VIỆN HÀN LÂM KHOA HỌC VÀ CÔNG NGHỆ VIỆT NAM
VIỆN TOÁN HỌC

ĐỖ DUY HIẾU

PHƯƠNG PHÁP PHỔ CỦA ĐỒ THỊ TRONG MỘT SỐ BÀI TOÁN TỔ HỢP CỘNG TÍNH

LUẬN ÁN TIẾN SĨ TOÁN HỌC

Hà Nội - 2019

VIỆN HÀN LÂM KHOA HỌC VÀ CÔNG NGHỆ VIỆT NAM
VIỆN TOÁN HỌC

ĐỖ DUY HIẾU

PHƯƠNG PHÁP PHỔ CỦA ĐỒ THỊ TRONG MỘT SỐ BÀI TOÁN TỔ HỢP CỘNG TÍNH

Chuyên ngành: Cơ sở toán học cho tin học
Mã số: 9.46.01.10

LUẬN ÁN TIẾN SĨ TOÁN HỌC

Người hướng dẫn:

PGS. TS. LÊ ANH VINH

Hà Nội - 2019

Tóm tắt

Trong Luận án này, chúng tôi sẽ sử dụng phương pháp phổ của đồ thị để nghiên cứu về lực lượng của một số tập hợp trên không gian vectơ trên trường và vành hữu hạn như: Hàm nở hai biến, tập khoảng cách và tập tích, tập tổng - tỉ số, tập khoảng cách trên đa tạp chính quy và tập thể tích khối. Luận án gồm 04 chương chính:

Trong Chương 1, chúng tôi nhắc lại kiến thức cơ bản liên quan đến phương pháp đại số tuyến tính trong đồ thị: ma trận kề, phổ của đồ thị, (n, d, λ) - đồ thị, Bổ đề trộn nở.

Trong Chương 2, chúng tôi nghiên cứu một số (n, d, λ) - đồ thị trên không gian vectơ $\mathbb{F}_q^n$ và $\mathbb{Z}_q^n$ như đồ thị tổng - tích, đồ thị tích - tổng, đồ thị tổng - bình phương, đồ thị tích, đồ thị Euclid hữu hạn.

Trong Chương 3, chúng tôi sử dụng pháp đồ thị để nghiên cứu một số bài toán tổ hợp cộng tính. Cụ thể, chúng tôi sẽ sử dụng các đồ thị xây dựng trong Chương 2 để đánh giá một số tập hợp như tập khoảng cách, tập tích, tập thể tích khối, tập tổng - tỉ số, hàm nở hai biến trên trường và vành hữu hạn.

Trong Chương 4, chúng tôi sử dụng phương pháp phổ của đồ thị mở rộng để nghiên cứu và đưa ra kết quả tổng quát cho tập khoảng cách của một tập trên đa tạp chính quy.

Abstract

In this thesis, we use the techniques from the spectral graph theory to study the cardinality of some sets in vector spaces over finite fields and finite rings, such as the images of two-variable expanders, the distance sets, the product sets, the sum - ratio sets, the volume set of boxes, and the distance sets in regular varieties. The thesis consist of four main chapters.

In Chapter 1, we recall some basic knowledge related to linear algebraic methods in the graph: the adjacency matrix, the spectrum of a graph, the definition and properties of (n, d, λ) - graph, and the expander mixing lemma.

In Chapter 2, we study some (n, d, λ) - graphs in vector spacesover finite fields and finite rings, such as the sum - product graph, the product - sum graph, the sum - square graph, the product graph, and the finite Euclidean graph.

In Chapter 3, we use the expanding properties of the graphs in Chapter 2 to evaluate the cardinalities of distance sets, product sets, volume sets of boxes, sum - ratio sets, and images of two-variable expanders in vector spaces over finite fields and finite rings.

In Chapter 4, we use the directed version of the expander mixing lemma to study the distance set problem in general regular varieties.

Lời cam đoan

Tôi xin cam đoan Luận án này là tập hợp các nghiên cứu của tôi. Những kết quả trích từ các bài báo viết chung đã nhận được sự cho phép sử dụng của các đồng tác giả. Các kết quả nêu trong Luận án là trung thực và chưa từng được một ai khác công bố.

Lời cảm ơn

Tôi xin chân thành cảm ơn PGS. TS. Lê Anh Vinh, người đã dẫn dắt tôi vào con đường nghiên cứu khoa học. Không chỉ là một người hướng dẫn khoa học tận tâm, chia sẻ của thầy với tôi về những buồn, vui đời thường suốt nhiều năm qua là một sự động viên, khích lệ lớn để tôi vững vàng hơn trong cuộc sống.

Tôi xin chân thành cảm ơn PGS. TSKH. Phan Thị Hà Dương và GS. TSKH. Ngô Đắc Tân đã góp ý để Luận án của tôi hoàn thiện hơn. Những lời chia sẻ, chỉ dạy của thầy cô trong suốt quá trình làm việc, nghiên cứu của tôi sẽ là hành trang quý báu để tôi tự tin hơn trên những chặng đường sắp tới.

Tôi xin cảm ơn TS. Phạm Văn Thắng đã đồng hành cùng tôi trên con đường nghiên cứu trong suốt thời gian qua.

Tôi xin cảm ơn ban lãnh đạo Viện Toán học, Phòng cơ sở toán học cho tin học và Trung tâm Đào tạo sau đại học đã cung cấp cho tôi một nơi làm việc tốt, một môi trường học thuật lành mạnh để học tập, nghiên cứu trong thời gian tôi làm nghiên cứu sinh ở đây.

Cuối cùng, tôi xin tỏ lòng biết ơn vô hạn tới gia đình tôi, những người luôn bên cạnh và thương yêu tôi vô điều kiện.

Hà Nội, ngày 27 tháng 02 năm 2019

Đỗ Duy Hiếu

Bảng các kí hiệu

1. Cho p là một số nguyên tố lẻ, $r \geq 2$ là một số tự nhiên và $q = p^r$.

$\lvert A \rvert$	là lực lượng của tập hợp A.
$\mathbb{Z}_q$	là vành hữu hạn có q phần tử.
$\mathbb{Z}_q^0$	là tập các phần tử không khả nghịch trên $\mathbb{Z}_q$.
$\mathbb{Z}_q^\times$	là tập các phần tử khả nghịch trên $\mathbb{Z}_q$.
$\mathbb{F}_q$	là trường hữu hạn có q phần tử.
$\mathbb{F}_q^*$	là các phần tử khác 0 của trường hữu hạn $\mathbb{F}_q$.

2. Cho f, g là các hàm số theo biến t.

$g \in o(f)$	có nghĩa là $g(t)/f(t) \to 0$ khi $t \to \infty$.
$f \gg g$	có nghĩa là $g \in o(f)$.
$f \gtrsim g$	có nghĩa là tồn tại hằng số $c > 0$, sao cho $f \geq cg$ khi t đủ lớn.
$f = \Theta(g)$	có nghĩa là tồn tại các hằng số c_1, $c_2 > 0$ sao cho $c_1 f \leq g \leq c_2 f$ khi t đủ lớn.

3. Cho $G = (V, E)$ là một đồ thị.

(x, y)	là một cạnh có hướng từ x đến y.
$\{x, y\}$	là cạnh vô hướng giữa x và y của đồ thị G.

