}}$ is represented by exactly two elements in $C_{\text{different}}$, the set $C_{\text{different}}$ must be exactly twice as large as $C_{\text{identical}}$ and so the desired number of configurations is

$$|C_{\text{identical}}| = \frac{|C_{\text{different}}|}{2} = \frac{(8 \cdot 7)^2}{2}.$$

Here is a general description of this type of counting argument. A function $f\colon X \to Y$ is *k-to-1* if for every y in Y, the number of $x \in X$ such that $f(x) = y$ is exactly k:

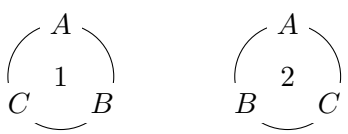
$$|\{x \in X\colon f(x) = y\}| = k \qquad \text{for every } y \in Y.$$

If we want to count the size of Y and have a k-to-1 function from X to Y where X is a set whose size we know, we can conclude that Y has size $|X|/k$.

Theorem 1 (The division rule)**.** *If $f\colon X \to Y$ is k-to-1, then $|Y| = |X|/k$.*

In the example we just did, $f\colon C_{\text{different}} \to C_{\text{identical}}$ is the function that takes the sequence (r_1r, r_1c, r_2r, r_2c) to the configuration in which one rook is at (r_1r, r_1c) and the other one is at position (r_2r, r_2c). Then f is a 2-to-1 map since each configuration in $C_{\text{identical}}$ is mapped to by exactly two sequences in $C_{\text{different}}$. We can conclude that $|C_{\text{identical}}| = |C_{\text{different}}|/2 = (8 \cdot 7)^2/2$.

Circular arrangements In how many ways can we seat n people at a round table? Two seating configurations are the same if one can be obtained from the other by a turn of the table. Such configurations are called *circular arrangements* of a set of n elements. For example, if $n = 3$ and the set is $\{A, B, C\}$, there are two possible circular arrangements:



We can count the number of circular arrangements using the division rule. Let P be the set of all permutations of n people and C be the set of all circular arrangements of these people. For each permutation $(p_1, \ldots, p_n)$, let $f(p_1, \ldots, p_n)$ be the circular arrangement obtained by seating person p_1 at the head of the table, p_2 next to p_1 clockwise, p_3 next to p_2 clockwise, and so on.

For example, when $n = 3$ and the three people are A(lice), B(ob) and C(harlie), then

$$\begin{aligned} f \text{ maps permutations } &(A, B, C),\ (B, C, A),\ (C, A, B) \text{ to circular arrangement 1} \\ \text{and permutations } &(A, C, B),\ (C, B, A),\ (B, A, C) \text{ to circular arrangement 2} \end{aligned}$$

and we see that f is 3-to-1: The $3! = 6$ permutations account for exactly $6/3 = 2$ circular arrangements.

For general n, f is n-to-1: The circular arrangement consisting of p_1, p_2, p_3, up to p_n in clockwise direction is mapped to by the n permutations

$$(p_1, p_2, p_3, \ldots, p_n), \quad (p_2, p_3, \ldots, p_n, p_1), \quad \ldots, \quad (p_n, p_1, \ldots, p_{n-2}, p_{n-1}).$$

Since there are $|P| = n!$ permutations of n people and $f\colon P \to C$ is n-to-1, by the division rule we conclude that there are $|C| = n!/n = (n-1)!$ circular arrangements of n people.

Subsets with a fixed number of elements In the last lecture we showed that a set of size n has exactly 2^n subsets. How many of those subsets are of size exactly k?

For example, a set of size 3 has 3 subsets of size 2. If the set is $\{1, 2, 3\}$ those subsets are

$$\{1, 2\},\ \{1, 3\}, \text{ and } \{2, 3\}.$$

A set of size 5 has 10 subsets of size 3. If the set is $\{1, 2, 3, 4, 5\}$ those subsets are

$$\begin{aligned} &\{1, 2, 3\},\ \{1, 2, 4\},\ \{1, 2, 5\},\ \{1, 3, 4\},\ \{1, 3, 5\}, \\ &\{1, 4, 5\},\ \{2, 3, 4\},\ \{2, 3, 5\},\ \{2, 4, 5\}, \text{ and } \{3, 4, 5\}. \end{aligned}$$

Counting such sets "by hand" may not be very reliable. We can do it systematically using rules from class.

