Anuran Makur
18 Sep 2023

5.1 ALGORITHMS:

- **Trial Division:**

Def: An integer $p \in \mathbb{Z}^+, p > 1$ is prime if the only positive integer factors of p are 1 and p.

Ex: 2, 3, 5, 7, 11, 13, 17, 19, ...

Prop: An integer $\overset{P}{p \in \mathbb{Z}^+, p > 1}$ is prime if and only if $\overset{Q}{2, 3, \dots, \lfloor\sqrt{p}\rfloor}$ do not divide p. → vacuously true for $p = 2, 3$

Proof: $(\Rightarrow)$ If p is prime, then $2, \dots, p-1$ do not divide p. So, $2, \dots, \lfloor\sqrt{p}\rfloor$ do not divide p. ← direct proof

$(\Leftarrow)$ If p is $\overset{\neg P}{\text{not}}$ prime, then $\exists k_1, k_2 \in \mathbb{Z}^+$, $1 < k_1, k_2 < p$ such that $\overset{R}{k_1 k_2 = p}$. ← since $k_1, k_2 \in \mathbb{Z}^+$

Assume that $\overset{Q}{2, 3, \dots, \lfloor\sqrt{p}\rfloor}$ do not divide p. Then, $k_1 > \lfloor\sqrt{p}\rfloor$ and $k_2 > \lfloor\sqrt{p}\rfloor$. Hence, $k_1 > \sqrt{p}$ and $k_2 > \sqrt{p}$.

This means that $\overset{\neg R}{k_1 k_2 > \sqrt{p}\sqrt{p} = p}$, which contradicts $\overset{R}{k_1 k_2 = p}$. $\square$

Therefore, one of $2, 3, \dots, \lfloor\sqrt{p}\rfloor$ divides p.

Proof by contradiction
$Q \to P \equiv \neg Q \vee P$
Assume $Q \wedge \neg P \to$ Derive contradiction

5.2 BIG-O:

Prop: Given $f : \mathbb{N} \to \mathbb{R}$ and $g : \mathbb{N} \to \mathbb{R}$, $g(x) \neq 0$, $f(x) = O(g(x))$ if and only if $\underbrace{\overline{\lim_{x\to\infty}}}_{\text{superior limit}} \frac{|f(x)|}{|g(x)|} < \underbrace{+\infty}_{\text{finite}}$.

Note: Can define big-O for any limiting value $x \to a$.

Thm: Let $f : \mathbb{N} \to \mathbb{R}$, $f(n) = \sum_{i=0}^{k} \underbrace{a_i}_{\text{real coefficients}} n^i$ be a polynomial with degree k. Then, $f(n) = O(n^k)$.

Proof: For every $n > 1$,
$$|f(n)| = \left|\sum_{i=0}^{k} a_i n^i\right| \underbrace{\leq}_{\text{triangle inequality}} \sum_{i=0}^{k} |a_i n^i| = \sum_{i=0}^{k} |a_i| n^i \leq \sum_{i=0}^{k} |a_i| n^i \cdot n^{k-i} = n^k \left(\sum_{i=0}^{k} |a_i|\right).$$
Hence, we can use $C = \sum_{i=0}^{k} |a_i|$ in the definition of big-O. $\square$

Prop: Big-O is transitive, i.e., $f(n) = O(g(n))$ and $g(n) = O(h(n)) \Rightarrow f(n) = O(h(n))$.

Proof: Suppose $f(n) = O(g(n))$ and $g(n) = O(h(n))$.
$\exists$ constants C_1, C_2, k_1, k_2 such that $|f(n)| \leq C_1 |g(n)|$ for all $n > k_1$ and $|g(n)| \leq C_2 |h(n)|$ for all $n > k_2$.
Hence, $|f(n)| \leq \underbrace{C_1 C_2}_{\text{new } C} |h(n)|$ for all $n > \underbrace{\max\{k_1, k_2\}}_{\text{new } k}$. $\square$
Thus, $f(n) = O(h(n))$.

Note: Combination rules exist for sums & products of functions.

Anuran Makur
18 Sep 2023

5.3 Complexity:

Prop: Big-Θ is an equivalence relation on the set of functions from $\mathbb{N} \to \mathbb{R}$.

Proof: (Reflexive) $f(n) = \Theta(f(n))$

(Symmetric) $f(n) = \Theta(g(n)) \Rightarrow g(n) = \Theta(f(n))$

(Transitive) $f(n) = \Theta(g(n))$ and $g(n) = \Theta(h(n))$

By transitivity of big-O, $f(n) = O(h(n))$ and $h(n) = O(f(n))$

Hence, $f(n) = \Theta(h(n))$. $\square$

Example 1: (Power Sum) $\sum_{i=1}^{n} i^k = \Theta(n^{k+1})$. $k \in \mathbb{Z}^+$

Proof: For all $n > 1$, $\sum_{i=1}^{n} i^k \leq \sum_{i=1}^{n} n^k = n^{k+1}$.

