$f(n) = O(g(n)) \iff \exists c, n_0 \in \mathbb{Z}_+ : \forall n \geq n_0 f(n) \leq c \cdot g(n)$
$f(n) = \Theta(g(n)) \iff f(n) = O(g(n)) \wedge g(n) = O(f(n))$

**Cool-Karp Thesis**: Tractable = polynomial time - P
**Turing machine**:

- $M(x)\downarrow$ means $M(x)$ halts eventually
- $M(x)\downarrow q$ means $M(x)$ halts eventually in state q
- $M(x)\uparrow$ means $M(x)$ never halts

**Language L**: set of strings over a given alphabet $\Sigma$.
**Recursive L:** Let $M$ a DTM, $M$ *decides* $L$ if:

- $w \in L \Rightarrow M(x) \downarrow yes$
- $w \notin L \Rightarrow M(x) \downarrow no$

$\exists M \Rightarrow L$ recursive
**r.e L:** as above but $w \notin L \Rightarrow M(x) \uparrow$
$M$ *accepts* $L$ and $L$ is *recusively enumerable (r.e)*
$L$ recursive $\Rightarrow L$ r.e.
**Complementary L:** $\overline{L} = \Sigma - L$. $L$ co-r.e. $\iff \overline{L}$ r.e.
$L$ r.e. and co-r.e. $\Rightarrow L$ decidable by a 2-tape TM

**Time bounds**: DTM $M$ operates within time $f(n)$ if $\forall w, M(w)$ terminates in $\leq f(w)$ steps.
$L$ *decided* by multi-tape DTM operating within $f(n) \Rightarrow L \in$ TIME$(f(n))$
**Multi Tape DTM:** given any $k$-tape DTM $M$ operating in $f(n)$, can construct $M'$ operating in $O(f(n^2))$ s.t. $M \equiv M'$
**Church's Thesis:** Effective = DTM-computable
**Invariance Thesis:** All *reasonable* sequential models of computation have same time complexity as DTMs up to a polynomial.
$\mathbf{P} = \bigcup_k$ TIME$(n^k)$ (independent of choice of model by IT).

**NDTM:** degree of non-det = max possible branching.
NDTM $M$ accepts $w$ if $M$ can reach the accepting state *yes* on *some* computation on input $w$
$M$ *accepts* $L$ iff $L = \{w \in (\Sigma - \{B\}\}^* : M$ accepts $w\}$
$M$ operates within time $f(n)$ if $\forall w, M(w)$ has depth $\leq f(|w|)$
$M$ *decides* $L$ within time $f(n)$ if:

- $M$ operates within $f(n)$
- $M$ *decides* $L$

**Simulating NDTM:** $L$ decided by NDTM $M$ in time $f(n) \Rightarrow$ decided by DTM $M'$ in time $O(c^{f(n)})$. $c > 1$ const $\Rightarrow$NTIME$(f(n)) \subseteq \bigcup_{c>1}$ TIME$(c^{f(n)})$

**NP** $= \bigcup_k$NTIME$(n^k)$, where $L \in$ NTIME $f(n)$ iff $L$ is decided by some (ND)TM operating within time $f(n)$
NDTM can be simulated by DTM $\Rightarrow$ $L$ r.e iff $L$ *accepted* by some DTM iff $L$ *accepted* by some NDTM

**Halting problem:** $H = \{M; x : M(x)\downarrow\}$ is undecidable.
**Proper function:** $f(n)$ is proper iff

- $f$ non-decreasing
- $\exists k$-tape I/O TM, for input $x, |x| = n$, outputs $f(n)$1s and operates in time $O(n + f(n))$ and space $O(f(n))$

