

**How Helpful are Sparse Sets?- II**  
**Exposition by William Gasarch**  
 $SAT_{17} \leq_m^p S, S \text{ Sparse} \Rightarrow SAT_{17} \in P$

## 1 Introduction

Let

$$SAT_{17} = \{\phi \mid \#(\phi) \equiv 0 \pmod{17}\}.$$

How hard is this set? By a variant of the result of Valiant-Vazarani we know that if  $SAT_{17} \in P$  then  $NP = R$ .

We ask a different question. Informally, how much information is in this set. One way to pin this down is to ask if it is reducible to a sparse set.

Lozano and Ogihara [1, 2] showed the following:

If there is a sparse set  $S$  such that  $SAT_{17} \leq_m^p S$  then  $SAT_{17} \in P$ .

We give an exposition of this results.

(They actually proved quite a bit more: they showed that if  $SAT_{17} \leq_{btt} S$  then  $SAT_{17} \in P$ .)

## 2 Defintions and Easy Lemma

**Def 2.1**

1.  $SAT_{17} = \{\phi \mid \#(\phi) \equiv 0 \pmod{17}\}$ .
2.  $LMOD_{17}$  is the set of all triples  $(\phi, y, i) \in FML \times \{0, 1\}^* \times \{0, \dots, 16\}$  such that
  - (a)  $\phi$  is a formula on  $v$  variables.
  - (b)  $y \in \{0, 1\}^v$ .
  - (c)  $|\{\vec{b} : \vec{b} \leq y \wedge \phi(b) = T\}| \equiv i \pmod{17}$ .
3. We define the ordering  $\prec$  on  $FML \times \{0, 1\}^* \times \{0, \dots, 16\}$  as follows:
  - (a) If  $y_1 < y_2$  (lex) then, for any  $\phi, i, j$ ,  $(\phi, y_1, i) \prec (\phi, y_2, j)$ .
  - (b) If  $y_1 = y_2$  (lex) and  $i < j$  then  $(\phi, y_1, i) \prec (\phi, y_2, j)$ .

- (c) If  $\phi_1 \neq \phi_2$  then, for all  $y_1, y_2, i_1, i_2$ ,  $(\phi_1, y_1, i_1)$  is not comparable to  $(\phi_2, y_2, i_2)$ .

**Def 2.2** Let  $v \in \mathbb{N}$ . If  $y \in \{0, 1\}^v$  then  $y^-$  is the string just below  $y$  in the lexicographic order.

**Lemma 2.3** *There is a polynomial time computable function  $g$  such that, for all  $\phi, y, i$*

1.  $(\phi, y, i) \in \text{LMOD}_{17}$  iff  $g(\phi, y, i) \in \text{LMOD}_{17}$ .
2.  $g(\phi, y, i) \prec (\phi, y, i)$

**Proof:**

ALGORITHM FOR  $g$

1. Input  $(\phi, y, i)$
2. Evaluate  $\phi(y)$ .
3. If  $\phi(y) = \text{TRUE}$  then output  $(\phi, y^-, i - 1 \pmod{17})$ .
4. If  $\phi(y) = \text{FALSE}$  then output  $(\phi, y^-, i \pmod{17})$ .

■

The following easy lemmas we leave to the reader

**Lemma 2.4**  $\text{LMOD}_{17} \leq_m^p \text{SAT}_{17}$ .

**Lemma 2.5** *Let EASYCASE be the set of all  $(\phi, 0^v, i)$  such that*

- $\phi$  has  $v$  variables.
- The number of  $b \in \{0, 1\}^v$  such that  $\phi(b)$  and  $b \leq 0^v$  is  $\equiv i \pmod{17}$ .

*(This is  $\text{LMOD}_{17}$  restricted to  $y = 0^v$  and is as silly and as easy as it looks.) The set EASYCASE is in  $P$ .*

### 3 Intuitions and Chains

Assume for this section that we have the following.

- $S$  is a sparse set.  $s(n)$  is the polynomial such that  $|S \cap \{0, 1\}^n| \leq s(n)$ .
- $\text{SAT}_{17} \leq_m^p S$  via reduction  $f$ . Let  $p$  be such that  $f$  runs in time  $p(n)$ .

Given  $\phi$ , we want to determine if  $\phi \in \text{SAT}_{17}$ . Assume  $\phi$  has  $v$  variables and is of length  $n$ . We think of this as trying to determine if  $(\phi, 1^v, 0) \in \text{LMOD}_{17}$ .

Note that the question  $(\phi, 0^v, i) \in \text{LMOD}_{17}$  is easy (by Lemma 2.5). So we want to somehow make our problem equivalent to this one, for some  $i$ . We offer several bad ideas and then a good one.

**Bad Idea I:** Let  $g$  be the function from Lemma 2.3.

$(\phi, 1^v, 0) \in \text{LMOD}_{17}$  iff  $g(\phi, 1^v, 0) \in \text{LMOD}_{17}$  iff  $g(g(\phi, 1^v, 0)) \in \text{LMOD}_{17}$  etc.

