**ĐẠI HỌC QUỐC GIA HÀ NỘI**
**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

---

**Lê Quang Hàm**

# XÂY DỰNG VÀ PHÂN LOẠI MỘT SỐ LỚP ĐỒ THỊ TỰA NGẪU NHIÊN TRONG KHÔNG GIAN VÉC TƠ TRÊN TRƯỜNG VÀ VÀNH HỮU HẠN

Chuyên ngành: Cơ sở Toán học cho Tin học
Mã số: 9460117.02

DỰ THẢO TÓM TẮT LUẬN ÁN TIẾN SĨ TOÁN TIN

**Hà Nội - 2021**

Công trình được hoàn thành tại: Khoa Toán - Cơ - Tin học, Trường Đại học Khoa học Tự nhiên, Đại học Quốc gia Hà Nội.

Người hướng dẫn khoa học: GS.TS. Lê Anh Vinh.

Phản biện:

Phản biện:

Phản biện:

Luận án sẽ được bảo vệ trước Hội đồng cấp Đại học Quốc gia chấm luận án tiến sĩ họp tại .....
vào hồi giờ ngày tháng năm 2021.

Có thể tìm hiểu luận án tại:

- Thư viện Quốc gia Việt Nam.
- Trung tâm Thông tin - Thư viện, Đại học Quốc gia Hà Nội.

# Mở đầu

## Tổ hợp cộng tính

Tổ hợp cộng tính là sự giao thoa giữa các chuyên ngành tổ hợp, lý thuyết số, giải tích Fourier và lý thuyết ergodic. Tổ hợp cộng tính nghiên cứu những khái niệm gần đúng của những cấu trúc đại số, như không gian véc tơ, nhóm, vành hoặc trường. Green đã mô tả tổ hợp cộng tính như sau: "Tổ hợp cộng tính nghiên cứu về các cấu trúc xấp xỉ như xấp xỉ nhóm, vành trường, đa thức và đồng cấu". Xấp xỉ nhóm có thể được xem như các tập con hữu hạn của một nhóm thỏa mãn gần như là đóng đối với các phép toán. Xấp xỉ nhóm và ứng dụng của nó (ví dụ, cho các các đồ thị nở, lý thuyết nhóm, xác xuất, lý thuyết mô hình,...) tạo thành một lĩnh vực rất năng động và hứa hẹn trong việc nghiên cứu tổ hợp cộng tính.

Các kỹ thuật áp dụng vào các bài toán tổ hợp cộng tính thường đa dạng và có thể có nguồn gốc từ nhiều lĩnh vực khác nhau. Ví dụ, Hamidoune, qua ý tưởng từ tính liên thông của đồ thị, đã đưa ra một công cụ mạnh để giải quyết một số bài toán tổ hợp cộng tính. Nathanson trong công trình của mình đã sử dụng bổ đề của Kőnig về sự tồn tại của các đường đi độ dài vô hạn trong đồ thị vô hạn, giới thiệu một lớp các cơ sở cộng tính mới, nó cũng là sự tổng quát hóa giả thuyết của Erdős - Turán về cơ sở cộng tính của các số nguyên dương. Trong bài báo của mình, Bibak đã dùng các công cụ từ lý thuyết mã hóa để đánh giá các hằng số Davenport. Các kỹ thuật từ lý thuyết thông tin đã được sử dụng để nghiên cứu các bất đẳng thức tập tổng. Sử dụng phương pháp lý thuyết đồ thị, Alon đã áp dụng vào nghiên cứu các tập không có tổng cấp $m$ trong nhóm Aben hữu hạn và trong các tập tổng-tự do của tập $[1, n]$.

Trong việc chứng minh giả thuyết đã tồn tại khá lâu về các cấp số cộng của Erdős. Green và Tao đã có một bước đột phát bằng việc kết hợp các phương pháp và ý tưởng từ tổ hợp, lý thuyết số, giải tích điều hòa, và lý thuyết ergodic.

Gần đây tổ hợp cộng tính đã tìm thấy các ứng dụng rất đáng chú ý vào khoa học máy tính và mật mã. Ví dụ, hàm nở, hàm trích xuất, tính tựa ngẫu nhiên, kiểm thử thuộc tính, lý thuyết độ phức tạp, khuếch đại độ khó, các

chứng minh có thể kiểm tra xác suất (PCPs), lý thuyết thông tin. Tổ hợp cộng tính cũng có các ứng dụng quan trọng trong bỏ phiếu điện tử (e-voting). Các phương pháp từ tổ hợp cộng tính cũng cung cấp một số kỹ thuật mạnh cho việc nghiên cứu bài toán ngưỡng, bài toán có tầm quan trọng đáng kể trong tổ hợp, khoa học máy tính, xác suất, vật lý thống kê và kinh tế.
Sự kết nối giữa các ý tưởng của tổ hợp cộng tính với lý thuyết các ma trận ngẫu nhiên có nhiều ứng dụng trong nhiều lĩnh vực của lý thuyết số, tổ hợp, khoa học máy tính vật lý toán học và lý thuyết, hóa học. Lĩnh vực này cũng có nhiều ứng dụng cho lý thuyết nhóm, giải tích, tổng mũ, lý thuyết độ phức tạp, hình học rời rạc, hệ động lực, và rất nhiều các ngành khoa học khác. Tổ hợp cộng tính đã có những tiến bộ rất nhanh sau khi nghiên cứu rất sâu về định lý Szemerédi, bằng chứng về sự tồn tại của các cấp số cộng dài trong các số nguyên tố của Green và Tao, cũng như các khái quát và ứng dụng của bài toán tổng - tích, và tiếp tục thấy những tiến bộ đáng kể.
Trong số các bài toán tổ hợp cộng tính, bài toán hàm nở cũng đã nhận được nhiều sự quan tâm của các nhà nghiên cứu, đặc biệt là về lĩnh vực toán học ứng dụng vào khoa học máy tính. Các kết quả được công bố cũng khá ấn tượng trong thời gian gần đây, nhất là từ khi Rudnev đã đưa phương pháp hình học vào các bài toán này. Tuy nhiên, các bài toán này một mặt vẫn chưa chứng minh được một cách triệt để, một mặt lại mở ra nhiều bài toán mới cần giải quyết.