Let $H_f = \{M; x : M$ accepts $x$ after $\leq f(n)$steps $\}$
$H_f \in$ TIME$(f(n)^3)$, $H_f \notin$ TIME$(f(\lfloor \frac{n}{2} \rfloor)) \Rightarrow$
**THT:** TIME$(f(\lfloor \frac{n}{2} \rfloor)) \subsetneq$ TIME$(f(n)^3)$ $\Rightarrow$TIME$(f(n)) \subsetneq$ TIME$(f(2n+1)^3) \Rightarrow P \subsetneq EXP := \bigcup_k$ TIME$(2^{n^k})$

**Balanced relations:** $R \subseteq \Sigma^* \times \Sigma^*$ is *polynomially balanced* if $\exists k \geq 1$ s.t. $(x, y) \in R \Rightarrow |y| \leq |x|^k$
$L \subseteq \Sigma^*, L \in NP$ iff $\exists$ *poly deciable, poly balanced* relation $R$ s.t. $L = \{x : (x, y) \in R$ for some y$\}$.

**Reduction:** $L_1 \leq_{Karp} L_2$ iff $\exists f \in P : x \in L_1$iff$f(x) \in L_2$
$L_1 \leq_{Cook} L_2$ iff in $x \in^? L_1$ we use a p-time algorithm that queries an *oracle* about $y \in^? L_2$ polynomially many times.
$L_1 \leq_K L_2$, $L_2 \in P/NP \Rightarrow L_1 \in P/NP$. $\leq$ transitive

**NP-hard:** $\forall L' \in NP, L' \leq L \Rightarrow L \in$ NP-hard
$L \in$ NP-hard $\wedge L \in NP \Rightarrow L \in$ NP-complete (NPC)
$L' \in$ NPC $\wedge$Ł $\in NP \leq L' \Rightarrow L \in NPC$

**NPI:**$D \in$ NP $\wedge D \notin$ P, NPC $\Rightarrow D \in$ NP-intermediate
P $\neq$ NP $\iff \exists D \in$ NPI

**Strongly NPC:** if $D \in$ NPC even when all parameters bounded by a polynomial in the length of the input

**Approximation algorithm:** for a min problem is $k$-optimal if it guarantees a solution not worse than $k\times$ optimal solution. TSP inapproximable but MTSP $d(A, C) \leq d(A, B) + d(B, C)$ is
**Vertex cover:** $U \subseteq nodes(G) : \forall (u, v) \in edges(G), u \in U \vee v \in U$
$VC(D)$: Given $G$ and $k, \exists U$ s.t. $|U| \leq k$ vertex cover? $\in$ NPC

**I/O k-tape TM:** read only input tape, $k - 2$ work tapes, write only output tape (k $\geq$ 2). Operates within $f(n)$ space if on every input size $|n|$ uses $\leq f(n)$ squares of each work tape
$L \in$(N)PSPACE$(f(n))$ if $L$ *decided* by I/O (N)DTM operating within space $f(n)$
(N)LOGSPACE = (N)SPACE$(\log(n)) := NL$
(N)PSPACE $= \bigcup_k$(N)SPACE$(n^k)$
TIME$(f(n)) \subseteq$ SPACE$(f(n))$
For proper f:

1. (N)TIME$(f(n)) \subseteq$ SPACE$(f(n)) \Rightarrow$ NP $\subseteq$ PSPACE
2. NSPACE$(f(n)) \subseteq$ TIME$(k^{\log(n)+f(n)}) \Rightarrow$ NL $\subseteq$ P
3. $f(n) \geq \log(n)$ : NSPACE$(f(n)) \subseteq$ SPACE $(f^2(n))$

(3) letting $f(n) = p(n) \Rightarrow$ NPSPACE = PSPACE ($\supseteq$ trivial)

**Savitch's Theorem:** RCH $\in$ SPACE$(\log^2(n))$ - used in (3) above

**Hierarchy thm:** $f = o(g) \Rightarrow \forall \epsilon > 0, \exists N : \forall n \geq N, f(n) \leq \epsilon g(n)$
$f, g$ proper $f = o(g) \Rightarrow$ (N)SPACE$(f(n)) \subsetneq$ (N)SPACE$(g(n))$
$\Rightarrow$ NL $\subsetneq$ NPSPACE = PSPACE (let $f(n) = \log n$ above)

