**Sparse Sets IV: SAT in coNP-sparse**
**Exposition by William Gasarch**

# 1 $\mathrm{SAT} \in \Pi_1^{\mathrm{p,SPARSE}}$ then $\Sigma_3^{\mathrm{p}} = \Pi_3^{\mathrm{p}}$

Recall that $A \in \Sigma_1^{\mathrm{p}}$ if there exists $B \in P$ such that

$$A = \{x \mid (\exists^p y)[B(x,y)]\}.$$

**Notation 1.1**

1. A set $A$ is in $\Sigma_1^{\mathrm{p,SPARSE}}$ if there exists a set $B$ and a sparse set $S$ such that $B \le_{\mathrm{T}}^{\mathrm{p}} S$ and
$$A = \{x \mid (\exists^p y)[B(x,y)]\}.$$
2. A set $A$ is in $\Pi_1^{\mathrm{p,SPARSE}}$ if there exists a set $B$ and a sparse set $S$ such that $B \le_{\mathrm{T}}^{\mathrm{p}} S$ and
$$A = \{x \mid (\forall^p y)[B(x,y)]\}.$$
3. For $i \ge 2$, $A \in \Sigma_i^{\mathrm{p,SPARSE}}$ if there exists $B \in \Pi_{i-1}^{\mathrm{p,SPARSE}}$ such that
$$A = \{x \mid (\exists^p y)[B(x,y)]\}.$$
4. For $i \ge 2$, $A \in \Pi_i^{\mathrm{p,SPARSE}}$ if there exists $B \in \Pi_{i-1}^{\mathrm{p,SPARSE}}$ such that
$$A = \{x \mid (\forall^p y)[B(x,y)]\}.$$

Our goal is to show that

$$\mathrm{SAT} \in \Pi_1^{\mathrm{p,SPARSE}} \rightarrow \Sigma_3^{\mathrm{p}} = \Pi_3^{\mathrm{p}}.$$

We will need this lemma that we had before:

**Lemma 1.2** *Let $M^{()}$ be a POTM and let $S$ be a sparse set. Then there exists a PTM $N$ and a polynomial $p$ such that the following holds.*

$$(\forall n \in \mathsf{N})(\exists u, |u| = p(n))(\forall w \in \{0,1\}^{\le n})[M^S(w) = N(w;u)].$$

**Lemma 1.3** *If* $\Pi_1^{\rm p} \subseteq \Sigma_1^{\rm p,SPARSE}$ *then* $\Sigma_2^{\rm p,SPARSE} \subseteq \Sigma_1^{\rm p,SPARSE}$.

**Proof:** Let $A \in \Sigma_2^{\rm p,SPARSE}$. Then by definition there exists a POTM $M^{()}$ and a sparse set $S_1$ such that

$$A = \{x \mid (\exists^p y)(\forall^p z)[M^{S_1}(x,y,z) = 1]\}.$$

Let $p$ be such that $M^{S_1}$ runs in time $p(n)$.

Let $N$ be the PTM obtained by applying Lemma 1.2 to $M^{()}$ . So

$$(\forall n)(\exists^p u)(\forall x \in \{0,1\}^n)(\forall^p y)(\forall^p z)[M^{S_1}(x,y,z) = N(x,y,z,;u)]$$

Let

$$B = \{\langle x,y,u\rangle \mid (\forall^p z)[N(x,y,z;u)] = 1\}.$$

We can define $A$ in terms of $B$ as follows:

$$A = \{x \mid (\exists^p u)(\exists^p y)[\langle x,y,u\rangle \in B \wedge (u \text{ codes } S_1 \cap \{0,1\}^{\leq p(n)})\}.$$

Note that $B \in \Pi_1^{\rm p}$ (no oracle needed). By the hypothesis $B \in \Sigma_1^{\rm p,SPARSE}$. Hence there exists a sparse set $S_2$ such that $B \leq_{\rm T}^{\rm p} S_2$. Let $M_1^{()}$ be the POTM that does that reduction.

