

Theory Qual

Fall 2017

Please answer all four questions below.

1. Let M be a finite automaton over the alphabet Σ with transition function $\delta : Q \times \Sigma^* \mapsto Q$. A *reset sequence* for M is a string $s \in \Sigma^*$ such that $\delta(q, s)$ is independent of $q \in Q$.
 - (a) Exhibit a finite automaton M that does not have a reset sequence.
 - (b) Show that there exists a constant c such that, if M has a reset sequence, then there exists one of length $|Q|^c$.
Hint: $c = 3$ works, but you will get full credit for any constant c .

2. For this problem you are to consider symbols (such as English letters) composed of lines and curves joined together. Such a symbol is called *traceable* if it can be drawn in one long stroke, without lifting the pencil.

For example, the symbols **E** and **A** are not traceable, but **C** and **M** are. (There are to be no “serifs” on these, for example **C** is just one arc.)

- (a) Under what condition(s) is a symbol traceable? Prove your answer is correct.
- (b) The *tracing number* of a symbol is the minimum number of times the pencil must be lifted to draw the symbol. For example, traceable symbols have tracing number 0. Give an efficient algorithm for computing the tracing number.

When answering these questions, explain how symbols are to be represented.

3. A *linear binary code* C of length n is a subspace of \mathbb{Z}_2^n . Such a code can be described by a generator matrix $G \in \mathbb{Z}_2^{k \times n}$ with $k = \dim(C)$ where the rows of G form a basis of C .

Two linear binary codes C_0 and C_1 of length n are called equivalent if there exists a permutation $\pi \in S_n$ such that

$$C_1 = \pi(C_0) \doteq \{\pi(x) \mid x \in C_0\}, \quad (1)$$

where $\pi(x) \doteq (x_{\pi(1)}, \dots, x_{\pi(n)})$.

In the Linear Code Equivalence problem (LCE) you are given two linear binary codes C_0 and C_1 of length n in the form of generator matrices, and need to decide whether there exists $\pi \in S_n$ such that (1) holds.

- (a) Establish a search-to-decision reduction for LCE, i.e., a polynomial-time reduction from finding a permutation π satisfying (1) to LCE.
 - (b) Show that graph isomorphism polynomial-time reduces to LCE.
4. A 3-4-Ising system is defined as follows:

Input: An undirected graph $G = (V, E)$

Output: $Z(G) = \sum_{\sigma: V \rightarrow \{0,1\}} 3^{m_=} 4^{m_{\neq}}$, where $m_=$ (resp. m_{\neq}) is the number of edges $e = (u, v) \in E$ such that $\sigma(u) = \sigma(v)$ (resp. $\sigma(u) \neq \sigma(v)$).

- (a) Prove that if one can approximate the number of independent sets of any bipartite graph within a factor 2 in polynomial time, then one can approximate the number of independent sets of any bipartite graph within any factor $(1 + \epsilon)$ in time polynomial in $1/\epsilon$ and the size of the graph.
- (b) Let $u, v \in V$ and $e = (u, v) \in E$. Consider the following construction, with some parameter k : Let $X_u = \{x_1, x_2, \dots, x_k\}$, $Y_u = \{y_1, y_2, \dots, y_k\}$, and $E_u = X_u \times Y_u$, then $(X_u \cup Y_u, E_u)$ forms a complete bipartite graph. Similarly define (X_v, Y_v, E_v) . Let $Z_e = \{s_e, s'_e, t_e, t'_e\}$, and

$$E_e = \{(s_e, s'_e), (t_e, t'_e)\} \cup (X_u \times \{s_e\}) \cup (Y_u \times \{t_e\}) \cup (X_v \times \{s'_e\}) \cup (Y_v \times \{t'_e\}),$$

all viewed as unordered pairs. Now describe the set of all independent sets of

$$(X_u \cup Y_u \cup X_v \cup Y_v \cup Z_e, E_u \cup E_v \cup E_e)$$

- (c) Prove that if we have an oracle that can approximate the number of independent sets of any bipartite graph within a factor 2, then we can approximate $Z(G)$ within a factor $1 + \epsilon$ in time polynomial in $|V|/\epsilon$.

G O O D L U C K !!