5: Hamming Distance

Problem Statement:
Let $PRIME_n$ be the problem of determining whether the Hamming distance between two given n-bit strings is a prime.
Prove that $R_{1/3}(PRIME_n) = \Omega(\text{n})$.

Analysis:
This problem seem nearly insurmountable to tackle from first principles and thus a natural approach is to attempt to reduce it to a known problem. In particular, this solution discusses a possible attempt to prove the bound using a reduction from the Disjointness problem, the only problem covered in class with $\Omega(n)$ randomized complexity while not being entirely intractable to the models covered in class. While I wasn't able to definitively show a provably correct reduction from the disjointness problem to the prime gap hamming distance problem, the solution discusses potential ideas for this.

Definitions:
Let $DISJ_n(x, y) = 1$ if x and y are disjoint and 0 otherwise

Claim.
$R_{1/3}(PRIME_n) = \Omega(n)$

Proof. Idea for reduction from $DISJ_n$ to $PRIME_n$:
Run the $PRIME_n$ protocol on the strings and if the gap hamming distance is prime, strings are more likely to be disjoint (was not able to prove this, but only able to observe from empirical testing).
If the assumption stands, then the protocol is better than random for prime numbers, and thus a random coin toss for non prime numbers while forcing us to incur significant amount of error (in particular error exponentially close to random guessing) but nonetheless provides a meaningful reduction.

During my research for this problem, I was able to come across a solution that proves the linear bound for the Index Problem where $INDEX_n(x, y) =$ x-th bit of y, and then goes on to reduce the Index Problem to the Gap Hamming Distance problem (which in turn can be used to obtain a simple reduction to the prime version discussed here). However, the reduction used incurs some error as it uses shared randomness to achieve its goals.

9: The Hat Problem

Problem Statement:
A group of n prisoners are brought into a room with n chairs arranged in a circle. Once they are all seated, each prisoner has a hat placed on their head. There are n distinct colors of hats, which are known to the prisoners beforehand, though colors may be repeated or not appear on any prisoner's head. Each prisoner can see everyone's hat color except for their own. The prisoners must then simultaneously call out a guess for their own hat color. The prisoners are set free if at least one of them guesses their own hat color correctly, and are all executed otherwise. Is it possible for the prisoners to guarantee that they will all be set free? The prisoners can devise a strategy before entering the room, but cannot communicate thereafter.

Analysis:
The idea is to have the prisoners co-ordinate in a way such that the guesses account for a maximal number of scenarios. In particular, this protocol attempts to have the prisoners guess all possible values that the sum of the hats colors (if colors were interpreted as numbers from 1 to n) could be, and in turn ensures that (exactly) one prisoner guesses correctly, thus guaranteeing success.

Definitions:
Let the colors be interpreted as numbers from 1 through n (any arbitrary ordering suffices)
Let c_i refer to the color of the i-th prisoner's hat
Let g_i refer to the guess made by the i-th prisoner

Claim.

$$Let g_i = i - \sum_{\forall j \neq i} c_j (mod n)$$
$$\exists i \text{ such that } g_i = c_i$$

Proof. The proof is simple, since every prisoner assumes the sum of the colors to be equivalent modulo n to their index and since there are n prisoners, every possible value that the sum of colors could be (modulo n) is considered and thus exactly one must guess the value correctly. Moreover, since there are n colors, exactly one color will be equivalent to the above expression and thus each prisoner is able to make the only valid guess (under their private assumption regarding the value of the sum of the colors of the hats).

References

[1] Roughgarden, Tim. Lecture 2: Lower Bounds for One-Way Communication: Disjointness, Index, and Gap-Hamming. Stanford, 15 Jan. 2015, theory.stanford.edu/ tim/w15/l/l2.pdf.