To do this, let X be the set of length k *sequences* of distinct numbers in the set $\{1, \ldots, n\}$. For example, when $n = 3$ and $k = 2$, X is the set

$$X = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 2)\}$$

Each size 2 subset of $\{1, 2, 3\}$ is represented twice by a sequence in X.

For general n and k, we can count the number of sequences in X using the generalized product rule: There are n choices for the first entry, $n-1$ choices for the second entry (for each first entry), $n-2$ choices for the third entry, and so on, until we reach the k-th entry and we are left with $n-k+1$ choices for it. By the generalized product rule,

$$|X| = n \cdot (n-1) \cdots (n-k+1).$$

Now let Y be the number of k-element subsets of the set $\{1, \ldots, n\}$ and $f\colon X \to Y$ be the function that maps each k element sequence to the subset consisting of its entries:

$$f((a_1, \ldots, a_k)) = \{a_1, \ldots, a_k\}.$$

The function f is $k!$-to-1: Each subset is mapped to by the $k!$ permutations of its entries.

By the division rule, we conclude that the size of Y — that is, the number of k-element subsets of $\{1, \ldots, n\}$ — is

$$|Y| = \frac{|X|}{k!} = \frac{n \cdot (n-1) \cdots (n-k+1)}{k!}. \tag{1}$$

This is an important enough number that there is special notation for it: It is written as $\binom{n}{k}$ (read "n choose k"). If we multiply both the numerator and denominator of (1) by $(n-k)!$ we get the nice formula

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

We just proved that

Theorem 2. *The number of k element subsets of an n element set is $\binom{n}{k}$.*

In the last lecture we gave a bijective function f from the set $\{0,1\}^n$ of bit sequences of length n to the set of *all* subsets of $\{1, \ldots, n\}$. The function maps a bit sequence to the set of positions that contain a one in the sequence:

$$f((b_1, \ldots, b_n)) = \{i \colon b_i = 1\}.$$

The size of the set $f((b_1, \ldots, b_n))$ equals the number of one entries in the bit sequence:

$$|f((b_1, \ldots, b_n))| = \text{number of } i \text{ such that } b_i \text{ equals one.}$$

Therefore the map f is a bijective function from (the set of) bit sequences of length n with exactly k ones to (the set of) subsets of $\{1, \ldots, n\}$ of size k. So these two sets have the same size.

Corollary 3. *The number of n bit sequences with exactly k ones is $\binom{n}{k}$.*

2 Poker hands

Five card poker is good setting in which we can practice our counting skills. In case you have never been to a casino, a card deck consists of 52 cards; each card has one of the 13 *face values* 2 3 4 5 6 7 8 9 J Q K A and one of the four *suits* ♠, ♡, ♢, ♣. In five card poker, you are dealt a hand consisting of five different cards, for example

$$8♠\ 9♢\ 2♢\ A♡\ 2♠$$

and you win a prize if your hand is of a special type. We'll apply counting rules to figure out the *probability* of various types of hands, assuming all five card hands are equally likely.

We will think of the card deck as a *set* of 52 cards and the hand as a 5-element subset of it, so the number of possible hands is $\binom{52}{5} = 2,598,960$. This is a large number, so counting hands "by hand" is impractical and we need to resort to the rules we learned.

Four-of-a-kind A hand is a *four-of-a-kind* if it contains four cards with the same value, for example:

$$\{K♠, K♡, K♢, K♣, 3♠\}$$

How many four-of-a-kind hands are there? We can specify a four-of-a-kind sequence completely and uniquely by giving the face value of the four-of-a-kind, the face value of the fifth card, and the suit of the fifth card. There are 13 choices for the face value of the four-of-a-kind. Each of them

leaves out 12 choices for the face value of the fifth card and 4 choices for its suit. By the generalized product rule, the number of four-of-a-kind hands is

$$13 \cdot 12 \cdot 4 = 624.$$

Assuming all five card hands are equally likely, the probability of a four-of-a-kind hand is

$$\frac{\text{number of four-of-a-kind hands}}{\text{number of possible hands}} = \frac{13 \cdot 12 \cdot 4}{\binom{52}{5}} = \frac{624}{2,598,960} \approx 0.00024.$$

Flush A hand is a *flush* if all five cards are of the same suit,[1] for example

$$\{Q\clubsuit, 10\clubsuit, 6\clubsuit, 3\clubsuit, 2\clubsuit\}$$

We can specify a flush uniquely by describing the suit of all the cards in it and their face values. The suit can be chosen in 4 ways and the five face values can be chosen in $\binom{13}{5}$ ways. By the product rule, the number of flushes is $\binom{13}{5} \cdot 4 = 5,148$. Assuming all hands are equally likely, the probability of a flush is $5,148/2,598,960 \approx 0.00198$. A flush is quite a bit more likely than a four-of-a-kind.

