CS 70 Cheat Sheet

Monday, November 04, 2013 11:16 PM

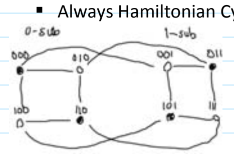
Error Correcting:

- A polynomial *P*(*x*) of degree at most *d* can be uniquely identified by knowing its value at *d*+ 1 points.
- There is a unique polynomial of degree at most *d* such that it hits all *d*+1 points.
- Erasure error: n + k
- General error: n + 2k
- Lagrange Interpolation:
  - $\Delta_i(x) = \frac{(x - x_{j_1})(x - x_{j_2}) \dots (x - x_{j_d})}{(x_i - x_{j_1})(x_i - x_{j_2}) \dots (x_i - x_{j_d})}, j \neq i$
  - P(x) =
    - $y_1\Delta_1(x) + y_2\Delta_2(x) + \cdots + y_{d+1}\Delta_{d+1}(x)$
  -
- Linear equations
  - Plug and chug in $ax^2 + bx + c = y$
- Berlekamp and Welch
  - If the e_1, e_2 …. e_k packets are corrupted so that the received points are r_1, r_2…r_k we can define E(x) = (x-e_1)(x-e_2)…(x-e_k) and Q(x) = P(x)*E(x). Then we use Q(i) = r_i * E(i) to solve for Q(x) and E(x) whose quotient is P(x). Q is of degree n + k - 1 and E is degree k with the first coefficient equal to 1.
- DON'T FORGET ABOUT MODULAR INVERSES
- X = y mod p
  - Y = gcd

Counting/Probability

- 1st rule of counting: If there are n_1 ways of making the first choice and for every way of making the first choice there are n_2 ways of making the second choice, and for every way of making the first 2 choices there are n_3 ways of making the third choice, then the total number of distinct objects that can be made by a succession of k choices is n_1* n_2... n_k
- 2nd rule of counting: If the order in which the choices is made does not matter, count the number of ordered objects (pretending order matters) and divide by the number of ordered objects per unordered object
  - $\binom{n}{k} = \frac{n!}{(n-k)!k!}$
  - $\frac{n!}{(n-k)!}$
- Sampling with replacement, but where order does matter
  - Balls and bins: ${}_{k+n-1}C_k$ | | n = # of items; k = locations
- $\sum_{i=1}^{n} a_0 k^i = a * \frac{1-k^n}{1-k}$
- $P[A|B] = \frac{P[A \cap B]}{P[B\}}$
- $\Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]} = \frac{\Pr[A] \times \Pr[B]}{\Pr[B]} = \Pr[A].$
- Mutual/pairwise independence
  - **Definition 10.2 (mutual independence)**: Events $A_1, \dots, A_n$ are mutually independent if for every subset $I \subseteq \{1, \dots, n\}$,
  $$\Pr[\cap_{i \in I} A_i] = \prod_{i \in I} \Pr[A_i].$$
- Product Rule:
  - $\Pr[A \cap B] = \Pr[A]\Pr[B|A].$
  - $\Pr[\cap_{i=1}^{n} A_i] = \Pr[A_1] \times \Pr[A_2|A_1] \times \Pr[A_3|A_1 \cap A_2] \times \cdots \times \Pr[A_n | \cap_{i=1}^{n-1} A_i].$
- **Theorem 10.2**: **[Inclusion/Exclusion]** For events $A_1, \dots, A_n$ in some probability space, we have
$$\Pr[\cup_{i=1}^{n} A_i] = \sum_{i=1}^{n} \Pr[A_i] - \sum_{\{i,j\}} \Pr[A_i \cap A_j] + \sum_{\{i,j,k\}} \Pr[A_i \cap A_j \cap A_k] - \cdots \pm \Pr[\cap_{i=1}^{n} A_i].$$
- Bayes' Rule:
  - $Pr[A|B] = \frac{Pr[B|A]\,Pr[A]}{Pr[B]}$
  - $Pr[A|B] = \frac{Pr[B|A]\,Pr[A]}{Pr[B|A]\,Pr[A] + Pr[B|\overline{A}]\,(1 - Pr[A])}$
- Total Probability Rule:
  - $Pr[B] = Pr[B|A]\,Pr[A] + Pr[B|\overline{A}]\,(1 - Pr[A])$
- Disjoint:
  - $\Pr[\cup_{i=1}^{n} A_i] = \sum_{i=1}^{n} \Pr[A_i].$
- Union Bound:
  - $\Pr[\cup_{i=1}^{n} A_i] \leq \sum_{i=1}^{n} \Pr[A_i].$

Graphs:

- Terms:
  - Undirected: edges bi-directional
  - Directed: edges one-directional
  - Degree (vertex): number of edges on vertex
  - In-degree: edges pointing to vertex
  - Out-degree: edges pointing out of vertex
  - Path: edges that connect two vertices
  - Cycle: path that starts and ends on same vertex
  - Bridge: edge whose removal would result in unconnected graph
- Eulerian Cycle: connected and
  - Undirected: every vertex even degree
  - Directed: every vertex's in-degree = out-degree
- Eulerian Path: connected and
  - Undirected: exactly two vertices whose degrees are odd
  - Directed: exactly one vertex whose in-degree is 1 greater than its out-degree and one vertex whose in-degree is
- Eulerian Tour
  - Undirected graph has an Eulerian tour iff graph is connected (except for isolated vertices) and every vertex has an even degree
- Hamiltonian Path/Cycle:
  - Traverses every vertex in a graph exactly once
- Hypercube
  - Graph whose vertices are n-bit strings and edges connect vertices which differ by exactly 1 bit
  - |Vertices| = 2^n
  - |Edges| = $n*2^{n-1}$
  - n-bit hypercube has
    - Eulerian Cycle iff n even
    - Always Hamiltonian Cycle
  - 

  - Theorems:
    - For any undirected graph, the sum of all the vertices' degrees is equal to twice the number of edges
    - No graph can have an odd number of vertices whose degrees are odd (odd-degree vertices always come in pairs)
    - In order to divide a hypercube into two sub-graphs, a number of edges that need to be removed is at least the number of vertices in the smaller sub-graph
  - Use induction
  - For iffs - short answer and use theorems/examples
  - In even degree graph, walk from u (can only get stuck at u)
  - removing tour from even degree graph = even degree graph

Given (1, 1), (2, 1), (3, 3) mod 7

$\Delta_1(x) = \frac{(x-2)(x-3)}{2} = 4(x^2-5x+6) \bmod 7$

$\Delta_2(x) = \frac{(x-1)(x-3)}{-1} = 6(x^2-4x+3)$

$\Delta_3(x) = \frac{(x-1)(x-2)}{2} = 4(x^2-3x+2)$

$P(x) = 4(x^2-5x+6)$
$+ 6(x^2-4x+3)$
$+ \cancel{12}^{5}(x^2-3x+2) \bmod 7$

$15x^2 - 59x + 52$
$= (1)x^2 + 4x + 3 \bmod 7$ ★

- $\binom{n}{k} = \binom{n}{n-k}$
- $\binom{n}{k+1} = \binom{n-1}{k} + \binom{n-2}{k} + \cdots + \binom{k}{k}$
- $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$
- P(bin|empty) = $\frac{n-1^m}{n} = \left(1 - \frac{1}{n}\right)^m$

- Probability of getting exactly r Heads from n tosses of a biased coin with Heads probability p is $\binom{n}{r} p^r (1 - p)^{n - r}$