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

Trước hết ta nhắc lại rằng với , không gian là không gian định chuẩn trên với chuẩn của phần tử được định nghĩa bởi:

.

**1.1 Định nghĩa.**Một tập hợp khác rỗng được gọi là một *dàn* nếu là một *nhóm cọng con rời rạc* của .

Ở đây tính chất rời rạc có nghĩa là tồn tại số sao cho với mọi thì .

Chú ý rằng định nghĩa trên không cho ta một hình ảnh hình học về dàn. Sau đây ta sẽ đưa ra một định nghĩa tương đương về dàn, định nghĩa này cho phép hình dung rõ ràng hơn về mặt hình học.

Giả sử  là các vector trong . Ta kí hiệu  là tập gồm các tổ hợp tuyến tính của  với hệ số nguyên, tức là

.

Rõ ràng  là một nhóm cọng con của , tuy nhiên không nhất thiết có tính chất rời rạc. Chẳng hạn khi , tập  là không rời rạc. 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 , như vậy mỗi vector trong dàn sẽ biểu diễn dưới dạng một tổ hợp tuyến tính với hệ số nguyên qua các vector trong cơ sở.

Số lớn nhất các vector độc lập tuyến tính trong một dàn được gọi là *số* *chiều* (dimension) hoặc *hạng* (rank) của và được kí hiệu bởi . Nếu  là một dàn với thì ta bảo có chiều đầy đủ. Trong trường hợp thì rõ ràng trong luôn tồn tại vector độc lập tuyến tính, nhưng các vector này có thể không tạo thành một cơ sở của . Tuy nhiên định lý sau đây chỉ ra rằng ta luôn xây dựng được một cơ sở của từ các vector này.

**1.2 Định lý.** Giả sử là một dàn trong ,  và  là các vector độc lập tuyến tính trong . Khi đó sẽ tồn tại ma trận tam giác dưới sao cho các vector  xác định bởi tạo thành một cơ sở của .

*Chứng minh.* Với , xét tập hợp .

Tập hợp này là hữu hạn do nếu  thì và tập  là hữu hạn, ngoài ra do . Do đó tồn tại phần tử dương bé nhất của , kí hiệu là . Theo định nghĩa , sẽ tồn tại các phần tử sao cho . Ta sẽ chứng minh rằng  là một cơ sở của .

Do nên hệ  là độc lập tuyến tính. Với thì do hệ  là hệ độc lập tuyến tính tối đại, sẽ tồn tại các số sao cho . Kí hiệu  và đặt , ta có  và . Nếu tất cả các  không nguyên, ta kí hiệu  là chỉ số lớn nhất mà , khi đó và  nếu . Từ



do ta có mâu thuẩn với  là phần tử bé nhất của . ■

Bây giờ giả sử  là một cơ sở của dàn L và  là một cơ sở khác. Do  là cơ sở nên mỗi vector  có thể biểu diễn qua cơ sở này:

.

Ma trận chuyển đổi cơ sở từ  sang  là . Khi đó ma trận chuyển cơ sở ngược lại là ma trận . Do các phần tử của  và  là các số nguyên nên  là các số nguyên. Từ tính chất  ta có ngay . Ngược lại nếu  thì ma trận  sẽ có các phần tử là các số nguyên và do đó  là một cơ sở của L. Điều này chứng tỏ:

**1.3 Định lý.** Ma trận chuyển đổi giữa hai cơ sở của dàn có các phần tử nguyên và định thức bằng .

Như vậy, một dàn bất kỳ trong  đều tồn tại một cơ sở. Cho dù tập có dạng  là một dàn hay không, một dàn bất kỳ đều có dạng với  là hệ độc lập tuyến tính. Điều ngược lại sau đây có thể chứng minh dễ dàng.

**1.4 Định lý.** Nếu  là hệ độc lập tuyến tính trong thì tập  là một dàn với .

Như không gian vector, một dàn có nhiều cơ sở. Phần tiếp theo sẽ khảo sát một khái niệm mới, bất biến qua cơ sở của dàn.

**1.5 Định nghĩa.** Giả sử *L* là một dàn với số chiều *k* và là một cơ sở của *L*. *Miền cơ bản* (hay *hình bình hành cơ bản*) *của L*, được định nghĩa là tập



Định lý sau đây cho biết vì sao miền cơ bản đóng vai trò quan trọng trong việc khảo sát dàn.

**1.6Mệnh đề.** Giả sử 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 .

*Chứng minh.* Giả sử  là cơ sở của L và . Khi đó  cũng là một cơ sở của . Do đó vector sẽ có biểu diễn  với . Bằng cách viết  dưới dạng  với  và , ta có  với  và . Bây giờ giả sử với  và . Nếu  và  thì . Do  là độc lập tuyến tính, ta có ngay  hay . Vì  và nên . Vậy và ■

Như vậy miền cơ bản sẽ phụ thuộc vào cơ sở của dàn. Phần tiếp theo giới thiệu một đặc trưng của miền cơ bản không phụ thuộc vào cơ sở.

