Bounded Query Functions with Limited Output Bits

Richard Chang Jon S. Squire

University of Maryland Baltimore County

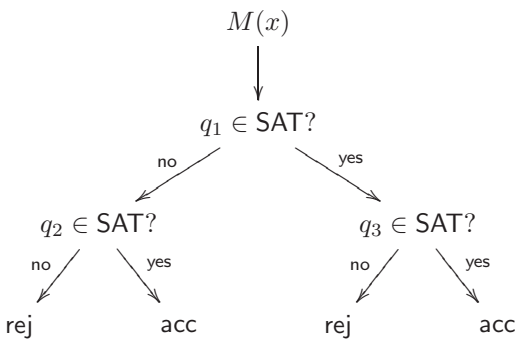
Bounded Query Classes

- Characterizes the complexity of NP-optimization problems. [Krentel '88]
  - Max-Clique-Size complete for $\mathrm{PF}^{\mathrm{SAT}[O(\log n)]}$.
  - Min-TSP-Length complete for $\mathrm{PF}^{\mathrm{SAT}[n^{O(1)}]}$.
- Characterizes the complexity of NP-approximation problems.
  [Chang '96] [Chang, Gasarch & Lund '97]:
  - 2-approximating Max-Clique-Size complete for $\mathrm{PF}^{\mathrm{SAT}[O(\log \log n)]}$.
  - 2-approximating Min-TSP-Length complete for $\mathrm{PF}^{\mathrm{SAT}[O(\log n)]}$.

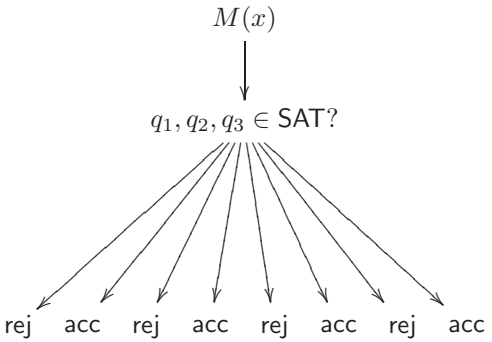
Additional Queries

- Usually more queries to SAT means more computational power:
  - $\mathrm{PF}^{\mathrm{SAT}[k]} = \mathrm{PF}^{\mathrm{SAT}[k+1]} \Longrightarrow \mathrm{P} = \mathrm{NP}$. [Beigel, Kummer, Stephan '95]
  - $\mathrm{P}^{\mathrm{SAT}[k]} = \mathrm{P}^{\mathrm{SAT}[k+1]} \Longrightarrow$ PH collapses. [Kadin '88]
- Functions: $\mathrm{PF}^{\mathrm{SAT}[O(\log n)]} = \mathrm{PF}^{\mathrm{SAT}[n^{O(1)}]} \Longrightarrow \mathrm{P} = \mathrm{NP}$. [Krentel '88]
  - $\mathrm{P} \neq \mathrm{NP} \Longrightarrow$ Min-TSP-Length is harder than Max-Clique-Size.
- Languages: $\mathrm{P}^{\mathrm{SAT}[O(\log n)]} = \mathrm{P}^{\mathrm{SAT}[n^{O(1)}]} \Longrightarrow$???
  - equivalent: $\mathrm{PF}^{\mathrm{SAT}\|[n^{O(1)}]} = \mathrm{PF}^{\mathrm{SAT}[n^{O(1)}]} \Longrightarrow$???
  - ??? $\Longrightarrow$ Min-TSP is harder than Max-Clique.
- Need to consider function vs language classes and parallel vs serial queries.

