September 2010

MADALGO seminar by Elad Verbin, Aarhus University

The Coin Problem, and Pseudorandomness for Branching Programs

Abstract:

The "Coin Problem" is the following problem: a coin is given, which lands on head with probability either $\frac{1}{2}+\beta$ or $\frac{1}{2}-\beta$. We are given the outcome of *n* independent tosses of this coin, and the goal is to guess which way the coin is biased, and to be correct with probability $\geq \frac{2}{3}$. When our computational model is unrestricted, the majority function is optimal, and succeeds when $\beta \geq c/\sqrt{n}$ for a large enough constant *c*. The coin problem is open and interesting in models that cannot compute the majority function.

In this talk I will present results on the coin problem in the model of read-once width-*w* branching programs. We prove that in order to succeed in this model, β must be at least $1/_{(\log n)^{\theta(W)}}$.

For constant *w* this is tight by considering the recursive tribes function. I will also discuss various generalizations and variants of this.

Finally, I will suggest one application for this kind of theorems:
I'll show that the INW generator ε-fools width-*w* read-once *permutation* branching programs, using seed length $O(\log n * \log\log n)$ when ε and *w* are both constant. I'll also show why we get this only for permutation branching programs, and what stops us from getting this for the non-permutation case.

We are looking for applications of the coin problem in other domains (e.g. streaming lower bounds).

Joint work with Joshua Brody