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

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

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

**Bad Idea II:** Let  $f(\phi, 1^v, 0) = z$ . Lets look at  $f(\phi, 0^v, 0)$ ,  $f(\phi, 0^v, 1)$ ,  $f(\phi, 0^v, 2)$ ,  $\dots$ ,  $f(\phi, 0^v, 16)$ . If ANY of them are  $z$  then GREAT! We would have our problem equivalent to an easy problem. If not then  $\dots$  oh well.

**Bad Ideas III:** Again let  $f(\phi, 1^v, 0) = z$ . Try to find a  $(\phi, y, i)$  such that  $f(\phi, y, i) = z$ . If so then we have

$$(\phi, 1^v, 0) \in \text{LMOD}_{17} \text{ iff } (\phi, y, i) \in \text{LMOD}_{17}.$$

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

Note that we do have two different ways to have membership-in- $\text{LMOD}_{17}$  be equivalent:

$$(\phi, y, i) \in \text{LMOD}_{17} \text{ iff } g(\phi, y, i) \in \text{LMOD}_{17}.$$

and also

If  $f(\phi, y, i) = f(\phi, y', i')$  then

$$(\phi, y, i) \in \text{LMOD}_{17} \text{ iff } (\phi, y', i') \in \text{LMOD}_{17}.$$

We will use both of these to march towards  $0^v$ . However realize- we might not get there!! We will set things up so that we either make progress or find out directly if  $(\phi, 1^n, 0) \in \text{LMOD}_{17}$ .

**Def 3.1** A *chain of length  $m$*  is a sequence of the form

- $((\phi, y_1, i_1), z_1))$
- $((\phi, y_2, i_2), z_2))$
- $\vdots$
- $((\phi, y_m, i_m), z_m))$

such that the following hold.

1.  $y_1 > y_2 > \dots > y_m$  in lex order.
2. For all  $j, k$

$$(\phi, y_j, i_j) \in \text{LMOD}_{17} \text{ iff } (\phi, y_k, i_k) \in \text{LMOD}_{17}.$$

(Hence either all of the triples are in  $\text{LMOD}_{17}$  or all are not in.

3. For all  $j$ ,  $f(\phi, y_j, i_j) = z_j$ . (Hence, given the last point, either all of the  $z$ 's are in  $S$  or all are not in  $S$ .)
4. All of the  $z_i$  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  $(\phi, 0^v, i)$  for some  $i$ . Then we have our question equivalent to an easy question.
2. The chain goes long enough that not all of the (different!) values of  $z$ 's can be in  $S$ . Hence at least one is not in  $S$ . By the definition of chain, none of them are in  $S$ , and we know that  $(\phi, 1^v, 0) \notin \text{LMOD}_{17}$ .

## 4 The Key Lemma

**Lemma 4.1** *Assume there is a sparse set  $S$  such that  $\text{LMOD}_{17} \leq_m^p S$ . Then there is a polynomial time algorithm that does the following. The input is a chain of length  $m$  whose last element  $y_m \neq 0^v$ . The output is either*

1.  $((\phi, y_{m+1}, z_{m+1}))$  that extends the chain, or
2. The membership status in  $\text{LMOD}_{17}$  of every  $(\phi, y, i)$  on the chain. (Recall that they are either all in or all out.)

**Proof:**

Here is the algorithm

1. Input is
  - $((\phi, y_1, i_1), z_1)$
  - $((\phi, y_2, i_2), z_2)$
  - $\vdots$
  - $((\phi, y_m, i_m), z_m)$
2. Compute  $(\phi, y, i) = g(\phi, y_m, i_m)$ . Compute  $z = f(\phi, y, i)$ . If  $z \notin \{z_1, \dots, z_m\}$  then
  - (a)  $y_{m+1} = y_m^-$
  - (b)  $i_{m+1} = i$
  - (c)  $z_{m+1} = z$ .
  - (d) Note that  $y_{m+1} = y_m^- < y_m$ . Note that  $(\phi, y_{m+1}, i_{m+1}) \in \text{LMOD}_{17}$  iff  $(\phi, y_m, i_m) \in \text{LMOD}_{17}$ .
3. (If you got here then  $f(g(\phi, y_m, i_m)) \in \{z_1, \dots, z_m\}$ .) Compute
$$f(\phi, 0^v, 0), f(\phi, 0^v, 1), \dots, f(\phi, 0^v, 16).$$

If any of them are in  $\{z_1, \dots, z_m\}$  then let  $i$  be such that  $f(\phi, 0^v, i) \in \{z_1, \dots, z_m\}$ . Note that

$$(\phi, y_1, z_1) \in \text{LMOD}_{17} \text{ iff } (\phi, 0^v, i) \in \text{LMOD}_{17}.$$

By Lemma 2.5 we can determine  $(\phi, 0^v, i) \in \text{LMOD}_{17}$  in polynomial time. We do so, output the answer, and EXIT.

