

Parallel Algorithm and Complexity - Samir Datta

Scribed: Soham Chatterjee

sohamchatterjee999@gmail.com

Website: sohamch08.github.io

2023

Contents

1	Addition of Two Numbers in Binary	2
1.1	Sequential (Ripple Carry)	2
1.2	Parallel (Carry Look Ahead Adder)	2
2	Iterated Addition	2
2.1	Iterated Addition of Logarithmically many n -bit numbers	3
2.2	Iterated Addition of n many n -bit numbers	3
3	$\text{IterAdd}_{n,n} \equiv \text{BCOUNT}_n \equiv \text{Threshold}_{n,m} \equiv \text{Majority}_n \equiv \text{MULT}_n \equiv \text{SORT}_{n,n}$	3
4	Parallel Random-Access Machine (PRAM)	6
5	Some Circuit Complexity Class Relations	8
6	Iterated Multiplication	10
7	Some Special Problems	11
8	Maximal Independent Set (MIS)	12
8.1	Matching and Independent Set of Line Graph	12
8.2	Luby's Algorithm (Randomized Algorithms)	12
8.3	Analysis of Luby's Algorithm	12
8.4	Derandomization	16
9	Perfect Matching in Bipartite Planer Graph	17

1 Addition of Two Numbers in Binary

Problem: ADD_{2n}

Input: Two n bit numbers $a = a_{n-1} \cdots a_1 a_0$ and $b = b_{n-1} \cdots b_1 b_0$

Output: $s = s_n \cdots s_1 s_0$ where $s \stackrel{\text{def}}{=} a + b$

1.1 Sequential (Ripple Carry)

For sum of any position i the two bits a_i , b_i and the carry generated by the previous position c_{i-1} is added. For the initial position we can set $c_0 = 0$. If we add two bits at most 2 bits is created. The right bit is called the sum bit and the left bit is the carry bit. $a_i + b_i + c_{i-1} = c_i s_i$. Then

$$s_i = a_i \oplus b_i \oplus c_{i-1} \text{ and } c_i = (a_i \wedge b_i) \vee (b_i \wedge c_{i-1}) \vee (c_{i-1} \wedge a_i)$$

Time Complexity: This algorithm takes $O(n)$ time complexity

1.2 Parallel (Carry Look Ahead Adder)

There is a carry that ripples into position i if and only if there is some position $j < i$ to the right where this carry is generated, and all positions in between propagate this carry. A carry is generated at position i if and only if both input bits a_i and b_i are on, and a carry is eliminated at position i , if and only if both input bits a_i and b_i are off. This leads to the following definitions:

For $0 \leq i < n$, let

$$g_i = a_i \wedge b_i$$

position i generates a carry

$$p_i = a_i \vee b_i$$

position i propagates a carry that ripples into it

So we can set for $1 \leq i \leq n$

$$c_i = \bigvee_{j=0}^{i-1} \left(g_j \wedge \bigwedge_{k=j+1}^{i-1} p_k \right)$$

Now the sumbits are calculated as before $s_i = a_i \oplus b_i \oplus c_{i-1}$ for $0 \leq i \leq n-1$ and $s_n = c_n$

Time Complexity: This algorithm takes $O(1)$ time complexity

Definition 1.1 (AC^0). *The class of circuits consists of the gates $(\vee_n, \wedge_n, \neg_1)$ (The subscript n or 1 denotes the fanin) of polynomial size and depth $O(1) = O(\log^0 n)$*

Theorem 1.1. $\text{ADD}_{2n} = \text{IterADD}_{2,n} \in AC^0$

2 Iterated Addition

Problem: $\text{IterADD}_{k,m}$

Input: k many m -bit numbers a_1, \dots, a_k

Output: The sum of the input numbers

Definition 2.1 (Length Respecting). *Let $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$. f is length respecting if for all $x, y \in \{0, 1\}^*$ $|f(x)| = |f(y)|$*

Definition 2.2 (Constant Depth Reduction). *Let $f, g : \{0, 1\}^* \rightarrow \{0, 1\}^*$ be length respecting. Then f is constant depth reducible to g or $f \leq_{cd} g$ if there is an unbounded fanin constant depth circuit computing f from the bits of g .*

2.1 Iterated Addition of Logarithmically many n-bit numbers

Theorem 2.1. $\text{IterADD}_{\log n, n} \leq_{cd} \text{IterADD}_{\log \log n, O(n)}$

Proof: We will denote $\log n = l$. We are given l many n -bit numbers a_1, \dots, a_l , where $\text{bin}(a_i) = a_{i,n-1} \dots a_{i,1} a_{i,0}$. We add all the l many bits at i th position of all numbers. we know if we add m bits then we have at most $\log m$

many bits. So adding the l many bits will take $\log l = \log \log n$ many bits. $s_k = \sum_{i=1}^l a_{i,k}$. Hence $\text{bin}(s_k) =$

$s_{k, \log l - 1} \dots s_{k,1} s_{k,0}$. Hence $\sum_{i=1}^l a_{i,k} = \sum_{j=0}^{\log l - 1} s_{k,j} 2^j$

$$\sum_{i=1}^l a_i = \sum_{i=1}^l \sum_{k=0}^{n-1} a_{i,k} 2^k = \sum_{k=0}^{n-1} \sum_{i=1}^l a_{i,k} 2^k = \sum_{k=0}^{n-1} \sum_{j=0}^{\log \log n - 1} s_{k,j} 2^j \cdot 2^k = \sum_{j=0}^{\log \log n - 1} \sum_{k=0}^{n-1} s_{k,j} 2^{j+k}$$

So this is converted to addition of $\log \log n$ many numbers of at most $n + \log \log n = O(n)$ many bits. ■ Recursing

like this we have $\text{IterADD}_{\log \log n, n} \leq_{cd} \text{IterAdd}_{2, O(n)}$. Hence

Theorem 2.2. $\text{IterADD}_{\log n, n} \leq_{cd} \text{IterAdd}_{2, O(n)}$ and therefore $\text{IterADD}_{\log n, n} \in AC^0$

Remark: Apart from this $O(\log^* n)$ method to prove $\text{IterADD}_{\log n, n} \in AC^0$ there is also another method in [Vinay Kumar's Lecture Notes](#)

2.2 Iterated Addition of n many n-bit numbers

We know $\text{IterAdd}_{n, n} \leq_{cd} \text{IterAdd}_{n, 1}$ but we dont know anything about $\text{IterAdd}_{n, n} \leq_{cd} \text{IterAdd}_{\log n, n}$. If that happens it will put $\text{IterAdd}_{n, n}$ to AC^0 .

Remark: $\text{IterAdd}_{n, 1}$ is also known as BCOUNT_n .

