SỬ DỤNG MAPLE ĐƯA DẠNG TOÀN PHƯƠNG KHÔNG SUY BIẾN TRÊN TRƯỜNG HỮU HẠN VỀ DẠNG CHÍNH TẮC

Nguyễn Duy Ái Nhân*, Trần Công Mẫn

Khoa Toán, Trường Đại học Khoa học, Đại học Huế

*Email: nguyenduyainhan.t2b@gmail.com

Ngày nhận bài: 18/3/2020; ngày hoàn thành phản biện: 14/4/2020; ngày duyệt đăng: 14/7/2020

TÓM TẮT

Các dạng toàn phương có hạng lớn hơn hoặc bằng 2 trên trường hữu hạn F_q, với q là lũy thừa của một số nguyên tố khác 2, luôn biểu diễn mọi phần tử của nhóm nhân các phần tử khác không F_q^*. Chính vì vậy, mọi dạng toàn phương không suy biến với hạng bằng n trên trường F_q, với n là số nguyên dương, luôn tương đương với dạng chính tắc

$$X_1^2 + \cdots + X_{n-1}^2 + X_n^2$$

hoặc

$$X_1^2 + \cdots + X_{n-1}^2 + aX_n^2$$

tùy thuộc vào biệt thức của dạng toàn phương đó có là một bình phương hay không. Với ý tưởng như vậy cùng việc sử dụng phần mềm Maple, bài báo đưa ra các đoạn lệnh lập trình để đưa một dạng toàn phương không suy biến trên trường hữu hạn F_q về dạng chính tắc, đồng thời chỉ ra ma trận chuyển cơ sở để thu được dạng chính tắc đó.

Từ khóa: dạng toàn phương, trường hữu hạn, phần mềm Maple.

1. MỞ ĐẦU

Cho V là không gian vectơ n-chiều trên trường K. Một dạng toàn phương trên V là một hàm $Q: V \to K$ thỏa mãn hai điều kiện

a) $Q(av) = a^2 Q(v)$ với mọi $a \in K$ và với mọi $v \in V$,

b) hàm $f: V \times V \to K$

$$(u, v) \mapsto Q(u + v) - Q(u) - Q(v)$$

là một dạng song tuyến tính.

Nếu Q là một dạng toàn phương trên V thì dạng song tuyến tính đối xứng

$$(\cdot): \quad V \times V \to K$$
$$(u, v) \mapsto u \cdot v = \frac{1}{2}[Q(u+v) - Q(u) - Q(v)]$$

gọi là tích vô hướng liên kết với Q trên V.

Với Q là một dạng toàn phương trên V và $S = \{e_1, \dots, e_n\}$ là một cơ sở của V, kí hiệu $a_{ij} = e_i \cdot e_j$ và đặt $A = \left[a_{ij}\right]_{n\times n} \in M(n, K)$ ta có A là một ma trận đối xứng, ma trận này được gọi là ma trận của dạng toàn phương Q ứng với cơ sở S của V và định thức của ma trận A được gọi là biệt thức của Q. Khi $v = \sum_{i=1}^{n} x_i e_i$ là một vecto bất kì của V, ta có

$$Q(v) = \sum_{1\le i,j\le n} a_{ij} x_i x_j = x^T A x$$

trong đó $x = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ là tọa độ của v đối với cơ sở S. Vì vậy, mọi dạng toàn phương trên K-không gian vecto n-chiều V đều có thể xem như là một đa thức thuần nhất bậc 2 theo n biến với hệ số trên K. Nếu ta đổi cơ sở $S = \{e_1, \dots, e_n\}$ sang cơ sở $S' = \{e_1', \dots, e_n'\}$ thì luôn tồn tại ma trận khả nghịch C, C là ma trận chuyển cơ sở từ S sang S', sao cho $x = Cx'$ với $x' = \begin{bmatrix} x_1' \\ \vdots \\ x_n' \end{bmatrix}$ là tọa độ của v đối với cơ sở S'. Khi đó,

$$Q(v) = x'^T (C^T A C) x'$$

ma trận A' của Q đối với cơ sở S' là $C^T AC$, với C^T là ma trận chuyển vị của C, và $\det(A') = \det(A)\,(\det(C))^2$.

Hai dạng toàn phương được gọi là tương đương nếu tồn tại ma trận khả nghịch C sao cho $C^T AC = A'$ trong đó A và A' lần lượt là ma trận của hai dạng toàn phương đã cho.

Trong [1], tác giả đã chỉ ra rằng nếu Q là dạng toàn phương với hạng lớn hơn hoặc bằng 2 (tương ứng, lớn hơn hoặc bằng 3) trên trường hữu hạn F_q, với q là lũy thừa của một số nguyên tố khác 2, luôn biểu diễn mọi phần tử khác không của F_q (tương ứng, mọi phần tử của F_q). Do đó, luôn tồn tại phần tử v_0 của V sao cho $Q(v_0) = 1$. Chính vì vậy, bằng cách lấy phần bù trực giao theo tích vô hướng liên kết với Q thì mọi dạng toàn phương với hạng n, với n lớn hơn hoặc bằng 2, luôn tương đương với một trong hai dạng $X_1^2 + \cdots + X_n^2$ hoặc $X_1^2 + \cdots + X_{n-1}^2 + aX_n^2$ (gọi là dạng chính tắc) tùy thuộc vào biệt thức có dạng là một bình phương hay không.