Full house A hand is a *full house* if it consists of three cards with one face value and two cards with another face value, for example

$$\{J\spadesuit, J\heartsuit, J\clubsuit, 6\heartsuit, 6\diamondsuit\}.$$

We can specify each full house completely and uniquely by giving the face value of the cards in the triple, the suits of the cards in the triple, the face value of the cards in the pair, and the suits of the cards in the pair. There are 13 choices for the face value of the triple, $\binom{4}{3}$ choices for the suits in the triple (three suits out of a set of four), 12 remaining choices for the face value of the pair, and $\binom{4}{2}$ choices for the suits of the cards in the pair. By the generalized product rule, the number of full house hands is

$$13 \cdot \binom{4}{3} \cdot 12 \cdot \binom{4}{2} = 13 \cdot 4 \cdot 12 \cdot 6 = 3,744.$$

Assuming all five card hands are equally likely, the probability of a full house is $3,144/2,598,960 \approx 0.00121$.

Two pairs A hand is a *two-pairs* if it has two cards of one face value, two cards of another face value, and a fifth card of yet another face value, for example

$$\{K\spadesuit, K\heartsuit, 10\spadesuit, 10\diamondsuit, 3\spadesuit\}.$$

Let us try to count the number of two-pairs hands: There are 13 choices for the face value of the cards in the first pair and $\binom{4}{2}$ choices for their suits; once these have been chosen, there are 12 choices for the face value of the cards in the second pair and $\binom{4}{2}$ choices for their suits. This leaves out 11 choices for the face value of the last card and 4 choices for its suit, giving a total of

$$13 \cdot \binom{4}{2} \cdot 12 \cdot \binom{4}{2} \cdot 11 \cdot 4 = 247,104.$$

This number is *not* an accurate count of the number of two-pairs. Our reasoning does not account for every two-pair hand uniquely! For example, the above hand is counted twice: Once, we count

[1] In poker there is also a "royal flush" and a "straight flush" that are sometimes counted separately. We will include those into our count of flushes.

the pair $\{K\spadesuit, K\heartsuit\}$ as a first pair and the pair $\{10\spadesuit, 10\diamondsuit\}$ as a second pair and the other time we count the two pairs in the opposite order.

Fortunately, our count of 247,104 is not useless. What this number counts is the number of *ordered* two-pairs, namely sequences consisting of a first pair of cards with the same face value, a second such pair of cards with another face value, and a fifth card with a third face value. There is a 2-1 map from the set of ordered two-pairs to the set of two-pairs: The map represents each two-pair by its two orderings. By the division rule, the number of two pairs is half the number of ordered two-pairs, namely $247,104/2 = 123,552$. Assuming equally likely hands, the probability of a two-pair is $123,552/2,598,960 \approx 0.04754$.

We'll count a couple more types of hands that may be of no particular use in poker but are good for counting practice.

All four suits How many hands are there in which each one of the four suits is represented, for example $\{2\spadesuit, 3\heartsuit, 3\diamondsuit, A\spadesuit, 6\clubsuit\}$ but not $\{7\spadesuit, 6\clubsuit, Q\diamondsuit, 10\spadesuit, 6\clubsuit\}$ ($\heartsuit$ is not represented).

We can describe each such hand by specifying a sequence consisting of the face values of four cards in four different suits (say in the order $\spadesuit, \heartsuit, \diamondsuit, \clubsuit$), plus a face value and a suit for the additional card. For example, the tuple $(10, A, 3, J, 5\diamondsuit)$ would represent the hand $H = \{10\spadesuit, A\heartsuit, 3\diamondsuit, J\clubsuit, 5\diamondsuit\}$. There are 13 choices for each of the first four face values; once these are fixed, there are 12 choices for the face value of the last card and 4 for its suit, so the number of desired sequences is $13^4 \cdot 12 \cdot 4$. The function that maps a sequence to the corresponding hand is 2-1: the last card in the sequence can be swapped with the one of the same suit among the first four. For example, the sequence $(10, A, 5, J, 3\diamondsuit)$ also represents the hand H. By the division rule, the number of hands in which all four suits are represented is $13^2 \cdot 12 \cdot 4/2 = 685,464$.

