Chapter 3: The Tournament Divide and Conquer Technique

Narn - Saiful Islam, Hanjia (Bruce) Lyu, Katherine Seeman and Shreyan Goswami
April 4, 2022
1. Background

2. Semi-feasible sets have small circuits

3. Optimal advice for semi-feasible sets

4. A quick detour to tournament theory

5. Back to optimal advice for semi-feasible sets
Complexity class: $A/f$

- Throughout the presentation, we assume our alphabet to be $\Sigma = \{0, 1\}$
- For any set $A$ and any function $f$, $A/f$ denotes the class of all sets $L$ such that for some function $h$ satisfying $(\forall n)[|h(n)| = f(n)]$ it holds that

$$L = \{x|\langle x, h(|x|)\rangle \in A\}$$
A Boolean circuit is a directed acyclic graph with a node being either an input/output node or a logic gate.

Each vertex is either one of the following logic gates \{\text{AND, OR, NOT}\} or an input value.

There is a set of exactly $m$ ($m$ is an integer $\geq 1$) nodes labeled as the outputs.

**Figure 1:** Boolean circuit

Boolean circuits

- A special case of Boolean circuit is when there is a single output node.
- If a circuit has n-inputs it can decide a string $x$ of length $|x| = n$.
- The circuit will return 1 if the input string is in the language else 0.
- To decide a language $L$, you will need a family of circuits $\{C_1, C_2, \ldots\}$ where the $C_i$ can accept strings of length $i$.
- $x \in L \iff C_{|x|}$ accepts $x$. 
Advice strings

- Advice string is an extra input to a Turing Machine that is allowed to depend on the length of input $x$ but not on the input itself.
- Boolean circuits can be used as an advice string.
A decision problem is in the complexity class $P/f(n)$ if there is a deterministic polynomial-time Turing machine, $M$, with the following property:

- For any $x$, $|x| = n$, there is an advice string $A$, of length $f(n)$ such that for any input $x$ and $A$, $M$ correctly decides if $x$ belongs to the language.

- The definition we saw in the first slide matches the definition of $P/f(n)$.
Complexity class: P/poly (Small circuits)

- Informally, a language $L$ is in P/poly if $L$ requires “small advice” / “small circuits”
- $\exists$ a family of boolean circuits $C_1, C_2, \ldots$ and an integer $k$ such that
  \[ ||C_i|| \leq i^k + k \]
- Note: Size of circuit is dependent on the number of logic gates in that circuit
- Alternatively there exist a function $f$ such that the length of $f(1), f(2)\ldots$ is polynomially bounded
Complexity class: P-sel (Semi-feasible sets)

- P is the class of sets that have polynomial-time membership algorithms
- P-sel denotes the class of sets that have polynomial-time semi-membership algorithms
- A language L is P-sel if there is a polynomial-time 2-ary function $f$ such that for each $x$ and $y$ it holds
  1. $f(x, y) \in \{x, y\}$
  2. $\{x, y\} \cap L \neq \emptyset \Rightarrow f(x, y) \in L$
- $f$ is called a selector function, chooses one that is “more likely” if exactly one of the two inputs is in the set
1. Background

2. Semi-feasible sets have small circuits

3. Optimal advice for semi-feasible sets

4. A quick detour to tournament theory

5. Back to optimal advice for semi-feasible sets
Consider a k-node graph $G$, having no self-loops with $V_G$ as the vertex set and $E_G$ as the edge set.

For each pair of distinct nodes $\{a, b\}$ we have either a directed edge from $a$ to $b$ or vice versa.

Imagine this graph to be a round-robin tournament in which every node is a player.
A round robin tournament is a tournament in which each competitor plays in turn against every other competitor.

An edge between two players is directed towards whichever of the two won the match they played.

There are no ties.

Each player defeats themselves.
• Informally, in a k-tournament, there exists a small collection of players such that every player in the tournament defeats at least one member of that small collection

• **Theorem 3.1**: If $G$ is a $k$-tournament on nodes $V_G = \{1, 2, \ldots, k\}$ then there exists a set $H \subseteq V_G$ such that
  1. $|H| \leq \lceil \log(k + 1) \rceil$
  2. for each $v \in V_G - H$, there is some $g \in H$ such that $(g, v) \in E_G$
Proof of Theorem 3.1

- Each player plays $k - 1$ games
- The total number of wins equals the total number of losses
- There must be some player that loses at least half the time i.e. must lose at least $\left\lceil \frac{k-1}{2} \right\rceil$ games
- If this was not the case then each player individually has strictly more wins than losses
Proof of Theorem 3.1 (contd.)