**1.7 Định nghĩa.** Giả sử *L* là một dàn với số chiều bằng *n* và *F* là miền cơ bản của *L*. Độ đo hay thể tích của *F* là  sẽ được gọi là *định thức của dàn L* và kí hiệu là *det(L).*

Trong trường hợp *n=2*, nếu 2 vector cơ sở của dàn *L* vuông góc nhau thì ta có . Tổng quát hơn ta có bất đẳng thức sau.

**1.8 Mệnh đề.(bất đẳng thức Hadamard)** Nếu L là một dàn với cơ sở  và F là miền cơ bản thì .

Mệnh đề sau đây cho cách tính định thức của dàn L theo các vector cơ sở của nó.

**1.9 Mệnh đề.** Giả sử  là dàn với số chiều *n* và  là miền cơ bản của *L* ứng với cơ sở  . Khi đó nếu thì định thức của *L* tính bởi công thức  trong đó.

*Chứng minh.* Độ đo hay thể tích của  trong  được tính bởi

.

Thực hiện phép đổi biến số từ các biến  sang các biến  với . Rõ ràng ma trận Jacobian của phép đổi biến số trên là  và miền cơ bản F là ảnh của hình hộp đơn vị  qua phép đổi biến, do đó .■

Một hệ quả của mệnh đề trên là định thức của dàn không phụ thuộc vào cơ sở của dàn, được khẳng định bởi mệnh đề sau.

**1.10 Hệ quả.** Giả sử  là một dàn có số chiều n. Khi đó mọi miền cơ bản của L đều có cùng thể tích. Do đó định thức  là một bất biến của dàn, không phụ thuộc vào cơ sở.

*Chứng minh.* Giả sử  và  là hai cơ sở của *L*, và là các miền cơ bản của L tương ứng với 2 cơ sở này và ,  là các định thức tương ứng (định nghĩa ở mệnh đề 1.9). Nếu kí hiệu A là ma trận chuyển cơ sở từ  sang  thì

.

Do đó

 





 (do *|det(A)|=1* theo mệnh đề 1.3)

. ■

**2. Một số bài toán trên dàn.**

Cho  là một dàn, .

**2.1 Bài toán tìm vector ngắn nhất (SVP-The Shortest Vector Problem).**

Tìm  mà .

**2.2 Bài toán tìm vector gần nhất (CVP-The Closest Vector Problem).**

cho trước , tìm mà .

**2.3 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 .

**2.4 Bài toán tìm vector xấp xỉ ngắn nhất:**

cho  là một hàm theo *n*, tìm  mà .

Chú ý rằng trong một số trường hợp, việc giải các bài toán trên là rất đơn giản. Chẳng hạn giả sử L có một cơ sở trực giao là .

Bài toán SVP: do vector sẽ có biểu diễn nên . Từ đây ta có ngay vector có độ dài ngắn nhất trong các vector  chính là lời giải của bài toán SVP.

Bài toán CVP: với  và  ta có .

Từ đây, lời giải của bài toán CVP là vector *v* tương ứng với các hệ số là các số nguyên gần  nhất.

**3. Tìm cơ sở thu gọn của dàn.**

Phần này trình bày 2 thuật toán tìm cơ sở thu gọn của một dàn cho trước. Đó là thuật toán Gauss trong trường hợp 2 chiều và tổng quát là thuật toán LLL. Các thuật toán này đóng vai trò quan trọng trong việc giải các bài toán ở phần 2 và áp dụng nhiều trong lĩnh vực thám mã.

**3.1 Thuật toán Gauss.**

Giả sử là một dàn,  và  là một cơ sở đã biết của *L*. Thuật toán Gauss cho phép từ cơ sở  xây dựng một cơ sở khác có độ dài ngắn hơn. Ý tưởng của Gauss là thay  bằng  với . Tuy nhiên do  có thể không nguyên nên có thể , do đó ta thay  với .

**3.1.1Mệnh đề.** Nếu thực hiện theo thuật toán sau:

***Loop***

***If***  ***then*** hoán đổi .

Tính .

***If*** m=0 ***then*** STOP ***Else*** .

***EndLoop***.

Ta sẽ thu được cơ sở mới với là vector ngắn nhất của *L*. Hơn nữa nếu  là góc giữa  thì  và .

*Chứng minh.* Ta chỉ chứng minh  là vector ngắn nhất của *L.* Thật vậy, khi thuật toán kết thúc ta phải có  và  (\*).

Một vector bất kỳ sẽ có dạng , khi đó:

 





 (do (\*))

 ( do )



 (chú ý  do  ).■

3.1.2 Ví dụ. (tấn công RSA trong trường hợp khóa yếu)

(Public Key Cryptanalysis, Phong Q. Nguyen, Recent Trends in Cryptography, 2008)

Xét hệ mã hóa RSA trong trường hợp  và các số là cùng chiều dài bit. Ta có các ước lượng sau:

.

Do  nên .

Như vậy, nếu đặt  thì .