Theorem 2.3. $\text{IterAdd}_{n, n} \leq_{cd} \text{IterAdd}_{n, 1}$

Proof: Let we given n many n -bit numbers a_1, \dots, a_n , where $\text{bin}(a_i) = a_{i,n-1} \dots a_{i,1} a_{i,0}$. First we compute $s_k = \sum_{i=1}^n a_{i,k}$ using BCOUNT_n for all $0 \leq k \leq n$. Now it becomes addition of $\log n$ many $O(n)$ bit numbers which we already know is in AC^0 by [Theorem 2.2](#). Hence $\text{IterAdd}_{n, n} \leq_{cd} \text{BCOUNT}_n$ ■

3 $\text{IterAdd}_{n, n} \equiv \text{BCOUNT}_n \equiv \text{Threshold}_{n, m} \equiv \text{Majority}_n \equiv \text{MULT}_n \equiv \text{SORT}_{n, n}$

Problem: MULT

Input: 2 n-bit numbers $a = a_0, \dots, a_{n-1}$, $b = b_0, \dots, b_{n-1}$

Output: $c = a \cdot b$

Theorem 3.1. $\text{MULT}_{n, n} \leq \text{IterAdd}_{n, n}$

Proof: Given a, b where $\text{bin}(a) = a_{n-1} \dots a_1 a_0$ and $\text{bin}(b) = b_{n-1} \dots b_1 b_0$ then obviously

$$a \cdot b = \sum_{i=0}^{n-1} a \cdot b_i \cdot 2^i$$

Define for all $0 \leq i \leq n-1$

$$c_i = \begin{cases} 0^{n-i-1} a_{n-1} \cdots a_1 a_0 0^i & \text{when } b_i = 1 \\ 0^{2n-1} & \text{otherwise} \end{cases}$$

i.e. $c_i = a \cdot 2^i$ if $b_i = 1$. Each c_i is of $2n-1 = O(n)$ many bits long. Hence we have $a \cdot b = \sum_{i=0}^{n-1} c_i$. Hence now we can use the $\text{IterAdd}_{n,n}$ gate to add the n many $O(n)$ many bits to find the multiplication of a and b . Therefore $\text{MULT}_n \leq \text{IterAdd}_{n,n}$. ■

Problem: Majority $_n$

Input: n bits a_{n-1}, \dots, a_0

Output: Find if at least half of the bits are 1

Theorem 3.2. Majority \leq MULT

Proof: Given a_0, \dots, a_{n-1} . Take the number a such that $\text{bin}(a) = a_{n-1} \cdots a_1 a_0$. Denote $l := \log n$. Define

$$A = \sum_{i=0}^{n-1} a_i \cdot 2^{li} \text{ and } B = \sum_{i=0}^{n-1} 2^{li}$$

where both A and B consists of n blocks of length l . We took l length block because summation of n bits takes at most l bits. Let $C = A \cdot B$. We represent C in binary as l length blocks where $C = \sum_{i=0}^{2n-1} c_i \cdot 2^{li}$. Each c_i is a l length

block. Then the middle block c_{n-1} have exactly the computation of the sum of the a_i . Therefore $c_{n-1} = \sum_{i=0}^{n-1} a_i$.

A and B are constructed in constant depth and fed into MULT gates yielding C . Now we have to compare c_{n-1} with $\frac{n}{2}$ which can be done in constant depth. ■

Problem: ExactThreshold $_{n,m}$

Input: n bits a_{n-1}, \dots, a_0

Output: Find if $\sum_{i=0}^{n-1} a_i = m$

We have another similar problem but we have greater than instead of equality.

Problem: Threshold $_{n,m}$

Input: n bits a_{n-1}, \dots, a_0

Output: Find if $\sum_{i=0}^{n-1} a_i \geq m$

Theorem 3.3. BCOUNT \leq ExactThreshold \leq Threshold \leq Majority

Proof: BCOUNT \leq ExactThreshold: Let $\sum_{i=0}^{n-1} a_i = \sum_{i=0}^{l=\log n} s_i \cdot 2^i$. Let for all $0 \leq j \leq l$, R_j denote the set of all numbers $r \in \{0, \dots, n\}$ whose j -th bit is 1 in its binary representation. Then we can say

$$s_j = \bigvee_{r \in R_j} \left[\sum_{i=0}^{n-1} a_i = r \right]$$

Now R_j don't depend on the input but only on the input n so it can be hardwired this into the circuit. Thus we have a circuit for BCOUNT which uses ExactThreshold.

ExactThreshold \leq Threshold: We know for any r and a variable x certainly

$$\llbracket x = r \rrbracket = \llbracket x \geq r \rrbracket \wedge \llbracket x < r + 1 \rrbracket$$

With this we have a constant depth circuit for ExactThreshold using the Threshold gates.

Threshold \leq Majority: We are given a_0, \dots, a_{n-1} . Let we want to find $\sum_{i=0}^{n-1} a_i \geq m$ then we have this following relations

$$\sum_{i=0}^{n-1} a_i \geq m \iff \begin{cases} \text{Maj}_{2n-2m} \left(a_0, \dots, a_n, \underbrace{1, \dots, 1}_{n-2m} \right) & \text{wher } m < \frac{n}{2} \\ \text{Maj}_{2m} \left(a_0, \dots, a_n, \underbrace{0, \dots, 0}_{n-2m} \right) & \text{wher } m \geq \frac{n}{2} \end{cases}$$

This Maj_{2n-2m} and Maj_{2m} can be constructed in constant depth. ■

Remark: Hence using the theorems above we have the final relation

$$\text{Majority} \leq \text{MULT} \leq \text{IterAdd}_{n,n} \leq \text{BCOUNT} \leq \text{ExactThreshold} \leq \text{Threshold} \leq \text{Majority}$$

which gives the following corollary

Corollary 3.4. $\text{IterAdd}_{n,n} \equiv \text{BCOUNT} \equiv \text{Threshold} \equiv \text{Majority} \equiv \text{MULT}$

Definition 3.1 (TC^0). Constant depth polynomial size unbounded fanin circuit family using the gates $\wedge, \vee, \neg, \text{Maj}$.
Alternating Definition: Constant depth polynomial size unbounded fanin circuit family using the gates \neg, Maj .

Theorem 3.5. Both the definitions of TC^0 are equivalent.

Theorem 3.6. $\text{IterAdd}_{n,n}, \text{BCOUNT}, \text{MULT} \in \text{TC}^0$

Proof: By Corollary 3.4 we have the result. ■

Problem: SORT

Input: n numbers with n bits each

Output: The sequence of the input numbers in non-decreasing order.

