CIRCUIT COMPLEXITY SCRIBE NOTES, 10/16/13

BENJAMIN GREENBERG

First we give some lower bounds on the size of circuits over B_2. In particular, we consider circuits that compute a function $f(x_1, \ldots, x_n)$ that depends on all its inputs. Trivially, $C_{B_2}(f) \geq n-1$ since $n-1$ gates are required just to incorporate all the inputs into a single circuit.

- (Schnorr, 1974) Lower bound of $2n-3$.
- (Paul, 1977) Lower bound of $2n - o(n)$ for the storage access function.
- (Stockmeyer, 1977) Lower bound of $2.5n - O(1)$.
- (N. Blum, 1984) Lower bound of $3n - o(n)$.
- (Kojevnikov) Lower bound of $7n/3$.

Some slightly larger lower bounds have been found if we modify our basis to $U_2 = B_2 \backslash \{\oplus, \equiv\}$.

- (Schnorr, 1974) Lower bound of $3n - O(1)$ on $\oplus$.
- (Zwick, 1991) Lower bound of $4n - O(1)$ on counting.
- (Iwana, Lachish, Morizaki, Razborov, 2001) Lower bound of $4.5n - o(n)$.
- (Iwana, Morizaki, 2002) Lower bound of $5n - o(n)$.

If we further limit our basis to $\{\wedge, \neg\}$ or $\{\vee, \neg\}$, we get a still better (though still linear) lower bound of $7n-7$ (Redkin, 1973).

We will give the proof of Schnorr's lower bound, but first we require a definition.

Definition. *$Q_{2,3}^n$ is the set of functions $f : \{0,1\}^n \to \{0,1\}$ with the following properties:*

(1) *f depends on all its inputs.*

(2) *If $n \geq 3$, then for any two distinct x_i, x_j inputs, there are at least 3 subfunctions of f that can be obtained by setting x_i, x_j equal to constants.*

(3) *For all inputs x_i, there is a constant setting c such that letting $x_i = c$ yields a function in $Q_{2,3}^{n-1}$.*

Exercise: Is $Q_{2,3}^n$ equivalently defined if we remove condition 3?

As a simple example of such a function, consider the n-ary function that checks whether the sum of its inputs is 0 modulo 3. It is readily seen that this function satisfies all three requirements of the definition.

Theorem (Schnorr, 1974). *Let* $f \in Q^n_{2,3}$. *Then* $C_{B_2} \geq 2n - 3$.

Proof. We proceed by induction on n. The base cases $n = 0$ and $n = 1$ are easy to check, since then $2n - 3 < 0$. If $n = 2$, $2n - 3 = 1$, and since f depends on all its inputs $C_{B_2}(f) \geq n - 1 = 1$, so this case is taken care of as well.

Now consider $n > 2$. Let C be a minimum size B_2-circuit for f. There is a gate g in C that takes as its inputs x_i and x_j. By minimality of C, $i \neq j$. Because g has only two possible outputs, at least one of x_i and x_j appears elsewhere in C as an input, as otherwise we would violate the requirement that setting these variables to constants yields at least 3 subfunctions of f.

Without loss of generality suppose x_i appears in some other gate g', and set $x_i = c$ such that the resulting function is in $Q^{n-1}_{2,3}$, which we can do by definition. This function can be computed by the circuit arrived at by removing at least g and g' from C, and by our inductive hypothesis any such circuit is of size at least $2(n-1)-3$. Hence, $Size(C) - 2 \geq 2(n-1) - 3$, establishing the claim. ☐

We now consider monotone functions.

Definition. *Let f be an n-ary Boolean function. f is monotone provided: If $a_i, b_i \in \{0,1\}$ and $a_i \geq b_i$, then $f(a_1, \ldots, a_n) \geq f(b_1, \ldots, b_n)$. A circuit is monotone if all its gates compute monotone functions.*

The only examples of monotone functions in B_2 are the two identity functions, constants, $\wedge$, and $\vee$.

Theorem. *Let C be a monotone circuit. Then C computes a monotone function.*

Proof. Induction on the number of gates in C. ☐

Conversely, if f is an n-ary monotone function, then it is computed by a monotone formula of size $\leq n2^n$.

Proof. Write f in DNF, and erase the negated variables from disjunctions, as well as duplicate conjunctions. This process is allowed since f is monotone, and the resulting formula has the appropriate size. ☐

We now consider lower bounds for monotone circuits.

Definition. *We define the clique function* $Clique_{n,k}(x_1, \dots, x_{\binom{n}{2}})$ *to be 1 if the graph defined by the edges* x_i *contains a* k*-clique and 0 otherwise. This function is clearly monotone since adding edges to a graph never destroys a clique.*

Theorem (Razborov, 1985). *For* $3 \leq k \leq n^{1/4}$*, any monotone circuit for* $Clique_{n,k}$ *has size* $\geq n^{\Omega(\sqrt{k})}$*.*

Definition. *A slice function is an* n*-ary Boolean function such that there exists* $k \leq n$ *such that* $f(x_1, \dots, x_n) = 0$ *if* $\sum_i x_i \leq k$ *and is* 1 *otherwise.*

To prove the final theorem of this section, we need the following theorem which will be proved later.

Theorem. *There are polynomial size monotone formulas for* $Th_k^n(x_1, \dots, x_n)$*.*

Theorem. *If* f *is a slice function and has* B_2 *circuit of size* m*, then it has a monotone circuit of size* $mn^{O(1)}$*.*

Proof. Let C be a B_2 circuit for f. Without loss of generality it is a $\{\wedge, \vee, \neg\}$-circuit with negations only on variables. This increases the size of the circuit by only a constant factor.

Now replace C with $Th_{k+1}^n(x_1, \dots, x_n) \vee (Th_k^n \wedge C^*)$, where C^* is C with each $\neg x_i$ replaced with $Th_k^n(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$. This computes the same function as C and is monotone, so we have found a circuit computing f that is linear in m and polynomial in n. □