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

1 SAT ∈ \Pi_{1}^{p, \text{Sparse}} \text{ then } \Sigma_{3}^{p} = \Pi_{3}^{p}

Recall that \( A \in \Sigma_{i}^{p} \) if there exists \( B \in P \) such that
\[
A = \{ x \mid (\exists y)[B(x,y)] \}.
\]

Notation 1.1

1. A set \( A \) is in \( \Sigma_{1}^{p, \text{Sparse}} \) if there exists a set \( B \) and a sparse set \( S \) such that \( B \leq_{T}^{p} S \) and
\[
A = \{ x \mid (\exists y)[B(x,y)] \}.
\]

2. A set \( A \) is in \( \Pi_{1}^{p, \text{Sparse}} \) if there exists a set \( B \) and a sparse set \( S \) such that \( B \leq_{T}^{p} S \) and
\[
A = \{ x \mid (\forall y)[B(x,y)] \}.
\]

3. For \( i \geq 2 \), \( A \in \Sigma_{i}^{p, \text{Sparse}} \) if there exists \( B \in \Pi_{i-1}^{p, \text{Sparse}} \) such that
\[
A = \{ x \mid (\exists y)[B(x,y)] \}.
\]

4. For \( i \geq 2 \), \( A \in \Pi_{i}^{p, \text{Sparse}} \) if there exists \( B \in \Pi_{i-1}^{p, \text{Sparse}} \) such that
\[
A = \{ x \mid (\forall y)[B(x,y)] \}.
\]

Our goal is to show that
\[
\text{SAT} \in \Pi_{1}^{p, \text{Sparse}} \rightarrow \Sigma_{3}^{p} = \Pi_{3}^{p}.
\]

We will need this lemma that we had before:

Lemma 1.2 Let \( M^{(i)} \) 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.
\[
(\forall n \in \mathbb{N})(\exists u, |u| = p(n))(\forall w \in \{0, 1\}^{\leq n})[M^{S}(w) = N(w; u)].
\]
Lemma 1.3 If $\Pi_1^p \subseteq \Sigma_1^p_{\text{SPARSE}}$ then $\Sigma_2^p_{\text{SPARSE}} \subseteq \Sigma_1^p_{\text{SPARSE}}$.

Proof: Let $A \in \Sigma_2^p_{\text{SPARSE}}$. Then by definition there exists a POTM $M^{(1)}$ and a sparse set $S_1$ such that

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

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

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

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

Note that $B \in \Pi_1^p$ (no oracle needed). By the hypothesis $B \in \Sigma_1^p_{\text{SPARSE}}$. Hence there exists a sparse set $S_2$ such that $B \leq_{\text{p}}^1 S_2$. Let $M_1^{(1)}$ be the POTM that does that reduction.

We now rewrite $A$:

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

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 $v_i \in S_1$? 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 $S_3 = \{< 0^n, |S \cap \{0, 1\}^{\leq n}| > \}$. 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 $< 0^{p(n)}, L > \in$
If the answer to all of these questions is YES then $u$ codes $S_1 \cap \{0, 1\} \leq^p \langle n \rangle$.
Else it does not.

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

$$\{(x, y, u) \mid M_{S_2}^S(x, y, u) = 1 \land (u \text{ codes } S_1 \cap \{0, 1\} \leq^p \langle n \rangle)\} \leq_T S$$

Hence we have shown that $A \in \Sigma_{i}^p, \text{SPARSE}.$

**Exercise 1** Let $S_1$ and $S_2$ be sparse sets. Define a set $S$ such that $S$ is sparse, $S_1 \leq_m S$, and $S_2 \leq_m S$. **End of Exercise**

**Exercise 2** Let $i, j \in \mathbb{N}$.
1. Show that if $\Pi_i^p \subseteq \Pi_j^p, \text{SPARSE}$ then $\Pi_i^p \subseteq \Sigma_j^p, \text{SPARSE}.$
2. Show that if $\Pi_i^p \subseteq \Pi_j^p, \text{SPARSE}$ then $\Sigma_i^p \subseteq \Sigma_j^p, \text{SPARSE}.$
3. Show that if $\Sigma_2^p, \text{SPARSE} \subseteq \Sigma_1^p, \text{SPARSE}$ then $\Sigma_3^p, \text{SPARSE} \subseteq \Sigma_1^p, \text{SPARSE}.$
4. Show that if $\Sigma_2^p, \text{SPARSE} \subseteq \Sigma_1^p, \text{SPARSE}$ then $(\forall k \geq 1)[\Sigma_k^p, \text{SPARSE} \subseteq \Sigma_1^p, \text{SPARSE}].$
5. Show that if $\Sigma_i^p, \text{SPARSE} \subseteq \Pi_j^p, \text{SPARSE}$ then $\Pi_i^p, \text{SPARSE} \subseteq \Sigma_j^p, \text{SPARSE}.$
6. Show that if $A \in \Sigma_i^p, \text{SPARSE}$ then $\overline{A} \in \Pi_i^p, \text{SPARSE}.$

**End of Exercise**

Our eventual goal is to show that if $\text{SAT} \in \Pi_1^p, \text{SPARSE}$ then $\Sigma_3^p = \Pi_3^p.$ Hence we need to look at sets that are complete for $\Sigma_3^p$ or $\Pi_3^p$. 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 $\Sigma_3^p$-complete. Note that any of $n_1, n_2,$ or $n_3$ be 0, but not all three.
2. $\overline{QBF}_3$ 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 $\Pi^p_3$-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 $\overline{QBF}_3$. The definition is inductive on the number of variables.

