Module 4.4: Which Combinatorial Formula Should I Use?

Gregory V. Bard

September 4, 2018

1 How to Use This Document

In Modules 4.1, 4.2, and 4.3, we learned the seven basic principles of combinatorics. They are the multiplication principle (sometimes called the restaurant principle), the exponent principle, the permutation principle, the complement principle, the factorial principle, the combinations principle, and the handshake principle. While these tools are easy to use, the tough part is picking the right tool for the right problem. In this workbook, you have 25 problems including hints and complete solutions. By working through what follows, you will grow accustomed to these tools, and know when to use them.

Section 2 will review the two fundamental questions, and remind you of the 2×2 chart which explains the relationship of our basic principles to those two questions. Section 3 presents a quirky but very pragmatic example from reliability engineering. It can be solved by two different methods, and of course, each method gives the same answer. Section 4 has the questions themselves. Section 5 gives a hint that represents the first half of the solution. Section 7 gives the rest of the solution—so you will always want to read the hint first, otherwise the answer won't make sense. Between them, Section 6 discusses how to compute the answer for problems that lie in the rare "fourth case."

2 The Fundamental Questions and the Chart

By now, you're aware that the two fundamental questions in a combinatorics question are "does order matter?" and "are repeats allowed?" Then, using the answers from those two questions, we can choose which principle we should be using.

	Repeats Allowed	Repeats not Allowed
Order Does Matter	Exponent Princ	Permutation Princ
Order Doesn't Matter	The Fourth Case	Combinations Princ

While I have your attention, it is good to remind you of the factorial principle: "There are $n!$ possible orderings of n objects." Also, the handshake

principle is just the combinations principle, with the second number stuck at 2. Over all, the table above can be used to solve almost all combinatorial problems. While the "fourth case" is rare, we will talk about that in Section 6 of this document.

Be warned, however, that sometimes none of the shortcut principles apply. In these cases, we fall back on the multiplication principle, and slowly work out the problem. Also, in some cases, more than one principle could work. This is weird, but when it happens, both principles must produce the same answer. We'll see an example of that now.

3 A Quirky Example

Suppose that a particular quad-core game console requires 4 microprocessors. The boss has recently switched vendors, and the newer (cheaper) vendor claims 96% of processors, or more, are functional. The boss doesn't understand what this means and how bad that really is.

In any case, in the latest shipment of 60 processors, 58 were functional, but 2 were non-functional. That's $96.6\overline{6}\%$ functional, so the vendor hasn't broken their promise. Unfortunately, it is not possible to detect a faulty microprocessor prior to building the console. Moreover, a console needs all four processors to be working if it is to function at all. If the microprocessors are picked from the batch at random, what is the probability that the console will work?

Clearly, repeats are not allowed, because while I can pick processors #26, #39, #12, and #41, I cannot pick #26, #39, #26, and #41—processor #26 cannot occupy two slots on the motherboard simultaneously. What is interesting is that we have no idea if order matters, or not. For example, consider a tray that will carry the microprocessors from the vendor's shipping package to the bench, where the console will be assembled. If we have a tray with numbered positions, indicating the 1st, 2nd, 3rd, and 4th processors chosen, then order matters. Alternatively, if the tray is just blank and empty, and we put the four processors on them to be carried to assembly, then order doesn't matter.

While this might seem remarkably inconvenient, we know that the same answer must come out each way, because the question "will this console be functional or not" is unambiguous. What is ambiguous is if we take the road toward that destination of "order matters," and use the permutations principle, or the road toward that destination of "order doesn't matter," and use the combinations principle. We should get the same final answer either way.

If order does matter, the probability is

$$\frac{P_{58,4}}{P_{60,4}} = \frac{10,182,480}{11,703,240} = 0.870056\cdots$$

which can be compared to

$$\frac{C_{58,4}}{C_{60,4}} = \frac{424,270}{487,635} = 0.870056\cdots$$

when order doesn't matter.

Furthermore, using the complement principle, we can compute that the probability of a non-working console is

$$1 - 0.870056\cdots = 0.129943\cdots$$

which is far too high. Surely a company cannot survive if more than 10% of their products are defective! Even 5% is too high.

There are two "take-away" lessons here. First, having components with a 96% reliability rate is simply awful. The reliability of the components should be far above 99% to ensure a reasonably low percentage of defective products. Second, there can be multiple roads to the solution of a combinatorial problem. Do not be alarmed if you and a study partner take different routes to the answer—that's okay. What matters is that you achieve the correct answer.

By the way, if you want to refer to this problem in emails to me or your classmates, you can call it Problem 4-4-1.

