CS642
(Circuit Complexity Theory)
Mid Semester Examination
Maximum Marks : 60

Starting date: 25 Feb 2013
Submission Date: 4 March 2013

NOTE: In the classes below, uniformity conditions are not specified. You may assume whatever suits the context.

A *MAJORITY* gate is an unbounded fan-in gate such that on input $x_1, x_2, \ldots, x_n$ to the gate, the gate outputs a 1 if and only if at least half of the input lines are 1, i.e., $\sum_{i=1,n} x_i \geq n/2$.

Define the class TC^0 to be the class of sets accepted by a family of polynomial-size, constant depth circuits with *all* the gates in the circuit being either MAJORITY gates or NOT gates.

For number $k > 1$, a MOD_k gate is an unbounded fan-in gate such that on input $x_1, \ldots, x_n$ to the gate, it outputs a 1 iff $\sum_{i=1}^{n} x_i \neq 0(\mathrm{mod} k)$.

Define the class $\mathrm{AC}^0[k]$ to be the class of sets accepted by a family of polynomial-sized, constant depth circuits with AND and MOD_k gates. Define $\mathrm{ACC} = \bigcup_{k>1} \mathrm{AC}^0[k]$.

The classes ACC and TC^0 are important classes because a number of basic operations belong to these. Let us first place these classes in the hierarchy of classes that we have seen.

- Show that $\mathrm{AC}^0 \subseteq \mathrm{ACC} \subseteq \mathrm{TC}^0 \subseteq \mathrm{NC}^1$. (5 marks)

Remember that we showed in the class that iterated addition and iterated multiplication (i.e., adding and multiplying n n-bit numbers) is in NC^1.

- Show that both these operations are in fact in TC^0. (15 marks)

There are a number of variations of MAJORITY gates. One such is *EXACT THRESHOLD* gates. These gates also have n inputs $x_1, \ldots, x_n$. Moreover, there are $n+1$ weights—$w_1, w_2, \ldots, w_n$, and w—associated with the gate with each weight being between 0 and 2^n. The EXACT THRESHOLD gate outputs a 1 if and only if $\sum_{i=1,n} w_i * x_i = w$.

- Show that any EXACT THRESHOLD gate can be simulated by a TC^0 circuit. Conversely, show that any MAJORITY gate can be simulated by a polynomial-size constant depth circuit containing EXACT THRESHOLD and NOT gates. Thus, the class defined by polynomial-size constant depth family of circuits with EXACT THRESHOLD and NOT gates is nothing but TC^0. (10 marks)

Another variation is that of *THRESHOLD* gates. Such a gate outputs a 1 if and only if $\sum_{i=1,n} w_i * x_i \geq w$. So MAJORITY gates are special kind of THRESHOLD gates where each w_i equals 1 and w equals $n/2$.

- Show that any THRESHOLD gate can also be simulated by a TC^0 circuit. (5 marks)

We do not know any lower bounds on even ACC (although we can prove that MAJORITY cannot be done by $\mathrm{AC}^0[k]$ circuits when k is a prime power). Clearly, there are no known lower bounds on TC^0 either. In fact, many people believe that $\mathrm{NC}^1 = \mathrm{TC}^0$. Lower bounds are known for depth-two TC^0 circuits—It has been shown that there is a set accepted by a family of depth-three TC^0 circuits that cannot be accepted by any family of depth-two TC^0 circuits. It is a rather involved proof. Here we look at a much simpler result.

- Show that the parity of n bits cannot be computed by any family of *depth-one* TC^0 circuits. A depth-one TC^0 circuit has just a single Majority gate. In fact, this holds even if we allow this gate to be a Threshold gate. Prove the result for this more general case. (10 marks)

The class ACC too has many nice properties. Here we look at one of them. Define $\mathrm{AC}^0[F]$ to be the class of sets accepted by families of constant depth circuits whose gates are *addition and multiplication* gates over the finite field F. The lines of these circuits carry elements of F instead of 1 and 0. However, the input and output lines still carry 1 or 0 (now treated as elements of F).

- Prove that $\mathrm{ACC} = \bigcup_F \mathrm{AC}^0[F]$. (15 marks)

You will need to make use of Dirichlet's theorem in the above proof. This theorem states that for any two relatively prime numbers a and b, the sequence of numbers $\{a + kb\}_{k>0}$ contains infinitely many prime numbers.