1. Show that the set of all finite bitstrings $\{0,1\}^*$ is countable.
2. Describe a Turing machine that computes function $y = 2x + 1$.
3. Show that $3n^2 + 6n + 7 = O(n^2)$.
4. Show that $2n^3 + 6n^2 + 6n + 1 = O(n^3)$.
5. Show that $n^3 \neq O(n^2)$.
6. Show that $n! \neq O(2^n)$.
7. Find functions $f(n)$ and $g(n)$ such that $f(n) = O(g(n))$, $g(n) \neq O(f(n))$, and $f(n) \neq o(g(n))$.
8. Given a list of functions in asymptotic notation, order them by growth rate (slowest to fastest).
9. Show that

$$\begin{array}{llllllllll} (a) & \Theta(n \log_2 n) & (b) & \Theta(n^2) & (c) & \Theta(n) & (d) & \Theta(1) & (e) & \Theta(2^n) \\ (f) & \Theta(n^3) & (g) & \Theta(n!) & (h) & \Theta(\log_2 n) & (i) & \Theta(n^2 \log_2 n) & (j) & \Theta(2^n \log^2 n) \end{array}$$

10. Check if the following conditions are true

$$\begin{array}{ll} (a) & \Theta(n+30) = \Theta(3n-1) \ , \\ (b) & \Theta(n^2 + 2n - 10) = \Theta(n^2 + 3n) \ , \\ (c) & \Theta(n^3 \cdot 3n) = \Theta(n^2 + 3n) \ . \end{array}$$

11. Write each of the following functions in O notation.

$$(a) \quad 5 + 0.001n^3 + 0.025n \qquad (b) \quad 500n + 100n^{1.5} \qquad (c) \quad 0.3n + 5n^{1.5} + 2.5n^{1.75}$$

12. Reduce SAT to 3–coloring.
13. Reduce 3–coloring to SAT.
14. Reduce SAT to clique.
15. Reduce clique to independent set.
16. Reduce clique to vertex cover.
17. Reduce independent set to vertex cover.
18. Reduce DDHP to DLP.
19. Reduce CDHP to DLP.
20. Reduce DDHP to CDHP.

21. Is graph G shown in Fig. 2 3–colorable? In case it is 3–colorable, provide a valid 3-coloring as a proof. If it is not 3-colorable, how could we prove this fact?

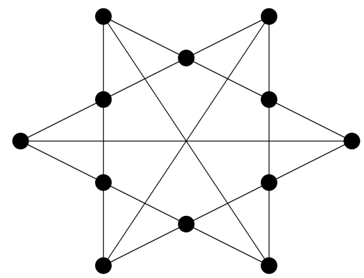

Figure 1: Graph G

22. Find a clique in the graph G below.

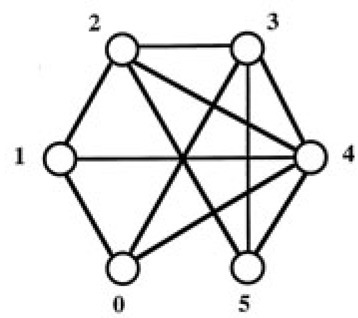

Figure 2: Graph G

1 Problem Definitions

Definition 1 (Boolean satisfiability problem (SAT))**.** The problem of determining if there exists an interpretation that satisfies a given Boolean formula.

Definition 2 (k–colorability problem)**.** Given a graph, decide if it can be colored using k colors such that no two adjacent vertices are colored with the same color.

Definition 3 (Clique problem)**.** The problem of determining the existence of a complete subgraph (a subset of vertices all adjacent to each other) in a given graph.

Definition 4 (Independent set problem)**.** The problem of determining the existence of a subset of vertices of a graph, such that no two vertices are adjacent in this subset.

Definition 5 (Vertex cover problem)**.** The problem of determining the existence of a subset of vertices of a graph that includes at least one endpoint of every edge of the graph.

Definition 6 (Discrete logarithm problem (DLP))**.** Given a multiplicative cyclic group G, its generator g, an element $h \in G$, find k such that $h^k = h$ in G.

Definition 7 (Computational Diffie–Hellman problm (CDHP))**.** Given a triplet (g, g^a, g^b) of elements of a multiplicative cyclic group G generated by g, for $a, b \in Z_n$, n being the number of elements in G, compute g^{ab} in G.

Definition 8 (Decisional Diffie–Hellman problem (DDHP))**.** Given a triplet (g^a, g^b, g^c) of elements of a multiplicative cyclic group G generated by g, decide whether $g^c = g^{ab}$ in G.