Ma 450: Mathematics for Multimedia
Homework Assignment 6

Prof. Wickerhauser

Due Friday, April 27th, 2012

1. Fix an integer $N > 1$ and consider a graph with vertices labeled $1, \ldots, N$. Suppose that vertex i is connected by an edge to vertex j if and only if i and j have different parity. Compute the total number of edges.

2. Construct a prefix code for the alphabet $A = \{a, b, c, d, e\}$ with codeword lengths 1,2,3,4,5 or prove that none exists.

3. Construct a prefix code for the 24-letter Greek alphabet $A = \{\alpha, \beta, \gamma, \ldots, \omega\}$ with longest codeword 4, or prove that none exists.

4. Suppose we have two prefix codes, $\mathbf{c}_0(a, b) = (1, 0)$ and $\mathbf{c}_1(a, b) = (0, 1)$, for the alphabet $A = \{a, b\}$. Show that the following *dynamic encoding* is uniquely decipherable by finding a decoding algorithm:

   Simple Dynamic Encoding Example

   ```
   dynamicencoding0( msg[], M ):
   [0] Initialize n=0
   [1] For m=1 to M, do [2] to [3]
   [2]    Transmit msg[m] using code n
   [3]    If msg[m]==‘b’, then toggle n = 1-n
   ```

   (This encoding is called dynamic because the codeword for a letter might change as a message is encoded, in contrast with the *static encodings* studied in this chapter. It gives an example of a uniquely decipherable and instantaneous code which is nevertheless not a prefix code.)

5. Suppose that A is a finite set, s is a fixed positive integer, and $p_k : A \to [0, 1]$ is a probability function on A for each $k = 1, \ldots, s$.

   (a) Show that the function $p : A^s \to [0, 1]$ defined by

   $$p(x_1, x_2, \ldots, x_s) \stackrel{\text{def}}{=} p_1(x_1)p_2(x_2)\cdots p_s(x_s)$$

   is a probability function on A^s.

   (b) Compute the entropy $H(p)$ in terms of $H(p_1), \ldots, H(p_s)$.

6. A k-ary tree is called *extended* if every *interior*, or non-leaf, vertex has all k children. Count, with proof, the extended k-ary trees of depth 3 or less.

7. Fix a positive integer n and consider the alphabet $A = \{a_1, \ldots, a_n, a_{n+1}\}$ with occurrence probabilities $p(a_i) = 2^{-i}$ for $i = 1, \ldots, n$, and $p(a_{n+1}) = 2^{-n}$.

   (a) Construct a Huffman code for the alphabet and compare its bit rate with $H(p)$.

   (b) Construct a canonical Huffman code for this alphabet, with the property that no letter has a codeword consisting of just 1-bits. Compute its bit rate.

8. What is the probability of an undetected error in 8 data bits in a $2 \times 2 \times 2$ array with crossed parity checks if the data bits each have an independent probability p of being flipped, but the 12 top, front, and left face parity bits are known to be correct?

9. Find a binary code with two 10-bit or shorter codewords, wherein restoration to the nearest codeword corrects any three or fewer bit flips.

10. Prove that casting out seventeens will detect all one-digit errors in hexadecimal arithmetic. Find an example one-hexadecimal-digit error undetected by casting out fifteens.

11. Will the combination of checksums c_9 and c_{11} distinguish all nonequal 2-decimal-digit positive integers?

12. Find a mod-2 polynomial of degree 3 that is relatively prime to $p(t) = t^7 + t^5 + t^3 + t$. (Hint: use Euclid's algorithm for mod-2 polynomials.)

13. Suppose that b is a prime number. Write $b = \ldots b_2 b_1 b_0$ (base 2) and let $p(t) = b_0 + b_1 t + b_2 t^2 + \cdots$ be the associated mod-2 polynomial. Prove or find a counterexample to the claim that p must be irreducible.

14. Suppose that $s > 0$ and $a > 1$ are integers with $\gcd(a, s) = 1$. Prove that there is some integer $N > 0$ such that $a^N - 1$ is divisible by s, but s does not divide $a^k - 1$ for any positive integer $k < N$. (This is Theorem 6.19 for integers rather than mod-2 polynomials.)

15. Find integers j, k, $0 < k < j < 32$, such that $s(t) = t^{32} + t^j + t^k + 1$ is an irreducible mod-2 polynomial, or prove that none exists. (Hint: try dividing one such $s(t)$ by $t + 1$.)