We now rewrite $A$:

$$A = \{x \mid (\exists^p u)(\exists^p y)[M_1^{S_2}(x,y,u) = 1 \wedge (u \text{ codes } S_1 \cap \{0,1\}^{\leq p(n)})\}.$$

How can we tell if $u$ codes $S_1 \cap \{0,1\}^{\leq p(n)}$? We can determine that $u$ codes the set $\{v_1,\ldots,v_L\}$. If we have access to $S_1$ we can ask $v_1 \in S_1$?, ..., $v_L \in S$? If any of them say NO then $u$ does not code $S_1 \cap \{0,1\}^{\leq p(n)}$. If they all say YES we still do not know that $u$ code $S_1 \cap \{0,1\}^{\leq p(n)}$. It could be that there is some element of $S_1 \cap \{0,1\}^{\leq p(n)}$ that is not in $\{v_1,\ldots,v_L\}$. We need a third sparse set to help us. Let

$$S_3 = \{< 0^n, |S \cap \{0,1\}^{\leq n}| > :; n \in \mathsf{N}\}.$$

We can also assume we know the polynomial $p$. So, to test if $u$ codes $S_1 \cap \{0,1\}^{\leq p(n)}$ we (1) ask, for each $i$, $1 \leq i \leq L$, $v_i \in S_1$, (2) ask if $< 0^{p(n)}, L > \in$

$S_3$. If the answer to all of these questions is YES then $u$ codes $S_1 \cap \{0,1\}^{\le p(n)}$. Else it does not.

Let $S$ be a sparse oracle that encodes $S_1$, $S_2$, and $S_3$. Note that the set

$$\{(x,y,u) \mid M_B^{S_2}(x,y,u) = 1 \wedge (u \text{ codes } S_1 \cap \{0,1\}^{\le p(n)})\} \le_{\mathrm{T}}^{\mathrm{p}} S$$

Hence we have shown that $A \in \Sigma_1^{\mathrm{p,SPARSE}}$.

■

**Exercise 1** Let $S_1$ and $S_2$ be sparse sets. Define a set $S$ such that $S$ is sparse, $S_1 \le_{\mathrm{m}}^{\mathrm{p}} S$, and $S_2 \le_{\mathrm{m}}^{\mathrm{p}} S$. **End of Exercise**

**Exercise 2** Let $i, j \in \mathsf{N}$.

1. Show that if $\Sigma_i^{\mathrm{p}} \subseteq \Pi_j^{\mathrm{p,SPARSE}}$ then $\Pi_i^{\mathrm{p}} \subseteq \Sigma_j^{\mathrm{p,SPARSE}}$.
2. Show that if $\Pi_i^{\mathrm{p}} \subseteq \Pi_j^{\mathrm{p,SPARSE}}$ then $\Sigma_i^{\mathrm{p}} \subseteq \Sigma_j^{\mathrm{p,SPARSE}}$.
3. Show that if $\Sigma_2^{\mathrm{p,SPARSE}} \subseteq \Sigma_1^{\mathrm{p,SPARSE}}$ then $\Sigma_3^{\mathrm{p,SPARSE}} \subseteq \Sigma_1^{\mathrm{p,SPARSE}}$.
4. Show that if $\Sigma_2^{\mathrm{p,SPARSE}} \subseteq \Sigma_1^{\mathrm{p,SPARSE}}$ then, $(\forall k \ge 1)[\Sigma_k^{\mathrm{p,SPARSE}} \subseteq \Sigma_1^{\mathrm{p,SPARSE}}]$.
5. Show that if $\Sigma_i^{\mathrm{p,SPARSE}} \subseteq \Pi_j^{\mathrm{p,SPARSE}}$ then $\Pi_i^{\mathrm{p,SPARSE}} \subseteq \Sigma_j^{\mathrm{p,SPARSE}}$.
6. Show that if $A \in \Sigma_i^{\mathrm{p,SPARSE}}$ then $\overline{A} \in \Pi_i^{\mathrm{p,SPARSE}}$.