4 The Questions

1. Remember, 4-4-1 was the "quirky example" that we just did in Section 3.

2. Let's imagine that you're working for a company making a new handheld-gaming gadget. There are eight possible attachments to choose from. The economy package contains the gadget with one attachment, the standard package contains the gadget with two attachments, and the deluxe package contains three attachments. For this particular device, it does not make sense to get the same attachment more than once. Moreover, the warehouse manager has decided to allocate time to pre-assembling and pre-sorting these gadget packages, to be ready for the holiday season. How many bins will be required, knowing that we need one bin for each possible package?

3. Suppose that on a 16-channel wifi network, each device will select a random channel when rebooted. Interference will occur if two devices select the same channel, by coincidence. If there are 7 devices on the network, what is the probability that interference will occur after a reboot?

4. Suppose a friend of yours works for a mutual fund. His job is to contribute to the decision-making process of which stocks to buy and sell. Yet, your friend's grandmother doesn't understand why this is a very hard task. Each of the analysts will respond with a 1st choice, 2nd choice, 3rd choice, 4th choice, and 5th choice of stock, and this fund focuses on the 500 stocks that are a member of the S&P500 index. To help grandma understand that this really is complicated, tell me how many possible preference lists could each analyst respond with?

5. When analyzing a large, multivariate data set, we can compute the correlation coefficient of any two variables. Therefore, there is one correlation coefficient computed for every possible pair of variables. If there are 40 variables in some data set, how many correlation coefficients do we obtain? In another data set, if we obtained 5671 correlation coefficients, how many variables were there?

6. At my high school, back in the early 1990s, you could choose from six languages—Hebrew, German, Chinese, Japanese, and the old standbys, Spanish, or French. My freshman class had 330 students in it. Looking at enrollment structures only, how many possible enrollments could there be? For example, it might be that 25 students choose Hebrew, 10 choose German, 35 choose Chinese, 15 choose Japanese, 194 choose Spanish, and 51 choose French. In planning for the right numbers of classrooms and seats, it doesn't matter who takes what language—instead, only the total number of students matters. How many such enrollment structures are possible? (By the way, each student takes exactly one language—it was forbidden to take multiple languages or to avoid foreign languages.)

7. Imagine that an elementary school is ordering 400 locks for student lockers. The school would like to have the combinations be without any repeated digits, as studies have shown that this makes it easier for young people to memorize. Somehow, this request was not communicated to the lock company until very late in the process. Suppose that the wheels of this lock are numbered 1–8, and that there are 3 wheels on the lock. To estimate the proportion of the 400 locks that have to be discarded or replaced (for not meeting the requirement), compute the probability that a random combination of this type has a repeated digit by coincidence.

8. Looking again at the previous problem, we can consider the weight of a binary string. The weight is the number of 1s. For example, a 56-bit secret key that is all 0s has weight zero. If it has all 0s except for one 1, then it has weight 1. If it is half-and-half, it has weight 28. If it has only three 0s, it has weight 53. In any case, how many possible weights are there for a 56-bit secret key?

9. Suppose that at a small fencing meet, every fencer will play every other fencer. If 11 fencers show up, then how many matches will be played? If at some other gathering, 136 matches are played, and we know that every fencer played every other fencer, then how many people showed up?

10. Some LCD displays use 18-bit color. How many colors are possible for such a display? Note, each bit string represents a color, and each color represents a bit string.

11. Suppose a combination lock has wheels numbered 1–8, and there are 5 wheels. How many combinations are possible for this lock? How long will

it take a thief to try all the combinations, in days, hours, minutes, and seconds, working at a rate of 1 attempt per second?

12. Imagine that at a truck repair shop, they have 200 tires, but unknown to anyone, 4 of them are flawed. An 18-wheeler comes in to have each of its tires replaced. What is the probability that the truck receives one or more damaged tires? Note: you might want to make a mental "guess" before you start, based on the idea that 98% of the tires are good, and only 2% are flawed.

13. Suppose that the video-game club has 47 members. Of course, no one can hold multiple offices. In how many ways could they select the following four officers: president, vice-president, secretary, and treasurer?

14. Suppose you have an internship working for a biomedical firm that manufactures pacemakers. In one particular model, there are 5 capacitors that govern the timing. Suppose that in one shipment of 100 capacitors, 97 are good but 3 are bad. What is the probability that, using capacitors drawn at random from this sample, that a pacemaker will have entirely good capacitors?