Bài toán mục tiêu mà Luận án hướng tới là nghiên cứu sự nở của một hàm trên các không gian hữu hạn. Dựa vào những kết quả đã được công bố của các nhà nghiên cứu khác, Luận án sẽ nghiên cứu mở rộng và cải thiện một số kết quả, cụ thể như sau:

1. Nghiên cứu các hàm nở bốn biến trên trường hữu hạn. Định hướng chứng minh một số lớp hàm nở bốn biến với ngưỡng 5/13 và 3/8.

2. Nghiên cứu hàm nở hai biến trên vành định giá. Mở rộng một số kết quả trên trường hữu hạn.

3. Nghiên cứu các hàm nở, đánh giá lực lượng của tập tích các ma trận trên nhóm Heisenberg.

Lý thuyết phổ đồ thị là một trong những phương pháp hiệu quả và được nghiên cứu nhiều trong thời gian gần đây trong việc giải quyết một số bài toán tổ hợp cộng tính.
Mục tiêu của Luận án sẽ xây dựng và phân loại một số lớp đồ thị tựa ngẫu nhiên trong không gian véc tơ trên trường hữu hạn, từ đó có thể áp dụng để đưa ra một số kết quả cho bài toán hàm nở tương ứng. Cụ thể, Luận án sẽ xây dựng một số lớp $(n, d, \lambda)$- đồ thị trên vành định giá hữu hạn, áp dụng vào việc chứng minh một số hàm hai biến có tính chất nở. Ngoài ra trong quá trình nghiên cứu, áp dụng một số kết quả từ phương pháp hình học liên thuộc và phương pháp giải tích Fourier, Luận án cũng đã thu được một số

kết quả mới là sự cải thiện đáng kể các kết quả trước đó.

Các chương tiếp theo của Luận án sẽ được trình bày như sau.
Chương 1. Trình bày các hàm nở bốn biến trong trường hữu hạn và trường nguyên tố, trong chương này chúng tôi sẽ đưa ra kết quả là sự phân lớp các hàm bốn biến bậc hai có tính chất nở với ngưỡng $\epsilon = 3/8$ trên trường hữu hạn và với ngưỡng $\epsilon = 5/13$ trên trường nguyên tố.
Chương 2. Trình bày các hàm nở trong nhóm Heisenberg, các kết quả này là sự cải thiện các kết quả của Hegyvári và Hennecart trong công trình [**?**] .
Chương 3. Đưa ra các kết quả hàm nở trong vành định giá hữu hạn, trong đó gồm có một số phân lớp đối với hàm hai và ba biến, và một số kết quả đối với hàm bốn biến.

# Chương 1

# Hàm nở bốn biến trên trường hữu hạn

## 1.1. Giới thiệu bài toán

Cho $\mathbb{F}_q$ là một trường hữu hạn cấp $q$. Định nghĩa hàm nở trên $\mathbb{F}_q$ được phát biểu như sau.

**Định nghĩa 1.1.1 (Hàm nở ).** *Cho $\mathcal{A} \subset \mathbb{F}_q^d$. Hàm $f : \mathbb{F}_q^d \to \mathbb{F}_q$ được gọi là nở nếu*

$$f(\mathcal{A}) \geq C_\epsilon |\mathcal{A}|^{\frac{1}{d}+\epsilon}$$

*trong đó $\epsilon > 0$ và $C_\epsilon$ là một hằng số.*

Việc nghiên cứu các hàm nở sẽ làm xuất hiện các bài toán cơ bản như chứng minh một hàm cho trước có tính chất nở, xây dựng một hàm có tính chất nở trong không gian cho trước, đánh giá chính xác độ nở của một hàm hoặc ứng dụng hàm nở cho các bài toán khoa học khác.

### 1.1.1. Hàm nở bốn biến

Chúng ta có thể phân lớp các hàm nở thành ba loại phụ thuộc vào độ nở như sau.

