

Exam #1 Study Questions -

1. Weighing - Suppose you do a two outcome experiment, like weighing, in which the outcomes are “balance” and unbalance,” and your machine can give one false reading. How many weighings do you need to distinguish among 16 coins exactly one of which is bad?
2. Sorting - Describe the following two sorting procedures in intelligible detail in your own words.(to be chosen)
3. Draw a diagram to illustrate the comparisons necessary to sort using Batcher’s algorithm with 16 keys to compare.
4. Derive an upper bound on the number of comparisons needed to find the median based on partitioning into 7.
5. Outline a proof, in your own words, of Shannon’s First Theorem.
6. Same for Shannon’s Second Theorem.
7. Here is an ordered list of frequencies of words. Create an optimal Huffman and an optimal Hu-Tucker (ordered) code for these words.
8. Is the following polynomial (with $1+1=0$) primitive?
9. Suppose you are considering remainders on dividing by primitive polynomial $p(x)$ (which will be stated explicitly). Find the polynomial $q(x)$ such that the remainder of $q(x^3)$ on dividing by $p(x)$ will be the zero remainder.
10. Write the spreadsheet instruction necessary to find the remainder of $xf(x)$ from that of $f(x)$, upon dividing by a (to be given) polynomial.
11. Write a matrix that describes a single error correcting code with 4 message bits and 3 check bits. Decode the following message with it.
12. Write the first 10 lines of the power remainder table for the following polynomial remainders.
13. What are the rules for multiplying and adding remainders.
14. If you do not know what primitive polynomial you are dividing by, when can you determine the remainder of the product of two remainders?
15. Does the following polynomial determine a two error correcting code?
16. Explain how you would decode in a two error correcting code given by polynomial $p(x)q(x)$ where the remainder of $q(x^3)$ on dividing by p is the zero remainder.
17. If you know the remainder t_1 and have a remainder table of third powers and a remainder table of first powers, how might you find its cube? Can you think of another way to find it?
18. Write the spreadsheet instruction necessary to find the remainder of $x^2 f(x)$ from that of $f(x)$, upon dividing by a (to be given) polynomial?

19. Write the spreadsheet instruction necessary to find the remainder of $x^3 f(x)$ from that of $f(x)$, upon dividing by a (to be given) polynomial.
20. Suppose we have a set S of elements, and S has cardinality N , which means that there are N elements all together. Suppose $f(x)$ for any element x of S is a randomly chosen (but fixed) element of S . Suppose we iterate f , starting with a random x , and forming successively $x, f(x), f(f(x)) \dots$ until we have a sequence of length $k+1$. What is the probability that all the elements in this sequence are distinct?
21. Suppose an experiment is repeated n times independently and an event occurs with probability p each time (independently). What is the probability that this event occurs k times? Apply Stirling's formula under the assumption that pn and $n(1-p)$ are large. What do you get?
22. Give a derivation in your own words of the Law of large numbers.
23. Give a derivation of Stirling's formula.
24. State and give a derivation of Tchebychev's inequality.
25. Find expressions for s_3 and s_2 (coefficients of given degree in a polynomial equation expressed in terms of its roots) in terms of t_1 and t_3 (sums of given powers of the roots) assuming there are 3 roots or less.
26. Suppose we use a 256 bit code BCH (one extra parity check bit) and the probability of error on each bit is 10^{-5} . How many errors must we correct so that we decode the message correctly with failure at most 1 per 10^{15} messages, (i) with each message being 256 bits? How about incorrect decoding at most one per 10^{18} messages?
27. Suppose we are considering remainders on dividing by a polynomial of degree 6 over the field consisting of 0 and 1. Then each power of x obeys the same equation as its square. Use this fact to produce a table of powers that obey the same equation. From this table deduce the number of check bits needed in a BCH code that corrects 5 errors, and one that corrects 10 errors.
28. Suppose you use a code that multiplies by the polynomial $p(x)p_{-1}(x)$ to encode, where $p_{-1}(x)$ is the polynomial you get by reversing the coefficients. That is, if $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_kx^k$, then $p_{-1}(x) = a_k + a_{k-1}x + a_{k-2}x^2 + \dots + a_0x^k$. Suppose further that you know that there are exactly two errors in the received message. Show that you can decode the received message to find the originally sent message. (In some cases it might not work if you don't know whether there are one or two errors.)