Mục lục

Lời mở đầu

Trong những năm gần đây, tổ hợp đã được ứng dụng vào các lĩnh vực khoa học khác nhau như: khoa học máy tính, vật lý, hóa học, ...Với sự mở rộng đó, nhiều bài toán tổ hợp mới ra đời cùng với nhiều phương pháp vốn thuộc các nhánh toán học khác đã được áp dụng để giải quyết như: xác suất, giải tích, đại số, hình học; nhờ đó đã thu được nhiều kết quả mới không hiển nhiên.

Luận án "Phương pháp phổ của đồ thị trong một số bài toán tổ hợp cộng tính" sử dụng (n, d, λ) - đồ thị và Bổ đề trộn nở để nghiên cứu các bài toán tổ hợp cộng tính. Những kết quả mới của Luận án được trình bày trong Chương 3 và Chương 4.

Trong Chương 3, chúng tôi sử dụng phương pháp phổ của đồ thị dựa vào (n, d, λ) - đồ thị và Bổ đề trộn nở để nghiên cứu một số bài toán như tập khoảng cách, tập tích, tập thể tích khối, tập tổng - tỉ số, hàm nở hai biến.

Tập khoảng cách, tập tích: Một bài toán mở cổ điển trong hình học tổ hợp là bài toán về khoảng cách của Erdős [20]. Bài toán yêu cầu chúng ta tìm số các khoảng cách khác nhau tối thiểu được xác định bởi một tập N điểm trên mặt phẳng Euclid. Erdős gọi số khoảng cách tối thiểu này là $g(N)$ và giả thuyết rằng $g(N) \gtrsim \frac{N}{\sqrt{LogN}}$. Ông cũng quan sát dựa trên một khẳng định hình học đơn giản trên đường tròn, rằng $g(N) \gtrsim N^{1/2}$. Số mũ $1/2$ đã được cải thiện một cách chậm chạp trong vòng hơn 50 năm qua bởi một loạt các lý luận phức tạp, sử dụng công cụ từ nhiều lĩnh vực khác nhau của toán học. Tháng 11 năm 2010, Guth và Katz [26] đã chứng minh được khẳng định gần tối ưu của bài toán này: trong tập N điểm bất kỳ trên mặt phẳng sẽ có $g(N) \gtrsim \frac{N}{LogN}$ khoảng cách phân biệt.

Một cách tương tự, phiên bản hữu hạn của bài toán khoảng cách của Erdős là việc đi tìm lực lượng tối thiểu của tập các khoảng cách xác định bởi các tập

N điểm trong không gian vectơ trên trường/vành hữu hạn.

Không gian Euclid hữu hạn $\mathbb{F}_q^n$ bao gồm các vectơ cột $\boldsymbol{x}$, với n là số tự nhiên và $n \geq 2$. Chúng ta nhắc lại định nghĩa khoảng cách giữa các điểm $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$

$$\|\boldsymbol{x} - \boldsymbol{y}\| = \sum_{j=1}^{n} (x_j - y_j)^2.$$

Cho tập điểm $\mathcal{E} \subset \mathbb{F}_q^n$, tập khoảng cách của $\mathcal{E}$ được định nghĩa như sau:

$$\Delta(\mathcal{E}) = \{\|\boldsymbol{x} - \boldsymbol{y}\| : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}\}.$$

Một cách tương tự, tập tích $\Pi(\mathcal{E})$ của $\mathcal{E}$ được định nghĩa như sau:

$$\Pi(\mathcal{E}) = \{\boldsymbol{x} \cdot \boldsymbol{y} : \boldsymbol{x}, \boldsymbol{y} \in \mathcal{E}\},$$

trong đó $\boldsymbol{x} \cdot \boldsymbol{y} = x_1 y_1 + \cdots + x_n y_n$ là tích vô hướng giữa hai vectơ.

Bourgain, Katz và Tao [12] đã đưa ra kết quả không hiển nhiên đầu tiên của bài toán này. Họ chứng minh rằng, nếu $\mathcal{E}$ là tập con của mặt phẳng hữu hạn và $\mathcal{E}$ không "quá lớn" thì tập khoảng cách xác định bởi $\mathcal{E}$ có ít nhất $|\mathcal{E}|^{1/2+c}$ phần tử với hằng số $c > 0$ nào đó. Tuy nhiên, chứng minh của họ không có tính định lượng và khó có thể áp dụng được trong không gian vectơ với chiều cao hơn.

Iosevich và Rudnev [34] sử dụng phương pháp giải tích Fourier, đã đưa ra một kết quả định lượng cho bài toán khoảng cách Erdős trên trường hữu hạn. Vu [54] sử dụng phương pháp phổ của đồ thị có hướng để nghiên cứu bài toán đánh giá tổng – tích trên trường hữu hạn, đã đưa ra một chứng minh khác cho kết quả của Iosevich và Rudnev. Một cách độc lập, khi nghiên cứu các tính chất của đồ thị Euclid và phi Euclid hữu hạn, Vinh [55] chứng minh lại kết quả này cùng các kết quả tổng quát khác trong không gian Euclid và không gian phi Euclid trên trường hữu hạn.

Các kết quả trên được Covert, Iosevich và Pakianathan [16] nghiên cứu trên vành hữu hạn từ năm 2011 với mục đích để hiểu rõ hơn lớp bài toán này trên lưới nguyên. Nhóm tác giả đã sử dụng giải tích Fourier, đưa ra kết quả cho tập khoảng cách và tập tích trên vành hữu hạn. Cụ thể, họ tìm điều kiện để tập khoảng cách và tập tích chứa toàn bộ các phần tử khả nghịch của vành $\mathbb{Z}_q$.

Trong phần đầu của Chương 3, sử dụng phương pháp phổ của đồ thị, chúng tôi đưa ra một cách chứng minh khác của tập khoảng cách và tập tích trên trường hữu hạn ngắn gọn hơn chứng minh của Hart và Iosevich đồng thời tìm điều kiện của tập $A \subset \mathbb{Z}_q$ để $|\Delta(A^n)|$, $|\Pi(A^n)| \gtrsim q$.

Tập thể tích khối: Trong Chương 3, chúng tôi đã nghiên cứu tập tích

$$\Pi(A^n) = \underbrace{AA + AA + \ldots + AA}_{n},$$

trong đó $\underbrace{AA + AA + \ldots + AA}_{n} = \{\sum_{i=1}^{n} x_i y_i \, : \, x_i, \, y_i \in A\}$. Một câu hỏi được đặt ra cho bài toán là nếu chúng ta thay thế phép cộng bằng phép nhân và ngược lại thì kết quả của bài toán sẽ như thế nào? Hart, Iosevich và Solymosi [29] đã chứng minh được với $A \subset \mathbb{F}_q$ thỏa mãn $|A| \geq Cq^{\frac{1}{2}+\frac{1}{2n}}$, trong đó C là một hằng số đủ lớn thì ta có:

$$\underbrace{(A \pm A) \cdot (A \pm A) \cdots (A \pm A)}_{n} = \mathbb{F}_q,$$

trong đó

$$\underbrace{(A \pm A) \cdot (A \pm A) \cdots (A \pm A)}_{n} = \{\Pi_{i=1}^{n}(x_i \pm y_i) \, : \, x_i, \, y_i \in A\}.$$

Balog [7] đã cải thiện kết quả trên. Cụ thể, Ông chứng minh với $A \subset \mathbb{F}_q$ thỏa mãn $|A| \geq q^{\frac{1}{2}+\frac{1}{2^k}}$ thì

$$\underbrace{(A - A) \cdot (A - A) \cdots (A - A)}_{2k+1} = \mathbb{F}_q,$$

với $k > 1$.

