LINEAR RECURRENCE RELATIONS

Def^n: Let $S(\mathbb{C})$ denote the set of all complex valued seq^{ns}.
A linear operator is a mapping $T : S(\mathbb{C}) \to S(\mathbb{C})$, which satisfies for each $\alpha \in \mathbb{C}$

$$T\left(\{x_n\}_{n=0}^{\infty} + \{\alpha y_n\}_{n=0}^{\infty}\right) = T\left(\{x_n\}_{n=0}^{\infty}\right) + \alpha T\left(\{y_n\}_{n=0}^{\infty}\right)$$

The kernel of the operator, denoted as Ker T, is the set

$$\left\{ \{x_n\}_{n=0}^{\infty} \in S(\mathbb{C}) : T\left(\{x_n\}_{n=0}^{\infty}\right) = \{0_n(=0)\}_{n=0}^{\infty} \right\}$$

An eigen vector of the operator T is a non zero seq^n $\{x_n\}_{n=0}^{\infty} \in S(\mathbb{C})$ such that there exist $\alpha \in \mathbb{C}$ with

$$T\left(\{x_n\}_{n=0}^{\infty}\right) = \{\alpha \cdot x_n\}_{n=0}^{\infty}$$

such α is called eigen value of the operator T.

Example: Take $x_0 = 1$, $x_1 = 1$, $x_3 = 3$ and for each integer $n \geq 0$

$$x_{n+3} = 5x_{n+2} - 8x_{n+1} + 4x_n$$

check that $\{x_n\}_{n=0}^{\infty} \longmapsto \{x_{1+n}\}_{n=0}^{\infty}$ is a linear operator
we denote such operator as R., i.e

$$R\left(\{x_n\}_{n=0}^{\infty}\right) = \{x_{1+n}\}_{n=0}^{\infty}$$

check that the aforemention seq^n satisfies

$$R^3\left(\{x_n\}_{n=0}^{\infty}\right) = 5R^2\left(\{x_n\}_{n=0}^{\infty}\right) - 8R\left(\{x_n\}_{n=0}^{\infty}\right) + 4R^0\left(\{x_n\}_{n=0}^{\infty}\right)$$

We may denote R^0 as identity operator I.

i.e $$R^3\left(\{x_n\}_{n=0}^{\infty}\right) = (5R^2 - 8R + 4I)\left(\{x_n\}_{n=0}^{\infty}\right)$$

i.e $$(R^3 - 5R^2 + 8R + 4I)\left(\{x_n\}_{n=0}^{\infty}\right) = \{0_n(=0)\}_{n=0}^{\infty}$$

check that $R^3 - 5R^2 + 8R + 4I$ is a linear operator on $S(\mathbb{C})$.

Def^n: A linear operator $R : S(\mathbb{C}) \to S(\mathbb{C})$ is said to be the right shift operator if $\{x_n\}_{n=0}^{\infty} \longmapsto \{x_{1+n}\}_{n=0}^{\infty}$

i.e $\{x_0, x_1, \ldots\} \longmapsto \{x_1, x_2 \cdots\}$

Example: Let α be a non zero complex number and $\{x_n(=\alpha^n)\}_{n=0}^{\infty}$

Check that $\forall$ positive integer k, $\{x_n(=\alpha^n)\}_{n=0}^{\infty}$ is a eigen vector with eigen value α^k of the right shift operator.

Problem 1: Solve the linear recurrence relation

$$\left.\begin{array}{l} x_0 = 2, \quad x_1 = 5 \quad \text{and } \forall \text{ integer } n \geq 0 \\ x_{n+2} = 5x_{n+1} - 6x_n \end{array}\right\} \text{——} \ (*)$$

Sol^n: We note that $(R^2 - 5R + 6I)(\{x_n\}_{n=0}^{\infty}) = \{O_n(=0)\}_{n=0}^{\infty}$ —— $(**)$

STEP1 : We associate the polynomial $P(x) = x^2 - 5x + 6$
$= (x-2)(x-3)$
with $(**)$ (such polynomial is called characteristic Polynomial with the recurrence relation $(*)$).

STEP2 : Find the roots of the characteristic polynomial:
Here it is 2 and 3.

STEP3 : Formation of general sol^n:
Here it is: $x_n = c_1 2^n + c_2 3^n$, where c_1 & c_2 are complex numbers.

STEP4 : Apply initial conditions of $(*)$ i.e $x_0 = 2$, $x_1 = 5$ to dermine the unique sol^n of $(*)$
Here using $n=0$, we have. $2 = c_1 + c_2$
and using $n=1$, we have $5 = 2c_1 + 3c_2$
Solving c_1 & c_2 we have $c_1 = 1 = c_2$

FINAL: Hence the unique sol^n of $(*)$ is
$x_n = 2^n + 3^n$ $\forall$ non-negative integer n.

Problem 2: Solve the following linear recurrence relation

$$\left.\begin{array}{l} x_0 = 1 \quad , x_1 = 1 \text{ and } \forall \text{ integer } n \geqslant 0 \\ x_{n+3} = 6x_{n+2} - 12x_{n+1} + 8x_n \end{array}\right\} \quad — (+)$$

Sol^n: We note that

$$(R^3 - 6R^2 + 12R - 8I)(\{x_n\}_{n=0}^{\infty}) = \{0_n (=0)\}_{n=0}^{\infty} \quad — (++)$$

STEP1: Identify the characteristic polynomial with the recurrence relation (+).

Here it is $x^3 - 6x^2 + 12x - 8$.

STEP2: Find the roots of the characteristic polynomial

Here, we note that

$$x^3 - 6x^2 + 12x - 8 = 0$$

$$\Leftrightarrow \quad (x-2)^3 = 0$$

i.e here 2 is the only root.

STEP3: Formation of general sol^n

Here it is $\forall$ integer $n \geqslant 0$ $x_n = (c_0 + c_1 n + c_2 n^2)2^n$, where c_0, c_1, c_2, are complex numbers.

STEP4: Apply initial conditions of (+) i.e $x_0 = 1$, $x_1 = 1$ to determine the unique sol^n of (+)

Check that here it is $c_0 = 1$, $c_1 = -\frac{3}{4}$ and $c_2 = \frac{1}{4}$.

FINAL: The unique sol^n of (+) is $\forall$ integer $n \geqslant 0$

$$x_n = 2^n\left(1 - \frac{3}{4}n + \frac{1}{4}n^2\right).$$

Problem 3: Solve the following linear recurrence relation

$$\left.\begin{array}{l} x_0=1,\ x_1=1,\ x_2=3 \text{ and } \forall \text{ integer } n \geq 0 \\ x_{n+3} = 5x_{n+2} - 8x_{n+1} + 4x_n \end{array}\right\} \text{ — } (+)$$

Sol^{n}: We note that

$$(R^3 - 5R^2 + 8R - 4I)(\{x_n\}_{n=0}^{\infty}) = \{0_n(=0)\}_{n=0}^{\infty}$$

STEP 1: Identify the characteristic polynomial with the recurrence relation (+)

Here it is $x^3 - 5x^2 + 8x - 4 = (x-2)^2(x-1)$

STEP 2: Find the roots of the characteristic polynomial

Here we note that

$$x^3 - 5x^2 + 8x - 4 = 0$$

$$(\Rightarrow) \quad (x-2)^2(x-1) = 0$$

i.e Roots are $2, 2, 1$.

STEP 3: Formation of general sol^{n}

Here it is $\forall$ integer $n \geq 0$

$$x_n = (c_0 + c_1 n)2^n + c_3 1^n = (c_0 + c_1 n)2^n + c_3$$

where c_0, c_1, c_3 are complex numbers

STEP 4: Apply initial conditions of (+), i.e $x_0 = 1$, $x_1 = 1$, $x_2 = 3$

Check that here it is $c_0 = -2$, $c_1 = 1$, $c_3 = 3$.

FINAL: The unique sol^{n} of (+) is

$\forall$ integer $n \geq 0$ $\quad x_n = (n-2)2^n + 3$

Example: If $\alpha_1, \alpha_2, \ldots, \alpha_K$ are roots of characteristic polynomial with multiplicity $r_1, r_2, \ldots r_K$ respectively of the linear recurrence relation

$$(R-\alpha_1 I)^{r_1} \circ (R-\alpha_2 I)^{r_2} \circ \cdots \circ (R-\alpha_K I)^{r_K} (\{x_n\}_{n=0}^{\infty}) = \{0_n(=0)\}_{n=0}^{\infty}$$

Then the general sol^{n} is

$$(c_{10} + c_{11} n + \cdots + c_{1r_1} n^{r_1})\alpha_1^n + (c_{20} + c_{21} n + \cdots + c_{2r_2} n^{r_2})\alpha_2^n$$

$$\cdots + (c_{K0} + c_{K1} n + \cdots + c_{Kr_K} n^{r_K})\alpha_K^n$$

Exercise: Solve the following homogeneous linear recurrence relations

(i) $x_0=1,\ x_1=1\ \forall$ integer $n\geq 0$ $\ x_{n+2}+2x_{n+1}+2x_n=0$

(ii) $x_0=3,\ x_1=-3\ \forall$ integer $n\geq 0$ $\ x_{n+2}=6x_{n+1}-9x_n$

(iii) $x_0=6,\ x_1=8\ \forall$ integer $n\geq 0$ $\ x_{n+2}=-4x_{n+1}-4x_n$

(iv) $x_0=6,\ x_1=8\ \forall$ integer $n\geq 0$ $\ x_{n+2}=4x_{n+1}-4x_n$

(v) $x_0=1,\ x_1=2,\ x_2=3,\ \forall$ integer $n\geq 0$ $\ x_{n+3}=9x_{n+2}-27x_{n+1}+27x_n$

NONHOMOGENEOUS RECURRENCE RELATION

Example: (Tower of Hanoi): Consider the recurrence relation

$$x_0=0$$
$$\forall \text{ integer } n\geq 0 \quad x_n=2x_{n-1}+1 \qquad \text{— } (*)$$

Then
$$x_n=2(2x_{n-2}+1)+1=2^2x_{n-2}+2+1$$
$$=2^2(2x_{n-3}+1)+2+1=2^3x_{n-3}+2^2+2+1$$
$$\vdots$$
$$=2^kx_{n-k}+2^{k-1}+2^{k-2}+\cdots+2+1$$
$$\vdots$$
$$=2^nx_0+2^{n-1}+2^{n-2}+\cdots+2+1$$
$$=2^{n-1}+2^{n-2}+\cdots+2+1=\frac{2^n-1}{2-1}=2^n-1$$

The seq^n $\{x_n(=2^n-1)\}_{n=0}^{\infty}$ is a sol^n of the non-homogeneous recurrence relation $(*)$.

Def^n: A k-term recurrence relation is said to be linear non homogeneous if it is of the form

$$x_{n+k}=\alpha_n+\sum_{i=1}^{k}c_i x_{n+k-i} \qquad \text{— } (A)$$

where $\{\alpha_n\}_{n=0}^{\infty}\in S(\mathbb{C})$, $c_i\in\mathbb{C}$ and $x_0,x_1,\ldots,x_{k-1}\in\mathbb{C}$.

Check that (A) can be expresses as

$$P(R)(\{x_n\}_{n=0}^{\infty})=\{\alpha_n\}_{n=0}^{\infty}$$

where $P(R)=R^k-\sum_{i=1}^{k}c_iR^{k-i}$.

Nov 4, 2020 9:30 AM

Problem : Solve the recurrence relation

$$(R-2I)^2(\{x_n\}_{n=0}^{\infty}) = \{\alpha_n(=3^n+2n)\}_{n=0}^{\infty} \quad — \; (+)$$

with initial condition x_0 and x_1

STEP1 : We need to solve

$$(R-2I)^2(\{x_n\}_{n=0}^{\infty}) = \{0_n(=0)\}_{n=0}^{\infty} \quad — \; (**)$$

Since $(**)$ is linear homogeneous recurrence relation we have the general solⁿ of $(**)$ is

$$(c_0+c_1 n)2^n.$$

"Formation of general solⁿ of $(**)$"

STEP 2 : Formation of perticular solⁿ and trial solⁿ of $(+)$

Let $\{y_n\}_{n=0}^{\infty}$ be a perticular solⁿ of $(+)$,

i.e $(R-2I)^2(\{y_n\}_{n=0}^{\infty}) = \{3^n+2n\}_{n=0}^{\infty}$

Suppose $y_n = d_1 3^n + d_2 n + d_3$ ∀ integer $n \geq 0$ (called trial solⁿ).

Then we have

$$\begin{aligned}
3^n+2n &= y_{n+2} - 4y_{n+1} + 4y_n \\
&= (d_1 3^{n+2} + d_2(n+2) + d_3) - 4(d_1 3^{n+1} + d_2(n+1) + d_3) \\
&\quad + 4(d_1 3^n + d_2 n + d_3) \\
&= d_1 3^n(3^2 - 4\cdot 3 + 4) + d_2[n+2-4(n+1)+4n] \\
&\quad + d_3[1-4+4] \\
&= d_1 3^n + d_2 n + (d_3 - 2d_2)
\end{aligned}$$

STEP3 : Formation of particular solⁿ of $(+)$ equating the coefficients with trial solⁿ of +

$d_1 = 1$

$d_2 = 2$

and $d_3 - 2d_2 = 0 \iff d_3 = 2d_2 = 4$

i.e $y_n = 3^n + 2n + 4$ ∀ integer $n \geq 0$

STEP4 : Formation of general solⁿ of $(+)$

Here it is

$$x_n = (c_0 + c_1 n)2^n + 3^n + 2n + 4 \quad \forall \text{ integer } n \geq 0$$

FINAL : Formation of one solⁿ of $(+)$

Determine c_0 & c_1 from the initial conditions x_0 & x_1.

Nov 4, 2020 9:30 AM

Here we list down some trial solⁿ

Given α_n $\forall$ integer $n \geq 0$ k is a positive integer and $c \in \mathbb{C}$	Trial solⁿ
$\alpha_n = c n^k r^n$ Eg. (a) $n r^n$ (b) $n^3 r^n$	$(a_0 + a_1 n + \cdots + a_k n^k) r^n$ where $a_0, \ldots a_k \in \mathbb{C}$ Eg (a) $(a_0 + a_1 n) r^n$ (b) $(a_0 + a_1 n + a_2 n^2) r^n$
$\alpha_n = c n^k r^n$ Here r is one of the root of chracteristic polynomial of the given recurrence relation with multiplicity m. Eg (a) $n r^n$ (b) $n^3 r^n$	$(a_0 + a_1 n + \cdots + a_k n^k) n^m r^n$ where $a_0, a_1 \cdots a_k \in \mathbb{C}$ Eg (a) $(a_0 + a_1 n) n^m r^n$ (b) $(a_0 + a_1 n + a_2 n^2) n^m r^n$
$\alpha_n = c r^n \cos \beta n$ $\beta \in \mathbb{R}$	$a_1 r^n \cos \beta n + a_2 r^n \sin \beta n$ where $a_1, a_2 \in \mathbb{C}$
$\alpha_n = c r^n \sin \beta n$ $\beta \in \mathbb{R}$	$a_1 r^n \cos \beta n + a_2 r^n \sin \beta n$ where $a_1, a_2 \in \mathbb{C}$

Exercise: Solve the non homogencous linear recurrence relation

$x_0 = 1, \; x_1 = 1 \;\; \forall$ integer $n \geq 0$ $\;\; x_{n+2} + 6x_{n+1} + 9x_n = \cos \alpha n$

Nov 4, 2020 9:30 AM

GENERATING FUNCTIONS

Defn: A generating function of the complex valued sequence $\{a_n\}_{n=0}^{\infty}$ is the (formal) power series

$$a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n,$$

denoted as $G_a(x)$.

Comment: The word "formal" means, we shall not bother about the radius of convergence of the above power series $G_a(x)$

Example: (a) $\{1_n (=1)\}_{n=0}^{\infty}$ i.e

$$G_1(x) = 1 + x + x^2 + \cdots \cdots = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$$

(b) $\{e_n (= \frac{1}{n!})\}_{n=0}^{\infty}$ i.e

$$G_e(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots = \sum_{n=0}^{\infty} \frac{x^n}{n!} = e^x$$

(c) For $\{a_n\}_{n=0}^{\infty}$ and $\{b_n\}_{n=0}^{\infty} \in S(\mathbb{C})$.

$$G_{a+b}(x) = G_a(x) + G_b(x) = (G_a + G_b)(x)$$

(d) For $\{a_n\}_{n=0}^{\infty}$ and $\{b_n\}_{n=0}^{\infty} \in S(\mathbb{C})$, we define

$$c_0 = a_0 b_0$$
$$c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 \quad \forall \text{ integer } n \geq 1$$

The convolution of $\{a_n\}_{n=0}^{\infty}$ and $\{b_n\}_{n=0}^{\infty}$ is $\{c_n\}_{n=0}^{\infty}$

i.e we have

$$G_c(x) = G_a * G_b(x) = G_b * G_a(x).$$
$$\|$$
$$c_0 + c_1 x + c_2 x^2 + \cdots$$

(e) A fun: $\delta_K : \mathbb{N} \to \mathbb{C}$ is called Dirac delta seq: if

$$\delta_K(n) = \begin{cases} 1 & \text{if } n = K \\ 0 & \text{if } n \neq K \end{cases}$$

We note that $(\delta_K * G_a)(x) = x^K G_a(x)$, where

$$G_a(x) = a_0 + a_1 x + a_2 x^2 + \cdots$$

(f) Let $G_a(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots$

$$G_a'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \cdots = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n$$

Oct 2, 2020 8:30 AM

Th :- Let N be a large positive integer and S be a finite multiset of the objects $a_1, a_2, \ldots a_n$

i.e $\forall\ i \in [n]$, there are N identical copies of the object a_i and $S = \{Na_1, Na_2, \ldots, Na_n\}$.

The number of k-combinations, where $k \leq nN$, of the multiset S is $\binom{n+k-1}{k}$.

Note : $\binom{n+k-1}{k} = \binom{n+k-1}{k-1}$

Proof : It will be done later

BINOMIAL & MULTINOMIAL THEOREM

Def^n: Let X be an n-set, a k-subset of X is a subset of X with size k and $\binom{X}{k}$ denotes the collection of all k-subsets of X. We define

$$\binom{n}{k} := \left|\binom{X}{k}\right|$$

Remark: If X and Y are two n-sets. Then there is a bijective mapping $f: X \to Y$. Such f induces a function (again denoted by f), $f: \binom{X}{k} \to \binom{Y}{k}$ by

$$f(A) = \{f(x) : x \in A\}, \text{ where } A \in \binom{X}{k}.$$

Verify that if $f: X \to Y$ is a bijective mapping then the induced map $f: \binom{X}{k} \to \binom{Y}{k}$ is a bijective mapping

Therefore $|X| = |Y|$ implies $\left|\binom{X}{k}\right| = \left|\binom{Y}{k}\right|$ by using bijective mapping principle of counting.

Claim: For each $A, B \in \binom{X}{k}$ there exist a bijective function $\pi : X \to X$ such that $\pi(A) = B$.

Proof of claim: Since $|A| = |B| = k$ & $|X \setminus A| = |X \setminus B| = n-k$, there exist a bijective mappings $f: A \to B$ and $g: X\setminus A \to X \setminus B$

Consequently $\pi: X \to X$ defined by

$$\pi(x) = \begin{cases} f(x) & \text{if } x \in A \\ g(x) & \text{if } x \in X \setminus A \end{cases}$$

is a bijective mapping with $\pi(A) = B$, and this establishes the claim.

Fix $A \in \binom{X}{k}$, now by the above claim we have

$$\{\pi(A) : \pi \in S_n(X)\} = \binom{X}{k}$$

Q: Count the no. of permutations $\lambda : X \to X$ such that $\lambda(A) = A$.

Note that $\pi \mapsto (\pi/_A, \pi/_{X\setminus A})$ is a bijective mapping from $\{\lambda \in S_n(X) : \lambda(A) = A\}$ to $S_k(A) \times S_{n-k}(X \setminus A)$ (verify it)

Therefore by bijective mapping principle of counting, we have

$$|\{\lambda \in S_n(X) : \lambda(A) = A\}| = |S_k(A) \times S_{n-k}(X\setminus A)|$$
$$= |S_k(A)| \times |S_{n-k}(X \setminus A)| = k!\,(n-k)!$$

Note that $\pi \sim \mu$, where $\pi, \mu \in S_n(X)$, if and only if $\pi(A) = \mu(A)$ is an equivalence relation.

$\boxed{A_1} \to \{\lambda \in S_n(X) : \lambda(A) = A\}$

$\boxed{B} \to \{\lambda \in S_n(X) : \lambda(A) = B\}$

$\boxed{C} \to \{\lambda \in S_n(X) : \lambda(A) = C\}$

What are the equivalence classes produced by the aforementioned equivalence relation into $S_n(X)$?

Answer: Roughly an equivalence class looks like
$$\{\pi \in S_n(X) : \pi(A) \text{ is same}\}.$$

An equivalence class with respect to the aforementioned equivalence relation into $S_n(X)$ is say
$$\{\pi_1, \pi_2, \cdots\cdots, \pi_N\} \subset S_n(X)$$
$$= \{\pi \in S_n(X) : \pi(A) = \pi_1(A) = \cdots = \pi_N(A)\}.$$
$$= \{\pi \in S_n(X) : \pi(A) \text{ is a } k\text{-subset of } X\}$$
$$= \{\pi \in S_n(X) : \pi(A) = B, \text{ for some } B \in \tbinom{X}{k}\}$$

Since there are exactly $\left|\binom{X}{k}\right|$ k-subsets of X, using the claim we have exactly $\left|\binom{X}{k}\right|$ no. of equivalence classes.

Two different equivalence classes have same size.

Let C & D be two k-subsets of X
Consider the following two equivalent classes
$$\{\pi \in S_n(X) : \pi(A) = C\}$$
$$\{\lambda \in S_n(X) : \lambda(A) = D\}.$$

claim: $|\{\pi \in S_n(X) : \pi(A) = C\}| = |\{\pi \in S_n(X) : \pi(A) = D\}|$

Proof of the claim: Exercise (Hint: use the previous claim).

This implies the set $S_n(X)$ can be decomposed into the equivalent classes, namely

$$\{\pi \in S_n(X) : \pi(A) \in \tbinom{X}{k}\}$$

Hence $$S_n(X) = \bigsqcup_{B \in \binom{X}{k}} \{\pi \in S_n(X) : \pi(A) = B\}.$$

i.e $$|S_n(X)| = \sum_{B \in \binom{X}{k}} |\{\pi \in S_n(X) : \pi(A) = B\}|$$

$$= |\tbinom{X}{k}| \cdot |\{\pi \in S_n(X) : \pi(A) = A\}|$$

i.e $$n! = |\tbinom{X}{k}| \cdot k!(n-k)!$$

Hence $$|\tbinom{X}{k}| = \frac{n!}{k!(n-k)!}$$

Comment: The technique to decompose the set $S_n(X)$ is called orbit-stabilizer technique.

NOV 6, 2020 8:30AM

SOLUTION OF RECURRENCE RELATION USING GENERATING FUNCTION

Example 1: We solve the recurrence $a_{n+1} = 2a_n \; \forall$ integer $n \geq 0$ with initial condition $a_0 = 1$

STEP 1 : Formation of generating fu^{n} related to $\{a_n\}_{n=0}^{\infty}$
Here it is

$$G_a(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n$$

STEP 2 : Use the recurrence relation to obtain a formula
Here note that

$$\begin{aligned} G_a(x) &= a_0 + \sum_{n=0}^{\infty} a_{n+1} x^{n+1} \\ &= a_0 + \sum_{n=0}^{\infty} 2a_n x^{n+1} \\ &= a_0 + 2x \sum_{n=0}^{\infty} a_n x^n \\ &= a_0 + 2x\, G_a(x) \end{aligned}$$

Observe the "formal" Power series here

Using initial cond^{n} $a_0 = 1$

i.e $(1-2x)\, G_a(x) = a_0$

$$\Rightarrow \quad G_a(x) = \frac{a_0}{1-2x} = \frac{1}{1-2x} = \sum_{n=0}^{\infty} 2^n x^n$$

FINAL : Conclude the sol^{n}
Here the required sol^{n} is $\{a_n (= 2^n)\}_{n=0}^{\infty}$

Example 2 : We solve the recurrence $a_{n+1} = 2a_n + 4^n \; \forall$ integer $n \geq 0$ with initial condition $a_0 = 1$

STEP 1 : Formation of generating fu^{n} related to $\{a_n\}_{n=0}^{\infty}$
Here it is

$$G_a(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n$$

STEP 2 : Use the recurrence relation to obtain a formula
Here note that

$$\begin{aligned} G_a(x) &= a_0 + \sum_{n=0}^{\infty} a_{n+1} x^{n+1} = a_0 + \sum_{n=0}^{\infty} (2a_n + 4^n)\, x^{n+1} \\ &= a_0 + 2x \sum_{n=0}^{\infty} a_n x^n + x \sum_{n=0}^{\infty} (4x)^n \\ &= a_0 + 2x\, G_a(x) + \frac{x}{1-4x} \end{aligned}$$

Using the initial cond^{n} $a_0 = 1$

i.e $(1-2x)\, G_a(x) = a_0 + \frac{x}{1-4x} = 1 + \frac{x}{1-4x}$

Nov 6, 2020, 8:30AM

i.e $$G_a(x) = \frac{1}{(1-2x)} + \frac{x}{(1-2x)(1-4x)} = \frac{1}{(1-2x)} + \frac{1}{2}\frac{(1-2x)-(1-4x)}{(1-4x)(1-2x)}$$

$$= \frac{1}{(1-2x)} + \frac{1}{2}\cdot\frac{1}{(1-4x)} - \frac{1}{2}\frac{1}{(1-2x)}$$

$$= \frac{1}{2}\cdot\frac{1}{1-2x} + \frac{1}{2}\frac{1}{1-4x}$$

$$= \sum_{n=0}^{\infty}\left(\frac{1}{2}(2x)^n + \frac{1}{2}(4x)^n\right) = \sum_{n=0}^{\infty}\left(\frac{1}{2}\cdot 2^n + \frac{1}{2}\cdot 4^n\right)x^n$$

FINAL: Conclude the sol^n

Here the required sol^n is $\left\{a_n\left(=\frac{1}{2}2^n + \frac{1}{2}4^n\right)\right\}_{n=0}^{\infty}$.

Example 3: We solve the recurrence $a_{n+2} + a_{n+1} - 6a_n = 0$ $\forall$ integer $n \geq 0$ with initial condition $a_0 = 1$, and $a_1 = 3$

STEP 1: Formation of generating fu^n related to $\{a_n\}_{n=0}^{\infty}$

Here it is

$$G_a(x) = a_0 + a_1x + a_2x^2 + \cdots = \sum_{n=0}^{\infty} a_n x^n$$

STEP 2: Use the recurrence relation to obtain a formula

Here it is

$$(1 + x - 6x^2)\, G_a(x) = 1 + 4x$$

$$\Rightarrow G_a(x) = \sum_{n=0}^{\infty}\left\{\frac{6}{5}2^n - \frac{1}{5}(-3)^n\right\}x^n$$

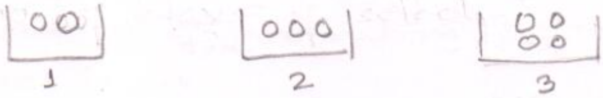
FINAL: Conclude the sol^n

Here required sol^n is $\left\{a_n\left(=\frac{6}{5}2^n - \frac{1}{5}(-3)^n\right)\right\}_{n=0}^{\infty}$

Nov 6, 2020 8:30 AM

APPLICATION OF GENERATING FUNCTION

Example : There are 3 boxes. The first box contains 2 balls, the second box contains 3 balls and the third box contains 4 balls.



- The no. of ways of selecting K balls with all or none balls from three boxes is the coefficeint of x^K in the expression

$$(1+x^2)(1+x^3)(1+x^4)$$

- The no. of ways of selecting k balls with one or none balls from three boxes is the coefficient of x^k in the expression

$$(1+x)(1+x)(1+x) = (1+x)^3$$

Remark : Suppose all the boxes contains large no of balls. Your job is to select K no. of balls from all the boxes

Conditions on the selection	Coefficient of x^k in the exprn
From box 1 at most n_1 balls From box 2 at most n_2 balls From box 3 at most n_3 balls	$(1+x+\cdots+x^{n_1})(1+x+\cdot+x^{n_2}) \times (1+x\cdots+x^{n_3})$
From box i at least m_i & atmost n_i balls $i=1,2,3$	$\prod_{i=1}^{3}(x^{m_i}+\cdots+x^{n_i})$
From box i exatly m_{i1} or $m_{i2}\cdots$ or m_{ij_i} balls	$\prod_{i=1}^{3}(x^{m_{i1}}+x^{m_{i2}}+\cdots+x^{m_{ij_i}})$

Oct 7, 2020 9:30 AM

BONOMIAL IDENTITIES

Th: Let A be an a-set and B be a b-set with $A \cap B = \phi$. Then

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} \quad \longleftarrow \text{(Binomial Theorem)}.$$

Binomial coefficient

Proof: Let $S = \{ (x_1, \cdots, x_n) : \forall i \in [n] \ x_i \in A \sqcup B \}$.

$$R = \bigsqcup_{p=0}^{n} \binom{[n]}{p} \times \{ (x_1 \cdots, x_p) : \forall i \in [p] \ x_i \in A \} \times \{ (y_1, \cdots, y_{n-p}) : \forall i \in [n-p] \ y_i \in B \}$$

Claim: There exist a bijection between S & R

Proof of claim: Exercise

Note $|S| = (a+b)^n$

$|R| = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$

Exercise: (A) If X is an n-set. Show that there exist a natural bijection between $\mathcal{P}(X)$ (i.e collection of all subsets of X) and 2^X (i.e collection of all mappings from X to $\{1,2\}$)

(Hint: Form $\mathcal{P}(X) = \bigsqcup_{k=0}^{n} \binom{X}{k}$ & deduce $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

(B) If X is an n-set. Show that there exist a natural bijection between $\binom{X}{k}$ and $\binom{X}{n-k}$ where k is an integer with $0 \le k \le n$. Deduce $\binom{n}{k} = \binom{n}{n-k}$

(C) If X & Y are disjoint n-sets. Find a natural bijection between $\binom{X \sqcup Y}{n}$ and $\bigsqcup_{k=0}^{n} \binom{X}{k} \binom{Y}{n-k}$.

Deduce $\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \sum_{k=0}^{n} \binom{n}{k}^2$.

Let X be an n-set and p & q are integers satisfing $0 \le p+q \le n$

$$\binom{X}{p,q} = \{(A,B) : A \subset X \text{ with } |A| = p,\ B \subset X \text{ with } |B| = q\ A \cap B = \phi\}$$

Exercise: Using orbit-stabilizer technique establish that

$$\left|\binom{X}{p,q}\right| = \frac{n!}{p!\,q!\,(n-p-q)!}.$$

Hint: Firstly, establish $\forall\ (A,B), (C,D) \in \binom{X}{p,q}$ [i.e $|A| = |C| = p$ & $|B| = |D| = q$ $A, B, C, D \subset X$]

there exist bijective mapping $\pi : X \to X$ such that $(\pi(A), \pi(B)) = (C, D)$

Secondly, fix $(A,B) \in \binom{X}{p,q}$ establish that

$$\{(\pi(A), \pi(B)) : \pi \in S_n(X)\} = \binom{X}{p,q}$$

Thirdly, count the no of permutations $\lambda : X \to X$ such that $\pi(A) = A$ & $\pi(B) = B$. Where $(A,B) \in \binom{X}{p,q}$.

Establish that

$$|\{\lambda \in S_n(X) : \lambda(A) = A,\ \lambda(B) = B\}| = |S_p(A)| \times |S_q(B)| \times |S_{n-p-q}(X \setminus (A \cup B))|$$
$$= p!\,q!\,(n-p-q)!$$

Finally, establish the equivalence relation on $S_n(X)$.

Count the no. of equivalence classes $\leftarrow$ (size of orbit)

Count the size of equivalence classes $\leftarrow$ (size of the Stabilizer)

Th: (Multinomial Theorem): Let for each $i \in [k]$, A_i be a set of size a_i and $\forall\ i, j \in [k]$ with $i \neq j$ $A_i \cap A_j = \phi$. Then

$$(a_1 + a_2 + \cdots + a_k)^n = \sum \frac{n!}{t_1!\,t_2! \cdots t_k!}\, a_1^{t_1} a_2^{t_2} \cdots a_k^{t_k}$$

Here the summation extenends over all non negative integer solⁿ of $t_1, \ldots, t_k$ satisfies $t_1 + \cdots + t_k = n$.

Nov 9, 2020 9:30 AM

EXPONENTIAL GENERATING FUNCTION

Defⁿ: An exponential generating fuⁿ of the complex valued seqⁿ $\{a_n\}_{n=0}^{\infty}$ is the formal power series

$$a_0 + \frac{a_1 x}{1!} + \frac{a_2 x^2}{2!} + \cdots$$

$$= \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n = eG_a(x)$$

Example: The exponential generating fuⁿ for the seqⁿ $\{1_n(=1)\}_{n=0}^{\infty}$ is

$$eG_1(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots$$

$$= e^x$$

Th: Let S be a multiset of k objects $b_1, b_2, \ldots, b_k$ with repetations $n_1, n_2, \ldots n_k$, where $\forall\, i \in [k]$, n_i is a positive integers i.e $S = \{n_1 b_1, n_2 b_2, \ldots, n_k b_k\}$

Let $\{a_n\}_{n=0}^{\infty}$ be a seqⁿ and $\forall$ integer $n \geq 0$, a_n denotes the number of n-permutation.

Then $$eG_a(x) = \prod_{i\in[k]} \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^{n_i}}{n_i!}\right)$$

Proof: Let

$$eG_a(x) = a_0 + \frac{a_1 x}{1!} + \frac{a_2 x^2}{2!} + \cdots$$

Note that $a_n = 0 \;\forall\, n \geq n_1 + n_2 + \cdots + n_k + 1$, so $eG_a(x)$ is a finite sum.

If we expand the product $\prod_{i\in[k]} \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^{n_i}}{n_i!}\right)$ as a sum, then the summands

$$\frac{x^{m_1}}{m_1!} \cdot \frac{x^{m_2}}{m_2!} \cdots \frac{x^{m_k}}{m_k!} = \frac{x^{m_1+m_2+\cdots+m_k}}{m_1!\, m_2! \cdots m_k!}$$

where $m_1, m_2, \ldots, m_k$ are integers with $\forall i \in [k]$

$$0 \leq m_i \leq n_i$$

i.e $$\prod_{i=1}^{k} \left(1 + \frac{x}{1!} + \cdots + \frac{x^{n_i}}{n_i!}\right) = \sum_{\substack{0\leq m_i \leq n_i \\ i\in[k]}} \frac{x^{m_1+m_2+\cdots+m_k}}{m_1!\, m_2! \cdots m_k!}$$

$$= \sum_{\substack{0\leq m_i \leq n \\ i\in[k]}} \frac{1}{m_1!\, m_2! \cdots m_k!} x^{m_1+m_2+\cdots+m_k} = \sum_{\substack{0\leq m_i \leq n \\ m_1+m_2+\cdots+m_k = n \\ i\in[k]}} \frac{n!}{m_1! \cdots m_k!} \frac{x^n}{n!}$$

Nov 9, 2020 9:30 AM

The coefficient of x^n in the summand expression

$$\sum_{\substack{0 \le m_i \le n_i \\ \forall i \in [k] \\ m_1 + \cdots + m_k = n}} \frac{n!}{m_1! \cdots m_k!}$$

Now note that $\frac{n!}{m_1! \cdots m_k!}$, where $\forall i \in [k]$ m_i is an integer with $0 \le m_i \le n_i$ & $m_1 + m_2 + \cdots + m_k = n$, represents the no of n-permutations of the multiset $\{m_1 b_1, \ldots, m_k b_k\}$.

Hence

$$a_n = \sum_{\substack{0 \le m_i \le n_i \ \forall i \in [k] \\ m_1 + \cdots + m_k = n}} \frac{n!}{m_1! \cdots m_k!} \qquad \square$$

Th: Let S be a multiset of k objects $b_1, b_2, \ldots, b_k$ with repetations $n_1, n_2, \ldots, n_k$, where $\forall i \in [k]$, n_i is a positive integer, i.e

$$S = \{n_1 b_1, n_2 b_2, \ldots, n_k b_k\}$$

Let a_n denotes the no of ways to represent the integer n as a sum of k non-negative integes, whenever $0 \le n \le n_1 + n_2 + \cdots + n_k$, otherwise $a_n = 0$, then

$$G_a(x) = \prod_{i \in [k]} (1 + x + x^2 + \cdots + x^{n_i})$$

Proof: Note that

$$G_a(x) = a_0 + a_1 x + a_2 x^2 + \cdots \cdots$$

where $a_n = 0$ $\forall$ integer $n \geq 1 + n_1 + n_2 + \cdots + n_k$

Also if we expand the $\prod_{i=1}^{k} (1 + x + x^2 + \cdots + x^{n_i})$ as sum, a typical summand is

$$x^{m_1} x^{m_2} \cdots x^{m_k}$$

where $m_1, m_2, \ldots, m_k$ are integers with $\forall i \in [k]$, $0 \le m_i \le n_i$.

$\therefore$ The coefficient of x^n in the summand expression of $\prod_{i=1}^{k} (1 + x + x^2 + \cdots + x^{n_i})$ is

$$\sum_{\substack{0 \le m_i \le n_i \ \forall i \in [k] \\ m_1 + \cdots + m_k = n}} 1 = a_n \qquad \square$$

Nov 9, 2020 9:30 AM

BOOLEAN ALGEBRA

Def^n: A non-empty set B, together with two binary operations + (addition) & $\cdot$ (multiplication) and one uniry operation $'$ (complementation) are called Boolean algebra denoted as & $(B, +, \cdot, ')$ if the following postulates are satisfied

1 : $+ : B \times B \to B$ & $\cdot : B \times B \to B$ are commutative
$(a,b) \mapsto a+b$ $(a,b) \mapsto a \cdot b$ $\forall a, b \in B$

ie $a+b = b+a$ and $a \cdot b = b \cdot a$

2 + is distributive over $\cdot$ and $\cdot$ is distributive over +
i.e $\forall a, b, c \in B$
$a \cdot (b+c) = a \cdot b + b \cdot c$ and $a + (b \cdot c) = (a+b) \cdot (a+c)$

3 $\exists$ two distinct elements 0 & 1 in B such that
$\forall a \in B$, $a + 0 = a$ and $a \cdot 1 = a$

4 $' ; B \to B$ satisfies $\forall a \in B$ $a + a' = 1$ and $a \cdot a' = 0$

Example: Let X be a non-empty set
$\mathcal{P}(X)$ = The set of subsets of X

$+ : \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$ ← Addition operation "binary"
$(A, B) \mapsto A \cup B$

$\cdot : \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X)$ ← Multiplication operation "binary"
$(A, B) \mapsto A \cap B$

$' ; \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$
$A \longmapsto A'$ ← Complementation operation "uninary"

Check that $(\mathcal{P}(X), +, \cdot, ')$ is a Boolean algebra.

