Lecture 9: Quantitative thinking

Combinatorial Methods (Winter 2023)
University of Toronto
Swastik Kopparty
Scribes: Mingxuan Teng, Elnaz Hessami Pilehrood

1 Counting distinct numbers in a multiplication table

1.1 Summary

By saying quantitative thinking, we want to gain a sense of counting. However, in many cases, it would be so difficult to count the precise number of objects. In those cases, we want to get a well estimation of the number of objects. So in the first half of the lecture, we attacked a famous problem, namely Erdős multiplication table problem, to try to "count" the number of distinct integers in a multiplication table.

Note that a multiplication table is simply that:

*	1	2	3	...
1	1	2	3	...
2	2	4	6	...
3	3	6	9	...

But before that, we first look at the prime number theorem

Theorem 1. *The prime number theorem states that* $\pi(N) \sim \frac{N}{log(N)}$

Definition 2. *$A(n)$ represents the number of distinct integers less than or equal to n^2.*

Definition 3. *$\omega(n)$ represents the number of distinct primes less than or equal to n.*

Since ω(n) is very hard to estimate, instead we try to estimate the average of it.

$$
\begin{aligned}
\frac{1}{N}\sum_{n}^{N}\omega(n) &= \frac{1}{N}\sum_{P}^{N}\lfloor\frac{N}{P}\rfloor \\
&= \frac{1}{N}\sum_{P}^{N}\frac{N}{P} + O(1) \\
&= \sum_{P}^{N}\frac{1}{P} + O(\frac{1}{N}\sum_{P}^{N}1) \\
&\approx log(log(N) + O(\frac{\pi(N)}{N}) \approx log(log(N) + O(1)
\end{aligned}
$$

Note that P represents for prime numbers.

Fact 4. *For almost all $n \leq N^2, \omega(n) = log(log(N))$*

We used this fact to estimate A(n), we want to show $A(n) = O(n^2)$. However, before that, if we consider the following problem:

Problem 1. *Consider $\omega(ab), ab \leq N^2, a \in [\sqrt{N}, N], b \in [\sqrt{N}, N]$*

$$\omega(ab) = \omega(a) + \omega(b) = log(log(N)) + log(log(N)) = 2log(log(N)) \tag{1}$$

Then this seems a contradiction to the above fact that for almost all $n \leq N^2, \omega(n) = log(log(N))$, why? Because $\omega(n)$ is additive but not complete additive, so we can't simply add $\omega(a)$ and $\omega(b)$ to get $\omega(ab)$, as that would cause repeated counting if a is not relatively prime to b. Hence we want to look at a simpler problem.

Definition 5. *A*(n): for $n \leq N, n = a * b, s.t (a, b) = 1$*

Fact 6.

$$A * (n) = O(N^2)$$

Theorem 7.

$$A * (n) = O(N^2) \implies A(n) = O(N^2)$$

Proof. Step1: for all $n \in A(N), n = ab$, we have n* $= \frac{a}{gcd(a,b)} * \frac{b}{gcd(a,b)}$ Then we want to look at A*$(\frac{N}{gcd(a,b)^2})$, we have $A(n) \leq \sum_d^N$ A*$(\frac{N}{d})$, where d is the common factor of a, b.

Step2: By the fact above, we know that $\forall \epsilon > 0, \exists \beta > 0, s.t$ A*(M) $\leq \epsilon M^2$. Fix ϵ, β, we have A*$(\frac{N}{d}) = \sum_d^{\frac{N}{\beta}}$ A*$(\frac{N}{d}) + \sum_{d \geq \frac{N}{d}}^N$ A*$(\frac{N}{d})$. Then we have A*$(\frac{N}{d}) \leq \sum_d^{\frac{N}{\beta}} \frac{N^2}{d^2} + \sum_{d \geq \frac{N}{d}}^N \frac{N^2}{d^2}$. Then we have A*$(\frac{N}{d}) \leq \epsilon N^2 \sum_d^{\frac{N}{\beta}} \frac{1}{d^2} + N^2 \sum_{d \geq \frac{N}{d}}^N \frac{1}{d^2}$, where $\epsilon N^2 \sum_d^{\frac{N}{\beta}} \frac{1}{d^2}$ is a constant which equals to $\epsilon N^2 * \frac{\pi^2}{6}$ and $N^2 \sum_{d \geq \frac{N}{d}}^N \frac{1}{d^2} \leq N^2 * N * \frac{\beta}{N^2} = N^2 * \frac{\beta}{N}$. Hence the whole equation is $O(N^2)$. $\square$

2 Counting distinct numbers in an addition table

2.1 Summary

Now what if instead of the multiplication table we looked at the addition table:

+	1	2	3	...
1	2	3	4	...
2	3	4	5	...
3	4	5	6	...

How many different numbers are in this table? We have $|[N]+[N]| = 2N-1$, counting the numbers from 2 to $2N$.
What about a subtraction table? We have $|[N]-[N]| = 2N-1$, counting the numbers from $1-N$ to $N-1$.

Let G be a finite abelian group with $+$, and a subset $H \subseteq G$. If $H \leq G$, then we have that $|H+H| = |H|$. Can we think of another subset H' of G such that $|H'+H'| = |H'|$?

Claim 1: Suppose $|H+H| = |H|$, then H is a coset.