4. Let  $y_{\text{begin}} = y_m$  and  $y_{\text{end}} = 0^v$ . Note that, since we got to this step,

$$(a) (\exists i \in \{0, \dots, 16\})[f(\phi, y_{\text{begin}}, i) \in \{z_1, \dots, z_m\}]$$

$$(b) (\forall i \in \{0, \dots, 16\})[f(\phi, y_{\text{end}}, i) \notin \{z_1, \dots, z_m\}]$$

Both of these properties will hold for all of the values that  $y_{\text{begin}}$  and  $y_{\text{end}}$  take later in the algorithm.

5. Let  $y_{\text{mid}}$  be the value halfway between  $y_{\text{begin}}$  and  $y_{\text{end}}$  lexicographically.

6. Compute

$$\{f(\phi, y_{\text{mid}}, 0), f(\phi, y_{\text{mid}}, 1), \dots, f(\phi, y_{\text{mid}}, 16)\}.$$

If

$$\{z_1, \dots, z_m\} \cap \{f(\phi, y_{\text{mid}}, 0), f(\phi, y_{\text{mid}}, 1), \dots, f(\phi, y_{\text{mid}}, 16)\} \neq \emptyset$$

then

$y_{\text{begin}} = y_{\text{mid}}$  else  $y_{\text{end}} = y_{\text{mid}}$ . (The reader can easily check that the property we stated for  $y_{\text{begin}}, y_{\text{end}}$  still holds.)

7. If  $y_{\text{end}} = y_{\text{begin}}^-$  then note and do the following.

(a) There is an  $i$ ,  $0 \leq i \leq 16$ , such that  $f(\phi, y, i) \in \{z_1, \dots, z_m\}$ . (Note that  $y = y_{\text{begin}}$ .)

(b) For all  $i$ ,  $0 \leq i \leq 16$ ,  $f(\phi, y^-, i) \notin \{z_1, \dots, z_m\}$ . (Note that  $y^- = y_{\text{end}}$ .)

(c) Compute  $g(\phi, y, i)$ . Note that it is of the form  $(\phi, y^-, j)$ . Note the following.

i.  $f(\phi, y^-, j) \notin \{z_1, \dots, z_m\}$ .

ii.  $(\phi, y^-, j) \in \text{LMOD}_{17}$  iff  $(\phi, y, i) \in \text{LMOD}_{17}$  iff  $z \in S$  iff  $(\phi, y_1, i_1) \in \text{LMOD}_{17}$ .

iii. Output the ordered pair  $((\phi, y^-, j), f(\phi, y^-, j))$ .

8. (We are only here if we didn't satisfy the IF of the last step.) GOTO Step 5.

■

## 5 The Main Theorem

**Theorem 5.1** *If there exists a sparse set  $S$  such that  $\text{SAT}_{17} \leq_m^p S$  then  $\text{SAT}_{17} \in P$ .*

**Proof:** By Lemma 2.4

$$\text{LMOD}_{17} \leq_m^p \text{SAT}_{17}.$$

By the premise

$$\text{SAT}_{17} \leq_m^p S.$$

Hence we have

$$\text{LMOD}_{17} \leq_m^p S.$$

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  $\phi$ .  $v$  be the number of variables in  $\phi$ . Let  $n$  be the length of  $(\phi, 0^v, 0)$ . We will write the last number with 5 bits, so formally its  $(\phi, 0^v, 00000)$ . This way all of the  $(\phi, y, i)$  we deal with will be the same length. Let  $n$  be that length. Note that  $|f(\phi, y, i)| \leq p(n)$ .
2. Let  $y_1 = 1^v$ ,  $i_1 = 0$ , and  $z_1 = f(\phi, y_1, z_1)$ . View  $((\phi, y_1, i_1), z_1)$  as the first element of a chain.
3. Apply the algorithm from Lemma 4.1 over and over again to the chain until one of the following occurs.
  - (a) The algorithm returns the actual answer to  $(\phi, y_1, i_1) \in \text{LMOD}_{17}$ . Output that answer and EXIT.
  - (b) The algorithm returns with  $(\phi, 0^v, i)$ . By Lemma 2.5 the question  $(\phi, 0^v, i) \in \text{LMOD}_{17}$  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  $z_i \notin S$ . By the definition of a chain, none of them are in  $\text{LMOD}_{17}$ . Output NO and EXIT.

■

## References

- [1] M. Ogiwara and A. Lozano. On one query self-reducible sets. In *Proceedings of the 6th IEEE Conference on Structure in Complexity Theory*, Chicago IL, pages 139–151. IEEE Computer Society Press, 1991.
- [2] M. Ogiwara and A. Lozano. On sparse hard sets for counting classes. *Theoretical Computer Science*, 112:255–275, 1993.