Hence, $\sum_{i=1}^{n} i^k = O(n^{k+1})$. [Big-O]

For all $n > 2$,
$$\sum_{i=1}^{n} i^k \geq \sum_{i=\lceil \frac{n}{2} \rceil}^{n} i^k \geq \underbrace{\sum_{i=\lceil \frac{n}{2} \rceil}^{n}}_{\geq \frac{n}{2} \text{ terms}} \left(\frac{n}{2}\right)^k \geq \left(\frac{n}{2}\right)\left(\frac{n}{2}\right)^k = \left(\frac{n}{2}\right)^{k+1}.$$

Hence, $\sum_{i=1}^{n} i^k = \Omega(n^{k+1})$. [Big-$\Omega$] $\square$

Example 2: $\log(n!) = \Theta(n \log(n))$. base 2

Proof: For $n > 1$, $n! \leq n^n$

$\Rightarrow \log(n!) \leq n \log(n)$

Hence, $\log(n!) = O(n \log(n))$. [Big-O]

For $n > 2$,
$$\log(n!) = \sum_{i=1}^{n} \log(i) \geq \sum_{i=\lceil \frac{n}{2} \rceil}^{n} \log(i) \geq \underbrace{\sum_{i=\lceil \frac{n}{2} \rceil}^{n}}_{\geq \frac{n}{2} \text{ terms}} \log\left(\frac{n}{2}\right) \geq \frac{n}{2} \log\left(\frac{n}{2}\right) = \frac{n \log(n)}{2} - \frac{\log(2)}{2} n.$$

For $n > 4$, $\frac{\log(2)}{2} n \leq \frac{n \log(n)}{4}$ $\left[\Leftrightarrow 2n \leq n \log(n) \Leftrightarrow 2 \leq \log(n) \Leftrightarrow 4 \leq n\right]$.

Thus, for $n > 4$, $\log(n!) \geq \frac{1}{2} n \log(n) - \frac{1}{4} n \log(n) = \frac{1}{4} n \log(n)$.

Hence, $\log(n!) = \Theta(n \log(n))$. [Big-$\Omega$] $\square$

Example 3: (Stirling's approximation)

$$\lim_{n \to \infty} \frac{n!}{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n} = 1.$$

Hence, $n! = \Theta\left(\sqrt{n} \left(\frac{n}{e}\right)^n\right)$.

Anuran Makur
25 Sep 2023

Practice Problems 1 Solutions:

1. $$\begin{aligned}(\neg Q\vee\neg P)\to(P\wedge Q) &\equiv \neg(Q\wedge P)\to(P\wedge Q) && \text{[De Morgan's Law]}\\ &\equiv \neg(P\wedge Q)\to(P\wedge Q) && \text{[Commutative Law]}\\ &\equiv (P\wedge Q)\vee(P\wedge Q) && \text{[Conditional-Disjunction Equivalence]}\\ &\equiv P\wedge Q && \text{[Idempotent Law]}\end{aligned}$$

$$\begin{aligned}[(\neg Q\vee\neg P)\to(P\wedge Q)]\to Q &\equiv (P\wedge Q)\to Q && \text{[above proof]}\\ &\equiv \neg(P\wedge Q)\vee Q && \text{[Conditional-Disjunction Equivalence]}\\ &\equiv (\neg P\vee\neg Q)\vee Q && \text{[De Morgan's Law]}\\ &\equiv \neg P\vee(\neg Q\vee Q) && \text{[Associative Law]}\\ &\equiv \neg P\vee T && \text{[Negation Law]}\\ &\equiv T && \text{[Domination Law]}\end{aligned}$$

Hence, tautology.

2. $$\underbrace{(p\vee q\vee r)}_{T}\wedge\underbrace{(\neg p\vee\neg q\vee\neg r)}_{T}$$ and for satisfiability

So, one of p,q,r is T and one of $\neg p,\neg q,\neg r$ is T.

Let $p=T$ and $q=F$. Then, $(p\vee q\vee r)\wedge(\neg p\vee\neg q\vee\neg r)=T$.

Hence, satisfiable with assignment $p=T, q=F, r=T$.

3. $\forall x\,(P(x)\vee Q(x))\not\equiv\forall x\,P(x)\vee\forall x\,Q(x)$

Domain $=\mathbb{Z}$, $P(x)=$ "x is even", $Q(x)=$ "x is odd"

$\forall x\,(P(x)\vee Q(x))$ is true.

$\forall x\,P(x)$ and $\forall x\,Q(x)$ are false.

$\exists x\,(P(x)\vee Q(x))\equiv\exists x\,P(x)\vee\exists x\,Q(x)$

Pf: Suppose $\exists x\,(P(x)\vee Q(x))$ is true. Then for some a in the domain, $P(a)$ is true or $Q(a)$ is true.
If $P(a)$ is true, then $\exists x\,P(x)$. If $Q(a)$ is true, then $\exists x\,Q(x)$ is true.
So, $\exists P(x)$ or $\exists x\,Q(x)$ is true, i.e., $\exists x\,P(x)\vee\exists x\,Q(x)$.

Suppose $\exists x\,P(x)\vee\exists x\,Q(x)$ is true. Then, $\exists x\,P(x)$ or $\exists x\,Q(x)$ is true.
If $\exists x\,P(x)$ is true, then there is some a in the domain so that $P(a)$ is true.
Hence, $P(a)\vee Q(a)$ is true. Thus, $\exists x\,(P(x)\vee Q(x))$ is true.
If $\exists x\,Q(x)$ is true, then there is some a in the domain so that $Q(a)$ is true.
Hence, $P(a)\vee Q(a)$ is true. Thus, $\exists x\,(P(x)\vee Q(x))$ is true. $\square$

Anuran Makur
25 Sep 2023

4. <u>Prop:</u> Given $n \in \mathbb{Z}$, n is even iff n^2+1 is odd.