* The element 0 (respectively, 1) is called additive identity (respectively, multiplicative identity)

* If we interchange the operations + and $\cdot$ and the additive identity and multiplicative identity in the def^n of Boolean algebra, it remains invariant. The operation + and $\cdot$ and the elements 0 and 1 are called dual of each other.

Th : Given two positive integers N and i, there is a unique way to expand N as a sum of binomial coefficients as follows:

$$N = \binom{n_i}{i} + \binom{n_{i-1}}{i-1} + \cdots + \binom{n_j}{j}$$

where j is a positive integer and $n_i \geq n_{i-1} \geq \cdots \geq n_j \geq j \geq 1$

Proof : Set $n_i = \max\{n : \binom{n}{i} \leq N\}$.

$$n_{i-1} = \max\left\{n : \binom{n}{i-1} \leq N - \binom{n_i}{i}\right\}.$$

In general, $n_{i-k} = \max\left\{n : \binom{n}{i-k} \leq N - \binom{n_i}{i} - \cdots - \binom{n_{i-k-1}}{i+k-1}\right\}$

where $k \in \{0, 1, 2, \ldots, i-1\}$.

The procedure of constructing the integers $n_i, n_{i-1}, \ldots$ must terminates, since $\binom{n}{1} = n \;\forall\; n \in \mathbb{N}$ and $k \in \{0, 1, 2, \ldots, i-1\}$.

This implies

$$N = \binom{n_i}{i} + \binom{n_{i-1}}{i-1} + \cdots + \binom{n_j}{j}$$

where i is an integer with $1 \leq j \leq i$.

Note that from the constructions of the integers $n_i, n_{i-1}, \ldots, n_j$ we have $n_i, n_{i-1}, \ldots, n_j$ are uniquely determined by N.

Claim : $n_{i-1} \leq n_i$

Proof of claim : Note that $\binom{n_i}{i} \leq N \leq \binom{1+n_i}{i} = \binom{n_i}{i} + \binom{n_i}{i-1}$ (Pascal's Identity)

Hence $0 \leq N - \binom{n_i}{i} \leq \binom{n_i}{i-1}$

Note that since $i \geq 1$, $\forall\; m \geq 1$ we have

$$\binom{m}{i-1} \leq \binom{m+1}{i-1}.$$

Therefore $\max\left\{m : \binom{m}{i-1} \leq N - \binom{n_i}{i}\right\} \leq n_i$

This establishes the claim.

Repetated use of the similar argument as in the claim we have (exercise! hint: use backward induction on i)

$$n_i \geq n_{i-1} \geq \cdots \geq n_j$$

If $N - \binom{n_i}{i} = 0$, then we have $N = \binom{n_i}{i}$ & the result holds with $j = i$

If $N - \binom{n_i}{i} \neq 0$ i.e $N - \binom{n_i}{i} \geq 1 = \binom{i-1}{i-1}$

i.e $\quad i-1 \leq \max\left\{n : \binom{n}{i-1} \leq N - \binom{n_i}{i}\right\} = n_{i-1}$

Arguing similarly we have (exercise!)

$$i-2 \leq n_{i-2}$$
$$i-3 \leq n_{i-3}$$
$$\vdots$$
$$j \leq n_j$$

$\square$

Pascal Identity: For each positive integer m

$$\binom{m}{k} + \binom{m}{k-1} = \binom{m+1}{k} \quad \leftarrow \text{Verify it !}$$

where $\quad 1 \leq k \leq m$

$$\begin{array}{ccccccccc}
 & & & \binom{1}{0} & & \binom{1}{1} & & & \\
 & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4}
\end{array}$$

$\boxed{\text{Pascal Triangle}}$

Combinatorial proof of Pascal' Identity:

Let $A = \left\{ X \in \binom{[m+1]}{k} : m+1 \in X \right\}$

$B = \left\{ X \in \binom{[m+1]}{k} : m+1 \notin X \right\}$

Hence $\quad |A| + |B| = \left|\binom{[m+1]}{k}\right| = \binom{m+1}{k}$

Note that $\forall\ X \in B$, $X \subset [m]$ i.e $B \subset \binom{[m]}{k}$

& for each $X \in \binom{[m]}{k}$ we have $X \in B$.

Hence $\quad |B| = \left|\binom{[m]}{k}\right| = \binom{m}{k}$

Again, $X \longmapsto X \setminus \{m+1\}$ is a <u>bijective</u> mapping (!) from A to $\binom{[m]}{k-1}$. Therefore

$$|A| = \left|\binom{[m]}{k-1}\right| = \binom{m}{k-1}$$

and the identity follows $\square$

Nov 10, 2020 9:30 AM

IMPORTANT PROPERTIES IN BOOLEAN ALGEBRA

Example : Take $B = \{1, 2, 3, 5, 6, 10, 15, 30\}$
= The set of all positive divisors of 30

$\forall\, a, b \in B$

Here
$0 = 1$
$1 = 30$

$a+b$ = Least common multiple of a and b

$a \cdot b$ = Greatest common divisor of a and b

$a' = \dfrac{30}{a}$

Then $(B, +, \cdot, ')$ is a Boolean algebra

[Comment: Generalize the above example]

Th : In Boolean algebra B, additive identity 0 and multiplicative identity 1 is unique.

Proof: Suppose $\bar{0}'$ be an additive identity. Then

$$\bar{0}' = 0 + \bar{0}' = 0$$

Using the property of $\bar{0}$ ($\forall a \in B$ $a + 0 = a$, $a + 0' = a$)

Using the property of 0

Similarly if $\bar{1}'$ be an multiplicative identity. Then

$$\bar{1}' = 1 \cdot \bar{1}' = 1$$ □

[Remark: 0 is called the zero element or zero & 1 is called the unit element or unit of the Boolean algebra $(B, +, \cdot, ')$.]

Th : In Boolean algebra B, $1' = 0$ (Dual property $0' = 1$)

Proof : $1' = 1' \cdot 1 \underset{?}{=} 1 \cdot 1' \underset{?}{=} 0$ □

Th : In Boolean algebra $a + a = a$ (Dual prop: $a \cdot a = a$) $\forall\, a \in B$.

Proof ; $a + a = (a+a) \cdot 1 = (a+a)\cdot(a+a')$
$= a + (a \cdot a')$
$= a + 0$
$= a$

The result follows since $a \in B$ is chosen arbitrarily. □

[Note : Interchange $+$ by $\cdot$ and 1 by 0 in the above we have $a \cdot a = a$, i.e $\forall a \in B$,
$a \cdot a = (a \cdot a) + 0 = (a \cdot a) + (a \cdot a') = a \cdot (a + a') = a \cdot 1 = a$]

NOV 10, 2020 9:30 AM

Th: In a Boolean algebra B, the following properties hold

(A) $a + I = I$ (Dual: $a \cdot 0 = 0$) $\forall a \in B$

(B) $a + (a \cdot b) = a$ (Dual $a \cdot (a+b) = a$) $\forall a, b \in B$

(C) $a'' = a$ $\forall a \in B$

(D) $(a+b)' = a' \cdot b'$ (Dual: $(a \cdot b)' = a' + b'$) $\forall a, b \in B$

(E) $a + (b+c) = (a+b) + c$ (Dual: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$) $\forall a, b, c \in B$.

Proof: (A) $a + I = (a+I) \cdot I = (a+I) \cdot (a+a') = a + (I \cdot a') = a + a' = I$

The result holds, since a is chosen arbitrarily.

(B) $a + (a \cdot b) = a \cdot I + a \cdot b = a \cdot (I + b) = a \cdot I = a$

The result holds, since a is chosen arbitrarily.

(C)
$$\begin{aligned} a'' = a'' \cdot I = a''(a'+a) &= a'' \cdot a' + a'' \cdot a \\ &= 0 + a'' \cdot a \\ &= a' \cdot a + a'' \cdot a \\ &= (a' + a'') \cdot a \\ &= I \cdot a \\ &= a \end{aligned}$$

The result holds, since a is chosen arbitrarily.

(D)
$$\begin{aligned} (a+b) + a' \cdot b' &= \{(a+b)+a'\}\{(a+b)+b'\} \\ &= (a+a')\{(a+b)+a'\}(b+b')\{(a+b)+b'\} \\ &= [a \cdot \{(a+b)+a'\} + a' \cdot \{(a+b)+a'\}][b \cdot \{(a+b)+b'\} \\ &\qquad + b'\{(a+b)+b'\}] \\ &= [a \cdot \{(a+b)+a'\} + a'][b \cdot \{(a+b)+b'\} + b'] \\ &= [a \cdot (a+b) + a \cdot a' + a'][b \cdot (a+b) + b \cdot b' + b'] \\ &= [a \cdot (a+b) + a'][b \cdot (a+b) + b'] \\ &= [a + a'][b + b'] \\ &= I \cdot I = I \quad \text{——} \ (*) \end{aligned}$$

Also,
$$\begin{aligned} (a+b) \cdot (a' \cdot b') &= a \cdot (a' \cdot b') + b \cdot (a' \cdot b') \\ &= a \cdot a' + a \cdot (a' \cdot b') + b \cdot b' + b \cdot (a' \cdot b') \\ &= a \cdot (a' + a' \cdot b') + b(b' + a' \cdot b') \\ &= a \cdot a' + b \cdot b' \\ &= 0 + 0 = 0 \quad \text{——} \ (**) \end{aligned}$$

Nov 10, 2020, 9:30 AM

From (+) & (++) we conclude $(a+b)' = a' \cdot b'$

The result holds since $a, b \in B$ is chosen arbitrarily.

Problem: If $a, b \in B$, satisfies $a+b = I$ and $a \cdot b = 0$, then $b = a'$

Sol^n: $b = b \cdot I = b \cdot (a'+a) = b \cdot a' + b \cdot a = b \cdot a' + a \cdot a'$

$= (b+a) \cdot a'$

$= I \cdot a' = a'$

(E) $a + (b+c) = (a+a') \cdot [a + (b+c)]$

$= a \cdot [a+(b+c)] + a'[a+(b+c)]$

$= a + [a' \cdot a + a'(b+c)]$

$= a + a' \cdot (b+c)$

$= a + a' \cdot b + a' \cdot c$

$(a+b) + c = (a+a')[(a+b)+c]$

$= a \cdot [(a+b)+c] + a'[(a+b)+c]$

$= a \cdot (a+b) + a \cdot c + a' \cdot (a+b) + a' \cdot c$

$= a + a \cdot c + a' \cdot a + a' \cdot b + a' \cdot c$

$= a + a \cdot a' + a' \cdot b + a' \cdot c$

$= a + a' \cdot b + a' \cdot c$

i.e $a + (b+c) = (a+b) + c$

The result holds, since a, b, c is chosen arbitrarily.

Nov 11, 2020, 9:30 AM

ORDER RELATIONS IN BOOLEAN ALGEBRA

Th: In a Boolean algebra B, if for some $a, b \in B$ $a+b=b$, then $a \cdot b = a$ (and conversely if for some $a, b \in B$ $a \cdot b = a$ then $a+b=b$.

Proof: Let $a, b \in B$ with $a+b=b$

Then $a \cdot b = a \cdot (a+b) = a$

Conversely, let $a, b \in B$ with $a \cdot b = a$

Then $a+b = a \cdot b + b = b + a \cdot b = b$ $\square$

Remark: Let B be a Boolean algebra, we say $a \leq b$ if and only if $a+b=b$ (or $a \cdot b = a$), where $a, b \in B$.

Check that B with respect to the relation $\leq$ forms a poset.

Def^n: A non-empty set P together with binary relation ρ i.e $\rho \subset P \times P$, is called partially ordered set or simply poset if such binary relation ρ is reflexive (i.e $(a,a) \in \rho$ $\forall a \in P$) anti-symmetric (i.e $\forall a, b \in P$, if $(a,b) \in \rho$ and $(b,a) \in \rho$, then $a=b$) transitive (i.e $\forall a,b,c \in P$, if $(a,b) \in \rho$ and $(b,c) \in \rho$ then $(a,c) \in \rho$).

We denote ρ as partially order relation.

Example: Let n be a positive integer. Check the following partial order relations

(a) The usual order relation $\leq$ on the set $[n]$

(b) The inclusion relation $A \subset B$, where $A, B \in 2^{[n]}$

(c) The division relation $a \mid b$ (i.e $b = ra$ for some $r \in \mathbb{Z}$), where $a, b \in \mathbb{Z}$.

NOTE: Let B be a Boolean algebra and $\forall a, b \in B$ $a \leq b$ if and only if $a+b=a$ is the partial order relation on B. Then we observe the following

* $0 \leq a$ $\forall a \in B$. (Since $\forall a \in B$ $a+0=a$). This implies 0 is the least element in the poset $(B, \leq)$. $\boxed{0 = \text{lub} B}$
* $a \leq 1$ $\forall a \in B$ (Since $\forall a \in B$ $a \cdot 1 = a$). This implies 1 is the greatest element in the poset $(B, \leq)$. $\boxed{1 = \text{glb} B}$

Def^n: A non-empty set L together with a partially order relation $\leq$ is called a lattice if every pair of elements of L has a least upper bound and a greatest lower bound.

The least upper bound of $a, b \in L$ is denoted as $a \vee b$ (read as a join b) and the greatest lower bound of $a, b \in L$ is denoted as $a \wedge b$ (read as a meet b)

Nov 11, 2020 9:30 AM

* The Boolean algebra B with respect to aforementioned partial order relation $\le$ (i.e the poset $(B, \le)$) forms a lattice.

Here note that $\forall a, b \in B$, we have $a \vee b = a + b$ and $a \wedge b = a \cdot b$

Defn: Let A be a non-empty subset B, where $(B, +, \cdot, ')$ is a Boolean algebra. The set A is said to be sub-Boolean algebra of B if under the same operations $+$, $\cdot$ and $'$ (restricted to A), A is also a Boolean algebra.

Propn: Let A be a sub-Boolean algebra of Boolean algebra B.

(a) If $a \in A$, the complement of a in A is same as the complement of $a \in B$.

(b) The unit element in A is same as the unit element 1 in B

(c) The zero element in A is same as the zero element 0 in B

Proof: (a) Let $' : B \to B$ the complementation mapping and $'/_A : A \to B$ be restriction of $'$ to A. Since A is sub-Boolean algebra of B we have $'/_A : A \to A$.

We denote $'/_A(a) = a'^A \ \forall a \in A$.

Let $a \in A$. We note that

$$a'^A = '/_A(a) = '(a) = a'$$

Since $a \in A$ is chosen arbitrarily, we have $\forall a \in A \ a'^A = a'$

(b) Let 1_A denote the multiplicative identity of A and $+/_A : A \times A \to B$ be the restriction of $+ : B \times B \to B$. Since A is sub-Boolean algebra of B, we have $+/_A : A \times A \to A$

Then $1_A = a +/_A a' = a + a' = 1$

(c) Let 0_A denote the additive identity of A and $\cdot/_A : A \times A \to B$ be the restriction of $\cdot : B \times B \to B$. Since A is sub-Boolean algebra of B, we have $\cdot/_A : A \times A \to A$.

Then $0_A = a \cdot/_A a' = a \cdot a' = 0$ $\square$

Comment: The unit 1 and zero 0 are members of any sub-Boolean algebra of Boolean algebra B.

Also note that $\{0, 1\}$ is a sub-Boolean algebra of B.

Nov 13, 2020 8:30 AM

SUB-BOOLEAN ALGEBRA

Th: Let A be a non-empty subset of the Boolean algebra $(B, +, \cdot, ')$. A forms a sub-Boolean algebra of B if the following cond$^{\underline{s}}$ are satisfied.

(a) If $a \in A$, $b \in A$, then $a+b \in A$

(b) If $a \in A$, $b \in A$, then $a \cdot b \in A$

(c) If $a \in A$, then $a' \in A$.

Proof: Let $a \in A$, then by condition (c) $a' \in A$. Consequently, $0 = a \cdot a' \in A$ and $1 = a + a' \in A$.

The conditions (a) & (b) implies $+ : A \times A \to A$, $(a, b) \mapsto a+b$ & $\cdot : A \times A \to A$, $(a, b) \mapsto a \cdot b$

Note that for $a, b \in A$ by conditions (a) & (b) both $a+b \in A \subset B$ and $b+a \in A \subset B$. In B, $a+b = b+a$ holds, this implies $a+b = b+a$ holds in A. Similarly $a \cdot b = b \cdot a$ holds in A. Since $a, b \in A$ is chosen arbitrarily we have $\forall a, b \in A$, $a+b \in A$ and $a \cdot b \in A$.

Arguing similarly we have $\forall a, b, c \in A$.

$$a + (b \cdot c) = (a+b) \cdot (a+c)$$

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Therefore A is a Boolean algebra by itself, consequently A is a sub-Boolean algebra of B. $\square$

Example: Let $X = \{a, b, c\}$. Consider the Boolean algebra $(\mathcal{P}(X), \cup, \cap, ')$, where $\mathcal{P}(X)$ denotes the set of all subsets of X [Note $\mathcal{P}(X)$ also denoted as 2^X]

Let $P = \{\phi, \{a\}, \{b, c\}, X\}$

$Q = \{\phi, \{b\}, \{a, c\}, X\}$

$R = \{\phi, \{c\}, \{a, b\}, X\}$

P, Q & R are three sub-Boolean algebra of $\mathcal{P}(X)$.

Th: The intersection of family of sub-Boolean algebras of the Boolean algebra B is a sub-Boolean algebra of B.

Proof: Let $\{A_\alpha : \alpha \in S\}$ be a collection of sub-Boolean algebras of B, where S is the index set.

claim: $\bigcap_{\alpha \in S} A_\alpha$ is a sub-Boolean algebra of B.

Nov 13, 2020 8:30 AM

Proof of claim: Note that $0, 1 \in \bigcap_{\alpha \in S} A_\alpha$, hence $\bigcap_{\alpha \in S} A_\alpha$ is a non-empty subset of B.

Let $a, b \in \bigcap_{\alpha \in S} A_\alpha$, i.e $a, b \in A_\alpha \ \forall \alpha \in S$.

Therefore, $a+b \in A_\alpha$ $a \cdot b \in A_\alpha$ and $a' \in A_\alpha$ $\forall \alpha \in S$

i.e $a+b \in \bigcap_{\alpha \in S} A_\alpha$, $a \cdot b \in \bigcap_{\alpha \in S} A_\alpha$ and $a' \in \bigcap_{\alpha \in S} A_\alpha$

Hence the claim is established, by the previous theorem

The proof of claim completes the proof of the result. $\square$

Defn: An element $e \neq 0$ in the Boolean algebra B is called an atom of B if $\forall x \in B$ $x \leq e$ implies either $x = 0$ or $x = e$.

Result: If e_1 & e_2 are two distrinct atoms in the Boolean algebra B, then $e_1 \cdot e_2 = 0$

Proof: Note that $e_1 \cdot e_2 \leq e_1$ and $e_1 \cdot e_2 \leq e_2$
(i.e $e_1 + e_1 \cdot e_2 = e_1$ and $e_2 + e_1 \cdot e_2 = e_2$)

Since e_1, is a atom we have $e_1 \cdot e_2 = 0$ or e_1 — ⊛

Again since e_2 is a atom, we have $e_1 e_2 = 0$ or e_2 — ⊛⊛

If $e_1 \cdot e_2 \neq 0$, then from ⊛ we have $e_1 = e_1 \cdot e_2$ and from ⊛⊛ we have $e_2 = e_1 \cdot e_2$, i.e $e_1 = e_1 \cdot e_2 = e_2$

— A contradiction to the assumption that e_1 & e_2 are distinct. $\square$

Result: If e is an atom and $e \leq x + y$ for some $x, y \in B$, then either $e \leq x$ or $e \leq y$.

Proof: If $e \cdot x = 0 = e \cdot y$, then
$e \leq x+y \Leftrightarrow e \cdot (x+y) = e \Leftrightarrow e \cdot x + e \cdot y = e \Leftrightarrow 0 + 0 = e \Leftrightarrow 0 = e$

Note that $e \cdot x \leq e$ (i.e $e + e \cdot x = e$) and similarly $e \cdot y \leq e$

Since e is an atom $e \cdot x = 0$ or e and $e \cdot y = 0$ or e

But $e \cdot x = 0 = e \cdot y$ implies $e = 0$, hence we have either $e \cdot x = e$ or $e \cdot y = e$. $\square$

i.e either $e \leq x$ or $e \leq y$.

Cor: If e is an atom and $e \leq x_1 + x_2 + \cdots + x_n$ for some $x_1, x_2, \ldots, x_n \in B$, then $e \leq x_i$ for some $i \in [n]$.

Proof: Exercise

Example: If $B = 2^{[3]}$, then $\{1\}, \{2\}, \{3\}$ are atoms in B.

Corollary: One can distribute n identical objects into k labelled boxes such that each box contains at least one identical object, into $\binom{n-1}{k-1}$ ways.

Exercise: Consider the eq^n $\sum_{i=1}^{k} x_i = n$, where n & k are positive integers.

Show that (a) the no. of negative integer sol^{n}s of the above eq^n is $\binom{n+k-1}{k-1}$.

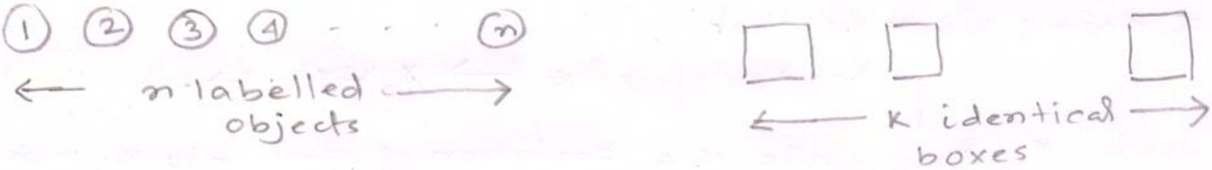
(b) the no. of positive integer sol^n of the above eq^n is $\binom{n-1}{k-1}$.

Proof of above corollary: We first distribute one object to each box. It results exactly $n-k$ identical objects are to be distributed among the labelled k boxes. By the above theorem it can be done in

$$\binom{n-k+k-1}{k-1} = \binom{n-1}{k-1} \text{ ways.} \qquad \square$$

Def^n: Let n & k be non-negative integers with $n \geq k$. The <u>Stirling numbers of second kind</u> denoted as $S_k^{II}(n) = S(n,k)$ is the total no. of partitions of $[n]$ into k non empty parts.

"The set $[n]$ is chopped in k parts"



Def^n: The <u>Bell number</u> $B(n)$, where n is a positive integer, is the total no. of partitions of $[n]$, i.e

$$B(n) = \sum_{i=0}^{n} S(n,i).$$

Th: Let n and k be positive integers with $n \geq k$, then

$$S(n,k) = S(n-1, k-1) + k\, S(n-1, k)$$

Proof : $\mathcal{S}([n], k)$ = The collection (set) of all partitions of $[n]$ into k non empty parts.

$\frac{2}{2}$

$\mathcal{A}$ = The collection (set) of all partitions of $[n]$ into k non empty parts, where n belongs to a singleton set "i.e one chop of the set $[n]$ is $\{n\}$"

$\mathcal{B}$ = The collection (set) of all partitions of $[n]$ into k non empty parts, where n belongs to non-singleton set.

Claim 1 : $|\mathcal{A}| = S(n-1, k-1)$

Proof of claim: Let $X_1, X_2, \ldots, X_k$ be a partition of $[n]$ into k non-empty parts. and one of $X_1, \ldots, X_k$ is $\{n\}$. Without loss of generality let $X_k = \{n\}$.

i.e $[n] = X_1 \sqcup X_2 \sqcup X_3 \sqcup \cdots \sqcup X_k$, $\forall i \in [k]$, $X_i \neq \phi$ & $X_k = \{n\}$

This induces a partition of $[n-1]$ into $(k-1)$ non-empty parts namely, $X_1, X_2, \ldots, X_{k-1}$.

Conversely, if $Y_1, Y_2, \ldots, Y_{k-1}$ is a partition of $[n-1]$ into $k-1$ non empty parts, then

$$Y_1, Y_2, \ldots, Y_{k-1}, \{n\}$$

is a partition of $[n]$ into k non-empty parts.

Hence a bijective correspondence exists between $\mathcal{A}$ and $\mathcal{S}([n-1], k-1)$, and the claim is established.

Claim 2 : $|\mathcal{B}| = k\, S(n-1, k)$.

Proof of claim: We note that

$$X_1, X_2, \ldots, X_k \longmapsto X_1 \setminus \{n\}, X_2 \setminus \{n\}, \ldots, X_k \setminus \{n\}$$

where $X_1, X_2, \ldots, X_k$ is a partition of $[n]$ into k- non-empty parts and note that $X_1 \setminus \{n\}, X_2 \setminus \{n\}, \ldots, X_k \setminus \{n\}$ is a partition of $[n-1]$ into k - non-empty parts.

Again for each partition of $[n-1]$ into k non-empty parts $Y_1, Y_2, \ldots, Y_k$

has exactly k preimages w.r.to aforementioned mapping

$$\left.\begin{array}{l} Y_1 \sqcup \{n\}, Y_2, \ldots \quad Y_k \\ Y_1, Y_2 \sqcup \{n\}, \ldots \quad Y_k \\ Y_1, Y_2, Y_3 \sqcup \{n\}, \ldots Y_k \\ \vdots \\ Y_1, Y_2, \ldots \quad Y_k \sqcup \{n\} \end{array}\right\}$$

Hence such mapping is k-to-1, onto mapping, Therefore the claim is established □

PIGEONHOLE PRINCIPLE

Th: (Pigeonhole Principle - simple version) If $(n+1)$ objects are distributed among n boxes, where n is a positive integer, then there exist at least one box which contain two or more objects.

Proof: Suppose none of the n boxes contains two or more objects. This means each of the n boxes contains at most one object. Hence there are at most n objects, however we are distributing $(n+1)$ objects. A contradiction arises. $\square$

Observation: There are 28 faculties at SPS NISER. At least 3 faculties of SPS share same birth month.

Here 12 boxes are labelled with the months of a year and 28 birth months of 28 faculties are 28 objects.

Th: (Pigeonhole Principle - strong and uniform version): If $mn+1$ objects are distributed among n boxes, where m & n are positive integers, then there exist at least one box which contains at least $m+1$ objects.

Proof: Suppose each of the n boxes contains at most m objects after distribution. Then there are mn objects which are to be distributed. Hence our assumption that each of the n boxes contains at most m objects is wrong i.e a contradiction arises. Hence at least one of the n boxes contains at least $m+1$ objects. $\square$

Th: (Pigeonhole Principle - strong version): If $m_1+\cdots+m_n-n+1$ objects are distributed among n labelled boxes with labelling $1, 2, \ldots n$, where $m_1, \ldots m_n, n$ are positive integers. Then there exist at least one i such that the box with label i contains at least m_i objects.

Proof: Suppose for each $i \in \{1, 2, \cdots n\}$, the box with label i contains less than m_i objects after distribution. Then there are at most $\sum_{i=1}^{n}(m_i - 1) = m_1 + \cdots + m_n - n$ objects are to be distributed.

But there are $m_1+\cdots+m_n-n+1$ objects. Hence our assumption for each $i \in \{1, 2, \cdots n\}$, the label i box contains at most m_i objects is wrong, i.e a contradiction arises. Hence for some i, the box with label i contains at least m_i objects. $\square$

Observation: "Objects" are "pigeons" and "boxes" are "pigeonholes".

Sept 14, 2020 9:30 AM

SOME APPLICATIONS OF PIGEONHOLE PRINCIPLE

2/2

Model: Let m and n are two positive integers with $\gcd(m,n)=1$.
Let a and b be two integers with $0 \le a \le m-1$ and $0 \le b \le n-1$
Then there exist a positive integer x satisfies both the conditions $x \equiv a \bmod m$ and $x \equiv b \bmod n$. The pigeonhole principle is applied to prove the existance of such x.

In number theory, the above existancial statement is referred as Chinese Remainder Theorem.

To prove the Chinese Remainder Theorem we construct the following n numbers

$$a, \; a+m, \; a+2m, \; \ldots \quad a+(n-1)m.$$

Note that all the above numbers satisfies modulo eq^n $x \equiv a \bmod m$. Now we claim the following

Claim: If $a+im \equiv r_i \bmod n \;\forall\; i \in \{0,1,2,\ldots,n-1\}$, then $\forall\; i,j \in \{0,1,\ldots n-1\}$ with $i \ne j$ satisfies $r_i \ne r_j$

Proof of claim: Suppose there exist $i,j \in \{0,1,\ldots,n-1\}$ with $i<j$ and $r_i = r_j$. This means $n \mid (j-i)m$. Since $\gcd(m,n)=1$, we have $n \mid (j-i)$. A contradiction arises, since $1 \le j-i \le n-1$, which establishes the claim.

Here we use the pigeonhole principle, considering the remainders $r_0, r_1, \ldots, r_{n-1}$ and b as $n+1$ objects and the complete (?) list of remainders $r_0, \ldots, r_{n-1}$ as n boxes. We conclude there exist a remainder (say) r_K, such that $b \equiv r_K \bmod n$, i.e $a+Km \equiv b \bmod n$. It shows that $a+Km$ is the required x satisfies $x \equiv a \bmod m$ and $x \equiv b \bmod n$.

Home work: Establish true/false with explanation.

A If at least $(n+1)$ objects are distributed among n boxes, where n is a positive integer, then there exist at least box which contain two or more objects.

B If at least $mn+1$ objects are distributed among n boxes, where m & n are positive integers, then there exist at least one box which contains at least $m+1$ objects.

C If at least $m_1+m_2+\cdots+m_n-n+1$ objects are distributed among n labelled boxes with labelling $1,2,\ldots,n$, where $m_1,\ldots m_n$ are positive integers, then there exist at least one i such that box with label i contains at least m_i objects

SOME APPLICATIONS OF PIGEONHOLE PRINCIPLE

Model : Let $a_1, a_2, \cdots, a_n$ are n integers, then there exist integers i and j, with $0 \le i < j \le n$ such that

$$n \mid (a_{i+1} + \cdots + a_j) \quad \left[\text{Read as } n \text{ "divides" } (a_{i+1} + \cdots + a_j)\right]$$

The pigeonhole principle is applied to prove the existance of such integers i and j. We contruct the following n numbers

$$a_1,\ a_1+a_2,\ a_1+a_2+a_3, \cdots\cdots, a_1+a_2+\cdots+a_n$$

If one of the above n numbers is divisible by n, then the result follows. Otherwise we have none of them is divisible by n. In this case, suppose

$$a_1 + \cdots + a_K \equiv r_K \bmod n,$$

then $r_K \in \{1, 2, \cdots, n-1\}$, for each $K \in \{1, 2, \cdots n\}$. Here we use the pigeonhole principle. We consider the n numbers $a_1, a_1+a_2, \cdots, a_1+a_2+\cdots+a_n$ as n objects and $(n-1)$ remainders $r_1, r_2, \cdots, r_{n-1}$ as boxes. We conclude there exists $i, j \in \{1, 2, \cdots n\}$ with $i<j$ and a remainder r such that

$$a_1 + \cdots + a_i \equiv a_1 + \cdots + a_j \equiv r \bmod n.$$

This means $\quad a_1 + \cdots + a_i = pn + r$ and

$$a_1 + \cdots + a_i + \cdots + a_j = qn + r$$

for some integer p, q. i.e

$$(a_1 + \cdots + a_i + \cdots + a_j) - (a_1 + \cdots + a_i) = qn + r - pn - r$$

$$\Leftrightarrow \quad a_{i+1} + a_{i+2} + \cdots\cdots + a_j = (q-p)n$$

i.e $\quad n \mid a_{i+1} + a_{i+2} + \cdots + a_j$

Th: (Erdős-Szekeres) Let m and n be positive integers and $\{x_n\}_{n=1}^{\infty}$ be a sequence of real numbers.

Then $x_1, x_2, \cdots, x_{mn+1}$ contains either a monotonically increasing subsequence with $m+1$ real numbers or a strictly decreasing subsequence with $n+1$ real numbers.

Proof: Suppose $x_1, \cdots, x_{mn+1}$ does not have any monotonically increasing subsequence with $m+1$ real numbers.

Let $\forall\ i \in [mn+1]$, the largest monotonically increasing subsequence of $x_i, x_{i+1}, \cdots, x_{mn+1}$ have exactly k_i real numbers.

Then $1 \le k_i \le m$.

We take $k_1, k_2, \cdots, k_{mn+1}$ as objects and m labelled boxes with labels $1, 2, \cdots, m$. If $k_j = i$, where $j \in [mn+1]$ and $i \in [m]$, we put k_j into the box with label i.

By using pigeonhole principle, we conclude that there exists at least one box with some label (say) r contains at least $n+1$ objects. It means among the $mn+1$ objects $k_1, k_2, \cdots, k_{mn+1}$ there are at least $n+1$ objects have same value r (say).

$$k_{\ell_1}, k_{\ell_2}, \cdots, k_{\ell_{n+1}}$$

Claim: $x_{\ell_1} > x_{\ell_2} > \cdots > x_{\ell_{n+1}}$ is the required strictly decreasing subsequence with $n+1$ real numbers.

Proof of the claim: Suppose $x_{\ell_i} \le x_{\ell_j}$ for some $i, j \in [n+1]$

So $x_{\ell_1}, x_{\ell_1+1}, \cdots x_{mn+1}$ and

$x_{\ell_2}, x_{\ell_2+1}, \cdots x_{mn+1}$

have monotonically increasing subseq^{ns} with $k_{\ell_i} = k_{\ell_j} = r$ real numbers. Therefore

$$x_{\ell_i}, \cdots, x_{\ell_j}, \cdots, x_{mn+1}$$

have monotonically increasing subseq^{n} with more than r real numbers. A contradiction arises which establishes the claim

The result follows from the claim.

Nov 16, 2020 9:30 AM

ATOMIC BOOLEAN ALGEBRA

Def^{n}: A Boolean algebra B is said to be atomic if each non-zero element of B dominates at least one atom, i.e $\forall x \in B$ with $x \neq 0$ either x is an atom or $\exists$ an atom e such that $e \leq x$.

A Boolean algebra B is said to be non-atomic if it has no atom.

Th: Every finite Boolean algebra is atomic.

Proof: Let B be a finite Boolean algebra and $x \in B$ with $x \neq 0$. To show either x is an atom or $\exists$ an atom e such that $e \leq x$ (i.e $e + x = x$)

Suppose x is not an atom. To show $\exists$ an atom e such that $e \leq x$.

Since x is not an atom, $\exists$ $x_1 \in B$ s.t $x_1 \neq 0$ and $x_1 \leq x$. If x_1 is an atom, then the required atom $e = x_1$. If x_1 is not an atom, then $\exists$ $x_2 \in B$ s.t $x_2 \neq 0$ and $x_2 \leq x_1$. continuing the same argument, we obtain an element $x_n \in B$ s.t $x_n \neq 0$ and

$$x_n \leq x_{n-1} \leq \cdots \leq x_2 \leq x_1 \leq x$$

Since B is finite, after continuing the procedure for finite no. of steps say N, we have the required atom $e = x_N$. □

Comment: Let X be an infinite set. Then $\{x\}$, where $x \in X$, is an atom in the Boolean algebra 2^X.

Conclusion: An atomic Boolean algebra may not be finite

Th: Every non-zero element in a finite Boolean algebra B can be uniquely expressed as the sum of no. of atoms.

Proof: Let $x \in B$ with $x \neq 0$. If x is an atom, then we are done. If x is not an atom, then by the above theorem, suppose $e_1 \in B$ is an atom satisfies $e_1 \leq x$ (i.e $x \cdot e_1 = e_1$).

Note that $x = x \cdot 1 = x(e_1 + e_1') = x \cdot e_1 + x \cdot e_1'$
$$= e_1 + x \cdot e_1' \quad \text{—} \; \circledast$$

Now, if $x \cdot e_1' = 0$, then $\circledast$ implies $x = e_1$, which is a contradiction. Hence $x \cdot e_1' \neq 0$.

Set $x_1 := x \cdot e_1'$. If x_1 is an atom, then from $\circledast$ we have
$$x = e_1 + x_1 \quad (\text{i.e sum of two atoms } e_1 \,\&\, x_1).$$

If x_1 is not an atom, then we continue our argument as before and we get an atom $e_2 \le x_1$ s.t.

$$x_1 = e_2 + x_1 \cdot e_1'$$

i.e $x = e_1 + e_2 + x_1 \cdot e_1'$

We proceed as before we have

$$x = e_1 + e_2 + \cdots + e_n + x_n e_{n-1}'$$

Since B is finite the process terminate in finite no. of steps. This means

$$x = e_1 + e_2 + \cdots + e_N + x_N \cdot e_{N-1}' \quad \text{— (**)}$$

Where $e_1 \ldots e_N$ are atoms and $x_N e_{N-1}'$ is a atom.

(**) is the required expression of x as a sum of atoms $e_1, \ldots, e_N$ and $x_N \cdot e_{N-1}'$.

Let $x = e_1 + e_2 + \cdots + e_N$ i.e x is expressed as sum of atoms
$= e_1^* + e_2^* + \cdots + e_M^*$ in two different ways.

Then there exist $i \in [N]$ s.t e_i is different from each of the $e_1^*, e_2^*, \ldots, e_M^*$, i.e $e_i \ne e_j^*$ $\forall j \in [M]$.

Hence $e_i \cdot e_j^* = 0$ $\forall j \in [M]$

$$e_i \le e_1^* + \cdots + e_M^*$$
$$\Rightarrow e_i \cdot (e_1^* + \cdots + e_M^*) = e_i$$
$$\Rightarrow e_i \cdot e_1^* + \cdots + e_i \cdot e_M^* = e_i$$
$$\text{i.e } 0 + \cdots + 0 = e_i \Rightarrow 0 = e_i$$

— A contradiction arises.

Hence $\forall i \in [N]$, e_i is same with at least one of $e_1^*, \ldots, e_M^*$.

Thus $M = N$ and the two representations differ by a permutation on $[N] = [M]$. But they are same in view of commutative property of $+$. □

Note: If $\{e_1, e_2, \ldots e_n\}$ denotes the set of all atoms in B then $\forall x \in B$

$$x = t_1 \cdot e_1 + t_2 \cdot e_2 + \cdots + t_n \cdot e_n$$

where $t_i \in \{0,1\} \subset B$ $\forall i \in [n]$.