**Space summary:** L $\subseteq$ NL $\subseteq$ P $\subseteq$ NP $\subseteq$ PSPACE (all $\subseteq$ conjectured $\subsetneq$ + know NL $\subsetneq$ PSPACE so one has to be proper)

**Complementary Problem:** $\overline{P}$ to P: $\forall x, P(x) \iff \neg\overline{P}(x)$
Language $L \subseteq \Sigma^* \Rightarrow \overline{L} = \Sigma^* - L$. $\overline{L} \in \mathcal{C} \Rightarrow$ L $\in$ co-$\mathcal{C}$
co-TIME/SPACE$(f(n))$ = TIME/SPACE$(f(n))$ (swap yes/no)
L $\leq$ L' $\Rightarrow \overline{L} \leq \overline{L'}$ and L' $\in$ co-NP $\Rightarrow L \in$ co-NP
Believed co-NP $\neq$ NP $\equiv$ NPC $\cap$ co-NP $= \emptyset \Rightarrow P \neq NP$
$f(n) \geq \log(n)$: co-NSPACE$(f(n))$=NSPACE$(f(n)) \Rightarrow$ co-NL=NL

**SI Thm:** directed $G, x \in G$, $|N(x)| \in$ NL (# nodes rch. from $x$)
$\exists$ NDTM $M : M$ *identifies* $N(x)$ - is a successful comp examining all $y \in G$, indicating whether $y \in N(x)$ (last step of prf above)

**Logspace red:** $L \leq_{log} L'$ iff $\exists f \in$ LOGSPACE: $x \in L$ iff $f(x) \in L'$
$\leq_{karp}$: $L, L' \in P \Rightarrow L \sim L'$, but meaningful PC and NLC by $\leq_{log}$
RCH is NLC (map $L$ to RCH on configuration graph of NDTM)
$\exists x_1 \forall x_2 \ldots \phi(x_1, \ldots, x_n) = tt :=$ QBF $\in$ PSPACE-complete

**Oracle Machine:** $M^{M'}$ in *deciding* $L$ uses an oracle $M'$
$P^L := \{L' : L'$ decidable in p-time using an oracle for $L\}$
NP, co-NP $\subseteq P^{NP} \subseteq$ PSPACE
**Polynomial Hierarchy:** $\Delta_0^P = \Sigma_0^P = \prod_0^P = P$
$\Delta_{n+1}^P = P^{\Sigma_n^P}$, $\Sigma_{n+1}^P = \text{NP}^{\Sigma_n^P}$, $\prod_{n+1}^P = \text{co-NP}^{\Sigma_n^P}$
P-oracle pointless $\Rightarrow \Delta_1^P = P$, $\Sigma_1^P =$ NP, $\prod_0^P =$ co-NP
$\Sigma_n^P \subseteq \Delta_{n+1}^P \subseteq \Sigma_{n+1}^P$, $\prod_n^P \subseteq \Delta_{n+1}^P \subseteq \prod_{n+1}^P$
**Logical characterisation:** $L \in \Sigma_i^P$ (i $\geq$ 1) iff $\exists$ *p-balanced* $R : L = \{x : \exists y R(x, y)\}$ and$\{x; y : (x, y) \in R\} \in \prod_{i-1}^P$
p-balanced: $R(x, y_1, \ldots, y_i) \Rightarrow |y_1|, \ldots, |y_i| \leq |x|^k$ for some $k$
$\equiv L \in \Sigma_i^P$ iff $\exists R$ p-balanced, p-decidable:
$L = \{x : \exists y_1 \forall y_2 \ldots R(x, y_1, \ldots, y_i)\}$ ($\forall$ for i even, $\exists$ for i odd)
$\exists \vec{x}_1 \forall \vec{x}_2 \ldots \phi(\vec{x}_1, \ldots, \vec{x}_n) = tt :=$ QBF$_n \in \Sigma_n^P$-complete
$\forall P \in$ PH, $P \leq$QBF$_n \leq$ QBF $\in$ PSPACE $\Rightarrow$ PH $\subseteq$ PSPACE

