Picking and certifying random primes

Cagdas Calik, René Peralta, Meltem Turan[1]

Information Technology Laboratory, NIST

Abstract. Cool multcomp stuff.

1 A lemma

Denote by f_n any function on variables $x_1, \ldots, x_n$. Let $C_\wedge(f)$ denote the multiplicative complexity of f.

Claim 1 : Let $n >= 1$. Let f_n be a non-constant function. For all f_{n-1} the following holds

$$C_\wedge(x_{n+1}f_n + f_{n-1}) = 1 + C_\wedge(f_n + f_{n-1}).$$

Proof:

Clearly

$$C_\wedge(x_{n+1}f_n + f_{n-1}) <= 1 + C_\wedge(f_n + f_{n-1}),$$

so it is enough to prove

$$C_\wedge(x_{n+1}f_n + f_{n-1}) > C_\wedge(f_n + f_{n-1}).$$

Suppose, for a contradiction, that there exists a circuit D, with at most $C_\wedge(f_n + f_{n-1})$ AND gates, that computes $f_{n+1} = x_{n+1}f_n + f_{n-1}$.

Assume, w.l.o.g. that D is in layered normal form.

Case 1, x_{n+1} is an input to an AND gate in D. Setting $x_{n+1} = 1$, kills at least one AND gate in D. The resulting circuit must compute f_n, but it has fewer than $C_\wedge(f_n + f_{n-1})$ AND gates, contradiction.

Case 2, a linear function $x_{n+1} + L_n$ is an input to an AND gate (L_n not a constant). Then setting $x_{n+1} = L_n$ kills a least one AND gate in D. The resulting circuit must compute $f_n + f_{n-1}$ because, in the space of functions on variables $x_1, \ldots, x_n$, setting $x_{n+1} = L_n$ is not a restriction. But this circuit has fewer than $C_\wedge(f_n + f_{n-1})$ AND gates, contradiction.