15. In how many ways can a fraternity of 24 members elect a president, vice-president, secretary, and treasurer? No one may hold multiple offices. After that election is over, a judicial board will be elected. The judicial board has five seats, and officers are excluded from running for the judicial board. In how many ways can the judicial board be selected?

16. A company has protected some proprietary files with the Data Encryption Standard (DES). That cipher uses a 56-bit secret key. How many possible keys are there? If a cryptanalyst's mini-supercomputer has 64 cores, and each core can try twenty million secret keys per second, how long will it take to guess and check all possible secret keys? Use a 365-day year, and respond in years, days, hours, and minutes.

17. Imagine that I'm packing for a business trip of eight days. I need to bring 8 shirts. They can be button downs, polos, or t-shirts. Of course, to blend in, if I'm going to California I should rely mostly on t-shirts, otherwise they might think me to be too conservative and stuffy. If I'm going to London or Paris, I definitely should use button downs, otherwise they might think me amateurish or very young. These two plans can be thought of as being $(0, 0, 8)$ and $(8, 0, 0)$. I'd probably want some sort of mix—for example, $(2, 3, 3)$ would represent two button downs, three polos, and three t-shirts. Climate might cause variations too. Assuming my wardrobe is sufficiently large, how many possible plans are there?

18. Suppose that six members of the state legislature are invited to speak at graduation, and that there are three democrats and three republicans among them. As it turns out, when they speak, they alternated

party. How many possible schedules would achieve that alternation? If the speakers spoke in random order, then what is the probability that the alternating of the political parties occurred by accident?

19. Let's suppose that there is a jury trial in New York City, with a 12-person jury. This jury was selected from a pool of 40 potential jurors—25 of whom are from Queens, and 15 of whom are from Brooklyn. The defendant happens to be from Brooklyn, and he is alarmed that all the jurors happen to be from Queens. In order to figure out whether or not to file a motion about this matter, the defense attorney wants to compute the probability that all the jurors would be from Queens by coincidence, if the jury had been selected randomly. After all, a majority of the pool was from Queens, and a minority of the pool was from Brooklyn. What is this probability?

20. There is a certain style of elections in situations with many candidates, called "Instant Run-off Voting." In an IRV election, each voter is presented with a list of candidates. They must rank each candidate, indicating who is their first choice, second choice, third choice, fourth choice, and so forth. For example, in an election with 12 candidates, voters might be asked to place the numbers 1, 2, 3, and 4, on the ballot, next to a list of 12 names, indicating their first, second, third, and fourth choices. How many possible ballots are there? How many ballots are possible if we extend the system to include fifth and sixth choices?

21. Suppose an airline wants to make record-locators that are sequences of six letters, but they wish to exclude `Q`, `O`, `I`, `J`, `U`, and `V`. How many possible record-locators are there? What is the probability that a random one contains an `X`?

22. How many 4-digit numbers are there? How many 4-digit numbers are palindromes? What is the probability that a four-digit number, selected at random from all possible four-digit numbers, is a palindrome?

23. In Module 4.1: "The Multiplication and Exponent Principles," we had two problems about Canadian Postal codes. It was explained that those codes have a letter, followed by number, a second letter, a second number, a third letter, and finally a third number. Note, the letters are always capital. However, it turns out that the details are a bit more complex. As of 2015, the Postal codes do not include the letters `D`, `F`, `I`, `O`, `Q` or `U`, and the first position also does not make use of the letters `W` or `Z`. With these additional facts in mind, compute how many postal codes are possible.

24. Suppose that on a relatively warm day at a fancy restaurant, only 5 customers have used the coat check. Unfortunately, the attendant has no idea who checked which coats. He hands them back randomly. What is the probability that every customer gets their actual coat back, by coincidence?

25. It is interesting to ask if knowing the weight of a cryptographic secret key helps a cryptanalyst guess the key. (The weight of a bit string was defined in Problem 8.) Suppose a cipher is using a 64-bit string as its key. Further suppose that we know the weight to be 10. In order to assess the usefulness of knowing the weight, we should compute how many 64-bit strings exist in general, and how many 64-bit strings have weight 10. Then we can see how much this new information narrows down the search.

5 The Hints

1. Remember, 4-4-1 was the "quirky example" that we talked about in Section 3.

2. We are told that it doesn't make sense for an attachment to be repeated, so we know that repeats are not allowed. Furthermore, since the attachments are just being put into packages, surely order does not matter. When order does not matter and repeats are forbidden, we know that we should use the Combinations Principle.