2 serial queries vs 3 parallel queries (languages)



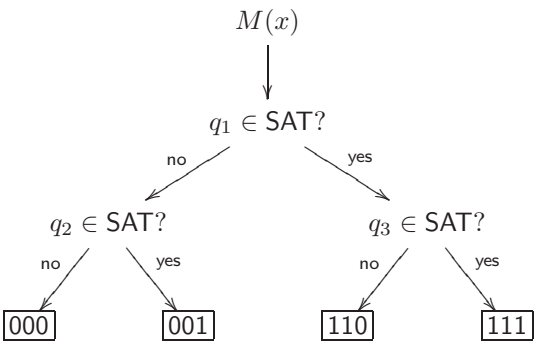
$\mathsf{P}^{\mathsf{SAT}[2]}$



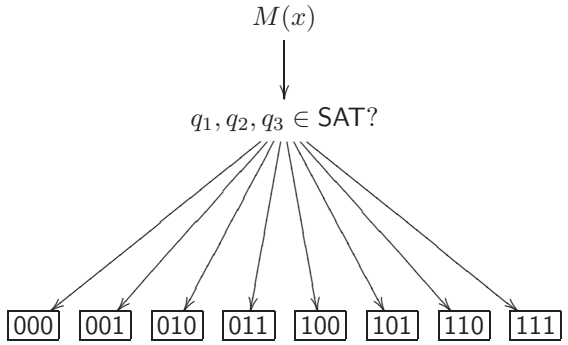
$\mathsf{P}^{\mathsf{SAT}\|[3]}$

- $\mathsf{P}^{\mathsf{SAT}[2]} \subseteq \mathsf{P}^{\mathsf{SAT}\|[3]}$, easy.
- $\mathsf{P}^{\mathsf{SAT}\|[3]} \subseteq \mathsf{P}^{\mathsf{SAT}[2]}$, mind changes. [Beigel '91]

2 serial queries vs 3 parallel queries (functions)



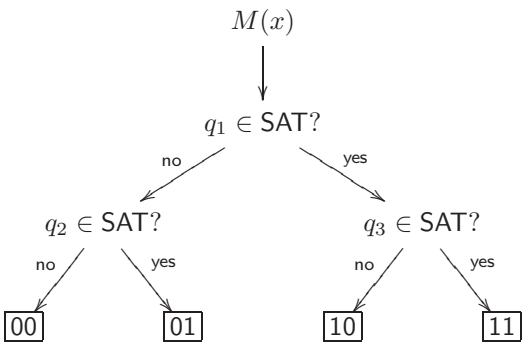
$\mathrm{PF}^{\mathrm{SAT}[2]}$



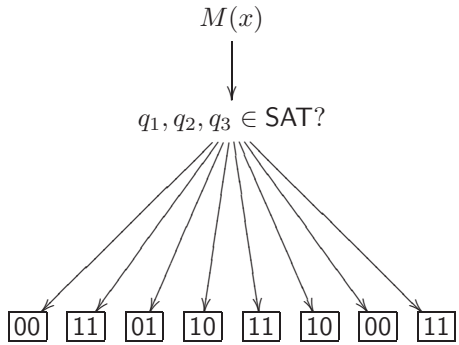
$\mathrm{PF}^{\mathrm{SAT}\|[3]}$

- $\mathrm{PF}^{\mathrm{SAT}[2]} \subseteq \mathrm{PF}^{\mathrm{SAT}\|[3]}$, still easy.
- $\mathrm{PF}^{\mathrm{SAT}\|[3]} \subseteq \mathrm{PF}^{\mathrm{SAT}[2]} \Longrightarrow \mathrm{P} = \mathrm{NP}$. [Beigel, Kummer, Stephan '95]
  - enumerability: $\mathrm{PF}^{\mathrm{SAT}[2]}$ can output only 4 values
  - for all X, $\left[\mathrm{PF}^{\mathrm{SAT}\|[3]} \subseteq \mathrm{PF}^{\mathrm{X}[2]} \Longrightarrow \mathrm{P} = \mathrm{NP} \right]$.