<u>Pf:</u> ($\Rightarrow$) n is even $\Rightarrow n = 2k$ for some $k \in \mathbb{Z}$

$$\Rightarrow n^2+1 = 4k^2+1 = 2\underbrace{(2k^2)}_{\in \mathbb{Z}}+1$$

$\Rightarrow n^2+1$ is odd.

($\Leftarrow$) We prove this by contraposition.

n is odd $\Rightarrow n = 2k+1$ for some $k \in \mathbb{Z}$

$$\Rightarrow n^2+1 = (2k+1)^2+1 = 4k^2+4k+1+1 = 2\underbrace{(2k^2+2k+1)}_{\in \mathbb{Z}}$$

$\Rightarrow n^2+1$ is even. $\square$

5. a) False

b) False $\quad (2^B = \mathcal{P}(B) = \{\emptyset, \{3\}, \{A\}, B\})$ ← power set

c) True $\quad |2^A| = |2^B| = 4$

d) True $\quad$ <u>Prop:</u> $A \subseteq B \Rightarrow A \times C \subseteq B \times C$.

<u>Pf:</u> Suppose $A \subseteq B$. Consider $(a,c) \in A \times C$.
Then $a \in B$ since $A \subseteq B$. Hence, $(a,c) \in B \times C$. $\square$
Thus, $A \times C \subseteq B \times C$.

6. a) $f: A \to B$, $f(1) = x$, $f(2) = y$, $f(3) = x$

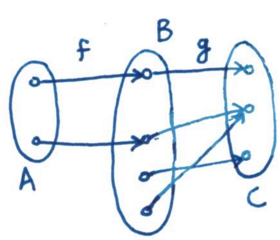
b) $f: B \to A$, $f(x) = 1$, $f(y) = 2$

c) $f: A \to A$, $f(t) = t$

d) No. <u>Pf:</u> Assume $f: A \to B$ is a bijection. Then f is one-to-one.
Since $|B| = 2$, but $|A| = 3$, one of the elements of B must have more than one preimage in A. ← Pigeonhole principle
Hence, f is not one-to-one. Contradiction! $\square$
So, f is not bijective.

e) $\left.\begin{array}{l} f_1: C \to B,\ f_1(5) = x \\ f_2: C \to B,\ f_2(5) = y \end{array}\right\}$ There are 2 functions.

7. No.



Here, f is injective and g is surjective, f is not surjective and g is not injective.
$|A| = 2 < 3 = |C|$.

8. <u>Reflexive:</u> $\forall a \in \mathbb{N}$, $a \leq a^2$ (True)

<u>Symmetric:</u> $\underset{1 \leq 2^2}{(1,2) \in R}$ but $\underset{2 > 1^2}{(2,1) \notin R}$ (False)

<u>Transitive:</u> $\underset{8 \leq 3^2}{(8,3) \in R}$ and $\underset{3 \leq 2^2}{(3,2) \in R}$ but $\underset{8 > 2^2}{(8,2) \notin R}$ (False)

} <u>Not equivalence relation.</u>

9. $$\begin{aligned} a_n &= 2a_{n-1} - n \\ &= 2(2a_{n-2} - (n-1)) - n \\ &= 2^2 a_{n-2} - (n + 2(n-1)) \\ &= 2^2(2a_{n-3} - (n-2)) - (n + 2(n-1)) \\ &= 2^3 a_{n-3} - (n + 2(n-1) + 2^2(n-2)) \\ &\vdots \\ &= 2^k a_{n-k} - \sum_{i=0}^{k-1}(n-i)2^i \\ &\vdots \\ (\text{set } k=n) &= 2^n a_0 - \sum_{i=0}^{n-1}(n-i)2^i \quad , \text{ where } a_0 = 1 \end{aligned}$$

$$a_n = 2^n - n\sum_{i=0}^{n-1}2^i + \sum_{i=0}^{n-1} i2^i \underset{\uparrow \text{ use } [*]}{=} 2^n - (2^n - 1)n + (n-2)2^n + 2$$

$$\boxed{a_n = n + 2 - 2^n}, \quad n \in \mathbb{N}$$

Let $S_n = \sum_{i=0}^{n-1} i2^i \Rightarrow 2S_n = \sum_{i=0}^{n-1} i2^{i+1} = \sum_{i=1}^{n}(i-1)2^i = \sum_{i=1}^{n} i2^i - \sum_{i=1}^{n} 2^i$

$$= \sum_{i=0}^{n-1} i2^i + n2^n - 2(2^n - 1)$$

$$= S_n + (n-2)2^n + 2$$

$$\Rightarrow \underline{\underline{S_n = (n-2)2^n + 2}} \quad [*]$$

10. $$\sum_{i=1}^{k}\sum_{j=1}^{n}(j-2) = \sum_{i=1}^{k}(-1+0+1+\cdots+n-2) = \sum_{i=1}^{k}\frac{n(n-3)}{2} = \boxed{\frac{kn(n-3)}{2}}$$

$$\sum_{i=1}^{10}(2^i + (-2)^i) = \sum_{i=1}^{10}2^i + \sum_{i=1}^{10}(-2)^i = \frac{2(2^{10}-1)}{(2-1)} + \frac{(-2)((-2)^{10}-1)}{(-2-1)} = 2^{11} - 2 + \frac{2}{3}(2^{10}-1) = \frac{4}{3}\cdot 2^{11} - \frac{8}{3} = \frac{8184}{3} = \boxed{2728}$$

