UCLA CS 298 Midterm

Nikola Samardzic

1 Problem 1

We will prove that $\Theta(n^2)$ bits are required to communicate wether the graphs are isomorphic.

Claim 1. $D(f) = O(n^2)$.

Proof. Alice can just communicate the lower triangle of the adjacency matrix of her graph. Since the adjecency matrix is symmetric, the lower triangle will uniquely define it. This will take $\frac{(n-1)(n-2)}{2}$ bits, which is $O(n^2)$. □

Claim 2. $D(f) = \Omega(n^2)$.

Proof. First, notice that isomorphism is an equivalence relation. Since there is a bijection between the sets of symmetric matrices of dimension $n \times n$ and graphs with enumerated nodes with n nodes *via* the adjacency matrix, we will be talking about matrices instead of graphs from now on. Arrange M_f so that equal matrices are in the same row and column and matrices within the same equivalence class are adjacent. This means M_f will have the diagonal equal to one. Along with these ones we will have ones fill in some of the squares that have their diagonal on the main diagonal of the matrix and these squares will not overlap (these squares represent equivalence classes). All other values outside the squares and diagonal will be zeros. Notices that any given graph with n nodes can have at most $n!$ distinct graphs be isomorphic to it (distinct here means that the adjacency matrix representations are not exactly the same). This is simply due to the fact that there are $n!$ permutations of any sequence with n distinct elements. Notice also that the matrix columns that construct a single square (equivalence class) are equal, and thus linearly dependent. Further, any two columns that construct two different squares are linearly independent, because all of the ones in one are zeros in the other and vis versa. There are $2^{\frac{(n-1)(n-2)}{2}}$ $n \times n$ symmetric matrices over $\mathbb{F}_2$ and thus just as many columns in M_f. The side length of each square is at most $n!$, which implies there are at least $\frac{1}{n!}2^{\frac{(n-1)(n-2)}{2}}$ squares. Since the number of squares is equal to the number of independent columns of M_f, we have $rk(M_f) \geq \frac{1}{n!}2^{\frac{(n-1)(n-2)}{2}}$. From here, $D(f) \geq \log rk(M_f) \geq \frac{(n-1)(n-2)}{2} - \log n! \geq \frac{(n-1)(n-2)}{2} - n \log n$ and $D(f) = \Omega(n^2)$. □

From the two claims, we get $D(f) = n^2 + o(n^2)$. ■

2 Problem 2

We will prove via the matrix rank bound that the deterministic complexity of the algorithm is at least $\Omega(n)$. First, let M_n be the matrix for the n-bit version of the problem, arranged so that the rows and columns represent numbers in increasing order starting at 0. Thus, M_f is $2^n \times 2^n$ dimensional. Let X_k be the row number (looking from the top down) of the first 1 in the k-th column looking from above downwards.

Claim 1. For all $k < \lceil 2^{\frac{n}{2}} \rceil$, $X_k = \lceil \frac{2^n}{k} \rceil$. Further, $2^n \leq kX_k < 2^{n+1}$.

Proof. First, prove that $M_n\left(\lceil \frac{2^n}{k} \rceil, k\right) = 1$. Clearly, $M_n(j,k) = 1$ is equivalent to $2^n \leq jk \mod 2^{n+1}$. Also, $k\lceil \frac{2^n}{k} \rceil > k\frac{2^n}{k} > 2^n$. Further, $k\lceil \frac{2^n}{k} \rceil < k\left(\frac{2^n}{k} + 1\right) < 2^n + 2^{\frac{n}{2}} + 1 < 2^{n+1}$, which implies that $\lceil \frac{2^n}{k} \rceil k = \lceil \frac{2^n}{k} \rceil k \mod 2^{n+1}$.

Now prove that for all $j < \lceil \frac{2^n}{k} \rceil$, $M_n(j,k) = 0$. Clearly, $kj < k\frac{2^n}{k} = 2^n$, which implies $M_n(j,k) = 0$. □

Claim 2. For all $i, j < \lfloor 2^{\frac{n}{2}} \rfloor$, $i < j \Rightarrow X_i > X_j$.