Definition 3.2. We define $un_n(k) \triangleq 1^k 0^{n-k}$ where $k \in \{0, \dots, n\}$

Problem: UCOUNT

Input: $a_0, \dots, a_{n-1} \in \{0, 1\}$

Output: $un_n \left(\sum_{i=0}^{n-1} a_i \right)$

Lemma 3.7. $\text{BCOUNT} \leq \text{UCOUNT}$

Proof: Given a_0, \dots, a_{n-1} suppose $b_1 \dots b_n = un_n \left(\sum_{i=0}^{n-1} a_i \right)$. Also let $b_0 = 1$ and $b_{n+1} = 1$. Then in the number $b_0 b_1 \dots b_n b_{n+1}$ there is at least one 1 from left and at least one 0 from right. Now take

$$d_j = b_j \wedge \neg(b_{j+1})$$

for all $0 \leq j \leq n$. Then if $d_j = 1$ that means $b_j = 1$ and $b_{j+1} = 0$ hence b_j is the last bit which is 1 afterwards every bit is 0. Hence there are in total j many 1's except b_0 . Therefore $\sum_{i=0}^{n-1} a_i = j$. So we take all $r \in 0, \dots, n$ such that the j th bit of r is on then define

$$c_j = \bigwedge_{i \in R_j} d_i$$

Hence if $c_j = 1$ then we can say $\sum_{i=0}^{n-1} a_i$ is such a number whose j th bit is 1. Thus we take $\text{BCOUNT}(a_0, \dots, a_{n-1}) = c_{\log n - 1} \cdots c_1 c_0$ ■

Theorem 3.8. $\text{UCOUNT} \equiv \text{BCOUNT}$

Theorem 3.9. $\text{UCOUNT} \leq \text{SORT} \leq \text{UCOUNT}$

Proof: $\text{UCOUNT} \leq \text{SORT}$: Given a_0, \dots, a_{n-1} define $A_i = a_i \underbrace{0 \cdots 0}_{n-1}$ for all $0 \leq i \leq n-1$. Sorting these

numbers the sequence of most significant bits in the ordered sequence is the $\text{un}_n \left(\sum_{i=0}^{n-1} a_i \right)$ reversed.

$\text{SORT} \leq \text{UCOUNT}$: Given $a_i = a_{i,n-1} \cdots a_{i,1} a_{i,0}$ for all $1 \leq i \leq n$. Define

$$c_{i,j} \triangleq \llbracket (a_i < a_j) \vee ((a_i = a_j) \wedge i \leq j) \rrbracket$$

$\forall 0 \leq i, j \leq n-1$. Now we define for all $1 \leq j \leq n$

$$c_j \triangleq \text{UCOUNT}(c_{0,j} \dots c_{n-1,j})$$

Hence first of all the number of 1's in $c_{0,j} \dots c_{n-1,j}$ is the number of a_i 's with value strictly less than a_j or if equal then index is less than or equal to j . Hence it represents the position of a_j when the numbers are sorted. Therefore c_j is the n -bit unary representation of the position of a_j in the ordered output sequence. If the ordered sequence is a'_1, \dots, a'_n then $a'_{c_j} = a_j$. Let $a'_i = a'_{i,n-1} \cdots a'_{i,0} a'_{i,1} a'_{i,0}$ for $1 \leq i \leq n$. Then

$$a'_{i,k} = 1 \iff \llbracket a'_i = a_j \rrbracket \wedge \llbracket a_{j,k} = 1 \rrbracket$$

Hence $a'_{i,k} = \bigwedge_{1 \leq j \leq n} (\llbracket c_j = 1^i 0^{n-i} \rrbracket \wedge a_{j,k})$. ■

Corollary 3.10. $\text{SORT} \in \text{TC}^0$

4 Parallel Random-Access Machine (PRAM)

In [KR90] many Parallel Machine Models are very well written and explained

Definition 4.1 (PRAM). A PRAM consists of an infinite sequence of processors P_1, P_2, \dots . Each processor P_i has its local memory realized as an infinite sequence $R_{i,0}, R_{i,1}, R_{i,2}, \dots$ of registers. Additionally there is a common (or global) memory given by the infinite sequence C_0, C_1, C_2, \dots of registers. Each register can hold as value a natural number, stored in binary as a bit string.

A particular PRAM is specified by a program and a processor bound. The program is a sequence of instructions S_1, S_2, \dots, S_s and the processor bound is a function $p : \mathbb{N} \rightarrow \mathbb{N}$

Workflow: Initially the input is distributed over the lowest numbered global memory cells. Then all the processors $P_1, \dots, P_{p(n)}$ start the execution of the program with the first instruction S_1 . Each instruction S_m is one of the following 9 types.

Instructions: Suppose a fixed processor P_r , $1 \leq r \leq p(n)$. Let $c, i, j, k \in \mathbb{N}$ and $1 \leq l \leq s$. We describe the instructions and their effect in turn. If S_m is one of the first 7 types then after the execution of S_m processor P_r continues with instruction S_{m+1}

1. $R_i \leftarrow c$: $R_{r,i}$ gets as value the constant c .
2. $R_i \leftarrow \#$: $R_{r,i}$ gets as value the number of the processor i.e. r
3. (Numerical Operations) $R_i \leftarrow R_j + R_k$, $R_i \leftarrow R_j - R_k$: The result of adding the contents of $R_{r,j}$ and $R_{r,k}$ (Subtracting) is stored in $R_{r,i}$. (If subtraction results in a negative number the $R_{r,i}$ gets value 0)
4. (Bitwise Operation) $R_i \leftarrow R_j \vee R_k$, $R_i \leftarrow R_j \wedge R_k$, $R_i \leftarrow R_j \oplus R_k$: The result of performing the bitwise OR (AND, PARITY) of the contents of $R_{r,j}$ and $R_{r,k}$ is stored in $R_{r,i}$.
5. (Shift Operation) $R_i \leftarrow \text{shl } R_j$, $R_i \leftarrow \text{shr } R_j$: If the contents of $R_{r,j}$ is a where $\text{bin}(a) = a_1 \cdots a_0$ then register $R_{r,i}$ will get the value b where $\text{bin}(b) = a_1 \cdots a_0 0$ (for shl) and $\text{bin}(b) = a_1 \cdots a_1$ (for shr)
6. (Indirect Addressing 1): $R_i \leftarrow (R_j)$: The contents of the global memory register whose number is given by the contents of $R_{r,i}$.
7. (Indirect addressing 2): $(R_i) \leftarrow R_j$: The contents of $R_{r,j}$ is copied to that global register whose number is given by the contents of $R_{r,i}$
8. (Conditional Jump) IF $R_i < R_j$ GOTO l : If the contents of $R_{r,i}$ is smaller in value than the contents of $R_{r,j}$ then processor P_r continues with the execution of instruction S_l ; otherwise it continues with the next instruction S_{m+1} .
9. HALT: The computation of processor P_r stops.

The computation of M stops when all the processors $R_1, \dots, R_{p(n)}$ have halted

Let $f : \mathbb{N}^* \rightarrow \mathbb{N}^*$. We say that a PRAM M computes f if the following holds: Given an input $(x_1, \dots, x_n) \in \mathbb{N}^n$ (input length: n) the x_i are first distributed in global memory cells C_1, \dots, C_n i.e. C_i is initialized to x_i for $1 \leq i \leq n$. Additionally C_0 is initialized to n . Then the computation of M is started. Let m be the contents of register C_0 after the computation stops. Then $f(x_1, \dots, x_n)$ is the vector from \mathbb{N}^m whose components are the numbers in the global register C_1, \dots, C_m

Definition 4.2 (EREW-PRAM). $E := \text{Exclusive}$, $R := \text{Read}$, $W := \text{Write}$

Question 1. Can n , n -bit numbers be sorted in $O(\log n)$ time on an EREW-PRAM? Bit arithmetic is allowed and each with polynomially many processors. Bit operation takes $O(1)$ time. Hence is $\text{SORT} \in \text{EREW}[\log n, \text{poly}(n)]$?

