$\oplus$ = exor

$F \to T \equiv T$

transitive if $a, b, c \in A$, $aRb \wedge bRc \to aRc$

asymmetric if $a, b \in A$ $aRb \to \neg(bRa)$

strict partial order iff trans + asymm

reflexive if aRa $\forall a \in A$ / irreflexive if aRa for no $a \in A$

antisymm if $a \neq b \in A$ $aRb \to \neg(bRa)$

Elizabeth A. Denys, page 1 of 2

stupid course logo problem! out of order pairs: sum i,j mod 2 if that is invariant

invariants can be vacuously true

$R: A \to B$ binary relation

injection iff $\forall a, a' \in A\ \forall b \in B$. aRb and $a'Rb \to a = a'$

surjection iff $\forall b \in B\ \exists a \in A . aRb$

total iff $\forall a \in A\ \exists b \in B . aRb$

function iff $\forall a \in A\ \forall b, c \in B$ aRb and $aRc \to b = c$

weak partial order: transitive, reflexive, antisymmetric

minimal element: if none below, but can have others w/ none below

maximal element: none above

minimum element: lower bound, only can have one

maximum element: upper bound

Mating Ritual: girl there, boy picks top remaining girl, girl tells favorite of suitors to come back, not told boy who visited crosses her off, repeat until only one boy/girl

A is "as big as" B iff surjection $A \to B$

A "same size as" B iff bijection $A \to B$

A "strictly bigger than" B iff A "as big as" B but B "not as big as" A

chain: subset $C \subseteq A$ which are all comparable / transitively related, all elements comparable

antichain: no two elements comparable

Well ordering principle proof:

1. Let C be set of counterexamples to (*) namely, C ::=
2. Assume for purpose of obtaining a contradiction that C is nonempty. Then by the WOP there is a smallest number $m \in C$. m must be at least _ as _
3. contradict assumption that there is a smallest counterexample. Thus, C empty so true for all

Power set "strictly bigger than" set

"as big as" and "same size as" transitive

lexicographic order: $(x, y) < (x', y')$ iff $x < x'$ or ($x = x'$ and $y < y'$)

well-founded partial order

depth of binary-2 PTG = max possible choices

totally ordered if all elements comparable

isomorphism ~ bijection for graphs

handshaking theorem: even number of vertices of odd degree

graph theory definitions:

2 vertices adjacent if joined by edge

edge incident to 2 vertices

degree = # of edges incident to vertex

$f: G_1 \to G_2$ bijection, f is isomorphism, G_1, G_2 isomorphic

path, connected, cycle

tree iff no cycles, unique path b/w any two vertices, $e + 1 = v$

bipartite = two-colorable = no bottlenecks

$|S| > |N(S)|$ – bottleneck

neighbors of S

Hall's matching condition

width – is w if can arrange vertices in a way such that each vertex is adjacent to at most w vertices that precede it in the sequence

discrete falls

bridge, connect

Stirling's

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$$

Asymptotic Notation

$f(x) \sim g(x)$ iff $\lim_{x \to \infty} f(x)/g(x) = 1$

$f(x) = o(g(x))$ iff $\lim_{x \to \infty} f(x)/g(x) = 0$

non-negative g, $f = O(g)$ iff $\limsup_{x \to \infty} |f(x)| / g(x) < \infty$

$f = O(g)$ iff $c \geq 0$ and x_0 st $x \geq x_0$, $|f(x)| \leq g(x)$

$f = \Theta(g)$ iff $f = O(g) \wedge g = O(f)$

Number theory!

for n, d; unique integers q, r, st $n = qd + r$ $0 \leq r < d$

p prime, k not multiple of p, $k^{p-1} \equiv 1 \pmod p$

pigeonhole principle

jellybeans of 6 flavors in 5 jars, 1 jar has 2 of same flavor

$v - e + f = 2$ Euler's formula

planar graph $e \leq 3v - 6$

as $3(e - v + 2) \leq 2e$

$e \leq 3v - 6$

$A(x) = \sum_{n=0}^{\infty} a_n x^n$, $B(x) = \sum_{n=0}^{\infty} b_n x^n$

$C(x) = A(x) B(x) = \sum_{n=0}^{\infty} c_n x^n$

with $c_n = a_0 b_n + a_1 b_{n-1} \cdots + a_n b_0$

$\phi(n)$ ::= # of pos integers < n rel prime to n

p prime $\phi(p^k) = p^k - p^{k-1}$ $k > 0$

$\phi(mn) = \phi(m) \cdot \phi(n)$ for $\gcd(m, n) = 1$

$\gcd(k, n) = 1$ $k^{\phi(n)} \equiv 1 \pmod n$

Combinatorial proof

define set

show $|S| = x$, show $|S| = y$

conclude $x = y$

$$\binom{n+k-1}{n} \to \frac{1}{(1-x)^k}$$

graph w/ max degree k is $(k+1)$ colorable.