2 serial queries vs 3 parallel queries (2-bit functions)



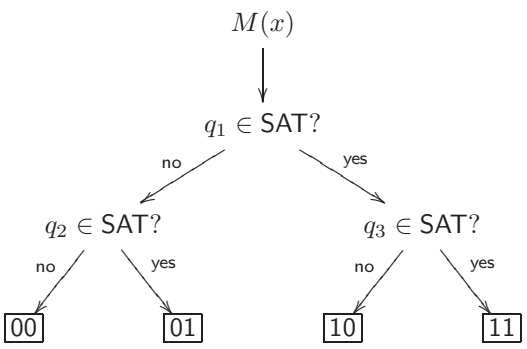
$\mathsf{PF}_2^{\mathsf{SAT}[2]}$



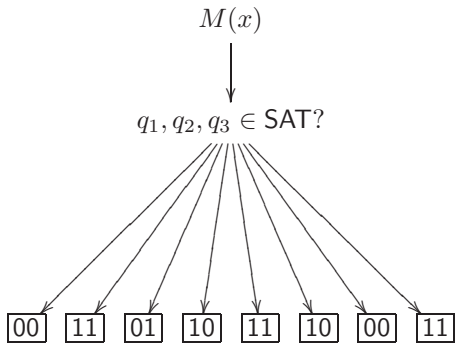
$\mathsf{PF}_2^{\mathsf{SAT}\|[3]}$

- functions limited to 2 bits of output (can't use enumerability arguments)
- there exists X such that $\mathsf{PF}_2^{\mathsf{SAT}\|[3]} \subseteq \mathsf{PF}_2^{X[2]}$
- $\mathsf{NP} = \mathsf{coNP} \Longrightarrow \mathsf{PF}_2^{\mathsf{SAT}[2]} = \mathsf{PF}_2^{\mathsf{SAT}\|[3]}$
- $\mathsf{PF}_2^{\mathsf{SAT}[2]} = \mathsf{PF}_2^{\mathsf{SAT}\|[3]} \Longrightarrow ???$

main theorem



$\mathrm{PF}_2^{\mathrm{SAT}[2]}$



$\mathrm{PF}_2^{\mathrm{SAT}\|[3]}$

Main Theorem: $\mathrm{PF}_2^{\mathrm{SAT}[2]} = \mathrm{PF}_2^{\mathrm{SAT}\|[3]} \Longrightarrow \mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$.

main theorem: proof structure

- $\mathsf{BL}_3 = (\mathsf{SAT} \wedge \overline{\mathsf{SAT}}) \vee \mathsf{SAT}$

  $= \{\ \langle F_1, F_2, F_3\rangle \mid (F_1 \in \mathsf{SAT} \wedge F_2 \in \overline{\mathsf{SAT}}) \vee F_3 \in \mathsf{SAT}\ \}$

- $\mathsf{coBL}_3 = \{\ \langle F_1, F_2, F_3\rangle \mid \langle F_1, F_2, F_3\rangle \notin \mathsf{BL}_3\ \}$

- BL_3 is $\leq_{\mathsf{m}}^{\mathsf{P}}$-complete for BH_3, the third level of the Boolean Hierarchy.

- $\mathsf{BL}_3 \leq_{\mathsf{m}}^{\mathsf{P}} \mathsf{coBL}_3 \implies \mathsf{BH}_3 = \mathsf{coBH}_3 \implies \mathsf{PH} \subseteq \Sigma_3^{\mathsf{P}}$. [Kadin '88, ...]

- We will show $\mathsf{PF}_2^{\mathsf{SAT}[2]} = \mathsf{PF}_2^{\mathsf{SAT}\|[3]} \implies \mathsf{BL}_3 \leq_{\mathsf{m}}^{\mathsf{P/poly}} \mathsf{coBL}_3$.