11. $$\sum_{j=1}^{n}\sum_{k=1}^{j} 1 = \sum_{j=1}^{n} j = \frac{n(n+1)}{2} = \boxed{O(n^2)} \quad (\text{also } \Theta(n^2))$$

12. $$f(n) = \frac{n^2}{n+1} + \log_2(n)$$

a) For $n > 1$, $\frac{n^2}{n+1} + \log_2(n) \le \frac{n^2}{n} + n \le 2n \quad (C = 2, k = 1)$

witnesses

Hence, $f(n)$ is $O(n)$.

b) For $n > 1$, $\frac{n^2}{n+1} + \log_2(n) \geq \frac{n^2}{n+1} \geq \frac{n^2}{2n} \geq \frac{n}{2} \quad (C = \frac{1}{2}, k = 1)$

Hence, $f(n)$ is $\Omega(n)$.

Thus, $\underline{\underline{f(n) \text{ is } \Theta(n)}}$.

Anuran Makur
25 Sep 2023

Anuran Makur
2 Oct 2023

Bézout's Identity:

For any $a,b \in \mathbb{Z}$ with $\gcd(a,b)=d$, there exist $s,t \in \mathbb{Z}$ such that $as+bt=d$.
Moreover, the integers of the form $as+bt$ with $s,t \in \mathbb{Z}$ are the multiples of d.

Proof:

Let k be the smallest positive integer that is a linear combination of a and b.
$\uparrow$ k exists by well-ordering principle

$k = am+bn$ for some $m,n \in \mathbb{Z}$
By division algorithm, $a = kq+r$ for some $q \in \mathbb{Z}$ and $r \in \{0,\dots,k-1\}$.
Hence, $r = a-kq = a-(am+bn)q = a(1-mq)+b(-nq)$.
Since k is the smallest such positive integer, $r=0$.
Hence, $k|a$. Similarly, $k|b$.
Thus, k is a common divisor of a and b.

Since $d|a$ and $d|b$, $d \mid am+bn = k$. So, $d \leq k$.
Hence, $k=d$ since $d=\gcd(a,b)$.

$\rightarrow$ This proves: $\exists s,t \in \mathbb{Z}$, $as+bt=\gcd(a,b)$
and $\gcd(a,b)$ is the smallest positive integer that is a linear combination of a and b.

Clearly, as $d=am+bn$, $du = amu+bnu$ for all $u \in \mathbb{Z}$.
So, all multiples of d can be represented as linear combinations of a and b.
Suppose there is a non-multiple, $dq+r$, with $q \in \mathbb{Z}$, $r \in \{1,\dots,d-1\}$, so that

$$dq+r = as+bt \quad \text{for some } s,t \in \mathbb{Z}$$

$$\Rightarrow \quad r = as+bt-(am+bn)q = a(s-mq)+b(t-nq)$$

This contradicts d being the smallest positive integer that is a linear combination of a and b.

$\rightarrow$ This proves: $\{as+bt : s,t \in \mathbb{Z}\} = \{du : u \in \mathbb{Z}\}$.

$\square$

Anuran Makur
16 Oct 2023

Example of Recursion:

$f(0) = 3$, $f(n+1) = 2f(n) + 3$ for $n \in \{0, 1, 2, \dots\}$ ← definition

$\Rightarrow$ $f(n) = 3 \cdot 2^{n+1} - 3$ for $n \in \{0, 1, 2, \dots\}$ ← closed-form formula

① Proof by backward substitution:

$$
\begin{aligned}
f(n+1) &= 2f(n) + 3 \\
&= 2[2f(n-1) + 3] + 3 \\
&= 2^2 f(n-1) + 3 + 3\cdot 2 \\
&= 2^2[2f(n-2) + 3] + 3 + 3\cdot 2 \\
&= 2^3 f(n-2) + 3 + 3\cdot 2 + 3\cdot 2^2 \\
&\ \ \vdots \\
&= 2^{k+1} f(n-k) + 3\sum_{i=0}^{k} 2^i && [k \in \{0, \dots, n\}] \\
&= 2^{k+1} f(n-k) + 3(2^{k+1} - 1) && [\text{geometric series}] \\
&= 2^{n+1} f(0) + 3(2^{n+1} - 1) && [k = n] \\
&= 3\cdot 2^{n+1} + 3\cdot 2^{n+1} - 3 \\
&= 3\cdot 2^{n+2} - 3
\end{aligned}
$$

Hence, $f(n) = 3\cdot 2^{n+1} - 3$ for $n \in \{0, 1, 2, \dots\}$. $\square$

② Proof by induction:

Basis step: $(n=0)$ $f(0) = 3\cdot 2^1 - 3 = 3$

Inductive step: For any $k \in \{0, 1, 2, \dots\}$, assume that $\underbrace{f(k) = 3\cdot 2^{k+1} - 3}_{\text{inductive hypothesis}}$.

$$
\begin{aligned}
f(k+1) &= 2f(k) + 3 && [\text{recursive formula}] \\
&= 2[3\cdot 2^{k+1} - 3] + 3 && [\text{by inductive hyp.}] \\
&= 3\cdot 2^{k+2} - 3 .
\end{aligned}
$$

Hence, $f(k) = 3\cdot 2^{k+1} - 3 \Rightarrow f(k+1) = 3\cdot 2^{k+2} - 3$.

