0368.4163 Randomness and Computation	Ronitt Rubinfeld
Lecture 1	
04 March 2009	Spring 2009

Scribes: D. Sotnikov

The Erdos Probabilistic Method

In order to prove the existence of a mathematical objec with desirable properties, is enough to define appropriate probability space and to show that a random point in the space is a mathematical object with the desirable properties with positive probability thus one can conclude that such a mathematical object exists. The important point is that this method of proof is nonconstructive so it does not create an example of object. (http://en.wikipedia.org/wiki/Probabilistic_method)

Example 1:

Let S be a set of objects and $s_1, ..., s_m \subseteq S$ each s_i is of size $l \geq 2$. Can we 2-color S so that each s_i has one of each color?

Claim: In the global case the answer is **No** but for special case $m < 2^{l-1}$ the answer is **Yes**.

Theorem 1: If $m < 2^{l-1}$ exist proper 2-coloring such that each s_i has one of each color.

Remark. Recall the union bound: $Pr[A \bigcup B] \leq Pr[A] + Pr[B]$

Proof of the Theorem 1:

- Randomly color elements of S to red/blue colors
- $\forall i \quad Pr[s_i \ monochromatic] = \frac{1}{2^l} + \frac{1}{2^l} = \frac{2}{2^l} = \frac{1}{2^{l-1}}$ (the probability to color all l elements to same color is $\frac{1}{2^l}$ and we have 2 colors)
- $Pr[\exists i \ s.t. \ s_i \ monochromatic] \leq \sum_{i=1}^{m} Pr[s_i \ monochromatic] \leq \frac{m}{2^{l-1}} < 1$ (union bound)
- $Pr[all \ s_i's \ properly \ colored] = 1 - Pr[\exists i \ s.t. \ s_i \ monochromatic] > 0$

$\Longrightarrow$exists setting of colors which gives proper coloring

□

Definition: For A a subset of positive integers, A is sum-free if $\nexists a_1, a_2, a_3 \in A$ s.t. $a_1 + a_2 = a_3$.

Example 2:

Let B be a set of positive integers. Is it always exists a subset A of B such taht A is sum-free and the size of A is $> \frac{|B|}{3}$?

For example for the set $B = \{1, ..., n\}$ two different subsets that satisfy the claim: $A = odd \ integers$ and $A' = \{\frac{n}{2} + 1, ..., n\}$, such that the size of each of them is $\approx \frac{n}{2}$.

Theorem: [Erdos] $\forall B = \{b_1, ..., b_n\}$ exists sum-free $A \subseteq B$ s.t. $|A| > \frac{n}{3}$.

Remark.

- $\mathbb{Z}_p = \#'s\ mod\ p = \{0..p-1\}$
- $\mathbb{Z}_p^* = \#'s\ mod\ p\ relative\ prime\ to\ p = \{1..p-1\}$

Proof of the Erdos Theorem:

- w.l.o.g. b_n is the maximal value of B.
- Pick prime $p > 2 \cdot b_n$ s.t. $p \equiv 2\,(mod\,3)$ (such number always exists, see the Dirichlet's theorem on arithmetic progressions http://en.wikipedia.org/wiki/Dirichlet%27s_theorem_on_arithmetic_progressions)
- $p = 2k + 3$ for some integer k.
- let $C = \{k + 1, ..., 2k + 1\}$, C is sum-free even $mod\,p$ because
  - $(k + 1) + (k + 1) = 2k + 2 > 2k + 1$
  - $(2k + 1) + (2k + 1) = 4k + 2 = k\,(mod\,p) = k < k + 1$.
- $\frac{|C|}{p-1} = \frac{k+1}{3k+1} > \frac{1}{3}$
- Pick $x \in_R \{1..p-1\} = \mathbb{Z}_p^*$
  - $\forall i \quad let\ d_i \leftarrow x \cdot b_i\,(mod\,p)$
  - $A_x \leftarrow \{b_i\ s.t.\ d_i \in C\}$

Now for finish the proof we need to show:

- $\forall x\ A_x$ is sum-free
- $\exists x\ s.t.\ |A_x| > \frac{n}{3}$

Claim 1: $\forall x\ A_x$ is sum-free

Proof of the Claim 1: In the way of contradiction, suppose that $\exists b_i, b_j, b_k \in A_x$ s.t. $b_i + b_j = b_k$ this implies that also $b_i + b_j \equiv b_k(modp)$, multiply both sides by x and get $x \cdot b_i + x \cdot b_j = x \cdot b_k\,(mod\,p)$ but $x \cdot b_i, x \cdot b_j, x \cdot b_k \in C$ contradiction to the fact that C is sum-free.

$\square$

Fact: $\forall y \in \mathbb{Z}_p^*$ and $\forall i$ there exists exactly one $x \in \mathbb{Z}_p^*$ s.t. $y \equiv x \cdot b_i\,(mod\,p)$, i.e., $\forall y\ Pr[b_i\ maps\ to\ y] = \frac{1}{p-1}$

Proof of the Fact: $\mathbb{Z}_p^*$ is group $b_i \in \mathbb{Z}_p^*$ so exists $b_i^{-1} \in \mathbb{Z}_p^*$so exists $x = y \cdot b_i^{-1} \in \mathbb{Z}_p^*$. If $x_1 \cdot b_i \equiv x_2 \cdot b_i\,(mod\,p) \Rightarrow$multiply both sides at from b_i^{-1} at the right and get $x_1 \equiv x_2\,(mod\,p)$.

$\square$

Claim 2:$\exists x\ s.t.\ |A_x| > \frac{n}{3}$

Proof of the Claim 2:

- From the fact that we just proved, we get that $\forall i\ |C|$ choices of x make $x \cdot b_i \in C$
- let define the indicator function $\sigma_i = \begin{cases} 1 & if\ x \cdot b_i \in C \\ 0 & otherwise \end{cases}$
- $E[\sigma_i] = Pr[\sigma_i = 1] = \frac{|C|}{p-1} > \frac{1}{3}$
- $E[|A_x|] = E[\Sigma\sigma_i] = \Sigma(E[\sigma_i]) > \frac{n}{3}$ (by the linearity of expectation)

$\Rightarrow \exists x\ s.t.\ |A_x| > \frac{n}{3}$ because if for all the x's $|A_x| \leq \frac{n}{3}$ then $\underset{x}{max}|A_x| \leq \frac{n}{3}$ and then expectation is less equal then $\frac{n}{3}$ in contradiction to $E[|A_x|] > \frac{n}{3}$.

$\square$