At least one ace Sometimes the size of the set can be figured out more easily by looking at its complement. How many hands are there that have *at least one* ace? Let A be the set of such hands. The complement of A is the set $\overline{A}$ of hands that do not contain an ace. The sets A and $\overline{A}$ partition all hands, so by the sum rule,

$$|A| + |\overline{A}| = \binom{52}{5}.$$

How many hands are there that do not contain an ace? Each such hand is a 5-element subset of the 48-element set obtained by taking out the four aces from the pack of cards and so $|\overline{A}| = \binom{48}{5}$. Therefore

$$|A| = \binom{52}{5} - \binom{48}{5} = 2,598,960 - 1,712,304 = 886,656.$$

One good way to check your answer is to try and solve the same problem in a different way. To do this, I wrote a computer program that counts the number of hands of a given kind by going over all possible five-card hands and counting only those that are of the appropriate kind. The program is a bit slow as it has to check almost 2.3 million hands each time. However it does eventually produce answers, and they are the same as the ones we calculated using counting rules.

3 Inclusion-exclusion

The sum rule allows us to calculate the size of a union of sets as a sum of the sizes of the sets, provided the sets are disjoint. If they are not disjoint, there is a more complicated formula called

the *inclusion-exclusion rule*.

Say Alice has 61 friends on Facebook, Bob has 39, and Charlie has 57. How many users are friends with at least one of them? We don't have enough information to answer this question since some of their friends could be common friends. So suppose we find out that Alice and Bob have 7 common friends, Alice and Charlie have 23 common friends, and Bob and Charlie have none. Can we answer now?

Let A, B and C be the sets of friends of Alice, Bob, and Charlie, respectively. We want to know the size of the set $A \cup B \cup C$.

Let's start with the size of $A \cup B$. If we add the number of elements in A to the number of elements in B, we have counted all the elements in $A \cup B$, but the elements in the intersection $A \cap B$ have been counted twice; if we subtract the size of $A \cap B$, we get the exact count

$$|A \cup B| = |A| + |B| - |A \cap B|. \tag{2}$$

So there are $61 + 39 - 7 = 93$ users who are friends with Alice or Bob.

We can now calculate the size of $A \cup B \cup C$ by applying formula (2) twice:

$$\begin{aligned} |A \cup B \cup C| &= |(A \cup B) \cup C| \\ &= |A \cup B| + |C| - |(A \cup B) \cap C| \\ &= |A \cup B| + |C| - |(A \cap C) \cup (B \cap C)|. \end{aligned}$$

To calculate $|A \cup B|$ we apply (2) directly. For the last set,

$$\begin{aligned} |(A \cap C) \cup (B \cap C)| &= |A \cap C| + |B \cap C| - |(A \cap C) \cap (B \cap C)| \\ &= |A \cap C| + |B \cap C| - |A \cap B \cap C|. \end{aligned}$$

After rearranging terms, we get the inclusion-exclusion formula for three sets:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|. \tag{3}$$

Plugging in the Facebook numbers, we get that $|A \cup B \cup C| = 61 + 39 + 57 - 7 - 23 - 0 + |A \cap B \cap C|$. The set $B \cap C$ is empty, so $A \cap B \cap C$ must also be empty. Adding all the numbers we get that 127 users are friends with at least one of Alice, Bob, and Charlie.

Avoiding patterns How many permutations of the 10 letters $\{a, b, c, d, e, f, g, h, i, j\}$ are there that *do not* contain any of the patterns hi, fad, and jig? For example, the permutations $edafjigcb$ and $jghiebfadc$ should not be counted because the first one contains jig and the second one contains both hi and fad.

Let A, B, and C be the sets of permutations that *contain* a hi, a fig, and a fad, respectively. We will first calculate the size of $A \cup B \cup C$ using the formula (3). How many elements does A have? This set contains the permutations in which hi must appear in sequence so we can think of these two letters as a single "symbol" that is permuted with the 8 other letters. This way we can view A as the set of permutations of the 9-element set $\{a, b, c, d, e, f, g, hi, j\}$ and $|A| = 9!$. Similarly we get $|B| = 8!$ and $|C| = 8!$.

