CS 70 Discrete Mathematics and Probability Theory
Fall 2012 Vazirani HW 7

1 Berlekamp-Welch

In this question, we'll take a birds-eye view to see how the Berlekamp-Welch error correcting scheme works. For all of these questions, assume that the alphabet is $\{a, b, c, d\}$, where $a = 0$, $b = 1$, etc.

1. Alice wants to send a 4-packet message "baba" to Bob along a noisy channel. How many packets should she send if one of the characters gets corrupted? What if two of them are corrupted?

–Solution & Exemplar–

$n = 4$, $k = 1$, message length $n + 2k = 6$.
$n = 4$, $k = 2$, message length $n + 2k = 8$.

2. For parts 2-6 of this question, assume that there are 2 errors. We will work over a Galois field $GF(p)$. What's the smallest p we can use?

–Solution & Exemplar–

$p \geq n + 2k$, and it should be prime so smallest is $p = 7$ for $k = 1$ and $p = 11$ for $k = 2$.

3. When Alice encodes her message, what is the degree of the polynomial $P(x)$?

–Solution & Exemplar–

4 points uniquely determine a polynomial of degree ≤ 3, so for a 4 character message, $\deg(P(x)) \leq 3$.

4. Say that the two errors occur en route at locations 0 and 2. What is the error polynomial and what are its roots?

–Solution & Exemplar–

$E(x) = x(x-2) = x^2 - 2x \equiv x^2 + 9x \mod 11$, with roots at $x = 0$ and $x = 2$, the locations of the errors.

5. What is the degree of $Q(x)$?

–Solution & Exemplar–

$Q(x) = P(x)E(x)$. $\deg(P(x)) \leq 3$ and $\deg(E(x)) = 2$.
$\deg(Q(x)) \leq \deg(P(x)) + \deg(E(x)) \leq 5$.
(Note that leading term of product of $P(x)E(x)$ may be $(a_3x^3)x^2 = a_3x^{2+3} = a_3x^5$.)

6. Bob receives the data "$2, 0, 4, 0, 4, 9, 0, 6$". Write out (but don't solve) the system of linear equations Bob can use to find out the locations of the errors.

–Solution & Exemplar–

$Q(x) = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$.
$E(x) = x^2 + b_1x + b_0$. For the following, work in $GF(11)$.

$$\begin{aligned}
a_0 &= 2b_0 \\
a_5 + a_4 + a_3 + a_2 + a_1 + a_0 &= 0 \\
10a_5 + 5a_4 + 8a_3 + 4a_2 + 2a_1 + a_0 &= 5 + 8b_1 + 4b_0 \\
a_5 + 4a_4 + 5a_3 + 9a_2 + 3a_1 + a_0 &= 0 \\
a_5 + 3a_4 + 9a_3 + 5a_2 + 4a_1 + a_0 &= 9 + 5b_1 + 4b_0 \\
a_5 + 9a_4 + 4a_3 + 3a_2 + 5a_1 + a_0 &= 5 + b_1 + 9b_0 \\
10a_5 + 9a_4 + 7a_3 + 3a_2 + 6a_1 + a_0 &= 0 \\
10a_5 + 3a_4 + 2a_3 + 5a_2 + 7a_1 + a_0 &= 5 + 9b_1 + 6b_0
\end{aligned}$$

Using this system of equations, Bob finds that $b_0 = 0$ and $b_1 = -2$, and computes $P(x) = \frac{Q(x)}{E(x)}$ to recover the original polynomial.

2 Secret Sharing with one Spy

Recall the secret sharing setup from the lecture notes. We have officials 1 to n who must share a launch code $s \in \mathbb{N}$, so that if k of them get together to launch a weapons strike they'll be able to recover s, but fewer officials are powerless. A prime number $q \geq s, n$ and a $k-1$ degree polynomial P are chosen so that modulo q, $P(0) = s$. For each $i = 1 \ldots n$, official i is then given $P(i)$. Given the P-values of k officials, the unique P can be reconstructed from the Lagrangian interpolation procedure and once that is done $s = P(0)$ can be regained. We also saw that $k-1$ officials cannot say anything about $P(0)$ as for each of the q choices for this value, there exists a polynomial passing through that point and the $k-1$ points provided by the officials.

Consider the same setting, but now one of the n officials is actually a spy. S/he is given one of the $P(i)$ values as usual, but now the spy – who wants to avoid activating the launch code – will lie about the value when it comes to reconstructing the secret s. The officials have only one chance at entering the code, so they must get it right. Fortunately, the officials know that there is a spy in their midst and so they decide to form *all* possible groups of k people out of the n in order to attempt to reconstruct s in many ways – since the spy can only affect a few of these groupings the officials hope that most of the reconstructed s's will be correct. Consider below the situation when each group of $k = 2$ of the n officials meet, where one of the n is the spy.

1. For the case $n = 2$, can the spy prevent the single non-spy official from learning about s by lying about his/her P-value? Can the official learn anything about s at all?