2. KẾT QUẢ

Trong [3], nhóm tác giả đã đưa ra các đoạn lệnh lập trình bằng phần mềm Maple để đưa dạng toàn phương không suy biến có hạng bằng 3 trên trường F_q về dạng chính tắc và chỉ ra cơ sở tương ứng. Trong trường hợp hạng của dạng toàn phương lớn hơn 3, việc tìm ma trận chuyển cơ sở để đưa ra dạng chính tắc phức tạp hơn.

Trong bài báo này, sau khi áp dụng [4] để rút ra ma trận của dạng toàn phương với hệ số trên trường hữu hạn F_q có đặc số khác 2, chúng tôi điều chỉnh các đoạn lệnh trong [3] và thiết lập vòng lặp để giải quyết vấn đề trong trường hợp dạng toàn phương có hạng lớn hơn hoặc bằng 2 tùy ý.

```
> restart:
  with(linalg): with(LinearAlgebra): with(student):
```

2.1. Kiểm tra dạng toàn phương và rút ra ma trận của dạng toàn phương. [4]

```
> matran := proc (tp, p)
    global A;
    local n, i, j, Ct, Ctrg, tp1, k, Xt;
        n := nops(indets(tp));
        tp1 := tp;
        for i to n do
            tp1 := subs(x[i] = k*x[i], tp1)
        end do;
        if is(tp1 = k^2*tp) = false then
            ERROR(`Dang toan phuong cho sai`)
        end if;
        A := Matrix(n, n);
        for i to n do
              A[i, i] := coeff(tp, x[i]^2) mod p;
              for j from i+1 to n do
                    A[i, j] := coeff(coeff(tp, x[i]), x[j])/2 mod p;
                    A[j, i] := A[i, j] mod p;
              end do
        end do;
        print(`Ma tran dang toan phuong A =`, A)
end proc;
```

2.2. Tìm vectơ biểu diễn 1 và đưa vào cơ sở mới:

Đoạn lệnh trong phần này tổng quát và ngắn gọn hơn đoạn lệnh đã được đưa ra ở [3].

```
> timX:=proc(A,p)
      local X, K, Ct, n,k, i:
      n:=ColumnDimension(A);
      K:=IdentityMatrix(n);
      while n>1 do
         X:=RandomVector(n,generator=rand(0..p-1));
         for i from 1 to n do
          if (simplify(X^(`%T`).A.X) mod p =1 and X[i]<>0)
          then
                X:=X mod p;
                 k:=i;
                Ct:=<X|DeleteColumn(K,k)>;
               return Ct ;
           end if;
        end do;
      end do;
end proc;
```

2.3. Thực hiện các phép đổi biến không suy biến đưa dạng toàn phương về dạng chính tắc và đưa ra ma trận chuyển cơ sở

```
> chinhtac := proc (A, p)
   local m, A0, A1, B, D1, F, G, H, K, M, N, Q, CH, CT, Y, n, i, j;
   if Determinant(A) mod p= 0 then ERROR(` Khong thoa dieu kien ve rank`) end if;
   n := Rank(A);
   A0 := A mod p;
   for i from 0 to n-1 do
        m := n-i+1;
        if i = 0 then
           K := IdentityMatrix(n);
           A1 := A0;
        elif i < n-1 then
           K := IdentityMatrix(n-i);
           A1 := SubMatrix(N, 2 .. m, 2 .. m);
        else A1 := N fi;
        B := timX(A1, p);
        D1 := (B^%T.A1.B) mod p;
        M := MatrixInverse(<Row(D1, 1)^%T| DeleteColumn(K, 1)>^%T) mod p;
        N := (M^%T.D1.M) mod p;
        F := (B.M) mod p;
```

```
        if i < n-1 then
            G := (DiagonalMatrix([IdentityMatrix(i), F])) mod p;
            if i = 0 then H := G else H := (H.G) mod p; end if;
        else G := (DiagonalMatrix([IdentityMatrix(n-2), F])) mod p;
        end if;
    end do;
    CH := (H.G) mod p;
    CT := (CH^%T.A.CH) mod p;
    print(`Ma tran chuyen co so=`, CH);
    print(`Ma tran cua dang chinh tac=`, CT);
    Y := Vector(n, symbol = 'y');
    print(`Dang chinh tac cua dang toan phuong la`);
    return (Y^%T.CT.Y);
    end proc;
```

