1. Computability, Complexity and Algorithms

(a) Let G be the complete graph on n vertices, and let $c : V(G) \times V(G) \to [0, \infty)$ be a symmetric cost function. Consider the following *closest point heuristic* for building a low cost traveling salesman tour. Begin with a trivial tour consisting of a single arbitrarily chosen vertex. At each step, identify the vertex u that is not on the tour but whose distance to a vertex on the tour is minimum. Suppose that the vertex on the tour that is nearest to u is v. That is, $c(u, v) = \min\{c(u', v') : u' \text{ is not in the tour, } v' \text{ is in the tour}\}$. Extend the tour to include u by inserting u just after v. More precisely, if the tour consists of the single vertex v, then replace it by the tour vuv. Otherwise pick an edge vw of the tour, remove it from the tour and add the edges vu and uw instead. Repeat until all vertices are on the tour. Prove that, if the cost function satisfies the triangle inequality, then the closest point heuristic returns a tour whose total cost is not more than twice the cost of an optimal tour.

(b) Show how, in polynomial time, we can transform one instance of the general traveling salesman problem (i.e. when the cost function is not guaranteed to satisfy triangle inequality) into another instance whose cost function satisfies triangle inequality and such that the two instances have the same optimal tours. Can such a polynomial time transformation be used to obtain a factor 2 approximation algorithm for the general traveling salesman problem? Justify your answer.

Solution: (a) The key observation is that vertices are added to the tour in the same order that Prim's algorithm would add them towards constructing an MST, and at cost twice that of an MST. The proof below formalizes this idea.

Let u_i and v_i be the critical vertices identified in iteration i. Suppose that prior to the insertion of u_i to the tour v_i was connected to w, and the insertion of u_i caused the removal of edge $\{v_i, w\}$ and the addition of edges $\{v_i, u_i\}$ and $\{u_i, w\}$. By triangle inequality we have $c(u_i, w) \leq c(v_i, w) + c(v_i, u_i)$, thus $c(u_i, w) - c(v_i, w) \leq c(v_i, u_i)$. Thus, the total increase of the cost of the tour during iteration i is $2c(v_i, u_i) = 2x_i$. And the cost of the output tour is $2\sum_{i=2}^{n} x_i$. Note further that Prim's MST algorithm, starting from the same initial vertex v_1, would have added vertices to an MST at the same order $v_2, v_3, \ldots, v_n$ and at cost $\sum_{i=2}^{n} x_i$. We also know that the MST cost lower bounds the cost of the optimal tour. The above combined imply that the cost of the output tour of the closest point heuristic is at most twice the cost of an optimal tour.

(b) Let I be an instance of the general TSP consisting of n cities and let $c_{ij} = c_{ji}$ be the distance between cities i and j. Let $m = \max_{i,j} c_{ij}$ be the maximum distance. We construct an instance I' by setting $c'_{ij} = c_{ij} + m$. To see that I' satisfies triangle inequality notice that for any three cities i, j and k we have: $c'_{ij} = c_{ij} + m \leq m + m \leq (c_{ik} + m) + (c_{kj} + m) = c'_{ik} + c'_{kj}$.

We first argue that every optimal tour for I is an optimal tour for I'. Let T be an optimal tour for I that has cost C. The cost of T in I' is $C + nm$. Suppose that there is a tour T' in I' with cost $C' < C + nm$. But then the cost of T' in I would be $C' - nm < C$, which contradicts the assumption that T is an optimal tour for I. Therefore T is also an optimal tour for I'.

We similarly argue that every optimal tour for I' is an optimal tour for I. So let T' be an optimal tour for I' that has cost C'. The cost of T' in I is $C' - nm$. Suppose that there is a tour T is I with cost $C < C' - nm$. But then the cost of T in I' would be $C + nm < C'$, which contradicts the assumption that T' is an optimal tour for I'. Therefore T' is also an optimal tour for I.

The above polynomial time transformation cannot be used to construct a factor 2 polynomial time approximation algorithm for the general TSP. In particular, let I be an instance of the general TSP and let I' be corresponding instance of TSP with triangular inequality that results from the above transformation. Using a factor 2 polynomial time approximation algorithm for I', we obtain a tour T' of cost C' with the guarantee that $C' \leq 2\text{OPT}(I')$. However, the cost of T' in I is $C = C' - nm$. We may thus write $C \leq 2\text{OPT}(I') - nm = 2\left(\text{OPT}(I) + nm\right) - nm$, or $C \leq 2\text{OPT}(I) + nm$, which does not constitute a factor 2 approximation guarantee.