$\therefore$ By induction, $f(n) = 3\cdot 2^{n+1} - 3$ for all $n \in \{0, 1, 2, \dots\}$. $\square$

Anuran Makur
25 Oct 2023

<u>NOTE:</u> Remainders of $\underbrace{11\cdots1}_{k+1 \text{ digits}}$ when divided by 6.

$$\underbrace{11\cdots1}_{k+1 \text{ digits}} = \sum_{i=0}^{k} 10^i \quad \text{for } k \geq 0$$

Observe that
$$10^0 \equiv 1 \pmod 6$$
$$10^1 \equiv 4 \pmod 6$$
$$10^2 \equiv 4 \pmod 6$$
$$\vdots$$

By induction, one can show that $10^i \equiv 4 \pmod 6$ for $i \geq 1$.

Hence, $\displaystyle\sum_{i=0}^{k} 10^i \equiv 1 + 4k \pmod 6$ for $k \geq 0$.

Clearly, $1 + 4k \equiv 1 + 4(k+3) \pmod 6$ for $k \geq 0$.

$\therefore$ The values of $\underbrace{111\cdots1}_{k+1 \text{ digits}}$ mod 6 will cycle with <u>period</u> 3.

Evaluating for $k = 0, 1, 2$, we have :
$$1 \bmod 6 = 1$$
$$11 \bmod 6 = 5$$
$$111 \bmod 6 = 3$$

$$\therefore \quad \boxed{\underbrace{11\cdots1}_{k+1 \text{ digits}} \bmod 6 = \begin{cases} 1, & k \equiv 0 \pmod 3 \\ 5, & k \equiv 1 \pmod 3 \\ 3, & k \equiv 2 \pmod 3 \end{cases}}$$

Anuran Makur
1 Nov 2023

Practice Problems 2 Solutions:

1. <u>Prop:</u> Given $a,b,c \in \mathbb{Z}$ with $a \neq 0$, if $a \mid b$ and $a \mid c$, then $a \mid bm+cn$ for all $m,n \in \mathbb{Z}$.

<u>Proof:</u> $a \mid b \Rightarrow b = ax$ for some $x \in \mathbb{Z}$

$a \mid c \Rightarrow c = ay$ for some $y \in \mathbb{Z}$

Hence,
$$\begin{aligned} bm + cn &= (ax)m + (ay)n \\ &= a(xm) + a(yn) \\ &= a\underbrace{(xm+yn)}_{\in \mathbb{Z}}, \quad \text{for all } m,n \in \mathbb{Z}. \end{aligned}$$

Thus, $a \mid bm+cn$ for all $m,n \in \mathbb{Z}$. $\square$

2. First note that $1! \equiv 1 \pmod 2$ and $n! = n(n-1)\cdots 3\cdot \underline{\underline{2}}\cdot 1 \equiv 0 \pmod 2$ for $n > 1$.

So, $\sum_{n=1}^{k} n! \equiv 1 \pmod 2$ for all $k \geq 1$.

$$\sum_{i=1}^{4m} i \overset{\text{arithmetic series}}{=} \underline{\underline{2}}m(4m+1) \equiv 0 \pmod 2 \text{ for all } m \geq 1.$$

Hence, $\boxed{\left(\sum_{n=1}^{k} n! + \sum_{i=1}^{4m} i\right) \bmod 2 = 1}$ for all $k,m \geq 1$.

3. Division algorithm:

$716 = 512(1) + 204$
$512 = 204(2) + 104$
$204 = 104(1) + 100$
$104 = 100(1) + 4$
$100 = 4(25) + 0$

Euclidean algorithm:
$$\begin{aligned} &\gcd(716,512) \\ &= \gcd(512,204) \\ &= \gcd(204,104) \\ &= \gcd(104,100) \\ &= \gcd(100,4) \\ &= \gcd(4,0) \\ &= \underline{\underline{4}} \end{aligned}$$

$\therefore \boxed{\gcd(716,512) = 4}$

4. <u>Prime factorizations:</u> $p^n = p^n$

$p^m = p^m$

$$\Rightarrow \boxed{\gcd(p^n, p^m) = p^{\min\{m,n\}}}$$

(Recall: Given $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, $\gcd(a,b) = p_1^{\min\{e_1,f_1\}} p_2^{\min\{e_2,f_2\}} \cdots p_k^{\min\{e_k,f_k\}}$.)

Anuran Makur
1 Nov 2023

5. **Bézout's Theorem:**

Given positive integers $a, b \in \mathbb{Z}$, the following are true:

1) $\gcd(a,b) = sa + tb$ for some integers $s, t \in \mathbb{Z}$ (called Bézout coefficients);
2) $\gcd(a,b)$ is the smallest positive integer that is a linear combination of a, b;
3) $\{as + bt : s, t \in \mathbb{Z}\} = \{\gcd(a,b)m : m \in \mathbb{Z}\}$.

The linear combinations of a,b are the multiples of $\gcd(a,b)$.

Since $\gcd(6,9) = 3$, by Bézout's Theorem, $6x + 9y = 3$ admits integer solutions x, y.

Bézout coefficients

By observation, $\boxed{x = -1 \text{ and } y = 1}$ is a solution.