Question 2. What about if bit arithmetic are not allowed?

Question 3. If comparisons are allowed can we say anything?

Answer: AKS (Ajtai–Komlós–Szemerédi) in their paper [Pad11] showed in $O(\log n)$ time

Question 4. If number of processors is $O(n)$ what can be said?

There are also other parallel machine models: CRCW ($C := \text{Concurrent}$), CREW, CROW ($O := \text{Owner}$), OROW. Concurrent means everyone can access the memory concurrently. Owner means only the processor who is the owner of a memory can access it.

In CRCW allows simultaneous read and writes. Hence we have to resolve write conflicts. Some commonly used methods of resolving write conflicts are COMMON, ARBITRARY, PRIORITY models.

Definition 4.3 (NC^1). Class of languages accepted by circuits of depth $O(\log n)$ and size $n^{O(1)}$ and fanin 2

Definition 4.4. Formulas are trees i.e. circuits with fanout 1

Theorem 4.1. In NC^1 formulas and circuits are equivalent.

Theorem 4.2. $\text{NC}^1 \subseteq \text{OROW}[\log n, \text{poly}(n)]$

Proof: For any circuit $C \in NC^1$ we create the OROW PRAM where each gate of C is a processor in the PRAM and each processor has the writing access of their own memory and for any edge $u \rightarrow v$ in C processor v has the reading access of the memory of u . With this OROW PRAM each processor can read memory from its children then writes the computed value in his memory location thus it computes C . Since C has size $n^{O(1)}$ the PRAM has $n^{O(1)}$ many processors and since the circuit has depth $O(\log n)$ the OROW PRAM takes $O(\log n)$ time to compute. ■

Open Question 4.3. $NC^1 \stackrel{?}{\supseteq} OROW[\log n, \text{poly}(n)]$

Definition 4.5 (AC^k, NC^k). The class of circuits consists of the gates (\vee, \wedge, \neg) (The subscript n or 1 denotes the fanin) of polynomial size and depth $O(1) = O(\log^k n)$
Similarly for NC^k but with fanin 2

Theorem 4.4. $AC^1 = CRCW[\log n, \text{poly}(n)]$

Proof: $AC^1 \subseteq CRCW[\log n, \text{poly}(n)]$: (COMMON) For any gate all its parents have similarly reading access of the memory of the gate and all its childs has writing access. But we use COMMON model to resolve write conflicts. For an OR gate if anyone evaluates to be 0 then it ignores and if its 1 then it writes 1. Thus everybody writes 1. Every OR gate by has 0 previously in the memory. Similarly for AND gate its the opposite.

$AC^1 \supseteq CRCW[\log n, \text{poly}(n)]$: Theorem 4.5, [SV84] ■

Theorem 4.5. Let $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ be a length-respecting function computed by the CRCW PRAM M in time $t(n)$. Let the processor bound of M be $p(n)$. Then there is a family \mathcal{C} of circuits that computes f where the depth of \mathcal{C} is $O(t(n))$ and size is polynomial in $n + t(n) + p(n)$.

Proof: See [Vol99, Theorem 2.56, Page 70] ■

5 Some Circuit Complexity Class Relations

Theorem 5.1. $AC^0 \subseteq NC^1$

Proof: For all unbounded gate in AC^1 circuit C with fanin s we can replace each gate with s many same gates of fanin 2 and depth $\log s$. Thus we have $AC^0 \subseteq NC^1$ ■

Theorem 5.2. $TC^0 \subseteq NC^1$

Proof: We will first show that using Redundant Algebra $ADD_{2n} \in NC^0$. In Redundant Algebra with base 4 while adding two digits the result can be at most in normal integers $-6, \dots, 6$. We only have to check for $\pm 6, \pm 5, \pm 3$. Other case we dont have to watch out.

$$\begin{array}{lll} 6 = 12 & 5 = 11 & 3 = \overline{11} \\ \overline{6} = \overline{12} & \overline{5} = \overline{11} & \overline{3} = \overline{11} \end{array}$$

For ± 4 it is the normal representation in this system ie 10 and $\overline{10}$ respectively. Now whenever we add two digits in this system in the sum result can be at most 2 digits. Among them we call the right most digit the sum digit or s and the left digit the carry digit c because it becomes the carry for the addition. Now see in all of the numbers the sum digit $|s| \leq 2$ and carry digit $|c| \leq 1$ So whenever we add a carry generated before to the current sum no new carry is generated because of the carry. So We dont have to look for carry generation and propagation. The carry generated at the previous position will add to the sum digit in the current position after getting added to that it will not further

propagate after getting added the final digit at the current place will be between 3 and $\bar{3}$ So we proved that addition of two n -bit numbers using Redundant algebra is in NC^0

Now we will show converting a number n from base 2 to base 4 is in NC^0 . let

$$n = \sum_{k=0}^m a_k 2^k = \sum_{k=0}^{\lfloor \frac{m}{2} \rfloor} (a_{2k+1} \times 2 + a_{2k}) 4^k \quad \text{if } m \text{ is odd then } a_{m+1} = 0$$

So we just take two bits in binary multiply the left one with 2 and add to the right one and we have the digit at base 4 in that position. So we can change base in NC^0 . From now on we will by default assume all the addition is done using Redundant Algebra.

Then we are done in showing $TC^0 \subseteq NC^1$. We will first show that adding n bits is in NC^1 ie $BCOUNT \in NC^1$. So we have n bits a_n, a_{n-1}, \dots, a_1 . We will group the bits into groups of two bits and add the two bits in each group. We can do the addition for all groups in parallel. And since we have already shown addition of two k -bit numbers is in NC^0 this takes constant depth and size since we are adding two bits. Now the number of bits are halved. We do the same process again and again. Each time it takes $\text{poly}(n)$ size and constant depth and at each iteration the number of numbers becomes half. So this whole process takes $O(\log n)$ many iterations. So adding n bits takes $\text{poly}(n)$ size and depth $O(\log n)$. So $BCOUNT \in NC^1$

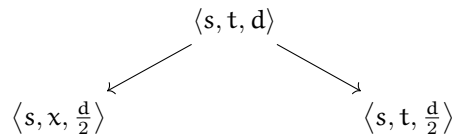
Now We will show that Majority $\in NC^1$. Let the addition of n bits we got is a and the Redundant Algebra representation of $\lceil \frac{n}{2} \rceil$ is b . Now we can calculate $-b$ with reversing the sign of every digit in b ie if $b = \sum_{i=0}^m a_i \times 4^i$ then $-b = \sum_{i=0}^m \bar{a}_i \times 4^i$. Now we add a and $-b$ which can be done in NC^0 . And now we will look for the left most negative digit. If there is none we output 1 i.e. majority of the bits are 1 and if there exists a negative bit then output is 0. Hence we have Majority $\in TC^0$. So $TC^0 \subseteq NC^1$. ■

Definition 5.1 (SAC^k). The class of circuits consists of the gates (\vee, \wedge, \neg) of polynomial size and depth $O(1) = O(\log^k n)$ but semi unbounded fanin i.e either \wedge gates have unbounded fanin and \vee gate have bounded fanin or \wedge gates have bounded fanin and \vee gates have unbounded fanin.