–Solution & Exemplar–

Let $P(x_o)$ be the value given to the official and $P(x_a)$ be the value given to the secret agent.
For $n = 2$, $P(x)$ is a degree ≤ 1 polynomial, uniquely determined by 2 points.
Yes, the spy can prevent the non-spy official from learning s by lying.
No, the official can't learn anything about s, as they only have $P(x_o)$ and cannot trust $P(x_a)$ for the reconstruction.

2. When there are $n = 3$ officials, three pairs will meet to attempt to reconstruct s – each official will meet twice. In this case can the officials successfully enter the launch code s?

–Solution & Exemplar–

No.
Suppose we have officials o_1, o_2 and a, the secret agent. In this scheme, we have the following matchings:

- (o_1, o_2), reconstruct $P'_{12}(x)$
- (o_1, a), reconstruct $P'_{1a}(x)$
- (o_2, a), reconstruct $P'_{2a}(x)$

Here, Officials 1 and 2 each see two distinct reconstructed polynomials, $P'_{12}(x) \neq P'_{1a}(x)$ and $P'_{12}(x) \neq P'_{2a}(x)$. However, 1 doesn't know if 2 or a is the spy and 2 doesn't know to trust 1 over a, so the officials can know nothing of the secret.

–Solution Note–

Note that the officials cannot apply Berlekamp-Welch to reconstruct the original polynomial in a case with one error; there would need to be one extra official for B-W to apply.

3. What about the case of $n \geq 4$?

–Solution & Exemplar–

Yes. In this case, each official will have more meetings with true officials than with the spy, whom they will only meet with once.
Applying Lagrangian interpolation, each official can then pick the polynomial that they reconstructed most frequently, or even just the one that they reconstructed more than once.

3 Trees

Prove that a connected undirected graph with n vertices and no cycles must have exactly $n-1$ edges. (This kind of a graph is called a *tree*).

–Solution–

Proof by strong induction on the size of the graph. Key insight for inductive step: remove an arbitrary edge from the graph of size $k+1$. This results in two connected acyclic sub-graphs disconnected from one another, each of size $\leq k$. Applying the inductive hypothesis and adding the removed edge back in the graph yields the result.

–Exemplar–

For a graph $G = (V, E)$, let $|E|$ represent the number of edges and $|V|$ represent the number of vertexes.

Proof: Proof by induction on n, the number of vertexes in the graph.
Base case: $n = 1$. Single vertex, 0 edges. $|E| = n - 1 = 0$.
Inductive hypothesis: $\forall n \leq k$, every connected undirected acyclic graph with $|V| = k$ must have $|E| = k - 1$.
Inductive step: Consider a connected undirected acyclic graph with $|V| = k + 1$. Remove some arbitrary edge (v_i, v_j) from the graph.
CLAIM: This results in two separate connected undirected acyclic graphs of size $\leq k$.

Proof: *The proof of this claim was proved in lecture, and is not necessary for full credit.* (v_i, v_j) is removed from the original connected undirected acyclic graph. Suppose v_i is still connected to v_j. Contradiction: Were v_i still connected to v_j, this would imply a cycle in the original graph (take path from v_i to v_j, and finish cycle with edge (v_i, v_j)). The original graph was connected, so there are two distinct sets of vertexes now, those reachable from v_i and those reachable from v_j, creating connected sub-graphs G_i and G_j. Note that G_i and G_j are also acyclic since removing an edge from a graph cannot introduce a cycle (i.e. a second path between two vertexes). □

Consider $|E_i|$ and $|E_j|$ to be the number of edges in subgraphs G_i and G_j respectively. Now, we have m vertexes in G_i and $(k+1) - m$ vertexes in G_j. We apply our inductive hypothesis to find $|E_i| = m - 1$ and $|E_j| = k - m$. Now, adding the removed edge back into the graph, $|E| = (m-1) + (k-m) + 1 = k$. By induction, we are done. □

4 Eulerian Tours

Consider a variation of the Eulerian tour problem. You now aim to find a path that starts and ends at the same vertex, and uses each edge *twice* (once in each direction). Show that you can find this tour in any connected graph.

–Solution–

Make use of the directed graph version of Eulerian Tours, proved in Lecture. A directed graph has an Eulerian Tour if and only if the in-degree of each vertex is equal to its out-degree. This has a similar proof to that for undirected Eulerian Tours. Using that fact, transform each undirected link into two directed links in opposite directions. This yields a directed graph where the in-degree is equal to the out-degree, and therefore has an Eulerian Tour.

Alternatively: Proof by simple induction on n, the number of vertexes in the graph.
Lemma: Prove that for any connected undirected graph with $n \geq 2$ vertexes, $\exists$ a vertex that can be removed while leaving a single connected subgraph of size $n-1$. A connected graph implies the existence of a (not necessarily simple) path connecting every vertex. This path must terminate at some vertex, and this vertex must be reached for the first time at the end of the path. This last vertex may be removed leaving a connected graph with $n-1$ vertexes.
Use the inductive hypothesis to identify the existence of an Eulerian Tour in graph of size k. Every vertex will be reached along this tour. Any time a vertex adjacent to the removed vertex is reached, follow the connecting edge twice and return to the original Eulerian Tour. This completes the proof.