**Định nghĩa 1.1.2.** *Cho $f : \mathbb{F}_q^d \to \mathbb{F}_q$. khi đó $f$*

- *Gọi là nở mạnh với ngưỡng $\epsilon$ nếu với mọi $A \subset \mathbb{F}_q$ sao cho $|A| \gg q^{1-\epsilon}$, ta có $|f(A, ..., A)| \geq q - k$, với hằng số dương cố định $k$.*
- *Gọi là nở vừa với ngưỡng $\epsilon$ nếu với mọi $A \subset \mathbb{F}_q$ thỏa mãn $|A| \gg q^{1-\epsilon}$, thì ta có $|f(A, ..., A)| \gg q$.*

- *Gọi là nở yếu với ngưỡng $0 < \epsilon < 1$ và $0 < \delta < 1$ nếu với mọi $A \subset \mathbb{F}_q$ thỏa mãn $|A| \gg q^{1-\epsilon}$, ta có $|f(A, ..., A)| \geq |A|^{\delta} q^{1-\delta}$.*

Đối với hàm nở bốn biến, sử dụng ước lượng tổng đặc trưng cộng tính, Sárkőzy trong công bố của mình đã chứng minh rằng các hàm $x+y+zt, xy+zt, (x-y)^2+(z-t)^2$ là nở vừa với ngưỡng $\epsilon = 1/3$. Sau đó, Vinh, bằng phương pháp phổ đồ thị, đã chứng minh rằng $xy + (z-t)^2, f(x) + g(y) + zt, f(x) + g(y) + (z-t)^2, f(x)g(y) + zt$ và $f(x)g(y) + (z-t)^2$ là các hàm nở vừa với ngưỡng 3/8 trong đó $f, g \in \mathbb{F}_q[x]$.
Nội dung chính của chương này là xây dựng và phân lớp một số hàm bốn biến là nở vừa với ngưỡng 5/13 trên trường nguyên tố hữu hạn và ngưỡng 3/8 trên trường hữu hạn. Công cụ chính của chúng tôi là một kết quả năng lượng của Koh, Mirzaei, Thang và Shen, một phiên năng lượng bản trên trường $\mathbb{F}_q$ và một định lý về hàm nở hai biến được chứng minh bởi Hegyvári và Hennecart. Kết quả đầu tiên là sự phân lớp các hàm bốn biến nở vừa với ngưỡng 5/13 trên trường nguyên tố hữu hạn $\mathbb{F}_p$.

**Định lý 1.1.1.** *Cho $\mathbb{F}_p$ là một trường nguyên tố. $f \in \mathbb{F}_p[x, y, z]$ là một đa thức bậc hai ba biến và không có dạng $g(h(x) + k(y) + l(z))$. $m(x)$ và $x^k$ là các đa thức độc lập affine với các bậc bị chặn. Định nghĩa $Q(u, v) = m(u) + u^k n(v)$, và $F(u, v, y, z) := f(Q(u, v), y, z)$, trong đó $k$ là một hằng số nguyên dương. Khi đó với $A \subset \mathbb{F}_p$ thỏa mãn $|A| \gg p^{8/13}$, ta có*

$$|F(A, A, A, A)| \gg p.$$

**Hệ quả 1.1.1.** *Các đa thức 4 biến sau đây là các hàm nở vừa với mũ $\frac{5}{13}$ trên trường nguyên tố:*

$$u(u+v)y + z, \qquad u(u+v) + yz, \qquad u(u+v)(y+z)$$
$$y(u(u+v) + z), \qquad (u(u+v) - y)^2 + z, \qquad (y-z)^2 + u(u+v).$$

Kết quả tiếp theo là sự phân lớp các hàm bốn biến nở vừa với ngưỡng 3/8 trên trường hữu hạn $\mathbb{F}_q$.

**Định lý 1.1.2.** *$\mathbb{F}_q$ là một trường hữu hạn tùy ý. $f \in \mathbb{F}_q[x, y, z]$ là một đa thức bậc hai ba biến và không có dạng $g(h(x)+k(y)+l(z))$. Gọi $m(x)$ và $x^k$ là các đa thức độc lập affine với các bậc bị chặn. Định nghĩa $Q(u, v) = m(u) + u^k n(v)$, và $F(u, v, y, z) := f(Q(u, v), y, z)$, trong đó $k$ là một hằng số nguyên dương. Cho $A \subset \mathbb{F}_q$ thỏa mãn $|A| \gg q^{5/8}$, ta có*

$$|F(A, A, A, A)| \gg q.$$

**Hệ quả 1.1.2.** *Đa thức 4- biến sau đây là một hàm nở vừa với mũ $\frac{3}{8}$ trên trường hữu hạn bất kỳ:*

$$u(u+v)y + z, \qquad u(u+v) + yz, \qquad u(u+v)(y+z)$$
$$y(u(u+v) + z), \qquad (u(u+v) - y)^2 + z, \qquad (y-z)^2 + u(u+v).$$

# Chương 2

# Hàm nở trên nhóm Heisenberg

## 2.1. Giới thiệu bài toán

Cho trường hữu hạn $\mathbb{F}_q$, trong đó $q$ là lũy thừa của một số nguyên tố lẻ. Với số nguyên $n \geq 1$, nhóm Heisenberg bậc $n$ trên trường hữu hạn $\mathbb{F}_q$, ký hiệu bởi $\mathcal{H}_n(\mathbb{F}_q)$, là nhóm nhân các phần tử có dạng:

$$[\mathbf{x}, \mathbf{y}, z] := \begin{pmatrix} 1 & \mathbf{x} & z \\ \mathbf{0} & I_n & \mathbf{y}^t \\ 0 & \mathbf{0} & 1 \end{pmatrix}$$

trong đó $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, $\mathbf{y}^t$ là véc tơ cột của $\mathbf{y}$ và $I_n$ là ma trận đơn vị $n \times n$. Khi đó phép nhân hai ma trận sẽ là

$$[\mathbf{x}, \mathbf{y}, z]\left[\mathbf{x}', \mathbf{y}', z'\right] = \left[\mathbf{x} + \mathbf{x}', \mathbf{y} + \mathbf{y}', z + z' + \mathbf{x} \cdot \mathbf{y}'\right]$$

trong đó $\mathbf{x} \cdot \mathbf{y}'$ là tích vô hướng của hai véc tơ $\mathbf{x}$ và $\mathbf{y}'$.