Proof. We will prove that for all $k \leq X_j$, $M_n(k,i) = 0$, which implies $X_i > X_j$. Specifically, let's show that $ki < 2^n$, which by claim 1 implies $M_n(k,i) = 0$. So, $ki \leq \lceil \frac{2^n}{j} \rceil i \leq \lceil \frac{2^n}{j} \rceil (j-1) = \lceil \frac{2^n}{j} \rceil j - \lceil \frac{2^n}{j} \rceil \leq \left(\frac{2^n}{j} + 1\right) j - \lceil \frac{2^n}{j} \rceil = 2^n + j - \lceil \frac{2^n}{j} \rceil < 2^n$ because $\lceil \frac{2^n}{j} \rceil \geq \frac{2^n}{j} > \frac{2^n}{2^{n/2}} = 2^{\frac{n}{2}} > j$. □

Claim 2 implies that the first $\lfloor 2^{\frac{n}{2}} \rfloor$ columns of M_n are in reduced row echelon form. Thus, $rk(M_n) \geq 2^{\frac{n}{2}} - 1$ and $D(f) \geq \log rk(M_n) = \Omega(n)$. ■

3 Problem 3

Let M_f be the matrix associated with our problem. Define the matrix $A = [\sum_{i=1}^{n} x_iy_i]_{xy} = \sum_{i=1}^{n}[x_iy_i]_{xy}$. Notice that non-zero entries in A correspond to zeros in M_f. Clearly, $rk_{\mathbb{F}_{18181}}(A) \leq rk_{\mathbb{Q}}(A) \leq \sum_{i=1}^{n} rk([x_iy_i]_{xy}]) = n$. Since 18181 is a prime number, we can conclude by Euler's theorem that for all $k \in \mathbb{F}_{18181}$, $k^{18180} \equiv 1 \mod 18181$, *i.e.* $k^{18180} = 1$ in $\mathbb{F}_{18181}$.

Define the matrix $A' = A \circ A \circ ... \circ A = A^{\circ 18180}$. Notice that $rk(A') \leq rk(A)^{18180} \leq n^{18180}$. Also, all non-zero entries of A become 1 in A' and all zero entries stay equal to zero. This implies that $M_f(x,y) = \neg A'(x,y)$ for all $x, y \in \{0,1\}^n$ and thus any fooling set of M_f is a fooling set of A'. So, $f_s(M_f) = f_s(A') \leq (1 + rk(A'))^2 \leq (1 + n^{18180})^2 < (n^{18180} + n^{18180})^2 = 4n^{2\cdot 18180} < n^{36361}$ for all $n \geq 4$. ■

4 Problem 4

We will prove via rectangle size bound on the ones that $N(f) = \Theta(n)$. Let M_f be the matrix for our problem. Set a uniform probability distribution μ over all the ones in M_f.

Claim 1. There are at least $2^{2(n-18181)}$ ones in M_f.

Proof. For all $x, y \in \{1,0\}^{n-18181}$, let's first demonstrate that there exists at least one pair $(x', y') \in \{1,0\}^{18181} \times \{1,0\}^{18181}$ such that $\sum_{i=1}^{n-18181} x_iy_i + \sum_{i=1}^{18181} x'_iy'_i \equiv 0 \mod 18181$. Set $k = \sum_{i=1}^{n-18181} x_iy_i \mod 18181$. Since $0 \leq k < 18181$, we can choose (x', y') such that $x'_i = y'_i = 1$ for all $1 \leq i \leq 18181 - k$ and $x'_j = y'_j = 0$ for all $18181 - k < j \leq 18181$. This pair obviously satisfies our condition as $\sum_{i=1}^{18181} x'_iy'_i = \sum_{i=1}^{18181-k} x'_iy'_i + \sum_{j=18181-k+1}^{18181} x'_jy'j = 18181 - k$ and thus $\sum_{i=1}^{n-18181} x_iy_i + \sum_{i=1}^{18181} x'_iy'_i = k + (18181 - k) \equiv 0 \mod 18181$.

From here we can see that for all $(x,y) \in \{0,1\}^n \times \{0,1\}^n$, for each pair of values of the first $n - 18181$ bits of both x and y, there are some values for the last 18181 bits of both numbers that give us $\sum x_iy_i \equiv 1 \mod 18181$. There are $2^{2\cdot 18181}$ pairs (x,y) for which the first $n - 18181$ bits are fixed. For each set of such $2^{2\cdot 18181}$ pairs, at least one of the pairs is $\equiv 0 \mod 18181$. Thus, we can partition M_f into $2^{2\cdot(n-18181)}$ sets such that for each set the first $n - 18181$ bits of x and the first $n - 18181$ bits of y are respectively equal. Each one of these sets will contain at least one set (x,y) such that $M_f(x,y) = 1$. Thus, M_f will have at least $2^{2\cdot(n-18181)}$ ones. □

From here we know that $\mu(x,y) \leq 2^{-2\cdot(n-18181)}$ for all $(x,y) \in f^{-1}(1)$.