Theorem 0.1: *Directed Eulerian Tour*
A connected directed graph has an Eulerian Tour if and only if the in-degree of a vertex is equal to the out-degree.

Proof: *This proof was given in Lecture, and is not necessary for full credit.*
($\Rightarrow$) An Eulerian Tour begins at some vertex v_α, and crosses to $v_{\alpha+1}$. After crossing, we remove this edge, as it cannot be used again. This decreases the out-degree of v_α by 1 and the in-degree of $v_{\alpha+1}$ by 1. This path ends at v_α, so it must continue, following an edge that decreases the out-degree of $v_{\alpha+1}$ by 1. When the path ends, the in-degree of v_α is decreased by 1, and the in and out degrees of every vertex must be 0. Therefore, the in-degree and out-degree of every vertex must have been equal.
($\Leftarrow$) By induction. $n = 1$, single vertex, trivially satisfied. Assume true for $n = k$ vertexes. For $n = k + 1$, we have some connected directed graph of size $k + 1$ with in-degree = out-degree for every vertex. Take any vertex in the graph. It has r inbound edges and r outbound edges. Create a bijection to map inbound-edges to out-bound edges, i.e. for vertex v_x, with edges (v_w, v_x) and (v_x, v_y), remove those two edges and introduce a new edge (v_w, v_y). This does not change the in-degree or out-degree of v_w or v_y. The result is a connected directed graph of size k, to which our inductive hypothesis applies. On the Eulerian Tour of this sub-graph, replace edges (v_w, v_y) with the original (v_w, v_x) and (v_x, v_y) pairs. This creates the Eulerian tour in the graph with $k + 1$ vertexes, completing the proof. □

To prove the claim in this problem, replace every undirected edges with two directed edges in opposite directions to create a directed graph; if every directed edge is crossed once, it is equivalent to every undirected edge being crossed twice in the original undirected graph. Apply the Directed Eulerian Tour theorem, noting that the in-degree and out-degrees of every vertex are equal, and the result follows immediately.

Lemma 0.1: *Ancillary Vertex Lemma*
Given a connected undirected graph $G = (V, E)$ $\exists v_i \in V$ such that $G \backslash v_i$ (the graph without vertex v_i) is a connected graph.

Proof: Given a connected undirected graph $G = (V, E)$, every vertex is reachable from any vertex in the graph. Therefore, there is a (not necessarily simple) path connecting every vertex $v_i \in V$. Let $v_\alpha, v_{\alpha+1}, \ldots, v_\Omega$ be the sequence of vertexes reached in this path. v_Ω must be reached only once in this sequence. Were v_Ω reached prior to the end of the path, it would not be the last vertex on the path connecting all vertexes, and there is a shorter sequence that reaches every vertex, or we have not yet reached every vertex and must find a longer sequence.
Were we to remove v_Ω, there is a path connecting vertexes in sequence $v_\alpha, v_{\alpha+1}, \ldots, v_{\Omega-1}$, so the subgraph $G \backslash v_\omega$ is connected. □

We use this lemma in the proof that every undirected connected graph has a path that crosses every edge exactly twice and returns to the original vertex.

Proof: Proof by induction on n, the number of vertexes in the graph $G = (V, E)$, i.e. $|V| = n$.
Base case: $n = 1$. No edges to cross, trivially satisfying claim.
Inductive Hypothesis: Suppose true for some undirected connected graph with $|V| = k \geq 1$.
Inductive Step: Given a connected undirected graph G, where $|V| = k + 1$. Using the Ancillary Vertex Lemma, we can remove one vertex v_Ω to yield a connected undirected graph with $|V \backslash v_\Omega| = k$. Apply the inductive hypothesis; a path exists in this subgraph crossing every edge twice and returning to the original vertex. This path crosses through all $v_i \in V \backslash v_\Omega$ adjacent to v_Ω in graph G. Construct the new tour as follows: Every time the original tour hits vertex v_i adjacent to v_Ω for the first time, cross the edge connecting v_i and v_Ω twice.
By induction, we are done. □

5 Hamiltonian Paths

Prove that a complete undirected graph with n vertices, $n \geq 3$, must have a Hamiltonian path. Does it have a Hamiltonian cycle? [Recall that a *complete* graph is one where every vertex has edges to all the other vertices].

–Solution & Exemplar–

Yes, it must have a Hamiltonian cycle.
Direct proof: Every vertex is connected to every other vertex. Thus, for $G = (V, E)$, $|V| = n \geq 3$, where G is complete, we can walk in sequence $v_1, v_2, \ldots, v_n$, as we have edges (v_1, v_2), (v_2, v_3), …, (v_{n-1}, v_n). Since $(v_1, v_n) \in E$ as well, we can complete the Hamiltonian cycle, by construction.