Cho $A \subset \mathbb{F}_q, \mathbf{E}, \mathbf{F} \subset \mathbb{F}_q^n$, ta ký hiệu

$$[\mathbf{E}, \mathbf{F}, A] := \{[\mathbf{x}, \mathbf{y}, z] : \mathbf{x} \in \mathbf{E}, \mathbf{y} \in \mathbf{F}, z \in A\},$$

và

$$[\mathbf{E}, \mathbf{F}, A]^d := \{[\mathbf{x}_1, \mathbf{y}_1, z_1]...[\mathbf{x}_d, \mathbf{y}_d, z_d] : [\mathbf{x}_i, \mathbf{y}_i, z_i] \in [\mathbf{E}, \mathbf{F}, A], i = \overline{1, d}\}.$$

Sử dụng ước lượng tổng tích, Hegyvári và Hennecart đã chứng minh được rằng nếu $A \subset \mathbb{F}_p$ với $|A| \geq p^{1/2}$, thì

$$|[A, A, 0][A, A, 0]| \gg \min\left\{p^{1/2}|[A, A, 0]|^{5/4}, p^{-1/2}|[A, A, 0]|^2\right\}.$$

Trong trường hợp tập $A$ nhỏ, Hegyvári và Hennecart đã thu được kết quả sau.

**Định lý 2.1.1** (Hegyvári-Hennecart)**.** *Cho $A \subset \mathbb{F}_p$. Với $|A| \leq p^{2/3}$. Khi đó, ta có*

$$|[A,A,0][A,A,0]| \gg |[A,A,0]|^{\frac{7}{4}}.$$

Một cách tương tự, Hegyvári và Hennecart đã mở rộng kết quả trên trường hữu hạn bất kỳ.

**Định lý 2.1.2** (Hegyvári-Hennecart)**.** *Cho $A$ là một tập con của $\mathbb{F}_q$. Với $|A| \geq q^{2/3}$. Khi đó*

$$|[A,A,0][A,A,0]| \gg q|[A,A,0]|.$$

Trên trường số thực, với bất kỳ tập con $A \subset \mathbb{R}$, sử dụng chặn liên thuộc điểm-mặt phẳng do Elekes và Tóth đưa ra và một biến thể năng lượng của Rudnev, Shkredov, và Stevens, Hegyvári và Hennecart đã chứng minh kết quả.

**Định lý 2.1.3.** *Cho tập hữu hạn số thực $A \subset \mathbb{R}$ với điều kiện $|A| \geq 2$. Khi đó*

$$|[A,A,0][A,A,0]| \gtrsim |[A,A,0]|^{\frac{15}{8}}.$$

Mục tiêu chính của chương này là cải thiện và mở rộng các kết quả trên trong trường hữu hạn $\mathbb{F}_q$ và trường số phức $\mathbb{C}$ bằng công cụ hình học và giải tích Fourier.
Kết quả đầu tiên là sự cải thiện của Định lý 2.1.2 trong trường hợp năng lượng cộng tính của $A$ nhỏ.

**Định lý 2.1.4.** *Cho $A$ là một tập con của $\mathbb{F}_q$. Năng lượng cộng tính của tập $A$ $\Lambda^+(A)$, là số các bộ bốn $(a,b,c,d) \in A^4$ thỏa mãn $a+b=c+d$. Giả sử rằng $\Lambda^+(A) \leq \frac{|A|^3}{K}$ với $K>0$ và $|A| \geq K^{1/3}q^{2/3}$. Khi đó*

$$|[A,A,0][A,A,0]| \gg Kq|[A,A,0]|.$$

Kết quả tiếp theo là một sự mở rộng của Định lý 2.1.2 trong $H_n(\mathbb{F}_q)$ với $n \geq 1$.

**Định lý 2.1.5.** *Cho $E$ là một tập con của $\mathbb{F}_q^n$. Với $|E| \gg q^{\frac{n}{2}+\frac{1}{4}}$. Khi đó*

$$|[E,E,0][E,E,0]| \gg q|[E,E,0]|.$$

Lưu ý rằng kết quả của Định lý 2.1.5 là chặt. Ta có thể cho $E$ là một không gian con trong $\mathbb{F}_q^n$, khi đó $[E,E,0][E,E,0] \subset [E,E,\mathbb{F}_q]$. Hơn nữa, số mũ $\frac{n}{2}+\frac{1}{4}$ không thể bị giảm tới $\frac{n}{2}$. Giả sử $q=p^2$, ta chọn $E=\mathbb{F}_p^n$, khi đó $|[E,E,0][E,E,0]| \ll p|[E,E,0]| = q^{1/2}|[E,E,0]|$.
Trên trường nguyên tố, nếu $E$ là một tập con của $\mathbb{F}_p^2$ và lực lượng của $E$ không quá lớn, ta có định lý sau trong $H_2(\mathbb{F}_p)$.

