NC

- **Definition:** By uniformity, we mean the circuit family $\{C_n\}$ that computes functions $\{\chi_{n,A}\}$ can be generated by a DTM in log space.
- **Definition:** Language A is in the class *nonuniform-*NC^i if there is a poly $p(n)$ and a constant k s.t. $\chi_{n,A}$ can be computed by a circuit C_n with (1) Gates in C_n has fanin 2. (2) C_n has depth $k(\log n)^i$. (3) The size of C_n is at most $p(n)$. If the gates have unbounded fanin, then we say A is in *nonuniform-*AC^i.

- Fact : $NC^i \subseteq AC^i \subseteq NC^{i+1}$.
- **Def:** *nonuniform*-$NC = \cup_{i \geq 0} NC^i$, $AC = \cup_{i \geq 0} AC^i$.
- **Eg.** The parity function of n variables is in NC^1. Why?
- **Eg.** Let X, Y be two boolean matrices of size $n \times n$. The product of X and Y is defined as $(XY)_{i,j}$ = $\vee_{k=1}^{n}(x_{i,k} \wedge y_{k,j})$. This problem is in AC^0, why?
- **Eg.** Given a directed graph and two vertices s and t, is there a path from s ot t? This problem is NL-complete. Why is this problem also in NC^2?
- **Thm:**(a) $NC \subseteq P$. (b) $NC^i \subseteq DSPACE((\log n)^i)$. (c) $NC^1 \subseteq L \subseteq NL \subseteq NC^2$. (d) $AC^0 \neq NC^1$.

P =? NC

- **Def:** A language B is said to be P-complete if it belongs to P and $\forall A \in P$ is log space reducible to B.
- **Def:**Circuit Value Problem (CVP): Given a circuit C and an assignment τ to its variables, determine whether the circuit value $C|_\tau$ equals 1.
- **Thm:** CVP is P-complete.
- Monotone Circuit Value (MCV): Same as CVP but with monotone circuit.
- Planar Circuit Value (MCV): Same as CVP but with plannar circuit.
- Odd Maximum Flow (OMF): Given a flow network, determine whether the max flow is an odd number.

Random Circuit and RNC

- A random circuit $C(x_1, \cdots, x_n, y_1, \cdots, y_m)$ is a circuit with regular input x and random input y, where each random input bit y_i can 0 or 1 with equal probability.
- Let a and b be two numbers satisfying $0 \leq a < b \leq 1$. A language $A \subseteq \{0,1\}^n$ is (a,b)-accepted by a random circuit $C(x,y)$ with n input variables if for all $x \in A$, we have $Pr[C(x,y) = 1] \geq b$ and for $x \in \{0,1\}^n - A$, we have $Pr[C(x,y) = 1] \leq a$.
- A language is in RNC, if there is a uniform family of NC circuits, with poly many random bits, that $(0, 1/2)$-accepts the language. It is clear that $NC \subseteq RNC$.
- $NC \subseteq P$ and $RNC \subseteq R$. But it is not clear that whether $RNC \subseteq P$.

RNC

- Perfect Matching: Given a bipartite graph $G = (A, B, E)$ with vertex set $A = \{u_1, \cdots, u_n\}$ and $B = \{v_1, \cdots, v_n\}$, determine G has a perfect matching or not.
- Isolation Lemma:(Mulmuley, Vazirani, Vazirani, 1987, Combinatorica) Let $S = \{x_1, \cdots, x_n\}$ with a weight w_i for each x_i, where each w_i is randomly chosen from 1 to $2n$. Let $\mathcal{F}$ be a family of subsets of S. For each set $T \in \mathcal{F}$, its weight is the total weight of elements in T. *Then with probability at least 1/2, there is a unique minimum-weight set T in $\mathcal{F}$.*

Proof of Isolation Lemma

- Call an element $x \in S$ bad if it is in some minimum weight subset but not all of them. A bad element exists iff the minimum-weight subset is NOT unique. What is the probability that an element is bad?
- Suppose all elements are set except x. Let U be the smallest total weight among all sets in F not containing x. Let W be the smallest total weight among all sets in F containing x. For the moment the weight of x is not decided yet. What happen if $W \geq U$?
- For $U - W > 0$: If x is set to be $U - W$, then x is bad, since the minimum weight is not unique. The probability is at most $1/2n$. Why? Thus there exists a bad element with probability at most $n \times 1/2n$=1/2. Thus,Prob[there is a unique minimum-weight set T in $\mathcal{F}$] $\geq 1/2$.

Theorem: Perfect matching in RNC

- Randomly assign weights from 1 to $2|E|$ to the edges in the bipartite graphs. Let w_{ij} be the weight on edge (u_i, v_j).
- Define the matrix A with $A[i,j] = 2^{w_{ij}}$. Note that $A[i,j] = 0$ if $(u_i, v_j) \notin E$.
- Compute $det(A) = \sum_\pi \sigma(\pi)\Pi_{i=1}^n A[i, \pi(i)]$.
- If the minimum weight perfect matching is unique, say W, then $det(A) = (2k+1)2^W$, for some integer K. Why? In other words, if G has no perfect matching then $Prob[det(A) \neq 0] = 0$, and G has one PM then $Prob[det(A) \neq 0] \geq 1/2$
- Compute $det(A)$ in in NC^2.