Sử dụng phương pháp phổ của đồ thị, trong phần tiếp theo của Chương 3 chúng tôi cải thiện kết quả của Balog trên trường hữu hạn, đồng thời mở rộng kết quả đó trên vành hữu hạn.

Tập tổng - tỉ số: Cho $A \subset \mathbb{R}$, nếu A là một cấp số cộng thì ta có:

$$|A + A| = 2|A| - 1$$

và

$$|A \cdot A| \gtrsim |A|^{2-\epsilon},$$

trong đó

$$A + A = \{a + b : a, b \in A\},$$

$$A \cdot A = \{a \cdot b : a, b \in A\}.$$

Tương tự, nếu $A = \{2^0, 2^1, \ldots, 2^N\}$, khi đó ta có:

$$|A \cdot A| = 2|A| - 1$$

và

$$|A + A| \gtrsim |A|^{2-\epsilon}.$$

Erdős và Szemerédi [19] chứng minh với $A \subset \mathbb{N}$ thì

$$\max\{|A + A|, |A \cdot A|\} \gtrsim |A|^{1+\epsilon},$$

với số $\epsilon > 0$. Đồng thời họ cũng đưa ra giả thuyết rằng

$$\max\{|A + A|, |A \cdot A|\} \gtrsim |A|^{2-\delta},$$

với $\delta > 0$ nào đó. Kết quả của Erdős và Szemerédi đã được Elekes [22], Mockenhaupt [37], Nathanson [40] và Roche - Newton [41] cải thiện. Hiện nay, kết quả tốt nhất là của Solymosi. Cụ thể, Solymosi [51] chứng minh được

$$\max\{|A + A|, |A \cdot A|\} \gtrsim |A|^{\frac{14}{11}-\epsilon}.$$

Lưu ý: Kết quả của Solymosi vẫn đúng trên trường số phức.

Ngoài ra, trong [15], [21] và [42] đã đưa ra các kết quả của bài toán tổng - tích cho trường hợp $|A + A|$ hoặc $|A \cdot A|$ bé.

Trên trường hữu hạn thì bài toán dường như phức tạp hơn do công cụ chính trong không gian Euclid không còn đúng nữa. Những kết quả đầu tiên trên trường hữu hạn được đưa ra trong [12], [14] và [11] là: Nếu $A \subset \mathbb{F}_p$ thỏa mãn $|A| \lesssim p^{1-\epsilon}$ với ϵ nào đó, khi đó tồn tại $\delta > 0$ sao cho

$$\max\{|A + A|, |A \cdot A|\} \gtrsim |A|^{1+\delta}.$$

Tuy nhiên, kết quả này chưa chỉ ra được mối liên hệ giữa ϵ và δ. Hart, Iosevich, Solymosi [29] đã chứng minh rằng với $A \subset \mathbb{F}_q$ thỏa mãn $q^{\frac{1}{2}} \lesssim |A| \lesssim q^{\frac{7}{10}}$ thì

$$\max\{|A + A|, |A \cdot A|\} \gtrsim \frac{|A|^{\frac{3}{2}}}{q^{\frac{1}{4}}}.$$

Cho tới thời điểm hiện tại, kết quả tốt nhất của bài toán này là của Roche - Newton - Rudnev - Shkredov [44]. Nhóm tác giả chứng minh rằng với $A \subset \mathbb{F}_p$ thỏa mãn $A \leq p^{5/8}$ thì

$$\max\{|A+A|, |A \cdot A|\} \gtrsim |A|^{1+\frac{1}{5}}.$$

Người ta hy vọng rằng sẽ thu được những kết quả tương tự khi thay thế tập tích bằng tập tỉ số. Roche-Newton [43] đã thu được những kết quả tương tự cho tập tổng - tỉ số. Trong phần tiếp theo của Chương 3, sử dụng phương pháp phổ của đồ thị, chúng tôi cũng thu được những kết quả tổng quát cho tập tổng - tỉ số trên trường và vành hữu hạn.

Hàm nở hai biến: Cho $\mathbb{F}_q$ là một trường hữu hạn với q phần tử, E là một tập con của $\mathbb{F}_q^d$, trong đó d là một số tự nhiên và $d \geq 2$. Với mọi hàm $f : \mathbb{F}_q^d \longrightarrow \mathbb{F}_q$, kí hiệu $f(E) = \{f(x) : x \in E\}$ là ảnh của f trên tập E. Chúng ta nói f là một hàm nở d biến với chỉ số ϵ nếu $|f(E)| \geq C_\epsilon |E|^{1/d+\epsilon}$ với mọi tập E. Một vấn đề đang được rất nhiều sự quan tâm là xác định các lớp hàm nở. Ví dụ, bài toán khoảng cách của Erdős [20], với hàm $\Delta : \mathbb{R}^d \times \mathbb{R}^d \longrightarrow \mathbb{R}$, trong đó $\Delta(x, y) = \|x - y\|$. Nó được giả thuyết là một hàm nở $2d$ biến với chỉ số nở $\epsilon = 1/2d$. Bourgain, Kart, Tao [12] đã đưa ra kết quả đầu tiên của bài toán khoảng cách của Erdős trên trường hữu hạn, họ chứng minh nếu q là số nguyên tố, $q = 3 \mod 4$ thì với mọi $\epsilon > 0$ và $\mathcal{E} \subset \mathbb{F}_q^2$ thỏa mãn $|\mathcal{E}| \leq C_\epsilon q^{2-\epsilon}$, khi đó sẽ tồn tại $\delta > 0$ sao cho $|\Delta(\mathcal{E})| \geq C_\delta |\mathcal{E}|^{\frac{1}{2}+\delta}$, với C_δ, C_ϵ là các hằng số. Từ kết quả trên, chúng ta khó xác định được mối quan hệ giữa ϵ và δ. Ngoài ra, Iosevich và Rudnev [34] đã chỉ ra rằng tồn tại các hằng số c_1, $c_2 > 0$ sao cho nếu có một tập $\mathcal{E} \subset \mathbb{F}_q^d$ mà $|\mathcal{E}| \geq c_1 q^{\frac{d}{2}}$, q là bội của số nguyên tố lẻ thì $|\Delta(\mathcal{E})| \geq c \min\left\{q, q^{\frac{1-d}{2}}|\mathcal{E}|\right\}$.

Cho A là tập con khác rỗng của trường hữu hạn $\mathbb{F}_q$. Khi đó tập tổng và tích được xác định như sau:

$$A + A = \{a + b : a, b \in A\} \text{ và } A \cdot A = \{a \cdot b : a, b \in A\}.$$

Bourgain [13] đã chứng minh rằng nếu $A \subset \mathbb{F}_q$ và $|A| \gtrsim q^{3/4}$ thì $A.A + A.A + A.A = \mathbb{F}_q$. Tiếp cận bằng phương pháp hình học, Hart và Iosevich [28, 30] đã chứng minh được rằng nếu $|A| > q^{1/2+1/2d}$ thì $\mathbb{F}_q^* \subset \underbrace{A.A + A.A + \ldots + A.A}_{d}$

và nếu $|A| \gtrsim q^{2/3}$ thì $\underbrace{A.A + A.A + \ldots + A.A}_{d} = \mathbb{F}_q^*$. Trường hợp được nghiên cứu nhiều nhất là $d = 2$. Sárközy [48, 49] đã chứng minh rằng với $|A| \gtrsim q^{2/3}$ thì $|A + A + A.A| \gtrsim q$ và với $|A| \gtrsim q^{3/4}$ thì $A + A + A.A = \mathbb{F}_q$.