**Định lý 2.1.6.** *Cho $\mathbb{F}_p$ là một trường nguyên tố với $p \equiv 3(\mod 4)$, và $E$ là một tập con của $\mathbb{F}_p^2$ với $|E| \ll p^{8/5}$. Khi đó*

$$|[E,E,0][E,E,0]| \gg |[E,E,0]|^{\frac{19}{15}}.$$

Khi $A$ là một nhóm con với phép toán nhân của $\mathbb{F}_p^*$, số mũ $\frac{7}{4}$ trong Định lý 2.1.1 có thể được cải thiện một cách đáng kể.

**Định lý 2.1.7.** *Cho $A$ là một nhóm con với phép nhân của $\mathbb{F}_p^*$ và $|A| \leq p^{1/2}\log p$. Khi đó*

$$|[A,A,0][A,A,0]| \gtrsim |[A,A,0]|^{\frac{151}{80}}.$$

Kết quả tiếp theo là một sự mở rộng của kết quả của Định lý 2.1.3 trên trường số phức.

**Định lý 2.1.8.** *Cho $A$ là một tập con của $\mathbb{C}$ với $|A| \geq 2$. Ta có*

$$|[A,A,0][A,A,0]| \gtrsim |A|^{\frac{29}{8}} = |[A,A,0]|^{\frac{29}{16}}.$$

# Chương 3

# Hàm nở trên vành định giá hữu hạn

## 3.1. Hàm nở hai biến trên vành định giá

### 3.1.1. Giới thiệu kết quả

Trên trường hữu hạn $\mathbb{F}_q$. Hegyvári and Hennecart đã thu được một số kết quả về hàm nở hai biến. Cụ thể, các tác giả đã chỉ ra rằng với các họ hàm hai biến nào đó $f(x,y)$ và $g(x,y)$, nếu $|A| = |B| = p^\alpha$ thì $\max\{|f(A,B), |g(A,B)|\} \gg |A|^{1+\Delta(\alpha)}$, với $\Delta(\alpha) > 0$. Chúng ta sẽ nêu dưới đây các phát biểu của họ. Trước khi nêu ra các kết quả, chúng ta cần định nghĩa bội của một hàm trên một nhóm con của trường hữu hạn.
Cho $G$ là một nhóm con trong $\mathbb{F}_p^*$, và $g : G \to \mathbb{F}_p$ là một hàm tùy ý, ta định nghĩa

$$\mu(g) = \max_t |\{x \in G : g(x) = t\}|.$$

Đầu tiên là hàm $f(x,y) = g(x)(h(x)+y)$ trên trường hữu hạn. Ta có các định lý sau.

**Định lý 3.1.1 (Hegyvári và Hennecart).** *Cho $G$ là một nhóm con của $\mathbb{F}_p^*$, và $f(x,y) = g(x)(h(x)+y)$ xác định trên $G \times \mathbb{F}_p^*$, trong đó $g, h : G \to \mathbb{F}_p^*$ là các hàm tùy ý. Đặt $m = \mu(g.h)$. Với các tập tùy ý $A \subset G$ và $B, C \subset \mathbb{F}_p^*$, ta có*

$$|f(A,B)||B.C| \gg \min\left\{\frac{|A||B|^2|C|}{pm^2}, \frac{p|B|}{m}\right\}.$$

Nếu $f(x,y) = x(1+y)$, thì ta được hệ quả của Định lý 3.1.1, kết quả này cũng đã được Garaev và Shen chứng minh trong một công trình của mình.

**Hệ quả 3.1.1.** *Với tập con tùy ý $A \subseteq \mathbb{F}_p \setminus \{0,-1\}$, ta có*

$$|A.(A+1)| \gg \min\left\{\sqrt{p|A|}, |A|^2/\sqrt{p}\right\}.$$

Với phiên bản phép cộng, ta có Định lý 3.1.1

**Định lý 3.1.2** (**Hegyvári và Hennecart**). *Cho $G$ là một nhóm con của $\mathbb{F}_p^*$, và $f(x,y) = g(x)(h(x)+y)$ xác định trên $G \times \mathbb{F}_p^*$, trong đó $g, h : G \to \mathbb{F}_p^*$ là các hàm tùy ý. Đặt $m = \mu(g)$. Với các tập tùy ý $A \subset G$ và $B, C \subset \mathbb{F}_p^*$, ta có*

$$|f(A,B)||B+C| \gg \min\left\{\frac{|A||B|^2|C|}{pm^2}, \frac{p|B|}{m}\right\}.$$

Chú ý nếu $C = A$ và $|A| = |B| = p^\alpha$ thì

$$\max\{|f(A,B)|, |A+B|\} \gg |A|^{1+\Delta(\alpha)},$$

trong đó $\Delta(\alpha) = \min\{1-1/2\alpha, (1/\alpha - 1)/2\}$.
Với hàm tùy ý $h : \mathbb{F}_q \to \mathbb{F}_q$ và $u \in \mathbb{F}_p$, ta định nghĩa $h_u(x) := h(ux)$. Hegyvári và Hennecart đã thu được một kết quả tổng quát của Định lý 3.1.1 như sau.