**Parallel algo:** p-time + poly processors $\Rightarrow$ p-time sequential algo
Addition parallelised with knockout $\Rightarrow O(\log(n))$
**Brent's Principle:** $W$ work and parallel time $T \Rightarrow \frac{W}{T}$ processors

**Boolean Circuits:** size = |gates|, depth = length of longest path
Made up of: tt, ff, $\neg, \wedge, \vee$
**CV:** given a variable-free circuit ($x_i \to$ tt/ff), determine its output
**Poly Circuits**: $L \subseteq \{0, 1\}^*$ has PCs if $\exists \mathcal{C} = \{\mathcal{C}_n : n = 0, 1, \ldots\}$:

1. $\exists p$ poly: $\forall n, |\mathcal{C}_n \leq p(n)|$
2. $\forall x \in \{0, 1\}^n, x \in L \iff \mathcal{C}_n(x) = tt$

$L \subseteq \{0, 1\}^* \in P \Rightarrow L$ has PCs ($\forall L \in P, L \leq_{log}$ CV - CV $\in P$-c)
Converse is <u>not</u> true (undecidable $L$ can have PCs)
**Uniform circuits:** $\mathcal{C}_n$ uniform if $\exists$ log-space bounded TM which given input $1^n$ returns the code of $\mathcal{C}_n$ (avoids cases like above)
$L \subseteq \{0, 1\}^* \in P \iff L$ has uniform PCs ($\forall L \in P, L \leq_{log}$ CV - CV $\in P$-c)
P $\neq$ NP $\Rightarrow$ NPC problems do not have uniform poly circuits

**P/poly**: suppose DTM $M$ has extra read-only input $A(n)$
M *decides* L *with advice* $A(n)$ if:

- $x \in L \Rightarrow M(x, A(|x|)) \downarrow yes$
- $x \notin L \Rightarrow M(x, A(|x|)) \downarrow no$

$L \in$ P/poly if decided by such a DTM in p-time and $\forall n, |A(n)| \leq$ some poly $p(n)$
$L \in$ P/poly iff $L$ has polynomial circuits $\Rightarrow P \subseteq$ P/poly

---

depth($\mathcal{C}_n$) $\leq f(n) \Rightarrow$ parallel time (PT) of $\mathcal{C}_n \leq f(n)$
size($\mathcal{C}_n$) $\leq g(n) \Rightarrow$ total work (TW) of $\mathcal{C}_n \leq g(n)$
**PT/WK**$(f(n), g(n)) \ni L \subseteq \{0,1\}^*$ iff $\exists$ uniform $\mathcal{C}$ deciding $L$ with $O(f(n))$ PT and $O(g(n))$ TW

---

**NC**:$= \bigcup_k$ PT/WK$(\log^k n, n^k)$
**NC**$_j := \bigcup_k$ PT/WK$(\log^j n, n^k)$
NC $\subseteq$ P, just map poly circuit to CV, NL $\subseteq$ NC$_2$
$L \in$ NC, $L' \leq_{log} L \Rightarrow L' \in$ NC (NC closed under reduction)
NC $\neq$ P $\Rightarrow$ [$L \in$ P-complete $\Rightarrow L \notin$ NC] (P-c cannot be efficiently parallelised)
NC$_1 \subseteq$ NC$_2 \subseteq \ldots \subseteq$ NC, collapses if NC-complete $\neq \emptyset$

---

$f, g \in$ LOGSPACE $\Rightarrow f \circ g \in$ LOGSPACE
**Borodin's Theorem**: NC$_1 \subseteq$ LOGSPACE
NC$_1 \subseteq$ L $\subseteq$ NL $\subseteq$ NC$_2$ $\Rightarrow$**PCT**: *PT poly related to seq space*