Shparlinski [50] chứng minh được rằng với $A, B, C \subset \mathbb{F}_q$ là các tập con đủ lớn thỏa mãn $|A||B||C| \gtrsim q^2$ thì $q - |A + B.C| \lesssim \frac{q^3}{|A||B||C|}$. Trong trường nguyên, từ kết quả của Glibichuk và Konyagin [24], ta có nếu $|A| < p^{1/2}$ thì $|A + A.A| \gtrsim |A|^{7/6}$. Wigderson [9] cũng chứng minh rằng $f = xy + z$ là một hàm nở trên trường hữu hạn $\mathbb{F}_q$. Roche-Newton, Rudnev và Shkredov [45] sử dụng [46] để cải thiện kết quả trên trường $\mathbb{F}$ tùy ý. Cụ thể, họ thu được kết quả sau: Với $A, B, C \in \mathbb{F}$ thỏa mãn $|A| = |B| = |C| = N \ll p^{2/3}$ thì

$$|AB + C| \gg N^{3/2}.$$

Aksoy-Yazici và đồng nghiệp [1] chứng minh kết quả tương tự cho hàm $f = x(y + z)$. Gần đây, Vinh, Thang và De Zeeuw [53] thu được kết quả tổng quát hơn cho hàm nở ba biến trên trường hữu hạn. Cụ thể, nhóm tác giả chứng minh rằng với $f \in F[x, y, z]$ là một đa thức bậc hai phụ thuộc vào từng biến và không có dạng $g(h(x) + k(y) + l(z))$. Khi đó, với $A, B, C \in \mathbb{F}$ thỏa mãn $|A| = |B| = |C| = N$ thì

$$|f(A, B, C)| \gg \min\{N^{3/2}, p\}.$$

Garaev và Shen [23] chứng minh $f = x(y + 1)$ là một hàm nở hai biến với $x, y \in A$ và tập A có kích thước lớn. Sử dụng bất đẳng thức tam giác Ruzsa, Timothy, Jones và Roche - Newton [52] đã thu được kết quả $f = x(y + 1)$ là một hàm nở hai biến với $x, y \in A$ và tập A có kích thước bé.

Trong phần cuối của Chương 3, chúng tôi cũng chứng minh được $f = x(y + 1)$ và $g = x + y^2$ là các hàm nở hai biến trên trường và vành hữu hạn với $x, y \in A$ và $|A| \gg q^{1/2}$.

Trong Chương 4, chúng tôi thay thế Bổ đề trộn nở bằng Bổ đề trộn nở mở rộng và Bổ đề trộn nở mở rộng cho đồ thị có hướng trong phương pháp phổ của đồ thị để nghiên cứu, tổng quát kết quả của tập khoảng cách trên đa tạp chính quy.

Đặt $D(\mathbf{x}) = x_1^2 + \cdots + x_d^2$ là một đa thức trong $\mathbb{F}_q[x_1, \ldots, x_d]$. Với $\mathcal{E} \subset \mathbb{F}_q^d$, khi đó tập khoảng cách của tập $\mathcal{E}$ có thể biểu diễn qua hàm D như sau:

$$\Delta(\mathcal{E}) = \{D(\mathbf{x} - \mathbf{y}) \colon \mathbf{x}, \mathbf{y} \in \mathcal{E}\}.$$

Đã có rất nhiều kết quả nghiên cứu về lực lượng của tập khoảng cách $\Delta(\mathcal{E})$, ví dụ như một số bài báo [12, 18, 17, 34, 36, 35]. Chương 4 của Luận án, chúng tôi nghiên cứu bài toán trong trường hợp $\mathcal{E}$ là một tập con của một đa tạp chính quy.

Năm 2007, Iosevich và Rudnev [34] sử dụng biến đổi Fourier đã thu được kết quả đầu tiên về khoảng cách phân biệt trên hình cầu đơn vị trên trường hữu hạn $\mathbb{F}_q^d$. Gần đây, Covert, Koh và Pi [18] nghiên cứu một kết quả tổng quát cho bài toán trên. Cụ thể, các tác giả trả lời cho câu hỏi: Tập con $\mathcal{E}$ của đa tạp chính quy $\mathcal{V}$ phải có độ lớn như thế nào để $\Delta_{k,D}(\mathcal{E}) = \mathbb{F}_q$ hoặc $|\Delta_{k,D}(\mathcal{E})| \gtrsim q$, trong đó

$$\Delta_{k,D}(\mathcal{E}) = \left\{D(\mathbf{x}^1 + \cdots + \mathbf{x}^k) \colon \mathbf{x}^i \in \mathcal{E}, 1 \leq i \leq k\right\}?$$

Sử dụng biến đổi Fourier, Covert, Koh và Pi [18] đã cải thiện được điều kiện của tập $\mathcal{E}$ để $\Delta_{k,D}(\mathcal{E}) = \mathbb{F}_q$ với $k \geq 3$. Trong Chương 4, sử dụng phương pháp phổ của đồ thị, chúng tôi đã tổng quát được kết quả trên khi thay hàm D bằng dạng toàn phương không suy biến và đa thức chéo

$$P(\boldsymbol{x}) = \sum_{j=1}^{d} a_j x_j^s \in \mathbb{F}_q[x_1, \ldots, x_d]$$

với $s \geq 2$, $a_j \neq 0$ với mọi $j = 1, \ldots, d$.

Chương 1

Kiến thức chuẩn bị

1.1. Ma trận kề

Giả sử $G = (V, E)$ là một đơn đồ thị vô hướng có tập đỉnh V, tập cạnh E. Đồ thị G có n đỉnh. Không mất tính tổng quát, ta có thể đánh số các đỉnh của đồ thị bằng các số 1, 2, ..., n. Khi đó ta có thể biểu diễn đồ thị bằng một ma trận vuông $A = (a_{ij})_{n\times n}$. Ma trận kề của đồ thị G được định nghĩa như sau:

Định nghĩa 1.1.1. *([10, Định nghĩa 2.1]) Cho $G = (V, E)$ là một đơn đồ thị, ma trận kề $A = (a_{ij})_{n\times n}$ của G được xác định như sau:*

$$a_{ij} = \begin{cases} 1 \text{ nếu } \{i, j\} \in E, \\ 0 \text{ nếu } \{i, j\} \notin E. \end{cases}$$

Chúng ta lưu ý rằng, nếu $\{i, j\} \in E$ thì $\{j, i\} \in E$ nên $a_{ij} = a_{ji}$. Do đó ma trận kề A là ma trận đối xứng.