**Định lý 3.1.3** (**Hegyvári và Hennecart**). *Cho $f(x,y) = g(x)h(y)(x^k+y^k)$ trong đó $g, h : G \to \mathbb{F}_p^*$ là các hàm xác định trên một nhóm con $G$ của $\mathbb{F}_p^*$. Chúng ta giả thiết rằng với $z$ cố định, $z \in G, g(xz)/g(x)$ và $h(xz)/h(x)$ nhận $O(1)$ các giá trị khác nhau khi $x \in G$ và $\max_u \mu(g.h_u.id) = O(1)$. Khi đó với các tập con tùy ý $A, B, C \subset G$, ta có*

$$|f(A,B)||A.C||B.C| \gg \min\left\{\frac{|A|^2|B|^2|C|}{p}, p|A||B|\right\}.$$

Điều kiện của các hàm $g$ và $h$ trong định lý trông có vẻ lạ lẫm. Cho ví dụ, người ta có thể lấy $g$ và $h$ là các hàm đơn điệu, hoặc các hàm có dạng $\lambda^{\alpha(x)}x^k$, trong đó $\lambda \in \mathbb{F}_p^*$ có cấp $O(1)$ và $\alpha(x)$ là một hàm tùy ý. Lưu ý trong các trường hợp đặc biệt, ta có thể thu được một số kết quả tốt hơn. Định lý sau đây là một ví dụ.

**Định lý 3.1.4** (**Hegyvári và Hennecart**). *Cho $A, B, C$ là các tập con trong $\mathbb{F}_p^*$ và $f(x,y) = xy(x+y)$ là một đa thức trong $\mathbb{F}_p[x,y]$. Khi đó ta có ước lượng sau*

$$|f(A,B)||B.C| \gg \min\left\{\frac{|A||B|^2|C|}{p}, p|B|\right\}.$$

Kết quả này là chặt khi $|A| = |B| \approx p^\alpha$ với $2/3 \le \alpha < 1$ vì, ví dụ, ta có thể lấy $A = B = C$ là một cấp số nhân độ dài $p^\alpha$, dễ dàng thấy rằng $|A.A| \ll |A|$, và $|f(A,A)| \le p$. Điều này nói lên rằng $|f(A,A)||A.A| \ll p|A|$. Trong chương này, chúng tôi sẽ mở rộng các kết quả đã được đề cập ở trên khi xét bài toán trong vành định giá hữu hạn. Kết quả đầu tiên là sự tổng quát hóa Định lý 3.1.1.

**Định lý 3.1.5.** *Cho $\mathcal{R}$ là một vành định giá hữu hạn cấp $q^r$, $G$ là một nhóm con của $\mathcal{R}^*$, và $f(x,y) = g(x)(h(x)+y)$ xác định trên $G \times \mathcal{R}^*$, trong đó $g, h : G \to \mathcal{R}^*$ là các hàm tùy ý. Đặt $m = \mu(g.h)$. Với $A \subset G$ và $B, C \subset \mathcal{R}^*$ tùy ý, ta có*

$$|f(A,B)||B.C| \gg \min\left\{\frac{q^r|B|}{m}, \frac{|A||B|^2|C|}{m^2 q^{2r-1}}\right\}.$$

Trong trường hợp, $f(x,y) = x(1+y)$, ta thu được ước lượng sau.

**Hệ quả 3.1.2.** *Với tập con tùy ý $A \subset \mathcal{R} \setminus \{\mathcal{R}^0, \mathcal{R}^0 - 1\}$, ta có*

$$|A(A+1)| \gg \min\left\{\sqrt{q^r|A|}, \frac{|A|^2}{\sqrt{q^{2r-1}}}\right\}.$$

Cũng giống Định lý 3.1.2, ta cũng thu được một phiên bản đối với phép cộng của Định lý 3.1.5 sau đây.

**Định lý 3.1.6.** *Cho $\mathcal{R}$ là một vành định giá hữu hạn cấp $q^r$, $G$ là một nhóm con của $\mathcal{R}^*$, và $f(x,y) = g(x)(h(x)+y)$ xác định trên $G \times \mathcal{R}^*$ trong đó $g$ và $h$ là các hàm tùy ý từ $G$ vào $\mathcal{R}^*$. Đặt $m = \mu(g)$. Với các tập $A \subset G$ và $B, C \subset \mathcal{R}^*$ tùy ý, ta có*

$$|f(A,B)||B+C| \gg \min\left\{\frac{q^r|B|}{m}, \frac{|A||B|^2|C|}{m^2 q^{2r-1}}\right\}.$$

Kết hợp Định lý 3.1.5 và 3.1.6 ta suy ra hệ quả.

**Hệ quả 3.1.3.** *Với hàm $f(x,y) = g(x)(x+y)$ sao cho $\mu(g) = O(1)$, và $A \subset \mathcal{R}^*$. Khi đó*

$$|f(A,A)| \times \min\{|A.A|, |A+A|\} \gg \min\left\{q^r|A|, \frac{|A|^4}{q^{2r-1}}\right\}.$$

Cuối cùng là sự tổng quát hóa các định lý tương tự như 3.1.3 và 3.1.4.

**Định lý 3.1.7.** *Cho $\mathcal{R}$ là một vành định giá hữu hạn cấp $q^r$, và $f(x,y) = g(x)h(y)(x+y)$ trong đó $g, h : G \to \mathcal{R}^*$ là các hàm xác định trên nhóm con $G$ của $\mathcal{R}^*$. Ta giả thiết rằng với mọi $z \in G$ cố định, $g(xz)/g(x)$ và $h(xz)/g(x)$ nhận $O(1)$ các giá trị khác nhau khi $x \in G$ và $\max_u \mu(g.h_u.id) = O(1)$. Khi đó với mọi $A, B, C \subset G$, ta có*

$$|f(A,B)||A.C||B.C| \gg \min\left\{q^r|A||B|, \frac{|A|^2|B|^2|C|}{q^{2r-1}}\right\}.$$

Một cách tương tự, ta có thể cải thiện Định lý 3.1.7 cho một số trường hợp đặc biệt của hàm $f(x,y)$. Định lý sau đây là một ví dụ.