3. It isn't the same thing if device 1 transmits on channel 14 and device 2 transmits on channel 5 versus device 1 transmitting on channel 5 versus device 2 transmitting on channel 14. Therefore, order matters. We will compute a number once, using the exponent principle, to represent that repeats are allowed. We will compute another number using the Permutation Principle, to represent no repeats.

4. Surely a particular company cannot simultaneously be your 3rd choice and your 1st choice, so repeats are forbidden. Clearly, order matters, because saying that 3M is your 1st choice and Agilent is your 2nd choice is different from saying Agilent is your 1st choice and 3M is your 2nd choice. Since order matters and repeats are forbidden, we use the Permutation Principle.

5. We are asked for the number of pairs. This is directly the Handshake Principle, but that's the Combinations Principle with the second number glued to two. Why? Well, in a pair of variables, it does not matter in which order I write the variables. The correlation coefficient of x and y equals the correlation coefficient of y and x. Also, it doesn't make sense to pair a variable to itself, when we say "a pair of variables." For this reason, repeats are not allowed. (Actually, you can compute the correlation coefficient of x and x if you wanted to, but you'd just get 1, so nobody ever does that.) Since order doesn't matter and repeats are forbidden, we are using the Combinations Principle.

6. The order does not matter here. That's because Alice taking Spanish and Bob taking French is the same as Bob taking Spanish and Alice taking French, in the sense that both increment Spanish and French exactly once each. Clearly, repeats are allowed because we have only 6 languages, so

we could not enroll even seven students without repeating a language. Since order doesn't matter and repeats are allowed, we are using the rare "fourth case."

7. Order matters, because if you have the right digits but in the wrong order, the lock will not open. We should use both the permutation principle and the exponent principle. The permutation principle will tell us how many there are, without the repeated digits, and the exponent principle will tell us how many there are, with the repeated digits.

8. There are two possible approaches here. The first is just common sense. The lowest possible weight is 0 and the highest possible weight is 56. Each of the numbers in $\{0, 1, 2, \ldots, 54, 55, 56\}$ is possible. Therefore, there are 57 possible weights.

   However, to solve this problem with the principles of combinatorics, we should realize that what we are doing is filling a binary string with 1s and 0s. When computing the weights, order does not matter. Repeats are allowed, because we only have two symbols, 0 and 1, so we couldn't even fill a 3-bit string without making a repeat. Since order doesn't matter and repeats are allowed, we are in the rare "fourth case." Computing the answer this way will allow us to gain trust in the formula for the fourth case.

9. Clearly, if Bob plays Dave or Dave plays Bob, that's the same thing, so order doesn't matter. It isn't possible for Bob to fence himself, so repeats are not allowed. When repeats are not allowed and order doesn't matter, we are using the Combinations Principle. Alternatively, this is the Handshake Principle, since each fencing match can be thought of as a handshake.

10. This problem is really asking "How many 18-bit strings are there?" A bit string is some sequence of 0s and 1s. Clearly, repeats must be allowed, because otherwise I can't even make a 3-bit or 4-bit strings with only two symbols—0 and 1—available to choose from. Also, order definitely matters. If you have 111111000000000000 that's deep red, while 000000000000111111 is deep blue. Since order matters and repeats are allowed, we use the Exponent Principle.

11. We were not told anything about repeats, so we must assume that repeats are allowed. However, it is very clear that order matters. If my combination is `85614`, and you try `56841`, then you surely won't be able to open my lock. Since order matters and repeats are allowed, then we are using the Exponent Principle.

12. This is similar to the "quirky example," 4-4-1, which was explained in Section 3 of this document.

13. No repeats are allowed, because no one can hold multiple offices. Order matters, because electing Bob as President and Alice as Vice-President is not the same thing as electing Alice as President and Bob as Vice-President. Since order matters and repeats are forbidden, we use the Permutation Principle.

14. This is similar to the "quirky example," 4-4-1, which was explained in Section 3 of this document.

15. We are told that no one may hold multiple offices, so we know that repeats are prohibited. What is fascinating is that for the officers, order matters, while for the judicial board, order does not matter. If we elect Ned-Ed-Fred-Ted for the officer positions, we are saying that Ned is president, Ed is vice-president, Fred is secretary, and Ted is treasurer. Contrastingly, if we elect Ed-Fred-Ned-Ted, then we are saying that Ed is president, Fred is vice-president, Ned is secretary, and Ted is treasurer. These are not the same. Yet, if you list the members of the judicial board in various orders, the composition of the board doesn't change. This means that we'll use the Permutations Principle for the officers, and the Combinations Principle for the judicial board.