The set $A \cap B$ contains those permutations that contain both hi and fad. We can view $A \cap B$ as the set of permutations of $\{b, c, e, g, j, hi, fad\}$, so $|A \cap B| = 7!$. Similarly, $|B \cap C| = 6!$. The set $A \cap C$ is empty because no permutation contains both hi and jig — the i must appear exactly once. Plugging into (3) we get

$$|A \cup B \cup C| = 9! + 8! + 8! - 7! - 6! = 437,760.$$

We want to know how many permutations *do not* contain a *hi*, a *fad*, or a *jig*. This is the complement of the set $A \cup B \cup C$, so the desired number is

$$|\overline{A \cup B \cup C}| = 10! - |A \cup B \cup C| = 3,628,800 - 437,760 = 3,191,040.$$

The general inclusion-exclusion principle for n sets follows the same pattern as formulas (2) and (3): To calculate the size of the union, we add the sizes of the individual sets, subtract the sizes of all pairs, add the sizes of all triples, and so on. The formula is more difficult to parse than the rule.

Theorem 4. *(Inclusion-exclusion formula) For any n finite sets $A_1, \ldots, A_n$,*

$$|A_1 \cup \cdots \cup A_n| = \sum_{I \subseteq \{1,\ldots,n\}} (-1)^{|I|+1} \Big| \bigcap_{i \in I} A_i \Big|.$$

The summation here ranges over all *subsets* of the indices $\{1, \ldots, n\}$. For each such subset, we have a term in the summation whose absolute value is the size of the intersection of the set with these indices (this is the set $\cap_{i \in I} A_i$) and whose sign is $+$ if I is of odd size and $-$ if I is of even size (this is the factor $(-1)^{|I|+1}$).

Derangements Each of n people turns in their hat. In how many ways can the hats be reassigned so that at least one person gets their own hat?

We represent the people by numbers from 1 to n and the assignment of hats to people by permutations of these numbers. For example, if $n = 4$, the permutation $(2, 3, 1, 4)$ represents the assignment in which 2's hat is given to 1, 3's hat is given to 2, 1's hat is given to 3, and 4 gets their own hat.

Let A_i be the set of assignments in which person i gets their own hat. These are represented by the permutations that fix i, namely entry i occurs in position i. The set $A_1 \cup \cdots \cup A_n$ represents those assignments in which at least one person gets their own hat. We are interested in the size of this set.

We apply the inclusion-exclusion formula to $A_1 \cup \cdots \cup A_n$. Let's figure out the sizes of each set A_i first. The set A_1 consists of those permutations in which a 1 occurs in the first position; the other $n-1$ numbers can occur in arbitrary order in the remaining $n-1$ positions, so $|A_1| = (n-1)!$. By the same reasoning we can conclude that $|A_i| = (n-1)!$ for every index i.

Let's now look at the pairwise $|A_i \cap A_j|$ and take $|A_1 \cap A_2|$ as a representative example. The set $A_1 \cap A_2$ contains those permutations that have a 1 in position 1 and a 2 in position 2; the other $n-2$ numbers can occur in arbitrary order in the remaining positions, so $|A_1 \cap A_2| = (n-2)!$. By the same reasoning, $|A_i \cap A_j| = (n-2)!$ for every distinct pair of indices i, j.

Continuing this line of reasoning, we get that $|\cap_{i \in I} A_i| = (n-3)!$ for every set of indices I of size 3, $(n-4)!$ for every set of indices of size 4, and so on.

We now apply the inclusion-exclusion formula. There are n terms of the type $|A_i|$, each of which has value $(n-1)!$; $\binom{n}{2}$ terms of the type $|A_i \cap A_j|$, each of which has value $(n-2)!$; and so on. Taking care of the changes in sign, we get that

$$\begin{aligned} |A_1 \cup \cdots \cup A_n| &= n \cdot (n-1)! - \binom{n}{2} \cdot (n-2)! + \binom{n}{3} \cdot (n-3)! - \ldots (+ \text{ or } -) \binom{n}{n} \cdot 0! \\ &= n! - \frac{n!}{2!} + \frac{n!}{3!} - \ldots (+ \text{ or } -)\ 1 \\ &= n! \cdot \Big(\frac{1}{1!} - \frac{1}{2!} + \frac{1}{3!} - \ldots (+ \text{ or } -) \frac{1}{n!} \Big). \end{aligned}$$

Using some calculus, it is possible to show that the number in the parenthesis equals $1 - 1/e$ plus or minus an error term that is at most $1/(n+1)!$, so

$$\frac{|A_1 \cup \cdots \cup A_n|}{n!} = 1 - \frac{1}{e} + \epsilon, \qquad \text{where } |\epsilon| \leq \frac{1}{(n+1)!}.$$

This formula tells us that if all hat reassignments were equally likely, the probability that someone gets back their own hat is very close to $1 - 1/e \approx 0.63212$.

