HW 5 Discreet

Bayard Walsh

November 2022

1 Password Strength

a) Let P1 consist of all 7-character passwords that can be formed with lowercase letters, uppercase letters, and digits. How large is P1, and how much will it cost to try every password in this set?

For P1, $n = 26 + 26 + 10$. $k = 7$ As password is sampling with replacement, $p1size = 62^7$ or 3521614606208 total combinations.
As a hacker can guess 523500000000 passwords per second, it would take 6.72705751 seconds to guess all combinations. At a price of 32.77 dollars per hour, this would cost the hacker 0.00910277778 dollars per second, or 0.0612349096 dollars (roughly 6 cents) to guess all the combinations.

b) Let P2 consist of all 7-character passwords that can be formed with lowercase letters, uppercase letters, digits, and special symbols from a set of 25 possibilities. How large is P2, and how much will it cost to try every password in this set?

For P2 size, $n = 26 + 26 + 10 + 25$. $k = 7$. As password is sampling with replacement, $p2size = 87^7$ or 37725479487783 total combinations.
As hacker can guess 523500000000 passwords per second, it would take 72.0639532 seconds to guess all combinations. At a price of 32.77 dollars per hour, this would cost the hacker 0.00910277778 dollars per second, or 0.65598215192 dollars (roughly 66 cents) to guess all the combinations.

c)Now suppose we change the way passwords are selected. We take a dictionary containing 7776 words2, and form a password by choosing k random words (with replacement) and concatenating them (with spaces). So, for example, with k=4, "astor melee itch envoy" is a possible password. (Note how easy it is to memorize such a password!) The attacker's job gets harder as k gets larger. What is the minimum value of k so that the attack will run in over 1000 years?

With replacement, there will be 7776^k possibilities. To get over 1000 years, you would need roughly 31,536,000,000 seconds. As a hacker can guess 523500000000

passwords per second, you would need $31,536,000,000 * 523500000000$ possibilities, or 16509096000000000000000 possibilities. Therefore, $16509096000000000000000 = 7776^k$. In this case, k would be roughly 5.7, so 6 would be the minimum integer K value.

2 Counting

a)How many strings of length 8 can we form with lower case letters that do not repeat any letters?
Approach: Apply sampling without replacement formula, where $n = 26$ and $k = 8$. 26 lowercase letters, length of string is 8, letters cannot be repeated.
Solution: (26!)/(18!).

b) How many strings of length 8 can we form with lowercase letters that may repeat letters, but never consecutively? (So, for instance, abadefgh is included because while it repeats a, the repetitions are not consecutive. On the other hand, aabdefgh is not included.)

Approach: Let the first value be any letter. Afterwards, add letters on such that each letter is not the previous letter. If letters are selected in this fashion, then the total amount of strings would be $26 * 25^7$ strings, where 26 represents the first digit and the following 25^7 represent the following 7 digits
Solution: $26 * 25^7$.

c) How many palindromes of length 8 can we form with lowercase letters? (A palindrome is a string that is the same when reversed.) How many of length 9 can we form with lowercase letters?

Approach: Every palindrome must have identical letters in reverse order. Therefore, in order to generate all palindromes on an **even** string length, generate all possible strings for half the size. Because palindrome values must be mirrored from the first half to the second half of the string, this will also be the overall amount of palindromes generated. As letters can be repeated in first half of string, use sampling with replacement. For palindromes of **odd** length, rounding up is permitted as the middle character can have any value and still be a palindrome.
Solution (length 8): 26^4
Solution (length 9): 26^5

3 Counting for Probability

a) Four people enter an elevator in the Logan Center, which has 11 floors. They all pick random floors (2 or greater, independently of the other's choices) and push the corresponding button (if someone already pressed their choice, then pushing the button has no effect.) What is the probability that the elevator stops at four consecutive floors on its way up? In your answer, describe your decision process. You do not need to simplify your answer.