16. This problem is really asking "How many 56-bit strings are there?" A bit string is some sequence of 0s and 1s. Clearly, repeats must be allowed, because otherwise I can't even make a 3-bit or 4-bit strings with only two symbols—0 and 1—available to choose from. Also, order definitely matters. Since order matters and repeats are allowed, we use the Exponent Principle.

17. Since the shirts are just going into my suitcase, and coming out at the destination, it is very clear that order does not matter. (Of course, if the problem had included information on what sort of shirt I need on Monday, Tuesday, et cetera, then that would be something else entirely.) Naturally, repeats are allowed, because I have only three types of shirts available to me in this problem, so I couldn't even plan for 4 days without a repeat. Since repeats are allowed but order does not matter, this is the rare "fourth case."

18. For the first part, the speakers are coming from two different sets. While I might be wrong, I do not see a straightforward way to apply the principles of combinatorics. Instead, we should fall back on the multiplication principle. Next, we should figure out how many random schedules there are. Since there are 6 speakers, we know there are $6! = 720$ possible orderings—that's the factorial principle.

19. For a jury, order doesn't matter. A jury is a set of people, so it doesn't matter if we say Alice and Bob are on the jury, or if we say that Bob and Alice are on the jury. Moreover, the same person cannot be photocopied or cloned to enable them to take up multiple seats on the 12-seat jury. For

this reason, clearly repeats are forbidden. When repeats are forbidden and order doesn't matter, we use the Combinations Principle.

20. Surely it does not make sense for the same candidate to be both my 2nd choice and my 3rd choice at the same time, so repeats are forbidden. Order matters, because saying that Fred is your 1st choice and Ned is your 2nd choice is different from saying Ned is your 1st choice and Fred is your 2nd choice. Since order matters and repeats are forbidden, we are using the Permutation Principle.

21. Since we are not told that repeats are prohibited, we must assume that repeats are allowed. Order matters, in the sense that if my record locator is PKNRZW, then that's not the same as KRZWPN. Since order matters and repeats are permitted, we are using the Exponent Principle. It is easier to find the probability that a random record locator *does not* contain an `X`, and then use the complement principle to get the probability that it *does* contain an `X`.

22. This problem is solved fairly easily as a multiplication principle problem, but I think it is fairly hard to solve it using the principles of combinatorics directly.

23. Since the six spots are being drawn from two different sets (letters and numerals), we cannot use the principles of combinatorics. Specifically, the first, third, and fifth positions are letters, but the second, fourth, and sixth positions are numerals. Therefore, we should fall back on the multiplication principle and build our model carefully.

24. Most students would recognize this as the Factorial Principle, but it can also be solved with the Permutations Principle. When we talk about how many different ways to order n objects, that's just $n!$. If we do not remember this, then we would say that order matters (because giving Alice's coat to Charlie and Charlie's coat to Alice is different from giving Alice's coat to Alice and Charlie's coat to Charlie). You cannot give the same coat to two different people (without cutting the coat in half) so repeats are forbidden. Since repeats are not allowed and order matters, this is the Permutations Principle.

25. First, we count the number of 64-bit strings in general. In bit strings, we only have 0 and 1 to work with. Therefore, we must allow repeats, otherwise we cannot even make a 3-bit string, let alone a 64-bit string. Order definitely matters, so we use the Exponent Principle.

    Second, to know how many have weight 10, what we really want to know is how many subsets of the numbers $\{1, 2, 3, \ldots, 62, 63, 64\}$, with 10 members, can be constructed. When we have a 10-member set, drawn from $\{1, 2, 3, \ldots, 62, 63, 64\}$, we can consider those the "addresses" of the ones, and all other spots are zeros. Another approach is to ask about 54-member sets, and think of those as the "addresses" of the zeros, letting all other

entries be ones. That's because a 64-bit string with weight 10 has 54 zeros and 10 ones. In combinatorics, if we have two ways to do a problem, we really should get the same answer each way.

6 Computing the Fourth Case

The formula for the fourth case isn't hard. Some students choose to memorize it and just dispense with the derivation. When assigning n objects (or people) into k categories, where order doesn't matter, and categories can be repeated, there are

$$C_{n+k-1,k-1} = C_{n+k-1,n}$$

possible choices.

My derivation, however, is one that some students like and some students find unsatisfying. In any case, imagine a freshman class at a high school, with 1000 freshmen, and they have their choices of studying Spanish, French, German, or Japanese. The principal isn't worried, just yet, at figuring out which students are taking which languages. At this moment, the principal just wants to know about the total enrollments in each language, to help with setting the schedule. How many possible enrollment structures are there?