**End of Exercise**

Our eventual goal is to show that if SAT $\in \Pi_1^{\mathrm{p,SPARSE}}$ then $\Sigma_3^{\mathrm{p}} = \Pi_3^{\mathrm{p}}$. Hence we need to look at sets that are complete for $\Sigma_3^{\mathrm{p}}$ or $\Pi_3^{\mathrm{p}}$. We will look at sets of quantified boolean formulas. In what follows keep in mind that $\phi$ is an arbitrary Boolean formula and the quantifiers are over Boolean values 0 and 1.

**Def 1.4**

1. $QBF_3$ is the set of all sentences of the form

   $$(\exists x_1,\ldots,x_{n_1})(\forall y_1,\ldots,y_{n_2})(\exists z_1,\ldots,z_{n_3})[\phi(x_1,\ldots,x_{n_1},y_1\ldots,y_{n_2},z_1,\ldots,z_{n_3})]$$

   that are true. ($\phi$ is quantifier free.)

   This set is $\Sigma_3^{\mathrm{p}}$-complete. Note that any of $n_1, n_2$, or $n_3$ be 0, but not all three.

2. $\overline{Q}BF_3$ is the set of all sentences of the form

$$(\forall x_1,\ldots,x_{n_1})(\exists y_1,\ldots,y_{n_2})(\forall z_1,\ldots,z_{n_3})[\phi(x_1,\ldots,x_{n_1},y_1\ldots,y_{n_2},z_1,\ldots,z_{n_3})]$$

   that are true. ($\phi$ is quantifier free.)

   This set is $\Pi_3^{\rm p}$-complete. Note that any of $n_1, n_2$, or $n_3$ be 0, but not all three.

We will use the following alternative definition of $\overline{Q}BF_3$. The definition is inductive on the number of variables.

**Def 1.5** A sentence $\psi$ is in $\overline{Q}BF_3$ if any of the following hold. (A sentence is NOT in $\overline{Q}BF_3$ if none of them hold.) In the below items $n_2$ and/or $n_3$ could be 0 which will cover cases with less than three alternations of quantifiers.

1. $\psi = (\forall x)[\phi(x)]$ and both $\phi(0)$ and $\phi(1)$ are true.

2. $\psi = (\exists x)[\phi(x)]$ and either $\phi(0)$ or $\phi(1)$ is true.

3. $\psi = (\exists x_1,\ldots,x_{n_1})(\forall y_1,\ldots,y_{n_2})[\phi(x_1,\ldots,x_{n_1},y_1,\ldots,y_{n_2})]$ and one of
   $(\exists x_2,\ldots,x_{n_1})(\forall y_1,\ldots,y_{n_2})[\phi(0,x_2,\ldots,x_{n_1},y_1,\ldots,y_{n_2})]$ or
   $(\exists x_2,\ldots,x_{n_1})(\forall y_1,\ldots,y_{n_2})[\phi(1,x_2,\ldots,x_{n_1},y_1,\ldots,y_{n_2})]$
   is in $\overline{Q}BF_3$. (Note that this is inducive on the number of variables. We are basing membership of $\psi$ in $\overline{Q}BF_3$ on membership of sentences with less variables.)

4. $\psi = (\forall x_1,\ldots,x_{n_1})(\exists y_1,\ldots,y_{n_2})(\forall z_1,\ldots,z_{n_3})[\phi(x_1,\ldots,x_{n_1},y_1,\ldots,y_{n_2},z_1,\ldots,z_{n_3})]$ and both
   $(\forall x_2,\ldots,x_{n_1})(\exists y_1,\ldots,y_{n_2})(\forall z_1,\ldots,z_{n_3})[\phi(0,x_2,\ldots,x_{n_1},y_1,\ldots,y_{n_2},z_1,\ldots,z_{n_3})]$ and
   $(\forall x_2,\ldots,x_{n_1})(\exists y_1,\ldots,y_{n_2})(\forall z_1,\ldots,z_{n_3})[\phi(1,x_2,\ldots,x_{n_1},y_1,\ldots,y_{n_2},z_1,\ldots,z_{n_3})]$
   are in $\overline{Q}BF_3$. (Note that this is inducive on the number of variables. We are basing membership of $\psi$ in $\overline{Q}BF_3$ on membership of sentences with less variables.)