Alternatively, we can find x, y systematically:

Euclidean algorithm:

[*] $9 = 6(1) + \underline{3}$
$6 = 3(2) + 0$

$\gcd(9,6) = \gcd(6,3) = \gcd(3,0) = \underline{\underline{3}}$

Backward substitution:

[*] $3 = 9 - 6 = 6(-1) + 9(1)$

$\therefore \boxed{x = -1 \text{ and } y = 1}$

6. Since $\gcd(5,14) = 1$, by Bézout's Theorem, $5x + 14y = 1$ admits integer solutions x, y.
The Bézout coefficient x is the inverse of 5 modulo 14 as $5x \equiv 1 \pmod{14}$.
By observation, $\boxed{x = 3 \text{ and } y = -1}$ is a solution.

Alternatively, we can find x, y systematically:

Euclidean algorithm:

[1] $14 = 5(2) + 4$
[2] $5 = 4(1) + \underline{1}$
$4 = 1(4) + 0$

$\gcd(14,5) = \gcd(5,4) = \gcd(4,1) = \gcd(1,0) = \underline{\underline{1}}$

Backward substitution:

[2] $1 = 5 - 4 \Rightarrow 1 = 5 - (14 - 5(2))$
[1] $4 = 14 - 5(2)$ $\quad = 5(3) + 14(-1)$

$\therefore \boxed{x = 3 \text{ and } y = -1}$

Hence, 3 is the inverse of 5 modulo 14, because $\gcd(5,14) = 1$ and Bézout's Theorem guarantees the existence of the inverse.

Anuran Makur
1 Nov 2023

7. **Prop:** $\displaystyle\sum_{i=0}^{n-1} \frac{i}{2^i} = 2 - \frac{n+1}{2^{n-1}}$ for all $n \geq 1$.

Proof:

Basis step: If $n=1$, $\displaystyle\sum_{i=0}^{1-1} \frac{i}{2^i} = \frac{0}{2^0} = \underline{0}$ and $\displaystyle 2 - \frac{1+1}{2^{1-1}} = 2 - \frac{2}{1} = \underline{0}$. Hence, $\displaystyle\sum_{i=0}^{1-1} \frac{i}{2^i} = 2 - \frac{1+1}{2^{1-1}}$ for $n=1$.

Inductive Hypothesis: Fix any arbitrary integer $k \geq 1$. Assume that $\displaystyle\sum_{i=0}^{k-1} \frac{i}{2^i} = 2 - \frac{k+1}{2^{k-1}}$.

Inductive step: We want to show that $\displaystyle\sum_{i=0}^{k} \frac{i}{2^i} = 2 - \frac{k+2}{2^k}$. ← [proposition at $k+1$]

$$\begin{aligned}
\sum_{i=0}^{k} \frac{i}{2^i} &= \sum_{i=0}^{k-1} \frac{i}{2^i} + \frac{k}{2^k} \\
&= 2 - \frac{k+1}{2^{k-1}} + \frac{k}{2^k} \qquad \text{[by inductive hypothesis]} \\
&= 2 - \frac{2(k+1) - k}{2^k} \\
&= 2 - \frac{k+2}{2^k}
\end{aligned}$$

This completes the inductive step.

$\therefore$ By the principle of mathematical induction, $\displaystyle\sum_{i=0}^{n-1} \frac{i}{2^i} = 2 - \frac{n+1}{2^{n-1}}$ for all $n \geq 1$. $\square$

8. **Prop:** $2n+3 \leq 2^n$ for all $n \geq 4$.

Proof:

Basis step: If $n=4$, $2(4)+3 = \underline{11}$ and $2^4 = \underline{16}$. Hence, $2(4)+3 \leq 2^4$ for $n=4$.

Inductive Hypothesis: Fix any arbitrary integer $k \geq 4$. Assume that $2k+3 \leq 2^k$.

Inductive step: We want to show that $2(k+1)+3 \leq 2^{k+1}$. ← [proposition at $k+1$]

$$\begin{aligned}
2(k+1)+3 &= 2k+5 \\
&= (2k+3)+2 \\
&\leq 2^k + 2 \qquad \text{[by inductive hypothesis]} \\
&\leq 2^k + 2^k \qquad \text{[as } 2 \leq 2^k \text{ for } k \geq 4\text{]} \\
&= 2^{k+1}
\end{aligned}$$

This completes the inductive step.

$\therefore$ By the principle of mathematical induction, $2n+3 \leq 2^n$ for all $n \geq 4$. $\square$

Remark: The proposition is not true for $n < 4$.

Anuran Makur
1 Nov 2023

9. Recurrence relation: $f(1)=2$, $f(2)=1$,
$f(n)=3f(n-1)-2f(n-2)$ for $n\geq 3$

Prop: $f(n)=3-2^{n-1}$ for all $n\geq 1$.

Proof:

Basis step: If $n=1$, $f(1)=\underline{\underline{2}}$ and $3-2^{1-1}=\underline{\underline{2}}$. Hence, $f(1)=3-2^{1-1}$ for $n=1$.

If $n=2$, $f(2)=\underline{\underline{1}}$ and $3-2^{2-1}=\underline{\underline{1}}$. Hence, $f(2)=3-2^{2-1}$ for $n=2$.

Inductive Hypothesis: Fix any arbitrary $k\geq 2$. Assume that $f(j)=3-2^{j-1}$ for all $j\in\{1,2,\dots,k\}$.

We assume all previous propositions although we only use two in the inductive step.