Imagine that we have 3 dividers, and 1000 chairs, that we will position into 1003 slots. These will allow us to figure out how many students are in each language. For example, let `h` be a chair, and let `|` be a divider. We'll seat the students in the order Spanish, French, German, and Japanese, with a divider between each language group. Consider

$$\underbrace{\text{hh}\cdots h}_{995}||\text{hhh}|\text{hh}$$

which means 995 take Spanish, 0 take French, 3 take German, and 2 take Japanese. Similarly

$$\underbrace{\text{hh}\cdots h}_{993}|\text{h}|\text{hhh}|\text{hhh}$$

means 993 take Spanish, 1 takes French, 3 take German, and 3 take Japanese. Finally

$$\underbrace{\text{hh}\cdots h}_{991}|\text{hh}||\text{hhhhhhh}$$

means 991 take Spanish, 2 take French, 0 take German, and 7 take Japanese.

As you can see, each sequence of chairs and dividers makes a enrollment structure, and each possible enrollment structure makes a sequence of chairs and dividers. With 1000 chairs and 3 dividers, we have 1003 objects.

Interestingly, if you tell me where the 3 dividers go, I automatically know where the 1000 chairs go, and there are $C_{1003,3}$ ways to place the dividers. Similarly, if you tell me where the 1000 chairs go, I automatically know where

the 3 dividers go, and there are $C_{1003,1000}$ ways to place the chairs. Therefore, we know that there are

$$C_{1003,3} = C_{1003,1000}$$

possible enrollment structures. We get the general formula by replacing 1000 with n, 3 with $k-1$ and 1003 with $n+k-1$. The general formula is

$$C_{n+k-1,k-1} = C_{n+k-1,n}$$

7 The Answers

1. Remember, 4-4-1 was the "quirky example" that we solved completely in Section 3.

2. We need to use the combinations principle to find out how many one-attachment, two-attachment, and three-attachment packages are possible. That will tells us how many bins are required. The calculation comes out to

   $$C_{8,1} + C_{8,2} + C_{8,3} = 8 + 28 + 56 = 92$$

   possible packages, and therefore 92 bins are required.

3. Using the exponent principle, we can compute that there are $16^7 = 268,435,456$ possible assignments regardless of repetition. Using the Permutations Principle, we have $P_{16,7} = 57,657,600$ possibilities excluding repetition. Thus, the probability of no interference is

   $$\frac{P_{16,7}}{16^7} = \frac{57,657,600}{268,435,456} = 0.214791\cdots$$

   which means that the probability of interference is

   $$1 - \frac{57,657,600}{268,435,456} = 0.785208\cdots$$

4. Tell grandma that there are $P_{500,5} = 30,629,362,512,000$ possible responses. That's between 30 trillion and 31 trillion responses.

5. For the first part, we know that there are 40 variables. Therefore, there are

   $$C_{40,2} = \frac{(40)(39)}{2} = 780$$

   correlation coefficients.

   For the second part, we know there are 5671 pairs. So we have to find n such that

   $$C_{n,2} = 5671$$

and that might be annoying with guess-and-check. However, if we recall the shortcut formula for the handshake principle, we obtain

$$\begin{aligned} n(n-1)/2 &= 5671 \\ n(n-1) &= 11,342 \\ n^2 - n &= 11,342 \\ n^2 - n - 11,342 &= 0 \\ n &= \left(1 \pm \sqrt{(-1)^2 - 4(1)(-11,342)}\right)/(2) \\ n &= \left(1 \pm \sqrt{45,369}\right)/2 \\ n &= (1 \pm 213)/2 \\ n &= 107 \text{ or } -106 \end{aligned}$$

Naturally, a negative number of variables does not make sense, so there must have been 107 variables in the data set. We can check our work with

$$(107)(106)/2 = 5671$$

6. We have 330 students and 6 six languages. Therefore, we can compute

$$C_{335,330} = 34,120,889,067$$

or alternatively

$$C_{335,5} = 34,120,889,067$$

enrollments are possible.

7. Using the exponent principle, we can compute that there are $8^3 = 512$ combinations possible, in general. There are $P_{8,3} = (8)(7)(6) = 336$ combinations without a repeated digit. Therefore, the probability of a random combination not repeating a digit is given by

$$\frac{P_{8,3}}{8^3} = \frac{336}{512} = 0.65625$$

Yet, this is not what was asked for! The complement principle tells us that the probability of a repeated digit occurring by accident is given by

$$1 - 0.65625 = 0.34375$$

8. We have 56 positions for bits, and we have 2 categories of bits—0s and 1s. We can compute

$$C_{57,56} = \frac{57!}{56!1!} = 57$$

or we can compute

$$C_{57,1} = \frac{57!}{1!56!} = 57$$

getting the correct answer, 57, in each case.