**Exercise 3** Show that the definitions of $\overline{Q}BF_3$ in Definition 1.4.2 and 1.5 are equivalent. **End of Exercise**
**Exercise 4** Show that if $\overline{Q}BF_3 \in \Sigma_3^{\rm p}$ then $\Sigma_3^{\rm p} = \Pi_3^{\rm p}$. **End of Exercise**

**Lemma 1.6** *If* $\Pi_3^{\rm p,SPARSE} \subseteq \Pi_1^{\rm p,SPARSE}$ *then* $\Sigma_3^{\rm p} = \Pi_3^{\rm p}$.

**Proof:**

To show that $\Sigma_3^{\rm p} = \Pi_3^{\rm p}$ we show that $\overline{Q}BF_3 \in \Sigma_3^{\rm p}$ and use Exercise above. Clearly $\overline{Q}BF_3 \in \Pi_3^{\rm p} \subseteq \Pi_3^{\rm p,SPARSE}$. Hence by hypothesis $\overline{Q}BF_3 \in \Pi_1^{\rm p,SPARSE}$. So there exists a POTM $M^{()}$ and a sparse set $S$ such that

$$\overline{Q}BF_3 = \{\psi \mid (\forall^p y)[M^S(\psi, y)]\}$$

Let $N$ be the PTM obtained by applying Lemma 1.2 to $M^{()}$.

We are going to look at the set of sets of strings $u$ that make $N(\psi, y; u) = M^S(\psi, y)$ for formulas of length $\le n$ and $y$ of the appropriate length.

$$ADV = \{(u, n) \mid (\forall \psi, |\psi| \le n)[\psi \in \overline{Q}BF_3 \text{ iff } (\forall^p y)[N(\psi, y; u) = 1]]\}.$$

We assume that $N(;)$ always outputs 0 or 1.

We show that we can express the set $ADV$ in terms of quantifiers. We use the recursive definition of $\overline{Q}BF_3$ (Definition 1.5).

$(u, n) \in ADV$ iff for all $\psi$, $|\psi| \le n$, the following hold. (The polynomial bounded quantifiers are bounded by a polynomial in $n$.)

1. Case 1: $\psi = (\forall x)[\phi(x)]$. ($x$ is a single Boolean variable)

   $(\phi(0) \wedge \phi(1)) \rightarrow (\forall^p y)[N(\psi, y; u) = 1]$.

   $\wedge$

   $(\neg\phi(0) \vee \neg\phi(1)) \rightarrow (\exists^p y)[N(\psi, y; u) = 0]$.

2. Case 2: $\psi = (\exists x)[\phi(x)]$. ($x$ is a single boolean variable.)

   $(\phi(0) \vee \phi(1)) \rightarrow (\forall^p y)[N(\psi, y; u) = 1]$

   $\wedge$

   $(\neg\phi(0) \wedge \neg\phi(1)) \rightarrow (\exists^p y)[N(\psi, y; u) = 0]$.

3. Case 3: $\psi = (\exists x_1, \ldots, x_{n_1})(\forall y_1, \ldots, y_{n_2})[\phi(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2})]$.

   (This includes the case of $n_2 = 0$.)

   Let

   $\psi_0 = (\exists x_2, \ldots, x_{n_1})(\forall y_1, \ldots, y_{n_2})[\phi(0, x_2, \ldots, x_{n_1}, y_1, \ldots, y_{n_2})]$

   and

   $\psi_1 = (\exists x_2, \ldots, x_{n_1})(\forall y_1, \ldots, y_{n_2})[\phi(1, x_2, \ldots, x_{n_1}, y_1, \ldots, y_{n_2})]$.

   $((\forall^p y)[N(\psi_0, y; u) = 1] \vee (\forall^p y)[N(\psi_1, y; u) = 1]) \rightarrow$
   $\quad (\forall^p y)[N(\phi, y; u) = 1]$.

   $\wedge$

   $((\exists^p y)[N(\psi_0, y; u) = 0] \wedge (\exists^p y)[N(\psi_1, y; u) = 0]) \rightarrow$
   $\quad (\exists^p y)[M^U(\psi, y) = 0]$.