Theorem 5.3. $AC^0 \subseteq TC^0 \subseteq NC^1 \subseteq L \subseteq NL \subseteq SAC^1 \subseteq AC^1 \subseteq NC^2 \subseteq AC^2 \subseteq \dots \subseteq NC^i \subseteq AC^i \subseteq \dots \subseteq NC = AC \subseteq P$

Proof: $NC^1 \subseteq L$: The idea is to simply evaluate the circuit using a depth-first search, which can be defined inductively as follows: visit the output gate of the circuit, visit the gates of the left subcircuit, visit the gates of the right subcircuit. At any moment, we store the number of the current gate, the path that led us there (as a sequence of left's and right's) and any partial values that were already computed. For example, we could have L, R (0), R (1), L, L, 347. This would mean that we are visiting gate 347 and we got there by going left, right, right, left and left. The 0 after the first R indicates that the left input of the second gate on the path evaluated to 0. When we are done visiting a gate (and computed its value), we return to the previous gate on the path. Note that we can recompute the number of that gate by following the path from the beginning. The space requirements of this algorithm are therefore determined by the maximum length of the path, which is equal to the depth of the circuit. The uniformity of the circuit is used when traveling through the circuit and evaluating its gates.

$NL \subseteq SAC^1$: We know PATH is NL – complete. Let there is a path $s \rightsquigarrow t$ of length d . Then there exists a vertex x in between s and t such that there exists a path of length $\frac{d}{2}$ from $s \rightsquigarrow x$ and $x \rightsquigarrow t$.



Since there exists one such vertex x and in circuit we will add all this in a big \vee gate for all vertices in the graph. We can represent this as a circuit

$$\langle s, t, d \rangle = \bigvee_{x \in V} \left(\left\langle s, x, \frac{d}{2} \right\rangle \wedge \left\langle s, t, \frac{d}{2} \right\rangle \right)$$

Like this we extend it to 1 length paths. In this circuit we are using \vee gates with unbounded fanin and \wedge gates with 2 fanin. Hence we have $NL \subseteq SAC^1$ ■

6 Iterated Multiplication

Problem: ItMult_{m,n}

Input: m many n-bit numbers are given

Output: The product of the given numbers

Theorem 6.1 (Chinese Remainder Theorem). *Let $k \in \mathbb{N}$, $P = p_1 p_2 \cdots p_k$. Let a_1, \dots, a_k be given. Then there is a unique number $a \in \{0, \dots, P-1\}$ such that $a \equiv a_i \pmod{p_i}$ for $1 \leq i \leq k$. More specifically, we have*

$$a = \left[\sum_{i=1}^k (a_i \pmod{p_i}) \right] \pmod{P}$$

where $r_i = \frac{p}{p_i}$ and $s_i = \left(\frac{p}{p_i}\right)^{-1} \pmod{p_i}$ (i.e. s_i is the multiplicative inverse of $r_i \pmod{p_i}$).

Theorem 6.2 (Prime Number Theorem). *Let $\Pi(n)$ denote the number of prime numbers not greater than n. Then*

$$\Pi(n) = \Theta\left(\frac{n}{\log n}\right)$$

Corollary 6.3. *Let p_k denote the kth prime. $p_n = O(n \log n)$*

Theorem 6.4. *Let p_i denote the ith prime. Then*

$$\prod_{i=1}^n p_i \leq 4^{n \log n}$$

Theorem 6.5. ItMult_{n,n} $\in TC^0$

Proof: Let $a_i = a_{i,n-1} \cdots a_{i,1} a_{i,0}$ for $1 \leq i \leq n$ be the given numbers which we want to multiply up. Hence

$$a = a_1 \cdot a_2 \cdots a_n < (2^n)^n = 2^{n^2} < p_1 \cdot p_2 \cdots p_{n^2}$$

Then take $p = p_1 \cdot p_2 \cdots p_{n^2}$. Then our goal is to compute $a \pmod{p}$. Our first goal is to compute $a \pmod{p_i}$ for all $1 \leq i \leq n^2$.

Now take $r_i = \frac{p}{p_i}$ and $s_i = \left(\frac{p}{p_i}\right)^{-1} \pmod{p_i}$. Then by [Chinese Remainder Theorem](#) we have

$$a = \sum_{i=1}^{n^2} (a \pmod{p_i}) \cdot r_i \cdot s_i$$

Now we have

$$a \pmod{p_j} = \prod_{i=1}^n a_i \pmod{p_j} = \prod_{i=1}^n (a_i \pmod{p_j})$$

Take

$$a'_{i,j} := a_i \pmod{p_j} = \left(\sum_{k=0}^{n-1} a_{i,k} \cdot 2^k \right) \pmod{p_j} = \sum_{k=0}^{n-1} a_{i,k} \cdot (2^k \pmod{p_j}) \quad \text{for } 1 \leq i \leq n, 1 \leq j \leq n^2$$

This gives n^3 many numbers all of which can be computed in constant depth. The values $2^k \pmod{p_j}$ can be hardwired into the circuit since they do not depend on the input but only the input length. So we can compute $a'_{i,j}$ using ItAdd and MULT gates (since we know they are already in TC^0) in constant depth. Using the [Corollary 6.3](#) we have $p_j = O(n^2 \log n)$ for all $1 \leq j \leq n^2$. Therefore all the $a'_{i,j}$ consists of $O(\log n)$ bits only.

For $1 \leq j \leq n^2$ let g_j be the generator of the multiplicative group $\mathbb{Z}_{p_j}^*$ group of the finite field \mathbb{Z}_{p_j} . Let for $k \in \{1, \dots, p_j - 1\}$ take $g^{m_j(k)} = k$ where $m_j(k) \in \{0, \dots, p_j - 2\}$. And we set $m_j(0) := p_j - 1$. So now we will compute $m_j(a'_{i,j})$. Since the numbers $a'_{i,j}$ contains $O(\log n)$ many bits, these computations can be done in constant depth. Therefore

$$m_j \left(\prod_{i=1}^n a_i \pmod{p_j} \right) = m_j \left(\prod_{i=1}^n (a_i \pmod{p_j}) \right) = \left(\sum_{i=1}^n m_j(a'_{i,j}) \right) \pmod{p_j - 1}$$

for $1 \leq j \leq n^2$. This can be computed in constant depth using ItAdd gates. The case when $a'_{i,j} = 0$ can be taken care of. These n^2 numbers have logarithmically many bits. Thus we can compute the value $\prod_{i=1}^n a_i \pmod{p_j}$ for $1 \leq j \leq n^2$ in constant depth. Finally we compute

$$a' := \sum_{j=1}^{n^2} \left(\prod_{i=1}^n a_i \pmod{p_j} \right) \cdot r_j \cdot s_j$$

in constant depth with ItAdd and MULT gates. The values r_j and s_j can be hardwired into the circuit since they don't depend on the input instead the length of the input.