- Add the player who loses at least half the games to set H
- Remove from consideration that player and all the players that defeat that player
- The new player set has at most $k - \left(1 + \left\lfloor \frac{k-1}{2} \right\rfloor \right) = \left\lfloor \frac{k}{2} \right\rfloor - 1$ players
- Consider the tournament by restricting to the edges in the old tournament between players of the reduced set
- Our argument is still valid in this new tournament
• At every step there will be a player who loses to at least half the other players in the reduced tournament, add that player to $H$ and reduce the tournament

• Eventually no vertices would be left and we would have our set $H$ having property 2 from the statement of the theorem.

• Recurrence relation $S(k) \leq 1 + S \left( \left\lceil \frac{k}{2} \right\rceil - 1 \right)$ for $k \geq 1$ and $S(0) = 0 \Rightarrow S(k) \leq \lfloor \log(k + 1) \rfloor$

• This concludes the proof for **Theorem 3.1**
• **Theorem 3.2** $P\text{-sel} \subseteq P/\text{poly}$

• **Proof outline**
  
  • At each length $n$ in any semi-feasible set $L$, denote $L^{\leq n}$ to be the strings of length $n$ in $L$
  
  • There will always exist a small set of strings in $L^{\leq n}$ such that every element in $L^{\leq n}$ defeats one of these strings, the winner decided by the selector function
  
  • This small set of nodes will be used as a ”small advice” set for $L$
  
  • Any string that defeats one of the strings in the advice string must be in $L$ (*important*)
Proof of Theorem 3.2

- Let $L$ be a semi-feasible set
- Consider the length $n$ strings in $L$ denoted by $L^{=n}$ and $f: \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ is a P-selector for $L$
- To prove $L \in P/poly$ we need to provide a function $g: \Sigma^* \rightarrow \Sigma^*$ and a set $A \in P$ such that

\[
(\forall x)[x \in L \iff \langle x, g(|x|) \rangle \in A] \quad (3.1)
\]

and $(\exists$ polynomial $q)(\forall n)[|g(n)| \leq q(n)]$
• WLOG $f(a, b) = f(b, a)$

• Consider a graph $G$ whose nodes are the elements of $L^n$, and such that for any $a, b \in L^n, a \neq b$, it holds that $(a, b) \in E_G \iff f(a, b) = b$

• This is indeed a tournament graph and the game is on
Consider a P-sel language $L$ and $f$ be a P-selector for $L$. Let $a, b, c, d \in L^n$. The figure on the right is the tournament induced on $a, b, c, d$ by $f$ such that

- $f(a, b) = b$
  equivalent: in a H2H match, $b$ beats $a$
- $f(b, c) = c$
- $f(c, a) = a$
- $f(a, d) = a$
- $f(b, d) = b$
- $f(d, c) = d$
• Applying **Theorem 3.1** to this tournament there exists $H_n$ such that $H_n$ contains only members of $L^n$

• **From property 2 of Theorem 3.1**, for every element $x \in L^n$ there is some element $g \in H_n$ satisfying $f(g, x) = x$

• If $x \in H_n$ then $f(x, x) = x$ is always true

• If $L$ contains no length $n$ elements, then $H_n = \emptyset$
• The advice function, $g(n)$, outputs $H_n$
• For each $n$, $H_n$ has at most $n + 1$ elements and each $n$ bits long, hence $H_n$ is polynomially long
• We now define the machine that will interpret this advice
• $A = \{ \langle x, y \rangle | \text{y is a (possibly empty) list of length n elements } v_1, \ldots v_z \text{ and for some } j \text{ it holds that } f(v_j, x) = x \}$
Concluding Theorem 3.2

- $A$ is in $P$ because $f$ is in $P$
- Does equation (3.1) hold?
- Let $x \in L$. Then $\langle x, g(|x|) \rangle \in A$
- Let $x \notin L$ and suppose $\langle x, g(|x|) \rangle \in A$
- Then for some $h_i \in H_n$ it must hold that $f(h_i, x) = x$.
- But the fact that $x$ has defeated some element in $L$ implies that $x \in L$ which contradicts the original assumption
- Therefore, if $x \notin L$ then $\langle x, g(|x|) \rangle \notin A$
- This proves $P\text{-sel} \subseteq P/\text{poly}$
Quick digression

- We have seen that potentially “small” advice string can help solve problems faster
- Finding these “small” pieces of advice string can be really difficult
- Set of primes is not known to be in P, but has small circuits
1. Background