4. Case 4:

   $\psi = (\forall x_1, \ldots, x_{n_1})(\exists y_1, \ldots, y_{n_2})(\forall z_1, \ldots, z_{n_3})[\phi(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}, z_1, \ldots, z_{n_3})]$

   (This includes the case of $n_3 = 0$.)

   Let

   $\psi_0 = (\forall x_2, \ldots, x_{n_1})(\exists y_1, \ldots, y_{n_2})(\forall z_1, \ldots, z_{n_3})[\phi(0, x_2, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}, z_1, \ldots, z_{n_3})]$

   and

   $\psi_1 = (\forall x_2, \ldots, x_{n_1})(\exists y_1, \ldots, y_{n_2})(\forall z_1, \ldots, z_{n_3})[\phi(1, x_2, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}, z_1, \ldots, z_{n_3})]$.

   The statement is:

   $(\forall^p y)[N(\psi_0, y; u) = 1] \wedge (\forall^p y)[N(\psi_1, y; u) = 1] \rightarrow (\forall^p y)[M^U(\phi, y) = 1]$.

   $\wedge$

   $(\exists^p y)[N(\psi_0, y; u) = 0] \vee (\exists^p y)[N(\psi_1, y; u) = 0] \rightarrow (\exists^p y)[N(\phi, y; u) = 0]$.

**Exercise 5** Show that the two defintions of $ADV$ given above are equivalent.
**End of Exercise**

Given the above we can rewrite $ADV$ using two poly predicates $B$ and $C$ as follows:

$$ADV = \{(u, n) \mid (\forall \psi)[(\exists^p y)[B(\psi, y)] \wedge (\forall^p z)[C(\psi, z)]]\}$$

This can easily be written in $\Pi_2^{\mathrm{p}}$ form. So the upshot is that $ADV \in \Pi_2^{\mathrm{p}}$.

Recall that

$$\overline{Q}BF_3 = \{\psi \mid (\forall^p y)[M^S(\psi, y)]\}$$

We rewrite this in terms of saying that there exists a string in $ADV$ that will help us.

$$\overline{Q}BF_3 = \{\psi \mid (\exists^p u)[u \in ADV \wedge (\forall^p y)[N(\psi, y; u)]\}$$

Since $ADV \in \Pi_2^{\mathrm{p}}$ and the other part of the internal statement is $\Pi_1^{\mathrm{p}}$ we have that $\overline{Q}BF_3 \in \Sigma_3^{\mathrm{p}}$. ▮

**Theorem 1.7**

1. *If* $\mathrm{SAT} \in \Pi_1^{\mathrm{p,SPARSE}}$ *then* $\Sigma_3^{\mathrm{p}} = \Pi_3^{\mathrm{p}}$.
2. *If* $\mathrm{TAUT} \in \Sigma_1^{\mathrm{p,SPARSE}}$ *then* $\Sigma_3^{\mathrm{p}} = \Pi_3^{\mathrm{p}}$.

**Proof:**

1)

If $\mathrm{SAT} \in \Pi_1^{\mathrm{p,SPARSE}}$ then, since SAT is NP-complete, $\Sigma_1^{\mathrm{p}} \subseteq \Pi_1^{\mathrm{p,SPARSE}}$.

By Exercise 2.1 $\Pi_1^{\mathrm{p}} \subseteq \Sigma_1^{\mathrm{p,SPARSE}}$.

By Lemma 1.3 $\Sigma_2^{\mathrm{p,SPARSE}} \subseteq \Sigma_1^{\mathrm{p,SPARSE}}$.

By Exercise 2.3 $\Sigma_3^{\mathrm{p,SPARSE}} \subseteq \Sigma_1^{\mathrm{p,SPARSE}}$.

By Exercise 2.5 $\Pi_3^{\mathrm{p,SPARSE}} \subseteq \Pi_1^{\mathrm{p,SPARSE}}$.

By Lemma 1.6 $\Sigma_3^{\mathrm{p}} = \Pi_3^{\mathrm{p}}$.

