Given B_n, we can balance it to obtain B'_n whose corresponding circuit is of depth $O(\log(n))$.

Define the *size of a node* to be the size of the subtree rooted at that node.

Suppose that for every node N of size m in B_n the two subformulas beneath it are of size between $\frac{1}{3}m$ and $\frac{2}{3}m$.

Then, the depth is $\log(n)$, bec. if we start a traversal at the root, and choose any path, at each step we reduce the number of remaining nodes by (at least) $\frac{2}{3}$, so we get to any leaf in (at most) $O(\log_{\frac{3}{2}}(|B_n|)) = O(\log(|B_n|)) = O(\log(p(n))) = O(\log(n))$ steps.

So we have trouble if there is a “bad” N.

Suppose that N is a node such that one of its subformulas is of size greater than $\frac{2}{3}m$ where m is the size of the circuit rooted at N.

We follow a path starting at N: for as long as a node has a child of size $> \frac{2}{3}m$ we take this child (say we take the right one when we have a choice).

We stop at the first node where both children have size $< \frac{2}{3}m$.

This node x has size $> \frac{2}{3}m$ but both its children have size $< \frac{2}{3}m$.

$\therefore$ one of the two children of x must have size $> \frac{1}{3}m$.

Let this node be called M, so $\frac{1}{3}m <$ (size of M) $< \frac{2}{3}m$.

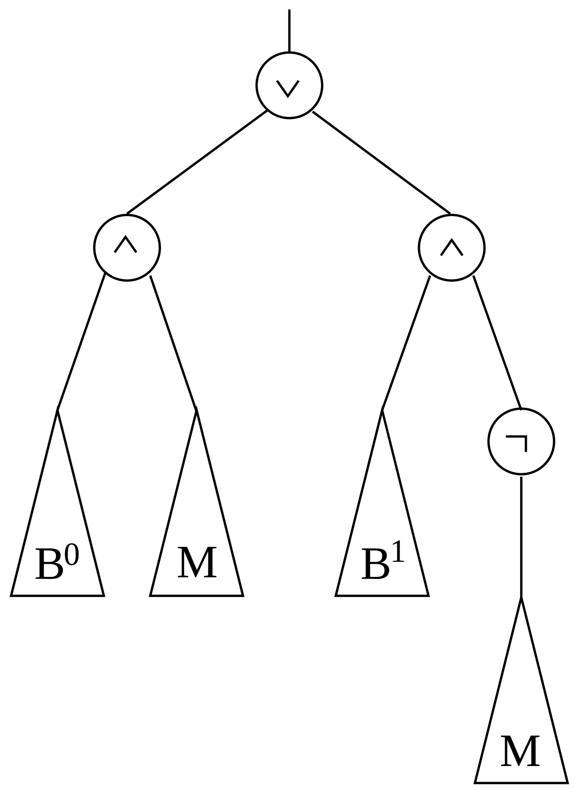
M is the spot where we are going to re-balance the subtree rooted at N.

(Note that by De Morgan we can assume that all negations come right after the inputs; i.e., we can "push" them to the inputs.)

Let B^0 be N where M is set to 0, and B^1 is N where M is set to 1.

We now replace the tree rooted at N with $(M \wedge B^0) \vee (\neg M \wedge B^1)$, where B^0, B^1, M are balanced recursively.

This produces a balanced N.



Boolean matrix multiplication

Input are two $m \times m$ matrices $A = \{a_{ij}\}, B = \{b_{ij}\}$. So there are $2m^2$ inputs and m^2 outputs: $C = \{c_{ij}\}$, where $c_{ij} = \bigvee_j (a_{ij} \wedge b_{jk})$.

The transitive closure of an $m \times m$ matrix A is:

$$A \vee A^2 \vee A^3 \vee \ldots \vee A^m$$

Property: if A is the adjacency matrix of a graph, then A^i has a 1 in position (j, k) iff there is a path of length i from j to k.

Thm: $\mathbf{NC}^1 \subseteq \mathbf{L}$.

Proof: Given w, construct $C_{|w|}$ in logspace; so the algorithm uses depth first search to evaluate the output gate, constructing the circuit as is necessary. We can remember the values of the gates on any path from the root to the leaves with logspace[a].

[a] Small problem: uniformity of the $\mathbf{NC}^i$ defined with logspace, but $\mathbf{NC}^1 \subseteq \mathbf{L}$.