**Def 1.5** A sentence $\psi$ is in $\overline{QBF}_3$ if any of the following hold. (A sentence is NOT in $\overline{QBF}_3$ 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 $\overline{QBF}_3$. (Note that this is inducive on the number of variables. We are basing membership of $\psi$ in $\overline{QBF}_3$ 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 $\overline{QBF}_3$. (Note that this is inducive on the number of variables. We are basing membership of $\psi$ in $\overline{QBF}_3$ on membership of sentences with less variables.)
Exercise 3 Show that the definitions of $QBF_3$ in Definition 1.4.2 and 1.5 are equivalent. End of Exercise

Exercise 4 Show that if $QBF_3 \in \Sigma^p_3$ then $\Sigma^p_3 = \Pi^p_3$. End of Exercise

Lemma 1.6 If $\Pi^p_3, SPARSE \subseteq \Pi^p_3, SPARSE$ then $\Sigma^p_3 = \Pi^p_3$.

Proof:
To show that $\Sigma^p_3 = \Pi^p_3$ we show that $QBF_3 \in \Sigma^p_3$ and use Exercise above.
Clearly $QBF_3 \in \Pi^p_3 \subseteq \Pi^p_3,SPARSE$. Hence by hypothesis $QBF_3 \in \Pi^p_1,SPARSE$.
So there exists a POTM $M^{(1)}$ and a sparse set $S$ such that

$$QBF_3 = \{ \psi \mid (\forall^p y)[M^S(\psi, y)] \}$$

Let $N$ be the PTM obtained by applying Lemma 1.2 to $M^{(1)}$.
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 $\leq n$ and $y$ of the appropriate length.

$$ADV = \{(u, n) \mid (\forall \psi, |\psi| \leq n)[\psi \in QBF_3 \text{ iff } (\forall^p y)[N(\psi, y; u) = 1]]\}.$$ We assume that $N(\cdot)$ always outputs 0 or 1.
We show that we can express the set $ADV$ in terms of quantifiers. We use the recursive definition of $QBF_3$ (Definition 1.5).
$(u, n) \in ADV$ iff for all $\psi$, $|\psi| \leq n$, 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)
   $$(\phi(0) \land \phi(1)) \land (\forall^p y)[N(\psi, y; u) = 1].$$

2. Case 2: $\psi = (\exists x)[\phi(x)]$. ($x$ is a single boolean variable.)
   $$(\phi(0) \lor \phi(1)) \land (\forall^p y)[N(\psi, y; u) = 1].$$
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
\[
\psi_1 = (\exists x_2, \ldots, x_{n_1})(\forall y_1, \ldots, y_{n_2})[\phi(1, x_2, \ldots, x_{n_1}, y_1, \ldots, y_{n_2})].
\]

\([\forall p y][N(\psi_0, y; u) = 1] \vee [\forall p y][N(\psi_1, y; u) = 1]\) \(\rightarrow\)
\([\forall p y][N(\phi, y; u) = 1] \wedge ([\exists p y][N(\psi_0, y; u) = 0] \vee [\exists p y][N(\psi_1, y; u) = 0]) \rightarrow [\exists p y][M^U(\phi, y) = 0].\)

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 definitions 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 $\Pi_p^2$ form. So the upshot is that $ADV \in \Pi_p^2$.

Recall that

$$QBF_3 = \{ \psi \mid (\forall^p y)[M^S(\psi, y)] \}$$

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

$$QBF_3 = \{ \psi \mid (\exists u)[u \in ADV \land (\forall^p y)[N(\psi, y; u)] \}$$

Since $ADV \in \Pi_p^2$ and the other part of the internal statement is $\Pi_p^1$ we have that $QBF_3 \in \Sigma_p^3$.

**Theorem 1.7**

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

**Proof:**

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

   By Exercise 2.1 $\Pi_1^p \subseteq \Sigma_2^{p,\text{SPARSE}}$

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

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

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

   By Lemma 1.6 $\Sigma_3^p = \Pi_3^p$.

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

2 A Different View of Sparseness

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

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


2. For all $n$

$$A \cap \{0, 1\}^{\leq n} = \{x \mid B(x, \text{ADV}(0^n))\}.$$  

We think of the string $\text{ADV}(0^n)$ as giving advice for all strings of length $\leq n$. The class $P/\text{poly}$ is often referred 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. $A \leq^p_T S$ where $S$ is sparse set.
2. $A \in P/\text{poly}$.

We can also look at $\Sigma^p_i$ with advice.

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

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

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

**Note 2.4** $\Sigma^p_i/\text{poly}$ we refer to as $\text{NP/\text{poly}}$.

We leave the following as an exercise.

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

1. $A \in \Sigma^{n, \text{SPARSE}}_i$.
2. $A \in \Sigma^p_i/\text{poly}$.

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 $A \in \Sigma_i^{p, \text{SPARSE}}$ iff $A' \in \Sigma_i^{p, \text{SPARSE}}$. (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 $\Sigma_i^{p, \text{SPARSE}}$ or both not in $\Sigma_i^{p, \text{SPARSE}}$.)

We restate The Karp Lipton Theorem and Yaps theorem for the contrast:

Karp Lipton Theorem:
\textbf{If} $SAT \in \text{P/poly}$ \textbf{then} $PH = \Sigma_2^p = \Pi_2^p$

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