Comment: If B is finite and $\{e_1, \ldots, e_n\}$ is the set of all atoms then $|B| = 2^n$.

Nov 16, 2020 9:30 AM

Th: In a finite Boolean algebra every non-zero element is the sum of all the atoms dominated by it.

Proof: Let x be a non-zero element in a finite Boolean algebra B.

Then by a previous theorem $\exists$ atoms $e_1, e_2, \cdots e_K \in B$ s.t.

$$x = e_1 + e_2 + \cdots + e_K$$

Let e be an atom, satisfies $e \leq x$.

Note that by a previous result we have

$$e \leq e_i \quad \text{for some } i \in [K]$$

Since e and e_i both are atoms, we have $e = e_i$ for some $i \in [K]$

Since such e is chosen arbitrarily, we have for each atom e with $e \leq x$, satisfies $e \leq e_i$ for some $i \in [K]$. $\square$

SOME APPLICATIONS OF PIGEONHOLE PRINCIPLE

Th: (Pigeonhole Principle - Twin version): If at most $n-1$ objects are distributed among n boxes, where n is a positive integer, then there exist at least one empty box.

Proof: Exercise

Th: (Dirichlet's Approximation) For each irrational number α there exist infinitely many rational numbers $\frac{p}{q}$ satisfies $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.

Proof: We fix α and prove the following claim

Claim: For each positive integer n, there exist positive integers p and q satisfies

$$|\alpha - \frac{p}{q}| < \frac{1}{nq} \leq \frac{1}{q^2}$$

Proof of claim: For the positive integer m, note that $m\alpha - \lfloor m\alpha \rfloor$ is an irrational number satisfies

$$0 < m\alpha - \lfloor m\alpha \rfloor < 1$$

We consider $(0, \frac{1}{n}), (\frac{1}{n}, \frac{2}{n}), \ldots, (\frac{n-1}{n}, 1)$ as n boxes and $n+1$ irrational nos.

$$\alpha - \lfloor \alpha \rfloor,\ 2\alpha - \lfloor 2\alpha \rfloor, \ldots, (n+1)\alpha - \lfloor (n+1)\alpha \rfloor$$

as $n+1$ objects to distribute among those n boxes.
Therefore by pigeonhole principle one box must contain at least two such irrational nos (say)

$$r\alpha - \lfloor r\alpha \rfloor \quad \text{and} \quad s\alpha - \lfloor s\alpha \rfloor \quad \text{with } r < s$$

This immediately implies,

$$\left| (s\alpha - \lfloor s\alpha \rfloor) - (r\alpha - \lfloor r\alpha \rfloor) \right| < \frac{1}{n}$$

$$\Rightarrow \left| (s-r)\alpha - (\lfloor s\alpha \rfloor - \lfloor r\alpha \rfloor) \right| < \frac{1}{n}$$

We set $p = \lfloor s\alpha \rfloor - \lfloor r\alpha \rfloor$ and $q = s - r$, then $q \leq n$ and

$$|q\alpha - p| < \frac{1}{n}$$

This establishes the claim, since

$$|\alpha - \frac{p}{q}| < \frac{1}{nq} \leq \frac{1}{q^2}$$

Let $\frac{p}{q}$ be the rational no satisfies $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.
We consider the positive irrational number $\beta = |\alpha - \frac{p}{q}|$.
By using archimedean property, we have the positive integer N, with $N > \frac{1}{\beta}$. Using the above claim there exist a

rational no. $\frac{r}{s}$ satisfies

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{Ns} \le \frac{1}{s^2}$$

This implies

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{Ns} < \frac{\beta}{s} < \beta = \left|\alpha - \frac{p}{q}\right|$$

Consequently $\frac{r}{s} \neq \frac{p}{q}$. This means we construct a different rational no $\frac{r}{s}$ with $\frac{r}{s} \neq \frac{p}{q}$ satisfies

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{s^2}$$

Using the mathematical induction we have infinitely many rational numbers $\frac{p}{q}$ satisfies

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

This completes the result. $\square$

Defⁿ: A graph G is a pair (V, E), where V is a non-empty set and E is a collection of sets of the form $\{a, b\}$, where $a, b \in V$.

Example: (a) $V = \{1, 2, 3\}$

$E = \{\{1,2\}, \{1,3\}, \{2,3\}\}$

Pictorial Representation:
(PR)

"Vertices" are represented by "dots" •

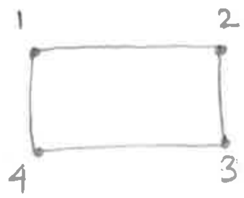
"Edges" are represented by "lines" connecting dots.

(b) $V = \{a, b, c\}$ PR:

$E = \{\{a,b\}, \{b,c\}\}$

(c) $V = \{1, 2, 3, 4\}$ PR:

$E = \{\{1,2\}, \{2,3\}, \{3,4\}, \{4,1\}\}$



(D) $V = \{1, 2, 3, 4\}$ PR:

$E = \{\{1,2\}, \{2,3\}, \{3,4\}, \{4,1\}, \{1,3\}, \{2,4\}\}$

Exercise: Find all the graphs, which contains at most 5 vertices

Hint: Use Pictorial Representations

Nov 17, 2020 9:30 AM

BOOLEAN FUNCTIONS

$\mathbb{Z}_2 = \{0, 1\}$

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

$0' = 1, \ 1' = 0$

$(\mathbb{Z}_2, +, \cdot, ')$ is a Boolean algebra

A Boolean variable is a variable that assumes only two values 0 & 1.

Def^n: Let n be a positive integer. A mapping $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$, where $\mathbb{Z}_2$ is a Boolean algebra is called a Boolean function of n Boolean variables

Example 1: $f : \mathbb{Z}_2^2 \to \mathbb{Z}_2$
$f(x, y) = x + y'$

i.e $f(0,0) = 0+1 = 1$ $\quad f(1,0) = 1+1 = 1$
$f(0,1) = 0+0 = 0$ $\quad f(1,1) = 1+0 = 1$

Exercise: Find all the Boolean functions from $\mathbb{Z}_2^2$ to $\mathbb{Z}_2$.

Example 2: $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2$
$f(x_1, x_2, x_3) = x_1 + x_2' + x_3$

Exercise: Let B_n denote the set of all Boolean fun^{n}s from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$
$B_n = \{ f : f : \mathbb{Z}_2^n \to \mathbb{Z}_2 \}$, where $\mathbb{Z}_2$ is a Boolean algebra.

Then B_n forms a Boolean algebra w.r.to

$+ : B_n \times B_n \to B_n$.
$+(f, g) = f+g$, here $f+g(x_1, \cdots, x_n) = f(x_1 \cdots x_n) + g(x_1 \cdots x_n)$

$\cdot : B_n \times B_n \to B_n$
$\cdot(f, g) = f \cdot g$; here $f \cdot g(x_1 \cdots x_n) = f(x_1 \cdots x_n) \cdot g(x_1 \cdots x_n)$

$' : B_n \to B_n$
$f'(x_1, \cdots, x_n) = [f(x_1, \cdots, x_n)]'$

Claim: The fun^{n}s of the form $x_1^{\epsilon_1} x_2^{\epsilon_2}$, where $x_i^{\epsilon_i} \in \{x_i, x_i'\}$, $i = 1, 2$ are atoms in the Boolean algebra B_2.

Note that $x_1^{\epsilon_1} x_2^{\epsilon_2}$ is one of following fun^{n}s
$\{ x_1 \cdot x_2, \ x_1 \cdot x_2', \ x_1' \cdot x_2, \ x_1' \cdot x_2' \}$

Proof of claim : Note that $x_1 \cdot x_2 = \begin{cases} 1 & x_1 = 1, x_2 = 1 \\ 0 & \text{otherwise} \end{cases}$

To show $x_1 \cdot x_2$ is an atom.

Let $h \in B_2$ satisfies $h + x_1 \cdot x_2 = x_1 \cdot x_2$, i.e $h \leq x_1 \cdot x_2$

Then $h(x_1, x_2) + x_1 \cdot x_2 = x_1 \cdot x_2$

Therefore $x_1 \cdot x_2 = 0 \Rightarrow h(x_1, x_2) = 0$

& $x_1 \cdot x_2 = 1 \Leftrightarrow x_1 = 1, x_2 = 1$, i.e $h(1,1) + 1 = 1$

If $h(1,1) = 1$, then $h = x_1 \cdot x_2$

If $h(1,1) = 0$, then $h = 0$

This implies $h \leq x_1 \cdot x_2$ then either $h = 0$ or $h = x_1 \cdot x_2$,

Similarly, $x_1 \cdot x_2'$, $x_1' \cdot x_2$ and $x_1' \cdot x_2'$ are atoms, which establishes the claim.

Claim : The fu^n^s of the form $x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots x_n^{\epsilon_n}$, where $x_i^{\epsilon_i} \in \{x_i, x_i'\}$ $i = 1, 2, \ldots, n$ are atoms in the Boolean algebra B_n.

Proof of claim : Exercise (Hint : such $x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots x_n^{\epsilon_n}$ assumes 1 only at one point and 0 otherwise)

NOTE : Here we have listed 2^n fu^n^s (atoms) of the form $x_1^{\epsilon_1} \cdot x_2^{\epsilon_2} \ldots x_n^{\epsilon_n}$, where $x_i^{\epsilon_i} \in \{x_i, x_i'\}$ $\forall\ i \in [n]$.

Example : Let $f : \mathbb{Z}_2^2 \to \mathbb{Z}_2$ be a Boolean function

$$f(x_1, x_2) = x_1 + x_2'$$

$\therefore$ $f(0,0) = 1$ $\qquad$ $f(1,0) = 1$

$f(0,1) = 0$ $\qquad$ $f(1,1) = 1$

$\therefore$ f assumes 1 at three points $(0,0)$, $(1,0)$ & $(1,1)$

Note that $x_1' \cdot x_2'$ assumes 1 only at $(0,0)$

$x_1 \cdot x_2'$ assume 1 only at $(1,0)$

$x_1 \cdot x_2$ assume 1 only at $(1,1)$

Hence $f(x_1, x_2) = x_1' \cdot x_2' + x_1 \cdot x_2' + x_1 \cdot x_2 \quad \forall\ x_1, x_2 \in \mathbb{Z}_2$

i.e $x_1 + x_2 = x_1' \cdot x_2' + x_1 \cdot x_2' + x_1 \cdot x_2 \quad \forall\ x_1, x_2 \in \mathbb{Z}$

NOV 17, 2020 9:30 AM

Example : Let $f: \mathbb{Z}_2^2 \to \mathbb{Z}_2$ be a fn i.e unit fn.

$f(x,y) = 1$

$f(0,0)=1$ $f(1,0)=1$

$f(0,1)=1$ $f(1,1)=1$

$$f(x_1,x_2) = x_1\cdot x_2 + x_1\cdot x_2' + x_1'\cdot x_2 + x_1'\cdot x_2'$$

$$= f(1,1)\, x_1\cdot x_2 + f(1,0)\, x_1\cdot x_2' + f(0,1)\, x_1' x_2 + f(0,0)\, x_1'\cdot x_2'$$

NOTE : Each Boolean fn $f: \mathbb{Z}_2^2 \to \mathbb{Z}_2$ can be expressed as

$$f(x,y) = f(0,0)\, x'y' + f(0,1)\, x'y + f(1,0)\, xy' + f(1,1)\, xy$$

In general $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$

$$f(x,y) = \sum f(\lambda_1,\lambda_2,\ldots\lambda_n)\, x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots x_n^{\epsilon_n}$$

$\lambda_i = 0$, then $x_i^{\epsilon_i} = x_i'$ $\lambda_i \in \{0,1\}$

$\lambda_i = 1$, then $x_i^{\epsilon_i} = x_i$ $\forall i \in [n]$

Remark : Each Boolean fn $f: \mathbb{Z}_2^n \to \mathbb{Z}_2$, where $\mathbb{Z}_2$ is a Boolean algebra, can be expressed as sum of the fns of the form $x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots x_n^{\epsilon_n}$, where $\forall\, i \in [n]$, $x_i^{\epsilon_i} \in \{x_i, x_i'\}$.

Thus we have proved the following theorem

Th : The Boolean algebra B_n is atomic and contains 2^n atoms of the form $x_1^{\epsilon_1} x_2^{\epsilon_2} \ldots x_n^{\epsilon_n}$, where $\forall\, i \in [n]$ $x_i^{\epsilon_i} \in \{x_i, x_i'\}$

Exercise : Rewrite the proof of the above theorem.

Nov 18, 2020 9:30 AM

NORMAL FORMS

Defⁿ: Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a Boolean fuⁿ. The expression of f as the sum of atoms in the Boolean algebra B_n is called disjunctive nomal form. of f.

Example: $\forall\ x_1, x_2 \in \mathbb{Z}_2$

$$x_1 + x_2 = x_1 x_2 + x_1 x_2' + x_1' x_2'$$

Atoms in B_2

The expression $x_1x_2 + x_1x_2' + x_1'x_2'$ is disjuntive normal form of the fuⁿ $x_1 + x_2$

Example: $\forall\ x, y, z \in \mathbb{Z}_2$

$$f(x,y,z) = (x+y+z)(x+y+z')(x+y'+z)(x'+y+z)$$

The expression $(x+y+z)(x+y+z')(x+y'+z)(x'+y+z)$ is conjuntive normal form of the fuⁿ $f(x,y,z)$.

Defⁿ: Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be a Boolean fuⁿ. The expression of f as the product of complement of atoms in Boolean algebra B_n is called conjunctive normal form.

Example: Consider the fuⁿ $f : \mathbb{Z}_2^3 \to \mathbb{Z}_2$

$$f(x,y,z) = yz + y'z'$$

Then

x	y	z	yz	$y'z'$	f	f'
0	0	0	0	1	1	0
0	0	1	0	0	0	1
0	1	0	0	0	0	1
0	1	1	1	0	1	0
1	0	0	0	1	1	0
1	0	1	0	0	0	1
1	1	0	0	0	0	1
1	1	1	1	0	1	0

Hence the disjuntive normal form of $f(x,y,z)$ is

$$x'y'z' + x'yz + xy'z' + xyz$$

The conjunctive normal form of $f(x,y,z)$ is

$$[f'(x,y,z)]' = [x'y'z + x'yz' + xy'z + xyz']'$$

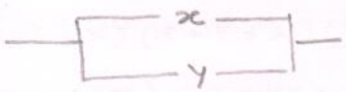
$$= (x+y+z')(x+y'+z)(x'+y+z')(x'+y'+z)$$

Nov 18, 2020 9:30 AM

SWITCHING CIRCUITS

A Boolean variable represents the state of the electrical "switch" and a Boolean fn represents the state of an electrical "circuits" where the switchs are present.

- State of switchs : Open or closed
- State of circuit : Current flows or does not flow
- Open switch allows to flow the current and closed switch does not allow to flow the current.
- For a switch x, x' denotes its complementary state i.e if x is open, then x' is closed and vice versa.
- Circuit representation of the addition of switches x & y i.e $x+y$ is



OR x & y connected in "parallel"

- Circuit representation of the multiplication of switches x & y i.e $x \cdot y$ is

OR x & y connected in "series"

- $x+y$ is open if at least one of the switchs x & y is open

x	y	$x+y$
0	0	0
0	1	1
1	0	1
1	1	1

0 represents switch is off (closed)
1 represents switch is on (open).

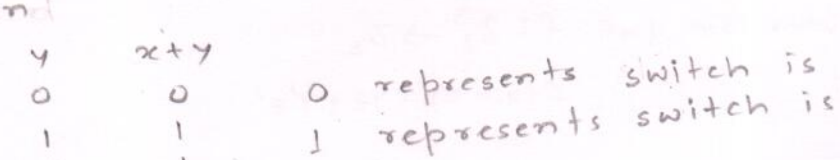
- $x \cdot y$ is open if both x and y are open

x	y	$x \cdot y$
0	0	0
0	1	0
1	0	0
1	1	1

Example : Let $f: \mathbb{Z}_2^3 \to \mathbb{Z}_2$ be a Boolean fn

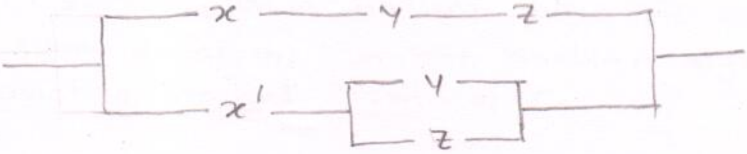
(A) $f(x,y,z) = xyz + xy'(z+z')$

The circuit representation (CR) of such f is



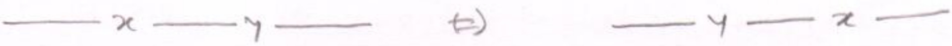
Nov 18, 2020 9:30 AM

(B) If $f(x,y,z) = xyz' + x'(y+z)$ $\forall$ $x,y,z \in \mathbb{Z}_2$, then its CR

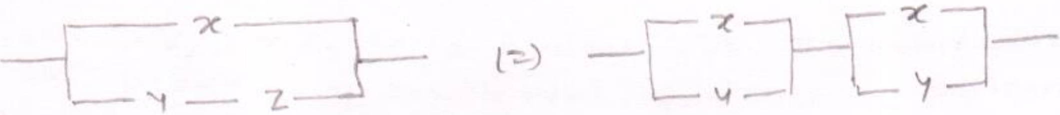


Circuit representations of operations

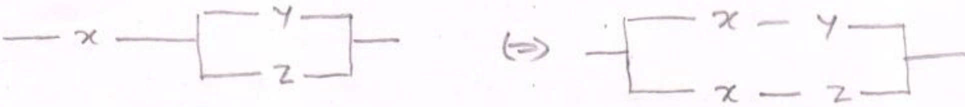
$$x+y = y+x$$



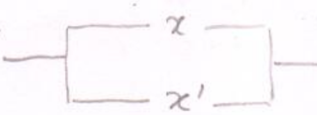
$$xy = yx$$



$$x + y \cdot z = (x+y)(x+z)$$



$$x \cdot (y+z) = x \cdot y + x \cdot z$$



$x + x' (\equiv 1)$

$x \cdot x' (\equiv 0)$

SOME APPLICATIONS PIGEONHOLE PRINCIPLE

Defn:
- A graph H is said to a subgraph of G if each vertex and edge of H is also a vertex and edge of G respectively.
- A graph is said to be complete graph if any two vertices form an edge (i.e for any two vertices a, b with $a \neq b$ $\{a,b\}$ form an edge). A complete graph with n vertices, where n is a positive integer, is denoted as $\mathbb{K}_n$.

Example: $\mathbb{K}_3$ PR: , $\mathbb{K}_5$ PR: 

$\mathbb{K}_4$ PR: ,

K_2 PR: 

OR

$\mathbb{K}_6$ PR: ,

Exercise: Show that complete graph with n vertices has $\frac{n(n-1)}{2}$ edges

Note: $\mathbb{K}_n$ contains $\mathbb{K}_{n-1}$ as a subgraph, where $n \geq 4$ is an integer.

Defn: The edge colouring by two colours of a graph G is a fun $C : E(G) \longrightarrow \{1,2\}$, where $E(G)$ denotes the edge set of the graph G.

Note: Edge colouring by two colours facilitates the following
- It provides a partition inside the edge set of a graph G namely $C^{-1}(1)$ and $C^{-1}(2)$ where $C : E(G) \longrightarrow \{1,2\}$ is the edge colouring.
- If $C : E(G) \rightarrow \{1,2\}$ is an edge colouring, then both $C^{-1}(1)$ and $C^{-1}(2)$ are subgraphs of G (under lens)
- When we quest for existance of certain subgraph H of the n vertex graph G, then we look for one among the $2^{|E(G)|}$ edge colouring with two colours of G identifies such subgraph H.

- We quest for a graph G such that any edge colouring by two colours produces a complete subgraph with r vertices i.e $\mathbb{K}_r$.
- We quest for a graph G such that any edge colouring by two colours produces either a complete subgraph with r vertices i.e $\mathbb{K}_r$ or a complete subgraph with s vertices i.e $\mathbb{K}_s$.

Note: Any edge colouring by two colours of $\mathbb{K}_3$ identifies the subgraph

Exercise: Find all the edge colouring with 2 colours of a graph with 4 vertices.

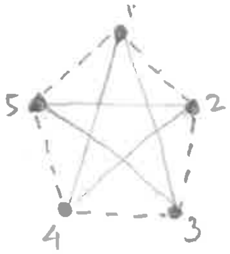
Def^n: Let r and s be two integers with $r \geq 2$ $s \geq 2$. The <u>Ramsey</u> number is the smallest positive integer n with the property that each edge colouring by two colours of $\mathbb{K}_n$ <u>produces</u> a monochromatic copy of $\mathbb{K}_r$ or $\mathbb{K}_s$

(i.e $\forall$ $c : E(\mathbb{K}_n) \to \{1,2\}$, if $c^{-1}(1)$ does not contain the subgraph $\mathbb{K}_r$, then $c^{-1}(2)$ must contain the subgraph $\mathbb{K}_s$)

Such positive integer n is denoted as $R(r,s)$.

Exercise: Show that there exists an edge colouring by two colours of $\mathbb{K}_5$ i(say) $c : E(\mathbb{K}_5) \to \{1,2\}$ such that neither $c^{-1}(1)$ nor $c^{-1}(2)$ contains the subgraph $\mathbb{K}_3$.

Sol^n:



$c : E(\mathbb{K}_5) \to \{1,2\}$

$$c(\{x,y\}) = \begin{cases} 1 & \text{if } \{x,y\} = \{1,2\} \\ & \quad = \{2,3\} \\ & \quad = \{3,4\} \\ & \quad = \{4,5\} \\ & \quad = \{1,5\} \\ 2 & \text{otherwise} \end{cases}$$

Then <u>such</u> c is the required edge colouring by two colours

---

Footnote: An edge colouring by two colours of $\mathbb{K}_n$, say $c : E(\mathbb{K}_n) \to \{1,2\}$ Produces <u>monochromatic copy of</u> $\mathbb{K}_r$ or $\mathbb{K}_s$ means either $c^{-1}(1)$ contains a copy of $\mathbb{K}_r$ or $c^{-1}(2)$ contains a copy of $\mathbb{K}_s$

Oct 19, 2020 9:30 AM

Def^n: Let n and K be positive integers with $n \geq K$. An unordered K-tuple $(a_1, a_2, \cdots, a_K)$ is said to be a <u>partition</u> of the integer n into K positive integers if $a_1, a_2, \cdots, a_K$ are positive integer and
$$n = a_1 + a_2 + \cdots + a_K$$
The integer $P_K(n)$ denotes the total no. of ways in which the integer n can be partitioned into K positive integers.

Th: Let n and K be positive integers with $n \geq K$, then
$$P_K(n) = P_{K-1}(n-1) + P_K(n-K)$$

Proof: $\mathcal{P}(n,K)$ = The set of all (unordered) partitions of the integer n into K positive integers
$$= \left\{ (a_1, a_2, \cdots, a_K) : \begin{array}{l} (a_1, \cdots a_K) \text{ is an unordered } K\text{-tuple} \\ \text{of positive integers satisfy} \\ a_1 + a_2 + \cdots + a_n = n \end{array} \right\}$$

$$\mathcal{A} = \{ (a_1, \cdots, a_K) \in \mathcal{P}(n,K) : a_i = 1 \text{ for some } i \in [K] \}$$

$$\mathcal{B} = \{ (a_1, \cdots, a_K) \in \mathcal{P}(n,K) : \forall\, i \in [K]\ a_i \geq 2 \}$$

Claim: $|\mathcal{A}| = P_{K-1}(n-1)$

Proof of claim: Let $(a_1, a_2, \cdots a_K) \in \mathcal{A}$, without loss of generality let $a_K = 1$. This induces a partition of the integer $(n-1)$ in $(K-1)$ positive integers namely $(a_1, a_2, \cdots a_{K-1})$. Conversely if $(b_1, b_2, \cdots, b_{K-1}) \in \mathcal{P}(n-1, K-1)$, then $(b_1, b_2, \cdots, b_{K-1}, 1) \in \mathcal{A}$. Hence a bijective correspondence exists between $\mathcal{P}(n-1, K-1)$ and $\mathcal{A}$, and the claim is established.

Claim: $|\mathcal{B}| = P_K(n-K)$

Proof of claim: We note that
$$(a_1, a_2, \cdots, a_K) \mapsto (a_1 - 1, a_2 - 1, \cdots, a_K - 1),$$
where $(a_1, \cdots a_K) \in \mathcal{B}$ and $(a_1 - 1, a_2 - 1, \cdots, a_K - 1) \in \mathcal{P}_K(n-K)$, is a one-one onto mapping, which establishes the claim. □

Oct 19, 2020, 9:30 AM

$\frac{2}{2}$

Th : One can distribute n identical objects into k identical boxes such that each box contains at least one identical object into $P_k(n)$ ways.

Proof: $\mathcal{D}$ = The set of all distributions of n identical objects into k identical boxes such that each box contains at least one identical object.

$\mathcal{P}(n,k)$ = The set of all (unordered) partitions of the integer n into k positive integers.

$$\mathcal{D} \longleftrightarrow \mathcal{P}(n,k)$$

Distribution of n identical objects into k identical boxes such that each box is non empty yields a partition of the integer n into k positive integers and vice versa. (Exercise)

So such distribution can be done in $|\mathcal{P}(n,k)| = p_k(n)$ ways. $\square$

Th: One can distribute n identical objects into k identical boxes into $\sum_{i=1}^{k} P_i(n)$ ways.

Proof: Exercise.

Example: In Statistical Mechanics, one encounters the situation of putting n particles into k distinct energy levels.

The n particles thus be considered an n objects and the k different energy levels as k distinguishable boxes.

THREE different statistics (situations) are obtained by making three different assumptions:

- Maxwell-Boltzman: Here n distinguishable objects (particles) are distributed into k distinguishable boxes (distinct energy levels). Hence the no. of possibilities is k^n
- Bose-Einstein: Here n identical objects (particles) are distributed into k distinguishable boxes (distinct energy levels). Hence the no. of possibilities is $\binom{n+k-1}{k-1}$
- Fermi-Dirac: Here n identical objects (particles) are distributed into k distinguishable boxes (distinct energy levels) but no box can hold more than one object (particle). Hence the no. of possibilities is $\binom{k}{n}$.

Nov 20, 2020 8:30 AM

BLOCK DESIGN

Defⁿ : An incidence system is a triple $(P, \mathcal{B}, I)$, where P and $\mathcal{B}$ are non empty sets and I is a non-empty subset of $P \times \mathcal{B}$.

The elements of P are called points and the elements of $\mathcal{B}$ are called blocks. I denotes the incident relation between P & $\mathcal{B}$.

Comment: $I \subset P \times B$, if $(p, B) \in I$, we usually write pIB and say that $p \in P$ is incident with $B \in \mathcal{B}$.

Example: (A) Take $P = \{a, b, c\}$

$$\mathcal{B} = \{\{a,b\}, \{b,c\}, \{c,a\}\}$$

$$I = \{(a,\{a,b\}), (a,\{c,a\}), (b,\{a,b\}), (b,\{b,c\}) \\ (c,\{b,c\}), (c,\{c,a\})\}$$

(B) Take a non-empty set P and $\mathcal{B}$ is a collection of subsets of P, then $(P, \mathcal{B}, \in)$ is an incidence system

Defⁿ : Let $(P_1, \mathcal{B}_1, I_1)$ and $(P_2, \mathcal{B}_2, I_2)$ be two incidence system. We say $(P_1, \mathcal{B}_1, I_1)$ and $(P_2, \mathcal{B}_2, I_2)$ are isomorphic if there exist two bijective fuⁿs $f: P_1 \to P_2$ and $g: \mathcal{B}_1 \to \mathcal{B}_2$ such that $\forall\ p \in P_1$ & $B \in \mathcal{B}_1$ if pI_1B, then $f(p) I_2 g(B)$ and if $f(p) I_2 g(B)$ then pI_1B.

Example: Let $(P_1, \mathcal{B}_1, \in)$ and $(P_2, \mathcal{B}_2, \in)$ be two incidence system such that "$\in$" is the incidence relation in both. (Thus for $i = 1, 2$, $\mathcal{B}_i$ is a collection of subsets of P_i)

Now $(P_1, \mathcal{B}_1, \in)$ and $(P_2, \mathcal{B}_2, \in)$ are isomorphic

Then there exist two bijective mappings $f: P_1 \to P_2$ & $g: \mathcal{B}_1 \to \mathcal{B}_2$ such that $\forall\ p \in P_1$ and $B \in \mathcal{B}$, if $p \in B$ then $f(p) \in g(B)$ and if $f(p) \in g(B)$ then $p \in B$.

Note that if $p \in B$, then $f(p) \in g(B)$ and if $f(p) \in g(B)$ then $p \in B$, where $p \in P_1$ & $B \in \mathcal{B}_1$.

This implies $g(B) = \{f(p) : p \in B\}$, $\forall\ B \in \mathcal{B}_1$

$$= f(B)$$

Thus g is determined by $f: P_1 \to P_2$. In this situation we abuse the notation and we say f is an isomorphism.

Example : Take $P = \{a, b, c\}$, $\mathcal{B} = \{\{a,b\}, \{a,c\}, \{b,c\}\}$

$I = \{(a, \{a,b\}), (a, \{a,c\}), (b, \{a,b\}), (b, \{b,c\})$
$(c, \{a,c\}), (c, \{b,c\})\}$.

& $P' = \{1, 2, 3\}$, $\mathcal{B}' = \{\{1,2\}, \{1,3\}, \{2,3\}\}$.

$I' = \in$

Then $f : P \to P'$ by $a \mapsto 1$, $b \mapsto 2$ & $c \mapsto 3$.
is an isomorphism.

Def^n: A $2-(v, k, \lambda)$ design or a 2-design with parameters (v, k, λ)
v, k, λ is an incidence system $(P, \mathcal{B}, I)$ satisfies
the following conditions.

ⓐ There are v points (i.e $|P| = v$)
ⓑ Each block $B \in \mathcal{B}$ is incident with exactly k points.
ⓒ Any two distrinct points are together incident with exactly λ blocks.

Example ;

Ⓐ Let P be a v-set (i.e $|P| = v$). $\mathcal{B}$ be the collection of all k-subsets of P & $I = \in$

Then $(P, \mathcal{B}, \in)$ is a $2-(v, k, \binom{v-2}{k-2})$ design.

Ⓑ Take $P = [7]$, $\mathcal{B} = \left\{ \begin{array}{l} \{1,2,3\}, \{1,4,5\}, \{1,6,7\} \\ \{2,4,6\}, \{2,5,7\}, \{3,4,7\}, \{3,5,6\} \end{array} \right\}$

$I = \in$.

Then $(P, \mathcal{B}, \in)$ is a $2-(7, 3, 1)$ design.

Ⓒ Take $P = [4]$, $\mathcal{B} = \{\{1,2\}, \{3,4\}, \{1,3\}, \{2,4\}, \{1,4\}, \{2,3\}\}$
& $I = \in$.

Then $(P, \mathcal{B}, \in)$ is a $2-(4, 2, 1)$ design.

Th: Let D be a $2-(v,k,\lambda)$ design. Then there are constants b and r such that there are exactly b blocks in D and each point of D is incident with exactly r blocks. These auxiliary parameters b & r satisfies the following formulas

(i) $r(k-1) = \lambda(v-1)$

(ii) $bk = rv$

$\boxed{\text{i.e } r = \frac{\lambda(v-1)}{k-1} \qquad b = \frac{\lambda v(v-1)}{k(k-1)}}$

Proof: (i) Fix a point x of D

$r(x)$ = The no. of blocks of D which are incident with x

Count two ways the following set of pairs

$\{(y,B) : y \neq x,\ x I B,\ y I B,\ B \text{ is block of } D\}$

Here I denote the incident relation

First way: There are $(v-1)$ choices of y. Having chosen y there are exactly λ choices of B s.t $\{x,y\} \subset B$.

Hence there are $(v-1)\lambda$ pairs,

Second way: There are $r(x)$ no. of blocks in D, which are incident with x. Hence there are $r(x)$ no. of choices of B. Having chosen B, there are exactly $(k-1)$ choices of y s.t $\{x,y\} \subset B$.

Hence there are $r(x) \cdot (k-1)$

Hence $(v-1)\lambda = |\{(y,B) : y \neq x,\ x I B,\ y I B,\ B \text{ is a block of } D\}|$

$= r(x)(k-1)$

So $r(x) = \frac{(v-1)\lambda}{k-1}$ is independent of choses of x

$\forall$ point x of D $r(x)$ is same. We denote this number as r.

(ii) Count two ways the following set of pairs.

$\{(x,B) : x \text{ is a point of } D \text{ and incident with the block } B \text{ of } D\}$

First way: There are v no. of choices of x. Having chosen x, there are r choises of B which are incident with x.

Hence there are $v \cdot r$ pairs

Second way: If we assume there are b blocks in D. Then there are b no. of choices of B. Having chosen B, there are k no. of choices of x which are incident with such B.

Hence there are $b \cdot k$ pairs

Therefore $v \cdot r = |\{(x,B) : x \text{ is a point of } D \text{ such that } x \text{ is incident with } B \text{ and } B \text{ is block of } D\}| = bk$ □

PRINCIPLE OF INCLUSION AND EXCLUSION

Th: (Inclusion and Exclusion theorem: Version I) Let A be a finite set and for each $i \in [n]$, $A_i \subset A$. Then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i\geq 1}^{n} |A_i| + (-1)^{2-1}\left(\sum_{1\leq i<j\leq n} |A_i \cap A_j|\right)$$

$$\cdots + (-1)^{k-1}\left(\sum_{1\leq i_1<i_2\cdots<i_k\leq n} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|\right)$$

$$\cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

Proof: Exercise. Hint: Use induction on n.

Th: (Inclusion and Exclusion theorem: Version II) Let $\Theta : \mathcal{P}([n]) \to \mathbb{R}$ be a mapping and $\Pi : \mathcal{P}([n]) \to \mathbb{R}$ be a mapping defined by:

$$\Pi(X) = \sum_{S \subseteq X} \Theta(S),$$

where $\mathcal{P}([n])$ denotes the collection of all subsets of $[n]$.

Then $$\Theta(X) = \sum_{S\subseteq X} (-1)^{|X|-|S|}\, \Pi(S), \quad \forall\ X \subset [n].$$

Proof:

$$\sum_{S\subseteq X} (-1)^{|X|-|S|}\, \Pi(S) = \sum_{S\subseteq X} (-1)^{|X|-|S|} \sum_{T\subseteq S} \Theta(T)$$

$$\overset{??}{=} \Theta(X) + \sum_{Y \subsetneq X} \Theta(Y)\left(\sum_{Y\subseteq S\subsetneq X} (-1)^{|X|-|S|}\right)$$

$$= \Theta(X) + \sum_{Y\subsetneq X} \Theta(Y)\left(\sum_{P\subseteq X\setminus Y} (-1)^{|P|}\right)$$

$$= \Theta(X) + \sum_{Y\subsetneq X} \Theta(Y)\left((-1+1)^{|X|-|Y|}\right) \;??$$

$$= \Theta(X)$$

This completes the proof.

Th: (Inclusion and exclusion theorem: Version III): Let X be a finite set and

$\forall i \in [m]$, P_i is a property. For each $x \in X$ and $i \in [m]$, either x satisfies property P_i or (exclusive "or") x does not satisfy property P_i. Let $S \subseteq [m]$

$$N(S) = \{x \in X : x \text{ satisfies property } P_i \ \forall i \in S\}$$

Then the no. of elements of X that satisfy none of the properties $P_1, P_2 \ldots P_m$ is given by

$$\sum_{S \subseteq [m]} (-1)^{|S|} |N(S)|$$

$$\left[\begin{array}{ll} X & P_1, P_2, \ldots, P_m \\ N(S) \subset X & S \subset [m] \end{array}\right]$$

Proof: Let $x \in X$ $\quad S_x = \{i \in [m] : x \text{ satisfies } P_i\} \subset S$

$$N(S) = \{x \in X : S \subset S_x\}$$

$$\sum_{S \subseteq [m]} (-1)^{|S|} |N(S)| = \sum_{S \subseteq [m]} (-1)^{|S|} |\{x \in X : S \subseteq S_x\}|$$

$$= \sum_{S \subseteq [m]} (-1)^{|S|} \sum_{\substack{x \in X \\ S \subset S_x}} 1$$

$$= \sum_{S \subseteq [m]} \sum_{\substack{x \in X \\ S \subset S_x}} (-1)^{|S|} = \sum_{S \subset S_x \subset [m]} \sum_{x \in X} (-1)^{|S|}$$

$$= \sum_{x \in X} \sum_{S \subseteq S_x} (-1)^{|S|}$$

$$= \sum_{x \in X} \sum_{S_x = \phi} 1 + \sum_{x \in X} \sum_{\substack{S_x \neq \phi, \\ S \subset S_x}} (-1)^{|S|}$$

$$= |\{x \in X : S_x = \phi\}| + \sum_{x \in X} (-1+1)^{|S_x|}$$

$$= |\{x \in X : S_x = \phi\}|$$

The result follows since

$$|\{x \in X : x \text{ does not satisfy property } P_1, P_2, \ldots, P_m\}|$$
$$= |\{x \in X : S_x = \phi\}| \qquad \square$$

Th: Let $S(n,k)$ denote the Stirling number of second kind, where n and k are positive integers with $n \geq k$, then

$$S(n,k) = \frac{1}{k!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$$

Proof: $A([n],[k])$ = The set of all functions $f:[n] \to [k]$

Recall $|A([n],[k])| = k^n$

$O([n],[k])$ = The set of all onto functions $f:[n] \to [k]$

We define properties $P_1, P_2, \ldots, P_k$ where $\forall i \in [k]$ P_i is the property that i does not belong to the image of $f \in A([n],[k])$.

Note that the set of elements of $A([n],[k])$ that satisfy none of the properties $P_1, P_2, \ldots, P_k$ is the set of all onto fu^ns. $O([n],[k])$.

For $S \subseteq [k]$, let

$$N(S) = \{ f \in A([n],[k]) : f \text{ satisfies property } P_i \text{ for each } i \in S \}$$

Claim: For $S \subseteq [k]$, $|N(S)| = (k-|S|)^n$.

Proof of claim: We note the following

$f \in N(S) \Leftrightarrow f$ satisfies property P_i for each $i \in S$

$\Leftrightarrow i$ does not belong to the image of f $\forall i \in S$

$\Leftrightarrow S$ is not in the image of f

$\Leftrightarrow f$ is a function from $[n]$ to $[k] \setminus S$

Hence the claim is established.