In fact, we can further show that for the general TSP, no polynomial time algorithm can give a factor 2 approximation, unless P = NP. In particular, let $G(V, E)$ be an instance of the (undirected) HC (Hamilton Cycle) problem which is known to be NP complete, and suppose we have a polynomial time algorithm $\mathcal{A}$ that approximates general TSP upto factor 2. Construct an instance I of general TSP as follows: There are n vertices and all edges between these vertices are present. If an edge $\{i, j\} \in E$ then set the cost $c_{ij} = c_{ji} = 1$. If an edge $\{i, j\} \notin E$ then set the cost $c_{ij} = c_{ji} = n + 2$. Now realize that, if $G(V, E)$ has a HC then $\text{OPT}(I) = n$, while if $G(V, E)$ does not have a HC then $\text{OPT}(I) \geq (n - 1) + (n + 2) = 2n + 1$. Therefore, if we run algorithm $\mathcal{A}$ on input I then, if $G(V, E)$ has a HC $\mathcal{A}$ will output a tour of cost at most $2n$, while if $G(V, E)$ does not have a HC $\mathcal{A}$ will output a tour of cost at least $2n + 1$. This immediately allows us to decide if $G(V, E)$ is Hamiltonian.

2. Analysis of Algorithms

(a) Recall that most known problems in the class NP exhibit the property of self-reducibility. Given an oracle for the decision version of the problem, this property helps yield a polynomial time algorithm for finding a solution to a "YES" instance of the problem. Give a proof of self-reducibility for the problem CLIQUE: Given an graph G and a number k, find a clique of size k in G.

(b) Recall the Isolating Lemma:
Let S be a set, $|S| = n$, and F be a family of subsets of S. Assign random weights to elements of S from $\{1, 2, \ldots, 2n\}$. Then with probability at least 1/2, there is a unique minimum weight set in F.

In this lemma, the weight of a set $A \in F$ is defined to be the sum of weights of elements in A. Prove the same lemma if the weight of a set $A \in F$ is defined to be the *product* of weights of elements in A.

Solution: **(a)** The self-reducibility tree will have (G, k) at root, with children:
A) Pick vertex v_1 in clique and let G_1 be the induced graph on the neighbors of v_1. The first child is $(G_1, k - 1)$—it corresponds to including v_1 in clique.
B) Remove v_1 from G to obtain graph G_2. The second child is (G_2, k)—corresponds to not including v_1 in clique.

(b) The argument is identical to the case when weight of a set is defined to be the sum of weights of elements.

3. Theory of Linear Inequalities

For a matrix A having m rows and a set $S \subseteq \{1, ..., m\}$, let A_S denote the submatrix of A consisting of the rows indexed by S. Let $\mathbf{1}$ denote the vector consisting of all 1's.

Let A be an $m \times n$ integral matrix and let b be a rational vector such that the linear system $Ax \leq b$ has at least one solution. Show that $Ax \leq b$ is totally dual integral if and only if (1) the rows of A form a Hilbert basis and (2) for each subset S of at most n inequalities from $Ax \leq b$, the linear programming problem $\min\{y^T b : y^T A = \mathbf{1}^T A_S,\ y \geq 0\}$ has an integral optimal solution.

Solution is available upon request.

4. Combinatorial Optimization

Let $\mathcal{S}$ be a finite set, let $X_1, \ldots, X_t$ be a partition of $\mathcal{S}$, and let $Y_1, \ldots, Y_l$ be a partition of $\mathcal{S}$. Consider the polytope P defined by $x \in \mathbb{R}^{\mathcal{S}}$ such that

$$\begin{aligned}&x(u) \geq 0 \text{ for all } u \in \mathcal{S},\\ &x(X_i) \leq 1 \text{ for all } 1 \leq i \leq t,\\ &x(Y_i) \leq 1 \text{ for all } 1 \leq i \leq l.\end{aligned}$$

Show that P is integral.

