1. Alice and Bob generate a session key using the Diffie-Hellman key establishment protocol. They agree on a finite cyclic group $\mathbb{Z}_{23}^{\times}$ generated by 5. What is the order of $\mathbb{Z}_{23}^{\times}$? Suppose that Alice's private exponent is 2, and Bob's private exponent is 3, what is the session key generated by Alice and Bob?

2. Consider the following key agreement protocol between Alice (A) and Bob (B). Prior to starting any communication, Alice and Bob generate their secret keys ω_A and ω_B. Alice generates the session key K. To share K with Bob, the following sequence of messages is executed.

   (1) Alice $\rightarrow$ Bob: $\omega_A \oplus K$.

   (2) Bob $\rightarrow$ Alice: $\omega_B \oplus \omega_A \oplus K$

   (3) Alice $\rightarrow$ Bob: $\omega_A \oplus \omega_B \oplus \omega_A \oplus K = \omega_B \oplus K$

   After receiving the last message, Bob computes $\omega_B \oplus \omega_B \oplus K = K$. At this point Alice and Bob have the shared key K which they use to encrypt the communication. Can adversary Carol obtain the key K by eavesdropping on the communication channel?

3. Provide prime factorization of the following integers:

   (a) 64 $\quad$ (b) 120

   (c) 375 $\quad$ (d) 47

4. Given a list of functions in asymptotic notation, order them by growth rate (slowest to fastest).

   $(a)\ \Theta(n \log_2 n)$ $\quad (b)\ \Theta(n^2)$ $\quad (c)\ \Theta(n)$ $\quad (d)\ \Theta(1)$ $\quad (e)\ \Theta(2^n)$

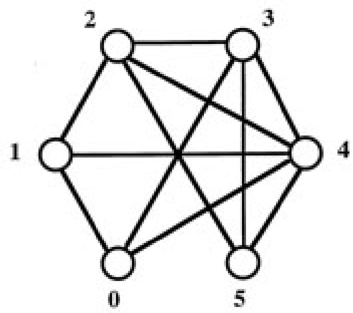
   $(f)\ \Theta(n^3)$ $\quad (g)\ \Theta(n!)$ $\quad (h)\ \Theta(\log_2 n)$ $\quad (i)\ \Theta(n^2 \log_2 n)$ $\quad (j)\ \Theta(2^n \log^2 n)$

5. Check if the following conditions are true

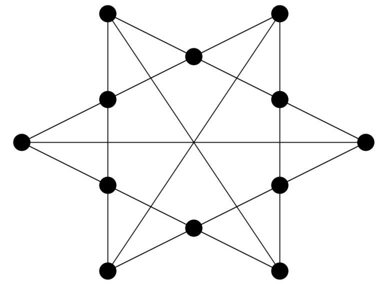
   $$(a)\quad \Theta(n+30) = \Theta(3n-1)\ ,$$
   $$(b)\quad \Theta(n^2+2n-10) = \Theta(n^2+3n)\ ,$$
   $$(c)\quad \Theta(n^3 \cdot 3n) = \Theta(n^2+3n)\ .$$

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

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



(a) Maximal clique problem

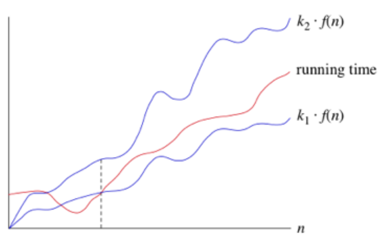


(b) graph 3-coloring program

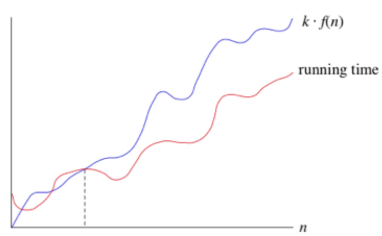
7. Find the maximal clique in the graph shown in Fig. 1a. A subgraph H of a graph G is a maximal clique in G if there is an edge between every pair of vertices in H, and there is no vertex in $G \setminus H$ conntected to every vertex in H.

8. Provide a 3-coloring of the graph shown in Fig. 1b so that any two adjacent vertices do not share the same color.

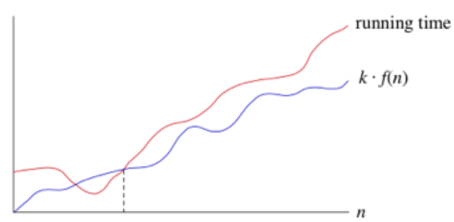
Asymptotic Bounds of Functions



(a) Growth rate is $\Theta(f(n))$



(b) Growth rate is $O(f(n))$



(c) Growth rate is $\Omega(f(n))$

Θ notation

The assertion $f(n) = \Theta(g(n))$ means that $f(n)$ is asymptotically bounded from above and from below by $g(n)$. See Fig. 2a Formally written

$$f(n) = \Theta(g(n)) \Longleftrightarrow \exists \varepsilon, k > 0, \exists n_0 \forall n > n_0 : \varepsilon \cdot g(n) \leqslant f(n) \leqslant k \cdot g(n) \ .$$

Big O notation

The assertion $f(n) = O(g(n))$ means that $f(n)$ asymptotically grows at most as fast as $g(n)$. It provides an asymptotic upper bound, without specifying a lower bound. See Fig. 2b. Formally written

$$f(n) = O(g(n)) \Longleftrightarrow \exists k > 0 \exists n_0 \forall n > n_0 : f(n) \leqslant k \cdot g(n) \ .$$

Ω notation

The assertion $f(n) = \Omega(g(n))$ means that $f(n)$ asymptotically grows at least as fast as $g(n)$. It provides an asymptotic lower bound without specifying an upper bound. See Fig. 2c. Formally written

$$f(x) = \Omega(g(x)) \Longleftrightarrow \exists\varepsilon > 0 \exists n_0 : \forall n > n_0 f(n) \geqslant \varepsilon \cdot g(n) \ .$$

Little o notation

The assertion $f(x) = o(g(x))$ means that $g(x)$ asymptotically grows much faster than $f(x)$.

$$f(x) = o(g(x)) \Longleftrightarrow \forall\varepsilon > 0 \exists n_o \forall n > n_0 : f(n) < \varepsilon \cdot g(n) \ .$$

In example, $2x = o(x^2)$, and $\frac{1}{x} = o(1)$. It can be seen that $2x^2 = O(x^2)$, but $2x^2 \neq o(x^2)$.

Little ω notation

The assertion $f(n) = \omega(g(n))$ means that $f(n)$ asymptotically grows much faster than $g(n)$.

$$f(x) = \omega(g(x)) \Longleftrightarrow \forall k > 0 \exists n_0 \forall n > n_0 : f(n) > k \cdot g(n) \ .$$