Therefore using the version II of inclusion and exclusion theorem and the above claim, we have

$$|O([n],[k])| = \sum_{S \subseteq [k]} (-1)^{|S|} |N(S)| = \sum_{S \subseteq [k]} (-1)^{|S|} (k-|S|)^n$$

$$= \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n$$

The result follows, since $S(n,k) = \frac{1}{k!} |O([n],[k])|$. $\square$

Oct 21, 2020 9:30 AM

Defⁿ: A permutation $\pi : [n] \to [n]$ is called <u>derangement</u> if for each $i \in [n]$, $\pi(i) \neq i$. The set of all derangements on $[n]$ is denoted as D_n.

Th: For each positive integer n,

$$|D_n| = \sum_{j=0}^{n} (-1)^j \binom{n}{j} (n-j)!$$

Proof: S_n = The set of all permutations on $[n]$

We define the properties $P_1, P_2, \ldots, P_n$, where $\forall i \in [n]$, P_i denote the property that $\pi(i) = i$, where $\pi \in S_n$

Note that the set of all elements of S_n that satisfy none of the properties $P_1, P_2, \ldots, P_n$ is the set of all derangements D_n

For $S \subseteq [n]$, let

$$N(S) = \{ \pi \in S_n : \pi \text{ satisfies properties } P_i \ \forall i \in S \}.$$

Claim: For $S \in [n]$, $|N(S)| = (n - |S|)!$

Proof of claim: We note the following

$$\begin{aligned}
\pi \in N(S) &\Leftrightarrow \pi \text{ satisfies property } P_i \ \forall i \in S \\
&\Leftrightarrow \pi(i) = i \ \forall i \in S \\
&\Leftrightarrow \pi : [n] \setminus S \to [n] \setminus S \text{ is an induced permutation on } [n] \setminus S.
\end{aligned}$$

Hence the claim is established.

Therefore using the version III of inclⁿ & exclⁿ principle and the above claim

$$|D_n| = \sum_{S \subseteq [n]} (-1)^{|S|} |N(S)| = \sum_{S \subseteq [n]} (-1)^{|S|} (n - |S|)!$$

Hence the result follows. $\square$

SOME APPLICATIONS OF PIGEONHOLE PRINCIPLE

Th: If $c : E(\mathbb{K}_6) \to \{1,2\}$ is an edge colouring with two colours of $\mathbb{K}_6$, then either $c^{-1}(1)$ or $c^{-1}(2)$ contains a "copy of $\mathbb{K}_3$"

Proof: Recall that the vertex set of $\mathbb{K}_6$ is $\{1,2,3,4,5,6\} = [6]$ and $\forall\ x, y \in [6]$ with $x \neq y$, $\{x, y\}$ is an edge of $\mathbb{K}_6$

Let $c : E(\mathbb{K}_6) \to \{1,2\}$ is an edge colouring by two colours of $\mathbb{K}_6$. We consider all the 5 edges

$$\{1,2\}, \{1,3\}, \{1,4\}, \{1,5\}, \{1,6\}$$

as 5 objects and two colours as 2 boxes

Using pigeonhole principle there exist 3 objects namely

$$\{1,a\}, \{1,b\}, \{1,c\}, \text{ where } a, b, c \in \{2,3,4,5,6\},$$

must have same colour, i.e either

$$\{\{1,a\}, \{1,b\}, \{1,c\}\} \subset c^{-1}(1)$$

$$\text{or } \{\{1,a\}, \{1,b\}, \{1,c\}\} \subset c^{-1}(2).$$

Without loss of generality, suppose

$$\{\{1,a\}, \{1,b\}, \{1,c\}\} \subset c^{-1}(1)$$

i.e $\{1,a\}, \{1,b\}, \{1,c\}$ receives the colour 1.

We consider all the 3 edges

$$\{a,b\}, \{a,c\}, \{b,c\}.$$

as 3 objects and two colours as 2 boxes

If all of them receives the colour 2, i.e

$$\{\{a,b\}, \{a,c\}, \{b,c\}\} \subset c^{-1}(2),$$

then $\{\{a,b\}, \{a,c\}, \{b,c\}\}$ is the required copy of $\mathbb{K}_3$.

Otherwise, using pigeonhole principle we conclude that at least one among $\{a,b\}$, $\{a,c\}$ and $\{b,c\}$ (say $\{a,b\}$) must receive colour 1. Therefore

$$\{\{1,a\}, \{1,b\}, \{a,b\}\} \subset c^{-1}(1)$$

i.e $\{\{1,a\}, \{1,b\}, \{a,b\}\}$ is the required copy of $\mathbb{K}_3$. $\square$

Corollary: $R(3,3) = 6$

Sept 22, 2020 9:30 AM

RAMSEY NUMBERS - I

Remark: The above corollary may be interpreted as "among any 6 persons either there exist a set of 3 persons who are known to each-other or there is a set of 3 persons who are unknown to each other." $\frac{1}{1}$

Th: $R(r,2) = r$ and $R(2,s) = s$, where $r \geq 2$ and $s \geq 2$ are integers.

Proof: Let $c : E(\mathbb{K}_r) \to \{1,2\}$ be an edge colouring with two colours of the graph (complete graph) $\mathbb{K}_r$.

Note that $E(\mathbb{K}_r) \subset c^{-1}(1) \sqcup c^{-1}(2)$

(symbol for disjoint uni

This means $c^{-1}(1)$ contains either all the edges of $\mathbb{K}_r$ or some edges of $\mathbb{K}_r$.

i.e $c^{-1}(1)$ contains either a copy of $\mathbb{K}_r$ or a copy of $\mathbb{K}_2$.

Therefore $R(r,2) \leq r$

Suppose, if possible, $R(r,2) \leq r-1$.

We consider the edge colouring by two colours

$$c : E(\mathbb{K}_{r-1}) \to \{1,2\}$$
$$c(\{x,y\}) = 1 \quad \forall \{x,y\} \in E[\mathbb{K}_{r-1}).$$

So $c^{-1}(1)$ contains a copy of $\mathbb{K}_{r-1}$ & $c^{-1}(2)$ is empty

i.e neither $c^{-1}(1)$ contains a copy of $\mathbb{K}_r$ nor $c^{-1}(2)$ contains a copy of $\mathbb{K}_2$

— A contradiction arises.

Hence $R(r,2) \geq r$. and the result follows

Similarly $R(2,s) = s$ (Exercise). □

Th: $R(r,s) = R(s,r)$, where $r \geq 2$ and $s \geq 2$ are integers

Proof: Exercise

Hint: If $c : E(\mathbb{K}_n) \to \{1,2\}$ is an edge colouring with two colours then $\bar{c} : E(\mathbb{K}_n) \to \{1,2\}$

$$\bar{c}(1) = c(2)$$
$$\bar{c}(2) = c(1)$$

is also an edge colouring by two colours, where n is a positive integer.

Nov 23, 2020 9:30 AM

FISHER INEQUALITY

Remark: b, v, r, k, λ are 5 parameters of any 2-design. They are related by $bk = rv$. $r(k-1) = \lambda(v-1)$.

Note that $r \geq \lambda$ is a necessary condition.
If $r = \lambda$, then $v = k$ & $b = r$ (i.e every point is incident with every block). Conversely if $v = k$, then $r = \lambda$.

We call a 2-design <u>non-trivial</u> if $r \geq \lambda + 1$ (equivaletly $v \geq k+1$). The number $r - \lambda$ is called the <u>order</u> of the 2-design.

Defn: The incidence system $(\mathcal{B}, P, I)$ is called dual incidence system of the incidence system $(P, \mathcal{B}, I)$.

Th: (Fisher's Inequality): The parameters of a non-trivial 2-design satisfy $b \geq v$ (equivalently $r \geq k$). Equality holds (i.e $b = v$ (equivalently $r = k$)) if and only if the dual of a 2-design is again a 2-design

Proof: (R. C. Bose) Let D be a non trivial 2-design

Let N be $b \times v$ incidence matrix of D
i.e Rows and columns of N are indexed by blocks and points

$$N = \begin{array}{c} \\ B_1 \\ B_2 \\ \vdots \end{array} \begin{array}{c} v_1 \; v_2 \cdots \\ \left[\begin{array}{ccc} & & \\ & & \\ & & \\ & & \end{array} \right]_{b \times v} \end{array}$$

Eg.
$$\begin{array}{c} \\ \{1,2,3\} \\ \{1,4,5\} \\ \{1,6,7\} \\ \{2,4,6\} \\ \{2,5,7\} \\ \{3,4,7\} \\ \{3,5,6\} \end{array} \begin{array}{c} \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \left[\begin{array}{ccccccc} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array} \right]_{7 \times 7} \end{array}$$

$\Big\{$ Incidence matrix: $[a_{ij}]_{b \times v} = N$
If $\mathcal{B} = \{B_1, B_2, \ldots, B_i, \ldots B_b\}$
$P = \{P_1, P_2, \ldots, p_j, \ldots P_v\}$ $\quad a_{ij} = \begin{cases} 1 & \text{if } p_j \in B_i \\ 0 & \text{othewise} \end{cases}$

In the incidence matrix N, each row has exactly k non zero entries and each column has exactly r non-zero entries.

Now $N^T N = [b_{ij}]_{v \times v}$ where $b_{ij} = \begin{cases} \lambda & \text{if } i \neq j \\ r & \text{if } i = j \end{cases}$

$= (r - \lambda) I_v + \lambda J_v$ where I_v is $v \times v$ identity matrix and $J_v = [c_{ij}]_{v \times v}$ with $c_{ij} = 1 \; \forall \, i, j$

Nov 23, 2020 9:30 AM

Note that $v = \text{rank}((r-\lambda)I_v + \lambda J_v) = \text{rank}(N^TN) = \text{rank}(N)$

Since N is a $b \times v$ matrix, we have

$$v = \text{rank}(N) \leq b.$$

Note that $v \leq b \iff k \leq r$

If $b = v$, then N is a square matrix order v and

$$v = \text{rank}(N).$$

Hence N is a non-singular (i.e invertible) square matrix of order v. Here each point is incident with k blocks (as $r = k$) and each block is incident with k points.

Note that $NN^T = [d_{ij}]_{b\times b}$, where $d_{ij} = \begin{cases} k & \text{if } i=j \\ \lambda & \text{if } i \neq j \end{cases}$

$$= (k-\lambda)I_v + \lambda J_v = (k-\lambda)I_b + \lambda J_b$$

$$\left[N^TN = (k-\lambda)I_v + \lambda J_v \iff N^T = (k-\lambda)I_vN^{-1} + \lambda J_vN^{-1} \right.$$
$$\iff NN^T = (k-\lambda)I_v + \lambda NJ_vN^{-1}$$
$$\left. \iff NN^T = (k-\lambda)I_v + \lambda J_v \quad \left[\text{As } r=k,\ NJ_v = kJ_v = J_vN\right] \right]$$

So the inner product between any two distinct rows of N^T is λ. This means any two distinct blocks are incident with λ points.

Thus if $b = v$ and $r = k$, then (a) there are v blocks (b) each point is incident with k blocks and (c) any two distinct point are incident with λ points

i.e the dual of D is a $2-(v,k,\lambda)$ design.

Conversely suppose dual of D is a $2-(v,k,\lambda)$ design. If v^* is no. of points in the dual of D. then $v^* = v$. But $v^* = b$, i.e $b = v$. □

Def^n: A $2-(v,k,\lambda)$ design is called square design if $b = v$ and $r = k$.

(i.e A design is square if its incidence matrix is a square matrix).

Sept 23, 2020 9:30 AM

$\left(\frac{1}{2}\right)$

RAMSEY NUMBERS - II

Th: $R(r,s) \le R(r-1,s) + R(r,s-1)$, where $r \geqslant 3$ and $s \geqslant 3$ are integers.

Proof: Let $N = R(r-1,s) + R(r,s-1)$. and consider an edge colouring by two colours (say) $c: E(\mathbb{K}_N) \longrightarrow \{1,2\}$.
We have to show $c^{-1}(1)$ contains a copy of $\mathbb{K}_r$ or $c^{-1}(2)$ contains a copy of $\mathbb{K}_s$.
We suppose $c^{-1}(2)$ does not contain a copy of $\mathbb{K}_s$
Therefore we have to show $c^{-1}(1)$ contains a copy of $\mathbb{K}_r$.
We fix a vertex x of $\mathbb{K}_N$ and consider

$$A_1 = \{a : c(\{x,a\}) = 1\}$$

$$A_2 = \{A : c(\{x,a\}) = 1\}$$

claim: Either $|A_1| \geqslant R(r-1,s)$ or $|A_2| \geqslant R(r,s-1)$

Proof of claim: Suppose (if possible) $|A_1| \le R(r-1,s) - 1$
and $|A_2| \le R(r,s-1) - 1$

This means,

$$N-1 = \left|\{y : c(\{x,y\}) = 1 \text{ or } c(\{x,y\}) = 2\}\right| = |A_1| + |A_2| \le R(r-1,s) + R(r,s-1) - 2 = N-2$$

— A contradiction arises, which establishes the claim.

Case I: Suppose $|A_1| \geqslant R(r-1,s)$ holds

In this case, we consider the subgraph with the vertices of A_1 of the complete graph $\mathbb{K}_N$ and call it (A_1, E_1). Since $N \geqslant R(r-1,s)$ we have either $c^{-1}(1)$ contains a copy of $\mathbb{K}_{r-1}$ or $c^{-1}(2)$ contains a copy of $\mathbb{K}_s$

Since we assume, $c^{-1}(2)$ does not contain a copy of $\mathbb{K}_s$. We have $c^{-1}(1)$ contain a copy of $\mathbb{K}_{r-1}$ and $E_1 \subseteq c^{-1}(1)$. Hence the edges of the complete subgraph with the vertices of $A_1 \uplus \{x\}$ is contained in $c^{-1}(1)$ and it contains a copy of $\mathbb{K}_r$ and the result follows.

Case II: Suppose $|A_2| \geqslant R(r,s-1)$ holds

In this case, we consider the complete subgraph with the vertices of A_2 of the complete graph $\mathbb{K}_N$ and call it (A_2, E_2)

Since $N \geq R(r, s-1)$, we have either $c^{-1}(1)$ contains a copy of $\mathbb{K}_r$ or $c^{-1}(2)$ contains a copy of $\mathbb{K}_{s-1}$.
If $c^{-1}(2)$ contains a copy of $\mathbb{K}_{s-1}$, then the edges of the complete subgraph with the vertices in $A_2 \sqcup \{x\}$ is contained in $c^{-1}(2)$ and it contains a copy of $\mathbb{K}_s$. A contradiction to our assumption. Hence $c^{-1}(1)$ contains a copy of $\mathbb{K}_r$ and the result follows.

Th: $R(r,s) \leq \binom{r+s-2}{s-1}$, where $r \geq 2$ and $s \geq 2$ are integers.

Proof: We prove this result using induction on the pairs (r,s). We have $R(2,2) = 2$. This means induction hypothesis is true for $(r,s) = (2,2)$.

We assume that for $2 \leq m \leq p$ and $2 \leq n \leq q$,

$$R(m,n) \leq \binom{m+n-2}{n-1}$$

Then we note that

$$R(m+1,n) \leq R(m,n) + R(m+1,n-1) \leq \binom{m+n-2}{n-1} + \binom{m+n-2}{n-2} = \binom{m+n-1}{n-1}$$

$$R(m,n+1) \leq R(m-1,n+1) + R(m,n) \leq \binom{m+n-2}{n} + \binom{m+n-2}{n-1} = \binom{m+n-1}{n}$$

$$R(m+1,n+1) \leq R(m,n+1) + R(m+1,n) \leq \binom{m+n-1}{n} + \binom{m+n-1}{n-1} = \binom{m+n}{n}$$

This shows that for $2 \leq m \leq p+1$ and $2 \leq n \leq q+1$,

$$R(m,n) \leq \binom{m+n-2}{n-1}$$

holds and the result follows. $\square$

Corollary: $R(k,k) \leq \binom{2k-2}{k-1}$, where $k \geq 2$ is an integer.

Proof: Exercise

Th: For each integer $k \geq 2$,

$$2^{\frac{k}{2}} < R(k,k) \leq \binom{2k-2}{k-1}$$

Proof: It will be discussed later.

Th: (Fisher's Inequality): The parameters of a non-trivial 2-design satisfy $b \geq v$ (equivalently $r \geq k$).

Proof: (R. Fisher) [Variance Trick]: Let D be a non-trivial 2-design. Fix a block B of D.

Let e_i denote the no. of blocks $B' \neq B$ such that B, B' both are incident with i no. of points of D, where $i \geq 0$ is an integer.

We count the set $\mathcal{F} := \{ B' : B' \neq B, B' \text{ is a block of } D \}$.

Note that $A' \sim B' \iff$ No. of points incident with A' and B is same as No. of points incident with B' and B

Then $\sim$ is an equivalence relation and for each integer $i \geq 0$ $\{ B' : i \text{ no. of points are incident with } B' \text{ and } B \}$ is an equivalence class containing e_i blocks.

Hence $\sum_{i \geq 0} e_i = |\mathcal{F}| = b - 1$. —— (A)

Next, we count the set of pairs in two ways.
$\{ (x, B') : B' \neq B, x \text{ is incident with } B \text{ and } B' \}$

First way: There are k choices of x. (as x is incident with B). Having chosen x, there are exactly $r-1$ choices of B' (Note there are r choices of blocks of D which are incident with x. It includes B also) in the aforementioned set.

Hence there are $k(r-1)$ members in the aforementioned set.

Second way: Note that $(x, A') \sim (y, B') \iff$ No of points incident with A' and B is same a no. of points incident with B' and B.

Then $\sim$ is an equivalence relation and for each integer $i \geq 0$ $\{ (x, B') : i \text{ no. of points are incident with } B \text{ \& } B' \}$ is an equivalence class containing ie_i such pairs.

Hence $\sum_{i \geq 0} ie_i = (r-1)k$. —— (B)

Next we count the set of triples in two ways.
$\{ (x, y, B') : B' \neq B, x \neq y, x \text{ \& } y \text{ are incident with } B' \}$.

First way: There are k choices of x. Having chosen x, there are $k-1$ choices of y. Having chosen y, there are exactly $(\lambda - 1)$ choices of B'

Hence there are $k(k-1)(\lambda-1)$ triples in the aforementioned set.

NOV 24, 2020 9:30 AM

Second way: Note that $(x,y,A') \sim (p,q,B') \Leftrightarrow$ No. of points incident with A' and B is same as no. of points incident with B' and B.

This is an equivalence relation and for each integer $i \geq 0$

$\{(x,y,B') : i$ no of points are incident with B & $B'\}$

is an equivalence class containing $i(i-1)e_i$ triples.

Hence $\sum_{i \geq 0} i(i-1)e_i = k(k-1)(\lambda-1)$ —— (C)

The variance trick is to use (A), (B) & (C) to calculate $\sum_{i \geq 0}(i - \frac{(r-1)k}{b-1})^2 e_i$, for the purpose to conclude $\sum_{i \geq 0}(i - \frac{(r-1)k}{b-1})^2 e_i \geq 0$

Note that $\sum_{i \geq 0}\left(i - \frac{(r-1)k}{b-1}\right)^2 e_i \underset{(Ex)}{=} (\lambda-1)k(k-1) - \frac{(r-1)^2k^2}{b-1} + (r-1)k$

Now $0 \leq (b-1)\left(\sum_{i \geq 0}\left(i - \frac{(r-1)k}{b-1}\right)^2 e_i\right) \underset{(Ex)}{=} (r-k)(r-\lambda)(v-k)$

using $bk = rv$ and $r(k-1) = \lambda(v-1)$.

Since D is a non-trivial 2-design we have $v-k>0$ & $r-\lambda>0$

Therefore $r \geq k$ (equivalently $b \geq v$) $\square$

Ramsey's Theorem on Graphs

Exposition by William Gasarch

1 Introduction

Imagine that you have 6 people at a party. We assume that, for every pair of them, either THEY KNOW EACH OTHER or NEITHER OF THEM KNOWS THE OTHER. So we are assuming that if x knows y, then y knows x.

Claim: Either there are at least 3 people *all of whom know one another*, or there are at least 3 people *no two of whom know each other* (or both).

Proof of Claim:

Let the people be $p_1, p_2, p_3, p_4, p_5, p_6$. Now consider p_6.

Among the other 5 people, either there are at least 3 people that p_6 knows, or there are at least 3 people that p_6 does not know.

Why is this?

Well, suppose that, among the other 5 people, there are at most 2 people that p_6 knows, and at most 2 people that p_6 does not know. Then there are only 4 people other than p_6, which contradicts the fact that there are 5 people other than p_6.

Suppose that p_6 knows at least 3 of the others. We consider the case where p_6 knows p_1, p_2, and p_3. All the other cases are similar.

If p_1 knows p_2, then p_1, p_2, and p_6 all know one another. HOORAY!

If p_1 knows p_3, then p_1, p_3, and p_6 all know one another. HOORAY!

If p_2 knows p_3, then p_2, p_3, and p_6 all know one another. HOORAY!

What if *none* of these scenarios holds? Then none of these three people (p_1, p_2, p_3) knows either of the other 2. HOORAY!

End of Proof of Claim

We want to generalize this observation.

Notation 1.1 N is the set of all positive integers. If $n \in \mathsf{N}$, then $[n]$ is the set $\{1, \ldots, n\}$.

Def 1.2 A *graph* G consists of a set V of vertices and a set E of edges. The edges are *unordered* pairs of vertices.

Note 1.3 In general, a graph can have an edge $\{i, j\}$ with $i = j$. Here, however, every edge of a graph is an unordered pair of *distinct* vertices (i.e., an unordered pair $\{i, j\}$ with $i \neq j$).

Def 1.4 Let $c \in \mathsf{N}$. Let $G = (V, E)$ be a graph. A *c-coloring of the edges of G* is a function $COL : E \rightarrow [c]$. Note that there are no restrictions on COL.

Note 1.5 In the Graph Theory literature there are (at least) two kinds of coloring. We present them in this note so that if you happen to read the literature and they are using coloring in a different way then in these notes, you will not panic.

- Vertex Coloring. Usually one says that the vertices of a graph are c-colorable if there is a way to assign each vertex a color, using no more than c colors, such that no two adjacent vertices (vertices connected by an edge) are the same color. Theorems are often of the form 'if a graph G has property BLAH BLAH then G is c-colorable' where they mean vertex c-colorable. We **will not** be considering these kinds of colorings.

- Edge Colorings. Usually this is used in the context of Ramsey Theory and Ramsey-type theorems. Theorems begin with 'for all c-coloring of a graph G BLAH BLAH happens' We **will** be considering these kinds of colorings.

Def 1.6 Let $n \in \mathsf{N}$. The *complete graph on n vertices*, denoted K_n, is the graph

$$\begin{aligned} V = & \ [n] \\ E = & \ \{\{i, j\} \mid i, j \in [n]\} \end{aligned}$$

Example 1.7 Let G be the complete graph on 10 vertices. Recall that the vertices are $\{1, \ldots, 10\}$. We give a 3-coloring of the edges of G:

$$COL(\{x, y\}) = \begin{cases} 1 & \text{if } x + y \equiv 1 \pmod 3; \\ 2 & \text{if } x + y \equiv 2 \pmod 3; \\ 3 & \text{if } x + y \equiv 0 \pmod 3). \end{cases}$$

Lets go back to our party! We can think of the 6 people as vertices of K_6. We can color edge $\{i, j\}$ RED if i and j know each other, and BLUE if they do not.

Def 1.8 Let $G = (V, E)$ be a graph, and let COL be a coloring of the edges of G. A set of edges of G is *monochromatic* if they are all the same color.

Let $n \geq 2$. Then G *has a monochromatic* K_n if there is a set V' of n vertices (in V) such that

- there is an edge between every pair of vertices in V': $\{\{i, j\} \mid i, j \in V'\} \subseteq E$
- all the edges between vertices in V' are the same color: there is some $l \in [c]$ such that $COL(\{i, j\}) = l$ for all $i, j \in V'$

We now restate our 6-people-at-a-party theorem:

Theorem 1.9 *Every 2-coloring of the edges of K_6 has a monochromatic K_3.*

2 The Full Theorem

From the last section, we know the following:

If you want an n such that you get a monochromatic K_3 no matter how you 2-color K_n, then $n = 6$ will suffice.

What if you want to guarantee that there is a monochromatic K_4? What if you want to use 17 colors?

The following is known as *Ramsey's Theorem.* It was first proved in [3] (see also [1], [2]).

For all $c, m \geq 2$, there exists $n \geq m$ such that every c-coloring of K_n has a monochromatic K_m.

We will provide several proofs of this theorem for the $c = 2$ case. We will assume the colors are RED and BLUE (rather than the numbers 1 and 2). The general-c case (where c can be *any* integer $i \geq 2$) and other generalizations may show up on homework assignments.

3 First Proof of Ramsey's Theorem

Given m, we really want n such that every 2-coloring of K_n has a RED K_m or a BLUE K_m. However, it will be useful to let the parameter for BLUE differ from the parameter for RED.

Notation 3.1 Let $a, b \geq 2$. Let $R(a, b)$ denote the least number, if it exists, such that every 2-coloring of $K_{R(a,b)}$ has a RED K_a or a BLUE K_b. We abbreviate $R(a, a)$ by $R(a)$.

We state some easy facts.

1. For all a, b, $R(a, b) = R(b, a)$.

2. For $b \geq 2$, $R(2, b) = b$: First, we show that $R(2, b) \leq b$. Given any 2-coloring of K_b, we want a RED K_2 or a BLUE K_b. Note that a RED K_2 is just a RED edge. Hence EITHER there exists one RED edge (so you get a RED K_2) OR all the edges are BLUE (so you get a BLUE K_b). Now we prove that $R(2, b) = b$. If $b = 2$, this is obvious. If $b > 2$, then the all-BLUE coloring of K_{b-1} has neither a RED K_2 nor a BLUE K_b, hence $R(2, b) \geq b$. Combining the two inequalities ($R(2, b) \leq b$ and $R(2, b) \geq b$), we find that $R(2, b) = b$.

3. $R(3, 3) \leq 6$ (we proved this in Section 1)

We want to show that, for every $n \geq 2$, $R(n, n)$ exists. In this proof, we show something more: that for all $a, b \geq 2$, $R(a, b)$ exists. We do not really care about the case where $a \neq b$, but that case will help us get our result. This is a situation where proving more than you need is easier.

Theorem 3.2

1. *$R(2, b) = b$ (we proved this earlier)*

2. *For all $a, b \geq 3$: If $R(a - 1, b)$ and $R(a, b - 1)$ exist, then $R(a, b)$ exists and*
$$R(a, b) \leq R(a - 1, b) + R(a, b - 1)$$

3. *For all $a, b \geq 2$, $R(a, b)$ exists and $R(a, b) \leq 2^{a+b}$.*

Proof:

Since we proved part 1 earlier, we now prove parts 2 and 3.

Part 2 Assume $R(a-1,b)$ and $R(a,b-1)$ exist. Let

$$n = R(a-1,b) + R(a,b-1)$$

Let COL be a 2-coloring of K_n, and let x be a vertex. Note that there are

$$R(a-1,b) + R(a,b-1) - 1$$

edges coming out of x (edges $\{x,y\}$ for vertices y).

Let NUM-RED-EDGES be the number of red edges coming out of x, and let NUM-BLUE-EDGES be the number of blue edges coming out of x. Note that

$$\text{NUM-RED-EDGES} + \text{NUM-BLUE-EDGES} = R(a-1,b) + R(a,b-1) - 1$$

Hence either

$$\text{NUM-RED-EDGES} \geq R(a-1,b)$$

or

$$\text{NUM-BLUE-EDGES} \geq R(a,b-1)$$

To see this, suppose, by way of contradiction, that both inequalities are false. Then

$$\begin{array}{rcl} \text{NUM-RED-EDGES} & + & \text{NUM-BLUE-EDGES} \\ \leq R(a-1,b)-1 & + & R(a,b-1)-1 \\ = R(a-1,b) & + & R(a,b-1)-2 \\ < R(a-1,b) & + & R(a,b-1)-1 \end{array}$$

There are two cases:

1. *Case 1:* NUM-RED-EDGES $\geq R(a-1,b)$. Let

   $$U = \{y \mid COL(\{x,y\}) = \text{RED}\}$$

   U is of size NUM-RED-EDGES $\geq R(a-1,b)$. Consider the restriction of the coloring COL to the edges between vertices in U. Since

   $$|U| \geq R(a-1,b),$$

   this coloring has a RED K_{a-1} or a BLUE K_b. Within Case 1, there are two cases:

(a) There is a RED K_{a-1}. Recall that all of the edges in

$$\{\{x,u\} \mid u \in U\}$$

are RED, hence all the edges between elements of the set $U \cup \{x\}$ are RED, so they form a RED K_a and WE ARE DONE.

(b) There is a BLUE K_b. Then we are DONE.

2. *Case 2:* NUM-BLUE-EDGES $\geq R(a,b-1)$. Similar to Case 1.

Part 3 To show that $R(a,b)$ exists and $R(a,b) \leq 2^{a+b}$, we use induction on $n = a+b$. Since $a,b \geq 2$, the smallest value of $a+b$ is 4. Thus $n \geq 4$.

Base Case: $n=4$. Since $a+b=4$ and $a,b \geq 2$, we must have $a=b=2$. From part 1, we know that $R(2,2)$ exists and $R(2,2)=2$. Note that

$$R(2,2) = 2 \leq 2^{2+2} = 16$$

Induction Hypothesis: For all $a,b \geq 2$ such that $a+b=n$, $R(a,b)$ exists and $R(a,b) \leq 2^{a+b}$.

Inductive Step: Let a,b be such that $a,b \geq 2$ and $a+b=n+1$.

There are three cases:

1. *Case 1:* $a=2$. By part 1, $R(2,b)$ exists and $R(2,b)=b$. Since $b \geq 2$, we have
$$b \leq 2^b \leq 4 \cdot 2^b = 2^2 \cdot 2^b = 2^{2+b}$$
Hence $R(2,b) \leq 2^{2+b}$.

2. *Case 2:* $b=2$. Follows from Case 1 and $R(a,b)=R(b,a)$.

3. *Case 3:* $a,b \geq 3$. Since $a,b \geq 3$, we have $a-1 \geq 2$ and $b-1 \geq 2$. Also, $a+b=n+1$, so $(a-1)+b=n$ and $a+(b-1)=n$. By the induction hypothesis, $R(a-1,b)$ and $R(a,b-1)$ exist; moreover,
$$R(a-1,b) \leq 2^{(a-1)+b} = 2^{a+b-1}$$
$$R(a,b-1) \leq 2^{a+(b-1)} = 2^{a+b-1}$$
From part 3, $R(a,b)$ exists and
$$R(a,b) \leq R(a-1,b) + R(a,b-1)$$

Hence

$$R(a,b) \le R(a-1,b) + R(a,b-1) \le 2^{a+b-1} + 2^{a+b-1} = 2 \cdot 2^{a+b-1} = 2^{a+b}$$

▮

Corollary 3.3 *For every $m \ge 2$, $R(m)$ exists and $R(m) \le 2^{2m}$.*

4 Second Proof of Ramsey's Theorem

We now present a proof that does not use $R(a,b)$. It also gives a mildly better bound on $R(m)$ than the one given in Corollary 3.3.

Theorem 4.1 *For every $m \ge 2$, $R(m)$ exists and $R(m) \le 2^{2m-2}$.*

Proof:

Let COL be a 2-coloring of $K_{2^{2m-2}}$. We define a sequence of vertices,

$$x_1, x_2, \ldots, x_{2m-1},$$

and a sequence of sets of vertices,

$$V_0, V_1, V_2, \ldots, V_{2m-1},$$

that are based on COL.

Here is the intuition: Vertex $x_1 = 1$ has $2^{2m-2} - 1$ edges coming out of it. Some are RED, and some are BLUE. Hence there are at least 2^{2m-3} RED edges coming out of x_1, or there are at least 2^{2m-3} BLUE edges coming out of x_1. To see this, suppose, by way of contradiction, that it is false, and let N.E. be the total number of edges coming out of x_1. Then

$$\text{N.E.} \le (2^{2m-3} - 1) + (2^{2m-3} - 1) = (2 \cdot 2^{2m-3}) - 2 = 2^{2m-2} - 2 < 2^{2m-2} - 1$$

Let c_1 be a color such that x_1 has at least 2^{2m-3} edges coming out of it that are colored c_1. Let V_1 be the set of vertices v such that $COL(\{v, x_1\}) = c_1$. Then keep iterating this process.

We now describe it formally.

$$
\begin{aligned}
V_0 = &\quad [2^{2m-2}] \\
x_1 = &\quad 1 \\
c_1 = &\quad \begin{cases} \text{RED} & \text{if } |\{v \in V_0 \mid COL(\{v, x_1\}) = \text{RED}\}| \geq 2^{2m-3} \\ \text{BLUE} & \text{otherwise} \end{cases} \\
V_1 = &\quad \{v \in V_0 \mid COL(\{v, x_1\}) = c_1\} \text{ (note that } |V_1| \geq 2^{2m-3})
\end{aligned}
$$

Let $i \geq 2$, and assume that V_{i-1} is defined. We define x_i, c_i, and V_i:

$$
\begin{aligned}
x_i = &\quad \text{the least number in } V_{i-1} \\
c_i = &\quad \begin{cases} \text{RED} & \text{if } |\{v \in V_{i-1} \mid COL(\{v, x_i\}) = \text{RED}\}| \geq 2^{(2m-2)-i}; \\ \text{BLUE} & \text{otherwise.} \end{cases} \\
V_i = &\quad \{v \in V_{i-1} \mid COL(\{v, x_i\}) = c_i\} \text{ (note that } |V_i| \geq 2^{(2m-2)-i})
\end{aligned}
$$

How long can this sequence go on for? Well, x_i can be defined if V_{i-1} is nonempty. Note that

$$|V_{2m-2}| \geq 2^{(2m-2)-(2m-2)} = 2^0 = 1$$

Thus if $i-1 = 2m-2$ (equivalently, $i = 2m-1$), then $V_{i-1} = V_{2m-2} \neq \emptyset$, but there is no guarantee that V_i $(= V_{2m-1})$ is nonempty. Hence we can define

$$x_1, \ldots, x_{2m-1}$$

Consider the colors

$$c_1, c_2, \ldots, c_{2m-2}$$

Each of these is either RED or BLUE. Hence there must be at least $m-1$ of them that are the same color. Let $i_1, \ldots, i_{m-1}$ be such that $i_1 < \cdots < i_{m-1}$ and

$$c_{i_1} = c_{i_2} = \cdots = c_{i_{m-1}}$$

Denote this color by c, and consider the m vertices

$$x_{i_1}, x_{i_2}, \cdots, x_{i_{m-1}}, x_{i_{m-1}+1}$$

To see why we have listed m vertices but only $m-1$ colors, picture the following scenario: You are building a fence row, and you want (say) 7 sections of fence. To do that, you need 8 fence posts to hold it up. Now think of the fence posts as vertices, and the sections of fence as edges between successive vertices, and recall that every edge has a color associated with it.

Claim: The m vertices listed above form a monochromatic K_m.
Proof of Claim:
First, consider vertex x_{i_1}. The vertices

$$x_{i_2}, \ldots, x_{i_{m-1}}, x_{i_{m-1}+1}$$

are elements of V_{i_1}, hence the edges

$$\{x_{i_1}, x_{i_2}\}, \ldots \{x_{i_1}, x_{i_{m-1}}\}, \{x_{i_1}, x_{i_{m-1}+1}\}$$

are colored with c_{i_1} $(= c)$.
Then consider each of the remaining vertices in turn, starting with vertex x_{i_2}. For example, the vertices

$$x_{i_3}, \ldots, x_{i_{m-1}}, x_{i_{m-1}+1}$$

are elements of V_{i_2}, hence the edges

$$\{x_{i_2}, x_{i_3}\}, \ldots \{x_{i_2}, x_{i_{m-1}}\}, \{x_{i_2}, x_{i_{m-1}+1}\}$$

are colored with c_{i_2} $(= c)$.
End of Proof of Claim ∎

5 Proof of the Infinite Ramsey Theorem

We now consider infinite graphs.

Notation 5.1 K_{N} is the graph (V, E) where

$$\begin{aligned} V &= \mathsf{N} \\ E &= \{\{x, y\} \mid x, y \in \mathsf{N}\} \end{aligned}$$

Def 5.2 Let $G = (V, E)$ be a graph with $V = \mathsf{N}$, and let COL be a coloring of the edges of G. A set of edges of G is *monochromatic* if they are all the same color (this is the same as for a finite graph).

G has a monochromatic K_{N} if there is an infinite set V' of vertices (in V) such that

- there is an edge between every pair of vertices in V'
- all the edges between vertices in V' are the same color

Theorem 5.3 *Every 2-coloring of the edges of K_{N} has a monochromatic K_{N}.*

Proof:

(Note: this proof is similar to the proof of Theorem 4.1.)

Let COL be a 2-coloring of K_{N}. We define an infinite sequence of vertices,

$$x_1, x_2, \ldots,$$

and an infinite sequence of sets of vertices,

$$V_0, V_1, V_2, \ldots,$$

that are based on COL.

Here is the intuition: Vertex $x_1 = 1$ has an infinite number of edges coming out of it. Some are RED, and some are BLUE. Hence there are an infinite number of RED edges coming out of x_1, or there are an infinite number of BLUE edges coming out of x_1 (or both). Let c_1 be a color such that x_1 has an infinite number of edges coming out of it that are colored c_1. Let V_1 be the set of vertices v such that $COL(\{v, x_1\}) = c_1$. Then keep iterating this process.

We now describe it formally.

$$\begin{aligned} V_0 &= \mathsf{N} \\ x_1 &= 1 \end{aligned}$$

$$c_1 = \begin{cases} \text{RED} & \text{if } |\{v \in V_0 \mid COL(\{v, x_1\}) = \text{RED}\}| \text{ is infinite} \\ \text{BLUE} & \text{otherwise} \end{cases}$$

$$V_1 = \{v \in V_0 \mid COL(\{v, x_1\}) = c_1\} \text{ (note that } |V_1| \text{ is infinite)}$$

Let $i \geq 2$, and assume that V_{i-1} is defined. We define x_i, c_i, and V_i:

$$x_i = \quad \text{the least number in } V_{i-1}$$

$$c_i = \begin{cases} \text{RED} & \text{if } |\{v \in V_{i-1} \mid COL(\{v, x_i\}) = \text{RED}\}| \text{ is infinite} \\ \text{BLUE} & \text{otherwise} \end{cases}$$

$$V_i = \quad \{v \in V_{i-1} \mid COL(\{v, x_i\}) = c_i\} \text{ (note that } |V_i| \text{ is infinite)}$$

How long can this sequence go on for? Well, x_i can be defined if V_{i-1} is nonempty. We an show by induction that, for every i, V_i is infinite. Hence the sequence

$$x_1, x_2, \ldots,$$

is infinite.