Thm: $\mathbf{NL} \subseteq \mathbf{NC}^2$.

Proof: PATH is **NL**-complete, and PATH can be computed with transitive closure, which in turn can be computed in $\mathbf{NC}^2$.

Thm: $\mathbf{NC} \subseteq \mathbf{P}$.

We define **P**-completeness with logspace reductions.

CIRCUIT-VALUE is **P**-complete.

A **probabilistic TM** M is a type of nondet TM where each nondet step is called a **coin-flip step** and has two legal next moves.

Define the probability of a branch b to be $\Pr[b] = 2^{-k}$, where k is the number of coin-flips on b. Define the probability of acceptance as:

$$\Pr[M \text{ accepts } w] = \sum_{\substack{b \text{ is an accepting} \\ \text{branch}}} \Pr[b]$$

We let

$$\Pr[M \text{ rejects } w] = 1 - \Pr[M \text{ accepts } w]$$

For $0 \leq \varepsilon < \frac{1}{2}$ we say that M recognizes language A with error probability ε if

1. $w \in A$ implies $\Pr[M \text{ accepts } w] \geq 1 - \varepsilon$
2. $w \notin A$ implies $\Pr[M \text{ rejects } w] \geq 1 - \varepsilon$

BPP is the class of languages that are recognized by probabilistic polynomial time TMs with an error probability $\frac{1}{3}$.

Amplification Lemma: Let $0 < \varepsilon < \frac{1}{2}$. If M_1 is probabilistic polytime with error probability ε, then for any polynomial $q(n)$, $\exists M_2$, equivalent to M_1, but with error probability $O(2^{-q(n)})$.

Proof: Let M_2 on input w run M_1 on w $q(n)$ many times, and then take the majority vote. The error probability of M_2 follows from the *Chernoff bound*:

> Suppose that $x_1, \ldots, x_m$ are independent random variables taking the values 1 and 0 with probabilities p and $1 - p$, respectively, and consider their sum $X = \sum_{i=1}^{m} x_i$. Then, for $0 \leq \theta \leq 1$, $\Pr[X \geq (1 + \theta)pm] \leq e^{-\frac{\theta^2}{3}pm}$.

In other words, the probability that a *binomial random variable* (as X is called) deviates from its expectation decreases exponentially with the deviation.

In our case, take $x_i = \begin{cases} 1 & i\text{-th run gives } \textit{incorrect} \text{ answer} \\ 0 & \text{otherwise} \end{cases}$, $\theta = 0$, $p = \varepsilon$, and $m = \frac{1}{2p}q(n)$.

Thm: PRIMES $\in$ **BPP**.

Proof:

Consider the following **assertion**:

> *There is an L in* **EXPTIME** *and* $\varepsilon > 0$ *such that for every circuit family* C_n *deciding* L *and for all sufficiently large* n, $|C_n| > 2^{\varepsilon \cdot n}$.

We don't know if this assertion is true or not; however we know the following.

Thm: If the assertion is true, then $\mathbf{BPP} = \mathbf{P}$. If the assertion is false, then $\mathbf{P} \neq \mathbf{NP}$.

An **alternating TM** is a nondet TM with an additional feature: all states (except the accepting and rejecting) are divided into universal and existential states.

When we run an alternating TM, we label each node with $\wedge$ or $\vee$, depending on whether the corresponding configuration has a universal or existential state.

All children of $\wedge$ must be accepting, and at least one child of $\vee$ must be accepting.

We have ATIME($t(n)$) and ASPACE($f(n)$).

AP, APSPACE, AL are defined analogously.

Eg. TAUT $= \{\langle\phi\rangle | \phi$ is a tautology$\}$ is in **AP**.

Eg. MIN-FORMULA $= \{\langle\phi\rangle | \phi$ is a minimal Boolean formula$\}$ is in **AP**, but it is not known to be in **NP** or **coNP**. (Universally select a shorter ψ, existentially select an assignment, and deterministically evaluate ϕ, ψ under this assignment, and accept if they evaluate to different values.)

Thm: For $f(n) \geq n$ we have

$$\mathrm{ATIME}(f(n)) \overset{(1)}{\subseteq} \mathrm{SPACE}(f(n)) \overset{(2)}{\subseteq} \mathrm{ATIME}(f^2(n))$$

and for $f(n) \geq \log(n)$ we have

$$\mathrm{ASPACE}(f(n)) \overset{(3)}{=} \mathrm{TIME}(2^{O(f(n))})$$

Cor: $\mathbf{AL} = \mathbf{P}$, $\mathbf{AP} = \mathbf{PSPACE}$, $\mathbf{APSPACE} = \mathbf{EXPTIME}$.