9. In the first part, with 11 fencers showing up, we have

$$C_{11,2} = \frac{11(10)}{2} = 55$$

matches that will take place. In the second part, we would have to find n such that $C_{n,2} = 136$, and that might be irritating with guess-and-check. However, if we remember the shortcut formula for the handshake principle, we have

$$\begin{aligned} C_{n,2} &= 136 \\ n(n-1)/2 &= 136 \\ n(n-1) &= 272 \\ n^2 - n &= 272 \\ n^2 - n - 272 &= 0 \\ n &= \left(1 \pm \sqrt{(-1)^2 - 4(1)(-272)}\right)/2 \\ n &= \left((1 \pm \sqrt{1089}\right)/2 \\ n &= (1 \pm 33)/2 \\ n &= 17 \text{ or } -16 \end{aligned}$$

Since it doesn't make sense for there to be -16 fencers, we know that the answer must be 17 fencers. We can check with $(17)(16)/2 = 136$, and be confident that we found the correct answer.

10. For 18 bits, $2^{18} = 262,144$ colors are possible.

11. We compute that there are $8^5 = 32,768$ combos for the lock. Then, 32,768 seconds is 0 days, 9 hours, 6 minutes, and 8 seconds.

12. We can use either combinations or permutations. Note that there are 4 flawed tires, but 196 good tires. Using combinations, we have $C_{196,18}$ sets of tires drawn only from the 196 good tires, compared to $C_{200,18}$ tires drawn from all 200 tires. The ratio is the probability of an 18-wheeler getting only good tires. We have

$$\frac{C_{196,18}}{C_{200,18}} = \frac{1.27258\cdots \times 10^{25}}{1.86134\cdots \times 10^{25}} = 0.683692\cdots$$

which means that the probability of having one or more flawed tires (using the complement principle) comes out to

$$1 - 0.683692\cdots = 0.316307\cdots$$

which is shockingly high—considering that 98% of the tires were good.

Using permutations, we have

$$\frac{P_{196,18}}{P_{200,18}} = \frac{8.14757 \times 10^{40}}{1.19170 \times 10^{41}} = 0.683692\cdots$$

and then computation is the same after that.

13. There are $P_{47,4} = 4,280,760$ possible ways for the election to go.

14. We can use either combinations or permutations. Note that there are 97 good capacitors and 3 bad capacitors in this shipment of 100 capacitors. Using combinations, we have $C_{97,5}$ sets of capacitors drawn only from the 97 good capacitors, compared to $C_{100,5}$ sets drawn from all 100 capacitors. The ratio is the probability of a pace-maker getting only good capacitors. We have

$$\frac{C_{97,5}}{C_{100,5}} = \frac{64,446,024}{75,287,520} = 0.855998\cdots$$

telling us that the probability is 85.59% of a pacemaker getting only good capacitors. This is surely not high enough.

15. We have 24 members and 4 officers, giving us

$$P_{24,4} = (24)(23)(22)(21) = 255,024$$

possible election outcomes. Those 4 officers cannot run for the judicial board, but the other 20 members can. We have

$$C_{20,5} = \frac{20(19)(18)(17)(16)}{5(4)(3)(2)(1)} = 15,504$$

possible election outcomes. It is rather a surprising difference.

16. We compute that $2^{56} = 7.20575\cdots \times 10^{16}$ keys are possible. That will require 5.62949×10^7 seconds which is 1 year, 286 days, 13 hours, 30 minutes. (By the way, if order didn't matter, there would be only 57 keys, a number we will compute in the next problem. That would be a truly absurd number of keys, far smaller than $7.20575\cdots \times 10^{16}$. It is for this reason that order matters in cryptographic secret keys.)

    By the way, there are cryptographic flaws in the DES that actually are hard to describe at this point, and which would cut this time in half. With those in mind, it would require 0 years, 325 days, 18 hours, 45 minutes to check *all* keys. This is the worst-case running time. Perhaps the first guess will be lucky, or perhaps all those guesses will be required, succeeding on the last one. On average, (what statisticians call "the expected value"), it would be half that, or 0 years, 162 days, 21 hours, and 22 minutes. If the cryptanalyst had more computers, it would be faster still.

    This is why no one should be using the Data Encryption Standard anymore. If you'd like to learn more about this, then consider reading *Brute Force: Cracking the Data Encryption Standard*, by Matt Curtain, published by Springer in 2005.