Consider the infinite sequence

$$c_1, c_2, \ldots$$

Each of the colors in this sequence is either RED or BLUE. Hence there must be an infinite sequence $i_1, i_2, \ldots$ such that $i_1 < i_2 < \cdots$ and

$$c_{i_1} = c_{i_2} = \cdots$$

Denote this color by c, and consider the vertices

$$x_{i_1}, x_{i_2}, \cdots$$

Using an argument similar to the one we used in the proof of Theorem 4.1 (to show that we had a monochromatic K_m), we can show that these vertices form a monochromatic K_{N}. ∎

6 Finite Ramsey from Infinite Ramsey

Picture the following scenario: Our first lecture on the Ramsey Theorem *began* by proving Theorem 5.3. This is not absurd: The proof we gave of the infinite Ramsey Theorem does not need some of the details that are needed in the proof we gave of the finite Ramsey Theorem.

Having proved the infinite Ramsey Theorem, we then want to prove the finite Ramsey Theorem. Can we prove the finite Ramsey Theorem *from* the infinite Ramsey Theorem? Yes, we can!

Theorem 6.1 *For every $m \geq 2$, $R(m)$ exists.*

Proof: Suppose, by way of contradiction, that there is some $m \geq 2$ such that $R(m)$ does not exist. Then, for every $n \geq m$, there is some way to color K_n so that there is no monochromatic K_m. Hence there exist the following:

1. COL_1, a 2-coloring of K_m that has no monochromatic K_m
2. COL_2, a 2-coloring of K_{m+1} that has no monochromatic K_m
3. COL_3, a 2-coloring of K_{m+2} that has no monochromatic K_m

   $\vdots$

j. COL_j, a 2-coloring of K_{m+j-1} that has no monochromatic K_m

   $\vdots$

We will use these 2-colorings to form a 2-coloring COL of K_{N} that has no monochromatic K_m.

Let $e_1, e_2, e_3, \ldots$ be a list of all unordered pairs of elements of N such that every unordered pair appears exactly once. We will color e_1, then e_2, etc.

How should we color e_1? We will color it the way an infinite number of the COL_i's color it. Call that color c_1. Then how to color e_2? Well, first consider ONLY the colorings that colored e_1 with color c_1. Color e_2 the way an infinite number of those colorings color it. And so forth.

We now proceed formally:

$$J_0 = \mathsf{N}$$

$$COL(e_1) = \begin{cases} \text{RED} & \text{if } |\{j \in J_0 \mid COL_j(e_1) = \text{RED}\}| \text{ is infinite} \\ \text{BLUE} & \text{otherwise} \end{cases}$$

$$J_1 = \{j \in J_0 \mid COL(e_1) = COL_j(e_1)\}$$

Let $i \geq 2$, and assume that $e_1, \ldots, e_{i-1}$ have been colored. Assume, furthermore, that J_{i-1} is infinite and, for every $j \in J_{i-1}$,

$$
\begin{aligned}
COL(e_1) = &\ COL_j(e_1)\\
COL(e_2) = &\ COL_j(e_2)\\
&\vdots\\
COL(e_{i-1}) = &\ COL_j(e_{i-1})
\end{aligned}
$$

We now color e_i:

$$COL(e_i) = \begin{cases} \text{RED} & \text{if } |\{j \in J_{i-1} \mid COL_j(e_i) = \text{RED}\}| \text{ is infinite} \\ \text{BLUE} & \text{otherwise} \end{cases}$$

$$J_i = \{j \in J_{i-1} \mid COL(e_i) = COL_j(e_i)\}$$

One can show by induction that, for every i, J_i is infinite. Hence this process *never* stops.

Claim: If K_{N} is 2-colored with COL, then there is no monochromatic K_m.

Proof of Claim:

Suppose, by way of contradiction, that there is a monochromatic K_m. Let the edges between vertices in that monochromatic K_m be

$$e_{i_1}, \ldots, e_{i_M},$$

where $i_1 < i_2 < \cdots < i_M$ and $M = \binom{m}{2}$. For every $j \in J_{i_M}$, COL_j and COL agree on the colors of those edges. Choose $j \in J_{i_M}$ so that all the vertices of the monochromatic K_m are elements of the vertex set of K_{m+j-1}. Then COL_j is a 2-coloring of the edges of K_{m+j-1} that has a monochromatic K_m, in contradiction to the definition of COL_j.

End of Proof of Claim

Hence we have produced a 2-coloring of K_{N} that has no monochromatic K_m. This contradicts Theorem 5.3. Therefore, our initial supposition—that $R(m)$ does not exist—is false. ▮

Note that two of our proofs of the finite Ramsey Theorem (the proofs of Theorems 3.2 and 4.1) give upper bounds on $R(m)$, but that our proof of the finite Ramsey Theorem *from* the infinite Ramsey Theorem (the proof of Theorem 6.1) gives no upper bound on $R(m)$.

7 Proof of Large Ramsey Theorem

In all of the theorems presented earlier, the labels on the vertices did *not* matter. In this section, the labels *do* matter.

Def 7.1 A finite set $F \subseteq \mathsf{N}$ is called *large* if the size of F is at least as large as the smallest element of F.

Example 7.2

1. The set $\{1, 2, 10\}$ is large: It has 3 elements, the smallest element is 1, and $3 \geq 1$.
2. The set $\{5, 10, 12, 17, 20\}$ is large: It has 5 elements, the smallest element is 5, and $5 \geq 5$.
3. The set $\{20, 30, 40, 50, 60, 70, 80, 90, 100\}$ is not large: It has 9 elements, the smallest element is 20, and $9 < 20$.
4. The set $\{5, 30, 40, 50, 60, 70, 80, 90, 100\}$ is large: It has 9 elements, the smallest element is 5, and $9 \geq 5$.
5. The set $\{101, \ldots, 190\}$ is not large: It has 90 elements, the smallest element is 101, and $90 < 101$.

We will be considering monochromatic K_m's where the underlying set of vertices is a large set. We need a definition to identify the underlying set.

Def 7.3 Let COL be a 2-coloring of K_n. A set A of vertices is *homogeneous* if there exists a color c such that, for all $x, y \in A$ with $x \neq y$, $COL(\{x, y\}) = c$. In other words, all of the edges between elements of A are the same color. One could also say that there is a monochromatic $K_{|A|}$.

Let COL be a 2-coloring of K_n. Recall that the vertex set of K_n is $\{1, 2, \ldots, n\}$. Consider the set $\{1, 2\}$. It is clearly both homogeneous and large (using our definition of large). Hence the statement

"for every $n \geq 2$, every 2-coloring of K_n has a large homogeneous set" is true but trivial.

What if we used $V = \{m, m+1, \ldots, m+n\}$ as our vertex set? Then a large homogeneous set would have to have size at least m.

Notation 7.4 K_n^m is the graph with vertex set $\{m, m+1, \ldots, m+n\}$ and edge set consisting of all unordered pairs of vertices. The superscript (m) indicates that we are labeling our vertices starting with m, and the subscript (n) is one less than the number of vertices.

Note 7.5 The vertex set of K_n^m (namely, $\{m, m+1, \ldots, m+n\}$) has $n+1$ elements. Hence if K_n^m has a large homogeneous set, then $n+1 \geq m$ (equivalently, $n \geq m-1$). We could have chosen to use K_n^m to denote the graph with vertex set $\{m+1, \ldots, m+n\}$, so that the smallest vertex is $m+1$ and the number of vertices is n, but the set we have designated as K_n^m will better serve our purposes.

Notation 7.6 $LR(m)$ is the least n, if it exists, such that every 2-coloring of K_n^m has a large homogeneous set.

We first prove a theorem about infinite graphs and large homogeneous sets.

Theorem 7.7 *If COL is any 2-coloring of K_{N}, then, for every $m \geq 2$, there is a large homogeneous set whose smallest element is at least as large as m.*

Proof: Let COL be any 2-coloring of K_{N}. By Theorem 5.3, there exist an infinite set of vertices,

$$v_1 < v_2 < v_3 < \cdots,$$

and a color c such that, for all i, j, $COL(\{v_i, v_j\}) = c$. (This could be called an infinite homogeneous set.) Let i be such that $v_i \geq m$. The set

$$\{v_i, \ldots, v_{i+v_i-1}\}$$

is a homogeneous set that contains v_i elements and whose smallest element is v_i. Since $v_i \geq v_i$, it is a large set; hence it is a large homogeneous set. ∎

Theorem 7.8 *For every $m \geq 2$, $LR(m)$ exists.*

Proof: This proof is similar to our proof of the finite Ramsey Theorem *from* the infinite Ramsey Theorem (the proof of Theorem 6.1).

Suppose, by way of contradiction, that there is some $m \geq 2$ such that $LR(m)$ does not exist. Then, for every $n \geq m-1$, there is some way to color K_n^m so that there is no large homogeneous set. Hence there exist the following:

1. COL_1, a 2-coloring of K_{m-1}^m that has no large homogeneous set
2. COL_2, a 2-coloring of K_m^m that has no large homogeneous set
3. COL_3, a 2-coloring of K_{m+1}^m that has no large homogeneous set

$\vdots$

j. COL_j, a 2-coloring of K_{m+j-2}^m that has no large homogeneous set

$\vdots$

We will use these 2-colorings to form a 2-coloring COL of K_{N} that has no large homogeneous set whose smallest element is at least as large as m.

Let $e_1, e_2, e_3, \ldots$ be a list of all unordered pairs of elements of N such that every unordered pair appears exactly once. We will color e_1, then e_2, etc.

How should we color e_1? We will color it the way an infinite number of the COL_i's color it. Call that color c_1. Then how to color e_2? Well, first consider ONLY the colorings that colored e_1 with color c_1. Color e_2 the way an infinite number of those colorings color it. And so forth.

We now proceed formally:

$$J_0 = \mathsf{N}$$

$$COL(e_1) = \begin{cases} \text{RED} & \text{if } |\{j \in J_0 \mid COL_j(e_1) = \text{RED}\}| \text{ is infinite} \\ \text{BLUE} & \text{otherwise} \end{cases}$$

$$J_1 = \{j \in J_0 \mid COL(e_1) = COL_j(e_1)\}$$

Let $i \geq 2$, and assume that $e_1, \ldots, e_{i-1}$ have been colored. Assume, furthermore, that J_{i-1} is infinite and, for every $j \in J_{i-1}$,

$$\begin{aligned} COL(e_1) = &\ COL_j(e_1) \\ COL(e_2) = &\ COL_j(e_2) \\ &\vdots \\ COL(e_{i-1}) = &\ COL_j(e_{i-1}) \end{aligned}$$

We now color e_i:

$$COL(e_i) = \begin{cases} \text{RED} & \text{if } |\{j \in J_{i-1} \mid COL_j(e_i) = \text{RED}\}| \text{ is infinite} \\ \text{BLUE} & \text{otherwise} \end{cases}$$

$$J_i = \ \{j \in J_{i-1} \mid COL(e_i) = COL_j(e_i)\}$$

One can show by induction that, for every i, J_i is infinite. Hence this process *never* stops.

Claim: If K_{N} is 2-colored with COL, then there is no large homogeneous set whose smallest element is at least as large as m.

Proof of Claim:

Suppose, by way of contradiction, that there is a large homogeneous set whose smallest element is at least as large as m. Without loss of generality, we can assume that the size of the large homogeneous set is equal to its smallest element. Let the vertices of that large homogeneous set be $v_1, v_2, \ldots v_{v_1}$, where $m \le v_1 < v_2 < \cdots < v_{v_1}$, and let the edges between those vertices be

$$e_{i_1}, \ldots, e_{i_M},$$

where $i_1 < i_2 < \cdots < i_M$ and $M = \binom{v_1}{2}$. For every $j \in J_{i_M}$, COL_j and COL agree on the colors of those edges. Choose $j \in J_{i_M}$ so that all the vertices of the large homogeneous set are elements of the vertex set of K^m_{m+j-2}. Then COL_j is a 2-coloring of the edges of K^m_{m+j-2} that has a large homogeneous set, in contradiction to the definition of COL_j.

End of Proof of Claim

Hence we have produced a 2-coloring of K_{N} that has no large homogeneous set whose smallest element is at least as large as m. This contradicts Theorem 7.7. Therefore, our initial supposition—that $LR(m)$ does not exist—is false. ▮

References

[1] R. Graham, A. Rothchild, and J. Spencer. *Ramsey Theory*. Wiley, 1990.

[2] B. Landmann and A. Robertson. *Ramsey Theory over the Integers*. AMS, 2003.

[3] F. Ramsey. On a problem of formal logic. *Proceedings of the London Mathematical Society*, 30:264–286, 1930. Series 2.

COUNTING PRINCIPLES

Defn: Let S be a non-empty set. A partition of S into K parts is a collection $\{B_1, B_2, \ldots, B_K\}$, where $\forall\ i,j \in [K]$ $B_i \subset S$ and $B_i \cap B_j = \begin{cases} \phi & \text{if } i \neq j \\ B_i & \text{if } i = j \end{cases}$

Addition principle of counting: If a finite non-empty set S is partitioned into K parts $B_1, B_2, \ldots, B_K$. Then

$$|S| = |B_1| + |B_2| + \cdots + |B_K| = \sum_{i=1}^{K} |B_i|$$

Example: If the first box contains m objects and the second box contains n objects, then the no. of ways of choosing one object either of the two boxes is $m+n$.

Subtraction principle of counting: Let $S \subseteq T$ be a finite set. We define $S^c = T \setminus S$, the complement of S in T. Then the subtraction principle of counting is

$$|\bar{S}| = |T| - |S|.$$

Example: T = set of students studying at NISER
S = set of students neither Mathematics nor Physics

If $|T| = 2000$, $|S| = 1800$, then compute the number $|S^c| = 200$. Note that there are $|S^c| = 200$ students studies either Mathematics or Physics.

Multiplication principle of counting: If a finite set $S = S_1 \times S_2 \times \cdots \times S_K$ then the multiplication principle of counting is

$$|S| = |S_1| \times |S_2| \times \cdots \times |S_K| = \prod_{i=1}^{K} |S_i|$$

Example: On assuming, any registered vehicle which can be registered by Govt. of Odisha is OD02 AC8581, what is the maximum possible vehicle can be registered by the Govt. of Odisha.

Bijective function principle of counting: Let S & R be sets. If there exist a bijective mapping $f: S \to R$, then bijective function principle of counting states that $|S| = |R|$

Example: (A) $S = \{1, 2, 3\} = [3]$ & $R = \{a, b, c\}$.
$1 \mapsto a$ $2 \mapsto c$ & $3 \mapsto b$.

(B) $R = \{ r \in \mathbb{N} : 1 \le r \le mn \ \gcd(r, mn) = 1 \}$
$S = \{ (a,b) \in \mathbb{N} \times \mathbb{N} : 1 \le a \le m, 1 \le b \le n, \gcd(a,m) = 1 = \gcd(b,n) \}$
There exist a bijective mapping between R & S
This establishes $\phi(mn) = \phi(m)\phi(n)$.

(C) Let $A = \{x_1, \dots, x_n\}$ be an n-set (in short)
2^A denotes set of all subsets of A and
$\{0,1\}^n := \{ (\epsilon_1, \epsilon_2, \dots, \epsilon_n) : \epsilon_i \in \{0,1\} \}$
Here take $S = 2^A$ and $R = \{0,1\}^n$
We map $\{x_{i_1}, \dots, x_{i_k}\}$ to $(\epsilon_1, \dots, \epsilon_n)$, where

$$\epsilon_j = \begin{cases} 1 & \text{if } j = i_1, j = i_2, \dots, j = i_k \\ 0 & \text{otherwise} \end{cases}$$

We call such a map as θ. i.e $\theta : 2^A \to \{0,1\}^n$

Note that θ is one-one and onto function. This implies
$|2^A| = |\{0,1\}^n| = 2^n$.

The double counting principle: Let A and B be two non-empty finite sets and $S = A \times B$.

The double counting principle is to count $|S|$ in two different ways

First way: We count $\sum_{a \in A} |\{b \in B : (a,b) \in S\}|$

Second way: We count $\sum_{b \in B} |\{a \in A : (a,b) \in S\}|$

We count S in two ways and such counting gives us the following identity

$$\sum_{a \in A} |\{b \in B : (a,b) \in S\}| = \sum_{b \in B} |\{a \in A : (a,b) \in S\}|.$$

Nov 27, 2020 8:30 AM

LATIN SQUARES

Def^{n}: An $[n]$-valued square matrix of order n (i.e. a fn^{t} $\pi : [n]\times[n] \to [n]$) is called a Latin square if $\forall i, j \in [n]$, the fn^{s} π_i and π^j, where $\pi_i(j) = \pi^j(i) = \pi(i,j)$, satifies the conditions that $\forall x \in [n]$, $\pi_i(x) = \pi_j(x)$ or $\pi^i(x) = \pi^j(x)$ implies $i=j$.

Claim: For each $i \in [n]$ the fn^{t} $\pi_i : [n] \to [n]$ is an one-one (hence onto) fn^{t} (Similarly $\forall j \in [n]$ the fn^{t} $\pi^j : [n] \to [n]$ is an one-one fn^{t}).

Proof of claim: For $i, x, y \in [n]$, suppose $\pi_i(x) = \pi_i(y)$

$$\Rightarrow \pi(i,x) = \pi(i,y)$$
$$\Rightarrow \pi^x(i) = \pi^y(i) \Rightarrow x = y.$$

The claim is established, since $i, x, y \in [n]$ is chosen arbitrarily.

Comment: For each $i \in [n]$, the fn^{s} π_i & π^i are permutations on $[n]$.

Example: (A)
$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \quad \begin{bmatrix} A & B & C & D \\ B & C & D & A \\ C & D & A & B \\ D & A & B & C \end{bmatrix} \quad \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix}$$

Comment: For an n-set T, one can take T-valued matrix of order n in the def^{n} of Latin square.

(B) If L is a Latin square, then interchange of any two rows (or columns) produces a Latin square. (Check T/F)

Observe the following and find the difference

1. $$\left(\begin{bmatrix} A & B & C & D \\ B & C & D & A \\ C & D & A & B \\ D & A & B & C \end{bmatrix}, \begin{bmatrix} 4 & 2 & 3 & 1 \\ 1 & 3 & 4 & 2 \\ 2 & 4 & 1 & 3 \\ 3 & 1 & 2 & 4 \end{bmatrix} \right) \mapsto \begin{bmatrix} A4 & B2 & C3 & D1 \\ B1 & C3 & D4 & A2 \\ C2 & D4 & A1 & B3 \\ D3 & A1 & B2 & C4 \end{bmatrix}$$

2. $$\left(\begin{bmatrix} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix} \right) \mapsto \begin{bmatrix} A1 & B2 & C3 & D4 \\ B4 & A3 & D2 & C1 \\ C2 & D1 & A4 & B3 \\ D3 & C4 & B1 & A2 \end{bmatrix}$$

NOV 27, 2020 8:30AM

3. $\left(\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \right) \mapsto \begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}$

Def$^{\underline{n}}$: Two Latin squares $\pi_1 : [n] \times [n] \to [n]$ and $\pi_2 : [n] \times [n] \to [n]$ is said to be <u>orthogonal</u> if for the fu$^{\underline{n}}$

$$\pi : [n] \times [n] \to [n] \times [n]$$

$$\pi(i,j) = (\pi_1(i,j), \pi_2(i,j))$$

satisfies the property that if $\pi(i,j) = \pi(p,q)$ then $(i,j) = (p,q)$.

Th: (Möbius Inversion Formula) Let $f : \mathbb{N} \to \mathbb{R}$ be a fun^{c}. The function $g : \mathbb{N} \to \mathbb{R}$ defined as

$$g(n) = \sum_{d \mid n} f(d).$$

Then

$$f(n) = \sum_{d \mid n} \mu(d)\, g\left(\tfrac{n}{d}\right) \quad \text{——} \quad (+)$$

Proof: We begin with the RHS of (+)

$$\sum_{d \mid n} \mu(d)\, g\left(\tfrac{n}{d}\right) = \sum_{d \mid n} \mu\left(\tfrac{n}{d}\right) g(d) = \sum_{d \mid n} \mu\left(\tfrac{n}{d}\right) \sum_{d' \mid d} f(d')$$

$$= \mu(1) f(n) + \sum_{\substack{d \mid n \\ d \neq n}} f(d) \Big(\sum_{d' \mid \frac{n}{d}} \mu(d') \Big)$$

$$= \mu(1) f(n) + \sum_{\substack{d \mid n \\ d \neq n}} f(d) \cdot 0$$

$$= \mu(1) f(n)$$

$$= f(n)$$

□

RECURRENCE RELATIONS

(K is a positive integer)

Def^n: A real valued sequence $\{x_n\}_{n=0}^{\infty}$ is said to satisfy K-term recurrence relation if there exist a fu^n $\lambda : \mathbb{R}^K \to \mathbb{R}$ such that $x_0, x_1, \ldots, x_{K-1}$ is known (referred as initial conditions) and for each integer $n \geq 0$

$$x_{n+K} = \lambda(x_{n+K-1}, \ldots, x_0)$$

We say the fu^n λ as a <u>K-term recurrence fu^n</u> or simply <u>recurrence fu^n</u>.

A fu^n $\theta : \mathbb{R}^K \to \mathbb{R}$ is said to be <u>linear fu^n</u> if

$$\theta(\bar{x} + \alpha\bar{y}) = \theta(\bar{x}) + \alpha\,\theta(\bar{y}),$$

where $\bar{x}, \bar{y} \in \mathbb{R}^K$ and $\alpha \in \mathbb{R}$.

A fu^n $\nu : \mathbb{R}^K \to \mathbb{R}$ is said to be <u>homogeneous fu^n</u> of degree n if for each $\alpha \in \mathbb{R}$,

$$\nu(\alpha x_1, \ldots, \alpha x_K) = \alpha^n \nu(x_1, \ldots, x_K).$$

Def^n: A real valued seq^n $\{x_n\}_{n=0}^{\infty}$ is said to satisfy K-term <u>linear recurrence</u> relation or simply <u>linear recurrence relation</u> if $\exists$ a K-term recurrence fu^n $\lambda : \mathbb{R}^K \to \mathbb{R}$ with initial conditions $x_0, x_1, \ldots, x_{K-1}$ which is also a linear fu^n.

Def^n: A real valued seq^n $\{x_n\}_{n=0}^{\infty}$ is said to satisfy K-term <u>homogeneous recurrence</u> relation or simply <u>homogeneous recurrence relation</u> of degree n if $\exists$ a K-term recurrence fu^n $\lambda : \mathbb{R}^K \to \mathbb{R}$ with initial conditions $x_0, \ldots, x_{K-1}$ which is also a homogeneous fu^n of degree n.

Example: The Fibonacci seq^n (numbers) $\{f_n\}_{n=0}^{\infty}$ is defined by the recurrence relation:-

$$f_n = f_{n-1} + f_{n-2}$$

for each integer $n \geq 2$, with $f_0 = 0$, $f_1 = 1$.

The Fibonacci seq^n $\{f_n\}_{n=0}^{\infty}$ satisfies 2-term linear recurrence relation

Note that $\lambda : \mathbb{R}^2 \to \mathbb{R}$, where $(x, y) \xmapsto{\lambda} x + y$ is the respective function.

Example : Let m be a positive integer and $\{x_n\}_{n=0}^{\infty}$ be a seq^n defined by the recurrence relation :-

$$x_n = x_{n-1}^{m-1} x_{n-2} + x_{n-1} x_{n-2}^{m-1}$$

for each integer $n \geq 2$, $x_0 = 1$, $x_1 = 1$.

Check that the seq^n $\{x_n\}_{n=0}^{\infty}$ satisfies 2-term homogeneous recurrence relation of degree m.

SOME RESULTS ON FIBONACCI NUMBERS AND THEIR RECURRENCE RELATIONS

Th : Let f_n denote the n-th term of the Fibonacci seq^n $\{f_n\}_{n=0}^{\infty}$. Then $1 + \sum_{i=1}^{n} f_{2i} = f_{2n+1}$, $1 + \sum_{i=1}^{n} f_{2i-1} = f_{2n}$

$$(f_n)^2 = f_{n+1} f_{n-1} + (-1)^{n+1}$$

Proof : Exercise! Hint : Use induction on n.

Th : Let f_n denote n-th Fibonacci number, then

$$\lim_{n \to \infty} \frac{f_{n+1}}{f_n} = \tau,$$

where $\tau = \frac{1+\sqrt{5}}{2}$ (Golden ratio)

The continued fraction associates with the sequence $\{x_n\}_{n=0}^{\infty}$ is the number

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \cdots}}}$$

Check that the continued fraction associated with the seq^n $\{1_n (=1)\}_{n=0}^{\infty}$ is $\tau = \frac{1+\sqrt{5}}{2}$.

Note that $\tau > 1$ and satisfies the property $\tau = 1 + \frac{1}{\tau}$, so τ is the positive root of the eq^n $x^2 - x - 1 = 0$, which is $\frac{1+\sqrt{5}}{2}$

Proof : We note that $1 + \frac{1}{1} = \frac{2}{1} = \frac{f_3}{f_2}$ $1 + \frac{1}{1+\frac{1}{1}} = \frac{3}{2} = \frac{f_4}{f_3}$ and we have the continued fraction for the finite seq^n upto k-terms i.e $\{1_n (=1)\}_{n=1}^{k}$ is $\frac{f_{k+1}}{f_k} := \tau_k$

Note that $\tau_{n+1} = 1 + \frac{1}{\tau_n}$ $\forall$ integer n;

Therefore for each integer $n \geq 2$, we have

$$|\tau_n - \tau| = \left|1 + \frac{1}{\tau_{n-1}} - 1 - \frac{1}{\tau}\right| = \frac{1}{\tau \tau_{n-1}} |\tau_{n-1} - \tau| \leq \frac{1}{\tau} |\tau_{n-1} - \tau|$$

$$\leq \frac{1}{\tau^{n-1}} |\tau_1 - \tau|$$

$$= \frac{\sqrt{5}}{2} \frac{1}{\tau^{n-1}}$$

The result follows since $0 < \frac{1}{\tau} < 1$. □

STIRLING NUMBERS AND THEIR RECURRENCE RELATIONS

Def: Let n and K be positive integers with $n \geq K$. A cycle of length ℓ is a permutation $\Pi : [n] \to [n]$ such that there exist ℓ integers say $1 \leq i_1 < i_2 \cdots < i_\ell \leq n$ with the property that

$$\Pi(i_\ell) = i_1$$
$$\Pi(i_j) = i_{j+1} \quad \forall j \in [\ell-1]$$
$$\Pi(i) = i \quad \forall i \in [n] \setminus \{i_1, \cdots i_\ell\}$$

We denote such cycle of length ℓ as $(i_1 i_2 \cdots i_\ell)$

We say two cycles $(i_1 i_2 \cdots i_\ell)$ and $(j_1 \cdots j_m)$ are disjoint if the sets $\{i_1, i_2, \cdots, i_\ell\}$ and $\{j_1, \cdots j_m\}$ have empty intersection.

Th: (Cycle decomposition theorem) For each permutation $\Pi : [n] \to [n]$ there exist a positive integer $K = K(\Pi)$ such that Π can be written as a product of K disjoint cycles of different length.

Proof: Exercise!

Def: Let $c(n,K)$ denote the total no. of permutations of $[n]$, which can be written as a product of K disjoint cycles of different lengths. The Stirling Numbers of first Kind is defined and denoted as

$$S_K^I(n) = s(n,K) = (-1)^{n-K} c(n,K)$$

Th: Let n & K be positive integers with $n \geq K$, then

$$c(n,K) = c(n-1, K-1) + (n-1)\, c(n-1, K).$$

Proof: Let $C([n],K)$ = The set of all permutations of $[n]$, which can be written as a product of K disjoint cycles of different lengths

$\mathcal{A}$ = The set of all permutations of $[n]$, which can be written as a product of K disjoint cycles of different lengths, where n belongs, is a cycle of length 1.

$\mathcal{B}$ = The set of all permutations of $[n]$, which can be written as a product of K disjoint cycles of different lengths where n belongs, is a cycle of length at least 2.

Claim: $|\mathcal{A}| = c(n-1, K-1)$

Proof of claim: Exercise

Claim: $|\mathcal{B}| = (n-1)\, c(n-1, K)$

Proof of claim: Exercise

□

Sept 28, 2020 9:30 AM

Example: (Handshaking Lemma). Suppose there are n people at a party and every will shake hands with everyone else. How many handshakes will occur?

Here we count the set $\{(x, \{x,y\}) : x, y \in [n], x<y\} = S$ (say)

Note that the set $[n] = \{1, 2, \cdots n\}$ represents set of one hand (right hand) of each people

First way: There are n choices for x and chosen x there are $n-1$ choices for $\{x,y\}$. Hence

$$|S| = n(n-1).$$

Second way: Suppose there are N no. of handshakes i.e there are N choices for $\{x,y\}$ and chosen a handshake $\{x,y\}$, there are 2 choices namely $(x, \{x,y\})$ and $(y, \{x,y\})$. Hence

$$|S| = 2N.$$

Thus using the double counting principle we have

$$2N = |S| = n(n-1)$$

i.e $N = \dfrac{n(n-1)}{2}$

i.e there are $\dfrac{n(n-1)}{2}$ no of handshakes.

Remark: If we number the people from 1 to n. To avoid counting a hand twice, we count for the person i only handshakes with persons of upper numbers. Then total no. of handshakes is

$$\sum_{i=1}^{n} (n-i) = \sum_{i=1}^{n-1} i$$

Thus we have the folloing identity

$$\sum_{i=1}^{n} (n-i) = \sum_{i=1}^{n-1} i = \frac{n(n-1)}{2}$$

[One can deduct an identify using counting]

Sept 28, 2020   9:30 AM

: $\underbrace{a_1\, a_1 \cdots a_1}_{n_1},\ \underbrace{a_2\, a_2 \cdots a_2}_{n_2}, \cdots\cdots ; \underbrace{a_t\, a_t \cdots a_t}_{n_t}$

i.e. n_1 identical copies of the object a_1
n_2 identical copies of the object a_2 $\forall\, i, j \in [t]$

$a_i \neq a_j$

n_t identical copies of the object a_t i.e. a_i & a_j are distinguishable

set of the objects is $\{a_1, a_2, \ldots, a_t\}$

Multiset of the objects is $\{n_1 \cdot a_1, n_2 a_2, \ldots, n_t a_t\}$

or $\{\underbrace{a_1 \cdots, a_1}_{n_1}, \underbrace{a_2, \cdots a_2}_{n_2}, \cdots\cdots, \underbrace{a_t \cdots a_t}_{n_t}\}$

A 4-tuple (a_1, a_2, a_1, a_3) and an one-one and onto function $\pi : [4] \to [4]$. $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$ $4 \mapsto 4$

referred as permutation

Then $(a_1, a_2, a_1, a_3) \xmapsto{\pi} (a_1, a_1, a_2, a_3)$

if $\pi : [4] \to [4]$, $1 \mapsto 3$, $3 \mapsto 1$, $2 \mapsto 2$, $4 \mapsto 4$.

Then $(a_1, a_2, a_1, a_3) \xmapsto{\pi} (a_1, a_2, a_1, a_3)$

Def^n: Let for each $i \in [t]$, there be a collection of n_i identical copies of the object a_i and K be an integer with $0 \leq K \leq n_1 + \cdots + n_t$.

- A K-tuple $(x_1, \cdots, x_K)$, where $\forall\, r \in [K]$ $x_r = a_i$ for some $i \in [t]$, is said to be unordered if for each Permutation $\pi : [K] \to [K]$ · $(x_{\pi(1)}, \cdots, x_{\pi(K)})$ is same as $(x_1, \cdots, x_K)$.

- A K-tuple $(x_1, \cdots, x_K)$, where $\forall\, r \in [K]$, $x_r = a_i$ for some $i \in [t]$, is said to be ordered if for each permutation $\pi : [K] \to [K]$, other than identity permutation and the permutations $\mu : [K] \to [K]$ with the property that $x_{\mu(i)} = x_{\mu(j)}$ whenever $x_i = x_j$, where $i, j \in [K]$, $(x_{\pi(1)}, \cdots, x_{\pi(K)})$ is not same as $(x_1, \cdots, x_K)$.

Sept 29, 2020 9:30 AM

PERMUTATIONS

Def^n: An one-one and onto function $\lambda : [n] \to [n]$ is called permutation, where n is a positive integer & $[n] := \{1, 2, \cdots n\}$
The set of all such permutations is denoted as S_n.

Example: (A) Take $n = 3$

$\lambda : [3] \to [3]$

$$\lambda(1) = 2 \quad \text{or} \quad 1 \xmapsto{\lambda} 2 \quad \text{or} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$\lambda(2) = 1 \qquad 2 \xmapsto{\lambda} 1$$
$$\lambda(3) = 3 \qquad 3 \xmapsto{\lambda} 3$$

† Three presentation of same permutation λ †

(B) Take $n = K$

$\lambda : [K] \to [K]$

$$\lambda(1) = 2 \qquad 1 \xmapsto{\lambda} 2$$
$$\lambda(2) = 3 \quad \text{OR} \quad 2 \xmapsto{\lambda} 3 \quad \text{OR} \quad \begin{pmatrix} 1 & 2 & \cdots & K-1 & K \\ 2 & 3 & & K & 1 \end{pmatrix}$$
$$\vdots \qquad\qquad \vdots$$
$$\lambda(K-1) = K \qquad K-1 \xmapsto{\lambda} K$$
$$\lambda(K) = 1 \qquad K \xmapsto{\lambda} 1$$

(C) $S_3 = \{\lambda : \lambda : [3] \to [3] \text{ is a permutation}\}$

$$= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Note: $|S_3| = 6$

Question: What is the $|S_n|$, where n is a positive integer?

Comment: Let $\lambda : [n] \to [n]$ and $\mu : [n] \to [n]$ be two mapping
Then $\lambda \circ \mu : [n] \to [n]$ defined by

$$\lambda \circ \mu(i) = \lambda(\mu(i))$$

is called <u>composition</u> of permutations λ and μ.
In general $\lambda \circ \mu$ & $\mu \circ \lambda$ are not same (Find examples).
However $\lambda \circ \mu$ (or $\mu \circ \lambda$) is again a permutation (Prove it)

Note: $$\begin{pmatrix} 1 & 2 & \cdots & K \\ \lambda(1) & \lambda(2) & & \lambda(K) \end{pmatrix} \begin{pmatrix} 1 & 2 & & K \\ \mu(1) & \mu(2) & & \mu(K) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & K \\ \lambda(\mu(1)) & \lambda(\mu(2)) & \cdots & \lambda(\mu(K)) \end{pmatrix}$$

ie $$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Sept 29, 2020 9:30 AM

Defⁿ: Let n & K be positive integers. A <u>K-permutation</u> of an n-set X (n-set means a set of size n) is an ordered K-tuple of the elements of X.

Note: An n-permutation of an n-set X is simply a permutation (of X).

Def: Let n & K be positive integers. A <u>K-combination</u> of an n-set X is an unordered K-tuple of the elements of X.

Th: Let n & K be positive integers with $n \geq K$. Then the number of K-permutations of an n-set is given by

$$n(n-1) \cdots (n-K+1).$$

Proof: Let X be an n-set and $(x_1, \ldots, x_K)$ be a K-permutation. The first element x_1 can be chosen n ways. Having chosen the first element x_1, the second element x_2 can be chosen in $(n-1)$ ways (out of the remaining $(n-1)$ elements). Proceeding in this manner, we have the last, i.e the Kth element x_K can be chosen in $n-(K-1)$ ways.

The result follows using multiplication principle of counting. □

Notation: $P(n,K)$ denotes the no of K-permutations of an n-set

i.e $P(n,K) = n(n-1) \cdots (n-K+1)$

Similarly, $C(n,K)$ denotes the no of K-combinations of an n-set.

Th: Let n and K be positive integers. Then

$$C(n,K) = \frac{P(n,K)}{P(K,K)}$$ = no. of K-permutations of an n-set

Proof: We count the set of all K-permutations of an n-set in two ways

First way: It is $P(n,K)$

Second way: Fix a K-combination $(x_1, \ldots, x_K)$ in $C(n,K)$ ways. If we order the chosen K-combination $(x_1, \ldots x_K)$, it yields a K-permutation. So we order the chosen K-combination in $P(K,K)$ ways.

Hence we have $P(n,K) = C(K,K)\,P(K,K)$ and the result follows

Nov 27, 2020 8:30 AM

LATIN SQUARES

Defⁿ: An $[n]$-valued square matrix of order n (i.e. a fnᶜ $\pi:[n]\times[n]\to[n]$) is called a Latin square if $\forall i,j\in[n]$, the fnᶜs π_i and π^j, where $\pi_i(j)=\pi^j(i)=\pi(i,j)$, satisfies the conditions that $\forall x\in[n]$, $\pi_i(x)=\pi_j(x)$ or $\pi^i(x)=\pi^j(x)$ implies $i=j$.

Claim: For each $i\in[n]$ the fnᶜ $\pi_i:[n]\to[n]$ is an one-one (hence onto) fnᶜ (Similarly $\forall j\in[n]$ the fnᶜ $\pi^j:[n]\to[n]$ is an one-one fnᶜ).

Proof of claim: For $i,x,y\in[n]$, suppose $\pi_i(x)=\pi_i(y)$

$$\Rightarrow \pi(i,x)=\pi(i,y)$$

$$\Rightarrow \pi^x(i)=\pi^y(i)\Rightarrow x=y.$$

The claim is established, since $i,x,y\in[n]$ is chosen arbitrarily.

Comment: For each $i\in[n]$, the fnᶜs π_i & π^i are permutations on $[n]$.

Example: (A)
$$\begin{bmatrix}1&2&3\\2&3&1\\3&1&2\end{bmatrix}\quad\begin{bmatrix}A&B&C&D\\B&C&D&A\\C&D&A&B\\D&A&B&C\end{bmatrix}\quad\begin{bmatrix}0&1&2&3&4\\1&2&3&4&0\\2&3&4&0&1\\3&4&0&1&2\\4&0&1&2&3\end{bmatrix}$$

Comment: For an n-set T, one can take T-valued matrix of order n in the defⁿ of Latin square.