By [Chinese Remainder Theorem](#) we have $a = a' \pmod{a'}$ that is $q := \left\lfloor \frac{a'}{p} \right\rfloor$ we have $a = a' - q \cdot p$. Since $r_j = \frac{p}{p_j}$ and $s_j \leq p_j$ we have $r_j \cdot s_j \leq p$. Therefore

$$a' = \sum_{j=1}^{n^2} \left(\prod_{i=1}^n a_i \pmod{p_j} \right) \cdot r_j \cdot s_j \leq \sum_{j=1}^{n^2} \left(\prod_{i=1}^n a_i \pmod{p_j} \right) p \leq \sum_{i=1}^{n^2} p_{n^2} p = n^2 \cdot p_{n^2} \cdot p \implies q \leq n^2 \cdot p_{n^2}$$

This the value of q is polynomial in n and can be determined by parallelly testing for all $i \leq n^2 \cdot p_{n^2}$ if $i \cdot p \leq a' \leq (i+1)p$ which can be done in constant depth and q is the one value of i for which the answer of this is yes. Then the result of the iterated multiplication is $a = a' - q \cdot p$. ■

7 Some Special Problems

Definition 7.1 (Approximate Majority or AM). For $x \in \{0, 1\}^n$ let $\text{wt}(x)$ be the number of ones in x . Then

$$\text{AM}(x) = \begin{cases} 0 & \text{if } \text{wt}(x) \leq \frac{n}{4} \\ 1 & \text{if } \text{wt}(x) \geq \frac{3n}{4} \\ \text{don't care} & \text{otherwise} \end{cases}$$

Theorem 7.1. [[Ajt83](#), Section 4] Approximate Majority $\in AC^0$

Theorem 7.2. [[MC89](#), Theorem 2.1, Corollary 2.2] Dyck $_k \in DLogTime - \text{Uniform } TC^0$

Theorem 7.3. [[Bus87](#)] Boolean Formula Value Problem $\in ALogTime$

Corollary 7.4. $NC^1 = ALogTime$

Theorem 7.5. [[GL18](#)] Tree Balancing $\in DLogTime - \text{uniform } TC^0$

8 Maximal Independent Set (MIS)

Theorem 8.1. $MIS \in P$

8.1 Matching and Independent Set of Line Graph

Definition 8.1 (Line Graph). *The line graph of the graph G , written $L(G)$ is the graph whose vertices are the edges of G , with $(e_1, e_2) \in E(L(G))$ when $e_1 \cap e_2 \neq \emptyset$*

Theorem 8.2. *Given a graph G a set of edges $S \subseteq E$ is a matching if and only if it is a independent set in the line graph $L(G)$*

Proof: (\Rightarrow) : Let S be a matching of G . Therefore for all $e_1, e_2 \in S$ we have $e_1 \cap e_2 = \emptyset$. Hence e_1, e_2 are not adjacent in $L(G)$. Hence S is an independent set of $L(G)$.

(\Leftarrow) : Let S be a independent set in $L(G)$. Then for all $e_1, e_2 \in S$, e_1 and e_2 are not adjacent. Therefore $e_1 \cap e_2 = \emptyset$. Hence the set S is a set of edges of G where none of them shares any endpoint. Hence S is a matching in G . ■

Fact 1. *Maximal (Maximum) Matching in G is an Maximal (Maximum) Independent Set in the line graph $L(G)$.*

8.2 Luby's Algorithm (Randomized Algorithms)

Definition 8.2 (RNC^k). *The class RNC^k is the class of problems that can be solved by a randomized algorithm that runs in $O(\log^k n)$ time with a polynomial number of processors.*

Remark: Therefore RNC is the randomized counterpart of NC . Luby's Algorithm puts MIS in RNC^2 . The main steps or the ideas of the algorithm are:

- The algorithm tries to find I in each stage.
- Each stage finds an independent set I in parallel, using calls on a
- Create a set S of candidates for I as follows: For each vertex v in parallel, include $v \in S$ with probability $\frac{1}{2d(v)}$
- For each edge in E if both its endpoints are in S , discard the one of lower degree, ties are resolved arbitrarily
- The resulting set is I

Here we denote for any $v \in V$ $d(v) := \deg(v)$.

8.3 Analysis of Luby's Algorithm

Now we will define certain things which will help us to analyze the algorithm:

- A vertex $v \in V$ is *good* if

$$\sum_{u \in N(v)} \frac{1}{2d(u)} \geq \frac{1}{6}$$

A pair of vertices $u, v \in V$ is said to be *good* if

$$\text{good}(u, v) \iff [(u, v) \in E] \wedge [\text{good}(u) \vee \text{good}(v)]$$

Intuitively a vertex is good if it has lots of neighbors of low degree. This will give it a decent chance of making into $N(I)$. Therefore in case of bad vertex $\text{bad}(v) = \neg \text{good}(v)$ and for a pair of vertices $u, v \in V$ we have $\text{bad}(u, v) = \neg \text{good}(u, v)$

Algorithm 1: Luby's Randomized Algorithm on MIS

```

1 begin
2    $A \leftarrow \emptyset$ 
3   while  $G \neq \emptyset$  do
4      $S \leftarrow \emptyset$ 
5      $I \leftarrow \emptyset$ 
6     for  $v \in V(G)$  in parallel do
7        $\lfloor$  add  $v$  to  $S$  with probability  $\frac{1}{2d(v)}$ 
8     for  $\{u, v\} \in E(G)$  in parallel do
9       if  $u \in S$  and  $v \in S$  then
10        if  $d(u) < d(v)$  then
11          delete  $u$  from  $S$ 
12        else if  $d(v) < d(u)$  then
13          delete  $v$  from  $S$ 
14        else if  $u < v$  then
15          delete  $u$  from  $S$ 
16        else
17          delete  $v$  from  $S$ 
18     Call the resulting set after deletions  $I$ 
19      $A \leftarrow A \cup I$ 
20      $G \leftarrow G \setminus (I \cup N(I))$ 
21 return  $A$ 

```

- We also define

$$\begin{aligned}
 N^-(v) &= \{u \in N(v) \mid d(u) \leq d(v)\} & d^-(v) &= |N^-(v)| \\
 N^+(v) &= \{u \in N(v) \mid d(u) > d(v)\} & d^+(v) &= |N^+(v)|
 \end{aligned}$$

Therefore we have $d^+(v) + d^-(v) = d(v)$.