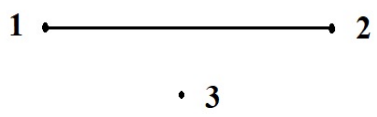
1.2. Phổ của đồ thị

Ma trận kề của một đồ thị vô hướng có tính đối xứng, do đó nó có đầy đủ các giá trị riêng thực và có một cơ sở trực giao là các vectơ riêng. Chúng ta có định nghĩa phổ của đồ thị như sau:

Định nghĩa 1.2.1. *([10, Chương 2]) Phổ của đồ thị G là tập các giá trị riêng (tính cả bội) của ma trận kề của đồ thị G.*

Lý thuyết phổ của đồ thị được xuất hiện lần đầu tiên vào những năm 1950. Đối với đồ thị với số đỉnh nhỏ, cách đơn giản nhất để tìm phổ là tìm nghiệm của đa thức đặc trưng $\chi(x) = det(A - xI)$.

Ví dụ 1.2.1. *Xét đồ thị G sau:*



Đồ thị G có ma trận kề là:

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Ta có, đa thức đặc trưng của ma trận A là:

$$det(A - xI) = \begin{vmatrix} -x & 1 & 0 \\ 1 & -x & 0 \\ 0 & 0 & -x \end{vmatrix} = -x(x^2 - 1) = x(1 - x)(1 + x).$$

Từ đó ta có phổ của đồ thị là $\lambda = -1, 0, 1$.

Đối với các đồ thị có kích thước lớn thì việc tính phổ của đồ thị thông qua tìm nghiệm của đa thức đặc trưng có thể gặp khó khăn.

Ví dụ 1.2.2. *Xét đồ thị* K_n. *Ma trận kề của* K_n *là*

$$A = \begin{pmatrix} 0 & 1 & 1 & ... & 1 \\ 1 & 0 & 1 & ... & 1 \\ . & . & . & ... & . \\ 1 & 1 & 1 & ... & 0 \end{pmatrix}.$$

Do K_n *là đồ thị chính quy bậc* $n - 1$ *nên A có một giá trị riêng* $\lambda = n - 1$ *ứng với vectơ riêng là* $\mathbf{1} = (1, 1, ..., 1)$. *Gọi* θ *là giá trị riêng của A khác* $n - 1$ *và* v_θ *là vectơ riêng tương ứng với giá trị riêng* θ. *Khi đó ta có* $v_\theta \perp \mathbf{1}$. *Mặt khác, ta có thể biểu diễn ma trận A như sau:*

$$A = J - I,$$

trong đó I là ma trận đơn vị, J là ma trận có tất cả các phần tử đều bằng một. Ta có:

$$Av_\theta = (J - I)v_\theta.$$

Do $v_\theta \perp \mathbf{1}$ *nên* $Jv_\theta = 0$. *Suy ra*

$$Av_\theta = -v_\theta.$$

Từ đó ta suy ra $\theta = -1$. *Giả sử giá trị riêng* $\lambda = n - 1$ *có bội* ℓ *và giá trị riêng* $\theta = -1$ *có bội k. Do vết của ma trận A bằng* 0 *và A có n giá trị riêng nên ta có:*

$$\ell + k = n \text{ và } (n-1)\ell - k = 0.$$

Suy ra $\ell = 1$, $k = n - 1$. *Vậy, phổ của đồ thị* K_n *là* $n - 1$ *bội* 1 *và* -1 *bội* $n - 1$.

Lưu ý: Hai đồ thị đẳng cấu thì chúng có cùng phổ.

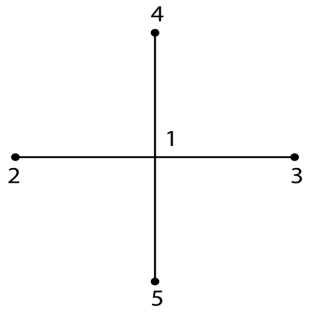
Đầu tiên, chúng ta nhắc lại định nghĩa hai đồ thị đẳng cấu.

Định nghĩa 1.2.2. *([25]) Cho hai đồ thị* $G = (V, E)$ *và* $G' = (V', E')$. *Hai đồ thị G và* G' *được gọi là đẳng cấu với nhau nếu tồn tại một song ánh* $f : V \to V'$ *sao cho* $\{u, v\}$ *là một cạnh của G khi và chỉ khi* $\{f(u), f(v)\}$ *là một cạnh của* G'.

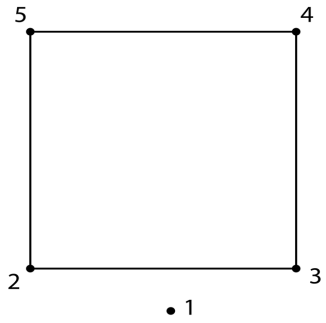
Giả sử G và G' là hai đồ thị đẳng cấu, chúng ta sẽ chứng minh chúng có cùng phổ. Gọi A và A' tương ứng là các ma trận kề của các đồ thị G và G'. Vì hai đồ thị đẳng cấu chỉ là sự sắp xếp lại các đỉnh nên ta có $A' = P^{-1}AP$, với P là ma trận hoán vị. Do đó, A và A' đồng dạng với nhau. Hai ma trận đồng dạng thì chúng có cùng giá trị riêng kể cả bội nên hai đồ thị G và G' có cùng phổ.

Câu hỏi ngược lại, nếu hai đồ thị có cùng phổ thì chúng có đẳng cấu với nhau hay không? Rất tiếc, câu trả lời là phủ định. Chúng ta xét ví dụ cụ thể sau:

Ví dụ 1.2.3. *Xét hai đồ thị* $K_{1,4}$ *và* $C_4 \cup K_1$. *Hai đồ thị này có cùng phổ là* $\lambda = -2, 0, 0, 0, 2$ *nhưng hai đồ thị này không đẳng cấu với nhau.*



$K_{1,4}$



$C_4 \cup K_1$

1.3. (n, d, λ) - đồ thị và Bổ đề trộn nở

Cho đồ thị G, gọi $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ là các giá trị riêng của ma trận kề của G. Đại lượng $\lambda(G) = \max\{\lambda_2, |\lambda_n|\}$ được gọi là giá trị riêng thứ hai của G. Đồ thị $G = (V, E)$ được gọi là (n, d, λ) - đồ thị nếu nó là đồ thị d - chính quy, có n đỉnh và giá trị riêng thứ hai của G bị chặn trên bởi λ. Một kết quả quen thuộc khi $\lambda \lesssim d$ thì G có những tính chất tương tự với đồ thị ngẫu nhiên $G(n, d/n)$, trong đó mỗi cạnh xuất hiện một cách độc lập với xác suất d/n (xem chi tiết ở [4, Chương 9]). Cho đồ thị G với hai tập đỉnh con (không nhất thiết phân biệt) $S, T \subset V$, kí hiệu $E(S, T)$ là số các cặp có thứ tự (s, t) sao cho $s \in S, t \in T$ và (s, t) là một cạnh của G. Bổ đề trộn nở sau đây là một công cụ rất quan trọng trong phương pháp phổ của đồ thị để nghiên cứu các bài toán tổ hợp cộng tính.