Claim 2. Every k-dimensional vector space over $\mathbb{F}_{18181}$ has at most 2^{ck} vectors such that all of their elements are in $\{0,1\}$ for some $c \in (0,1]$.

Proof. I can't prove this, but believe there is a proof for $c = 1$ (this fact is used in the conclusion of the problem solution). The argument goes as follows: Let $\{u_1, ..., u_k\}$ be a set of basis vectors for the vector space. I believe that this basis set can be chosen so that each of the u_i's controls solely some subset of the dimensions of the vector space. That is, for all i, there exists a k such that $(u_i)_k \neq 0$ and $(u_j)_k = 0$ for all $j \neq i$ (*e.g.* $(1,1,0)$ controls the first two dimensions, and in the basis $\{(1,1,0),(1,0,0)\}$ it solely controls the second dimension). From here it is obvious that if a vector v whose elements are only from $\{0,1\}$ is in the vector space it is defined by a linear combination of the basis vectors $\lambda_1u_1 + ... + \lambda_ku_k$ and that the solely controlled dimensions for a specific vector u_i have to all be 0 or 1 in v for all i and also that all of the values of v in dimensions that are not sole dimensions of any of the basis vectors u_i are uniquely determined by the values in the fields that are sole dimensions for the u_i's. This directly implies that there could be at most 2^k vectors with all elements from $\{0,1\}$ in the vector space, as any of those vectors is uniquely defined by choosing wether the sole dimensions of each of the basis vectors will be set to 0 or 1 and there are k basis vectors in total. Note also that not all combinations of values of 0 or 1 of the sole dimensions may be in the vector space. However, this is just used as a convenient upper bound. □

Claim 3. All 1-monochromatic rectangles on M_f have less than 2^n elements.

Proof. Let $R = A \times B$ be a 1-monochromatic rectangle on M_f. Then for all $(x,y) \in span(A) \times span(B)$, $x \cdot y = 0$, because two sets of orthogonal vectors must span orthogonal subspaces. Note that here $span(X)$ means all linear combinations of vectors in X over $\mathbb{F}_{18181}$ and that the inner product is also over F_{18181}. Now let $A' = span(A) \cap \{0,1\}^n$, $B' = span(A) \cap \{0,1\}^n$ and $R' = A' \times B'$. Then, R' is clearly 1-monochromatic. Notice that $|R'| \geq |R|$. Further, $dim(A') + dim(B') \leq n$ as A' and B' are orthogonal over $\mathbb{F}_{18181}$. [1] Thus, $|R| \leq |R'| = |A| \cdot |B| \leq 2^{dim(A')+dim(B')} \leq$

[1] Here we use the linear algebra fun fact that for all n-dimensional vector spaces V over a field F and subspaces U of V, $dim(U) + dim(U^\perp) = n$. This we prove by looking at the linear transformation $T_u : V \to F$ defined as $T_u(x) = x^Tu$. Then $U^\perp = \cap_{u \in U} \ker T_u$. Now we fix a set of basis vectors for U, $\{u_1, ..., u_k\}$ and let $T : V \to F^k$ be defined as $T(x) = (x^Tu_i)_{i=1}^{k}$. Notice that $U^\perp = \ker T$ and by rank-nullity theorem $U^\perp = n - dim[im(T)]$. Now see that $dim[im(T)] = k$, as the matrix that defines the linear transformation T is $(u_1, ..., u_k)$, which has rank k since the u_i's form a basis. Thus $dim[U^\perp] = n - k$. Link to proof source.

