1 Định nghĩa thời gian đa thức

Theo sách

@booksilverman2008introduction, title=An introduction to mathematical cryptography, author=Silverman, Joseph H and Pipher, Jill and Hoffstein, Jeffrey, volume=1, year=2008, publisher=Springer

Định nghĩa: Giả sử chúng ta đang cố gắng giải quyết một loại bài toán toán học nhất định, trong đó đầu vào của bài toán là một số có kích thước có thể thay đổi. Ví dụ, hãy xem xét Bài Toán Phân Tích Số Nguyên Tố, đầu vào của bài toán là một số N và đầu ra là một thừa số nguyên tố của N. Chúng ta quan tâm đến việc biết thời gian cần thiết để giải bài toán này theo kích thước của đầu vào. Thông thường, người ta đo kích thước của đầu vào bằng số bit của nó, vì đó là lượng bộ nhớ cần thiết để lưu trữ đầu vào.

Giả sử rằng có một hằng số $A \geq 0$, không phụ thuộc vào kích thước của đầu vào, sao cho nếu đầu vào có độ dài $O(k)$ bit, thì nó mất $O(k^A)$ bước để giải bài toán. Khi đó bài toán được gọi là có thể giải được trong thời gian đa thức.

2 Tại sao LLL lại chạy trong thời gian đa thức

Ta có bổ đề giới hạn độ dài cơ sở LLL: Giả sử rằng chúng ta có một cơ sở $v_1, v_2, \ldots, v_n \in \mathbb{R}^m$ cho một lưới L là LLL giảm, thì bất đẳng thức sau đây đúng:

$$\|v_1\|^2 \leq 2^{n-1}\|x\|^2$$

đối với mọi $x \in L$ với $x \neq 0$.

Bổ đề 4.2

Xét cơ sở $v_1, v_2, ..., v_n \in \mathbb{R}^m$ cho lưới L được rút gọn bởi thuật toán LLL. Khi đó:

$$\|v_1\|^2 \leq 2^{\frac{n-1}{2}}\|x\|^2 \quad (14)$$

đối với mọi $x \in L$, với $x \neq 0$.

Về cơ bản, Bổ đề 4.2 nói rằng độ dài của v_1, vectơ đầu tiên của cơ sở được rút gọn bởi thuật toán LLL, không vượt quá $2^{\frac{n-1}{2}}$ lần độ dài của bất kỳ vectơ $x \in L$, bao gồm cả vectơ ngắn nhất. Một lần nữa, chúng ta có thể thay thế hằng số trong (Điều kiện Lovász 4) bằng δ để có được kết quả tổng quát hơn:

$$\|v_1\| \leq \frac{4}{4\delta - 1} \cdot 2^{\frac{n-1}{2}}\lambda(L)$$

Người ta cũng thường làm việc với $\delta = \frac{1}{4} + \frac{3}{4}\frac{n}{n-1}$ để đảm bảo $\delta < 1$ và đảm bảo thời gian chạy đa thức của thuật toán LLL. Khi đó, chúng ta có phiên bản đơn giản hơn:

$$\|v_1\| \leq \frac{2}{\sqrt{3}} \cdot n\lambda(L)$$

Điều này dẫn đến hàm xấp xỉ $\psi(n) = \frac{2}{\sqrt{3}} \cdot n$. Mặc dù là cấp số nhân trong thứ hạng của mạng, nhưng kết quả này vẫn là một thành tựu vì hàm gần đúng không phụ thuộc vào kích thước đầu vào và thuật toán LLL lần đầu tiên cho phép giải quyết SVP chính xác theo chiều cố định [9].