Solution. Let $\mathcal{M}_1$ be the partition matroid with ground set $\mathcal{S}$ defined by the partition $X_1, \ldots, X_t$, and similarly let $\mathcal{M}_2$ be the partition matroid defined by the partition $Y_1, \ldots, Y_l$. Let the respective rank functions be r_1 and r_2. The rank of a set Z in $\mathcal{M}_1$ is the number of distinct indices i such $Z \cap X_i \neq \emptyset$. Thus, for all $Z \subseteq \mathcal{S}$ and for all indices i, $r_1(Z) = r_1(Z \cap X_i) + r_1(Z \setminus X_i)$. It follows that set Z is non-separable in $\mathcal{M}_1$ if and only if $Z \subseteq X_i$ for some index i. Also, if $Z \subseteq X_i$ for some index i and $x \in X_i$, then $r_1(Z) = r_1(Z \cup \{x\})$. We conclude that the non-separating flats of the matroid $\mathcal{M}_1$ are exactly the sets $X_1, X_2, \ldots, X_t$. Thus, the matroid polytope of $\mathcal{M}_1$ is given by $x \in \mathbb{R}^{\mathcal{S}}$ such that

$$\begin{aligned}&x(u) \geq 0 \text{ for all } u \in \mathcal{S}\\ &x(X_i) \leq 1 \text{ for all } 1 \leq i \leq t.\end{aligned}$$

Equivalently, this set of inequalities implies every inequality of the form $x(Z) \leq r_1(Z)$ for all $Z \subseteq \mathcal{S}$. Similarly, the matroid polytope of $\mathcal{M}_2$ is given by $x \in \mathbb{R}^{\mathcal{S}}$ such that $x(u) \geq 0$ for all $u \in \mathcal{S}$ and $x(Y_i) \leq 1$ for all $1 \leq i \leq l$. The statement now follows from the characterization of the matroid intersection polytope.

The statement can also be shown by defining an auxiliary bipartite multigraph G as follows. The vertex set of G is $X_1, \dots, X_t, Y_1, \dots, Y_l$ and edges of G are $\{e_x : x \in \mathcal{S}\}$. To see the how the endpoints of e_x are defined, consider an element $x \in \mathcal{S}$. Let i and j be defined such that $x \in X_i$ and $x \in Y_j$. Then the edge e_x has one endpoint equal to X_i and one end equal to Y_j. The statement now follows as a restatement of the matching polytope in G.

5. Graph Theory

Let $k \geq 1$ be an integer, let G be a 2-connected graph, let x, y be distinct vertices of G, and assume that every vertex of G other than x or y has degree at least k. Prove that G has a path with ends x and y of length at least k.

Solution: We proceed by induction on k. The statement clearly holds for $k = 1$; thus we assume that $k \geq 2$ and that the statement holds for $k - 1$. Let $G' := G \backslash x$. If G' is 2-connected, then let $x' \in V(G') - \{y\}$ be a neighbor of x. It exists, because G is 2-connected. Notice that every vertex of G' other than y has degree at least $k - 1$. By induction there exists a path P' in G' from x' to y of length at least $k - 1$; then $P' + x$ is as desired. Thus we may assume that G' is not 2-connected, and hence $G' = A \cup B$, where A and B are subgraphs of G' such that $|V(A) \cap V(B)| = 1$ and $V(A) - V(B) \neq \emptyset \neq V(B) - V(A)$. We may assume that $y \in V(B)$, and that A is minimal. It follows that A is a block is 2-connected or isomorphic to K_2. Let y' be the unique vertex in $V(A) \cap V(B)$. Since G is 2-connected, x has a neighbor $x'' \in V(A) - \{y'\}$. By induction the graph A has a path P from x'' to y' of length at least $k - 1$. Let Q be a path in B from y' to y. Then $P \cup Q + x$ is as desired.

6. Probabilistic methods

Let $v_1, v_2, \dots v_n$ be n vectors from $\{\pm 1\}^n$ chosen uniformly and independently. Let M_n be the largest pairwise dot product in absolute value: i.e

$$M_n = \max_{i \neq j} |v_i \cdot v_j|$$

Prove that

$$\frac{M_n}{2\sqrt{n \ln n}} \to 1$$

in probability as $n \to \infty$.

Hint. Consider the first and second moment methods applied to the number of pairs of vectors whose dot product exceeds (and falls below, respectively) $2\sqrt{n \ln n}$.

Solution: To show $\frac{M_n}{2\sqrt{n \ln n}}$ converges to 1 in probability we must show that for every $\epsilon > 0$,

$$\Pr[\left|\frac{M_n}{2\sqrt{n \ln n}} - 1\right| > \epsilon] \to 0 \text{ as } n \to \infty$$

Therefore it is enough to show the following two facts:

1. $\Pr[M_n \geq (1+\epsilon)2\sqrt{n \ln n}] \to 0$
2. $\Pr[M_n \geq (1-\epsilon)2\sqrt{n \ln n}] \to 0$