(B) If L is a Latin square, then interchange of any two rows (or columns) produces a Latin square. (Check T/F)

Observe the following and find the difference

1. $$\left(\begin{bmatrix}A&B&C&D\\B&C&D&A\\C&D&A&B\\D&A&B&C\end{bmatrix},\begin{bmatrix}4&2&3&1\\1&3&4&2\\2&4&1&3\\3&1&2&4\end{bmatrix}\right)\mapsto\begin{bmatrix}A4&B2&C3&D1\\B1&C3&D4&A2\\C2&D4&A1&B3\\D3&A1&B2&C4\end{bmatrix}$$

2. $$\left(\begin{bmatrix}A&B&C&D\\B&A&D&C\\C&D&A&B\\D&C&B&A\end{bmatrix},\begin{bmatrix}1&2&3&4\\4&3&2&1\\2&1&4&3\\3&4&1&2\end{bmatrix}\right)\mapsto\begin{bmatrix}A1&B2&C3&D4\\B4&A3&D2&C1\\C2&D1&A4&B3\\D3&C4&B1&A2\end{bmatrix}$$

NOV 27, 2020 8:30AM

3. $\left(\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix} \right) \mapsto \begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{bmatrix}$

Def$^{\underline{n}}$: Two Latin squares $\pi_1 : [n]\times[n] \to [n]$ and $\pi_2 : [n]\times[n] \to [n]$ is said to be <u>orthogonal</u> if for the fn$^{\underline{c}}$

$$\pi : [n]\times[n] \to [n]\times[n]$$

$$\pi(i,j) = (\pi_1(i,j), \pi_2(i,j))$$

satisfies the property that if $\pi(i,j) = \pi(p,q)$ then $(i,j) = (p,q)$.

Oct 12, 2020, 9:30 AM

$\frac{1}{2}$

COUNTING PROBLEMS ON LABELLED AND UNLABELLED OBJECTS

Defn: A labelled collection of n objects means n distinguishable objects and unlabelled collection of n objects means n indistinguishable objects.

Example: A collection of n apples or a collection of n identical objects are example of unlabelled collection.

O O O . . . . O
← n identical objects →

[1] [2] . . . . . [K]
← K labelled boxes →

Problem: How many ways you can distribute n identical objects into K distinguishable boxes.

Special case of the problem: How many ways you can distribute 10 (identical) biscuits among 3 students. Amit, Naren and Raju.

Soln

STEP 0: O O O O O O O O O O ← 10 biscuits

—— —— ← 2 separator

STEP 1: Place these two separator among the 10 biscuits

e.g. (1) OO | OOOOO | OOO i.e [2B] [5B] [3B]
A N R — A N R

(2) OOOO | OOOO | OO i.e [4A] [4B] [2B]
A N R — A N R

(3) OOOOOO | OOOO | i.e [6B] [4B] [0B]
A N R — A N

STEP 2: Consider 12 biscuits. choose any two of them and throw it and replace the chosen two biscuits by two separators.

Oct 12, 2020 9:30 AM

Th: One can distribute n identical objects into K labelled boxes into $\binom{n+K-1}{K-1}$ ways.

$\frac{2}{2}$

Proof: Let B be the set of labelled boxes.
Note that $|B| = K$,
For each distribution D, of n identical objects into B, we associate a function $r_D : B \to \mathbb{N}$ as

$r_D(b)$ = No. of identical objects received by the box b with respect to distribution D.

We note that for each distribution $D \in \mathcal{D}$

$$\sum_{b \in B} r_D(b) = n,$$

where $\mathcal{D}$ denotes the collection of all distributions of n identical objects into K labelled boxes.

[Note we need to know $|\mathcal{D}| = ?$]

Note that $|\mathcal{D}| = |\{r_D : D \in \mathcal{D}\}|$

Establish it (Exercise: Hint: Show that $D \mapsto r_D$ from $\mathcal{D}$ to $\{r_D : D \in \mathcal{D}\}$ is a well defined one-one onto map)

$$= |\{f : [K] \to \mathbb{N} : f(1) + f(2) + \cdots + f(K) = n\}|$$

claim: $|\{f : [K] \to \mathbb{N} : f(1) + f(2) + \cdots + f(K) = n\}| = \left|\binom{[n+K-1]}{K-1}\right|$

Proof of claim: $\forall\ B \in \binom{[n+K-1]}{K-1}$ we associate in a unique way a function $f_B : [K] \to \mathbb{N}$ with $f(1) + \cdots + f(K) = n$

Let $B \in \binom{[n+K-1]}{K-1}$ & $B = \{i_1, i_2, \ldots, i_{K-1}\}$ WLOG $i_1 < i_2 \cdots < i_{K-1}$

$f_B(1) = |\{i : i < i_1\}|$

$f_B(2) = |\{i : i_1 < i < i_2\}|$

$\vdots$

$f_B(K-1) = |\{i : i_{K-2} < i < i_{K-1}\}|$

$f_B(K) = |\{i : i_{K-1} < i\}|$

Note that $f(1) + f(2) + \cdots + f(K) = n$.

Conversely, for a function $f : [K] \to \mathbb{N}$ with $f(1) + f(2) + \cdots + f(K) = n$ we associate the $(K-1)$-set $\{i_1, i_2, \ldots i_{K-1}\}$ in the "inverse way" where

$i_1 = f(1) + 1$

$i_2 = f(1) + f(2) + 2$

$\vdots$

$i_{K-1} = f(1) + f(2) + \cdots + f(K-1) + K-1$

Hence the claim is established. and the result follows. $\square$

Sept 16, 2020, 8:30 AM

We have

1 2 ... n $\boxed{1}$ $\boxed{2}$ ... $\boxed{K}$

← n distinguishable objects →   ← K distinguishable boxes →

Th: One can distribute n distinguishable objects into K distinguishable boxes into K^n ways.

Proof: Distribution of n distinguishable objects into K distinguishable boxes yields a function $d:[n] \to [K]$, where

$d(i)$ = the label of the box where object i is distributed

Conversely if $f:[n]\to[K]$ is a function then $f^{-1}(1), f^{-1}(2), \ldots, f^{-1}(K)$ is a partition on $[n]$ into K distinguishable parts. So such distribution can be done in

$$\left|\{f : f:[n]\to[K] \text{ is a function}\}\right| = K^n \text{ ways} \qquad \square.$$

Th: One can distribute n distinguishable objects into K distinguishable boxes such that each box contains atleast one distinguishable object into $K!\,S(n,K)$ ways.

Proof: Distribution of n distinguishable objects into K distinguishable boxes such that each box is non-empty results an onto function from $[n]$ to $[K]$ and vice versa.

$O([n],[K])$ = The collection of all onto fu^ns from $[n]$ to $[K]$.

We define an equivalence relation on $O([n],[K])$.

$f \sim g$, where $f, g \in O([n],[K])$, if and only if $\exists$ a permutation $\pi:[K]\to[K]$ such that $g = \pi \circ f$

Let $[f]$ denote the equivalence class containing $f \in O([n],[K])$.

then $|[f]| = K!$.

Claim: There are $S(n,K)$ no. of equivalence classes with respect to the afore mentioned equivalence relation.

Proof of the claim: We first establish that if $f, g \in O([n],[K])$ such that the unordered K-tuple

$(f^{-1}(1), f^{-1}(2), \ldots, f^{-1}(K))$ and $(g^{-1}(1), g^{-1}(2), \ldots, g^{-1}(K))$

are same, then $\exists$ a permutation $\pi:[K]\to[K]$ such that $f = \pi \circ g$.

Sept 16, 2020 8:30 AM

$[n] \xrightarrow{f} [k] \xrightarrow{\lambda} [k]$.

$[n] \xrightarrow{g} [k] \xrightarrow{\phi} [k]$.

Let $\lambda : [k] \to [k]$ & $\phi : [k] \to [k]$ are the permutations such that

$\lambda \circ f = \phi \circ g$

Then $\pi = \lambda^{-1} \circ \phi$ is the required permutation

This implies two differerent partitions of $[n]$ into k non empty parts represents two different equivalent classes

Since there are $S(n,k)$ no. of partitions of $[n]$ into k non empty parts. So such distribution can be done in $|\Theta([n],[k])| = k!\,S(n,k)$ ways which equals the no. of partitions of $[n]$ into k non-empty distinguishable parts. $\square$

Cor. There are $k!\,S(n,k)$ no. of onto fu^{n}s from $[n]$ to $[k]$.

APPLICATIONS OF INCLUSION & EXCLUSION THEOREM.

Th: If $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, where $\forall\, i \in [k]$, $n_i \geq 1$ are integers, and p_i is a prime no.

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

Here ϕ denotes Euler's phi fu$\overset{n}{=}$.

Proof: For each $i \in [k]$, let P_i denote the property that $x\ (\in [n])$ is divisible by the prime p_i.

Claim: The set of elements of $[n]$ that satisfies none of the properties $P_1, P_2, \ldots, P_k$ is the set

$$R = \{x \in [n] : \gcd(x, n) = 1\}.$$

$\boxed{\text{Recall that } \phi(n) = |R|}$

Proof of claim: We note that if x does not satisfy the property P_i for some $i \in [k]$, then $\gcd(x, p_i) = 1$.

This implies $\exists\ u, v \in \mathbb{Z}$ s.t $xu + p_i v = 1 \Leftrightarrow (xu + p_i v)^{n_i} = 1$

$$\Leftrightarrow x\left(\sum_{j=0}^{n_i-1} \binom{n_i}{j} x^{n_i-j-1} u^{n_i-1} p^j v^j\right) + p^{n_i} v^{n_i} = 1$$

i.e $\gcd(x, p_i^{n_i}) = 1$

Therefore we have if x does not satisfy the property P_i for some $i \in [k]$, then $\gcd(x, p_i^{n_i}) = 1$

So if x does not satisfy none of $P_1, P_2, \ldots, P_k$, then $\exists$ $u_i, v_i \in \mathbb{Z}$ with $i \in [k]$ such that

$$(x u_1 + p_1^{n_1} v_1)(x u_2 + p_2^{n_2} v_2) \cdots (x u_k + p_k^{n_k} v_k) = 1$$

$$\Leftrightarrow \quad xU + nV = 1 \quad \text{for some } U, V \in \mathbb{Z}.$$

Therefore $\gcd(x, n) = 1$ and consequently $x \in R$.

Conversely if $x \in R$, then $\gcd(x, n) = 1$. Then $\exists$ $U, V \in \mathbb{Z}$ s.t

$$xU + nV = 1$$

$$\Leftrightarrow \quad xU + p_j\left(\frac{n}{p_j} V\right) = 1 \quad \forall\ j \in [k].$$

Hence $\gcd(x, p_j) = 1 \quad \forall\ j \in [k]$

i.e x does not satisfy $P_1, P_2, \ldots, P_k$

The claim is established

Claim : For $S \subseteq [n]$, $|N(S)| = \dfrac{n}{\prod_{i \in S} p_i}$

Proof of claim: We note the following

$$x \in N(S) \Leftrightarrow x \text{ satisfies property } P_i \ \forall i \in S$$
$$\Leftrightarrow p_i \mid x \quad \forall i \in S$$
$$\Leftrightarrow \prod_{i \in S} p_i \mid x \quad \text{since } \forall i,j \in S \text{ with } i \neq j \ \gcd(p_i, p_j) = 1$$

Hence we have

$$N(S) = \left\{ x \in [n] : x = r\left(\prod_{i \in S} p_i\right), \ r = 1, 2, \cdots, \frac{n}{\prod_{i \in S} p_i} \right\}$$

Which establishes the claim.

Now using the version (ii) of inclusion & exclusion theorem and the above claims

$$\phi(n) = |R| = \sum_{S \subseteq [k]} (-1)^{|S|} |N(S)| = \sum_{S \subseteq [k]} (-1)^{|S|} \frac{n}{\prod_{i \in S} p_i}$$
$$= n \sum_{S \subseteq [k]} \frac{(-1)^{|S|}}{\prod_{i \in S} p_i}$$
$$= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Note: Convention $\prod_{i \in \phi} p_i = 1$

MORE RESULTS ON EULER PHI FUNCTION

Th: For each positive integer n, $n = \sum_{d \mid n} \phi(d)$

Proof: Let $\gcd(x, n) = d$ then $\exists\, u, v \in \mathbb{Z}$ s.t $xu + nv = d \Leftrightarrow \frac{x}{d} u + \frac{n}{d} v = 1$.
So $x \mapsto \frac{x}{d} (:= y)$ is a bijective mapping from
$$\{x \in [n] : \gcd(x, n) = d\} \text{ to } \{y \in [\tfrac{n}{d}] : \gcd(y, \tfrac{n}{d}) = 1\}$$

Hence $|\{x \in [n] : \gcd(x, n) = d\}| = \phi\left(\frac{n}{d}\right)$

Note that $\{x \in [n] : \gcd(x, n) = d\} = \phi$ if and only if $d \nmid n$

Hence
$$n = \left| \bigsqcup_{d=1}^{n} \{x \in [n] : \gcd(x, n) = d\} \right| = \left| \bigsqcup_{d \mid n} \{x \in [n] : \gcd(x, n) = d\} \right|$$
$$= \sum_{d \mid n} |\{x \in [n] : \gcd(x, n) = d\}|$$
$$= \sum_{d \mid n} \phi\left(\frac{n}{d}\right) = \sum_{d \mid n} \phi(d). \quad \square$$

THE MÖBIUS FUNCTION

Def^n: The Möbius fun: $\mu : \{n \in \mathbb{N} : n \geq 1\} \to \{-1, 0, 1\}$ is defined in the following way:

$\mu(1) = 1$; for $n = \prod_{i=1}^{k} p^{n_i}$, where $i \in [k]$ and $n_i \geq 1$ are integers,

$$\mu(n) = \mu\left(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}\right) = \begin{cases} (-1)^k & \text{if } n_1 = n_2 = \cdots = n_k = 1 \\ 0 & \text{if } n_j \geq 2 \text{ for some } j \in [k]. \end{cases}$$

Th: For each positive integer n,

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases}$$

Proof: If $n = 1$, then the only divisor of 1 is $d = 1$. Hence $\sum_{d \mid n} \mu(d) = \mu(1) = 1$.

So suppose $n \geq 2$ and $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$

$$= \prod_{i=1}^{k} p_i^{n_i}.$$

Then we have

$$\sum_{d \mid n} \mu(d) = \sum_{d \mid p_1 \cdots p_k} \mu(d) = \sum_{S \subseteq [k]} (-1)^{|S|} = \sum_{i=0}^{k} \binom{k}{i} (-1)^i = 0$$

Cor: For each positive integer $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$,

$$\frac{\phi(n)}{n} = \sum_{d \mid n} \frac{\mu(d)}{d}.$$

Proof: Note that

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) = n \sum_{S \subseteq [k]} \frac{(-1)^{|S|}}{\prod_{i \in S} p_i}$$

$$= n \sum_{d \mid p_1 \cdots p_k} \frac{\mu(d)}{d}$$

$$= n \sum_{d \mid n} \frac{\mu(d)}{d} \qquad \square$$

Th : For each integer $n \geq 2$, $S(n,2) = 2^{n-1}-1$.

Proof: Note that $S(2,2)=1$. Hence by using the previous theorem

$$S(n,2) = 1 + 2S(n-1,2) = 1 + 2 + 2^2 + \cdots + 2^{n-2}\underbrace{S(2,2)}_{=1} = 2^{n-1}-1$$

Proof : $\mathcal{S}([n],2)$ = The collection (set) of all partitions of $[n]$ into 2 non-empty parts

& $\mathcal{P} = \{(A,B) : A \sqcup B = [n],\ A \neq \phi \neq B\}$ ← Note that the symbol $A \sqcup B$ is meaningful iff $A \cap B = \phi$

$|\mathcal{P}| = 2^n - 2$ (Exercise!)

Note that if $(A,B) \in \mathcal{P}$ then $(B,A) \in \mathcal{P}$ and $(A,B),(B,A)$ represents exactly one partition of $[n]$ into 2 non-empty parts namely A, B. (Why! Hint: Boxes are not labelled) Hence such mapping from $\mathcal{P}$ to $\mathcal{S}([n],2)$ is a 2-to-1, onto mapping. Hence

$$2\,|\mathcal{S}([n],2)| = \mathcal{P}.$$

i.e

$$S(n,2) = \frac{2^n-2}{2} = 2^{n-1}-1$$

□

Th : $S(n,n-1) = \binom{n}{2}$

Proof : Exercise (Hint: Apply PHP, to conclude that partition of $[n]$ into $(n-1)$ non-empty parts produces a unique part consist of 2 elements of $[n]$)

Th : One can distributes n distinguishable objects into k identical boxes such that each box contain at least one distinguishable object, into $S(n,k)$ ways.

Proof : $\mathcal{D}$ = The set of all distributions of n distinguishable objects into k identical boxes such that each box contain at least one distinguishable object.

$\mathcal{S}([n],k)$ = The set of all partitions of $[n]$ into k non empty part

Let $[n] = \{1,2,\cdots,n\}$ is the set of n distinguishable objects. We distribute these n objects into k identical boxes such that each box is non-empty.
For $x,y \in [n]$, we say $x \sim y$ if and only if x & y are in same bo
This yields a equivalence relation on $[n]$. Such equivalence relation produces equivalence classes, which is the required partition on $[n]$.

Oct 14, 2020 9:30 AM

We associate each $D \in \mathcal{D}$ with the unique equivalence relation on $[n]$ with respect to D (i.e $x \sim y$, where $x, y \in [n]$, if and only if x & y are in same box under D). Thus we have a bijective corresponce (Exercise) between

$\mathcal{D} \longleftrightarrow$ All equivalence relation on $[n]$ which produces exactly K non-empty equivalence classes.

Hence $|\mathcal{D}| = |\mathcal{S}([n],k)| = S(n,k)$. $\square$

Th: One can distribute n distinguishable objects into K identical boxes into $\sum_{i=1}^{K} S(n,i)$

$$S(n,0) + S(n,1) + \cdots + S(n,K)$$

Proof: Exercise

The Pigeonhole Principle

1 Pigeonhole Principle: Simple form

Theorem 1.1. *If $n+1$ objects are put into n boxes, then at least one box contains two or more objects.*

Proof. Trivial. $\square$

Example 1.1. Among 13 people there are two who have their birthdays in the same month.

Example 1.2. There are n married couples. How many of the $2n$ people must be selected in order to guarantee that one has selected a married couple?

Other principles related to the pigeonhole principle:

- If n objects are put into n boxes and no box is empty, then each box contains exactly one object.
- If n objects are put into n boxes and no box gets more than one object, then each box has an object.

The abstract formulation of the three principles: Let X and Y be finite sets and let $f : X \longrightarrow Y$ be a function.

- If X has more elements than Y, then f is not one-to-one.
- If X and Y have the same number of elements and f is onto, then f is one-to-one.
- If X and Y have the same number of elements and f is one-to-one, then f is onto.

Example 1.3. In any group of n people there are at least two persons having the same number friends. (It is assumed that if a person x is a friend of y then y is also a friend of x.)

Proof. The number of friends of a person x is an integer k with $0 \le k \le n-1$. If there is a person y whose number of friends is $n-1$, then everyone is a friend of y, that is, no one has 0 friend. This means that 0 and $n-1$ can not be simultaneously the numbers of friends of some people in the group. The pigeonhole principle tells us that there are at least two people having the same number of friends. $\square$

Example 1.4. Given n integers $a_1, a_2, \ldots, a_n$, not necessarily distinct, there exist integers k and l with $0 \le k < l \le n$ such that the sum $a_{k+1} + a_{k+2} + \cdots + a_l$ is a multiple of n.

Proof. Consider the n integers

$$a_1, \quad a_1 + a_2, \quad a_1 + a_2 + a_3, \quad \ldots, \quad a_1 + a_2 + \cdots + a_n.$$

Dividing these integers by n, we have

$$a_1 + a_2 + \cdots + a_i = q_i n + r_i, \quad 0 \le r_i \le n-1, \quad i = 1, 2, \ldots, n.$$

If one of the remainders $r_1, r_2, \ldots, r_n$ is zero, say, $r_k = 0$, then $a_1 + a_2 + \cdots + a_k$ is a multiple of n. If none of $r_1, r_2, \ldots, r_n$ is zero, then two of them must the same (since $1 \le r_i \le n-1$ for all i), say, $r_k = r_l$ with $k < l$. This means that the two integers $a_1+a_2+\cdots+a_k$ and $a_1+a_2+\cdots+a_l$ have the same remainder. Thus $a_{k+1}+a_{k+2}+\cdots+a_l$ is a multiple of n. $\square$

Example 1.5. A chess master who has 11 weeks to prepare for a tournament decides to play at least one game every day but, in order not to tire himself, he decides not to play more than 12 games during any calendar week. Show that there exists a succession of consecutive days during which the chess master will have played exactly 21 games.

Proof. Let a_1 be the number of games played on the first day, a_2 the total number of games played on the first and second days, a_3 the total number games played on the first, second, and third days, and son. Since at least one game is played each day, the sequence of numbers $a_1, a_2, \ldots, a_{77}$ is strictly increasing, that is, $a_1 < a_2 < \cdots < a_{77}$. Moreover, $a_1 \geq 1$; and since at most 12 games are played during any one week, $a_{77} \leq 12 \times 11 = 132$. Thus

$$1 \leq a_1 < a_2 < \cdots < a_{77} \leq 132.$$

Note that the sequence $a_1 + 21, a_2 + 21, \ldots, a_{77} + 21$ is also strictly increasing, and

$$22 \leq a_1 + 21 < a_2 + 21 < \cdots < a_{77} + 21 \leq 132 + 21 = 153.$$

Now consider the 154 numbers

$$a_1,\ a_2,\ \ldots,\ a_{77},\ a_1 + 21,\ a_2 + 21,\ \ldots,\ a_{77} + 21;$$

each of them is between 1 and 153. It follows that two of them must be equal. Since $a_1, a_2, \ldots, a_{77}$ are distinct and $a_1 + 21, a_2 + 21, \ldots, a_{77} + 21$ are also distinct, then the two equal numbers must be of the forms a_i and $a_j + 21$. Since the number games played up to the ith day is $a_i = a_j + 21$, we conclude that on the days $j + 1$, $j + 2$, …, i the chess master played a total of 21 games. □

Example 1.6. Given 101 integers from $1, 2, \ldots, 200$, there are at least two integers such that one of them is divisible by the other.

Proof. By factoring out as many 2's as possible, we see that any integer can be written in the form $2^k \cdot a$, where $k \geq 0$ and a is odd. The number a can be one of the 100 numbers $1, 3, 5, \ldots, 199$. Thus among the 101 integers chosen, two of them must have the same a's when they are written in the form, say, $2^r \cdot a$ and $2^s \cdot a$ with $r \neq s$. if $r < s$, then the first one divides the second. If $r > s$, then the second one divides the first. □

Example 1.7 (Chines Remainder Theorem). Let m and n be relatively prime positive integers. Then the system

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

has a solution.

Proof. We may assume that $0 \leq a < m$ and $0 \leq b < n$. Let us consider the n integers

$$a, \quad m + a, \quad 2m + a, \quad \ldots, \quad (n-1)m + a.$$

Each of these integers has remainder a when divided by m. Suppose that two of them had the same remainder r when divided by n. Let the two numbers be $im + a$ and $jm + a$, where $0 \leq i < j \leq n - 1$. Then there are integers q_i and q_j such that

$$im + a = q_i n + r \quad \text{and} \quad jm + a = q_j n + r.$$

Subtracting the first equation from the second, we have

$$(j - i)m = (q_j - q_i)n.$$

Since $\gcd(m, n) = 1$, we conclude that $n | (j - i)$. Note that $0 < j - i \leq n - 1$. This is a contradiction. Thus the n integers $a, m + a, 2m + a, \ldots, (n-1)m + a$ have distinct remainders when divided by n. That is, each of the n numbers $0, 1, 2, \ldots, n - 1$ occur as a remainder. In particular, the number b does. Let p be the integer with $0 \leq p \leq n - 1$ such that the number $x = pm + a$ has remainder b when divided by n. Then for some integer q, $x = qn + b$. So

$$x = pm + a = qn + b,$$

and x has the required property. □

2 Pigeonhole Principle: Strong Form

Theorem 2.1. *Let $q_1, q_2, \ldots, q_n$ be positive integers. If*

$$q_1 + q_2 + \cdots + q_n - n + 1$$

objects are put into n boxes, then either the 1st box contains at least q_1 objects, or the 2nd box contains at least q_2 objects, $\ldots$, the nth box contains at least q_n objects.

Proof. Suppose it is not true, that is, the ith box contains at most $q_i - 1$ objects, $i = 1, 2, \ldots, n$. Then the total number of objects contained in the n boxes can be at most

$$(q_1 - 1) + (q_2 - 1) + \cdots + (q_n - 1) = q_1 + q_2 + \cdots + q_n - n,$$

which is one less than the number of objects distributed. This is a contradiction. □

The simple form of the pigeonhole principle is obtained from the strong form by taking $q_1 = q_2 = \cdots = q_n = 2$. Then

$$q_1 + q_2 + \cdots + q_n - n + 1 = 2n - n + 1 = n + 1.$$

In elementary mathematics the strong form of the pigeonhole principle is most often applied in the special case when $q_1 = q_2 = \cdots = q_n = r$. In this case the principle becomes:

- If $n(r-1)+1$ objects are put into n boxes, then at least one of the boxes contains r or more of the objects. Equivalently,

- If the average of n nonnegative integers $a_1, a_2, \ldots, a_n$ is greater than $r - 1$, i.e.,

  $$\frac{a_1 + a_2 + \cdots + a_n}{n} > r - 1,$$

  then at leats one of the integers is greater than or equal to r.

Example 2.1. A basket of fruit is being arranged out of apples, bananas, and oranges. What is the smallest number of pieces of fruit that should be put in the basket in order to guarantee that either there are at least 8 apples or at least 6 bananas or at least 9 oranges?

Answer: $8 + 6 + 9 - 3 + 1 = 21$.

Example 2.2. Given two disks, one smaller than the other. Each disk is divided into 200 congruent sectors. In the larger disk 100 sectors are chosen arbitrarily and painted red; the other 100 sectors are painted blue. In the smaller disk each sector is painted either red or blue with no stipulation on the number of red and blue sectors. The smaller disk is placed on the larger disk so that the centers and sectors coincide. Show that it is possible to align the two disks so that the number of sectors of the smaller disk whose color matches the corresponding sector of the larger disk is at least 100.

Proof. We fix the larger disk first, then place the smaller disk on the top of the larger disk so that the centers and sectors coincide. There 200 ways to place the smaller disk in such a manner. For each such alignment, some sectors of the two disks may have the same color. Since each sector of the smaller disk will match the same color sector of the larger disk 100 times among all the 200 ways and there are 200 sectors in the smaller disk, the total number of matched color sectors among the 200 ways is $100 \times 200 = 20,000$. Note that there are only 200 ways. Then there is at least one way that the number of matched color sectors is $\frac{20{,}000}{200} = 100$ or more. □

Example 2.3. Show that every sequence $a_1, a_2, \ldots, a_{n^2+1}$ of $n^2 + 1$ real numbers contains either an increasing subsequence of length $n + 1$ or a decreasing subsequence of length $n + 1$.

Proof. Suppose there is no increasing subsequence of length $n+1$. We suffices to show that there must be a decreasing subsequence of length $n+1$.

Let ℓ_k be the length of the longest increasing subsequence which begins with a_k, $1 \le k \le n^2+1$. Since it is assumed that there is no increasing subsequence of length $n+1$, we have $1 \le \ell_k \le n$ for all k. By the strong form of the pigeonhole principle, $n+1$ of the n^2+1 integers $\ell_1, \ell_2, \ldots, \ell_{n^2+1}$ must be equal, say,

$$\ell_{k_1} = \ell_{k_2} = \cdots = \ell_{k_{n+1}},$$

where $1 \le k_1 < k_2 < \cdots < k_{n+1} \le n^2+1$. If there is one k_i $(1 \le i \le n)$ such that $a_{k_i} < a_{k_{i+1}}$, then any increasing subsequence of length $\ell_{k_{i+1}}$ beginning with $a_{k_{i+1}}$ will result a subsequence of length $\ell_{k_{i+1}}+1$ beginning with a_{k_i} by adding a_{k_i} in the front; so $\ell_{k_i} > \ell_{k_{i+1}}$, which is contradictory to $\ell_{k_i} = \ell_{k_{i+1}}$. Thus we must have

$$a_{k_1} \ge a_{k_{2+1}} \ge \cdots \ge a_{k_{n+1}},$$

which is a decreasing subsequence of length $n+1$. □

3 Ramsey Theory

Theorem 3.1 (Ramsey Theorem). *Let S be a finite set with n elements. Let $P_r(S)$ be the collection of all r-subsets of S with $r \ge 1$, i.e.,*

$$P_r(S) = \{X \subseteq S : |X| = r\}.$$

Then for any integers $p, q \ge r$ there exists a smallest integer $R(p,q;r)$ such that, if $n \ge R(p,q;r)$ and $P_r(S)$ is 2-colored with two color classes $\mathcal{C}_1$ and $\mathcal{C}_2$, then there is either a p-subset $S_1 \subseteq S$ such that $P_r(S_1) \subseteq \mathcal{C}_1$, or a q-subset $S_2 \subseteq S$ such that $P_r(S_2) \subseteq \mathcal{C}_2$.

Proof. We proceed by induction on p, q, and r. For $r=1$, we have $R(p,q;1) = p+q-1$. Note that every element of $P_1(S)$ is a singleton set and $|P_1(S)| = |S|$. For an n-set S with $n \ge p+q-1$, if $|\mathcal{C}_1| \ge p$, we take any p-subset $S_1 \subseteq \bigcup_{X \in \mathcal{C}_1} X$, then obviously $P_1(S_1) \subseteq \mathcal{C}_1$. If $|\mathcal{C}_1| < p$, then $|\mathcal{C}_2| \ge q$; we take any q-subset $S_2 \subseteq \bigcup_{X \in \mathcal{C}_2} X$ and obviously have $P_1(S_2) \subseteq \mathcal{C}_2$. Thus $R(p,q;1) \le p+q-1$. For $n = p+q-2$, let $\mathcal{C}_1$ be the set of $p-1$ singleton sets and $\mathcal{C}_2$ the set of the other $q-1$ singleton sets. Then it is impossible to have a p-subset $S_1 \subseteq S$ such that $P_1(S_1) \subseteq \mathcal{C}_1$ or a q-subset S_2 such that $P_1(S_2) \subseteq \mathcal{C}_2$. Thus $R(p,q;1) \ge p+q-1$.

Moreover, for any integer $r \ge 1$ it can be easily verified that

$$R(r,q;r) = q, \quad R(p,r;r) = p.$$

In fact, for $p = r$, let S be a q-set. For a 2-coloring $\{\mathcal{C}_1, \mathcal{C}_2\}$ of $P_r(S)$, if $\mathcal{C}_1 = \emptyset$, then $P_r(S) = \mathcal{C}_2$ and obviously $P_r(S_2) \subseteq \mathcal{C}_2$ for $S_2 = S$. If $\mathcal{C}_1 \ne \emptyset$, take an r-subset $A \in \mathcal{C}_1$; obviously, $P_r(A) = \{A\} \subseteq \mathcal{C}_1$. Thus $R(k,q;k) \le q$. Let $|S| \le q-1$. If $\mathcal{C}_1 = \emptyset$, then $\mathcal{C}_2 = P_r(S)$. It is clear that there is neither an r-subset $A \subseteq S$ such that $P_r(A) \subseteq \mathcal{C}_1$ nor a q-subset $B \subseteq S$ such that $P_r(B) \subseteq \mathcal{C}_2$. Thus $R(r,q;r) \ge q$. It is similar for the case $R(p,r;r) = p$.

Next we establish a recurrence relation about $R(p,q;r)$ for $r \ge 2$ as follows:

$$R(p,q;r) \le R(p_1,q_1;r-1)+1, \quad p_1 = R(p-1,q;r), \quad q_1 = R(p,q-1;r).$$

Let $n \ge R(p_1,q_1;r-1)+1$ and $|S| = n$. Take an element $x \in S$ and let $S_1 = S - \{x\}$. Then $|S_1| = n-1$ and $|S_1| \ge R(p_1,q_1;r-1)$. Let $\{\mathcal{C}, \mathcal{D}\}$ be a 2-coloring of $P_r(S)$ and let

$$\mathcal{C}_1 = \{A \in \mathcal{C} : x \notin A\}, \quad \mathcal{D}_1 = \{A \in \mathcal{D} : x \notin A\}.$$

Obviously, $\{\mathcal{C}_1, \mathcal{D}_1\}$ is a 2-coloring of $P_r(S_1)$. Let

$$\mathcal{C}_x = \{A \in P_{r-1}(S_1) : A \cup \{x\} \in \mathcal{C}\}, \quad \mathcal{D}_x = \{A \in P_{r-1}(S_1) : A \cup \{x\} \in \mathcal{D}\}.$$

For any $A \in P_{r-1}(S_1)$, it is obvious that either $A \cup \{x\} \in \mathcal{C}$ or $A \cup \{x\} \in \mathcal{D}$; then either $A \in \mathcal{C}_x$ or $A \in \mathcal{D}_x$. Thus $\{\mathcal{C}_x, \mathcal{D}_x\}$ is a 2-coloring of $P_{r-1}(S_1)$. Since $|S_1| \ge R(p_1,q_1;r-1)$ and by the induction hypothesis on k, we have (I) there exists a p_1-subset $X \subseteq S_1$ such that $P_{r-1}(X) \subseteq \mathcal{C}_x$, or (II) there exists a q_1-subset $Y \subseteq S_1$ such that $P_{r-1}(Y) \subseteq \mathcal{D}_x$.

Case (I): Since $p_1 = R(p-1, q; r)$ and $\{\mathcal{C}_1, \mathcal{D}_1\}$ is a 2-coloring of $P_r(S_1)$, by induction hypothesis on p (when r is fixed) there exists either a $(p-1)$-subset $X_1 \subseteq X$ such that $P_r(X_1) \subseteq \mathcal{C}_1 \subset \mathcal{C}$ or a q-subset $Y_1 \subseteq X$ such that $P_r(Y_1) \subseteq \mathcal{D}_1 \subset \mathcal{D}$. In the former case, consider the p-subset $X' = X_1 \cup \{x\} \subseteq S$. For any r-subset $A \subset X'$, if $x \notin A$, obviously $A \subset X_1$, so $A \in \mathcal{C}$; if $x \in A$, obviously $A - \{x\}$ is an $(r-1)$-subset of X, so $A - \{x\} \in \mathcal{C}_x$, then $A = (A - \{x\}) \cup \{x\} \in \mathcal{C}$. This means that X' is an r-subset of S and $P_r(X') \subseteq \mathcal{C}$. In the latter case, we already have a q-subset $Y_1 \subseteq S$ such that $P_r(Y_1) \subseteq \mathcal{D}$.

Case (II): Since $q_1 = R(p, q-1; r)$ and $\{\mathcal{C}_1, \mathcal{D}_1\}$ is a partition of $P_r(S_1)$, then by induction hypothesis on q (when r is fixed) there exists either a p-subset $X_1 \subseteq X$ such that $P_r(X_1) \subseteq \mathcal{C}_1 \subset \mathcal{C}$ or a $(q-1)$-subset $Y_1 \subseteq X$ such that $P_r(Y_1) \subseteq \mathcal{D}_1 \subset \mathcal{D}$. In the former case, we already have a p-subset $X_1 \subseteq S$ such that $P_r(X_1) \subseteq \mathcal{C}$. In the latter case, we have a q-subset $Y' = Y_1 \cup \{x\} \subset S$ and $P_r(Y') \subseteq \mathcal{D}$.

Now we have obtained a recurrence relation:

$$R(p, q; r) \leq R\Big(R(p-1, q; r), R(p, q-1; r); r-1\Big) + 1.$$

□

Theorem 3.2. *Let S be an n-set. Let $q_1, q_2, \ldots, q_k, r$ be positive integers such that $q_1, q_2, \ldots, q_k \geq r$. Then there exists a smallest integer $R(q_1, q_2, \ldots, q_k; r)$ such that, if $n \geq R(q_1, q_2, \ldots, q_k; r)$ and for any k-coloring $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_k\}$ of $P_r(S)$ there is at least one i $(1 \leq i \leq k)$ and a q_i-subset $S_i \subseteq S$ such that $P_r(S_i) \subseteq \mathcal{C}_i$.*

Proof. We proceed induction on k. For $k = 1$, then $P_r(S)$ is a 1-coloring of $P_r(S)$ itself; the theorem is obviously true. For $k = 2$, it is Theorem 3.1. For $k \geq 3$, let $\mathcal{D}_i = \mathcal{C}_i$ for $1 \leq i \leq k-2$ and $\mathcal{D}_{k-1} = \mathcal{C}_{k-1} \cup \mathcal{C}_k$. By the induction hypothesis there exists the integer $q'_{k-1} = R(q_{k-1}, q_k; r)$ and subsequently the integer $R(q_1, \ldots, q_{k-2}, q'_{k-1}; r)$.

Now for $|S| = n \geq R(q_1, \ldots, q_{k-2}, q'_{k-1}; r)$, since $\{\mathcal{D}_1, \ldots, \mathcal{D}_{k-1}\}$ is a $(k-1)$-coloring of $P_r(S)$, there exists either at least one q_i-subset $S_i \subseteq S$ such that $P_r(S_i) \subseteq \mathcal{D}_i = \mathcal{C}_i$ with $1 \leq i \leq k-2$ or a q'_{k-1}-subset $S'_{k-1} \subseteq S$ such that $P_r(S'_{k-1}) \subseteq \mathcal{D}_{k-1}$. In the former case, nothing is to be proved. In the latter case, let $\mathcal{D}'_{k-1} = \{A \in P_r(S'_{k-1}) : A \in \mathcal{C}_{k-1}\}$ and $\mathcal{D}'_k = \{A \in P_r(S'_{k-1}) : A \in \mathcal{C}_k\}$, then $\{\mathcal{D}'_{k-1}, \mathcal{D}'_k\}$ is a 2-coloring of $P_r(S'_{k-1})$. Since $|S'_{k-1}| = q'_{k-1} = R(q_{k-1}, q_k; r)$, there exists either a q_{k-1}-subset $S_{k-1} \subseteq S'_{k-1}$ such that $P_r(S_{k-1}) \subseteq \mathcal{D}'_{k-1}$ or a q_k-subset $S_k \subseteq S$ such that $P_r(S_k) \subseteq \mathcal{D}'_k$. Note that $\mathcal{D}'_{k-1} \subseteq \mathcal{P}_{k-1}$ and $\mathcal{D}'_k \subseteq \mathcal{P}_k$. Then there exists either a q_{k-1}-subset $S_{k-1} \subseteq S$ such that $P_r(S_{k-1}) \subseteq \mathcal{C}_{k-1}$ or a q_k-subset $S_k \subseteq S$ such that $P_r(S_k) \subseteq \mathcal{C}_k$.