Approach: Stopping at four consecutive floors will range from (start floor, stop floor) (2,5) to (8,11). $8-2+1=7$ (include starting at floor 2). This has range 7, therefore there are 7 of these possible consecutive floor sets. However, button pressing ordering does not matter. Therefore, the buttons can be pressed by any person in the elevator. Therefore, there are !4 ways to express each combination of button pressing to reach a possibility. Therefore, E =!4∗7. The sample space is all possible buttons (11-1, as floor one cannot be pressed) sampling with replacement 4 times.
Solution probability: $Pr(e) = (7*!4)/10^4$

4 Poker Hands

a) A face card is a card with rank Jack, Queen, or King. What is the probability that a 5 card hand is all face cards?

Process: take the odds of picking a single face card, and then assume that the card picked was desired. Then update the deck and chain the odds. Therefore, 12 face cards out of a 52 card deck, and as the hands progress face cards are taken out, so the number of potential face cards decreases, as well as the overall deck size is decremented by 1.
Solution: 12/52 * 11/51 * 10/50 * 9/49 *8/48

b) What is the probability that a 5 card hand contains no face cards?

Process: take the odds of picking a single card, and then assume that the card picked was desired. Then update the deck and chain the odds. Therefore, 40 non face cards out of a 52 card deck, and as the hand progresses non-face cards are taken out, so the number of potential non-face cards decreases, as well as the overall deck size is decremented by 1.
Solution: 40/52 * 39/51 * 38/50 * 37/49 *36/48

c) What is the probability that 5 card hand contains a four-of-a-kind, where the four-of-a-kind rank is a face card?

Process: There are 3 possible face card ranks (king, queen, jack). Pick one. Then, pick the number of ways to draw the four of a kind of a given suit. This will be 4 choose 4, which simplifies to 1 (treating ordering as unimportant). Then pick the possibilities for the 5th card. This will have any value not already picked. Therefore, there are 48 compliment cards to each hand of 4 of a kind. This defines the amount of possible hands, so divide this by the universe of all possible cards combinations for probability. Possible hands is 52 choose 5.
Solution: $\binom{3}{1}\binom{4}{4}\binom{48}{1}/\binom{52}{5}$ This simplifies to $(3 * 48)/\binom{52}{5}$

5 More Counting

a) If we throw 10 fair ten-sided dice, what is the probability that we miss exactly one face? (That is, every possible value from 1 to 10 is shown on some die except for one value.)

Approach: We want all possible combinations of 9 die rolls on a ten sided die where there are 9 unique combinations. This can also be considered as removing a single value from the set of $\{1 \dots 10\}$. Therefore, this value would be 10. We then want to multiply for each unique duplicate. There are 9 potential duplicates. Therefore, $9 * 10$ models all possible combinations where one face is missed. We want to model the ordering of this set, which can be achieved by !10. However, we want to divide by 2 to correct the over counting from the duplicate case. Divide this by all possible roles to find probability.
Solution: $((10 * 9) * (!10/2))/(10^{10})$

b) An urn contains 20 balls, numbered 1, . . . , 20. We draw 5 balls from the urn without replace- ment, noting their order. What is the probability that the numbers drawn are increasing? (Hint: The solution may be easier to see if you solve this directly for drawing 20 balls first, then 19, then 18.)

Approach: Consider the possible orderings of 5 balls when drawn with replacement. There would be !5 ways of expressing this value. As the numbers are unique, there is only way that they could be strictly increasing. Therefore, 1 possibility out of !5 ways of ordering
Solution: 1/!5

c) Suppose we shuffle together 8 standard decks of cards (so the resulting deck has $8 \cdot 52 = 416$ cards). How many different 8-card hands are possible? As with poker hands, order does not matter. It also does not matter which deck the cards came from.

Process: First, note that the size of the universe is not influential in this case as it is bigger than the object edge cases; in other words, we could draw 8 of the same card, so we have a theoretically infinite sized deck (in that we won't run out of ace of spades before we run out of spaces for cards in our hand). Therefore, we can model the hand is having 8 objects (potential card draws) and 52 classes (unique cards). Using the Bose-Einstein theorem for sampling from a set A of n elements with repetition and without order, we get the following formula. Solution:$\binom{52+8-1}{8}$ which simplifies to $\binom{59}{8}$

6 Contributors List

Hunter Smith, Grey Singh, Leon Zhang, Nafis Khan