Lemma 8.3. For any $v \in V$

$$bad(v) \implies d^+(v) \geq 2d^-(v) \iff d^-(v) \leq \frac{d(v)}{3} \iff d^+(v) \geq \frac{2d(v)}{3}$$

Proof: We make the graph directed where if $(u, v) \in E$ previously then the direction of this edge will be

$$u \rightarrow v \iff \llbracket d(u) < d(v) \rrbracket \vee \left(\llbracket d(u) = d(v) \rrbracket \wedge \llbracket u < v \rrbracket \right)$$

Then $d^-(v)$ in the original graph indicates the in-degree of v and $d^+(v)$ indicates the out-degree of v . Therefore $d^+(v) \geq \frac{2d(v)}{3}$ means out-degree of v is twice more than the in-degree of v . Now assume the statement is not true. Let v is *bad*. Then

$$\frac{1}{6} > \sum_{u \in N(v)} \frac{1}{2d(u)} \geq \sum_{u \in N^-(v)} \frac{1}{2d(u)} \geq \sum_{u \in N^-(v)} \frac{1}{2d(v)} \geq \frac{d^-(v)}{2d(v)} > \frac{d(v)}{3} \times \frac{1}{2d(v)} \geq \frac{1}{6}$$

Hence contradiction. ■

Lemma 8.4. At least half of the edges in the graph are good

Proof: We again construct the same directed graph from G as in the proof of [Lemma 8.3](#). If $(u, v) \in E$ then the direction of this edge will be

$$u \rightarrow v \iff \llbracket d(u) < d(v) \rrbracket \vee \left(\llbracket d(u) = d(v) \rrbracket \wedge \llbracket u < v \rrbracket \right)$$

Now for any edge $e = (u, v) \in E$

$$\text{bad}(e) \iff \text{bad}(u) \wedge \text{bad}(v)$$

Let the direction of e is $u \rightarrow v$. Since e is bad the vertex v is bad. Therefore using [Lemma 8.3](#) out-degree of v is twice more than the in-degree of v . Hence there is at least two edges out-going from v . Let those edges are $e_1 = v \rightarrow w_1$ and $e_2 = v \rightarrow w_2$. Hence for every bad vertex there are two edges in E . Hence

$$2|\{e \in E \mid \text{bad}(e)\}| \leq |E|$$

Therefore we have $2\#\text{bad}(e) \leq \#\text{good}(e) + \#\text{bad}(v) \implies \#\text{good}(e) \geq \#\text{bad}(e) \implies 2\#\text{good}(v) \geq |E|$. ■

Lemma 8.5. For any $v \in V$

$$\Pr[v \notin I \mid v \in S] \leq \frac{1}{2}$$

Proof: If $v \in S$ and $v \notin I$ only if there exists some element of $N^+(v)$ which is also in S . Then

$$\begin{aligned} \Pr[v \notin I \mid v \in S] &= \Pr[\exists u \in N^+(v) \cap S \mid v \in S] \\ &\leq \sum_{u \in N^+(v)} \Pr[u \in S \mid v \in S] \\ &= \sum_{u \in N^+(v)} \Pr[u \in S] && \text{[Pairwise independence]} \\ &\leq \sum_{u \in N^+(v)} \frac{1}{2d(u)} \leq \sum_{u \in N^+(v)} \frac{1}{2d(v)} \\ &\leq \frac{d(v)}{2d(v)} && \text{[Lemma 8.3]} \\ &\leq \frac{1}{2} \end{aligned}$$

■

Lemma 8.6. For any $v \in V$

$$\Pr[v \in I] \geq \frac{1}{4d(u)}$$

Proof: We have

$$\begin{aligned} \Pr[v \in I] &= \Pr[v \in I \mid v \in S] \Pr[v \in S] \\ &\geq (1 - \Pr[v \notin I \mid v \in S]) \frac{1}{2d(v)} \\ &= \frac{1}{2} \times \frac{1}{2d(v)} = \frac{1}{4d(v)} && \text{[Lemma 8.5]} \end{aligned}$$

■

Lemma 8.7. *If $v \in V$ is good then*

$$\Pr[v \in N(I)] \geq \frac{1}{36}$$

Proof: We will consider two cases.

Case 1: v has a neighbor u of degree 2 or less. Then using [Lemma 8.6](#)

$$\Pr[v \in N(I)] \geq \Pr[u \in I] \geq \frac{1}{4d(u)} \geq \frac{1}{8}$$

Case 2: $d(u) \geq 3$ for all $u \in N(v)$. Then for all $u \in N(v)$ we have $\frac{1}{2d(u)} \leq \frac{1}{6}$. Now since v is good we have $\sum_{u \in N(v)} \frac{1}{2d(u)} \geq \frac{1}{6}$. Therefore there must exist a subset $M(v) \subseteq N(v)$ such that

$$\frac{1}{6} \leq \sum_{u \in M(v)} \frac{1}{2d(u)} \leq \frac{1}{3} \quad (1)$$

Therefore

$$\begin{aligned} \Pr[v \in N(v)] &\geq \Pr[\exists u \in M(v) \cap I] \\ &= \sum_{u \in M(v)} \Pr[u \in I] - \sum_{\substack{u, w \in M(v) \\ u \neq w}} \Pr[u \in I \wedge w \in I] && \text{[Inclusion-Exclusion]} \\ &= \sum_{u \in M(v)} \frac{1}{4d(u)} - \sum_{\substack{u, w \in M(v) \\ u \neq w}} \Pr[u \in S \wedge w \in S] && \text{[Lemma 8.6]} \\ &= \sum_{u \in M(v)} \frac{1}{4d(u)} - \sum_{\substack{u, w \in M(v) \\ u \neq w}} \Pr[u \in S] \Pr[w \in S] && \text{[Pairwise independence]} \\ &= \sum_{u \in M(v)} \frac{1}{4d(u)} - \sum_{u \in M(v)} \sum_{w \in M(v)} \frac{1}{2d(u)} \frac{1}{2d(w)} \\ &= \sum_{u \in M(v)} \frac{1}{2d(u)} \left[\frac{1}{2} - \sum_{w \in M(v)} \frac{1}{2d(w)} \right] \\ &\geq \frac{1}{6} \left(\frac{1}{2} - \frac{1}{3} \right) = \frac{1}{36} && \text{[By (1)]} \end{aligned}$$

■

Lemma 8.8. *If $e \in E$ is good then*

$$\Pr[e \text{ is deleted}] \geq \frac{1}{36}$$

Proof: If the edge $e = (u, v) \in E$ is deleted then either u or v is good vertex. Let u is good. Since e is deleted then $\Pr[u \in N(I)] \geq \frac{1}{36}$ by [Lemma 8.7](#). Hence

$$\Pr[e \text{ is deleted}] \geq \Pr[\text{good}(u) \wedge u \in N(I)] + \Pr[\text{good}(v) \wedge v \in N(I)] \geq \frac{1}{36}$$

■

Lemma 8.9. Let X be the random variable representing the number of deleted edges. Then

$$\mathbb{E}[X] \geq \frac{|E|}{72}$$

Proof: Take the indicator random variable for each edge $e \in E$

$$X_e = \begin{cases} 1 & \text{if } e \text{ is deleted} \\ 0 & \text{otherwise} \end{cases}$$

Therefore $X = \sum_{e \in E} X_e$. Then we have

$$\begin{aligned} \mathbb{E}[X] &= \mathbb{E} \left[\sum_{e \in E} X_e \right] = \sum_{e \in E} \mathbb{E}[X_e] \\ &\geq \sum_{\text{good}(e)} \mathbb{E}[X_e] \geq \sum_{\text{good}(e)} \Pr[e \text{ is deleted}] \\ &\geq \sum_{\text{good}(e)} \frac{1}{36} && [\text{Lemma 8.8}] \\ &\geq \frac{|E|}{2} \times \frac{1}{36} = \frac{|E|}{72} && [\text{Lemma 8.4}] \end{aligned}$$

