# Parallel Computation classes NC \& RNC, 

Algorithms and Complexity II
6/3/2014
Galenianou Myrto

## Until now

- Sequential computations
- Bounded amount of computational activity at each instant
-TM
-multistring TM
- RAM
- Exception : NDTM


# Parallel models of computation -Uniform family of circuits 

- A Boolean circuit C is defined as a finite directed acyclic graph.
- Each vertex corresponds to a gate
- The size of $C$ is the total number of gates
- The depth of $C$ is the total number of nodes in the longest path in C


## Parallel models of computation -Uniform family of circuits

- A uniform family of boolean circuits is a family of circuits $\mathrm{C}=\left(\mathrm{C}_{1}, C_{2}, \ldots\right)$ where all circuits in the family are connected to the same algorithmic idea
- For functions $f(n), g(n): \mathrm{N} \rightarrow \mathrm{N}$
- The parallel time of C is $O(f(n))$
- The total work of $C$ is $O(g(n))$


## Parallel models of computation -Uniform family of circuits

- def. Class PT/WK(f(n), $g(n))$ : the class of all languages $L \subseteq\{0,1\}^{*}$ such that there is a uniform family of circuits $C$ deciding $L$ with $\mathrm{O}(\mathrm{f}(\mathrm{n}))$ parallel time and $\mathrm{O}(\mathrm{g}(\mathrm{n}))$ total work


## Parallel models of computation -Parallel Random Access Machines

- A RAM program is a finite sequence $\Pi=\left(\pi_{1}, \pi_{2}, \ldots, \pi_{m}\right)$ of instructions that edit memory cells
- A PRAM is a sequence of RAMs $P=\left(\Pi_{1}, \Pi_{2}, \ldots, \Pi_{q}\right)$

■ Each RAM program works in parallel with the others

- $q$ is a function; $q=q(m, n)$, where $m$ is the number of integers in the input and $n$ the total length of the integers


## Parallel models of computation -Parallel Random Access Machines

■ Uniform family $\quad P=\left(P_{m, n}: m, n \geq 0\right)$

- function F mapping finite sequences of integers to finite sequences of integers
- Then $P$ computes $F$ in parallel time $f(n)$, using $\mathrm{g}(\mathrm{n})$ processors.

■ TH: If $L \subseteq\{0,1\}^{*}$ is in $\operatorname{PT} / \mathrm{NK}(f(n), g(n))$, then there is a uniform PRAM that computes the corresponding function $F$ mapping $\{0,1\}^{*}$ to $\{0,1\}$ in parallel time $\mathrm{O}(\mathrm{f}(\mathrm{n})$ ), using $O\left(\frac{g(n)}{f(n)}\right)$ processors.

- TH : Suppose that a function $F$ can be computed by a uniform PRAM in parallel time $f(n)$ with $g(n)$ processors, where $f(n)$ and $g(n)$ can be computed from $1^{n}$ in logarithmic space. Then there is a uniform family of circuits of depth $\mathrm{O}(\mathrm{f}(\mathrm{n})(\mathrm{f}(\mathrm{n})+\operatorname{logn})$ and size
$O\left(g(n) f(n)\left(n^{k} f(n)+g(n)\right)\right.$ which computes the binary representation of $F$.


## The Class NC

$$
N C=P T / W K\left(\log ^{k} n, n^{k}\right)
$$

- Problems solvable in polylogarithmic parallel time with polynomial amount of total work.
- Subclasses: $N C_{j}=P T / W K\left(\log ^{j} n, n^{k}\right)$
- NC closed under reductions
- Open problem : NC=P?


## P-completeness

- Odd Max Flow is not in NC
- Odd Max Flow is P-complete

■ Odd Max Flow: Given a network $N=(V, E, s, t, c)$ is the maximum flow value odd?

- MCV $\leq$ Odd Max Flow


## Monote Circuit Value

- A monotone boolean circuit's output cannot change from true to false when one input changes from false to true.

■ Monotone circuits do not contain : ᄀ gates

- Monotone circuit value is circuit value applied to monotone circuits.

C


f- standar flow


## RNC Algorithms

def. A language $L$ is in RNC if there is a uniform family of NC circuits with the following additional properties:

- $C_{n}$ specializes in strings of length n and has $\mathrm{n}+\mathrm{m}(\mathrm{n})$ input gates; $m(n)$ :additional gates, the random bits needed for the algorithm
- If x , of length n is in L then at least half of the $2^{m(n)}$ bit strings y of length $\mathrm{m}(\mathrm{n}), C_{n}$ outputs are TRUE on input $\mathrm{x} ; \mathrm{y}$
- If $x \notin L$ outputs FALSE on x ; y for all y .


## An RNC problem

- Does a bipartie graph have a perfect matching?
-Monte Carlo alg. for matching with symbolic determinants
-NC algorithm for arithmetic determinants
- If we know the answer to the decision problem, we compute the perfect matching using dynamic programming techniques.


## Minimum-weight perfect-matching

- Each edge has a weight $w_{i, j}$
- We want to minimize $\quad w(\pi)=\sum_{i=1}^{n} w_{i, \pi(i)}$
- There is an algorithm in NC for this problem, which works under 2 conditions

1) small weights, polynomial in $n$
2) $\pi$ is unique

- We proved that if the minimum weight perfect matching exists and is unique, it can be computed in parallel

■ We also know how to test in RNC whether a perfect matching exists

- How can we guarantee that the minimumweight matching is unique?


## The Isolating Lemma

- Suppose that the edges in E are assigned independently and randomly weights between 1 and 2|E|. If a perfect matching exists, then with probability at least $1 / 2$ the minimum-weight perfect matching is unique.

■Thank you!

