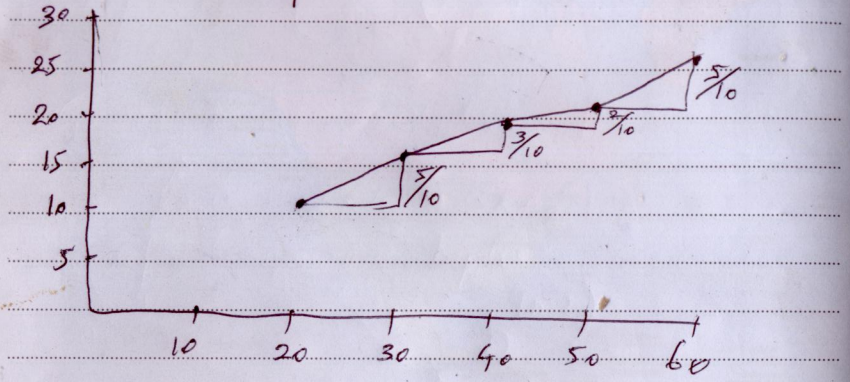
16/04/2014 Random coin toss experiment.

21 January Tuesday 21-01-2014

	blue	total	blue / white
blues	11	20	after 20 coin tosses
	16	30	after 30 coin tosses
	19	40	after 40 coin tosses
	21	50	after 50 coin tosses
	26	60	after 60 coin tosses



11, 16, 19, 21, 26

$\frac{5}{10}, \frac{3}{10}, \frac{2}{10}, \frac{5}{10}$

Distinct partitions (restricted partitions with distinct parts):

Glaisher - Euler's thm - no of partitions with distinct parts = no of partitions with odd parts.

$\prod_{i=1}^{\infty}(1+x^i)$ is generating function

$= \sum q(n) x^n$ number of distinct partitions of n

22-01-2014 January Wednesday 22

Number of valid multiparty voting patterns
= number of distinct partitions of n ($q(n)$)
= number of hashfns with distinct collision chain sizes (without permutation)

Finding one such distinct partition is NP-hard

$a_1 * 1 + a_2 * 2 + a_3 * 3 + a_4 * 4 + \cdots + a_n * n = n$

($a_i = 0$ or $a_i = 1$ for some a_i)

Out of 2^n possible bit patterns only $q(n)$ patterns are valid (distinct partitions)

Above is a variant of money changing problem with denominations 1, 2, 3, 4, ... n and finding the Sylvester denumerants (0 or 1)

Thus it is a direct reduction from NP-hard money changing problem.

Thus finding one valid multiparty voting pattern (distinct parts) is NP-Complete

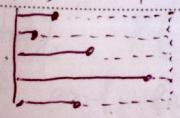
Above always has a biggest part (max choice) (Subset sum problem is also (similar to the above) (non-uniform collision chain).

⇒ Finding such a hash functions is NP-complete (impossible order)

⇒ Democracy with tiebreaker is NP-complete (Alternative proof without SAT circuits for voters)

$2 + 1 + 5 + 6 + 3 = 17$

$4 + 5 + 1 + 0 + 3 = 13$



$6 \times 5 = 30$

December 2013

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

February 2014

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	

Schur's theorem

Number of denumerants for diophantine equation $a \cdot 1 + a_2 \cdot 2 + a_3 \cdot 3 + \cdots + a_n \cdot n$ is given by Schur's theorem and is $= n$

thus a lower bound for number of hash functions (since (order (permutation) is ignored)

$x_0 = c_1 a_1 + \cdots + c_n a_n$ if $x = n$

for

$n = 1 * a_1 + 2 * a_2 + 3 * a_3 + \cdots + n * a_n$

number of denumerant tuples:

$$= \frac{n^{n-1}}{(n-1)!\, a_1 a_2 \cdots a_n} \simeq \frac{n^{(n-1)}}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n a_1 a_2 \cdots a_n}$$

$$\simeq \frac{1 * e^n}{\sqrt{2\pi n}\,(n)^{a_1 a_2 \cdots a_n}} \simeq \frac{e^n}{\sqrt{2\pi}\,(a_1 a_2 \cdots a_n) \times n^{1.5}}$$

1) find one such denumerant (NP-hard due to reduction from MCP)
2) Permute $\leq (n!)$

Ka. Srinivasan
17/4/2014

Thus finding a multipartisan voting with no two candidates getting equal votes is NP-complete.

COLLISION PRONE

Maximizing hash collisions is necessary for clustering similar data into a single collision chain (opposite of collision resistance) (DNA similarities and voice data similarities need to maximize collisions)

COLLISION FREE

Collision Resistant Hash Function is a one-way function such that any randomized polynomial time algorithm finds collision with negligible probability $(f(x) = f(y))$.

Restricted partitions can be classified as following:

1. Set of partitions in which no part exceeds k (more COLLISION FREE)
2. Set of partitions in which no part is less than k. (more COLLISION PRONE)

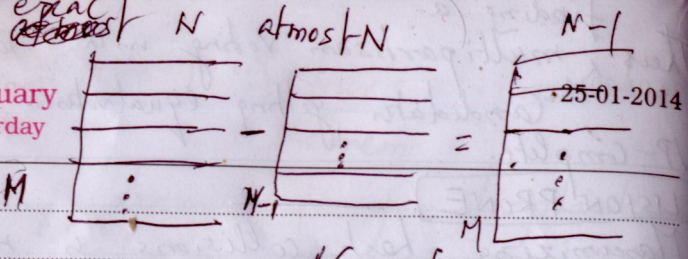
① is more Collision-Free (when mapped to a hash table)
② is more Collision-Maximizing (when mapped to a hash table)

Recurrence relation for ①

$P(N, M; n) = P(N, M-1, n) + P(N-1, M, n-M)$.

n is partitioned into M parts and each part of size at most N

25 January Saturday



Subtracting the above recurrence for (1) from P(n) gives (2) (set of partitions in which no part is less than a constant)

Ka Shrinivasan
17/04/2014

26 Sunday

Republic Day, 26-01-2014

December 2013

S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

27-01-2014

January Monday 27

February 2014

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	