15-859FF: Coping with Intractability **CMU, Fall 2019**
HW #3 (out Tuesday Oct 15, 2019) **Due:** Thursday Oct 31, 2019

You may discuss all problems on this HW with others, but groups of size at most 3, please. Please write down the names of your collaborators. Also, you should write your solutions yourself.

Exercises

Exercises are for fun and edification, please do not submit. **But do solve them, we may need ideas from there later in the course, or even in this HW!**

1. In the Odd Cycle Transversal (OCT) problem, we are given an undirected graph G and an integer k, and the goal is to determine if one can find k edges such that removing these eliminated all odd cycles (equivalently makes the graph bipartite). Prove that OCT is in FPT when parameterized by solution size k.

2. Given two positive integers m, n, recall the extended Euclidean algorithm that find integers a, b such that $am + bn = \gcd(m, n)$.

   (a) To show that the algorithm runs in time polynomial in the number of bits to represent m, n, let $\min(m, n) \in [F_k, F_{k+1})$ where F_k is the kth Fibonacci number. Show, by induction, that the Euclidean algorithm takes at most k iterations. Finally, using that $F_k = \Theta(\phi^k)$ for ϕ being the golden ratio, infer that the number of iterations is $O(\log \min(m, n))$.

   (b) Show that when $m = F_k$ and $n = F_{k+1}$, the algorithm actually takes $\Omega(k)$ rounds.

3. Given any matrix B, the following operations are called *unimodular*: (i) swap two columns, (ii) negate the entries of some column, and (iii) add an integer multiple of some column to another column. If A is obtained from B using unimodular operations, show that $|det(A)| = |det(B)|$.

4. Show that matrix U is unimodular iff U^{-1} is unimodular.

5. (You saw this on Piazza.) Recall that the determinant is a multilinear antisymmetric function mapping its columns to scalars. (I.e., it's a linear function of any column when you fix the other cols, and that swapping two cols flips the sign.) Also, for square matrices, $det(AB) = det(A)det(B)$. Now consider a matrix $B \in \mathbb{R}^{d \times d}$, whose columns are linearly independent vectors $b_1, b_2, \ldots, b_d$ in $\mathbb{R}^d$. We think of these d vectors as a basis.

   (a) Only for this first part, assume the b_is are orthogonal, so $\langle b_i, b_j \rangle = 0$ for all $i \neq j$. (Here the braket notion denotes the inner product, so $\langle x, y \rangle = x^\intercal y = \sum_{i=1}^d x_i y_i$. Then infer that $|det(B)| = \prod_i \|b_i\|$, the product of the norms of the vectors.

   (b) Now don't assume orthogonality any more. Run the Gram-Schmidt orthogonalization algorithm on the columns of B (in this order) to get vectors $b_1^*, b_2^*, \ldots, b_d^*$, where $b_1^* = b_1$ and each subsequent b_i^* is orthogonal to the preceding vectors. Let matrix B' contain these new vectors as columns. Show that the determinants are unchanged, i.e.,$det(B') = det(B)$.

   (c) Consider the parallelopiped $P := \{\sum_i \lambda_i b_i \mid \lambda_i \in [0, 1) \ \forall i\} = \{B\lambda \mid \lambda \in [0, 1)^d\}$. Show that $vol(P)$, the volume of this P, is given by $|det(B')| = |det(B)|$. (Start with $d = 2$, and draw a picture.)

(d) Consider the linear transformation $f(x) := Tx$ given by a matrix $T \in \mathbb{R}^{d \times d}$. Observe that the volume of the parallelopiped given by the transformed vectors $Tb_1, \ldots, Tb_n$ is given $|det(T)|vol(P)$.

6. In the basis reduction algorithm for the 2-dimensional case, we stopped when $\|b_1\| \leq \|b_2\|$ and $\mu = \frac{\langle b_1, b_2 \rangle}{\langle b_1, b_1 \rangle} \in [-1/2, 1/2]$. If $\|b_2\| < \|b_1\|$, we swapped the two and repeated. Show that it suffices to stop when $\|b_2\| \geq \|b_1\|(1 - \varepsilon)$. Show that if we are start with integer-valued linearly-independent vectors b_1, b_2, this algorithm stops in time $O(\log \frac{\min(\|b_1\|, \|b_2\|}{\varepsilon})$.