---

**Primes:** if $n$ composite, its factors serve as *witnesses*
PRIME $\in$ NP: guess $r < p$, check $r$ primitive root (p-time):

- $r^{p-1} = 1 \mod p$
- $\forall q : q$ prime $, q|(p-1), r^{\frac{p-1}{q}} \neq 1 \mod p$

$p$ prime iff $\exists r$ so $s$ is a witness to $p$'s primality
+ have to check $q$s are prime, but procedure is p-time
**Fermat witness:** $p$ prime $\Rightarrow \forall 0 < a < p, a^{p-1} = 1 \mod p$
$\exists 0 < a < n : a^{n-1} \neq 1 \mod n \Rightarrow n$ comp ($a$ fermat witness)
**Probabilistic computation:** pick $a$ at random, $n$ composite iff $a$ fermat witness (FW)
**Carmichael number**: composite $c > 0 : \forall a$ FW of $c$, coprime$(a, c)$ - no easier to guess a FW than factor
**Riemann witness (RW)**: $n = 1 + m \cdot 2^k, a < n, a^m \neq 1 \mod n \wedge \forall i = 0, 1, \ldots k-1$ $a^{m \cdot 2^i} \neq -1 \mod n \Rightarrow$ n comp
$n$ composite $\Rightarrow n$ has $\geq \frac{3n}{4}$ witnesses (F or R)
**Rabin's primality algo**: pick $0 < a < n$ if $a$ witness $\Rightarrow$ composite, else *probably* prime - iterate to improve
PRIME $\in$ P, not known if $\in$ P-complete or NC

---

**Monte Carlo algorithm**: for language $L$, probabilistic s.t:

- $x \notin L$ returns *no*
- $x \in L$ returns *yes* with probability $> \frac{1}{2}$

**Precise**: (ND)TM M is precise if $\exists f(n)$ : M takes exactly $f(n)$ steps on input of length $n$. $M$ *decides* $L$ in time $f(n) \Rightarrow$ $\exists$ NDTM M' precise, $D = 2$, M' *decides* L in time $Of(n)$
**MC TM**: p-time precise NDTM $M_{D=2}$, s.t $\forall x, |x| = n$:

- $x \notin L \Rightarrow$ all computations fail
- $x \in L \Rightarrow > \varepsilon$ of $2^{p(n)}$ computations (leaves) succeed

$\varepsilon$ usually $= \frac{1}{2}$, can be $0 < \varepsilon \leq 1$ - iterate $m$ times to improve:
$x \notin L$ we always reject, $x \in L$ have $\varepsilon^m \to 0$ chance of error

---

**RP**: $L \in$ RP iff $L$ has p-time MCTM. P $\subseteq$ RP $\subseteq$ NP
**ZPP** = RP $\cap$ co-RP (L $\in$ ZPP has a Las-Vegas algorithm)
PRIME $\in$ RP, ZPP (and actually $\in$ P)
**BPP**: $L \in$ BPP if $\exists$ NDTM M:

- $x \in L \Rightarrow > \delta$ of computations (leaves) succeed
- $x \notin L \Rightarrow > \delta$ of computations (leaves) fail

$\delta$ usually $= \frac{3}{4}$, can be $\frac{1}{2} < \delta \leq 1$ - iterate $m$ times to improve
RP $\subseteq$ BPP = co-BPP $\subseteq \Sigma_2^P \cap \prod_2^P$

---

**Function problem:** e.g. FSAT: find satisfying assignment
$L \in$ NP iff L $= \{x : \exists y R_L(x, y)\}$ $R_L$ p-decidable, p-balanced
L $\to$ FL: given $x$ find $y : R_L(x, y)$ - return *no* if $\nexists y$
**FNP**: all such problems
**FP**: FL $\in$ FNP solvable in p-time, FNP = FP iff P = NP
**TFNP** $\ni$ R if $\forall x \exists y : (x, y) \in R$ (R total: know $\exists$ solution)
FP$^{\text{NP}}$ = function problems in FP with help of NPC oracle
TSP $\in$ FP$^{\text{NP}}$-complete