Bổ đề 1.3.1. *(Bổ đề trộn nở, [2]) Giả sử $G = (V, E)$ là một (n, d, λ) - đồ thị với hai tập $S, T \subset V$, ta có:*

$$\left| E(S, T) - \frac{d|S||T|}{n} \right| \leq \lambda \sqrt{|S||T|}.$$

Chứng minh. Giả sử đồ thị G có n đỉnh là $V = \{1, 2, ..., n\}$. Kí hiệu

$$\chi_S = (\chi_S(1), \chi_S(2), ..., \chi_S(n))^T$$

và

$$\chi_T = (\chi_T(1), \chi_T(2), ..., \chi_T(n))^T$$

là các vectơ đặc trưng của tập S và T. Các tọa độ của χ_S, χ_T được xác định như sau: $\chi_X(i) = 1$ nếu đỉnh $i \in X$ và bằng 0 trong trường hợp còn lại.

Giả sử $\{v_0, v_1, \ldots, v_{n-1}\}$ là một cơ sở trực chuẩn của không gian vectơ $\mathbb{R}^n$ bao gồm các vectơ riêng $\{v_0, v_1, \ldots, v_{n-1}\}$ của ma trận kề A của G. Ta có $v_0 = \frac{1}{\sqrt{n}}\mathbf{1}$ với $\mathbf{1} = (1, 1, \ldots, 1)^T$. Xét biểu diễn tuyến tính $\chi_S = \sum_i \alpha_i v_i$ và $\chi_T = \sum_j \beta_j v_j$.

Khi đó, số cạnh giữa hai tập đỉnh S, T là:

$$\begin{aligned} E(S, T) &= \chi_S^T A \chi_T \\ &= (\sum_i \alpha_i v_i^T) A (\sum_j \beta_j v_j) \\ &= (\sum_i \alpha_i v_i^T)(\sum_j \beta_j A v_j) \\ &= \sum_i \lambda_i \alpha_i \beta_i. \end{aligned}$$

Do $\alpha_0 =< \chi_S, \frac{1}{\sqrt{n}}\mathbf{1} >= |S|/\sqrt{n}$, $\beta_0 =< \chi_T, \frac{1}{\sqrt{n}}\mathbf{1} >= |T|/\sqrt{n}$, ta có:

$$E(S, T) = \lambda_0 \frac{|S||T|}{n} + \sum_{i=1}^{n-1} \lambda_i \alpha_i \beta_i.$$

Sử dụng bất đẳng thức tam giác và định nghĩa của λ, ta có:

$$\begin{aligned} |E(S, T) - \frac{d|S||T|}{n}| =& |\sum_{i=1}^{n-1} \lambda_i \alpha_i \beta_i| \\ \leq& \sum_{i=1}^{n-1} |\lambda_i \alpha_i \beta_i| \\ \leq& \lambda \sum_{i=1}^{n-1} |\alpha_i \beta_i|. \end{aligned}$$

Áp dụng bất đẳng thức Cauchy - Schwartz, ta thu được:

$$\begin{aligned} |E(S, T) - \frac{d|S||T|}{n}| \leq& \lambda \|\chi_S\|_2 \|\chi_T\|_2 \\ =& \lambda \sqrt{|S||T|}, \end{aligned}$$

kết thúc chứng minh. □

Hanson, Lund và Roche-Newton [27] đã chứng minh kết quả tương tự Bổ đề trộn nở cho số cạnh giữa hai đa tập đỉnh. Cụ thể, ta có bổ đề sau:

Bổ đề 1.3.2. *(Bổ đề trộn nở mở rộng, [27]) Cho $G = (V, E)$ là một (n, d, λ) - đồ thị. Cho B và C là hai đa tập đỉnh của G, khi đó*

$$\left| E(B, C) - \frac{d|B||C|}{n} \right| \leq \lambda \sqrt{\sum_{b \in B} m_B(b)^2} \sqrt{\sum_{c \in C} m_C(c)^2}$$

với $m_X(x)$ là bội của x trong X.

Cho $G = (V, E)$ là một đồ thị có hướng có n đỉnh thỏa mãn $|N^+(x)| = |N^-(x)| = d$ với mọi $x \in V$, trong đó $N^+(x)$ là tập đỉnh đi ra của đỉnh x, $N^-(x)$ là tập đỉnh đi vào của đỉnh x. Chúng ta định nghĩa ma trận kề của G là A_G như sau:

$$a_{ij} = \begin{cases} 1 & \text{nếu } (i, j) \in E, \\ 0 & \text{nếu } (i, j) \notin E. \end{cases}$$

Giả sử $\lambda_1 = d, \lambda_2, \ldots, \lambda_n$ là các giá trị riêng của A_G. Các giá trị riêng có thể có giá trị phức nên chúng ta không thể sắp xếp chúng nhưng có thể chứng minh được $|\lambda_i| \leq d$ với mọi $1 \leq i \leq n$. Chúng ta định nghĩa $\lambda(G) = \max_{|\lambda_i| \neq d} |\lambda_i|$.

Ma trận A là ma trận chuẩn tắc nếu $A^t A = A A^t$, với A^t là ma trận chuyển vị của A. Ta nói rằng đồ thị có hướng là đồ thị chuẩn tắc nếu ma trận kề của nó là ma trận chuẩn tắc. Cho đồ thị chuẩn tắc G, gọi $N^+(x, y)$ là tập các đỉnh z sao cho $(x, z), (y, z)$ là các cạnh của G và $N^-(x, y)$ là tập các đỉnh z sao cho (z, x), (z, y) là các cạnh của G, chúng ta có thể chứng minh được đồ thị G là đồ thị chuẩn tắc khi và chỉ khi $|N^+(x, y)| = |N^-(x, y)|$ với mọi cặp đỉnh x, y.

Đồ thị có hướng G được gọi là một (n, d, λ) - đồ thị có hướng nếu G là một đồ thị chuẩn tắc có n đỉnh, d - chính quy (tức là $|N^+(x)| = |N^-(x)| = d$ với mọi đỉnh x) và $\lambda(G) \leq \lambda$. Cho G là một (n, d, λ) - đồ thị có hướng với hai tập đỉnh $B, C \subset V$. Gọi $\mathcal{E}(B, C)$ là số cặp (b, c) sao cho $b \in B$, $c \in C$ và $(b, c) \in E(G)$, trong đó $E(G)$ là tập cạnh của đồ thị G. Vu [54] đã phát triển mở rộng Bổ đề trộn nở cho đồ thị có hướng như sau:

Bổ đề 1.3.3. *(Bổ đề trộn nở cho đồ thị có hướng, [54]) Cho $G = (V, E)$ là một*

(n, d, λ) - đồ thị có hướng. Với hai tập đỉnh $B, C \subset V$, ta có:

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

Sử dụng kĩ thuật tương tự trong chứng minh [27, Bổ đề 16] và [54, Bổ đề 3.1], chúng tôi cũng thu được kết quả tương tự như trong đồ thị vô hướng với các đa tập đỉnh.

Bổ đề 1.3.4. *(Bổ đề trộn nở mở rộng cho đồ thị có hướng) Cho $G = (V, E)$ là một (n, d, λ) - đồ thị có hướng. Cho B và C là hai đa tập đỉnh của đồ thị G, ta có:*

$$\left|\mathcal{E}(B, C) - \frac{d}{n}|B||C|\right| \leq \lambda\sqrt{\sum_{b\in B} m_B(b)^2}\sqrt{\sum_{c\in C} m_C(c)^2}$$

với $m_X(x)$ là bội của x trong X.