$H_n ::= \sum_{i=1}^{n} \frac{1}{i}$, $\ln(n+1) \leq H_n \leq 1 + \ln n$

k to 1 function $f: A \to B$

k elements of A to each element of B

$\Pr\{A - B\} = \Pr\{A\} - \Pr\{A \cap B\}$

$\Pr\{A\} = \Pr\{A - B\} + \Pr\{A \cap B\}$

$$\binom{n}{\alpha n} \leq \frac{2^{n H(\alpha)}}{\sqrt{2\pi\alpha(1-\alpha)n}}$$

$H(\alpha) = \alpha \log_2 \frac{1}{\alpha} + (1 - \alpha) \log_2 \frac{1}{1-\alpha}$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

$\Pr\{C \mid H\} = \frac{\Pr\{C \cap H\}}{\Pr\{H\}}$

C, H independent $\to \Pr\{C \mid H\} = \Pr\{C\}$

or $\Pr\{A \cap B\} = \Pr\{A\} \Pr\{B\}$

NETWORKS!

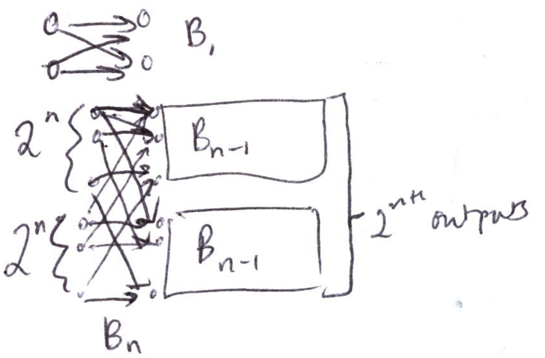
congestion - largest # of paths through a single switch

max congestion - max over all permutations π of min over all paths of the congestion of paths

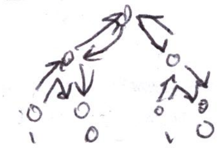
latency - longest path over $P_{i,\pi(i)}$

max latency - max over all permutations π of min over all paths of latency of paths

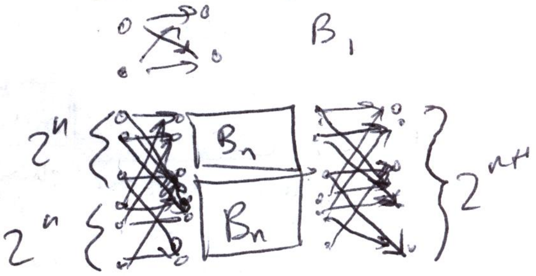
Butterfly network



binary tree



Beneš



network	diameter	switch size	# switches	congestion
Complete binary tree	$2\log N+2$	3×3	$2N-1$	N
appendix → 2-D array	$2N$	2×2	N^2	2
butterfly	$\log N+2$	2×2	$N(\log(N)+1)$	$\sqrt{N}$ or $\sqrt{N/2}$ *
Beneš	$2\log N+1$	2×2	$2N\log N$	1

$N=2^n$ inputs

$\sqrt{N}$ if 2^n, n even

$\sqrt{\frac{N}{2}}$ if 2^n n odd

$\Pr\{S\}=1$; $A_0, A_1, \ldots$ pairwise disjoint sets then $\Pr\{\bigcup_{i\geq 0} A_i\} = \sum_{i\geq 0} \Pr\{A_i\}$

S countable if $S=\{w_0, w_1, \ldots\}$

$\Pr\{\bigcup_{i\geq 0} A_i\} \leq \sum_{i\geq 0} \Pr\{A_i\}$

$\Pr\{A\} = \Pr\{A|E\}\cdot\Pr\{E\} + \Pr\{A|\overline{E}\}\cdot\Pr\{\overline{E}\}$

Russell's Paradox

S variable ranging over all sets, define $W ::= \{S \mid S \notin S\}$

so by definition, $S \in W$ iff $S \notin S$ for every S. Let $S=W$, $W \in W$ iff $W \notin W$

but sets cannot be in themselves

need previously defined bases

$a|b \Rightarrow a|bc$

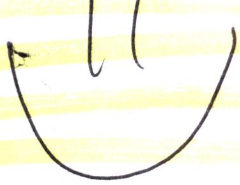
$a|b \wedge b|c \rightarrow a|c$

$a|b \wedge a|c \rightarrow a|(sb+tc)$

$c\neq 0$, $a|b$ iff $ca|cb$

Fund Thm of Arithm

$n = p_1 p_2 p_3 \cdots p_j$ p_i primes



$\gcd(a,b) = sa + tb$ for at least one (s,t)