To prove 1. we use the first-moment method. Let X be the number of pairs of vectors with dot product $\geq (1+\epsilon)2\sqrt{n \ln n}$. If $M_n \geq (1+\epsilon)2\sqrt{n \ln n}$, then $X \geq 1$. We will use Markov's Inequality, $\Pr[X \geq 1] \leq \mathbb{E}X$. We write

$$X = X_{1,2} + \dots + X_{i,j} + \dots$$

where $X_{i,j} = 1$ if $|v_i \cdot v_j| \geq (1+\epsilon)2\sqrt{n \ln n}$ and 0 otherwise.

$$\mathbb{E}X_{i,j} = \Pr[|v_i \cdot v_j| \geq (1+\epsilon)2\sqrt{n \ln n}] = \exp\left(-2(1+\epsilon)^2 \ln n(1+o(1))\right)$$

using a Chernoff bound, since $v_i \cdot v_j$ is distributed as a simple symmetric random walk of n steps, and so

$$\begin{aligned}\mathbb{E}X &= \binom{n}{2}\mathbb{E}X_{i,j} \\ &\leq \frac{n^2}{2}\frac{1}{n^{2(1+\epsilon)^2}} = o(1)\end{aligned}$$

which proves 1.

To prove 2. we use the second-moment method. Let Y be the number of pairs of vectors with dot product $\geq (1-\epsilon)2\sqrt{n \ln n}$. Similar to the above, we let $Y_{i,j} = 1$ if $|v_i \cdot v_j| \geq (1-\epsilon)2\sqrt{n \ln n}$ and 0 otherwise. Then we have

$$\begin{aligned}\mathbb{E}Y &= \binom{n}{2}\mathbb{E}Y_{i,j} \\ &\geq \frac{n^2}{2}\frac{1}{n^{2(1-\epsilon)^2}} = \omega(1)\end{aligned}$$

To bound the variance, we write

$$\begin{aligned}\operatorname{var}(Y) &= \sum_{i \neq j} \operatorname{var}(Y_{i,j}) + \sum_{(i,j) \neq (k,l)} \operatorname{cov}(Y_{i,j}, Y_{k,l}) \\ &\leq \mathbb{E}Y + \sum_{(i,j) \neq (k,l)} \operatorname{cov}(Y_{i,j}, Y_{k,l})\end{aligned}$$

Now if (i,j) and (k,l) are disjoint pairs of pairs of vectors, then $Y_{i,j}$ and $Y_{k,l}$ are independent and so have covariance 0. If they overlap, say $Y_{i,j}$ and $Y_{i,k}$, the covariance is still 0: conditioned on $v_i \cdot v_j$, $v_i \cdot v_k$ still has the distribution of a SSRW of n steps. And so all the covariances are 0, giving $\operatorname{var}(Y) \leq \mathbb{E}(Y)$. Then we apply Chebyshev:

$$\Pr[Y=0] \le \frac{\mathrm{var}(Y)}{(\mathbb{E}Y)^2} \le \frac{1}{\mathbb{E}Y} = o(1)$$

which completes the proof of 2.

7. Algebra

Let F be a finite field with cardinality q.

(i) For how many $a \in F$ does the polynomial $x^5 - a$ have a root in F?

(ii) For how many $a \in F$ does the polynomial $x^5 - a$ split completely into linear factors over F?

Express your answers in terms of q.

Solution: For $a = 0$ there is clearly a root (and x^5 splits into linear factors over F). For $a \neq 0$, the polynomial $x^5 - a$ has a root in F if and only if a is in the image of the homomorphism $\varphi : F^\times \to F^\times$ defined by $x \mapsto x^5$. By the first isomorphism theorem (for groups), $F^\times/\ker(\varphi) \cong \mathrm{im}(\varphi)$. Concretely, $\ker(\varphi)$ consists of all fifth roots of unity in F, so it is cyclic of order 1 or 5. Since $|\ker(\varphi)|$ divides $|F^\times| = q-1$, if $5 \nmid q-1$ then $\ker(\varphi)$ is trivial and $\mathrm{im}(\varphi) = q-1$. If $5 \mid q-1$ then $x^5 - 1$ divides $x^{q-1} - 1$, and since $x^{q-1} - 1$ splits into linear factors over F it follows that $|\ker(\varphi)| = 5$. Thus $\mathrm{im}(\varphi) = (q-1)/5$ in this case. In summary (adding in $a = 0$), the answer to the question (i) is

$$\begin{cases} q & \text{if } q \not\equiv 1 \pmod 5 \\ \frac{q-1}{5} + 1 & \text{if } q \equiv 1 \pmod 5. \end{cases}$$