■

Theorem 8.10. Luby's Algorithm puts $\text{MIS} \in \text{RNC}^2$

8.4 Derandomization

Theorem 8.11. Bertrand's Postulate For any integer $n > 1$ there always exists at least one prime p with

$$n < p < 2n$$

From the proof of [Lemma 8.5](#) and [Lemma 8.7](#) we can see that we don't need the vertices to be independent. Pairwise independent is enough for the analysis. We construct pairwise independent family of functions by taking a prime p in the range n to $2n$ (such prime exists because of [8.11](#)) and then we can assume the vertices of the graph are the elements of the finite field \mathbb{Z}_p . Now for each vertex u we take $a(u)$ be an integer in \mathbb{Z}_p such that $\frac{1}{2d(u)} \approx \frac{a(u)}{p}$ that is $\frac{a(u)}{p}$ is as close as possible to $\frac{1}{2d(u)}$. Then we denote $A_u := \{0, 1, \dots, a(u) - 1\}$. We can take A_u as any subset of \mathbb{Z}_p of size $a(u)$. Hence probability of landing in this set is $\frac{a(u)}{p} \approx \frac{1}{2d(u)}$.

Now we choose x and y uniformly at random \mathbb{Z}_p and define the function

$$f_{x,y} : v \mapsto x + vy \pmod{p}$$

Now for any $u, v, \alpha, \beta \in \mathbb{Z}_p$ where $u \neq v$ then there exists exactly one solution to the linear system

$$x + uy = \alpha \quad x + vy = \beta$$

since the matrix $\begin{bmatrix} 1 & u \\ 1 & v \end{bmatrix}$ is invertible and

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & u \\ 1 & v \end{bmatrix}^{-1} \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Therefore

$$\begin{aligned}
\Pr_{x,y \in \mathbb{Z}_p} [f_{x,y}(u) \in A_u \wedge f_{x,y}(v) \in A_v] &= \Pr_{\substack{\alpha \in A_u \\ \beta \in A_v}} [x + uy = \alpha \wedge x + vy = \beta] \\
&= \frac{1}{p^2} |\{(x, y) \mid x + uy \in A_u \wedge x + vy \in A_v\}| \\
&= \frac{1}{p^2} \sum_{\alpha \in A_u} \sum_{\beta \in A_v} |\{(x, y) \mid x + uy = \alpha \wedge x + vy = \beta\}| \\
&= \frac{1}{p^2} \sum_{\alpha \in A_u} \sum_{\beta \in A_v} 1 \\
&= \frac{1}{p^2} a(u)a(v) = \frac{a(u)}{p} \frac{a(v)}{p} \approx \frac{1}{2d(u)} \frac{1}{2d(v)}
\end{aligned}$$

So we take the family of pairwise independent functions $\mathcal{H} = \{f_{x,y} \mid x, y \in \mathbb{Z}_p\}$. We can construct this family with only $2 \log p = O(\log n)$ random bits (while choosing x, y). Hence there are total $2^{O(\log n)} = n^{O(1)}$ many functions. So $|\mathcal{H}| = n^{O(1)}$.

So we in parallel consider all possible strings of $O(\log n)$ length representing all possible outcomes of the $O(\log n)$ random bits. From each of this string we construct the function in \mathcal{H} and carry on the algorithm deterministically. Since we expect to delete at least a constant fraction of the edges (16 8.9) one of the functions must delete at least that many edges. So we pick the function which deletes the most edges and throw the other parallel computation away and then repeat the whole process. Everything is deterministic and at least a constant fraction of the edges are removed at each stage.

For each stage we choose different the prime p and then do the process as discussed above.

9 Perfect Matching in Bipartite Planer Graph

References

- [Ajt83] M. Ajtai. “ Σ_1^1 -Formulae on finite structures”. In: *Annals of Pure and Applied Logic* 24.1 (1983), pp. 1–48. ISSN: 0168-0072. doi: [https://doi.org/10.1016/0168-0072\(83\)90038-6](https://doi.org/10.1016/0168-0072(83)90038-6). URL: <https://www.sciencedirect.com/science/article/pii/0168007283900386>.
- [SV84] Larry Stockmeyer and Uzi Vishkin. “Simulation of Parallel Random Access Machines by Circuits”. In: *SIAM Journal on Computing* 13.2 (1984), pp. 409–422. doi: [10.1137/0213027](https://doi.org/10.1137/0213027). eprint: <https://doi.org/10.1137/0213027>. URL: <https://doi.org/10.1137/0213027>.
- [Bus87] S. R. Buss. “The Boolean Formula Value Problem is in ALOGTIME”. In: *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*. STOC ’87. New York, New York, USA: Association for Computing Machinery, 1987, pp. 123–131. ISBN: 0897912217. doi: [10.1145/28395.28409](https://doi.org/10.1145/28395.28409). URL: <https://doi.org/10.1145/28395.28409>.
- [MC89] David A. Mix Barrington and James Corbett. “On the relative complexity of some languages in NC¹”. In: *Information Processing Letters* 32.5 (1989), pp. 251–256. ISSN: 0020-0190. doi: [https://doi.org/10.1016/0020-0190\(89\)90052-5](https://doi.org/10.1016/0020-0190(89)90052-5). URL: <https://www.sciencedirect.com/science/article/pii/0020019089900525>.
- [KR90] Richard M. KARP and Vijaya RAMACHANDRAN. “CHAPTER 17 - Parallel Algorithms for Shared-Memory Machines”. In: *Algorithms and Complexity*. Ed. by JAN VAN LEEUWEN. Handbook of Theoretical Computer Science. Amsterdam: Elsevier, 1990, pp. 869–941. ISBN: 978-0-444-88071-0. doi: <https://doi.org/10.1016/B978-0-444-88071-0.50022-9>. URL: <https://www.sciencedirect.com/science/article/pii/B9780444880710500229>.
- [Vol99] Heribert Vollmer. “Relations to Other Computation Models”. In: *Introduction to Circuit Complexity: A Uniform Approach*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 35–78. ISBN: 978-3-662-03927-4. doi: [10.1007/978-3-662-03927-4_3](https://doi.org/10.1007/978-3-662-03927-4_3). URL: https://doi.org/10.1007/978-3-662-03927-4_3.
- [Pad11] “Ajtai–Komlós–Szemerédi Sorting Network”. In: *Encyclopedia of Parallel Computing*. Ed. by David Padua. Boston, MA: Springer US, 2011, pp. 16–16. ISBN: 978-0-387-09766-4. doi: [10.1007/978-0-387-09766-4_2379](https://doi.org/10.1007/978-0-387-09766-4_2379). URL: https://doi.org/10.1007/978-0-387-09766-4_2379.
- [GL18] Moses Ganardi and Markus Lohrey. “A Universal Tree Balancing Theorem”. In: *ACM Trans. Comput. Theory* 11.1 (Oct. 2018). ISSN: 1942-3454. doi: [10.1145/3278158](https://doi.org/10.1145/3278158). URL: <https://doi.org/10.1145/3278158>.