4 Error-correcting codes*

An error-correcting code is a scheme that allows for Alice to communicate with Bob reliably in an environment where some of the data in transit may be corrupted. Suppose that Alice wants to send a k-bit message to Bob through an unreliable channel, with any one of the 2^k strings in $\{0,1\}^k$ being a possible message. Some of the bits that Alice sends over may be corrupted, but we will assume that they don't go missing and they always arrive in the correct order. How can Bob ensure that he receives Alice's intended message in spite of the corruptions?

To answer this question we need a model of how corruptions occur. In many scenarios one models the corruptions *probabilistically*; for instance, each bit may be flipped to its opposite value independently with some probability. Instead we will consider an *adversarial* communication channel in which an imaginary adversary Eve is given a budget e of errors she can introduce. After observing Alice's transmission Eve can flip up to e of the transmitted bits. So the string received by Bob differs from the one sent by Alice in up to e positions that are not known to Bob.

In order to achieve reliable communication, Alice and Bob agree to encode each possible k-bit message x by a longer n-bit *codeword* $C(x)$ and transmit this codeword through the channel. The code C can be viewed as a function from the set of k-bit message strings to the set of n-bit codewords, that is from the set $\{0,1\}^k$ to the set $\{0,1\}^n$. How should Alice and Bob choose the function C? To understand this, let's first think of some bad choices of C. If two distinct codewords $C(x)$ and $C(x')$ differ in at most e positions then Eve can always introduce ambiguity: Had Alice sent the codeword $C(x)$, Eve can always corrupt it into $C(x')$ and Bob will not know whether the intended message was x or x'. So to ensure *error detection*, it is necessary that any two codewords differ in more than e positions. This is also sufficient: If every pair of codewords differs in more than e positions then Eve cannot turn the codeword sent by Alice into any other codeword, so Bob will in principle be able to recover the original message (if his received word is in the image of C) or be able to tell that a transmission error occurred (if not).

For example, suppose $k = 2$, $n = 3$, and $C\colon \{0,1\}^2 \to \{0,1\}^3$ is the following code

$$C(\texttt{00}) = \texttt{000} \quad C(\texttt{01}) = \texttt{001} \quad C(\texttt{10}) = \texttt{101} \quad C(\texttt{11}) = \texttt{110}.$$

Since any two codewords differ in (at least) two coordinates, Bob can detect a single error (that is, error detection is possible when $e = 1$). However, although Bob can *detect* a single error, he cannot *correct* it. If he receives, for example, the corrupted word `011` he will know that an error occurred in transmission, but won't know if Alice's intended message was `00` or `01`.

How should Alice and Bob choose the code C to enable error correction? Let us again think of some bad choices of C. If two distinct codewords $C(x)$ and $C(x')$ differ in at most $2e$ positions then Eve can use the following strategy to introduce ambiguity. When Alice sends the codeword $C(x)$, Eve corrupts half of the positions in which $C(x)$ and $C(x')$ differ and leaves the other half uncorrupted. For example, if $C(x) =$ `00101001`, $C(x') =$ `11101100`, and $e = 2$, upon receiving $C(x)$ Eve can flip the first two bits and hand the corrupted word `11101001` to Bob. From Bob's

perspective, this corrupted word is consistent with both the messages x and x', so he won't know which one was intended by Alice.

On the other hand, if any pair of codewords $C(x)$ and $C(x')$ differ in at least $2e+1$ positions then in principle Bob should be able to correct from up to e errors: Upon receiving the corrupted word y, the message x is determined by the unique codeword $C(x)$ that differs from y in e or fewer positions. This can be proved formally by contradiction: If there exist two codewords $C(x)$ and $C(x')$, each of which differs from y in e or fewer positions, then $C(x)$ and $C(x')$ can only differ in those positions in which $C(x)$ differs from y or $C(x')$ differs from y, which is at most $2e$.

To summarize, a potential code allows for detecting to e errors if every pair of codewords differs in more than e positions, and for correcting up to e errors if every pair of codewords differs in more than $2d$ positions. This motivates the notion of distance.

Definition 5. A code $C\colon \{0,1\}^k \to \{0,1\}^n$ has *distance* more than d if for all $x \neq x'$, the strings $C(x)$ and $C(x')$ differ in more than d positions.