Inductive step: We want to show that $f(k+1)=3-2^{k}$. ← [proposition at k+1]

$$\begin{aligned} f(k+1) &= 3f(k)-2f(k-1) && \text{[recurrence]}\\ &= 3(3-2^{k-1})-2(3-2^{k-2}) && \text{[by inductive hypothesis]}\\ &= (9-6)-3\cdot 2^{k-1}+2\cdot 2^{k-2}\\ &= 3-\tfrac{3}{2}\cdot 2^{k}+\tfrac{1}{2}\cdot 2^{k}\\ &= 3-2^{k} \end{aligned}$$

This completes the inductive step.

∴ By strong induction, $f(n)=3-2^{n-1}$ for all $n\geq 1$. □

10. $S_1=\{1,-2,4,-8,16,-32,\dots\}$ ← powers of -2

The set $S_1\subseteq\mathbb{Z}$ is recursively defined as:

Basis step: $1\in S_1$

Recursive step: If $x\in S_1$, then $-2x\in S_1$.

$S_2=\{a\in\mathbb{Z}\mid a\equiv 3 \pmod 4\}$ ← all integers of the form $4q+3$ for $q\in\mathbb{Z}$

The set $S_2\subseteq\mathbb{Z}$ is recursively defined as:

Basis step: $3\in S_2$

Recursive step: If $x\in S_2$, then $x+4\in S_2$ and $x-4\in S_2$.

11. Let $f:\mathbb{Z}^+\to\{0,1,2,3,4\}$ represent the function computed by func.

For $n\geq 2$, $f(n)=3f(n-1) \bmod 5 = 3(3f(n-2)\bmod 5)\bmod 5 \overset{\uparrow}{=} 3^2 f(n-2)\bmod 5 \overset{\text{Backward substitution}}{=} \cdots = 3^{n-1}f(1)\bmod 5$ ← $f(1)=3$

[ab mod M = (a mod M)(b mod M) mod M]

∴ For $n\geq 1$, $f(n)=\boxed{3^n \bmod 5}$.

$3^0\equiv \underline{1} \pmod 5$, $3^1\equiv 3 \pmod 5$, $3^2\equiv 4\pmod 5$, $3^3\equiv 2 \pmod 5$, $3^4\equiv \underline{1}\pmod 5$, … [cycles…]

$$\therefore\ \boxed{f(n)=\begin{cases}1, & n\equiv 0 \pmod 4\\ 3, & n\equiv 1 \pmod 4\\ 4, & n\equiv 2\pmod 4\\ 2, & n\equiv 3 \pmod 4\end{cases}}\quad \text{for } n\geq 1.$$

Anuran Makur
1 Nov 2023

12\. a) $\dfrac{10}{1}\cdot\dfrac{9}{2}\cdot\dfrac{8}{3}\cdot \cdots \cdot\dfrac{2}{9}\cdot\dfrac{1}{10}$ ← no. of choices / ← position index

$\boxed{10!}$ ways

b) $\underbrace{\dfrac{E}{1}\ \dfrac{E}{2}\ \dfrac{E}{3}\ \dfrac{E}{4}}_{4!}\ \times\ \underbrace{\dfrac{H}{5}\ \dfrac{H}{6}\ \dfrac{H}{7}\ \dfrac{H}{8}\ \dfrac{H}{9}\ \dfrac{H}{10}}_{6!}$ ← no. of permutations

E = easy, H = hard

$\boxed{4!\,6!}$ ways

c) Approach 1: Let N = non-interesting question, I = interesting question

$\underset{1}{\sqcup}\ N\ \underset{2}{\sqcup}\ N\ \underset{3}{\sqcup}\ N\ \underset{4}{\sqcup}\ N\ \underset{5}{\sqcup}\ N\ \underset{6}{\sqcup}\ N\ \underset{7}{\sqcup}\ N\ \underset{8}{\sqcup}\ N\ \underset{9}{\sqcup}$ ← 8 N questions

9 possible positions for interesting questions

No. of ways = $8! \times C(9,2) \times 2! = 8!\cdot P(9,2) = \boxed{8!\cdot 9\cdot 8}$

order the N questions; choose 2 positions for I questions; order the I questions

Approach 2: By Sum rule, $\underbrace{\begin{bmatrix}\text{no. of ways}\\ \text{I questions are}\\ \text{adjacent}\end{bmatrix}}_{X} + \underbrace{\begin{bmatrix}\text{no. of ways}\\ \text{I questions}\\ \text{not adjacent}\end{bmatrix}}_{Y} = \underbrace{\begin{bmatrix}\text{total no.}\\ \text{of ways}\end{bmatrix}}_{=10!}$.

← all ways to order 10 questions

Assume we have 9 objects:

N,N,N,N,N,N,N,N,[II].

group the two I questions

Then,

$X = 9! \times 2!$ ← no. of ways to order 2 I questions in the group

$9!$: no. of ways to order 9 objects

$\therefore\ Y = 10! - X = \boxed{10! - 9!\,2!}$ ways

[Remark: Of course, $8!\cdot 9\cdot 8 = 10! - 9!\,2!$.]

d) Let I = interesting, H = hard but non-interesting, E = easy

Case 1: Block of the form [H I H I H] exists.

No. of ways to order [HIHIH] = $P(4,3)\cdot 2! = 4!\,2!$

No. of ways to order E, E, E, E, H, [HIHIH] = $6!$

⇒ No. of ways with [HIHIH] = $6!\,4!\,2!$

Case 2: Block of the form [HIIH] exists.

