Math 1350 **The Art of Secret Writing** **Fall 2012**

Review for Exam 2

Skills to practice:

- Counting and Probability
  - Counting the number of ways something can happen, both with order mattering and without.
  - Calculating the probabilities of successive events, i.e. draw one marble from the urn, then draw another.
  - Using the probability notation.
- Estimating keyword length for the Vigenere cipher using the Friedman and Kasiski tests.
- Splitting a cipher text into the correct number of cosets for a given keyword length.
- Matching of scrawls and signatures.
- Taking the dot product of vectors.
- Converting a number from one base to another.
- Adding and subtracting in other bases (2 and 26).
- Predetermine the length of a number in binary without converting it.
- Evaluating Boolean functions.
- Compare the growth rate of functions given to you.
- Manipulating exponential and logarithmic functions.
- Classify functions using "Big-Oh" notation.
- Estimating the computational complexity of an algorithm.

Concepts to be applied:

- The four rules of probabilities:
  - The probability of the null event is zero, the probability of anything happening is one.
  - If two events are mutually exclusive then the probability of either of them happening is the sum of the probabilities of either of them happening.
  - If two events are independent of each other then the probability of them both happening is the product of the probabilities of each one happening.
  - The probability of something not happening is one minus the probability of it happening.
- Index of Coincidence as a measure of how likely it is to draw two random letters from a text and have them be the same letter. Friedman test.
- Kasiski test, looking for repeating patterns in a Vigenere enciphered text.
- Use signatures and scrawls of texts to characterize them as "English-like" or "polyalphabetically substituted."
- Calculating the keyword of a Vigenere cipher.
- Place-number systems of different bases.
- Formulae for Boolean functions.
- Growth rate of functions.
- Computational complexity and cost.

Vocabulary:

- Scrawl
- Signature
- Coset
- Independent events
- Mutually exclusive events
- Permutations and combinations
- Boolean function
- Bits
- Prime counting function, Euler ϕ function
- "Big-O" of [blank]
- Computational infeasible

Practice problems:

Task 1. *On 2d6 what is the probability of rolling a 2, 3, or a 4? Of rolling a 10, 11, or 12? Of rolling a 5, 6, 7, 8, or 9?*
$\frac{6}{36}$, $\frac{6}{36}$, $\frac{24}{36}$

Task 2. *Suppose you have an unfair coin that comes up heads with probability one third. What is the probability that out of four tosses you get exactly two heads?*
$C(4,2) \times \frac{4}{81} = \frac{24}{81}$

Task 3. *You have a box. I have placed into this box 120 marbles, 60 green, 40 yellow, 20 brown. What is the probability that draw two yellows them a green without replacing the marbles each time? Now what if I replace them each time instead?*

$\frac{40}{120} \times \frac{39}{119} \times \frac{60}{118}$, $\frac{40}{120} \times \frac{40}{120} \times \frac{60}{120}$

Task 4. *What is the likely length of the keyword for this following message?*

`NAEBZUYHWPDHHIKKEHZVNAELNAEWDEVPEOFSPNZWNAEVLRVWPRILMLVWSIEJD`

canyouhelpmewiththiscanicantseemtoopenitcansareterriblethings. keyword: lard Write out the coset corresponding to the second key letter.

By Kasiski test, 4.

Task 5. *Barr 2.8 exercise 5*

Task 6. *Let $\vec{a} = (-1, 2, 4)$, $\vec{b} = (2, 4, 6)$, and $\vec{c} = (8, 1, 1)$. Calculate $\vec{a} \cdot \vec{b}$, $\vec{b} \cdot \vec{c}$, and $\vec{a} \cdot \vec{c}$.*

$-2 + 8 + 24 = 30$, $16 + 4 + 6 = 26$, $-8 + 2 + 4 = -2$

Task 7. *The there is an attached scrawl from a coset of a Vigenere cipher. Where are the five peaks? Which one is the tallest? And what is the most likely key letter for this coset?*

The H peak, D.

Task 8. *Write the decimal number 1729 in base 2, 8, and 26. Convert the base 26 number BEEF into decimal.*

11011000001, 3301, *BON*, 20,389

Task 9. *How many binary digits would it take to write out the course number 1350 in binary? Base 8? Base 26?*

$11 \geq \log_2(1350)$, $4 \geq \log_8(1350)$, $3 \geq \log_{26}(1350)$

Task 10. *Given a Boolean function $f(x_1, x_2, x_3) = (x_1x_3 + x_2\ MOD\ 2, x_3x_2 + x_1\ MOD\ 2)$ evaluate $f(101)$ and $f(010)$.*

11, 11

Task 11. *Rank in order of the over all growth rate:*

$$2^n \qquad n^{4/3} \qquad e^n \qquad n^4 + 100n^3 \qquad \frac{1 - 4n^{10}}{n + n^5}.$$

$n^{4/3}$, $n^4 + 100n^3$, $\frac{1-4n^{10}}{n+n^5}$, 2^n, e^n

Task 12. *Write which Big-Oh the following functions belong to:*

- $(\frac{1}{2}n)^4$
- $\ln(3n + 4)$
- 2^{-n}
- $\frac{n^3 - n^n}{3n+5}$
- n^4

$\mathcal{O}(n^4)$, $\mathcal{O}(\ln(n))$, $\mathcal{O}(2^{-n})$, $\mathcal{O}(\frac{n^n}{n})$, $\mathcal{O}(n^4)$

Task 13. *Barr 3.2 exercise 8*

Task 14. *Let us try to sort a list of names in a way that a computer can. Remember that a computer will have to check each letter as a separate operation so comparing a pair of words can take several operations. Suppose you already have a list of 20 five letter names listed alphabetically. We want to add a 21st name to the list. Describe an algorithm to do this step by step and then give best case and worst case estimates of how many operations are needed. What are your estimates if you have n 5 letter names in your list? What complexity class is the algorithm you described?*

The task is alphabetizing a list of names. The algorithm is a step by step set of instructions to do this. The best case is 1 operation the worse is $100 = 20 \times 5$ operations. If n is the number of names in the list then worst case is $5n \in \mathcal{O}(n)$.

Task 15. *Pictures 2 and 3 are scrawls of a plain text and cipher text, which one is which and justify. For comparison Picture 4 is the scrawl of English.*

Picture 2 is more like Picture 4 than Picture 3 is.