15-354: Computational Discrete Math — K. Sutner

Assignment 8 — Due: November 9, 2006

Problem 1: Kraft's Inequality (50 pts.)

Background

Kraft's inequality is a combinatorial lemma that is often used in the theory of prefix codes; it is also crucial for the construction of Chaitin's Ω.

Kraft's Lemma:
Let $S \subseteq \mathbf{2}^\star$ be a prefix set of binary words. Then

$$\sum_{x \in S} 2^{-|x|} \leq 1$$

On the other hand, given natural numbers ℓ_n such that

$$\sum_{n \geq 1} 2^{-\ell_n} \leq 1$$

there exists a prefix set $S = \{ s_n \mid n \} \subseteq \mathbf{2}^\star$ such that $\ell_n = |s_n|$. S is said to realize (ℓ_n). For example, $\ell_n = n$ produces $\sum 2^{-\ell_n} = 1$ and can be realized by $s_n = 0^{n-1}1$.

Task

A. Prove the first part for any finite set S.

B. Prove the second part for any finite set S.

C. Conclude that the lemma holds for arbitrary sets.

Comment

Try to be as algorithmic in the second part as possible. For the sake of TA sanity, let's all assume that (ℓ_n) is an ordered sequence.

What exactly is needed to make the transition to the infinite case?

Problem 2: Characteristic 2 (50 pts.)

Background

As we have seen in class, there is a unique finite field of size p^k for any prime p and $k \geq 1$. When $p = 2$ it is particularly easy to give efficient implementations of the arithmetic in these fields.

Task

A. Explain how to implement the finite field $\mathbb{F}_{2^5}$.

B. How difficult is it to implement addition and multiplication in your system? How about division?

C. How many primitive elements are there in $\mathbb{F}_{2^5}$?

D. What are all the subfields of $\mathbb{F}_{2^5}$? Why?

E. How does all of this carry over to $\mathbb{F}_{2^k}$? What is the main difficulty in implementing the field of size 2^{1000}?