2. Semi-feasible sets have small circuits

3. Optimal advice for semi-feasible sets

4. A quick detour to tournament theory

5. Back to optimal advice for semi-feasible sets
• P-sel \subseteq P/poly. What is this poly(nomial)?
• Can we say a bit more about the number of advice bits?
• Some useful notations
  □ Linear denotes the class of all functions $f$ such that $f(n) = O(n)$.
  □ Quadratic denote the class of all functions $f$ such that $f(n) = O(n^2)$. 
Theorem 3.5 \( \text{P-sel} \subseteq \text{P/quadratic} \)

Count the number of advice bits

- How many strings are in the advice function?
P-sel $\subseteq$ P/quadratic

**Theorem 3.5** P-sel $\subseteq$ P/quadratic

Count the number of advice bits

- How many strings are in the advice function? $(n + 1)$
- Length of each string?
Theorem 3.5 P-sel $\subseteq$ P/quadratic

Count the number of advice bits

- How many strings are in the advice function? $(n + 1)$
- Length of each string? $n$
- Number of bits needed to represent the advice function $= n \times (n + 1)$ which is $O(n^2)$

- Quadratic advice is sufficient for a P advice interpreter.
- Is linear advice sufficient (with more powerful advice interpreter)?
To determine membership (e.g., $x \in L$) we need

- A linear advice string $g(|x|)$
- An advice interpreter $A \in C$

Formally, if $L \in C/\text{linear}$,

- $(\forall x)[x \in L \iff \langle x, g(x) \rangle \in A]$ and
- $(\exists q \in \text{linear})(\forall n)[|g(n)| = q(n)]$
If $L \in \text{PP}$, there exists a PPTM such that

- for each $x \in L$ the machine accepts with Probability $\geq \frac{1}{2}$, and
- for each $x \not\in L$ the machine accepts with Probability $< \frac{1}{2}$.
Let $L \in \text{P-sel}$ and $f$ is the P-selector function. Without loss of generality, let $f(a, b) = f(b, a)$

- $f(a, b) = f'(\max(a, b), \min(a, b)) = f(b, a)$

Consider a tournament graph $G$ as in the Figure. $f(a, b) = a$ is analogous to “player a beating player b in the tournament”.

- $f(a, b) = f(b, a) = a$
- $f(b, c) = f(c, b) = c$
- $f(a, c) = f(c, a) = a$
Let $L \in \text{P-sel}$. For strings of length $n$, construct a (directed) tournament graph $G_n(V_{G_n}, E_{G_n})$.

- $V_{G_n} = \{x \mid x \in L^n\}$
- $E_{G_n} = \{(a, b) \mid a \in V_{G_n} \land b \in V_{G_n} \land f(a, b) = f(b, a) = b\}$

Our advice function will be the census function of $L$ at the given length, i.e., $g(n) = ||L^n||$, padded if needed with leading zeros so as to be exactly $n + 1$ bits long.
Number of bits of the advice string

- Advice string = number of vertices in the tournament graph
- \( g(n) = \|L^n\| = \|V_{G_n}\| = ? \)
Number of bits of the advice string

- Advice string = number of vertices in the tournament graph
- $g(n) = |L^n| = |V_{G_n}| = \sum 0 \leq g(n) \leq 2^n$
- $2^n + 1$ distinct values, $(n + 1)$ bits are sufficient
Moment of challenge

On input string $x$,

- $\|\{z|n = |z| \land f(x, z) = z\}\| = ?$
- Any relation to the census value $g(n)$?
- **RECAP:** $g(n) = \|L^n\|$
On input string $x$,

- $||\{z|n = |z| \land f(x, z) = z\}|| = ?$
- Any relation to the census value $g(n)$?

If $x \in L$,

- Only strings in $L$ (vertices of the tournament graph) can defeat $x$.
- Number of such strings $= g(n)$.
- $||\{z|n = |z| \land f(x, z) = z\}|| \leq g(n)$
\( L \in \text{P-sel} \Rightarrow L \in \text{PP/linear} \)

On input string \( x \),

- \(|\{z | n = |z| \land f(x, z) = z\}| = ?\)
- Any relation to the census value \( g(n) \)?

If \( x \not\in L \),

- All strings in \( L \) (vertices of the tournament graph) will surely defeat \( x \) (by definition of P-sel set, \( f(a, b) = a \) when \( a \in L \) and \( b \not\in L \)).
- \( x \) defeats itself.
- \(|\{z | n = |z| \land f(x, z) = z\}| > g(n)\)
On input string $x$,
If $x \in L$,
- $||\{z|n = |z| \land f(x, z) = z\}|| \leq g(n)$ is True

If $x \notin L$,
- $||\{z|n = |z| \land f(x, z) = z\}|| \leq g(n)$ is False

$x \in L \iff ||\{z|n = |z| \land f(x, z) = z\}|| \leq g(n)$
Let $A = \{\langle x, m \rangle | m \geq ||\{z|f(x, z) = z \land |x| = |z|}\}||\}$ where $m$ is interpreted as a binary representation of an integer.

