Sparse Sets II: Showing $SAT \le_m S \rightarrow P = NP$ Using Chains
Exposition by William Gasarch

1 Introduction

We give another proof that if $SAT \le_m S$ then $P = NP$. Recall the definition of $LSAT$.

Def 1.1 LSAT (called *Left Sat*) is the set of ordered pairs (ϕ, z) such that

1. ϕ is a Boolean formula. Let n be the number of variables.
2. $z \in \{0,1\}^n$ is viewed as an assignment.
3. There exists $x \preceq z$ such that $\phi(x)$.

$LSAT$ has a very nice property which we define more generally.

Def 1.2 A set A is 1-word self reducible if there is a function $g : A \rightarrow A \cup \{Y, N\}$ such that the following hold:

1. If $g(x) = Y$ then $x \in A$.
2. If $g(x) = N$ then $x \notin A$.
3. If $g(x) \notin \{Y, N\}$ then (1) $g(x) < x$ in the lexicographic order, and (2) $x \in A$ iff $g(x) \in A$.

Exercise 1: Show that $LSAT$ is 1-word self-reducible.

Def 1.3 If $z \in \{0,1\}^n - 0^n$ then z^- is the element of $\{0,1\}^n$ that is JUST below z in the lex ordering.

2 Intuitions and Chains

Assume for this section that we have the following:

1. S is a sparse set. $s(n)$ is the polynomial such that $|S \cap \{0,1\}^n| \le s(n)$.
2. g is the function from Exercise 1 for $LSAT$.

Given ϕ, we want to determine if $\phi \in SAT$. Assume ϕ has n variables. We think of this as trying to determine if $(\phi, 1^n) \in LSAT$.

Bad Idea I: Let g be the function from Exercise 1.

Try to build a chain from $(\phi, 1^n)$ down to $(\phi, 0^n)$.

$(\phi, 1^n) \in LSAT$ iff $g(\phi, 1^n) \in LSAT$ iff $g(g(\phi, 1^n)) \in LSAT$ etc.

The good news is that everytime we apply g we get a z-value that is (one) lower in the lex ordering, since $g(\phi, z)$ is of the form (ϕ, z^-). More good news- each step is easy to compute.

The bad news- it will take 2^n steps before we get to $(\phi, 0^n)$.

The bad news sociologically- I didn't use the reduction to a sparse set.

Bad Idea II: Again let $f(\phi, 1^n) = w$. Try to find a z such that $f(\phi, z) = w$. If so then we have

$$(\phi, 1^n) \in LSAT \text{ iff } (\phi, z) \in LSAT.$$

This may be getting us closer to $(\phi, 0^n)$. However, if we keep doing this we could, as in Bad Idea I, be taking steps towards $(\phi, 0^n)$ that are too small to get there in polynomial time. Also, how do we find such a z?

Note that we do have two different ways to have membership-in-$LSAT$ be equivalent:

$$(\phi, z) \in LSAT \text{ iff } g(\phi, z) \in LSAT.$$

and also

If $f(\phi, z) = f(\phi, z')$ then

$$(\phi, z) \in LSAT \text{ iff } (\phi, z') \in LSAT.$$

We will use both of these to march towards 0^n. However realize- we might not get there!! We will set things up so that we either make progress or find out directly if $(\phi, 1^n) \in LSAT$.

Def 2.1 A *chain of length m* is a sequence of the form

- $((\phi, z_1), w_1))$
- $((\phi, z_2), w_2))$
- $\vdots$
- $((\phi, z_m,), w_m))$

such that the following hold.

1. $z_1 > z_2 > \cdots > z_m$ in lex order.
2. For all j, k
$$(\phi, z_j) \in LSAT \text{ iff } (\phi, z_k) \in LSAT.$$
(Hence either all of the pairs are in $LSAT$ or all are not in.
3. For all j, $f(\phi, z_j) = w_j$. (Hence, given the last point, either all of the w's are in S or all are not in S.)
4. All of the w_i are DIFFERENT.

Good Idea: We will try to build a chain. One of two things must happen.

1. The chain will go all the way down to $(\phi, 0^n)$.
2. The chain goes long enough that not all of the (different!) values of w's can be in S. Hence at least one is not in S. By the defintion of chain, none of them are in S, and we know that $(\phi, 1^n) \notin LSAT$.