A simple way to achieve arbitrarily large distance is by repetition, e.g.

$$C(\texttt{0100}) = \underbrace{\texttt{00}\cdots\texttt{0}}_{d+1}\underbrace{\texttt{11}\cdots\texttt{1}}_{d+1}\underbrace{\texttt{00}\cdots\texttt{0}}_{d+1}\underbrace{\texttt{00}\cdots\texttt{0}}_{d+1}.$$

This type of code, called a repetition code, is reliable but not particularly efficient in terms of the amount of information transmitted: A k-bit message is encoded by a codeword of length $n = (d+1)k$, so the ratio between the length of the codeword and the length of the message grows linearly with the distance (i.e. the number of errors). Is it possible to do better?

The Gilbert-Varshamov bound Consider the following greedy strategy for designing the code C. Choose the first codeword c_1 arbitrarily in $\{0,1\}^n$. Then choose the second codeword c_2 arbitrarily, provided that it differs from c_1 in more than d positions. Then choose c_3 arbitrarily, provided that it differs from both c_1 and c_2 in more than d positions. Keep going while possible. When you get stuck, take k as large as possible and identify the first 2^k codewords $c_1, c_2, \ldots, c_{2^k}$ with $C(\texttt{00}\cdots\texttt{0}), C(\texttt{00}\cdots\texttt{1}), \cdots, C(\texttt{11}\cdots\texttt{1})$ in some arbitrary way.

When does the process we described terminate? For termination to occur after K steps, there can be no strings left in $\{0,1\}^n$ that differ from all of c_1 up to c_K in more than d positions. In other words, it must be that

$$S_1 \cup S_2 \cup \cdots \cup S_K = \{0,1\}^n$$

where S_i is the set of strings that differ from c_i in at most d positions. A union of sets can never be larger than the sum of their sizes, so

$$|S_1| + |S_2| + \cdots + |S_K| \geq |S_1 \cup S_2 \cup \cdots \cup S_K| = |\{0,1\}^n| = 2^n. \tag{4}$$

The set S_i consists of all strings in $\{0,1\}^n$ that differ from c_i in at most d positions. Each such string y is uniquely specified by the set of positions in which y and c_i differ. As this map between elements of S_i and subsets of $\{1,\ldots,n\}$ of size at most d is a bijection, the size of S_i equals the number of subsets of the set $\{1,\ldots,n\}$ of size at most d. Therefore

$$|S_i| = \tbinom{n}{0} + \tbinom{n}{1} + \cdots + \tbinom{n}{d} \qquad \text{for all } i.$$

Plugging into (4) we obtain that

$$K \cdot \left(\tbinom{n}{0} + \tbinom{n}{1} + \cdots + \tbinom{n}{d}\right) \geq 2^n.$$

Since $k = \lfloor \log K \rfloor$, it follows that

$$k \geq n - \lceil \log(\tbinom{n}{0} + \tbinom{n}{1} + \cdots + \tbinom{n}{d}) \rceil. \tag{5}$$

We just proved that

Theorem 6. *For all integers n, k, and d satisfying (5) there exists a code $C\colon \{0,1\}^k \to \{0,1\}^n$ of distance more than d.*

To get a better idea of what this means we need to understand the sum of binomial coefficients $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{d}$. When d is larger than $n/2$, the identity $\binom{n}{d} = \binom{n}{n-d}$ gives that

$$\begin{aligned}\tbinom{n}{0} + \tbinom{n}{1} + \cdots + \tbinom{n}{d} &= \tfrac{1}{2}(\tbinom{n}{0} + \cdots + \tbinom{n}{d}) + \tfrac{1}{2}(\tbinom{n}{n-d} + \cdots + \tbinom{n}{n}) \\ &\leq \tfrac{1}{2}(\tbinom{n}{0} + \tbinom{n}{1} + \cdots + \tbinom{n}{n}) \\ &= 2^{n-1}\end{aligned}$$

because the expression $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}$ counts each subset of $\{1, \ldots, n\}$ exactly once. In this case, inequality (5) does not tell us anything particularly interesting. Indeed, when $d > n/2$ more than half of the codeword symbols are corrupted and reliable communication is essentially impossible.