No. of ways to order [HIIH] = $P(4,2)\cdot 2! = 4!$

No. of ways to order E, E, E, E, H, H, [HIIH] = $7!$

⇒ No. of ways with [HIIH] = $7!\,4!$

Case 3: 2 blocks of the form [HIH] exist. Let the interesting questions be I_1, I_2.

$\underbrace{\underline{4}\ I_1\ \underline{3}}_{\text{block 1}}\ ,\ \underbrace{\underline{2}\ I_2\ \underline{1}}_{\text{block 2}}$ ← no. of choices for H question

No. of ways to construct blocks = $4!$

No. of ways to order E, E, E, E, $[HI_1H]$, $[HI_2H]$ = $6!$

⇒ No. of ways with $[HI_1H], [HI_2H] = 6!\,4!$

By sum rule, no. of ways = $\underbrace{6!\,4!\,2!}_{\text{case 1}} + \underbrace{7!\,4!}_{\text{case 2}} + \underbrace{6!\,4!}_{\text{case 3}} = 6!\,4!\,(2+7+1) = \boxed{10\cdot 6!\,4!}$

13\. Boxes are colors. Objects are socks. Place a sock in the box corresponding to its color.

By pigeonhole principle, Dirichlet must draw $\boxed{\text{6 socks}}$.

k = 5 boxes, k+1 guarantees a pair

Anuran Makur
8 Dec 2023

Computational linguistics | Theory of computation/ Automata theory | Formal languages

Grammar		Machine/ Automaton (Machine → output; Automaton → no output)		Language		Expressions (→ symbolic, → recursive def.)
Type 0/ Phrase-structured	$\equiv$	Turing machine (D = ND)	$\equiv$	Turing recognizable/ Recursively enumerable		
$\supsetneq$		V		$\supsetneq$		
Type 1/ Context-sensitive	$\equiv$	(Non-deterministic) Linear bounded automaton	$\equiv$	Context-sensitive		
$\supsetneq$		V		$\supsetneq$		
Type 2/ Context-free	$\equiv$	(Non-deterministic) Pushdown automaton (D<ND)	$\equiv$	Context-free	$\equiv$	μ-Regular
$\supsetneq$		V		$\supsetneq$		V
Type 3/ Regular	$\equiv$	Finite-state automaton (D = ND)	$\equiv$	Regular	$\equiv$	Regular

Chomsky-Schützenberger hierarchy

Applications: Computable problems

Applications: Natural languages, compilers and programming languages

Applications: Compilers and programming languages

Applications: Pattern matching in text data

* D = deterministic
* ND = non-deterministic
* D = ND means both machines have same power to accept languages

TABLE OF COMPUTABILITY CONCEPTS

PRACTICE PROBLEMS 3:

Anuran Makur
8 Dec 2023

10) Regex: $\Sigma = \{a, b\}$

Σ-strings with even no. of a's $= b^*(ab^*ab^*)^*$

—— " —— odd —— " —— $= b^*(ab^*ab^*)^*ab^*$

Consider strings on Σ of length $2k$

$\underbrace{\;}_{1}\underbrace{\;}_{2}\underbrace{\;}_{3}\underbrace{\;}_{4}\cdots\underbrace{\;}_{k}$ ← pairs of symbols } Effective alphabet $= \{aa, bb, ab, ba\}$

Define $\underline{A \triangleq ab \cup ba}$ and $\underline{B \triangleq aa \cup bb}$, and let $\hat{\Sigma} = \{A, B\}$.

Equivalently, consider strings on $\hat{\Sigma}$ of length k.

① $\hat{\Sigma}$-strings of length k with even no. of A's $=$ Σ-strings of length $2k$ with even no. of a's and b's

② $\hat{\Sigma}$-strings of length k with odd no. of A's $=$ Σ-strings of length $2k$ with odd no. of a's and b's

} Can prove these

Σ-strings with even no. of a's and odd no. of b's ← length must be $2k+1$

→ Case 1: Start with b. Remaining $2k$-length string has even no. of a's and b's.

→ Case 2: Start with a. Remaining $2k$-length string has odd no. of a's and b's.

Σ-strings with even no. of a's and odd no. of b's

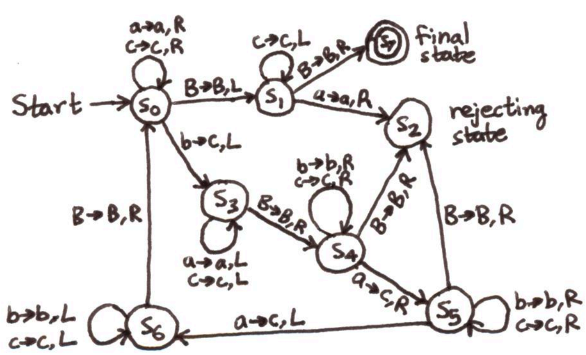
$= \boxed{(b\,B^*(AB^*AB^*)^*) \cup (a\,B^*(AB^*AB^*)^*AB^*)}$, where $A = ab \cup ba$ and $B = aa \cup bb$

8c) $S \to \underline{SUS} \to \underline{TUT}US \to T\underline{Ta}S\,TUS \to TTaSTU \to TTa\underline{SUS}TU \to TTaS\,\underline{TaS}\,STU$

$\to TTaSTaSST \to TTa\underline{SUS}TaSST \to TTa\overset{*}{S}\,\underline{Ta\overset{*}{S}}\,\overset{*}{S}Ta\overset{**}{S}ST \to TTaTaTaT$

aa bb a ab a ba a bb

12)



} Turing machine state diagram