3 The Key Lemma

Lemma 3.1 *Assume there is a sparse set S such that $LSAT \leq_{\mathrm{m}}^{\mathrm{p}} S$. Then there is a polynomial time algorithm that does the following. The input is a chain of length m whose last element $z_m \neq 0^n$. The output is either*

1. $((\phi, z_{m+1}, w_{m+1})$ *that extends the chain, or*

2. *The membership status in LSAT of every* (ϕ, z) *on the chain. This includes* $(\phi, 1^n)$ *so we are DONE.*

Proof:

Here is the algorithm

1. Input is
   - $((\phi, z_1), w_1))$
   - $((\phi, z_2), w_2))$
   - $\vdots$
   - $((\phi, z_m), w_m))$
2. Compute $(\phi, y) = g(\phi, z_m)$. Compute $w = f(\phi, z)$. If $w \notin \{w_1, \ldots, w_m\}$ then
   (a) $z_{m+1} = z_m{}^-$
   (b) $w_{m+1} = w$.
   (c) Note that $z_{m+1} = z_m^- < z_m$. Note that $(\phi, z_{m+1}) \in LSAT$ iff $(\phi, z_m) \in LSAT$.
3. (If you got here then $f(g(\phi, z_m)) \in \{w_1, \ldots, w_m\}$.) Compute $f(\phi, 0^n)$. If it is in $\{w_1, \ldots, w_m\}$ then AH-HA! We know that $(\phi, 1^n) \in$ LSAT iff $(\phi, 0^n) \in LSAT$. We can determine $(\phi, 0^n) \in LSAT$ in polynomial time. We do so, output the answer, and EXIT.
4. Let $z_{\text{begin}} = z_m$ and $z_{\text{end}} = 0^n$. KEY PROPERTY: $f(\phi, z_{\text{begin}}) \in \{w_1, \ldots, w_m\}$ but $f(\phi, z_{\text{end}}) \notin \{w_1, \ldots, w_m\}$.
5. Let z_{mid} be the value halfway between z_{begin} and z_{end} lexicographically.
6. Compute $\{f(\phi, z_{\text{mid}})$ If $f(\phi, z_{\text{mid}}) \in \{w_1, \ldots, w_m\}$ then $z_{\text{begin}} = z_{\text{mid}}$ else $z_{\text{end}} = z_{\text{mid}}$. NOTE- (verify for yourself). KEY PROPERTY STILL HOLDS.
7. If $z_{\text{end}} = z_{\text{begin}}^-$ then compute $g(\phi, z_{\text{begin}})$. If its Y then we are DONE- $(\phi, 1^n) \in LSAT$. If not then its $(\phi, (z_{\text{begin}})^-) = (\phi, z_{\text{end}})$. So we have $(\phi, z_{\text{begin}}) \in LSAT$ iff $(\phi, z_{\text{end}}) \in LSAT$. And we also have $f(\phi, z_{\text{end}}) \neq \{w_1, \ldots, w_m\}$. So we can extend the chain by $(\phi, z_{\text{end}}, f(\phi, z_{\text{end}}))$.

■

4 The Main Theorem

Theorem 4.1 *If there exists a sparse set S such that $SAT \leq_{\mathrm{m}}^{\mathrm{p}} S$ then $SAT \in P$.*

Proof: If $SAT \leq_{\mathrm{m}}^{\mathrm{p}} S$ then

$$LSAT \leq_{\mathrm{m}}^{\mathrm{p}} S.$$

Let f be the reduction and let p be the polynomial that bounds its running time. Let S be $s(n)$-sparse. That is, $|S \cap \{0,1\}^n| \leq s(n)$.

Here is the algorithm.

1. Input ϕ. n be the number of variables in ϕ. Note that $|f(\phi, y)| \leq p(n)$.
2. Let $z_1 = 1^n$, and $w_1 = f(\phi, z_1)$. View $((\phi, z_1), w_1)$ as the first element of a chain.
3. Apply the algorithm from Lemma 3.1 over and over again to the chain until one of the following occurs.
   (a) The algorithm returns the actual answer to $(\phi, z_1) \in LSAT$. Output that answer and EXIT.
   (b) The algorithm returns with $(\phi, 0^n)$. The question $(\phi, 0^n) \in LSAT$ can easily be answered. Do so and output the answer.
   (c) The chain has $s(p(n)) + 1$ elements in it. Since S is sparse and the reduction is time $p(n)$, these numbers cannot all be in S. Hence there exists some $w_i \notin S$. By the defintion of a chain, none of them are in $LSAT$. Output NO and EXIT.

■