Chứng minh. Giả sử đồ thị G có hướng có n đỉnh là $V = \{1, 2, ..., n\}$. Kí hiệu

$$\mathcal{M}_B = (m_B(1), m_B(2), ..., m_B(n))^T$$

và

$$\mathcal{M}_C = (m_C(1), m_C(2), ..., m_C(n))^T,$$

trong đó $m_X(i)$ là bội của i trong tập X.

Do G chuẩn tắc nên ta có thể giả sử $\{v_0, v_1, \ldots, v_{n-1}\}$ là một cơ sở trực chuẩn của không gian vectơ $\mathbb{R}^n$ bao gồm các vectơ riêng $\{v_0, v_1, \ldots, v_{n-1}\}$ của ma trận kề A của G. Ta có $v_0 = \frac{1}{\sqrt{n}}\mathbf{1}$ với $\mathbf{1} = (1, 1, \ldots, 1)^T$. Xét biểu diễn tuyến tính $\mathcal{M}_B = \sum_i \alpha_i v_i$ và $\mathcal{M}_C = \sum_j \beta_j v_j$.

Khi đó, số cạnh từ tập đỉnh B đến tập đỉnh C là

$$\begin{aligned}
\mathcal{E}(B, C) &= \mathcal{M}_B^T A \mathcal{M}_C \\
&= (\sum_i \alpha_i v_i^T) A (\sum_j \beta_j v_j) \\
&= (\sum_i \alpha_i v_i^T)(\sum_j \beta_j A v_j) \\
&= \sum_i \lambda_i \alpha_i \beta_i.
\end{aligned}$$

Do $\alpha_0 =< \mathcal{M}_B, \frac{1}{\sqrt{n}}\mathbf{1} >= |B|/\sqrt{n}$, $\beta_0 =< \mathcal{M}_C, \frac{1}{\sqrt{n}}\mathbf{1} >= |C|/\sqrt{n}$, ta có:

$$\mathcal{E}(B, C) = \lambda_0 \frac{|B||C|}{n} + \sum_{i=1}^{n-1} \lambda_i \alpha_i \beta_i.$$

Sử dụng bất đẳng thức tam giác và định nghĩa của λ, ta có:

$$\begin{aligned} |\mathcal{E}(B, C) - \frac{d|B||C|}{n}| =& |\sum_{i=1}^{n-1} \lambda_i \alpha_i \beta_i| \\ \leq& \sum_{i=1}^{n-1} |\lambda_i \alpha_i \beta_i| \\ \leq& \lambda \sum_{i=1}^{n-1} |\alpha_i \beta_i|. \end{aligned}$$

Áp dụng bất đẳng thức Cauchy - Schwartz, ta thu được:

$$\begin{aligned} |\mathcal{E}(B, C) - \frac{d|B||C|}{n}| \leq& \lambda \|\mathcal{M}_B\|_2 \|\mathcal{M}_C\|_2 \\ =& \lambda \sqrt{\sum_{b \in B} m_B(b)^2} \sqrt{\sum_{c \in C} m_C(c)^2}, \end{aligned}$$

kết thúc chứng minh. □

Chương 2

Một số (n, d, λ) - đồ thị

(n, d, λ) - đồ thị là công cụ chính của phương pháp phổ của đồ thị mà chúng ta sẽ sử dụng trong các chương tiếp theo. Lưu ý rằng, chúng ta cần xây dựng các đồ thị khác nhau phụ thuộc vào mỗi bài toán. Vì vậy, trong chương này, chúng tôi sẽ xây dựng một số (n, d, λ) - đồ thị được cho bởi các phương trình đại số trên trường và vành hữu hạn. Trong các tham số n, d, λ thì tham số n và d xác định khá đơn giản. Vì vậy, làm thế nào để xác định được λ chính là vấn đề khó khăn nhất. (n, d, λ) - đồ thị G trên không gian R ($R = \mathbb{F}_q$ hoặc $\mathbb{Z}_q$) thường được định nghĩa như sau:

- Tập đỉnh thường là $V = R \times R \times .... \times R$ hoặc $R^\times \times R^\times \times .... \times R^\times$.
- Hai đỉnh $\boldsymbol{a}, \boldsymbol{b}$ của đồ thị được nối với nhau bởi một cạnh khi và chỉ khi $f(\boldsymbol{a}, \boldsymbol{b}) = t$, trong đó $t \in R$ và $f : V \times V \to R$ là một hàm số.

Chúng ta đánh giá λ qua các bước sau:

- *Bước 1:* Đếm số nghiệm của hệ phương trình

  $$f(\boldsymbol{a}, \boldsymbol{x}) = t \text{ và } f(\boldsymbol{b}, \boldsymbol{x}) = t,$$

  với $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x} \in V(G)$.

- *Bước 2:* Từ số nghiệm của hệ phương trình trên ta biểu diễn được A^2 thông qua A bằng một phương trình đại số, giả sử phương trình đó là:

  $$A^2 = h(A),$$

  với h là một hàm số nào đó.

- *Bước 3:* Từ $A^2 = h(A)$, tính chất của ma trận đối xứng và tính chất của đồ thị chính quy để tìm λ.

Chúng ta sử dụng phương pháp trên để đi tìm các tham số n, d, λ của một số (n, d, λ) - đồ thị.

2.1. Đồ thị tổng - bình phương

2.1.1. Đồ thị tổng - bình phương trên trường hữu hạn

Đồ thị tổng - bình phương $\mathcal{FS}_q$ trên trường hữu hạn $\mathbb{F}_q$ được định nghĩa như sau: Tập đỉnh của đồ thị tổng - bình phương $\mathcal{FS}_q$ là tập $\mathbb{F}_q \times \mathbb{F}_q$. Hai đỉnh $\boldsymbol{a} = (a_1, a_2)$ và $\boldsymbol{b} = (b_1, b_2) \in V(\mathcal{FS}_q)$ được nối với nhau bởi một cạnh $\{\boldsymbol{a}, \boldsymbol{b}\} \in E(\mathcal{FS}_q)$ khi và chỉ khi $a_1 + b_1 = (a_2 + b_2)^2$. Ta có định lí sau:

Định lí 2.1.1. *Đồ thị $\mathcal{FS}_q$ là một*

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

Chứng minh. Trước hết, ta nhận xét rằng $\mathcal{FS}_q$ là đồ thị q - chính quy và có q^2 đỉnh. Bây giờ chúng ta đánh giá cho giá trị riêng của đồ thị. Với $\boldsymbol{a} = (a_1, a_2) \neq \boldsymbol{b} = (b_1, b_2) \in V(\mathcal{FS}_q)$ ta đếm số nghiệm của hệ phương trình sau:

$$a_1 + x_1 = (a_2 + x_2)^2,\ b_1 + x_1 = (b_2 + x_2)^2 \text{ với } \boldsymbol{x} = (x_1, x_2) \in V(\mathcal{FS}_q).$$

Hệ có nghiệm duy nhất

$$\begin{aligned} x_1 &= \left(\frac{a_1 - b_1}{a_2 - b_2} + (a_2 - b_2)\right)^2 /4 - a_1, \\ x_2 &= \left(\frac{a_1 - b_1}{a_2 - b_2} - (a_2 + b_2)\right) /2, \end{aligned}$$

nếu $a_2 \neq b_2$ và không có nghiệm trong trường hợp khác. Nói cách khác, hai đỉnh khác nhau $\boldsymbol{a} = (a_1, a_2)$ và $\boldsymbol{b} = (b_1, b_2)$ có duy nhất một đỉnh chung nếu $a_2 \neq b_2$ và không có đỉnh chung trong trường hợp khác.

