Notes for Lecture 4
Malka Rosenthal

Proof of Statement C of Switching Lemma, con’t
If $\|\text{dom}(\pi_1)\| \geq s$, let $S$ be the first $s$ variables in $\text{dom}(\pi_1)$ and let $\sigma = \hat{\pi}_1|_S$. Otherwise, 
Note: There exists some $i$ with $\rho \pi_1(D_i) \neq 1$ since otherwise $f|_{\rho \pi_1} \equiv 1$. This is impossible as $f|_\rho \neq 1$ (as earlier in proof) and $\pi_1$ only sets fewer than $s$ literals in $C_j$, a conjunct with at least $s + 1$ variables. Let
$$i_2 = \min\{i : \rho \pi_1(D_i) \neq 1\}$$
Let
$$S_2 = (D_{i_2} \setminus \text{dom}(\rho \pi_1)) \cap \text{dom}(\pi).$$
Let $\pi_2 = \pi|_{S_2}$.
Define $\tilde{\pi}_2$ as follows:
$$\tilde{\pi}_2(i) = \begin{cases} * & i \notin S_2 \\ 1 & \pi_i \in D_{i_2} \\ 0 & \pi_i \notin D_{i_2} \end{cases}$$
Thus:
- $\text{dom}(\pi_2) = \text{dom}(\tilde{\pi}_2)$.
- $\pi_2 \neq \tilde{\pi}_2$, as for example, $\rho \pi_2(D_{i_2}) = 1$ and $\rho \tilde{\pi}_2(D_{i_2}) \neq 1$.
- $\rho \pi_1(D_{i_2}) = *$. (It is $\neq 0$ as $\pi_1$ can be extended to $\pi$ which makes $D_{i_2}$ true.)
- $\forall l < i_2 \ \rho \pi_1(D_l) = 1$. (By def’n of $i_2$)
- For any setting $\pi'$ of the literals in $\text{dom}(\pi) \setminus \text{dom}(\pi_1 \pi_2)$, we have
  $$\left\{ \begin{array}{l} \rho \pi_1 \tilde{\pi}_2 \pi'(D_{i_2}) \in \{0, *\} \\ \forall l < i_2 \ \rho \pi_1 \tilde{\pi}_2 \pi'(D_l) = 1 \end{array} \right.$$
For $1 \leq j \leq k - 1$, $\gamma_j$ will describe how (in which places) $\pi_j$ and $\tilde{\pi}_j$ differ. Let $D_{ij}$ be a disjunction of literals on the variables $\{x_j, \ldots, x_{j+i}\}$. Let the $i^{th}$ bit of $\gamma_j$,

$$\gamma_j (i) = \begin{cases} * & \pi_j (x_j) \notin \text{dom}(\pi_j) \text{ or } l > r \\ 0 & \pi_j (x_j) = \tilde{\pi}_j (x_j) \\ 1 & \pi_j (x_j) \neq \tilde{\pi}_j (x_j) \end{cases}$$

Let $\gamma_k$ be as follows: Let $D_{ik}$ be a disjunction of literals on the variables $\{x_i, \ldots, x_{k+i}\}$ and let the $i^{th}$ bit of $\gamma_k$,

$$\gamma_k (i) = \begin{cases} * & \pi_k (x_k) \notin \text{dom}(\sigma) \text{ or } l > r' \\ 0 & \text{otherwise} \end{cases}$$

For $k \leq j \leq s$, let $\gamma_j = \{\ast\}^t$.

Let $\gamma = \gamma_1 \gamma_2 \ldots \gamma_s$ (concatenate the strings together). Note that $|\gamma| = st$.