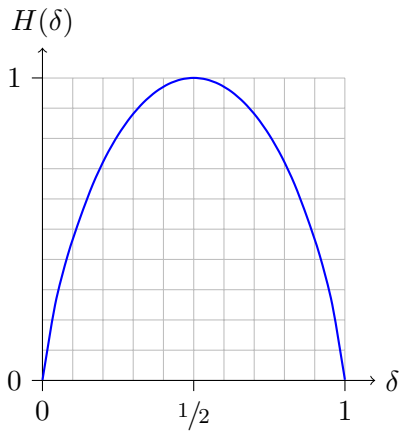
Let us now focus on the setting where $d \leq n/2$. We will look at the asymptotic behaviour of (5) when $d = \delta n$ for some constant δ between 0 and $1/2$ and n is large. The term $\binom{n}{d}$ is the largest one in the sum $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{d}$ so let us try to understand the behaviour of this term first. Using Stirling's estimate of the factorial, we can write

$$\begin{aligned}\binom{n}{\delta n} &= \frac{n!}{(\delta n)!((1-\delta)n)!} \\ &= (1+o(1)) \cdot \frac{\sqrt{2\pi n} \cdot (n/e)^n}{\sqrt{2\pi\delta n} \cdot (\delta n/e)^{\delta n} \cdot \sqrt{2\pi(1-\delta)n} \cdot ((1-\delta)n/e)^{(1-\delta)n}} \\ &= (1+o(1)) \cdot \frac{1}{\sqrt{2\pi\delta(1-\delta)n}} \cdot 2^{(-\delta\log\delta - (1-\delta)\log(1-\delta))n}.\end{aligned}$$

The function

$$H(\delta) = -\delta \log \delta - (1-\delta)\log(1-\delta)$$

for $0 < \delta < 1$ and $H(0) = H(1) = 0$ is called the *binary entropy* function. Here is a plot of it.



Plugging in the estimate for $\binom{n}{\delta n}$ we obtain the following asymptotic bound for the last term in (5) (assuming δ is between 0 and $1/2$):

$$\begin{aligned}\log\left(\tbinom{n}{0} + \tbinom{n}{1} + \cdots + \tbinom{n}{\delta n}\right) &\leq \log(\delta n)\tbinom{n}{\delta n} \\ &= \log\left((1+o(1)) \cdot \sqrt{\delta n/2\pi(1-\delta)} \cdot 2^{H(\delta)n}\right) \\ &= H(\delta)n + O(\log n).\end{aligned}$$

In fact, it is possible to eliminate the pesky $O(\log n)$ from this expression and obtain a bound that is valid for all n, not only those that are sufficiently large.

Claim 7. *For all $d \leq n/2$,*

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{d} \leq 2^{H(d/n)\cdot n}.$$

Proof. Since $d \leq n/2$, d is at most than $n-d$ and we have the inequality

$$\sum_{k=0}^{d}\binom{n}{k} \leq \sum_{k=0}^{d}\binom{n}{k}\left(\frac{n-d}{d}\right)^{d-k} = \left(\frac{n-d}{d}\right)^{d} \cdot \sum_{k=0}^{d}\binom{n}{k}\left(\frac{d}{n-d}\right)^{k}.$$

We now use the binomial identity $\sum_{k=0}^{n}\binom{n}{k}x^k = (1+x)^n$ with $x = d/(n-d)$ to obtain the inequality

$$\sum_{k=0}^{d}\binom{n}{k}\left(\frac{d}{n-d}\right)^{k} \leq \sum_{k=0}^{n}\binom{n}{k}\left(\frac{d}{n-d}\right)^{k} = \left(1+\frac{d}{n-d}\right)^{n} = \left(\frac{n}{n-d}\right)^{n}.$$

Putting the two inequalities together we obtain that for $\delta = dn$,

$$\sum_{k=0}^{d}\binom{n}{k} \leq \frac{n^n}{d^d(n-d)^{n-d}} = \frac{1}{\delta^{\delta n}\cdot(1-\delta)^{(1-\delta)n}} = 2^{H(\delta)\cdot n}.$$

□

Theorem 6 and Claim 7 give the following corollary.

Corollary 8. *If $d \leq n/2$ and $k \geq \lfloor(1-H(d/n))\cdot n\rfloor$ then there exists a code $C\colon \{0,1\}^k \to \{0,1\}^n$ of distance more than d.*

For instance, if we allow the codeword to be three times as long as the message, that is $n = 3k$ then Corollary 8 says that there exists a code of distance $d \approx 0.174n$ (as $H(0.174) \approx 2/3$). In contrast, the repetition code with these parameters has distance only 3.

References

This lecture is based on Chapter 15 of the text *Mathematics for Computer Science* by E. Lehman, T. Leighton, and A. Meyer. Section 4 is based on these lecture notes of Venkatesan Guruswami.