MIDTERM II STUDY GUIDE, SELECTED SOLUTIONS

CHRIS CRUTCHFIELD

1. Polynomials, Secret Sharing and Error-correcting Codes

Solution 4.

(a) For all i, we have p choices for $f(i)$. Therefore we have p^p possible functions total.
(b) There are p^p apparently distinct polynomials on GF_p.
(c) Let $p(x)$ and $r(x)$ be two apparently distinct functions, but suppose that they're equal on GF_p. Consider the polynomial $f(x) = p(x) - r(x)$. This polynomial has at least one non-zero coefficient, but is zero on GF_p. But f is then a degree $p-1$ polynomial that is zero on p points, hence it must be the zero polynomial. This is a contradiction.
(d) Therefore each of these p^p apparently distinct polynomials must correspond to one of the p^p distinct functions.

2. Discrete Probability

Solution 4.

(a)

$$\frac{1}{\binom{100}{20}}$$

(b)

$$\frac{\binom{98}{18}}{\binom{100}{20}}$$

(c)

$$\Pr[CC|W] = \frac{\Pr[CC \cap W]}{\Pr[W]} = \frac{\Pr[CC] - \Pr[CC \cap \overline{W}]}{1 - \Pr[\overline{W}]} = \frac{\binom{98}{18} - \binom{96}{18}}{\binom{100}{20} - \binom{98}{20}}$$

(d)

$$\Pr[W] = 1 - \frac{\binom{98}{20}}{\binom{100}{20}}$$

$$\Pr[CC] = \frac{\binom{98}{18}}{\binom{100}{20}}$$

And we can easily check that $\Pr[CC]\Pr[W] \neq \Pr[CC \cap W]$.

(e) Let E be the event that at least one state has two members on the committee. Then

$$\Pr[E] = 1 - \Pr[\overline{E}] = 1 - \frac{\binom{50}{20}2^{20}}{\binom{100}{20}}.$$

Last updated April 5, 2006.

Solution 5.

We note that $B_1 = p$, $A_1 = q$. Also $B_n = pA_{n-1} + qB_{n-1}$ and $A_n = pB_{n-1} + qA_{n-1}$.

Therefore

$$\begin{aligned} B_n - A_n &= pA_{n-1} + qB_{n-1} - pB_{n-1} - qA_{n-1} \\ &= (p-q)A_{n-1} - (p-q)B_{n-1} \\ &= -(p-q)^n \end{aligned}$$

Solution 6. Let M be the event that it's a male. Let F be the event that it's a female. Let C be the event that the person is colorblind.

$$\begin{aligned} \Pr[M|C] &= \frac{\Pr[C|M]\Pr[M]}{\Pr[C|M]\Pr[M] + \Pr[C|F]\Pr[F]} \\ &= \frac{\frac{1}{5}\cdot\frac{1}{4}}{\frac{1}{5}\cdot\frac{1}{4} + \frac{1}{3}\cdot\frac{3}{4}} \\ &= \frac{1}{6} \end{aligned}$$

Solution 7.

(a) Let B be the event that it's a biased coin, and let N be the event that it's a normal coin. Let H be the event that it lands heads.

$$\begin{aligned} \Pr[B|H] &= \frac{\Pr[H|B]\Pr[B]}{\Pr[H|B]\Pr[B] + \Pr[H|N]\Pr[N]} \\ &= \frac{1\cdot\frac{1}{n}}{1\cdot\frac{1}{n} + \frac{1}{2}\cdot\frac{n-1}{n}} \\ &= \frac{2}{n+1} \end{aligned}$$

(b) Let B and N be as before. Let H^k be the event that k heads land.

$$\begin{aligned} \Pr[B|H^k] &= \frac{\Pr[H^k|B]\Pr[B]}{\Pr[H^k|B]\Pr[B] + \Pr[H^k|N]\Pr[N]} \\ &= \frac{1\cdot\frac{1}{n}}{1\cdot\frac{1}{n} + \frac{1}{2^k}\cdot\frac{n-1}{n}} \\ &= \frac{2^k}{2^k+n-1} \end{aligned}$$

(c)

$$\Pr[F|H^k] + \Pr[B|\overline{H^k}] = \frac{n-1}{2^k+n-1} + 0$$