Homework 33

Joe Baker, Brett Schreiber, Brian Knotten

April 10, 2018

61

Show that $NP = L - PCP(log(n))$.

First we must show that $L - PCP(log(n)) \subseteq NP$. Let $l \in L - PCP(log(n))$, then l can be decided by a probabilistically checked logspace machine M using $r(n)$ random bits and one pass over the proof π. M only has 1-way access to the proof π, but an NP problem can be solved with turing machines with 2-way access to a certificate. From M we can construct a Turing machine M' which can accept in polynomial time using π as the certificate and following the execution of M.

Next we show that $NP \subseteq L - PCP(log(n))$. We will show that $3SAT$ can be verified by an $L - PCP(log(n)$ verifier. The proof string π that is verified is the assignment to m variables $x_0x_1x_2...x_m$ repeated n times where n is the number of clauses. The logspace verifier is defined as follows:

```
On input $(\pi, \phi)$ where $\pi$ is the proof string and $\phi$ is the instance of the clauses:
    Keep counter variables $i, j$ for $\pi$ and $\phi$.
    Set $\pi = 0$ and $\phi = 0$.
    While $i < m$ and $j < n$:
        If $x_i$ satisfies the clause $\phi_j$, increment both $i$ and $j$.
        Else, only increment $j$.
    If $i$ reaches the end of the proof string before all clauses are satisfied, reject.
    Otherwise, if all clauses are satisfied, accept.
```

This verifier only makes one pass over the proof string. But each clause has a full set of assignments to work with, so every variable can be passed over for every clause. So the verifier can check the satisfiability of every clause by checking every input to each clause. One last thing to consider is that the counters use logspace. The highest number an index can be is the highest number of variables possible (since there are always more variables than clauses in $3SAT$). In the worst case, each clause has 3 unique variables. So there can be up to $3n$ variables. So the proof string can be of size $3n$ variables $*n$ clauses $= 3n^2$ bits in the proof string. Keeping track of a number takes a log number of bits according to Shannon, so the verifier needs $log(3n^2) = 2log(n) + 2log(3)$, which is $O(logn)$. So the verifier can verify an instance of 3SAT with one pass on the proof string and with a log number of bits.