**Định lý 3.1.8.** *Cho $\mathcal{R}$ là một vành định giá hữu hạn cấp $q^r$. $A, B, C$ là các tập con trong $\mathcal{R}^*$, hàm $f(x,y) = xy(g(x)+y)$, trong đó $g$ là một hàm từ $\mathcal{R}^*$ vào $\mathcal{R}^*$, và $\mu(g^2.id) = O(1)$. Khi đó ta có*

$$|f(A,B)||B.C| \gg \min\left\{q^r|B|, \frac{|A||B|^2|C|}{q^{2r-1}}\right\}.$$

Để chứng minh các kết quả đối với hàm nở hai biến đã nêu trên, chúng ta sử dụng các kết quả từ lý thuyết phổ đồ thị sau.

### 3.1.2. Đồ thị tổng-tích trên vành định giá hữu hạn

$G$ gọi là $(n,d,\lambda)$-đồ thị nếu nó là đồ thị $d$-đều $n$ đỉnh và giá trị riêng thứ hai $\lambda(G)$ của nó nhỏ hơn hoặc bằng $\lambda$.

**Bổ đề 3.1.1.** *Cho $G = (V,E)$ là một $(n,d,\lambda)$-đồ thị. Với hai tập tùy ý $B, C \subset V$, ta có*

$$\left|e(B,C) - \frac{d|B||C|}{n}\right| \leq \lambda\sqrt{|B||C|}.$$

Chúng ta sẽ sử dụng Bổ đề trên cho việc chứng minh các kết quả hàm hai biến, việc còn lại cần tiến hành là xây dựng các $(n,d,\lambda)$-đồ thị phù hợp với bài toán. Kết quả dưới đây sẽ là công cụ chính đó.

**Định nghĩa 3.1.1.** *Đồ thị tổng-tích $\mathcal{SP}_\mathcal{R}$ được định nghĩa như sau. Tập đỉnh của đồ thị tổng-tích $\mathcal{SP}_\mathcal{R}$ là tập $V(\mathcal{SP}_\mathcal{R}) = \mathcal{R} \times \mathcal{R}$. Hai đỉnh $U = (a,b)$ và $V = (c,d) \in V(\mathcal{SP}_\mathcal{R})$ được nối với nhau bằng một cạnh, $(U,V) \in E(\mathcal{SP}_\mathcal{R})$, nếu và chỉ nếu $a + c = bd$.*

**Bổ đề 3.1.2.** *Cho vành định giá hữu hạn $\mathcal{R}$, đồ thị tổng-tích, $\mathcal{SP}_\mathcal{R}$, là một*

$$\left(q^{2r}, q^r, \sqrt{2rq^{2r-1}}\right) - \text{đồ thị.}$$

## 3.2. Hàm nở ba biến trên vành định giá

### 3.2.1. Giới thiệu kết quả

Sử dụng kết quả liên thuộc điểm-mặt phẳng của Yazici, Chúng tôi sẽ chứng minh một số kết quả cho hàm nở ba biến sau đây.

**Định lý 3.2.1.** *Cho $\mathcal{R}$ là một vành định giá hữu hạn cấp $q^r$ và đa thức*

$$f(x,y,z) = axy + r(x) + s(y) + t(z),$$

*trong đó* $r, s, t \in \mathcal{R}[u]$ *có bậc không quá hai, với* $a \neq 0$, *và* $t(z) \neq \text{const}$ *có hệ số cao nhất* $m$ *khả nghịch.* $A, B, C \subset \mathcal{R}$ *và giả thiết thêm rằng* $|C| \geq 2q^{r-1}$ *nếu* $t(z)$ *bậc hai. Khi đó,*

$$|f(A,B,C)| \geq \frac{1}{8} \min\left\{q^r, \frac{|A||B||C|}{q^{2r-1}}\right\}.$$

Với cách tiếp cận tương tự Định lý 3.2.1, chúng tôi đã chứng minh kết quả sau đây. Kết quả này cũng đã được Hiep chứng minh với một cách hoàn toàn khác.

**Định lý 3.2.2.** *Cho* $A$ *là một tập con của* $\mathcal{R}$. *Giả sử* $q^{3r-1} \leq |A+A||A|^2$, *khi đó ta có*

$$|A^2 + A^2||A+A|^2 \geq \frac{1}{2}|A|^2 q^r.$$

*Vậy*

$$\max\left\{|A+A|, |A^2+A^2|\right\} \geq 2^{-\frac{1}{3}} |A|^{2/3} q^{r/3}.$$

Kết quả tiếp theo là một chặn dưới cho tổng $A^3 + A^3$ thay cho $A^2 + A^2$ trong Định lý 3.2.2.

**Định lý 3.2.3.** *Cho* $A \subset \mathcal{R}$ *với* $\dfrac{|A+A|^4}{|A|} \geq q^{3r-1}$, *khi đó ta có*

$$\max\left\{|A+A|, |A^3+A^3|\right\} \gg q^{r/10}|A|^{9/10}.$$

Các kết quả sau đây cũng dựa trên ý tưởng của Định lý 3.2.1.

