**Một số vấn đề liên quan đến dàn**

**và áp dụng vào thám mã**

**1.Định nghĩa và một số tính chất của dàn.**

**2.Một số bài toán trên dàn.**

**3.Thuật toán tìm cơ sở thu gọn của dàn.**

**4.Áp dụng vào thám mã.**

**1.1 Định nghĩa dàn**

●Chuẩn trong  : với  .

● là một *dàn* nếu là một *nhóm cọng con rời rạc* của .

Rời rạc: 

●Phần tử sinh của dàn: , kí hiệu .

Nếu là một dàn, ta bảo rằng sinh bởi hay  là các phần tử sinh ra dàn .

Nếu thêm  là độc lập tuyến tính, ta bảo hệ là một cơ sở của *L*.

●Số chiều của dàn: số lớn nhất các vector độc lập tuyến tính trong dàn , kí hiệu .

●

● ●

● ●

● ●

●v2 ●

●v1

● ●

●

● ●

**Dàn trong R2 với cơ sở v1,v2.**

**1.2 Cơ sở của dàn**

**●**Tồn tại cơ sở:là dàn trong ,  và  là các vector

độc lập tuyến tính trong . Tồn tại ma trận tam giác dưới sao cho

các vector  xác định bởi tạo thành một cơ sở của .

● Ma trận chuyển đổi giữa 2 cơ sở của dàn có các phần tử nguyên

và định thức bằng .

● Nếu  là hệ độc lập tuyến tính trong  thì tập 

là một dàn với .

**1.3 Miền cơ bản**

● là một cơ sở của *L*. *Miền cơ bản* (*hình bình hành cơ bản*) *của L* là tập



● là một dàn với số chiều *n* và *F* là miền cơ bản của *L*. Khi đó mỗi vector

sẽ có biểu diễn duy nhất dạng  với  và .

**●** Định thức của dàn: *F* là miền cơ bản của dàn *L*, độ đo hay thể tích của *F* là 

sẽ được gọi là *định thức của dàn L* và kí hiệu là *det(L).*

**● ●**

**● ● ●**

**● ●**

**● ●v4 ●**

**●V2 ●**

**F(v1,v2) ●v3 ●**

**● ● ●**

**●V1 ●**

**● ● ●**

**Hai miền cơ bản tương ứng với hai cơ sở v1, v2 và v3, v4.**

**1.3 Miền cơ bản (tt).**

**●** Bất đẳng thức Hadamard:  là cơ sở của dàn L và F là miền cơ bản thì

.

● Tính định thức của dàn: Giả sử  là dàn với cơ sở  . Khi đó nếu thì  trong đó.

● Giả sử  là một dàn có số chiều *n*. Khi đó  là một bất biến của dàn, không phụ thuộc vào cơ sở.

**2. Một số bài toán trên dàn.**

Cho  là một dàn, .

●Bài toán tìm vector ngắn nhất (SVP-The Shortest Vector Problem):

Tìm  mà .

●Bài toán tìm vector gần nhất (CVP-The Closest Vector Problem):

cho trước , tìm mà .

●Bài toán tìm cơ sở ngắn nhất (SBP-The Shortest Basis Problem): tìm cơ sở  của L ngắn nhất theo một nghĩa nào đó, chẳng hạn  hay .

●Bài toán tìm vector xấp xỉ ngắn nhất:

cho  là một hàm theo *n*, tìm  mà .