- Still get $\mathsf{coNP} \subseteq \mathsf{NP/poly} \implies \mathsf{PH} \subseteq \Sigma_3^{\mathsf{P}}$.

main theorem: spiting function

- $\mathsf{ODD}_3^{\mathsf{SAT}} = \{\ \langle F_1, F_2, F_3\rangle \mid$ number of $F_i \in \mathsf{SAT}$ is odd $\}$.
- Define $\mathcal{Q}_{32}$ a two-bit function such that $\mathcal{Q}_{32}(F_1, F_2, F_3) = ab$ where

$$a = 1 \iff \langle F_1, F_2, F_3\rangle \in \mathsf{BL}_3$$

$$b = 1 \iff \langle F_1, F_2, F_3\rangle \in \mathsf{ODD}_3^{\mathsf{SAT}}.$$

- $\mathcal{Q}_{32} \in \mathsf{PF}_2^{\mathsf{SAT}\|[3]}$
- intuition: a $\mathsf{PF}_2^{\mathsf{SAT}[2]}$ machine can compute BL_3 or $\mathsf{ODD}_3^{\mathsf{SAT}}$, not both.
- less intuitive: spite a $\mathsf{PF}_2^{\mathsf{SAT}[2]}$ machine by giving it easy instances of $\mathcal{Q}_{32}$.

easy instances of $\mathcal{Q}_{32}$

- Defn: $\langle F_1, F_2, F_3 \rangle$ is nested if:

$$F_3 \in \mathsf{SAT} \Longrightarrow F_2 \in \mathsf{SAT} \quad \text{and} \quad F_2 \in \mathsf{SAT} \Longrightarrow F_1 \in \mathsf{SAT}$$

- Let $F_1' = F_1 \vee F_2 \vee F_3$, $F_2' = F_2 \vee F_3$ and $F_3' = F_3$.

  Then $\langle F_1', F_2', F_3' \rangle$ is nested and

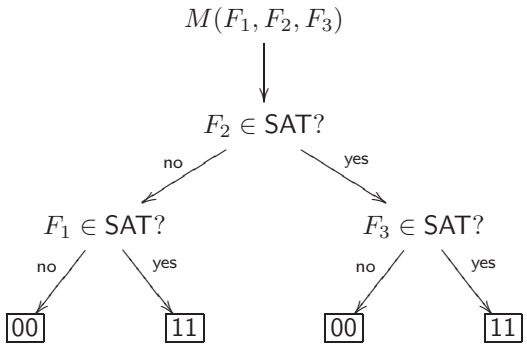
$$\langle F_1, F_2, F_3 \rangle \in \mathsf{BL}_3 \iff \langle F_1', F_2', F_3' \rangle \in \mathsf{BL}_3$$

- If $\langle F_1, F_2, F_3 \rangle$ is nested then $\mathcal{Q}_{32} = 00$ or 11 since

$$\langle F_1, F_2, F_3 \rangle \in \mathsf{BL}_3 \iff \langle F_1, F_2, F_3 \rangle \in \mathsf{ODD}_3^{\mathsf{SAT}}$$

- A $\mathsf{PF}_2^{\mathsf{SAT}[2]}$ machine can compute $\mathcal{Q}_{32}$ on nested instances.