Problems

The Cygan et al book provides hints to its problems. Please try to solve these problems yourself before looking at these hints! Recall the notation $O^*(c^n)$ to denote $O(c^n \text{poly}(n))$; this helps avoid repeating polynomial factors in many places below. Please solve any four of the six problems.

1. Early in the course, we saw that vertex cover on 3-uniform hypergraphs is in FPT when parameterized by the size of the vertex cover. Prove that assuming P $\neq$ NP, vertex cover on 3-uniform hypergaphs is not in FPT when parameterized by the size of vertex cover above some arbitrary matching (in particular above the size of the maximum matching).

   Formally, the parameter is now $k - \nu$, where k is the size of the optimal vertex cover, and ν is the size of the largest matching in the hypergraph. Recall that a matching in a 3-uniform hypergraph is a collection of vertex disjoint hyperedges.

2. Exercises 3.21 and 3.22 of the text.

3. Given a graph $G = ([n], E)$, define an $n \times n$ matrix T where we set $T_{ij} = x_{ij}$ if $i < j$ and $(i, j) \in E$, $T_{ij} = -x_{ji}$ if $i > j$ and $(i, j) \in E$, and $T_{ij} = 0$ otherwise. Show that G contains a perfect matching if and only if $det(T)$ is not identically zero.

   (Hint; Observe that every nonzero term in the expansion of the determinant corresponds to a digraph where every vertex has in-degree and out-degree 1 and is only connected to neighbors in the original (undirected) graph. This digraph must be a union of disjoint directed cycles. What happens when there is an odd-length cycle?)

   What is the degree of the polynomial $P(x) := det(T)$? Use the Schwartz-Zippel Lemma to show that substituting independent random values from the field $\mathbb{F}_q$ (where prime $q \in [2n, 4n]$), computing the determinant of the resulting matrix (over this field), and returning `Yes` if and only if the answer is non-zero, is correct with probability at least 1/2.

4. A square matrix U is *unimodular* if its entries are integer-valued, and $|det(U)| = 1$. Show that a matrix is unimodular if and only if it can be converted to the identity matrix by performing unimodular operations. (See Exercise 3 for the definition of unimodular operations.) Hint: the extended Euclidean algorithm.

5. Recall Minkowski's theorem about the presence of short vectors in lattices. We now give an algorithmic version.

   (a) Give an polynomial-time algorithm that takes a lattice Λ (described by a basis B), and finds a lattice point of Euclidean length at most $2^{cd}|det(\Lambda)|^{1/d}$, for some absolute constant $c > 0$. (Note that the runtime should be polynomial even in d.)

Now we can use the above part to give an algorithmic version of Dirichlet's simultaneous approximation theorem. Consider the $d+1$-dimensional lattice generated by the basis

$$B = \begin{pmatrix} 1 & & & & & \alpha_1 \\ & 1 & & 0 & & \alpha_2 \\ & & 1 & & & \alpha_3 \\ & & & 1 & & \alpha_4 \\ & 0 & & & 1 & \alpha_d \\ & & & & & \varepsilon/Q \end{pmatrix}.$$

Let $b_1, \ldots, b_n$ be its columns.

(a) Suppose we find a non-zero vector $v := \sum_i \lambda_i b_i$ in this lattice with $\|v\| \leq \varepsilon$. Then argue that (i) $\lambda_{d+1} \neq 0$, and (ii) $|\lambda_i + \alpha_i \lambda_{d+1}| \leq \varepsilon$ for all $i = 1, \ldots, d$. Use this to find $p_i, q \in \mathbb{Z}$ with $0 < q \leq Q$ and $|\frac{p_i}{q} - \alpha_i| \leq \frac{\varepsilon}{q}$ for all i.

(b) Finally, show that by setting $Q := 2^{c(d+1)(d+1)}\varepsilon^{-d}$, we can find such a non-zero vector v in poly(d) time. Assume that arithmetic operations on numbers of size poly($d, \log \|B\|_\infty$) can be done in polynomial time. The size of a number is measured by how many bits it takes to write it.

6. Show that any lattice Λ admits a basis B such that the shortest vector of Λ can be written as $\sum_i \lambda_i \mathbf{b}_i$, where each $\lambda_i \in \mathbb{Z}$ has absolute value at most $f(d)$. Use this to give an exact algrithm to find a shortest vector in Λ in FPT time $g(d)\text{poly}(n)$. *(Hint: consider the LLL basis.)*