2^n. □

Claims 1 and 3 show that $RS(f) \leq RS_\mu(f) = \max_R \mu(R) \leq 2^n \cdot 2^{-2(n-18181)} = 2^{-n+2\cdot 18181}$. By Theorem 4.7, $N(f) \geq \log \frac{1}{RS(f)} \geq \log\left(2^{n-2\cdot 18181}\right) = n - 2\cdot 18181$. Further, we know that $N(f) \leq n$, as the protocol were Alice sends all of her bits to Bob is deterministic and has complexity n and $N(f) \leq D(f)$. Thus, $N(f) = \Theta(n)$ and specifically $N(f) = n + o(n)$. ■

5 Problem 5

It is clear that $\Theta(n^2)$ bits are sufficient, as Alice can communicate a basis of its vector space to Bob, and Bob can then deterministically determine if the two subspaces are orthogonal. The basis can always be communicated in at most n^2 bits, as the basis can contain a maximum of n vectors, each of which contains exactly n bits (assuming here that the vector spaces are over $\mathbb{F}_2$).

Thus, we are left to prove that $N(f) = \Omega(n^2)$.

Claim 1. The number of k-dimensional subspaces of an n-dimensional vector space over the field $\mathbb{F}_q$ for any prime number q is given by the *Gaussian binomial coefficient*: $\binom{n}{k}_q = \frac{(1-q^n)(1-q^{n-1})...(1-q^{n-k+1})}{(1-q)(1-q^2)...(1-q^k)}$, for all $k < n$.

Proof. Linear subspaces are defined by the linear basis that spans them. Let's follow through with a combinatorial argument. The first vector of the basis can be chosen from $q^n - 1$ vectors (any vector except 0). The second vector can be selected from $q^n - q$ vectors (any vector except the q multiples of the first). The third vector can be selected from $q^n - q^2$ vectors (any vector except the q^2 linear combinations of the first two). And so on...

This will give us the number of ordered linearly independent vectors that span all the k-dimensional subspaces of the original space: $(q^n - 1)(q^n - q)...(q^n - q^{k-1})$. However, we have over-counted the number of k-dimensional vector spaces as one k-dimensional vector is spanned by multiple sets of basis vectors. How many? To get the number of k-dimensional subspaces, we need to divide the number of ordered linearly independent vectors that span k-dimensional subspaces of the original subspace by the number of ordered linearly independent vectors that span a specific k-dimensional vector space.

By an analogy to the problem we already solved, the number of ordered linearly independent vectors that span a specific k-dimensional vector space is $(q^k - 1)(q^k - q)...(q^k - q^{k-1})$. This gives us $\frac{(1-q^n)(1-q^{n-1})...(1-q^{n-k+1})}{(1-q)(1-q^2)...(1-q^k)}$. □

Claim 2. Any $\lfloor \frac{n}{2} \rfloor$-dimensional subspace has a unique $\lceil \frac{n}{2} \rceil$-dimensional orthogonal complement.

Proof. Both existence and uniqueness is the direct consequence of the theorem in the footnote of Problem 4 as $\lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil = n$, *i.e.* we use the fact that the orthogonal complement exists and is unique.

Now define the matrix of this problem M_f with rows and columns corresponding to subspaces of the original vector space.

Claim 3. M_f has a fooling set of size at least $\binom{n}{\lfloor \frac{n}{2} \rfloor}_2$.

Proof. Let S be the set of all $\lfloor \frac{n}{2} \rfloor$-dimensional vector subspaces. Let T be the set of all $\lceil \frac{n}{2} \rceil$-dimensional vector subspaces. Directly from claim 2 and the fact that $\binom{n}{\lfloor \frac{n}{2} \rfloor}_2 = \binom{n}{\lceil \frac{n}{2} \rceil}_2$ we know that there is a bijection $g : S \to T$ such that $M_f(x, g(x)) = 1$ and $M_f(x, y) = 0$ for all $y \neq g(x)$. Thus, the set $\{(x, f(x)) : x \in S\}$ is a 1 fooling set of M_f. □

Thus, $N(f) \geq \lceil \log fs_1(f) \rceil \geq \log \binom{n}{\lfloor \frac{n}{2} \rfloor}_2 = \log \left[\frac{2^n - 1}{2^{n/2} - 1} \cdot \frac{2^{n-1} - 1}{2^{n/2-1} - 1} \cdot ... \cdot \frac{2^{n-n/2} - 1}{2 - 1}\right] \geq \log\left[(2^{n/2} - 1)^{n/2}\right] > \log\left[2^{\frac{n^2}{8}}\right] = \frac{n^2}{8}$.

Thus, $N(f) = \Theta(n^2)$ ■

6 Problems 6 and 7

I was not able to make meaningful progress on these problems.