**Cryptography**: Encoding algorithm E, Encoding key e, Plain text x, Ciphertext $y = E(e, x)$, $x = D(d, y)$
**One time pad**: $x, y \in \{0,1\}^*, d = e$ arbitrary string $|e| = |d| = |x|$, $E(e, x) = x \oplus x, D(d, y) = d \oplus y = d \oplus E(e, x)$
**Public key:** $d$ private to receiver, $e$ public: $D(d, E(e, x)) = x$
Should be infeasible to deduce $d$ and $x$ without knowing $d$
Not unbreakable, guess $x$, check $E(e, x) = y$ ($\in$ FNP, $|x| \leq |y|^k$)
PK only if $FP \neq FNP \equiv P \neq NP$, even yet need poly $f$ that is *difficult* to invert
**One way function**: $f : \Sigma^* \to \Sigma^*$

- $f$ 1-1 and $\forall x \exists k : |x|^{\frac{1}{k}} \leq |f(x)| \leq |x|^k$
- f $\in$ FP and $f^{-1} \notin FP$

Candidates:

- $f_{MULT}(p, q)$ check p, q prime in p-time, if not ret input (1-1)
- $f_{EXP}(p, \vec{q}, r, x) = (p, \vec{q}, r^x \mod p)$ check p prime in p-time, r primitive root of p ($r$ needs $\vec{q}$, not believed findable in p-time)

Both have no known p-time inversion algorithms

---

**Coprime**: $m, n$ if HCF = 1
Let $p, q$ prime, coprime$(e, \phi(pq))$, $\phi(pq) = pq - p - q + 1$, $x < pq$
(*Euler* $\phi(n) = \#m : 1 \leq m < n$ HCF(m, n) = 1)
$f_{RSA}(x, e, p, q) = (x^e \mod pq, pq, e)$, ret input if any *lets* broken
N.B: reveals $e, pq$ but not $p, q$ or $\phi(pq)$
**RSA PK:** public: $pq, e$, private: $pq, d$ (e.g. $e$ v large prime)
coprime$(a, n) \Rightarrow a^{\phi(n)} = 1 \mod n$
**Trapdoor** $f$: one-way $f$:

- can efficiently sample domain
- there is a poly function $d$ of the input that trivialises the inverse problem

$f_{RSA}$:easy to find primes, with $d = e^{-1} \mod \phi(pq)$ easy to invert

---

**UP**: *unambigious* NDTMS ($\forall x \exists \leq 1$ accepting computation)
P $\subseteq$ UP $\subseteq$ NP, one-way $f$ iff P $\neq$ UP

---

**Zero knowledge proofs:** every NPC problem has one

---

**Things to look out for**:
In composition questions always mention bounds on i/o sizes!
Hamiltonian Circuit: visits every vertex exactly once, no repeats
Don't be afraid to construct a new NP problem to use as oracle
Removing method doesn't always work for uniqueness check
For uniqueness, define another NP problem an use oracle
Cannot bank on a 'no' of an NDTM, only 'yes'
$A \subseteq B \Rightarrow$ co-A $\subseteq$ co-B
Use a counter in NDTM for NL to not go on forever
NC$_1 \subseteq$ L $\subseteq$ NL $\subseteq$ NC$_2 \subseteq$ NC $\subseteq$ P
$A$ adj matrix, $A^k$ nodes reachable in exactly $k$
$(A + I)^k$ nodes reachable in $\leq k$ (binomial expansion)
Can play around, $(A^2 + 1)^k$ is even, $A(A^2 + 1)^k$ is odd
FNP $\subseteq FP^{NP}$
$P^{P^{NP}} = P^{NP}$
(co-NP)-complete = co-NPC
Good luck bruddas, if in doubt, $P = NP$