If $A \in PP$ (and it is true indeed), then for any input $x$, we can simulate the PPTM for $A$ on input $\langle x, g(|x|) \rangle$ and accept/reject accordingly. Here, $g(|x|)$ is the advice string of size $(n + 1)$ bits.

The following condition for $L \in PP/linear$ is satisfied:

- $(\forall x)[x \in L \iff \langle x, g(x) \rangle \in A]$ and
- $(\exists q \in linear)(\forall n)[|g(n)| = q(n)]$

So $(\forall L \in P\text{-}sel)[L \in PP/linear]$
\( A \in \text{PP} \)

\[ A = \{ \langle x, m \rangle | m \geq \| \{ z | f(x, z) = z \land |x| = |z| \} \| \} \] where \( m \) is interpreted as a binary representation of an integer.

\( M \) is a PPTM for \( A \):

Here \( n = |x| \)
\[ A = \{ \langle x, m \rangle | m \geq \| \{ z | f(x, z) = z \land |x| = |z| \} \| \} \] where \( m \) is interpreted as a binary representation of an integer.

Let \( n = |x| \).
If \( \langle x, m \rangle \in A \), we have \( x \in L \) \[ \text{Prob}(M \text{ accepts } \langle x, m \rangle) \geq \frac{1}{2} \times \frac{(2^n - m)}{2^n} + \frac{1}{2} \times \frac{m}{2^n} \] \[ = \frac{1}{2} \]
\[ A = \{ \langle x, m \rangle | m \geq \| \{ z | f(x, z) = z \land |x| = |z| \} \| \} \] where \( m \) is interpreted as a binary representation of an integer.

Let \( n = |x| \).

If \( \langle x, m \rangle \notin A \), we have \( x \notin L \)

\[
\Pr(M \text{ rejects } \langle x, m \rangle) > \frac{1}{2} \times \frac{m}{2^n} + \frac{1}{2} \times \frac{(2^n - m)}{2^n} = \frac{1}{2}
\]

\[
\Pr(M \text{ accepts } \langle x, m \rangle) < \frac{1}{2}.
\]
1. Background

2. Semi-feasible sets have small circuits

3. Optimal advice for semi-feasible sets

4. A quick detour to tournament theory

5. Back to optimal advice for semi-feasible sets
PP is a very powerful class. $\text{PP} \supseteq \text{NP}$ and, within the flexibility of Turing reductions, PP contains the entire polynomial hierarchy. Can we do better?

Let's take a quick detour to some interesting results from the tournament theory.
\[ R_{i,G}(v) = R_{i-1,G} \cup \{ z \in V_G \mid (\exists w \in R_{i-1,G}(v))[ (w, z) \in E_G] \} \]
$R_{0,G}(\nu) = \{\nu\}$
$R_{1,G}(v)$
$R_{i,G}(S)$ versus $R_{i,G}(v)$
$R_{i,G}(S)$ versus $R_{i,G}(v)$
$R_{i,G}(S)$ versus $R_{i,G}(v)$
\[ V_G = R_{1,G}(H) \]
$V_G = R_{1,G}(H)$
\[ V_G = R_{1,G}(H) \]
\( V_G = R_{1,G}(H) \)
$V_G = R_{1,G}(H)$
$V_G = R_{1,G}(H)$
\[ V_G = R_{1,G}(H) \]
$V_G = R_{1,G}(H)$
\( V_G = R_{1,G}(H) \)
\[ V_G = R_{1,G}(H) \]
$V_G = R_{1,G}(H)$
Is there a node that can reach all the other nodes in a $k$-tournament? If yes, how many steps does it need to take to reach the “furthest” node?
In a k-tournament, $V_G = R_{k-1,G}(v)$
In a k-tournament, $V_G = R_{k-1,G}(v)$
In a $k$-tournament, $V_G = R_{k-1, G}(v)$
In a $k$-tournament, $V_G = R_{k-1,G}(v)$
In a k-tournament, \( V_G = R_{k-1,G}(v) \)
In a k-tournament, $V_G = R_{k-1,G}(v)$
In a k-tournament, \( V_G = R_{k-1,G}(v) \)
In a $k$-tournament, $V_G = R_{k-1,G}(v)$
$k - 1$ is still too large. Can we push the limit?
In a k-tournament, $V_G = R_{2,G}(v)$
In a k-tournament, \( V_G = R_{2,G}(v) \)
In a k-tournament, $V_G = R_{2,G}(v)$
In a k-tournament, $V_G = R_{2,G}(v)$
In a k-tournament, $V_G = R_{2,G}(v)$
In a k-tournament, $V_G = R_{2,G}(v)$
In a k-tournament, \( V_G = R_{2,G}(v) \)
In a k-tournament, $V_G = R_{2,G}(v)$
In a k-tournament, $V_G = R_{2,G}(v)$
In a k-tournament, $V_G = R_{2,G}(v)$
In a k-tournament, \( V_G = R_{2,G}(v) \)
In a k-tournament, $V_G = R_{2,G}(v)$
In a k-tournament, $V_G = R_{2,G}(v)$
In a $k$-tournament, $V_G = R_{2,G}(v)$
In a k-tournament, $V_G = R_{2,G}(v)$
In a k-tournament, $V_G = R_{2,G}(v)$
1. Background