2)

If $\mathrm{TAUT} \in \Sigma_1^{\mathrm{p,SPARSE}}$ then by Exercise 2.6 $\mathrm{SAT} \in \Pi_1^{\mathrm{p,SPARSE}}$. By part 1 we have $\Sigma_3^{\mathrm{p}} = \Pi_3^{\mathrm{p}}$. ▮

# 2 A Different View of Sparseness

**Def 2.1** A set $A$ is in P/poly if there exists a polynomial $p$, a function $\mathrm{ADV} : 0^* \rightarrow \{0,1\}^*$, and a polynomial prediate $B$ such that the following hold.

1. For all $n$, $\mathrm{ADV}(0^n) \in \{0,1\}^{p(n)}$.

2. For all $n$
$$A \cap \{0,1\}^{\le n} = \{x \mid B(x, \mathrm{ADV}(0^n))\}.$$

We think of the string $\mathrm{ADV}(0^n)$ as giving advice for all strings of length $\le n$. The class P/poly is often refered to as 'poly time with advice'.

We leave the following as an exercise.

**Lemma 2.2** *Let $A \subseteq \{0,1\}^*$. The following are equivalent.*

1. *$A \le_{\mathrm{T}}^{\mathrm{p}} S$ where $S$ is sparse set.*
2. *$A \in \mathrm{P/poly}$.*

We can also look at $\Sigma_i^{\mathrm{p}}$ with advice.

**Def 2.3** We assume that $i$ is odd. For $i$ even a similar definition holds. A set $A$ is in $\Sigma_i^{\mathrm{p}}$/poly if there exists a polynomial $p$, a function $\mathrm{ADV} : 0^* \rightarrow \{0,1\}^*$, and a polynomial prediate $B$ such that the following hold.

1. For all $n$, $\mathrm{ADV}(0^n) \in \{0,1\}^{p(n)}$.
2. For all $n$
$$A \cap \{0,1\}^n = \{x \mid (\exists y_1)(\forall y_2)\cdots(\exists y_i)[B(x, y_1, y_2, \ldots, y_i, \mathrm{ADV}(0^n))]\}.$$

**Note 2.4** $\Sigma_1^{\mathrm{p}}$/poly we refer to as NP/poly.

We leave the following as an exercise.

**Lemma 2.5** *Let $A \subseteq \{0,1\}^*$. The following are equivalent.*

1. *$A \in \Sigma_i^{\mathrm{p,SPARSE}}$.*
2. *$A \in \Sigma_i^{\mathrm{p}}$/poly.*

We also need the following which we leave as an exercise.

**Notation 2.6** If $X$ and $Y$ are sets then $X \Delta Y$ is $(X - Y) \cup (Y - X)$. Note that $X \Delta Y$ is the set of elements where $X$ and $Y$ differ.

**Lemma 2.7** *Let $A, A' \subseteq \{0,1\}^*$. If there exists a polynomial $s$ such that, for all $n$,*

$$|(A \cap \{0,1\}^{\leq n}) \Delta (A' \cap \{0,1\}^{\leq n}| \leq s(n)$$

*then $A \in \Sigma_i^{\mathrm{p,SPARSE}}$ iff $A' \in \Sigma_i^{\mathrm{p,SPARSE}}$. (We are saying that if $A$ and $A'$ only differ by a polynomial amount on each length $n$, then $A$ and $A'$ are similar enough that they are either both in $\Sigma_i^{\mathrm{p,SPARSE}}$ or both not in $\Sigma_i^{\mathrm{p,SPARSE}}$.)*

We restate The Karp Lipton Theorem and Yaps theorem for the contrast:
Karp Lipton Theorem:
**If** $SAT \in \mathrm{P/poly}$ **then** $\mathrm{PH} = \Sigma_2^{\mathrm{p}} = \Pi_2^{\mathrm{p}}$

Yap's Theorem:
**If** $SAT \in \text{co-NP/poly}$ **then** $\mathrm{PH} = \Sigma_3^{\mathrm{p}} = \Pi_3^{\mathrm{p}}$