a technical lemma

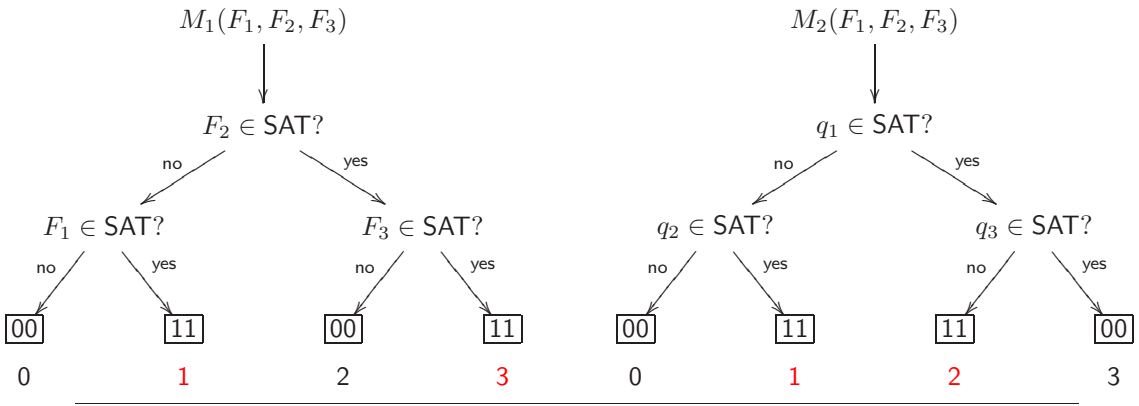


Technical Lemma:

Suppose that a $\mathsf{PF}_2^{\mathsf{SAT}[2]}$ machine M computes $\mathcal{Q}_{32}$. Let $\langle F_1, F_2, F_3 \rangle$ be nested. If the output sequence of $M(F_1, F_2, F_3)$ is not $\langle 00, 11, 00, 11 \rangle$, then we can construct $\langle G_1, G_2, G_3 \rangle$ in polynomial time such that

$$\langle F_1, F_2, F_3 \rangle \in \mathsf{BL}_3 \iff \langle G_1, G_2, G_3 \rangle \in \mathsf{coBL}_3.$$

a technical lemma: example



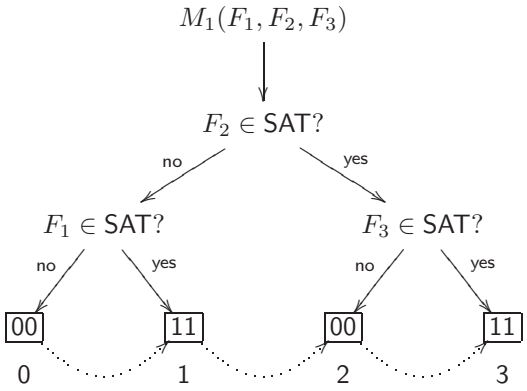
$\langle F_1, F_2, F_3 \rangle \in \mathsf{BL}_3 \iff$ true path has output 11

$\iff$ true path for M_2 has index 1 or 2

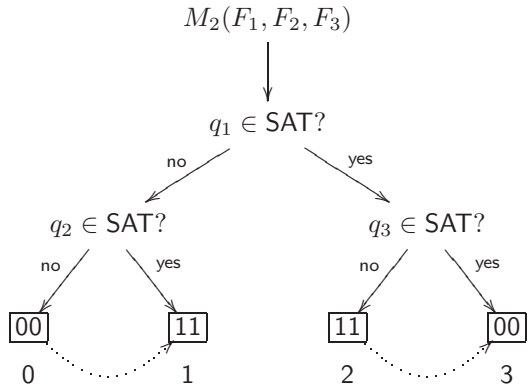
$\iff (q_1 \vee q_2) \in \mathsf{SAT}$ and $(q_1 \wedge q_3) \in \overline{\mathsf{SAT}}$

$\iff \langle \mathsf{TRUE}, (q_1 \vee q_2), (q_1 \wedge q_3) \rangle \in \mathsf{coBL}_3$

a technical lemma: details



3 mind changes



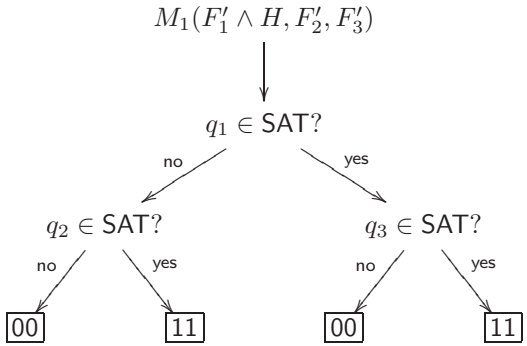
2 mind changes

- construct p_i s.t. $p_i \in$ SAT iff index of the true path $\geq i$.
- construct truth table for "M outputs 11 on the true path"
- number and type of mind changes determines if the truth table is reducible to BL_1, BL_2, BL_3, coBL_1, coBL_2 or coBL_3. [Wagner & Wechsung '85]