2.4. Ví dụ minh họa

Đưa dạng toàn phương $x_1^2 + x_1x_2 + x_2^2 + 2x_2x_3 + 2x_3^2 + 4x_4^2 - x_5^2$ trên trường hữu hạn F_5 về dạng chính tắc.

```
> tp := x[1]^2+x[1]*x[2]+x[2]^2+2*x[2]*x[3]+2*x[3]^2+4*x[4]^2-x[5]^2;
```

$$tp := x_1^2 + x_1 x_2 + x_2^2 + 2 x_2 x_3 + 2 x_3^2 + 4 x_4^2 - x_5^2$$

```
> matran(tp, 5);
```

$$Ma\ tran\ dang\ toan\ phuong\ A =, \begin{bmatrix} 1 & 3 & 0 & 0 & 0 \\ 3 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{bmatrix}$$

```
> chinhtac(A, 5);
```

$$Ma\ tran\ chuyen\ co\ so=, \begin{bmatrix} 3 & 1 & 3 & 0 & 2 \\ 3 & 2 & 3 & 3 & 2 \\ 4 & 0 & 0 & 4 & 1 \\ 4 & 1 & 1 & 3 & 1 \\ 4 & 0 & 0 & 0 & 2 \end{bmatrix}$$

$$Ma\ tran\ cua\ dang\ chinh\ tac=, \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}$$

Dang chinh tac cua dang toan phuong la

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 + 3\,y_5^2$$

3. KẾT LUẬN

Quá trình lập trình bằng Maple giúp việc tính toán, rút gọn dạng toàn phương nhanh chóng và thuận tiện hơn. Bài báo đã giải quyết hoàn toàn việc đưa các dạng toàn phương không suy biến có hạng lớn hơn hoặc bằng 2 trên trường hữu hạn F_q có đặc số khác 2 về dạng chính tắc, đồng thời chỉ ra ma trận chuyển cơ sở để thu được dạng chính tắc đó.

TÀI LIỆU THAM KHẢO

[1]. J. - P. Serre (1973). *A Course in Arithmetic, Part I - Algebraic Methods.* Springer - Verlag.

[2]. L. Bernadin (2014). *Maple Programming Guide*. Website: https://drive.google.com/file/d/1Tt90NS84BCwXiFwAsl26zV9Oq4Q1IPdV/view?usp=sharing.

[3]. Nguyễn Duy Ái Nhân, Trần Công Mẫn (2018). Sử dụng Maple đưa dạng toàn phương có hạng bằng 3 trên trường hữu hạn về dạng chính tắc. *Tạp chí Khoa học và Công nghệ, Trường Đại học Khoa học, Đại học Huế*, tập 12, số 1, trang 11-16.

[4]. Phan Đức Châu. Sử dụng Maple để đưa dạng toàn phương về dạng chính tắc. Website: https://drive.google.com/file/d/0B1OYuSEJ2W-lYVNraVJqVWdENmc/view.

REDUCTION OF NONDEGENERATE QUADRATIC FORM OVER FINITE FIELD TO CANONICAL FORM BY USING MAPLE

Nguyen Duy Ai Nhan*, Tran Cong Man

Faculty of Mathemetics, University of Sciences, Hue University

*Email: nguyenduyainhan.t2b@gmail.com

ABSTRACT

A quadratic form of rank $n \geq 2$ over finite field F_q, where q is a power of a prime number $p \neq 2$, represents all elements of F_q^*. Thus, every nondegenerate quadratic form of rank $n \geq 2$ over F_q is equivalent to form

$$X_1^2 + \cdots + X_{n-1}^2 + X_n^2$$

or

$$X_1^2 + \cdots + X_{n-1}^2 + aX_n^2$$

depending on whether itsdiscriminant is a square or not. Following that idea and using Maple, this paper gives some codes, which reduce a nondegenerate quadratic form over finite field F_q to the canonical form and give the change of basis matrix.

Keywords: finite field, Maple quadratic form.

Nguyễn Duy Ái Nhân sinh ngày 22/07/1989 tại Thừa Thiên Huế. Năm 2011, bà tốt nghiệp cử nhân ngành Sư phạm Toán tại Trường Đại học Sư phạm, ĐH Huế. Năm 2013, bà tốt nghiệp thạc sĩ chuyên ngành Đại số và Lý thuyết số tại Trường Đại học Sư phạm, ĐH Huế. Hiện nay, bà giảng dạy tại Trường Đại học Khoa học, ĐH Huế.

Trần Công Mẫn sinh ngày 04/10/1982 tại Đà Nẵng. Năm 2004, ông tốt nghiệp cử nhân ngành Toán học tại Trường Đại học Khoa học, ĐH Huế. Năm 2009, ông tốt nghiệp thạc sĩ chuyên ngành Toán Giải tích tại Trường Đại học Sư phạm, ĐH Huế. Hiện nay, ông giảng dạy tại Trường Đại học Khoa học, ĐH Huế.

Lĩnh vực nghiên cứu: toán tin ứng dụng.