Summarizing the above argument we obtain the recurrence relation:

$$R(q_1, q_2, \ldots, q_k; r) \leq R(q_1, q_2, \ldots, q_{k-2}, q'_{k-1}; r).$$

□

For positive integers $q_1, q_2, \ldots, q_k, r$ such that $q_1, q_2, \ldots, q_k \geq r$, $R(q_1, q_2, \ldots, q_k; r)$ are called *Ramsey numbers*. For any permutation $(\sigma_1, \sigma_2, \ldots, \sigma_k)$ of $(1, 2, \ldots, k)$, we have

$$R(q_{\sigma_1}, q_{\sigma_2}, \ldots, q_{\sigma_k}; r) = R(q_1, q_2, \ldots, q_k; r).$$

Proposition 3.3 (Pigeonhole Principle: The Strong Form). *If $r = 1$, then the Ramsey number $R(q_1, q_2, \ldots, q_k; 1)$ is the smallest integer n such that if the elements of an n-set are colored with k colors $c_1, c_2, \ldots, c_k$, then either there are q_1 elements of color c_1, or q_2 elements of color c_2, ..., or q_k elements of color c_k. Moreover,*

$$R(q_1, q_2, \ldots, q_k; 1) = q_1 + q_2 + \cdots + q_k - k + 1.$$

4 Applications of the Ramsey Theorem

Theorem 4.1. *For positive integers $q_1, \ldots, q_k$ there exists a smallest positive integer $R(q_1, \ldots, q_k; 2)$ such that, if $n \geq R(q_1, \ldots, q_k; 2)$ and for any edge coloring of the complete graph K_n with k colors $c_1, \ldots, c_k$, there is at least one i $(1 \leq i \leq k)$ such that K_n has a complete subgraph K_{q_i} of the color c_i.*

Proof. Each edge of K_n can be considered as a 2-subset of its vertices. □

In the book of Richard Brualdi, the Ramsey numbers $R(q_1, \ldots, q_k; 2)$ are denoted by $r(q_1, \ldots, q_k)$.

Theorem 4.2 (Erdös-Szekeres). *For any integer $k \geq 3$ there exists a smallest integer $N(k)$ such that, if $n \geq N(k)$ and for any n points on a plane having no three points through a line, then there is a convex k-gon whose vertices are among the given n points.*

Before proving the theorem we prove the following two lemmas first.

Lemma 4.3. *Among any 5 points on a plane, no three points through a line, 4 of them must form a convex quadrangle.*

Proof. Join every pair of two points by a segment to have a configuration of 10 segments. The circumference of the configuration forms a convex polygon. If the convex polygon is a pentagon or a quadrangle, the problem is solved. Otherwise the polygon must be a triangle, and the other two points must be located inside the triangle. Draw a straight line through the two points; two of the three vertices must be located in one side of the straight line. The two vertices on the same side and the two points inside the triangle form a quadrangle. □

Lemma 4.4. *Given $k \geq 4$ points on a plane, no 3 points through a line. If any 4 points are vertices of a convex quadrangle, then the k points are actually the vertices of a convex k-gon.*

Proof. Join every pair of two points by a segment to have a configuration of $k(k-1)/2$ segments. The circumference of the configuration forms a convex l-polygon. If $l = k$, the problem is solved. If $l < k$, there must be at least one point inside the l-polygon. Let $v_1, v_2, \ldots, v_l$ be the vertices of the convex l-polygon, and draw segments between v_1 and $v_3, v_4, \ldots, v_{l-1}$ respectively. The point inside the convex l-polygon must be located in one of the triangles $\triangle v_1v_2v_3, \triangle v_1v_3v_4, \ldots, \triangle v_1v_{l-1}v_l$. Obviously, the three vertices of the triangle with a given point inside together with the point do not form a convex quadrangle. This is a contradiction. □

Proof of Theorem 4.2. We apply the Ramsey theorem to prove Theorem 4.2. For $k = 3$, it is obviously true. Now for $k \geq 4$, if $n \geq R(k, 5; 4)$, we divide the 4-subsets of the n points into a class $\mathcal{C}$ of 4-subsets whose points are vertices of a convex quadrangle, and another class $\mathcal{D}$ of 4-subsets whose points are not vertices of any convex quadrangle. By the Ramsey theorem, there is either k points whose any 4-subset belongs to $\mathcal{C}$, or 5 points whose any 4-subset belongs to $\mathcal{D}$. In the formal case, the problem is solved by Lemma 4.4. In the latter case, it is impossible by Lemma 4.3. □

Theorem 4.5 (Schur). *For any positive integer k there exists a smallest integer N_k such that, if $n \geq N_k$ and for any k-coloring of $[1, n]$, there is a monochromatic sequence $x_1, x_2, \ldots, x_l$ $(l \geq 2)$ such that $x_l = \sum_{i=1}^{l-1} x_i$.*

Proof. Let $n \geq R(l, \ldots, l; 2)$ and let $\{A_1, \ldots, A_k\}$ be a k-coloring of $[1, n]$. Let $\{\mathcal{C}_1, \ldots, \mathcal{C}_k\}$ be a k-coloring of $P_2([1, n])$ defined by

$$\{a, b\} \in \mathcal{C}_i \quad \text{if and only if} \quad |a - b| \in A_i, \quad \text{where} \quad 1 \leq i \leq k.$$

By the Ramsey theorem, there is one r $(1 \leq r \leq k)$ and an l-subset $A = \{a_1, a_2, \ldots, a_l\} \subset [1, n]$ such that $P_2(A) \subseteq \mathcal{C}_r$. We may assume $a_1 < a_2 < \cdots < a_l$. Then

$$\{a_i, a_j\} \in \mathcal{C}_r \quad \text{and} \quad a_j - a_i \in A_r \quad \text{for all } i < j.$$

Let $x_i = a_{i+1} - a_i$ for $1 \leq i \leq l - 1$ and $x_l = a_l - a_1$. Then $x_i \in A_r$ for all $1 \leq i \leq l$ and $x_l = \sum_{i=1}^{l-1} x_i$. □

5 Van der Waerden Theorem

The Van der Waerden theorem states that for any k-coloring of the set $\mathbb{Z}$ of integers there always exists a monochromatic progression series.

Let $[a, b]$ denote the set of integers x such that $a \leq x \leq b$. Two tuples $(x_1, \ldots, x_m)$ and $(y_1, \ldots, y_m)$ of $[1, l]^m$ are said *l-equivalent*, written $(x_1, \ldots, x_m) \sim (y_1, \ldots, y_m)$, if all entries before the last l in each tuple are the same. For instance, for $l = 5$, $m = 4$,

$$(3, 5, 2, 5) \sim (3, 5, 2, 5), \quad (2, 4, 5, 2) \sim (2, 4, 5, 4), \quad (4, 3, 1, 4) \sim (2, 3, 2, 1), \quad (3, 5, 5, 1) \not\sim (3, 5, 2, 4).$$

Obviously, l-equivalence is an equivalence relation on $[0, l]^m$. All tuples of $[0, l - 1]^m$ are l-equivalent.

Definition 5.1. For integers $l, m \geq 1$, let $A(l, m)$ denote the statement: For any integer $k \geq 1$ there exists a smallest integer $N(l, m, k)$ such that, if $n \geq N(l, m, k)$ and $[1, n]$ is k-colored, then there are integers $a, d_1, d_2, \ldots, d_m \geq 1$ such that $a + l\sum_{i=1}^{m} d_i \leq n$ and for each l-equivalence class E of $[0, l]^m$,

$$\left\{ a + \sum_{i=1}^{m} x_i d_i : (x_1, \ldots, x_m) \in E \right\}$$

is monochromatic (having the same color).

When $m = 1$, there are only two l-equivalence classes for $[0, l]^m$, i.e.,

$$\{0, 1, 2, \ldots, l-1\} \quad \text{and} \quad \{l\}.$$

The statement $A(l, 1)$ means that for any integer $k \geq 1$ there exists a smallest integer $N(l, 1, k)$ such that, if $n \geq N(l, 1, k)$ and $[1, n]$ is k-colored, then there are integers $a, d \geq 1$ such that $a + ld \leq n$ and the sequence, $a, a+d, a+2d, \ldots, a+(l-1)d$, is monochromatic.

Theorem 5.2 (Graham-Rothschild). *The statement $A(l, m)$ is true for all integers $l, m \geq 1$.*

Proof. We proceed induction on l and m. For $l = m = 1$, the 1-equivalence classes of $[0, 1]$ are $\{0\}$ and $\{1\}$; the statement $A(1, 1)$ states that for any integer $k \geq 1$ there exists a smallest integer $N(1, 1; k)$ such that, if $n \geq N(1, 1; k)$ and $[1, n]$ is k-colored, then there are integers $a, d \geq 1$ such that $a + d \leq n$, and both $\{a\}$ and $\{a + d\}$ are monochromatic. This is obviously true and $N(1, 1; k) = 2$. We divide the induction argument into two statements:

(I) *If $A(l, m)$ is true for some $m \geq 1$ then $A(l, m+1)$ is true.*

(II) *If $A(l, m)$ is true for all $m \geq 1$ then $A(l+1, 1)$ is true.*

The induction goes as follows: The truth of $A(1, 1)$ implies the truth of $A(1, m)$ for all $m \geq 1$ by (I). Then by (II) the statement $A(2, 1)$ is true. Again by (I) the statement $A(2, m)$ is true for all $m \geq 1$. Continuing this procedure we obtain that $A(l, m)$ is true for all $l, m \geq 1$.

Proof of (I): Let the integer $k \geq 1$ be fixed. Since $A(l, m)$ is true, the integer $N(l, m, k)$ exists and set $p = N(l, m, k)$. Since $A(l, 1)$ is true, the integer $N(l, 1, k^p)$ exists and we set $q = N(l, 1, k^p)$, $N = pq$. Let $\phi : [1, N] \longrightarrow [1, k]$ be a k-coloring of $[1, N]$. Let $\psi : [1, q] \longrightarrow [1, k]^p$ be a k^p-coloring of $[1, q]$ defined by

$$\psi(i) = \Big(\phi((i-1)p+1),\, \phi((i-1)p+2),\, \ldots,\, \phi((i-1)p+p)\Big), \quad 1 \leq i \leq q. \tag{1}$$

Since $A(l, 1)$ is true, then for the k^p-coloring ψ of $[1, q]$ there are integers $a, d \geq 1$ such that

$$a + ld \leq q$$

and

$$\{a + xd : x = 0, 1, 2, \ldots, l-1\}$$

is monochromatic, i.e.,

$$\psi(a + xd) = \text{constant}, \quad x = 0, 1, 2, \ldots, l-1. \tag{2}$$

Note that $[(a-1)p+1, ap] \subseteq [1, pq]$ because $a \leq q$. Since $A(l, m)$ is true, then when ϕ is restricted to the p-set $[(a-1)p+1, ap]$ there are integers $b, d_1, d_2, \ldots, d_m \geq 1$ such that

$$(a-1)p + 1 \leq b, \quad b + l\sum_{i=1}^{m} d_i \leq ap,$$

and for each l-equivalence class E of $[0, l]^m$,

$$\left\{ b + \sum_{i=1}^{m} x_i d_i : (x_1, \ldots, x_m) \in E \right\}$$

is monochromatic, i.e.,

$$\phi\left(b+\sum_{i=1}^{m} x_i d_i\right) = \text{constant}, \quad (x_1,\ldots,x_m)\in E. \tag{3}$$

Recall that our job is to prove that $A(l, m+1)$ is true. For the k-coloring ϕ of $[1, N]$, we have had the integers

$$b, d_1, d_2, \ldots, d_{m+1} \geq 1, \quad \text{where} \quad d_{m+1} = dp.$$

Since $b + l\sum_{i=1}^{m} d_i \leq ap$ and $a + ld \leq q$, we have

$$b + l\sum_{i=1}^{m+1} d_i \leq ap + ldp = (a+dl)p \leq pq = N.$$

Now for any two l-equivalent tuples $(x_1,\ldots,x_{m+1})$ and $(y_1,\ldots,y_{m+1})$ of $[0,l]^{m+1}$, consider the numbers

$$\alpha = b + \textstyle\sum_{i=1}^{m+1} x_i d_i, \quad \beta = b + \sum_{i=1}^{m+1} y_i d_i,$$

$$\alpha_0 = b + \textstyle\sum_{i=1}^{m} x_i d_i, \quad \beta_0 = b + \sum_{i=1}^{m} y_i d_i.$$

Notice that our job is to show that α and β have the same color, i.e., $\phi(\alpha) = \phi(\beta)$. We divide the job into three cases:

Case 1. $x_{m+1} = y_{m+1} = l$. Then $x_i = y_i$ for all $1 \leq i \leq m$. Thus $\alpha = \beta$, and obviously, $\phi(\alpha) = \phi(\beta)$.

Case 2. $x_{m+1} = l$ and $y_{m+1} \leq l-1$, or, $x_{m+1} \leq l-1$ and $y_{m+1} = l$. This implies that $(x_1,\ldots,x_{m+1})$ and $(y_1,\ldots,y_{m+1})$ are not l-equivalent. This is a contradiction.

Case 3. $x_{m+1}, y_{m+1} \in [0, l-1]$. Then $(x_1,\ldots,x_m)$ and $(y_1,\ldots,y_m)$ are l-equivalent. It follows from (2) that $\psi(a) = \psi(a + x_{m+1}d)$, and by definition (1) of ψ, the corresponding coordinates of $\psi(a)$ and $\psi(a+x_{m+1}d)$ are equal, i.e.,

$$\phi\Big((a-1)p+i\Big) = \phi\Big((a+x_{m+1}d-1)p+i\Big), \quad i = 1, 2, \ldots, p.$$

Since $(a-1)p+1 \leq b \leq \alpha_0 \leq b + l\sum_{i=1}^{m} d_i \leq ap = (a-1)p+p$, there exists $j \in [1,p]$ such that $\alpha_0 = (a-1)p+j$. We then have

$$\alpha = \alpha_0 + x_{m+1}dp = (a-1)p + j + x_{m+1}dp = (a + x_{m+1}d - 1)p + j.$$

Thus

$$\phi(\alpha) = \phi\Big((a+x_{m+1}d-1)p+j\Big) = \phi\Big((a-1)p+j\Big) = \phi(\alpha_0).$$

Similarly, $\phi(\beta) = \phi(\beta_0)$. Since $(x_1,\ldots,x_m)$ and $(y_1,\ldots,y_m)$ are l-equivalent, it follows from (3) that $\phi(\alpha_0) = \phi(\beta_0)$. Therefore $\phi(\alpha) = \phi(\beta)$. This means that $A(l, m+1)$ is true and

$$N(l, m+1, k) \leq N(l, m, k) \cdot N\left(l, 1, k^{N(l,m,k)}\right).$$

Proof of (II): Fix an integer $k \geq 1$. Since $A(l,m)$ is true for all $m \geq 1$, the statement $A(l,k)$ is true and $N(l,k,k)$ exists. Let $N = 2N(l,k,k)$ and let ϕ be a k-coloring of $[1,N]$. Notice that the restriction of ϕ on $[1, N(l,k,k)]$ is a k-coloring. Then there are integers $a, d_1, d_2, \ldots, d_k \geq 1$ such that

$$a + l\sum_{i=1}^{k} d_i \leq N(l,k,k),$$

and for l-equivalent tuples $(x_1,\ldots,x_k), (y_1,\ldots,y_k) \in [0,l]^k$,

$$\phi\left(a + \sum_{i=1}^{k} x_i d_i\right) = \phi\left(a + \sum_{i=1}^{k} y_i d_i\right).$$

Consider the $k+1$ tuples (none of them are l-equivalent)

$$(0,0,\ldots,0),\ (l,0,\ldots,0),\ (l,l,\ldots,0),\ \ldots,\ (l,l,\ldots,l)$$

of $[0,l]^k$ to have $k+1$ distinct integers

$$a,\ a+ld_1,\ a+l(d_1+d_2),\ \ldots,\ a+l(d_1+d_2+\cdots+d_k).$$

At least two of them, say $a+l(d_1+\cdots+d_\lambda)$ and $a+l(d_1+\cdots+d_\mu)$ with $\lambda<\mu$, must have the same color, i.e.,

$$\phi\left(a+l\sum_{i=1}^{\lambda}d_i\right)=\phi\left(a+l\sum_{i=1}^{\mu}d_i\right). \tag{4}$$

For any $x\in[0,l-1]$, the two tuples

$$(\underbrace{l,\ldots,l}_{\lambda},\underbrace{x,\ldots,x}_{\mu-\lambda},0,\ldots,0)\quad\text{and}\quad(\underbrace{l,\ldots,l}_{\lambda},\underbrace{0,\ldots,0}_{\mu-\lambda},0,\ldots,0)$$

of $[0,l]^k$ are l-equivalent. Thus the numbers $a+l\sum_{i=1}^{\lambda}d_i+x\sum_{i=\lambda+1}^{\mu}d_i$ for $x\in[0,l-1]$ have the same color by ϕ, i.e.,

$$\phi\left(a+l\sum_{i=1}^{\lambda}d_i+x\sum_{i=\lambda+1}^{\mu}d_i\right)=\text{constant},\quad x=0,1,2,\ldots,l-1.$$

Combining this with (4) we have

$$\phi\left(a+l\sum_{i=1}^{\lambda}d_i+x\sum_{i=\lambda+1}^{\mu}d_i\right)=\text{constant},\quad x=0,1,2,\ldots,l-1,l.$$

Recall that our job is to prove the truth of $A(l+1,1)$. Let $b=a+l\sum_{i=1}^{\lambda}d_i$ and $d=\sum_{i=\lambda+1}^{\mu}d_i$. Then we have had the integers $b,d\geq 1$ such that

$$b+(l+1)d=a+l\sum_{i=1}^{\lambda}d_i+(l+1)\sum_{i=\lambda+1}^{\mu}d_i=a+l\sum_{i=1}^{\mu}d_i+\sum_{i=\lambda+1}^{\mu}d_i\leq N(l,k,k)+N(l,k,k)=N$$

and for the k-coloring ϕ of $[1,N]$, the l-equivalence class $\{0,1,2,\ldots,l\}$ of $[0,l+1]^1$ have the same color, i.e.,

$$\phi(b+xd)=\text{constant},\quad x=0,1,2,\ldots,l.$$

This means that the statement $A(l+1,1)$ is true. □

The truth of $A(l,m)$ for $m=1$ is called the Van der Waerden theorem.

Corollary 5.3 (Van der Waerden Theorem). *For any positive integers k and l there exists a smallest integer $N(l,k)$ such that, if $n\geq N(l,k)$ and $[1,n]$ is k-colored, then there is a monochromatic arithmetic sequence of length l in $[1,n]$.*

Supplementary Exercises

1. For the game of Nim, let us restrict that each player can move one or two coins. Find the winning strategy for each player.

2. Let n be a positive integer. In the game of Nim let us restrict that each player can move only $i\in\{1,2,\ldots,n\}$ coins each time from one heap. Find the winning strategy for each player.

3. Given $m(m-1)^2+1$ integral points on a plane, where m is odd. Show that there exists m points whose center is also an integral point.

We consider

$$S = \left\{ (x_1, \cdots, x_k) : (x_1, \cdots, x_k) \text{ is ordered } k\text{-tuple from the set } \{a_1, \cdots, a_n\} \right\}.$$

Here n & k are positive integers with $n \geq k$.

We say two elements of S say $(x_1 \cdots x_k)$ and $(y_1 \cdots y_k)$ are equivalent if $\exists$ a permutation $\pi : [k] \to [k]$ such that

$y_1 = x_{\pi(1)}, \; y_2 = x_{\pi(2)}, \; \cdots, \; y_k = x_{\pi(k)}$

Exercise : Show that such relation on S is an equivalence relation.

Note : Eequivalence relation produces equivalence classes. Here one equivalence class can be represented by the the <u>unordered</u> k-tuple $(x_1, \cdots, x_k)$.

Def: Let S be a finite multiset of the objects $a_1, a_2, \cdots, a_n$ $\forall i \in [n]$, there are k_i identical copies of the object a_i.

i.e $S = \{ k_1 a_1, k_2 a_2, \cdots, k_n a_n \}$

A k-permutation of the multiset S is an ordered k-tuple of the objects $a_1, \cdots, a_n$.

A k-combination of the multiset S is a unordered k-tuple of the objects $a_1, \cdots, a_n$.

Th : Let N be a large positive integer and S be a finite multiset of the objects $a_1, \cdots, a_n$
$\forall i \in [n]$, there are N identical copies of the object a_i

i.e $S = \{ Na_1, Na_2, \cdots, Na_n \}$

The number of k-permutations of the multiset S is atmost n^k

Note here $N \gg n$

Proof: We choose a k-permutation of the multiset S say $(x_1, x_2, \cdots, x_k)$. So $\forall j \in [k]$, we can choose x_j is one of $a_1, a_2, \cdots a_n$. Hence by multiplication principle there are at most n^k k-permutations.

Sept 30, 2020 9:30AM

Th: Let S be a finite multiset of the objects $a_1, a_2, \cdots a_n$ and $\forall i \in [n]$ there are k_i identical copies of a_i. i.e

$$S = \{k_1 a_1, k_2 a_2, \cdots\cdots, k_n a_n\}$$

Let $k = k_1 + k_2 + \cdots\cdots + k_n$

Then the number of k-permutations of the multiset S is

$$\frac{k!}{k_1!\, k_2! \cdots k_n!}$$

Proof: Recall that a k-permutation of the multiset S is a k-tuple $(x_1, x_2, \cdots, x_k)$, where $\forall\ i \in [k]$ $x_i \in \{a_1, \cdots, a_n\}$.

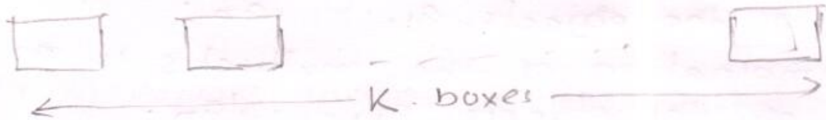
Note that there exist $i_1, i_2, \cdots, i_{k_1} \in [k]$ such that

$$x_{i_1} = x_{i_2} = \cdots = x_{i_{k_1}} = a_1$$

In general, there exist $i_{j_1}, i_{j_2}, \cdots, i_{jk_j} \in [k]$ such that

$$\forall\ j \in [n] \quad x_{i_{j_1}} = x_{i_{j_2}} = \cdots = x_{i_{jk_j}} = a_j$$

We can think of it this way. There are k boxes and we want to put exactly one of the object $a_1, \cdots, a_n$ in each of the boxes



Since there are k_1 identical copies of object a_1, we choose k_1 boxes and fill it with a_1. We can do this in $\binom{k}{k_1}$ ways

Having chosen k_1 boxes, we choose k_2 boxes and fill it with a_2. We can do this in $\binom{k-k_1}{k_2}$ ways.

In genral, having chosen $k_1 + k_2 + \cdots + k_{j-1}$ boxes, we choose k_j boxes and fill it with a_j, where $j \in \{2, 3, \cdots n\}$

We can do this in $\binom{k - k_1 - k_2 \cdots - k_{j-1}}{k_j}$ ways.

Using multiplication principle of counting, we have the no. of k-permutations of the multiset S is

$$\binom{k}{k_1}\binom{k-k_1}{k_2}\binom{k-k_1-k_2}{k_3} \cdots \binom{k-k_1-\cdots-k_{n-1}}{k_n}$$

$$= \frac{k!}{k_1!\, k_2! \cdots k_n!}$$

□

Three-dimensional force microscopy of cells in biopolymer networks

Julian Steinwachs[1], Claus Metzner[1], Kai Skodzek[1], Nadine Lang[1], Ingo Thievessen[1], Christoph Mark[1], Stefan Münster[2], Katerina E Aifantis[3] & Ben Fabry[1]

We describe a technique for the quantitative measurement of cell-generated forces in highly nonlinear three-dimensional biopolymer networks that mimic the physiological situation of living cells. We computed forces of MDA-MB-231 breast carcinoma cells from the measured network deformations around the cells using a finite-element approach based on a constitutive equation that captures the complex mechanical properties of diverse biopolymers such as collagen gels, fibrin gels and Matrigel. Our measurements show that breast carcinoma cells cultured in collagen gels generated nearly constant forces regardless of the collagen concentration and matrix stiffness. Furthermore, time-lapse force measurements showed that these cells migrated in a gliding motion with alternating phases of high and low contractility, elongation, migratory speed and persistence.

The migration of cells through the fibrous network of the extracellular matrix is an integral part of many biological processes, including tissue morphogenesis, wound healing and cancer metastasis[1]. To migrate through the pores of the dense meshwork of the extracellular matrix, cells must generate considerable forces that are exerted on the matrix[2–5]. Accurate measurement of these traction forces is crucial for understanding the invasion of cancer cells or the migration of immune cells in tissue[5,6].

One can estimate traction forces by culturing cells on artificial two-dimensional (2D) or three-dimensional (3D) substrates with known stiffness and measuring the substrate deformations as the cells adhere and migrate[7–11]. Present methods for traction-force reconstruction rely on the linear force-displacement response of the substrate. However, the connective tissues of most organs are highly nonlinear, as are reconstituted tissue equivalents such as collagen and fibrin gels, both of which stiffen strongly under shear[12–14] and collapse with an abnormal apparent Poisson's ratio greater than 1 when stretched[15–18] (**Fig. 1**).

In this report we describe a method for measuring cell traction forces in physiologically relevant 3D biopolymer networks with highly nonlinear mechanical properties. With our method, we studied the contractility, migration and shape changes of breast carcinoma cells in collagen gels with differing concentrations and matrix stiffness. During migration, breast carcinoma cells underwent alternating phases of high and low contractility, elongation, migratory speed and persistence, all of which showed high temporal correlation. On average, these cells did not respond to higher matrix stiffness with greater contractility, which can be partially explained by impaired cell elongation in denser gels.

RESULTS

Macrorheology and constitutive equation for collagen gels

To measure 3D cell traction from the deformation of the surrounding collagen network matrix, we combined existing micromechanical models with a continuum description: on a small spatial scale corresponding to a fiber segment, we considered that the local deformation of the fiber segment does not follow the deformation of the bulk. This so-called non-affine behavior is caused by fiber buckling, straightening or stretching[14,19–24] and gives rise to a pronounced nonlinear stress-strain relationship and collapse of the material under uniaxial stretch (**Fig. 1a**,**b**). Beyond the length scale of the typical interconnection distance, however, the strain of the fiber approximates the macroscopic strain λ (ref. 14), depending on the orientation of the fiber and the applied deformation (equation (2)). We assumed that deformations become affine for a sufficiently large volume of material, and thus we were able to compute the stress-strain response by averaging the force contributions of all fibers contained in such a volume[12] (**Fig. 1c**).

The mechanical properties of collagen fibers can be described by a nonlinear potential function $w(\lambda)$ with stiffness $w''(\lambda)$ that exhibits three distinct regimes (equation (1)). Under compression, the fibers buckle, and the stiffness falls exponentially with a characteristic strain scale d_0. For small extensions, the fibers have a constant stiffness κ_0. If the fibers are stretched beyond the linear strain range λ_s, the stiffness increases exponentially with a characteristic strain scale d_s (**Fig. 1e**). By averaging the stress contributions of many fibers[12], assuming an isotropic and homogeneous distribution (**Supplementary Notes 1–3**), one can derive a constitutive equation (equation (3)) that describes the mechanical behavior of the bulk material.

[1]Department of Physics, University of Erlangen-Nuremberg, Erlangen, Germany. [2]Department of Biological Physics, Max Planck Institute for the Physics of Complex Systems, Dresden, Germany. [3]Department of Civil Engineering and Engineering Mechanics, University of Arizona, Tucson, Arizona, USA. Correspondence should be addressed to J.S. (julian.steinwachs@fau.de).

RECEIVED 25 FEBRUARY; ACCEPTED 19 OCTOBER; PUBLISHED ONLINE 7 DECEMBER 2015; DOI:10.1038/NMETH.3685

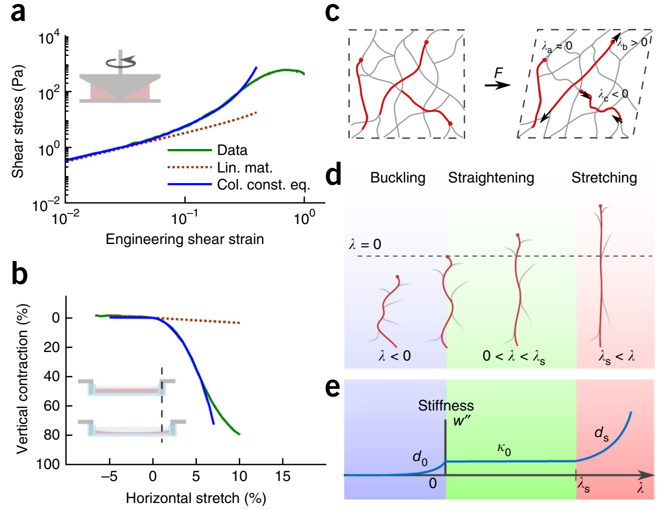


Figure 1 | Macrorheology of collagen type I gels and semi-affine model description. (**a**) Shear stress versus shear strain of a 2.4–mg ml^{-1} collagen gel measured in a cone-plate rheometer (representative of $n = 5$). Lin. mat., predictions from a linear material model; Col. const. eq., predictions from a constitutive equation for collagen gels. (**b**) Vertical contraction and expansion of a 2.4–mg ml^{-1} collagen gel under uniaxial compression and stretch. Lines color-coded according to the key in **a**. (**c**) Non-affine deformations (stretch and compression) of individual collagen fibers, depending on their orientation. (**d**) Fiber buckling under compressional strain ($\lambda < 0$), fiber straightening under small extensional strain ($0 < \lambda < \lambda_s$) and fiber stretching under large extensional strain ($\lambda_s < \lambda$). (**e**) Fiber stiffness versus fiber strain ($w''(\lambda)$) for the same regimes shown in **d**, characterized by an exponential decrease with a characteristic strain scale d_0 for buckling, a constant stiffness κ_0 for small extensional strain and an exponential increase with a characteristic strain scale d_s for large extensional strain.

We determined the four parameters of our constitutive equation (d_0, κ_0, λ_s and d_s) by means of two types of experiments. First, we measured the stress-strain relationship for simple shear deformation in a cone-plate rheometer (**Fig. 1a**). We found a linear regime followed by pronounced strain stiffening beyond a shear of ~3% that was well described by an exponential behavior[13,16,21]. Second, we measured the vertical (z) contraction of collagen gel when it was uniaxially stretched in the x-direction while the strain in the y-direction was fixed at 0% (**Fig. 1b**). Collagen gels exhibited strong vertical contraction under stretch, with a horizontal-to-vertical stretch ratio of ~8 (**Fig. 1b**), indicating an apparent Poisson's ratio considerably greater than 1. Additionally, we measured the horizontal gel dilation under uniaxial compression. The gel expanded only weakly in the vertical direction, revealing the fundamental asymmetry of the material resulting from fiber buckling (**Fig. 1b**).

Our material model (equation (3)) reproduced our experimental data (the strain stiffening, the high apparent Poisson's ratio and the stretch-versus-compression asymmetry) well up to 30% of compression, 30% of shear and 7% of uniaxial stretch (**Fig. 1**). Moreover, measurements of collagen gels with different concentrations (0.6, 1.2 and 2.4 mg ml^{-1}), fibrin gels and Matrigel showed that our material model captured the rheology of these biopolymer networks (**Supplementary Notes 4–8**).

This constitutive equation allowed us to compute the gel deformations and stress in response to arbitrary forces, geometries and boundary conditions using a finite-element approach. For finite-element analysis, we represented the geometry of the gel with a mechanically coupled mesh of simple tetrahedra (**Supplementary Note 2**). Our analysis showed that collagen gels stiffened strongly under dilating forces of cells, resulting in steric hindrance against migration (**Supplementary Note 9**). In contrast, gel stiffening was weak with contracting cell forces. This mechanical behavior of collagen gels led to more efficient migration for elongated cells with polarized tractions (**Supplementary Note 9**).

Experimental validation with point-like forces

To experimentally test the validity of the material model in combination with the finite-element approach, we applied forces of 10–30 nN using 5-µm magnetic beads attached to the surface of a collagen gel in a magnetic-tweezers setup (**Fig. 2a**,**b**). We measured the resulting local gel displacement by tracking fluorescent marker beads in the gel (**Fig. 2c**). Time-lapse recordings of the matrix response showed predominantly elastic behavior with negligible viscosity and plasticity (**Fig. 2** and **Supplementary Note 10**). We then predicted the local gel displacement from the known magnetic forces and the mechanical parameters of the gel as measured with an extensional rheometer (**Fig. 2f–h** and **Supplementary Note 5**). The predicted displacement field overestimated the maximum displacement near the bead but was in good agreement with measurements at distances of more than 50 µm from the point of force application (**Fig. 2g**). In particular, our measurements confirmed the model prediction of a highly asymmetric displacement field. We found that the gel deformed strongly under tension (**Fig. 2**) but not under compression, as compressive stresses propagated poorly owing to fiber buckling. By contrast, the displacement field in a linear material (**Fig. 2h**) was centered on the external force.

In a second test, we reconstructed the applied point-like force of the magnetic bead from the measured collagen displacement field. We minimized the mismatch between the simulated and the measured local gel displacement by adjusting the position, direction and magnitude of the simulated force. The fitted force position, on average, coincided precisely with the centroid of the measured bead position, with an s.d. of 4 µm for different measurements (**Fig. 2d**). The fitted force amplitude was on average 22% higher than the applied magnetic force, with an s.d. of 33% for different measurements (**Fig. 2e**).

Unconstrained 3D force reconstruction

In contrast to the point-like force on a magnetic bead, the spatial distribution of forces around living cells is unknown. Unconstrained force reconstruction does not rely on cell-surface information and makes no prior assumptions about the 3D force field of the cell. This creates a computational problem, as the number of fit parameters (force vectors) is the same as the number of measured data points (displacement vectors). To prevent overfitting, we introduced a regularization approach that allowed cell forces to be present only in a portion of the measured volume. Each node of the finite-element mesh was assigned a weight with which external forces at that node were penalized. When the penalty was iteratively lowered for nodes with high forces, the prevailing cell forces condensed onto a few nodes, and small forces due to uncorrelated measurement noise were minimized

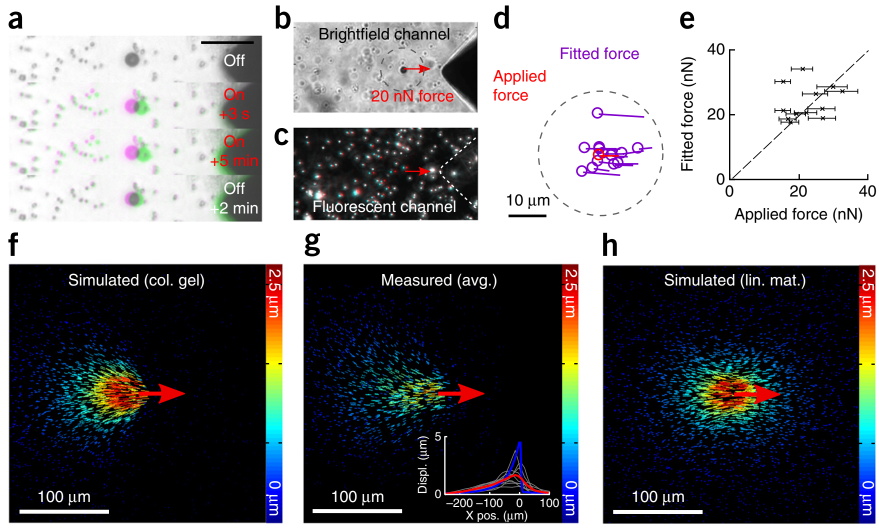


Figure 2 | Experimental validation of the constitutive equation for collagen gels. (**a**) Image recordings (representative of 13 measurements) of the magnetic bead, small fiducial marker beads and the magnetic needle tip during force application at different time points (in green) overlaid with an image of the unstrained configuration (in magenta). Colors from fiducial markers that did not move grade to black. Scale bar, 20 µm. (**b**) Brightfield image of the magnetic-tweezers experiment. The dashed circle corresponds to the dashed circle in **d**. (**c**) Overlay of fluorescent images of the marker beads before (cyan) and after (red) a force of 20 nN was applied to the beads. Red arrow indicates the direction of the applied force as in **b**. (**d**) Reconstructed forces (position, direction and magnitude) of magnetic beads from 13 independent measurements. The length of the lines is normalized to the magnitude of the known applied force (red). The dashed circle corresponds to the dashed circle in **b**. (**e**) Reconstructed force magnitude versus applied force magnitude. Horizontal error bars indicate the error (r.m.s.) in the applied force due to variations in bead size. (**f**) Simulated displacement around a point-like force of 20 nN. Col. gel., collagen gel. (**g**) Measured displacement around a point-like force of 20 nN averaged (avg.) over 13 measurements. Inset shows the local matrix displacements (Displ.) along the *x*-axis through the point of force application (at $x = 0$). Simulated displacements are shown in blue, individual measurements from different beads are in gray, and the average is in red. Pos., position. (**h**) Simulated displacements around a point-like force of 20 nN for a linear material (lin. mat.).

in the rest of the volume. The strength of the regularization was controlled by the parameter α. By running unconstrained force reconstruction on the above-described data set of matrix displacements around a point-like force, we found that the total force (the vector sum of all forces around the magnetic bead) depended little on α for values less than 0.3 pN^2 µm^{-2} (**Supplementary Note 11**). The systematic force error was less than 1% with an s.d. of 30% between individual measurements. When averaged over many beads, however, the reconstructed forces appeared blurred and were systematically shifted 30 µm away from the direction of force application (Discussion).

Traction forces of living cells

To measure the force-induced deformation of a collagen gel, we imaged the collagen network around the cells with confocal reflection microscopy before and after force relaxation with cytochalasin D and evaluated the local displacement field via 3D particle image velocimetry (**Fig. 3** and **Supplementary Note 12**). Unconstrained reconstructed cellular forces were localized near but not exactly on the surfaces of cells (**Fig. 3b,c**). To quantify this error, we projected the cellular force together with brightfield images of a given cell onto the *x*-*y* plane and plotted the average force density versus the distance to the cell edge. Forces were systematically shifted away from the cell edge by approximately 18 µm (**Fig. 3f**) (see Discussion).