main theorem: strategy

- Input $\langle F_1, F_2, F_3 \rangle$, construct nested $\langle F_1', F_2', F_3' \rangle$.
- If $M(F_1', F_2', F_3')$ has output not $\langle 00, 11, 00, 11 \rangle$, we win.
- Get H from advice function. Advice says whether $H \in$ SAT.
- Case 1: $H \in$ SAT and $M(F_1' \wedge H, F_2', F_3')$ has output not $\langle 00, 11, 00, 11 \rangle$
  - $\langle F_1' \wedge H, F_2', F_3' \rangle$ is still nested, we win
- Case 2: $H \notin$ SAT and $M(F_1' \wedge H, F_2', F_3')$ has output $\langle 00, 11, 00, 11 \rangle$
  - 10 not in the output $\implies F_3 \notin$ SAT, we win
- Case 3: $M(F_1' \wedge H, F_2', F_3')$ has output $\langle 00, 11, 00, 11 \rangle \iff H \in$ SAT.
  - P/poly algorithm for SAT, we win

missing 10



$H \notin$ SAT and 10 not in the output

- $F_3 \in \mathsf{SAT} \implies F_3' \in \mathsf{SAT} \implies F_2' \in \mathsf{SAT} \implies F_1' \in \mathsf{SAT}$
- $F_3 \in \mathsf{SAT}$ and $H \notin \mathsf{SAT} \implies \mathcal{Q}_{32}(F_1' \wedge H, F_2', F_3') = 10$
- $F_3 \notin \mathsf{SAT} \implies (\langle F_1, F_2, F_3 \rangle \in \mathsf{BL}_3 \iff F_1 \in \mathsf{SAT}$ and $F_2 \notin \mathsf{SAT})$
- $\langle F_1, F_2, F_3 \rangle \in \mathsf{BL}_3 \iff \langle \mathsf{TRUE}, \mathsf{F}_1, \mathsf{F}_2 \rangle \in \mathsf{coBL}_3$

advice construction: advisees trick

- Use "advisees trick". [Amir, Beigel, Gasarch '90, '00 &'0?]
- Defn: H is an advisor for $\langle x_1, x_2, x_3 \rangle$ if
  - $H \in$ SAT and $M(x_1' \wedge H, x_2', x_3')$ has output not $\langle 00, 11, 00, 11 \rangle$ or
  - $H \notin$ SAT and $M(x_1' \wedge H, x_2', x_3')$ has output $\langle 00, 11, 00, 11 \rangle$.
- Let $\mathcal{A}(H)$ be the set of advisees of H among remaining triples $\langle x_1, x_2, x_3 \rangle$.
- Add H with most advisees to the advice string as long as $\mathcal{A}(H)$ contains at least $1/4$ of the remaining triples.
- After polynomial number of steps:
  - Either each $\langle x_1, x_2, x_3 \rangle$ has an advisor in the advice string
  - or we have a "BPP algorithm" for H not included in the advice string

putting it together: P/poly reduction from BL_3 to coBL_3

- Input $\langle F_1, F_2, F_3 \rangle$, construct nested $\langle F_1', F_2', F_3' \rangle$.
- If $M(F_1', F_2', F_3')$ has output not $\langle 00, 11, 00, 11 \rangle$, done.
- Check if there is an advisor H for $\langle F_1, F_2, F_3 \rangle$ in the advice string.
  - $H \in \mathsf{SAT} \implies M(F_1' \wedge H, F_2', F_3')$ has output not $\langle 00, 11, 00, 11 \rangle$.
  - $H \notin \mathsf{SAT} \implies M(F_1' \wedge H, F_2', F_3')$ has output missing 10.
- Otherwise:
  - check if any of F_1, F_2, F_3 is an advisor in the advice string.
  - Run P/poly algorithm for remaining F_i.
  - Know whether $F_1 \in \mathsf{SAT}$, $F_2 \in \mathsf{SAT}$ and $F_3 \in \mathsf{SAT}$.
  - Output trivial $\langle G_1, G_2, G_3 \rangle$.