**Note:** $\gamma$ contains exactly $s$ symbols which are not equal to * as

$$|\text{dom}(\pi_1 \ldots \pi_{k-1}\sigma)| = s = |\text{dom}(\tilde{\pi}_1 \ldots \tilde{\pi}_{k-1}\sigma)|.$$

Thus $\gamma$ is of the form

$$\ast^n b_1 \ast^{n_1} \ldots b_s \ast^{n_s}$$

where $b_i \in \{0, 1\}$ for $0 \leq i \leq s$ and $0 \leq n_i \leq 2t$ for $0 \leq i \leq s - 1$. This is because each $\gamma_j$ must contain at least one bit $\in \{0, 1\}$ until there have been $s$ bits $\neq \{\ast\}$.

Therefore, to describe $\gamma$ given $s$ and $t$, we can use a string of the form $\pi y_{b_1} y_{b_2}$ with $z$ giving instructions to interpret the next $s \log 2t = \lfloor y_{b_1} \rfloor$ bits as values of $n_1, \ldots, n_s$ (as $n_i \leq 2t$ for $1 \leq i \leq s - 1$) and to interpret $y_{b_i}$ with $| y_{b_i} | = s$ as the $s$ $b_i$’s.

We have shown that

$$K(\gamma(s, t)) \leq s \log 2t + s + c_2$$

**Claim:** $K(\rho f, l, s) \leq \log \big( \binom{n}{l} \big) + n - l + s \log 8t + c$.

**Proof:** Given $f, l, s$, we can build $\rho$ with a description of the form $\pi y_{\rho}, y_1$ where $y_{\rho}$ is a string of length $\log \big( \binom{n}{l} \big) + n - l + s + c_1$ and $y_1$ is a string of length $s \log 2t + s + c_2$.

Building such a $y_{\rho}$ is possible as $\rho \in R^{2t}$ and building such a $y_1$ is possible by (1) above.

$\pi$ will have constant length and will contain the following instructions:
• Use $f$ to find $n$ and $t$.

• Use $s$ and $t$ to compute $|y| = s \log 2t + s + c_2$.

• Use $y_{\rho'}$ to compute $\rho'$ and $y_s$ to compute $\gamma$.

• Express $f$ as $f = \bigwedge_i D_i$ and find $i_1 = \min \{ i : \rho'(D_i) \neq 1 \}$.

• Use $D_{i_1}$ and $\gamma_1$ to find

$$\text{dom}(\pi_1) = \{ \text{variables in } D_{i_1} \text{, corresponding to non-stars in } \gamma_1 \}$$

Recall that $\gamma_1$ is just the first $t$ variables in $\gamma$ so $\gamma_1$ is given once $\gamma$ has been found.

Note:

$$\pi_1 = \rho' \mid_{\text{dom}(\pi_1)} \text{ as } \rho' = \rho \tilde{x}_1 \tilde{x}_2 \ldots \tilde{x}_{k-1} \sigma$$

• Build $\pi_1$ as follows:

$$\pi_1(i) = \begin{cases} 
* & i \notin \text{dom}(\pi_1) \\
\gamma_j \oplus \tilde{x}_1(i) & x_i = j^{th} \text{ variable in } D_{i_1}
\end{cases}$$

• Let $i_2 = \min \{ i : \rho \tilde{x}_1 \tilde{x}_2 \ldots \tilde{x}_{k-1} \sigma(D_i) \neq 1 \}$.

As above, find $\text{dom}(\pi_2)$ and build $\pi_2$. Continuing in this manner, build $\pi_3, \ldots, \pi_{k-1}, \sigma$. (Recall that $s$ is given so we know when $\sigma$ has been found.)

• Finally,

$$\rho' = \rho' \mid_{\{1, \ldots, n\} \setminus \text{dom}(\pi_1 \ldots \pi_{k-1}, \sigma)}$$

Thus, using $\mathfrak{N}_{\rho', y_s}$ we can find $\rho$ and we have shown that

$$K(\rho|f, l, s) \leq \log \left( \begin{array}{c} n \\ l - s \end{array} \right) + n - l + s + c_1 + s \log 2t + s + c_2$$

$$= \log \left( \begin{array}{c} n \\ l - s \end{array} \right) + n - l + s \log 8t + c$$

which completes the proof.