$\gcd(ka, kb) = k\cdot\gcd(a,b)$ $k>0$

$\gcd(a,b)=1 \wedge \gcd(a,c)=1$, $\gcd(a,bc)=1$

$a|bc$ and $\gcd(a,b)=1 \Rightarrow a|c$

$\gcd(a,b) = \gcd(b, \text{rem}(a,b))$

$a \equiv \text{rem}(a,n) \pmod{n}$

Elizabeth A. Denys, page 2 of 2

random walks

$out(x) ::= \{y \mid x \to y$ is an edge of the graph$\}$

then $\sum_{y \in out(x)} p(x,y) = 1$

$\sum_{x \in V} d(x) = 1$ distribution

stationary: $\hat{d} = d$ so $d(x) = \sum_{y \in in(x)} d(y) \cdot p(y,x)$

indicator random variables → maps everything to 0 or 1

probability density function PDF

$PDF_R : V \to [0,1]$ - $PDF_R(x) = Pr\{R = x\}$

$\sum_{x \in V} PDF_R(x) = 1$

cumulative distribution function CDF

$CDF_R(x) = Pr\{R \le x\}$

$CDF_R : \mathbb{R} \to [0,1]$

Polling

$S_n ::= \sum_{i=1}^{n} K_i$ all same prob that

K_i ↑ Bernoulli vars

$\frac{S_n}{n}$ fraction for event → statistical estimate of p

for $\frac{1}{2} > \epsilon > 0$, $Pr\{|\frac{S_n}{n} - p| \ge \epsilon\} \le \frac{1+2\epsilon}{2\epsilon} \cdot \frac{2^{-n(1-H((1/2)-\epsilon))}}{\sqrt{2\pi(1/4-\epsilon^2)n}}$

at confid level, p is in $-\epsilon + \frac{S_n}{n}$ to $\frac{S_n}{n} + \epsilon$ | - confidence level

Bernoulli Distribution

$PDF_B(0) = p$ $\quad CDF_B(0) = p$

$PDF_B(1) = 1-p$ $\quad CDF_B(1) = 1$

Uniform Dist

$PDF_U(k) = \frac{1}{N}$ - total #

$CDF_U(k) = \frac{k}{N}$

Binomial Distribution

$PDF_J(k) = \binom{n}{k} p^k (1-p)^{n-k}$

$PDF_J(\alpha n) \le \frac{2^{nH(\alpha)}}{\sqrt{2\pi\alpha(1-\alpha)n}} \cdot p^{\alpha n}(1-p)^{(1-\alpha)n}$

$H(\alpha) ::= \alpha \log_2 \frac{1}{\alpha} + (1-\alpha)\log_2 \frac{1}{1-\alpha}$

if $p = \frac{1}{2}$

$PDF_J(\alpha n) \le \sqrt{\frac{2}{\pi n}}$

$CDF_J(k) = \sum_{i=0}^{k} PDF_J(i)$

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

$CDF_J(\alpha n) \le \frac{1-\alpha}{1-\frac{\alpha}{p}} PDF_J(\alpha n)$

$\le \frac{1+\alpha}{1-\frac{\alpha}{p}} \cdot \frac{2^{nH(\alpha)}}{\sqrt{2\pi\alpha(1-\alpha)n}} \cdot p^{\alpha n}(1-p)^{(1-\alpha)n}$

confidence levels

at the % confidence level

– of all samplings will give within range

mean time to failure

fails w/ prob p

$E[crash] = \sum_{i \in \mathbb{N}} i \, Pr\{R = i\}$

$= \sum_{i \in \mathbb{N}} i(1-p)^{i-1} p = \frac{1}{p}$

expectation / average value / expected value / mean

$E[R] ::= \sum_{x \in range(R)} x \cdot Pr\{R = x\} = \sum_{x \in range(R)} x \cdot PDF_R(x)$

for indicator vars $E[I_A] = Pr\{A\}$

linearity of expectation

$E[\alpha_1 R_1 + \alpha_2 R_2] = \alpha_1 E[R_1] + \alpha_2 E[R_2]$

expectation of binary distribution

$E[one] = p$

$E[x \text{ of them}] = px$

Expected prob ~~mul~~ multiplication

$E[R_1 \cdot R_2] = E[R_1] \cdot E[R_2]$

Condition of Expectation

$E[R \mid A] ::= \sum_{r \in range(R)} r \cdot Pr\{R = r \mid A\}$

total expectation $E[R] = \sum_i E[R \mid A_i] Pr\{A_i\}$ ← linear combinations work

partition