2. Semi-feasible sets have small circuits

3. Optimal advice for semi-feasible sets

4. A quick detour to tournament theory

5. Back to optimal advice for semi-feasible sets
Recap - The class of P-sel and interesting results

- P-sel denotes the class of sets that have polynomial-time semi membership algorithms
- $P\text{-sel} \subseteq P/quadratic$
- $P\text{-sel} \subseteq PP/linear$
  However, the entire polynomial time hierarchy is contained in PP via Turing-reductions.

  *Can we do better?*
Recap - Graph Theory Results

- For any $L \in \text{P-sel}$ with selector function $f$, we can define a tournament $G$ where $(a, b) \in E_G \iff f(a, b) = b$.
- By Theorem 3.9, in any $k$-tournament, there exists a vertex which can reach any other vertex by a path of length 2.
**Recall:** \( L \in \text{NP/linear} \) if there is a linear advice string \( g(n) \) and an advice interpreter which decides \( A \in \text{NP} \) such that,

- \((\forall x)[x \in L \iff \langle x, g(|x|) \rangle \in A]\) and
- \((\exists q \in \text{linear})(\forall n)[|g(n)| = q(n)]\)
Theorem 3.10

Let \( L \in \text{P-sel} \) with selector function \( f \). Then \( L \in \text{NP/linear} \) with advice function

\[
g(n) = \begin{cases} 
1^{n+1} & L = \emptyset \\
0w_n & \text{else}
\end{cases}
\]
What is the magic string $w_n$?

We know that in any tournament, there exists a node which can reach every other node with a path of length at most two. Let $w_n$ be this string in the tournament induced on $L^n$ by $f$. 
... and advice interpreter which decides the set
\[ A = \{ \langle x, w_n \rangle \mid \text{there is a path of length at most two in the tournament induced on } L^{=n} \text{ by } f, \text{ from } x \text{ to } w_n \} \]
Proof of 3.10

Note $g(|x|)$ is linear and $A \in \text{NP}$.

Claim: For $L \in \text{P-sel}$, $x \in L \iff \langle x, w_n \rangle \in A$

- if $x \in L$ then $\langle x, g(|x|) \rangle \in A$ because we have selected $w_n$ such that $x$ can be reached from it via a path of length at most two by the tournament structure.
- if $x \notin L$, suppose $\langle x, g(|x|) \rangle \in A$. This means $x$ must defeat at most two strings, one of which is always $w_n$ and possibly another which itself defeats $w_n$. However we have chosen $w_n \in L$ so this is a contradiction. Thus $\langle x, g(|x|) \rangle \notin A$.

We have shown $\text{P-sel} \subseteq \text{NP/linear}$.
Claim: P-sel is closed under complementation.

Let $L \in \text{P-sel}$ with selector function $f$ and w.l.o.g. assume $f(a, b) = f(b, a)$. Then $\overline{L} \in \text{P-sel}$ with selector function

$$f'(a, b) = \begin{cases} b & \text{if } f(a, b) = a \\ a & \text{if } f(a, b) = b \end{cases}$$

The corollary immediately follows.
Corollary

Each semi-feasible set can be accepted with linear advice via a NP machine with linear non-determinism.

This NP machine works as follows:

- Check whether $x = w_n$ *path length is 0
- Check whether $f(x, w_n) = x$ *path length is 1
- Non-deterministically guess all strings $y$ of length $n$ and check whether $f(x, y) = x$ & $f(y, w_n) = y$ *path length is 2

Then we only require $n$ guess bits
Thank you