Proof of (1): Depth first search of the alternating TM's computation tree, not recording configurations, but only the nondet choice (in base $b =$ degree of nondet).

Proof of (2): Given $c_{\text{init}}, c_{\text{accept}}$ of the det TM, the alternating TM branches existentially to guess a mid-point configuration c, and then branches universally to check that $c_{\text{init}} \rightsquigarrow c \rightsquigarrow c_{\text{accept}}$. The depth of the recursion is

$$\log(\text{nr. of config.}) = \log(2^{O(f(n))}) = O(f(n))$$

and at each step we require $O(f(n))$ space to write a configuration.

Proof (3) $\subseteq$: construct the entire computation tree ($2^{O(f(n))}$ many nodes), and mark accepting nodes: at first, only the accepting configurations are accepting nodes. Then, scan the graph repeatedly, and if a universal (existential) configuration is such that all (at least one) of its children are (is) accepting, mark it accepting.

Proof (3) $\supseteq$: In time $2^{O(f(n))}$, the computational tableau is of size $2^{O(f(n))} \times 2^{O(f(n))}$, so it cannot be stored in space $f(n)$. However, four pointers into the tableau can be stored:

s_1	s_2	s_3
	s	

When the first pointer is in s, existentially guess s_1, s_2, s_3, and universally check that they yield s.

In the first row, the answer can be verified directly since we know the input. We start the recursion in the lower-left corner.

A Σ_i**-alternating TM** is an alternating TM that contains at most i runs of universal or existential steps, starting with existential.

Π_i**-alternating TM** starts with a universal step.

Polynomial time hierarchy:

$\Sigma_i\mathbf{P} = \bigcup_k \Sigma_i\mathrm{TIME}(n^k)$ and

$\Pi_i\mathbf{P} = \bigcup_k \Pi_i\mathrm{TIME}(n^k)$ and

$\mathbf{PH} = \bigcup_i \Sigma_i\mathbf{P} = \bigcup_i \Pi_i\mathbf{P}$

Note that $\mathbf{NP} = \Sigma_1\mathbf{P}$ and $\mathbf{coNP} = \Pi_1\mathbf{P}$, and MIN-FORMULA is in $\Pi_2\mathbf{P}$.

It is also possible to express the **PH** as follows: suppose $L \in \Sigma_i\mathbf{P}$. Then, there exists a polytime relation R such that:

$$w \in L \iff \exists\bar{y}_1\forall\bar{y}_2 \dots Q\bar{y}_i R(w, \bar{y}_1, \bar{y_2}, \dots, \bar{y}_i)$$

here $\bar{z}$ denotes one or more variables. $\Pi_i\mathbf{P}$ can be defined analogously, but starting with $\forall$.

Thm: If $\mathbf{P} = \mathbf{NP}$, then **PH** *collapses* to the first level, i.e., $\mathbf{PH} = \mathbf{P}$.

Proof: It suffices to show that for any i, if $\Sigma_i\mathbf{P} = \Pi_i\mathbf{P}$, then $\Sigma_{i+1}\mathbf{P} = \Sigma_i\mathbf{P}$. This is easy to show.

Thus, it is not known if **PH** is a sequence of properly contained classes, but it is believed to be so.

Thm: $\mathrm{QSAT}_i = \{\langle\psi\rangle | \psi = \exists\bar{y}_1\forall\bar{y}_2 \dots Q\bar{y}_i\phi(\bar{x}, \bar{y}_1, \bar{y_2}, \dots, \bar{y}_i) \text{ is sat. }\}$. is $\Sigma_i\mathbf{P}$-complete.

Analogous to **PH** there is **AH**, the Arithmetical Hierarchy, where R is required to be recursive, and we talk of $\Sigma_i\mathbf{Rec}$ and $\Pi_i\mathbf{Rec}$.

Thm: For all i, $\Sigma_{i+1}\mathbf{Rec} \neq \Sigma_i\mathbf{Rec}$.

Proof: Consider $\Sigma_1\mathbf{Rec} = \mathbf{RE}$, and $\Sigma_0\mathbf{Rec} = \mathbf{Rec}$; they were separated by diagonalization; now generalize this argument to higher classes.