17. We have 8 days that require shirts, and 3 categories of shirts. Therefore, we can compute

$$C_{10,8} = \frac{10!}{8!2!} = 45$$

or we can compute

$$C_{10,2} = \frac{10!}{2!8!} = 45$$

and either way, we get that there are 45 possible plans.

18. We have three democrats and three republicans. First, let's analyze the situation if a democrat speaks first. We'd have three choices for the first speaker, three choices for the second speaker, two choices for the third speaker, two choices for the fourth speaker, one choice for the fifth speaker, and one choice for the sixth speaker. We have then

$$(3)(3)(2)(2)(1)(1) = 36$$

arrangements, plus another 36 if a republican speaks first. This brings us to 72 orderings which have the parties alternating. Since there are 720 orderings overall, the probability that the parties alternate by coincidence is

$$\frac{72}{6!} = \frac{72}{720} = \frac{1}{10}$$

which is surprisingly high.

19. We will solve this problem by computing how many juries are possible drawing all 12 jurors from Queens, and computing how many juries are possible when drawing 12 jurors from the 40 person pool. The probability will be the ratio of these numbers. We have

$$\frac{C_{25,12}}{C_{40,12}} = \frac{5,200,300}{5,586,853,480} = 0.000930810\cdots$$

and we conclude that the probability of this happening by coincidence is slightly less than 1 in 1000. I think that perhaps filing a motion is in order.

20. There are $P_{12,4} = 11,880$ possible ballots before the extension. If we extend the rules, $P_{12,6} = 665,280$ ballots are possible.

21. While the English alphabet has 26 letters, we have banned 6 of them, leaving 20 letters. So, there are $20^6 = 64,000,000$ record locators. If we exclude letter `X`, there are $19^6 = 47,045,881$ of them. The probability of *not having* an `X` is given by

$$\frac{47,045,881}{64,000,000} = 0.735091\cdots$$

so the probability of *having* an `X` is given by

$$1 - \frac{47,045,881}{64,000,000} = 0.264908\cdots$$

22. First, let's count the number of 4-digit numbers. For the first position, we can have a 1, 2, 3, ..., 9, but not a 0. Thus there are 9 choices for that position. Each of the other positions can be any numeral, so there are 10 choices for those. We conclude that there are

$$(9)(10)(10)(10) = 9000$$

possible 4-digit numbers.

Now for palindromes, we still have 9 choices for the first position. For the second position, we have 10 choices. (The reasons are the same as in the previous paragraph.) For the third position, we are forced to photocopy the numeral placed in the second position—that is our only possibility. Likewise, the fourth position must be a photocopy of the numeral placed in the first position. We have

$$(9)(10)(1)(1) = 90$$

possible 4-digit palindromes.

Thus the probability that a 4-digit number is a palindrome is given by $90/9000 = 1/100$.

23. For the third and fifth position, we exclude six letters out of the 26-letter English alphabet, leaving us with 20. We further exclude 2 of those, resulting in 18, for the first position. The second, fourth, and sixth positions are numerals, and there are 10 possibilities there. This leaves us with

$$(18)(10)(20)(10)(20)(10) = 7,200,000$$

possible postal codes.

24. Using the factorial principle, there are $5! = 120$ possible orderings of the coats. Using the permutation principle, there are $P_{5,5} = 120$ possible orderings. Only one of those orderings is the correct one. Therefore, the probability is $1/120$.

25. By now we know that there are 2^{64} possible 64-bit strings. That turns out to be

$$2^{64} = 1.84467\ldots \times 10^{19}$$

We are interested in knowing how many of those have weight 10. That will be

$$C_{64,10} = \frac{64!}{54!10!} = 1.51473\cdots \times 10^{11}$$

or equivalently

$$C_{64,54} = \frac{64!}{10!54!} = 1.51473\cdots \times 10^{11}$$

depending if you want to think of a weight 10 string of 64 bits as having 10 ones (the first computation) or as having 54 zeros (the second computation). Of course, each way gives us the same answer.

To put this in perspective, recall that in Problem 16, we had a cryptanalyst whose mini-supercomputer had 64 cores, and each core can try twenty million secret keys per second. While we were not asked about this, it might give us a frame of reference. In the situation where we know the weight to be ten, $1183.38\cdots$ seconds are required, which is 0 hours, 19 minutes, and 43 seconds. That's in stark contrast to the general case of 2^{64} secret keys, which would require 14,411,484,375 seconds, which is 456 years, 359 days, 14 hours, and 6 minutes.

As you can see, the cryptanalyst acquires a tremendous advantage when the weight is known, in this situation.