Proof: If $0 \in H$, then $H \subseteq H+H$, so $H+H = H$. If $0 \notin H$, then we can shift to get

$$|(H-h)+(H-h)| = |H+H| = |H| = |H-h|.$$

Claim 2: Suppose $|H-H| < \frac{3}{2}|H|$. Then, $H-H$ is a subgroup.

Proof: First we will prove that $\forall x \in H-H$, $|H \cap (H+x)| > \frac{1}{2}|H|$. We will prove this by contradiction: suppose there exists $x \in H-H$ such that $|H \cap H+x| \leq \frac{1}{2}|H|$. If $y \notin H \cap (H+x)$, then $y \in H$ and $y \notin H+x$. This means $\forall z \in H$, $y \neq z+x$. Then $y \neq z+a-b$ and $y-a \neq z-b$ for some $a, b \in H$ and all $z \in H$. We have $|H|$ choices for z and $\geq \frac{1}{2}|H|$ choices for y, which is a contradiction.

Now to prove the claim, note that $\forall x, y \in H-H$, $(H+x) \cap (H+y) \neq \emptyset$. Consider z such that $z \in H+x$ and $z \in H+y$. This means $z = k+x = k'+y$, where $k, k' \in H$. So, $x-y = k'-k \in H-H$.

Freiman-Ruzsa: Suppose we have a finite $A \subseteq \mathbb{Z}$ and $|A+A| = O(|A|)$, then A is a generalized arithmetic progression.

Consider $2^{[N]} = \{2^0, 2^1, 2^2, ..., 2^{N-1}\}$; we have $|2^{[N]} \cdot 2^{[N]}| = 2N-1$. For most sets, $|A+A| \approx |A|^2$ and $|A \cdot A| \approx |A|^2$.

Erdos-Szemeredi Theorem: For any $A \subseteq \mathbb{Z}$, we have

$$\max\{\ |A+A|\ ,\ |A \cdot A|\ \}\ >>\ |A|^{2-o(1)}$$

where $o(1) \to 0$ as $|A| \to \infty$.

Solymosi (2009): Given two finite sets of positive real numbers A and B, we have

$$|A \cdot B| \cdot |A+A| \cdot |B+B|\ >>\ \frac{|A|^2|B|^2}{\log(|A| \cdot |B|)}$$

Let $r_{A*B}(x) = |\ \{(a,b) \in A \times B : a*b = x\}\ |$. For example,

$$\sum_{x \in A*B} r_{A*B}(x)\ =\ |A \times B|\ =\ |A| \cdot |B|.$$

$$r_{A*B}(x)^2 \;=\; |\;\{(a,a',b,b') \in A^2 \times B^2 :\; a*b = a'*b' = x\}\;|,$$

and

$$\sum_{x\in A*B} r_{A*B}(x)^2 \;=\; |\;\{(a,a',b,b') \in A^2 \times B^2 :\; a*b = a'*b'\}\;|.$$

Let's look at

$$\Big(\sum_{x\in A\cdot B} r_{A\cdot B}(x)\Big)^2 \;\le\; \Big(\sum_{x\in A\cdot B} r_{A\cdot B}(x)^2\Big)\Big(\sum_{x\in A\cdot B} 1^2\Big),$$

$$|A|^2\;|B|^2 \;\le\; \Big(\sum_{x\in A\cdot B} r_{A\cdot B}(x)^2\Big)\;|A|\cdot|B|.$$

So it is enough to show that $\sum_{x\in A\cdot B} r_{A\cdot B}(x)^2 \;<<\; |A+A|\cdot|B+B|\cdot\log(|A|\cdot|B|)$.

Let $S \;=\; \sum_{x\in A\cdot B} r_{A\cdot B}(x)^2 \;=\; \sum_{x\in B\div A} r_{B\div A}(x)^2$; the left side is counting (a,a',b,b') such that $ab = a'b'$, and the right side is counting (a,a',b,b') such that $\frac{b}{a} = \frac{b'}{a'}$. We have $\max_{x\in B\div A}\; r_{B\div A}(x) \le \min\{|A|,|B|\}$. Write

$$S \;=\; \sum_j \sum_{\substack{2^{j-1}<r(m)\le 2^j\\ m\in B\div A}} r_{B\div A}(x)^2 \;\le\; \log|c| \sum_{\substack{2^{j-1}<r(m)\le 2^j\\ m\in B\div A}} r_{B\div A}(x)^2$$

$$j \;\le\; \log\min\{|A|,|B|\} \;=\; \log|c|$$

it's enough to show that $S \le |A+A|\cdot|B+B|$.

Let $M = \{m_1, m_2, ..., m_l\}$, $m_1 < m_2 < ... < m_l$,

$$S' \;=\; \sum_{i=1}^{l} r_{m_i}(x)^2 \;\le\; \sum_{i=1}^{l} r_{m_i}(x)\cdot r_{m_{i+1}}(x) \;=$$

let $L_{m_i} \;=\;$ lattice points on line slope m_i; if $p \in L_m + L_{m'}$, where $m \ne m'$, $r_{L_m+L_{m'}}(p) = 1$ and $|L_m + L_{m'}| = |L_m|\cdot|L_{m'}|$, so

$$=\; \sum_{i=1}^{l}\; |L_{m_i}|\cdot|L_{m_{i+1}}| \;=\; \sum_{i=1}^{l}\; |L_{m_i} + L_{m_{i+1}}| \;\le$$

$$\le\; |A\times B + A\times B| \;=\; |A+A|\cdot|B+B|.$$