In addition to cell forces, our model allowed us to compute the principal matrix stress (**Fig. 3d**) and the principal matrix stiffness (**Fig. 3e**). Both tended toward zero in the region of the cell where the material was compressed and the fibers buckled, in essence creating a hole where the contracting cell was located. This suggests that cell forces are used almost exclusively to pull collagen fibers centripetally toward the cell. Therefore, our approach describing cellular forces as a 3D force field in a

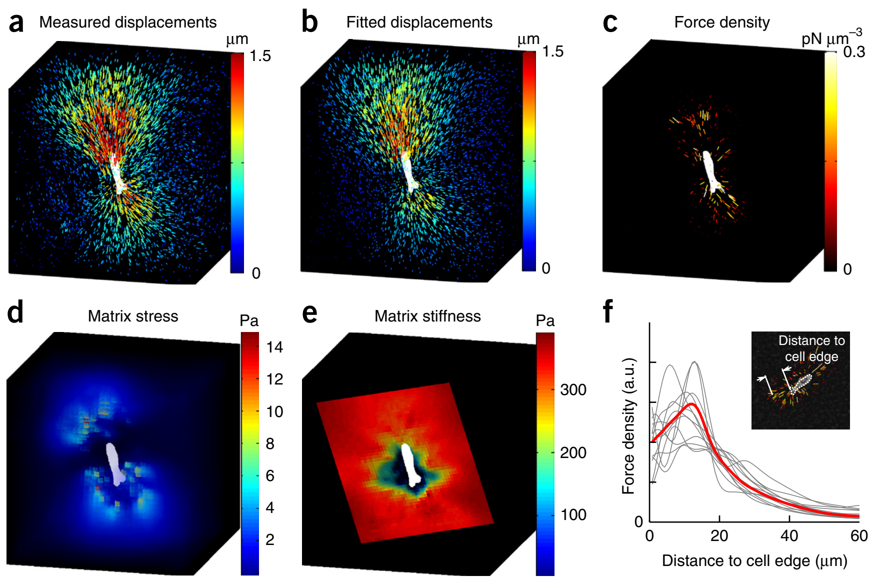


Figure 3 | Reconstruction of cellular forces inside a 1.2–mg ml^{-1} collagen gel. (**a**) Measured displacements around a single MDA-MB-231 breast carcinoma cell. (**b**) Regularized displacement field around the cell in **a**. (**c**) Force density around the cell in **a** and **b** as calculated from the regularized displacements shown in **b**. (**d**) Principal matrix stress as calculated from the regularized displacement field. (**e**) Principal matrix stiffness as calculated from the regularized displacement field. (**f**) Reconstructed force density in arbitrary units (a.u.) around individual cells ($n = 12$; gray curves) as a function of the distance to the cell edge as illustrated in the inset. The average force density is shown in red.

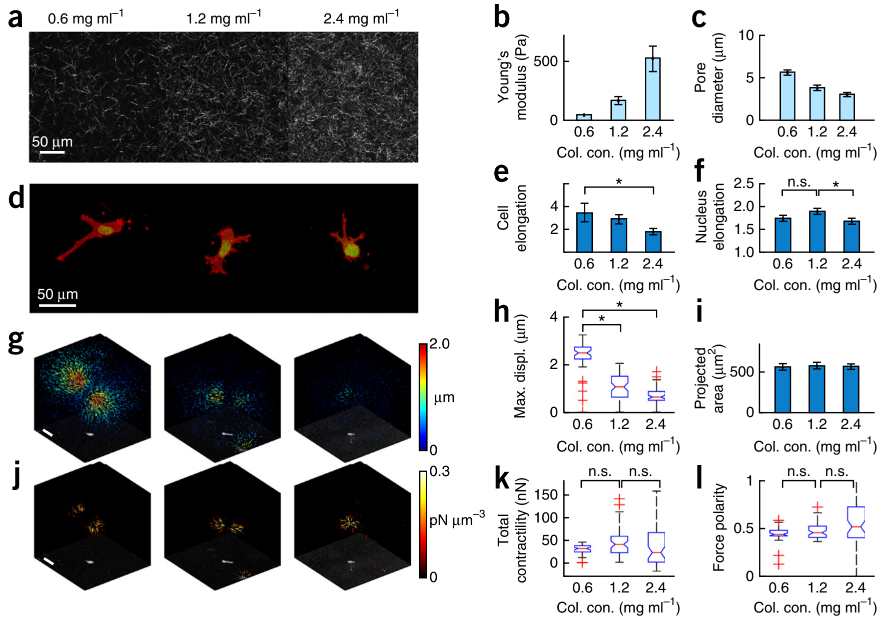


Figure 4 | Contractility of MDA-MB-231 cells in gels with different collagen concentrations. (**a**) Collagen fiber network imaged using confocal reflection microscopy. (**b**,**c**) Linear Young's modulus of collagen gels (**b**) and pore diameter of the network (**c**). (**d**) Morphology of cells (actin in red, chromatin in green) embedded in collagen gel. (**e**,**f**) Cell elongation (**e**) and elongation of the nucleus (**f**) in cells embedded in collagen gel. (**g**) 3D matrix displacement fields of the collagen gel around embedded cells. Density and hue of marks indicate the magnitude of the local displacement vector. (**h**) Maximum cell-induced matrix displacement (Max. displ.). (**i**) Projected area of cells embedded in collagen gel. (**j**) 3D force density of cells embedded in collagen gels. Density and color intensity of marks are proportional to the local force density. Scale bars in **g**,**j**, 50 µm. (**k**,**l**) Total contractility (**k**) and force polarity (**l**) of cells in collagen gel. For all box plots, the central (red) mark indicates the median, the edges of the box denote the 25th and 75th percentiles, the whiskers extend to the most extreme data points not considered outliers, and outliers are plotted individually (red crosses). Notches indicate s.e. $*P \leq 0.05$, Student's t-test assuming unequal variances including the outliers. Col. con., collagen concentration; n.s., not significant ($P > 0.05$).

continuous material, without a 'hole' to accommodate the cell, does not lead to force overestimation[11].

As a measure of cell contractility, we quantified the total magnitude of the projected force vectors pointing toward the cell center (**Supplementary Note 13**). From a data set of 63 MDA-MB-231 cells in a 1.2–mg ml^{-1} collagen gel, we measured a total contractility of 47.6 ± 3.4 nN (geometric mean ± s.e.m.). The total contractility for the same cell line grown on a planar collagen-coated polyacrylamide substrate (Young's modulus: 5 kPa) has been reported[25,26] as ~270 nN.

To quantify the geometry of the 3D cellular force fields, we decomposed the contractile force into force contributions from three principal components of an orthogonal coordinate system aligned with the force field of the cell (**Supplementary Note 13**). For a force dipole, the force polarity approaches 1, whereas for an isotropic force field, the force polarity approaches 1/3. The force polarity of MDA-MB-231 cells was 0.47 ± 0.01 (mean ± s.e.m., n = 63), indicating that about half of the total contractility could be expressed by a single force dipole.

Contractile cell forces contribute to the strain stiffening of a collagen matrix surrounding cells. To quantify this, we computed for every cell the mechanical work needed to achieve a small additional matrix deformation. MDA-MB-231 cells stiffened the bulk of the collagen gel on average by 3.2% ± 0.5% (mean ± s.e.m.), in agreement with numerical simulations that also indicated little strain stiffening of the bulk of the collagen matrix around contractile cells (**Supplementary Note 9**). In contrast, the collagen matrix showed a pronounced stiffening response to dilatational forces that occur when a cell is attempting to squeeze through a narrow pore (**Supplementary Note 9**).

Constrained 3D force reconstruction

Unconstrained force reconstruction can robustly resolve total cell contractility down to 5 nN for displacement noise levels in excess of 200 nm, but the method has limited localization accuracy (**Fig. 3f** and **Supplementary Notes 14–17**). To avoid the systematic shift and blurring of the reconstructed forces, one can constrain their localization to the cell surface. To demonstrate this, we fluorescently stained the cytoplasm of HT1080 fibrosarcoma cells, imaged the cells with confocal microscopy, and segmented them by thresholding. We assigned a zero-penalty weight to nodes of finite elements with a distance to the cell surface of less than half the mesh size; the remaining computation was identical to the unconstrained method. The force localization of the constrained method was superior to that of the unconstrained method (**Supplementary Note 18**), but both methods gave similar values for the total contractility and force polarity.

Traction forces in gels of varying collagen concentration

To study how cells respond to changes in matrix stiffness and density, we measured traction forces of MDA-MB-231 cells embedded in collagen gels with different concentrations (0.6 (n = 48), 1.2 (n = 63) and 2.4 mg ml^{-1} (n = 64)) where the linear stiffness increased from 44 Pa to 513 Pa and the average pore diameter decreased from 5.6 µm to 3.0 µm (**Fig. 4a–c**)[27]. Fluorescent staining of the actin cytoskeleton showed that cells in the denser gels were more rounded and had smaller and thinner protrusions than cells in gels with lower collagen concentrations (**Fig. 4d–f**). However, the projected cell area in these different gels, and therefore the cell volume, was the same. Matrix deformations induced by the cells decreased with increasing collagen concentration (**Fig. 4g–i**), but the total cell contractility, measured using unconstrained force reconstruction, remained the same, as did the force polarity (**Fig. 4j–l** and **Supplementary Note 19**).

Time-lapse force microscopy

Reflection microscopy minimizes photodamage and allows for long-term measurements (>24 h) of migration trajectories, cell morphology and traction forces (**Supplementary Videos 1** and **2**). To investigate the coordination of traction forces during cell migration

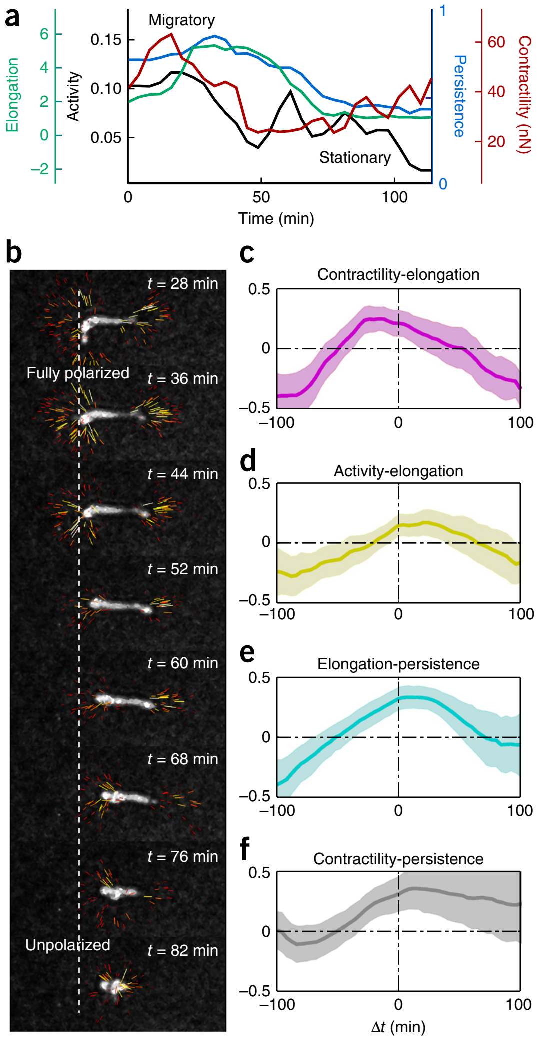


Figure 5 | Time-lapse force microscopy of a breast carcinoma cell inside collagen gel. (**a**) Time course of contractility, elongation, migratory activity and migratory persistence of an MDA-MB-231 breast carcinoma cell embedded in a 3D collagen gel (1.2 mg ml^{-1}). (**b**) Force field of the cell shown in **a**. (**c**–**f**) Cross-correlation of force fluctuations, cell morphology and migration parameters for different time lags averaged over 20 cells. (**c**) Contractility versus elongation. (**d**) Activity versus elongation. (**e**) Elongation versus persistence. (**f**) Contractility versus persistence. Shaded area around curves indicates ±1 s.e.

through a disordered 3D collagen matrix, we simultaneously measured the time course of contractility, cell elongation, migration persistence p and migration activity a (calculated from the momentary cell speed v according to $a = v(1 - p^2)^{0.5}$ (**Fig. 5a**,**b**)[28]. We found that for MDA-MB-231 cells, all four parameters were significantly correlated for time lags between 0 and ±15 min (**Fig. 5c**–**f** and **Supplementary Note 20**). This implies that phases of rapid cell movements with high persistence and activity were accompanied by large contractile forces and pronounced cell elongation. Conversely, phases during which the cells remained stationary were accompanied by small contractile forces and more rounded cell shapes. For lag times greater than ±1 h, the correlations between these parameters were negative, implying that migratory phases lasted for approximately 1 h. Moreover, phases of high contractility were accompanied by further cell lengthening (**Supplementary Note 20**).

DISCUSSION

Our underlying assumption of the biopolymer network as a mechanical continuum is violated at the scale of individual fibers or single network pores. Therefore, the spatial resolution of the reconstructed forces is limited by the length scale at which the continuum assumption breaks down. Accordingly, we attribute the variability and positional errors in reconstructed forces in the magnetic bead experiments (**Fig. 2g**) to local heterogeneity in the fiber structure of the gels (density, fiber orientation, fiber thickness and connectivity) as described previously[29]. The spatial resolution of the reconstructed force is therefore limited to around 30 μm (**Supplementary Note 11**). Further, blurring of the reconstructed forces is caused by the size of the finite elements, the presence of measurement noise and the necessary regularization (**Supplementary Note 14**). Finally, collagen fibers under compression can bear only little mechanical stress, and therefore all discrepancies between the continuum model and the real situation of an inhomogeneous collagen gel must be reconciled by forces that arise in the tensed region of the collagen gel. If confocal image stacks of fluorescently labeled cells are available, one can avoid this problem by restricting the reconstructed forces to the cell surface (**Supplementary Note 18**).

Our statistical force fluctuations of 30% due to measurement errors are considerably smaller than the >50% fluctuations in the total force magnitude between individual cells (**Fig. 4k**). Therefore, our measurement error does not markedly degrade the quality of the data or require the measurement of a considerably larger number of cells for statistical significance. **Table 1** summarizes the sensitivity, accuracy and spatial resolution of the constrained and unconstrained 3D force reconstruction methods.

Our finding of constant traction forces for collagen gels of different densities and stiffness is in contrast to cell behavior on planar substrates, where cell tractions increase with higher substrate stiffness and with increasing ligand density[30–32]. A possible explanation that reconciles these conflicting findings is that a smaller pore size in the denser and stiffer 3D matrices may impede cell elongation and the formation of cell protrusions, and hence may reduce force generation. In support of this hypothesis, we found that the contractility of a subpopulation of elongated cells with an aspect ratio greater than 2.0 was significantly ($P < 0.05$, Student's two-tailed t-test assuming unequal variances) greater in 1.2 mg ml^{-1} collagen gels than in 0.6 mg ml^{-1} collagen gels (**Supplementary Note 21**).

Our method can be used to study the dynamics of cell migration in a 3D environment. We noted that untreated MDA-MB-231 cells alternated between highly migratory and more stationary phases. During migratory phases cells had an elongated shape and high contractility. The cross-correlation between these parameters was highest for a time lag of zero. Thus we found no evidence that phases of elongation, contraction and motility

Table 1 | Sensitivity, accuracy (error) and spatial resolution of 3D force reconstruction

	Unconstrained	Constrained
Sensitivity	5 nN[a]	5 nN[a]
Error (relative bias ± s.d.)	<1% ± 30%[b]	+22% ± 33%[b]
Spatial resolution (bias ± s.d.)	30 μm ± 30 μm[b,c]	0 μm ± 4 μm[b]

[a]For a 384-Pa (Young's modulus) collagen gel and 60-nm spatial resolution of local gel displacement. [b]For a point force of 10–30 nN. [c]Spatial bias is in the force direction.

are shifted relative to one another, as one would expect with an 'inchworm' type of motion in which contraction leads to cell shortening and force relaxation leads to cell lengthening. Rather, during the migratory phases, MDA-MB-231 cells seemed to glide through the gel in a steady process of simultaneous adhesion and de-adhesion.

These results demonstrate that our 3D traction force microscopy method can contribute to understanding of the physical mechanisms of cell migration in physiologically relevant environments.

METHODS

Methods and any associated references are available in the online version of the paper.

Note: Any Supplementary Information and Source Data files are available in the online version of the paper.

ACKNOWLEDGMENTS
We thank J.P. Butler (Harvard University) for helpful discussions and for developing a method to locate the force epicenter from a 3D vector field, and we thank P. Strissel (University Clinics Erlangen) for help with Matrigel experiments. We acknowledge E. Wagena (Radboud University Nijmegen) for generating dual-color HT1080 fibrosarcoma cells, which were a gift from K. Wolf (Radboud University Nijmegen, the Netherlands). This work was supported by the German Research Foundation (DFG) Research Training Group 1962 "Dynamic Interactions at Biological Membranes: From Single Molecules to Tissue," the US National Institutes of Health (NIH-HL65960) and the Emerging Fields Initiative of the University of Erlangen–Nuremberg.

AUTHOR CONTRIBUTIONS
J.S., B.F., S.M., I.T., N.L. and K.S. designed the setup and performed the experiments; J.S., C. Metzner and K.E.A. developed the material model and mathematical tools; J.S., C. Metzner and C. Mark wrote the data-acquisition and analysis software; J.S., S.M. and B.F. wrote the article.

COMPETING FINANCIAL INTERESTS
The authors declare no competing financial interests.

1. Friedl, P., Zanker, K.S. & Brocker, E.B. Cell migration strategies in 3-D extracellular matrix: differences in morphology, cell matrix interactions, and integrin function. *Microsc. Res. Tech.* **43**, 369–378 (1998).
2. Zaman, M.H. *et al.* Migration of tumor cells in 3D matrices is governed by matrix stiffness along with cell-matrix adhesion and proteolysis. *Proc. Natl. Acad. Sci. USA* **103**, 10889–10894 (2006).
3. Friedl, P. & Wolf, K. Proteolytic interstitial cell migration: a five-step process. *Cancer Metastasis Rev.* **28**, 129–135 (2009).
4. Friedl, P., Wolf, K. & Lammerding, J. Nuclear mechanics during cell migration. *Curr. Opin. Cell Biol.* **23**, 55–64 (2011).
5. Koch, T.M., Muenster, S., Bonakdar, N., Buttler, J.P. & Fabry, B. 3D traction forces in cancer cell invasion. *PLoS ONE* **7**, e33476 (2012).
6. Lämmermann, T. *et al.* Rapid leukocyte migration by integrin-independent flowing and squeezing. *Nature* **453**, 51–55 (2008).
7. Dembo, M. & Wang, Y.L. Stresses at the cell-to-substrate interface during locomotion of fibroblasts. *Biophys. J.* **76**, 2307–2316 (1999).
8. Butler, J.P., Tolic-Norrelykke, I.M., Fabry, B. & Fredberg, J.J. Traction fields, moments, and strain energy that cells exert on their surroundings. *Am. J. Physiol. Cell Physiol.* **282**, C595–C605 (2002).
9. Sabass, B., Gardel, M.L., Waterman, C.M. & Schwarz, U.S. High resolution traction force microscopy based on experimental and computational advances. *Biophys. J.* **94**, 207–220 (2008).
10. Legant, W.R. *et al.* Multidimensional traction force microscopy reveals out-of-plane rotational moments about focal adhesions. *Proc. Natl. Acad. Sci. USA* **110**, 881–886 (2013).
11. Legant, W.R. *et al.* Measurement of mechanical tractions exerted by cells in three-dimensional matrices. *Nat. Methods* **7**, 969–971 (2010).
12. Storm, C., Pastore, J.J., MacKintosh, F.C., Lubensky, T.C. & Janmey, P.A. Nonlinear elasticity in biological gels. *Nature* **435**, 191–194 (2005).
13. Arevalo, R.C., Urbach, J.S. & Blair, D.L. Size-dependent rheology of type-I collagen networks. *Biophys. J.* **99**, L65–L67 (2010).
14. Münster, S. *et al.* Strain history dependence of the nonlinear stress response of fibrin and collagen networks. *Proc. Natl. Acad. Sci. USA* **110**, 12197–12202 (2013).
15. Voytik-Harbin, S.L., Roeder, B.A., Sturgis, J.E., Kokini, K. & Robinson, J.P. Simultaneous mechanical loading and confocal reflection microscopy for three-dimensional microbiomechanical analysis of biomaterials and tissue constructs. *Microsc. Microanal.* **9**, 74–85 (2003).
16. Vader, D., Kabla, A., Weitz, D. & Mahadevan, L. Strain-induced alignment in collagen gels. *PLoS ONE* **4**, e5902 (2009).
17. Roeder, B.A., Kokini, K. & Voytik-Harbin, S.L. Fibril microstructure affects strain transmission within collagen extracellular matrices. *J. Biomech. Eng.* **131**, 031004 (2009).
18. Brown, A.E., Litvinov, R.I., Discher, D.E., Purohit, P.K. & Weisel, J.W. Multiscale mechanics of fibrin polymer: gel stretching with protein unfolding and loss of water. *Science* **325**, 741–744 (2009).
19. Onck, P.R., Koeman, T., van Dillen, T. & van der Giessen, E. Alternative explanation of stiffening in cross-linked semiflexible networks. *Phys. Rev. Lett.* **95**, 178102 (2005).
20. Heussinger, C., Schaefer, B. & Frey, E. Nonaffine rubber elasticity for stiff polymer networks. *Phys. Rev. E* **76**, 031906 (2007).
21. Stein, A.M., Vader, D.A., Weitz, D.A. & Sander, L.M. The micromechanics of three-dimensional collagen-I gels. *Complexity* **16**, 22–28 (2011).
22. Sheinman, M., Broedersz, C.P. & MacKintosh, F.C. Nonlinear effective-medium theory of disordered spring networks. *Phys. Rev. E* **85**, 021801 (2012).
23. Stylianopoulos, T. & Barocas, V.H. Volume-averaging theory for the study of the mechanics of collagen networks. *Comput. Methods Appl. Mech. Eng.* **196**, 2981–2990 (2007).
24. Licup, A.J. *et al.* Stress controls the mechanics of collagen networks. *Proc. Natl. Acad. Sci. USA* **112**, 9573–9578 (2015).
25. Kraning-Rush, C.M., Carey, S.P., Califano, J.P., Smith, B.N. & Reinhart-King, C.A. The role of the cytoskeleton in cellular force generation in 2D and 3D environments. *Phys. Biol.* **8**, 015009 (2011).
26. Lautscham, L.A. *et al.* Migration in confined 3D environments is determined by a combination of adhesiveness, nuclear volume, contractility, and cell stiffness. *Biophys. J.* **109**, 900–913 (2015).
27. Lang, N.R. *et al.* Estimating the 3D pore size distribution of biopolymer networks from directionally biased data. *Biophys. J.* **105**, 1967–1975 (2013).
28. Metzner, C. *et al.* Superstatistical analysis and modelling of heterogeneous random walks. *Nat. Commun.* **6**, 7516 (2015).
29. Mickel, W. *et al.* Robust pore size analysis of filamentous networks from 3D confocal microscopy. *Biophys. J.* **95**, 6072–6080 (2008).
30. Pelham, R.J. Jr. & Wang, Y. Cell locomotion and focal adhesions are regulated by substrate flexibility. *Proc. Natl. Acad. Sci. USA* **94**, 13661–13665 (1997).
31. Engler, A. *et al.* Substrate compliance versus ligand density in cell on gel responses. *Biophys. J.* **86**, 617–628 (2004).
32. Reinhart-King, C.A., Dembo, M. & Hammer, D.A. The dynamics and mechanics of endothelial cell spreading. *Biophys. J.* **89**, 676–689 (2005).

ONLINE METHODS

Biopolymer gel synthesis. We mixed rat tail collagen (Collagen R, 2 mg/ml, Matrix Bioscience, Berlin, Germany) and bovine skin collagen (Collagen G, 4 mg/ml, Matrix Bioscience) at a ratio of 1:1. We then added 10% (vol/vol) sodium bicarbonate (23 mg/ml) and 10% (vol/vol) 10× DMEM (Gibco). We adjusted the solution to pH 10 with 43 μl of 1 M NaOH and polymerized it at 37 °C, 95% humidity and 5% CO_2 for 1 h. For final collagen concentrations of 1.2 mg/ml and 0.6 mg/ml, we diluted the solution before polymerization with a mixture of 1 volume part $NaHCO_3$, 1 part 10× DMEM and 8 parts H_2O. We polymerized fibrin gels with a final concentration of 4.0 mg/ml human fibrinogen after mixing with 0.05 NIH units/ml human α-thrombin (both from Haemochrome Diagnostics) in buffer containing 0.15 M NaCl, 20 mM CaCl, 25 mM HEPES at pH 7.4 for 1 h at room temperature. We polymerized Matrigel (BD Bioscience) at a concentration of 10 mg/ml (undiluted) at 37 °C, 5% CO_2 and 95% relative humidity for 1 h.

Mechanical description of collagen gels. We assumed that the collagen network deforms in an affine way beyond a certain length scale, and that below that scale, individual fiber segments deform in a non-affine way and evade mechanical stress using their internal degrees of freedom (**Fig. 1d**). This can be described by a nonlinear and asymmetric energy potential function $w(\lambda) = w(\Delta l/l)$ of the fibers. The potential function $w(\lambda)$ of individual collagen fibers is expected to exhibit three distinct regimes: buckling, straightening and stretching. The differential fiber stiffness $w''(\lambda)$ can thus be described with only four parameters: (i) a buckling coefficient d_0 describing an exponential decrease in fiber stiffness under compression, (ii) linear stiffness κ_0, (iii) critical strain for the onset of strain stiffening λ_s and (iv) an exponential strain stiffening coefficient d_s (**Fig. 1d,e**).

$$w''(\lambda) = \kappa_0 \begin{cases} e^{\lambda/d_0} & \forall \lambda < 0 \\ 1 & \forall 0 < \lambda < \lambda_s \\ e^{(\lambda - \lambda_s)/d_s} & \forall \lambda_s < \lambda \end{cases} \tag{1}$$

With a mean field approach, the deformation λ of a fiber is defined by the change in length Δl relative to the fiber's end-to-end distance in the unstressed state, $\lambda = \Delta l/l$. The value of λ is determined by the fiber displacement field $\vec{U}$ and the local average deformation field $F = \text{grad}\,\vec{U}$ according to

$$\lambda = |F\vec{e}_\Omega| - 1 \tag{2}$$

with unit vector $\vec{e}_\Omega$ pointing in the direction of the fiber orientation Ω. The mechanical stress of the fiber is then

$$w'(\lambda) = \int_0^\lambda w''(\lambda) d\lambda$$

Integration from zero implies that the material has no pre-stress. One can derive a constitutive equation that relates the nominal stress tensor N to the deformation field F by averaging the stress contributions of many fibers, assuming an isotropic and homogeneous distribution[12] (**Supplementary Note 2**).

$$N_{ij} = \left\langle w'(|F\vec{e}_\Omega| - 1) \frac{(F\vec{e}_\Omega)_i \cdot (\vec{e}_\Omega)_j}{|F\vec{e}_\Omega|} \right\rangle_\Omega \tag{3}$$

Rheometer experiment. We used a cone-plate rheometer to measure the stress-strain relationship of collagen gels for simple shear deformation. The collagen was polymerized inside the rheometer setup. The cone-plate rheometer applied a simple shear deformation such that the strain energy density depended only on the engineering shear strain. We obtained the linear stiffness κ_0, the stiffening coefficient d_s and the characteristic strain λ_s at the onset of stiffening by minimizing the error between the measured and computed stress-strain relationships (**Supplementary Note 4**).

Uniaxial stretch experiment. We cast collagen gel, fibrin gel or Matrigel into a flexible polydimethylsiloxane dish with a sulfo-SANPAH (sulfosuccinimidyl 6-(4′-azido-2′-nitrophenylamino) hexanoate) activated surface. After polymerization, the gel in the dish was stretched uniaxially at a rate of 6% per hour with a stepper-motor device[33], and the height of the gel as a function of applied stretch was measured with a microscope[34]. We fit the buckling coefficient d_0 of our constitutive equation (equation (3)) to best match the measured relationship of vertical versus horizontal strain. We took the other three material parameters of the constitutive equation from the shear rheometer experiment (**Supplementary Note 4**) in the case of collagen and from extensional rheometer experiments in the cases of fibrin and Matrigel.

The vertical contraction of a gel under horizontal stretching can be converted to an apparent Poisson's ratio, which in the case of collagen is considerably greater than 1. According to linear elastic theory, a Poisson's ratio of >0.5 leads to a negative bulk modulus, implying that the undeformed configuration of the material is unstable. The Poisson's ratio of a hydrogel, however, is that of the composite material, which in the case of a collagen gel consists of collagen fibers and water. When a collagen gel is stretched, water can be released. Moreover, the apparent Poisson's ratio of a collagen gel is highly asymmetric and nonlinear. For compression, the apparent Poisson's ratio is much less than 0.5 (**Fig. 1b**).

Extensional rheometer. For measuring the stress-strain relationship under uniaxial stretch, a cylinder of collagen, fibrin or Matrigel was cast between two parallel plates (diameter, 5 cm; gap, 3 mm) (**Fig. 2a**). The lower plate was connected to a precision scale (AND GR-200), and the upper plate was mounted on a motorized micromanipulator (Eppendorf Injectman). The gel was extended at a rate of 10 μm/s, and the weight was continuously recorded. The force-extension curve of the gel was corrected for the mechanical compliance of the device. The stress-strain relationship was computed from the corrected force-extension curve and the known geometry of the gel cylinder. The material parameters were then obtained as described for the shear rheometer experiment (**Supplementary Note 4**).

Finite-element method. To solve the constitutive equation (equation (3)) for arbitrary geometries and boundary conditions, we used a finite-element method in which the material was represented by a mesh of mechanically coupled tetrahedra. Given a set of displacements of the nodes (cornerpoints of the tetrahedra), we calculated the nodal forces as the derivative of the total strain energy of the material by the displacements of the respective nodes (**Supplementary Note 2**). In the case of a point-like force applied to the surface of a gel, the mesh also included the free top surface. All other boundaries were fixed. The considered gel region around a cell was larger than 480 µm.

Magnetic-tweezers experiment. We measured the material displacement field in response to a point-like force at the surface by applying a lateral force of 10–30 nN to a superparamagnetic bead (Microparticles Berlin, Germany; diameter, 5 µm) with magnetic tweezers[5,35]. The gel was decorated with 1-µm fluorescent beads (FluoSpheres, Molecular Probes) that served as fiducial markers. A stack of images around the magnetic bead was acquired before and 10 min after the onset of force application. The displacement of each fluorescent marker was then obtained from the image data as described in ref. 5. The measured displacements were interpolated to a regular finite-element mesh with a grid constant of 7.5 µm in the case of unconstrained force reconstruction, or to an irregular mesh with increasing mesh density near the magnetic bead in the case of constrained (point-like) force reconstruction. The coefficient of variation (CV) of the bead radius was ~5% as stated by the manufacturer, which led to an error (CV) of the applied force of 15%.

Constrained force reconstruction through direct fitting. Given a set of measured displacements of fluorescent markers inside a gel, we minimized the mismatch between the simulated and the measured gel displacements by shifting the location of force application in the simulation, as well as by adjusting the force amplitude and direction. The simulated displacement fields were calculated for a discrete set of force amplitudes and were linearly interpolated between these discrete solutions. The simulated displacement field was shifted, rotated and interpolated onto the positions of the fluorescent markers for which the displacement was measured. We then minimized the least-square error by randomly varying the shift, rotation and amplitude parameters until convergence was reached.

Cell culture. Cells were cultured in 25-cm^2 flasks without surface coating in DMEM (1 g/l D-glucose) with 10% FBS, 1% penicillin and streptomycin at 37 °C, 5% CO_2 and 95% humidity. Cells were passaged every 3 d. Trypsin-EDTA was used to detach cells. Cells were mixed with collagen solution before polymerization at a concentration of 15,000 cells/ml and incubated for 12 h before experiments. MDA-MB-231 breast carcinoma cells were obtained from ATTC; dual-color H2B-GFP/cytoplasmic TagRFP HT1080 fibrosarcoma cells were a gift from Katarina Wolf and were generated by Esther Wagena (Radboud University Nijmegen). All cell lines were checked with a mycoplasma PCR detection kit (Minerva Biolabs).

Fiber-pattern matching. To measure the displacement field of the matrix surrounding the cells, we imaged the collagen network directly using confocal reflection microscopy (Leica SP5X, 20× dip-in water-immersion objective (numerical aperture (NA) 1.0)). Confocal reflection microscopy needs only low laser intensities and prevents photodamage of the cells. From two stacks of confocal reflection images (voxel size of 0.72 µm in all dimensions, field of view of 370 µm in all dimensions) that were taken before and after cell force relaxation with cytochalasin D, we obtained the cell-induced deformation field over a regular grid with a 7.5-µm mesh size by particle image velocimetry as follows. The algorithm we used calculated the cross-correlation between corresponding local sections (12 × 12 × 12 voxels) of the two stacks. It then shifted the section of the first stack by subvoxel increments using trilinear interpolation. This shift corresponded to a displacement vector. To find the local displacement with the highest cross-correlation, we used the downhill simplex method[36]. The accuracy of the deformation measurements was 60 nm (r.m.s.) (**Supplementary Note 12**). For 1.2-mg/ml gels with an average pore size of 3.8 µm, the optimal mesh size of the gel subvolumes used for cross-correlation, and thus the spatial resolution of the algorithm, was 7.5 µm (**Supplementary Note 12**).

Force reconstruction. We reconstructed the 3D force field (force per volume) inside a continuous material, assuming that cellular forces could exist everywhere inside the considered volume. This left us with a computational problem, as the number of fitted parameters (force vectors) equaled the number of data points (measured displacement vectors). We therefore used a regularization method. We performed regularization by minimizing a target function ($\underline{u}$) that was the sum of the ordinary least-square displacement error and a locally weighted norm of the nodal forces.

$$L(\underline{u}) = \left\| \underline{u} - \underline{u}_{\text{measured}} \right\|^2_{\underline{\underline{P}}} + \left\| \underline{f}(\underline{u}) \right\|^2_{\underline{\underline{A}}}$$

where $\|\underline{x}\|^2_{\underline{\underline{Q}}}$ denotes $\underline{x}^T \underline{\underline{Q}}\,\underline{x}$. The diagonal matrix $\underline{\underline{P}}$ has a value of 1 if the displacement of the corresponding node is known and a value of 0 if the displacement reconstruction algorithm is not able to measure the local displacement, or if the corresponding node lies outside of the imaged section. The matrix $\underline{\underline{A}}$ is a diagonal matrix containing the local penalty weights. If $\underline{\underline{A}}$ is proportional to the identity matrix (this corresponds to the Tikhonov regularization method), all nodal forces are penalized and therefore underestimated. To address this issue, we used the maximum-likelihood regression method, which iteratively assigns a lower penalty weight to nodes that have a high force[37].

$$A_{ii} = \begin{cases} \alpha, |f_i| < 1.345 \cdot \mathit{median}\,(|\underline{f}|) \\ \dfrac{\alpha \cdot 1.345 \cdot \text{median}\,(|\underline{f}|)}{|f_i|}, |f_i| > 1.345 \cdot \mathit{median}\,(|\underline{f}|) \end{cases}$$

This procedure reliably penalizes forces due to uncorrelated displacement noise but not cell forces, which are accompanied by long-ranging and correlated displacements. Thus, the algorithm finds the cell forces in an unconstrained manner. It is also possible to constrain the forces to the surface of the cell by predefining low or zero values for the local-penalty-weight matrix $\underline{\underline{A}}$ at specific points corresponding to the cell surface (**Supplementary Note 18**).

The locally weighted norm of the nodal forces, $\left\| \underline{f}(\underline{u}) \right\|^2_{\underline{\underline{A}}}$, is nonlinear in $\underline{u}$, and therefore $L(\underline{u})$ cannot be easily minimized. We expanded $\underline{f}(\underline{u})$ as a first-order Taylor series for nodal displacements $\underline{u} + \underline{\Delta u}$ (**Supplementary Note 9**), using the stiffness tensor K (**Supplementary Note 3**).

$$L(\underline{u} + \underline{\Delta u}) = \left\| \underline{u} + \underline{\Delta u} - \underline{u}_{\text{measured}} \right\|^2_{\underline{\underline{P}}} + \left\| \underline{f_u} + \underline{\underline{K_u}} \cdot \underline{\Delta u} \right\|^2_{\underline{\underline{A}}}$$

doi:10.1038/nmeth.3685

To find the value of $\underline{\Delta u}$ that minimized this expression, we solved the following equation using the conjugate gradient method[38]:

$$(\underline{\underline{P}} + \underline{\underline{K_u}} \cdot \underline{\underline{A}} \cdot \underline{\underline{K_u}}) \cdot \underline{\Delta u} = \underline{\underline{P}} \cdot (\underline{u_{\text{measured}}} - \underline{u}) - \underline{\underline{K_u}} \cdot \underline{\underline{A}} \cdot \underline{f_u}$$

We then added $\underline{\Delta u}$ to the estimated nodal displacements $\underline{u}$ and updated the Taylor coefficients $\underline{f_u}$ and $\underline{\underline{K_u}}$ and the local weight matrix $\underline{\underline{A}}$ for the next iteration until convergence was reached.

To compute the total contractility of a cell without bias caused by noise forces from regions outside the cell, we computed for every node $\vec{r_n}$ of the gel the contractile force C_{tot} as the scalar product of the force at that node with a unit vector pointing toward the cell force center $\vec{r_c}$ (ref. 39) (**Supplementary Note 13**).

The source code of the algorithm, including the 3D particle image velocimetry and the unconstrained force reconstruction, is available under MIT license on the collaborative coding platform GitHub (https://github.com/Tschaul/SAENO) and is free to download. A compiled version of the software and a tutorial are provided as **Supplementary Software**, together with a sample data set (http://lpmt.biomed.uni-erlangen.de/3DTractions/SampleData.rar).

Analysis of cell migration. We extracted the center-of-mass movement of the cells from their brightfield projections. The movement of the center of mass is described as a persistent random motion with time-varying migratory activity and migratory persistence. We extracted the time courses of both of these parameters from the measured trajectories using a Bayesian method of sequential inference[28]. Only cells that were not undergoing cell division during measurements were included in the correlation analysis.

Statistical analysis. Differences between measurements were considered statistically significant at $P < 0.05$ by Student's two-tailed t-test assuming unequal variances.

33. Bonakdar, N. *et al.* Biomechanical characterization of a desminopathy in primary human myoblasts. *Biochem. Biophys. Res. Commun.* **419**, 703–707 (2012).
34. Faust, U. *et al.* Cyclic stress at mHz frequencies aligns fibroblasts in direction of zero strain. *PLoS ONE* **6**, e28963 (2011).
35. Kollmannsberger, P. & Fabry, B. High-force magnetic tweezers with force feedback for biological applications. *Rev. Sci. Instrum.* **78**, 114301 (2007).
36. Nelder, J.A. & Mead, R. A simplex method for function minimization. *Comput. J.* **7**, 308–313 (1965).
37. Huber, P.J. *Robust Statistics* (John Wiley & Sons, 1981).
38. Tikhonov, A.N. Solution of incorrectly formulated problems and the regularization method. *Soviet Mathematics Doklady* **4**, 1035–1038 (1963).
39. Hersch, N. *et al.* The constant beat: cardiomyocytes adapt their forces by equal contraction upon environmental stiffening. *Biol. Open* **2**, 351–361 (2013).