extensions

- For all $k \geq 2$, $\mathrm{PF}_2^{\mathrm{SAT[k]}} = \mathrm{PF}_2^{\mathrm{SAT}\|[2^k-1]} \Longrightarrow \mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$
  - basically the same proof
  - need to generalize the technical lemma
- For all $j \geq 2$ and $k \geq 2$, $\mathrm{PF}_{\mathrm{j}}^{\mathrm{SAT[k]}} = \mathrm{PF}_{\mathrm{j}}^{\mathrm{SAT}\|[2^k-1]} \Longrightarrow \mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$
  - already known: [Amir, Beigel & Gasarch]

    $$\mathrm{PF}_{2^k-1}^{\mathrm{SAT[k]}} = \mathrm{PF}_{2^k-1}^{\mathrm{SAT}\|[2^k-1]} \Longrightarrow \text{ PH collapses.}$$

  - Fix $k \geq 2$. Then, for $j > 2$, show that

    $$\mathrm{PF}_{\mathrm{j}}^{\mathrm{SAT[k]}} = \mathrm{PF}_{\mathrm{j}}^{\mathrm{SAT}\|[2^k-1]} \Longrightarrow \mathrm{PF}_2^{\mathrm{SAT[k]}} = \mathrm{PF}_2^{\mathrm{SAT}\|[2^k-1]}$$

more extensions

- $\mathrm{PF}_2^{\mathrm{SAT}\|[6]} \subseteq \mathrm{PF}_2^{\mathrm{SAT}[3]} \Longrightarrow \mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$
  - already known: $\mathrm{PF}_2^{\mathrm{SAT}[3]} \subseteq \mathrm{PF}_2^{\mathrm{SAT}\|[6]} \Longrightarrow \mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$
  - in general: for all $j \geq 2$ and $k \geq 3$,

    $$\mathrm{PF}_{\mathrm{j}}^{\mathrm{SAT}\|[2^{\mathrm{k}}-2]} \subseteq \mathrm{PF}_{\mathrm{j}}^{\mathrm{SAT}[\mathrm{k}]} \Longrightarrow \mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}$$

- Most general theorem known so far:

  For all j, k and ℓ such that $1 < j \leq k < \ell \leq 2^k - 1$,

  if $2^k - (\ell + 1) < 2^j - 2$ and $2^k - (\ell + 1) < \ell - 1$, then

  $$\mathrm{PF}_{\mathrm{j}}^{\mathrm{SAT}\|[\ell]} \subseteq \mathrm{PF}_{\mathrm{j}}^{\mathrm{SAT}[\mathrm{k}]} \Longrightarrow \mathrm{PH} \subseteq \Sigma_3^{\mathrm{P}}.$$

conclusion & open problems

- Conclusion: 3 parallel queries to SAT more powerful than 2 serial queries, except for 1-bit functions (languages)
- Open Problem: $\mathsf{PF}_2^{\mathsf{SAT}\|[5]} \subseteq \mathsf{PF}_2^{\mathsf{SAT}[3]} \implies ???$
  - A $\mathsf{PF}_2^{\mathsf{SAT}[3]}$ machine can make 5 mind changes and output all four two-bit strings 00, 01, 10, 11.
- Open Problem: $\mathsf{PF}_3^{\mathsf{SAT}\|[4]} \subseteq \mathsf{PF}_3^{\mathsf{SAT}[3]} \implies ???$
  - A $\mathsf{PF}_3^{\mathsf{SAT}[3]}$ machine can make 4 mind changes and output 5 of the 8 three-bit strings in $\{0,1\}^3$.
  - Don't know how to take advantage of the 3 missing strings.