Ungraded Homework Solutions

CSC 152 – Cryptography

Please notify me of any errors you find. If you need help, ask.

1) When choosing a random card, the card values 2–8 each have probability 1/13 of being selected from a regular deck and probability 0 of being selected from a pinochle deck. The cards 9–A each have probability 1/13 of being selected from a regular deck and probability 1/6 of being selected from a pinochle deck. This means we can leverage the differences in probabilities to get some advantage: either guess "standard deck" when seeing 2–8, or guess "pinochle deck" when seeing 9–A (these are actually identical strategies but with complementary if-conditions). Here's a distinguishing algorithm.

```
x = f()
if (x is 9, 10, J, Q, K, or A)
   guess "pinochle"
else
   guess "standard"
```

The resulting advantage is Pr[guesses pinochle | deck is pinochle] − Pr[guesses pinochle | deck is standard] = $1 - 6/13 = 7/13$.

2) Since numbers 31–34 cannot occur on a 30 sided die, one strategy is to look for them. If we see at least one, then the die must be 34 sided. We can infer that it is slightly more likely to be a 30-sided die if we see no 31–34 sides. Here's a distinguishing algorithm based on this strategy.

```
Query f() q times, getting values x1, x2, ..., xq
if any of x1, ..., xq are greater than 30
   return "34 sided"
else
   return "30 sided"
```

Next calculate advantage Adv = Pr[guess 30-sided|30-sided die in box] − Pr[guess 30-sided|34-sided die in box] = $1 - (30/34)^q$.

3) You could compute the GCD of 16 with 0 through 15, and keep the ones whose GCD is 1. Or, you can determine 16's prime factors and eliminate all their multiples. Both strategies eliminate numbers that share a factor with 16.

Since 16's only prime factor is 2, it's easy to eliminate all the multiples of 16's prime factors. Just eliminate all the even values in $\mathbb{Z}_{16}$. So, the elements of $\mathbb{Z}_{16}$ with a multiplicative inverse are 1, 3, 5, 7, 9, 11, 13, 15. Finding the inverses is a matter of brute for search: $1 \cdot 1 \bmod 16 = 1$, $3 \cdot 11 \bmod 16 = 1$, $5 \cdot 13 \bmod 16 = 1$, $7 \cdot 7 \bmod 16 = 1$, $9 \cdot 9 \bmod 16 = 1$, $11 \cdot 3 \bmod 16 = 1$, $13 \cdot 5 \bmod 16 = 1$, and $15 \cdot 15 \bmod 16 = 1$.