For (ii), note first that if $5 \mid q$ then $x^5 - a = (x-\alpha)^5$ for some $\alpha \in F$, and in particular the polynomial splits into linear factors for all q values of a. Suppose, therefore, that $5 \nmid q$. If $a \neq 0$ and $x^5 - a$ splits completely into linear factors over F, then the ratio of two roots would be a primitive 5th root of unity in F, which generates a subgroup of order 5 in $F^\times$, and hence $5 \mid q-1$. Conversely, if $5 \nmid q-1$ then the argument above shows that all primitive 5th roots of unity belong to F and thus as soon as $x^5 - a$ has a single root in F it splits completely into linear factors over F. So the answer to question (ii) is

$$\begin{cases} 1 & \text{if } q \not\equiv 0,1 \pmod 5 \\ q & \text{if } q \equiv 0 \pmod 5 \\ \frac{q-1}{5} + 1 & \text{if } q \equiv 1 \pmod 5. \end{cases}$$

7. Linear Algebra

Given $A \in \mathbb{R}^{m\times n}$ with $m > n$ and $\underline{j} = (j_1, \ldots, j_n) \in [1,m]^n$, call $A^{\underline{j}}$ the $n \times n$ minor of A formed by the j_i-th, $i = 1, \ldots, n$, rows of A. Given $A, B \in \mathbb{R}^{m\times n}$ show that

$$\det(A^T B) = \sum_{\underline{j}\in J} \det(A^{\underline{j}}) \det(B^{\underline{j}}),$$

where J is the set of multi-indexes $\underline{j}$ such that $1 \leq j_1 < j_2 < \ldots < j_n \leq m$. Use the above to show that

$$\det(A^T B)^2 \leq \det(A^T A)\det(B^T B).$$

Solution: We have

$$\det(A^T B) = \sum_{\sigma\in S^n}(-1)^\sigma \prod_{i=1}^{n}\sum_{j=1}^{m} A_{j,i}B_{j,\sigma(i)} = \sum_{\sigma\in S^n}\sum_{\underline{j}\in[1,m]^n}(-1)^\sigma\prod_{i=1}^{n} A_{j_i,i}B_{j_i,\sigma(i)}$$

where S^n is the set of permutation on n elements. Obesrve now that, given $\underline{j}\in[1,m]^n$, if $j_i = j_{i'}$ then for every $\sigma\in S^n$ we can consider $\tau\in S^n$ such that $\tau(i) = \sigma(i')$, $\tau(i') = \sigma(i)$ and $\tau(l) = \sigma(l)$ for $l \neq i, i'$. We get

$$\prod_{i=1}^{n} A_{j_i,i}B_{j_i,\sigma(i)} = \prod_{i=1}^{n} A_{j_i,i}B_{j_i,\tau(i)}$$

while $(-1)^\sigma = -(-1)^\tau$. We can thus replace the sum over $\underline{j}\in[1,m]^n$ with a sum over $\underline{j}$ such that $j_i \neq j_i'$ for $i \neq i'$. This is equivalent to summing on $\underline{j}\in J$ and permuting the elements of $\underline{j}$. More precesely

$$\det(A^T B) = \sum_{\sigma\in S^n}\sum_{\underline{j}\in J}\sum_{\tau\in S^n}\prod_{i=1}^{n}(-1)^\sigma A^{\underline{j}}_{\tau(i),i}B^{\underline{j}}_{\tau(i),\sigma(i)} = \tag{1}$$

$$= \sum_{\underline{j}\in J}\left(\sum_{\tau\in S^n}\prod_{i=1}^{n}(-1)^\tau A^{\underline{j}}_{\tau(i),i}\right)\left(\sum_{\sigma\in S^n}\prod_{i=1}^{n}(-1)^\sigma B^{\underline{j}}_{\sigma(i),i}\right) = \tag{2}$$

$$= \sum_{\underline{j}\in J}\det(A^{\underline{j}})\det(B^{\underline{j}}). \tag{3}$$

The last inequality follows by observing that

$$\det(A^T B)^2 = \left(\sum_{\underline{j}\in J}\det(A^{\underline{j}})\det(B^{\underline{j}})\right)^2 \leq \tag{4}$$

$$\leq \left(\sum_{\underline{j}\in J}\det(A^{\underline{j}})\det(A^{\underline{j}})\right)\left(\sum_{\underline{j}\in J}\det(B^{\underline{j}})\det(B^{\underline{j}})\right) = \tag{5}$$

$$= \det(A^T A)\det(B^T B). \tag{6}$$