**Định lý 3.2.4.** *Cho* $f$ *là một đa thức bậc hai một biến với các hệ số trên* $\mathcal{R}$. *Nếu* $q^{3r-1} \leq |A+f(A)||A|^2$, *thì*

$$|f(A)+A| \geq 2^{-\frac{1}{3}} |A|^{2/3} q^{r/3}.$$

**Định lý 3.2.5.** *Cho* $A \subset \mathcal{R}$ *với* $|A| \geq q^{r-1/3}$, *khi đó ta có*

$$\max\{|A-A|, |AA+AA|\} \geq 2^{-\frac{1}{3}} |A|^{2/3} q^{r/3}.$$

Kết quả tiếp theo là một ước lượng dạng tổng - tích trên vành định giá hữu hạn.

**Định lý 3.2.6.** *Cho* $d$ *là một số nguyên với* $d \geq 1$ *và* $A$ *là một tập con của* $\mathcal{R}$. *Giả sử* $|AA||A|^2 \geq q^{3r-1}$, *khi đó ta có*

$$|A^d + A^d| . |AA|^2 \gg q^r |A|^2,$$

*hoặc*

$$\max\left\{|A^d + A^d|, |AA|\right\} \gg q^{\frac{r}{3}} |A|^{2/3}.$$

## 3.3. Hàm nở bốn biến trên vành định giá

Sử dụng chặn liên thuộc điểm - đường trên $\mathcal{R}^2$, Luận án chứng minh một số hàm bốn biến sau là nở vừa với ngưỡng 3/8.

**Định lý 3.3.1.** *Cho $\mathcal{R}$ là một vành định giá hữu hạn cấp $q^r$, và $A$ là một tập trong $\mathcal{R}$ sao cho $|A| \gg q^{\frac{8r-3}{8}}$. Khi đó các hàm $F_1(u,v,y,z) = u(u+v)y + z, F_2(u,v,y,z) = u(u+v)+yz, F_3(u,v,y,z) = u(u+v)(y+z), F_4(u,v,y,z) = y(u(u+v)+z), F_5(u,v,y,z) = (u(u+v)-y)^2 + z,$ và $F_6(u,v,y,z) = (y-z)^2 + u(u+v)$. thỏa mãn*

$$|F_i(A,A,A,A)| \gg q^r$$

*với $i \in \{1,...,6\}$.*

# KẾT LUẬN

Bằng các phương pháp nghiên cứu đã nêu trên, Luận án đã thu được những kết quả cụ thể như sau:

1. Phân lớp hàm nở vừa bốn biến với số mũ $\epsilon = 3/8$ trên trường hữu hạn. Phân lớp hàm nở vừa bốn biến với số mũ $\epsilon = 5/13$ trên trường nguyên tố, cả hai đã cải thiện một số kết quả rời rạc và rất ít trước đó.

2. Chứng minh một số kết quả hàm nở trong nhóm Heisenberg. Đây là sư cải thiện và mở rộng các kết quả của Hegyvári và Hennecart đưa ra.

3. Phân lớp một số hàm nở hai biến trên vành định giá hữu hạn, mở rộng các kết quả của Hegyvári và Hennecart trên trường hữu hạn. Đưa ra một lớp hàm nở ba biến trên vành định giá hữu hạn. Chứng minh một số hàm bốn biến trên vành định giá hữu hạn là nở vừa, mở rộng các kết quả Hegyvári và Hennecart trên trường hữu hạn.

Luận án đóng góp một số kết quả mới cho lớp các hàm nở trong không gian hữu hạn. Làm phong phú thêm các kết quả nghiên cứu trong lĩnh vực tổ hợp cộng tính.
Với phương pháp tiếp cận, Luận án tiếp tục khẳng định những lợi thế của các phương pháp đang được các nhà nghiên cứu sử dụng: phương pháp phổ đồ thị, phương pháp giải tích Fourier và phương pháp hình học.
Các kết quả cũng như phương pháp nghiên cứu được sử dụng trong Luận án có thể là một tài liệu tham khảo cho những người làm công tác nghiên cứu quan tâm đến lĩnh vực này, có thể về mặt phương pháp cũng như có thể cho việc nghiên cứu các ứng dụng cho ngành khoa học máy tính.
Trong thời gian tới, tác giả sẽ tập trung nghiên cứu các hàm nở với ngưỡng nhỏ hơn, tìm hiểu các ứng dụng trong khoa học máy tính lý thuyết, và các mối quan hệ với các chủ để khác nhau của Hình học Tổ hợp.

.

## DANH SÁCH
## CÁC CÔNG TRÌNH LIÊN QUAN ĐẾN LUẬN ÁN

1. L. Q. Ham, P. V. Thang and L. A. Vinh (2017), "Conditional expanding bounds for two-variable functions over finite valuation rings", *European Journal of Combinatorics*, pp 114-123.

2. Le Quang Ham, Nguyen Van The, Phuc D. Tran and Le Anh Vinh (2020), "On three-variable expanders over finite valuation rings", *Forum Math*, pp 17–27.

3. D. N. V. Anh, L. Q. Ham, D. Koh, M. Mirzaei, H. Mojarrad and T. Pham (2021), "Moderate Expanders Over Rings", *Journal of Number Theory*, pp 223-233.

4. Dao Nguyen Van Anh, Le Quang Ham, Doowon Koh, Thang Pham and Le Anh Vinh (2020), "On a theorem of Hegyvári and Hennecart", *Pacific Journal of Mathematics*, pp 407–421.

.