Gọi M là ma trận kề của $\mathcal{FS}_q$. Khi đó ta có:

$$M^2 = J + (q-1)I - E, \tag{2.1.1}$$

trong đó J là ma trận có tất cả các phần tử đều bằng một, I là ma trận đơn vị và E là ma trận kề của đồ thị $\mathcal{S}_E$, $V(\mathcal{S}_E) = \mathbb{F}_q \times \mathbb{F}_q$ và hai đỉnh $\boldsymbol{a}, \boldsymbol{b} \in V(\mathcal{S}_E)$ được nối với nhau bởi một cạnh $\{\boldsymbol{a}, \boldsymbol{b}\} \in V(\mathcal{S}_E)$ khi và chỉ khi $a_2 = b_2$. Suy ra $\mathcal{S}_E$ là đồ thị $(q-1)$ - chính quy. Do $\mathcal{FS}_q$ là đồ thị q - chính quy nên q là một giá trị riêng của M với vectơ riêng tương ứng là $\mathbf{1}$. Đồ thị $\mathcal{FS}_q$ liên thông, do đó giá trị riêng q có bội một. Rõ ràng đồ thị $\mathcal{FS}_q$ có chứa tam giác nên không phải là đồ thị hai phần. Do đó, gọi θ là giá trị riêng khác của đồ thị $\mathcal{FS}_q$ thì $|\theta| < q$. Gọi $\boldsymbol{v}_\theta$ là vectơ riêng ứng với giá trị riêng θ. Lưu ý $\boldsymbol{v}_\theta \in \mathbf{1}^\perp$, suy ra $J\boldsymbol{v}_\theta = 0$. Do đó từ (2.1.1) ta có $(\theta^2 - q + 1)\boldsymbol{v}_\theta = -E\boldsymbol{v}_\theta$. Thêm vào đó $\mathcal{S}_E$ là đồ thị $(q-1)$ - chính quy nên tất cả các giá trị riêng của $\mathcal{S}_E$ bị chặn trên bởi $q-1$. Suy ra $\theta^2 \leq 2(q-1)$, dẫn tới điều phải chứng minh. □

2.1.2. Đồ thị tổng - bình phương trên vành hữu hạn

Đồ thị tổng - bình phương RS_q trên vành hữu hạn $\mathbb{Z}_q$ được định nghĩa như sau: Tập đỉnh của đồ thị tổng - bình phương RS_q là tập $\mathbb{Z} \times \mathbb{Z}_q^\times$. Hai đỉnh $\boldsymbol{a} = (a_1, a_2)$ và $\boldsymbol{b} = (b_1, b_2) \in V(RS_q)$ được nối với nhau bởi một cạnh $\{\boldsymbol{a}, \boldsymbol{b}\} \in V(RS_q)$ khi và chỉ khi $a_1 + b_1 = (a_2 + b_2)^2$. Ta có định lí sau:

Định lí 2.1.2. *Đồ thị tổng - bình phương là một*

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

Chứng minh. Trước hết, ta nhận xét rằng đồ thị tổng - bình phương RS_q là một đồ thị $(p^r - p^{r-1})$ - chính quy và có $p^{2r} - p^{2r-1}$ đỉnh. Với $\boldsymbol{a} = (a_1, a_2)$ và $\boldsymbol{b} = (b_1, b_2) \in V(RS_q)$ ta đếm số nghiệm của hệ phương trình sau:

$$a_1 + x_1 = (a_2 + x_2)^2,\ b_1 + x_1 = (b_2 + x_2)^2 \text{ với } \boldsymbol{x} = (x_1, x_2) \in V(RS_q).$$

Từ đó ta có:

$$x_1 = (a_2 + x_2)^2 - a_1, \tag{2.1.2}$$

$$2x_2(a_2 - b_2) = (a_1 - b_1) - (a_2^2 - b_2^2). \tag{2.1.3}$$

Với mỗi x_2 thỏa mãn phương trình (2.1.3) tồn tại duy nhất x_1 thoả mãn phương trình (2.1.2). Suy ra số nghiệm của hệ phương trình là số nghiệm của phương

trình (2.1.3). Giả sử $0 \leq \alpha \leq r-1$ thỏa mãn $p^\alpha = (a_2 - b_2,\, p^r)$. Ta xét hai trường hợp sau:

Trường hợp 1. Nếu $((a_1 - b_1) - (a_2^2 - b_2^2),\, p^r) \neq p^\alpha$ thì phương trình (2.1.3) vô nghiệm.

Trường hợp 2. Nếu $((a_1 - b_1) - (a_2^2 - b_2^2),\, p^r) = p^\alpha$, đặt $\beta = 2(a_2 - b_2)/p^\alpha$, $\gamma = ((a_1 - b_1) - (a_2^2 - b_2^2))/p^\alpha$. Khi đó $x_2 = \gamma/\beta$. Thay vào (2.1.3) ta được p^α nghiệm x_2 thỏa mãn phương trình (2.1.3). Hay nói cách khác, hai đỉnh $\boldsymbol{a} = (a_1,\, a_2)$ và $\boldsymbol{b} = (b_1,\, b_2) \in V(RS_q)$ thỏa mãn p^α=$(a_2 - b_2,\, p^r) = ((a_1 - b_1) - (a_2^2 - b_2^2),\, p^r)$ thì có p^α đỉnh chung.

Gọi A là ma trận kề của đồ thị RS_q, khi đó ta có:

$$A^2 = J + (p^r - p^{r-1} - 1)I - \sum_{\alpha=0}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1} (p^\alpha - 1)F_\alpha,$$

trong đó I là ma trận đơn vị cấp $p^{2r} - p^{2r-1}$, J là ma trận vuông cấp $p^{2r} - p^{2r-1}$ có tất cả các phần tử đều bằng một. Đồ thị E_α có tập đỉnh trùng với tập đỉnh của RS_q. Hai đỉnh $\boldsymbol{a} = (a_1,\, a_2)$, $\boldsymbol{b} = (b_1,\, b_2) \in V(RS_q)$ được nối với nhau bởi một cạnh khi và chỉ khi $p^\alpha = (a_2 - b_2,\, p^r) \neq ((a_1 - b_1) - (a_2^2 - b_2^2),\, p^r)$. Cố định đỉnh $\boldsymbol{a} = (a_1,\, a_2)$, đỉnh $\boldsymbol{b} = (b_1,\, b_2)$ được nối với đỉnh $\boldsymbol{a}$ bởi một cạnh khi và chỉ khi

$$2(a_2 - b_2) = t_1 p^\alpha \text{ với } t_1 \in \mathbb{Z}_{r-\alpha}^\times \text{ và } (a_1 - b_1) - (a_2^2 - b_2^2) \neq t_2 p^\alpha \text{ với } t_2 \in \mathbb{Z}_{r-\alpha}^\times.$$

Từ đó, ta suy ra E_α là một đồ thị $(p^{r-\alpha} - p^{r-\alpha-1})(p^r - p^{r-\alpha} + p^{r-\alpha-1})$ - chính quy. Đồ thị F_α có tập đỉnh trùng với tập đỉnh của RS_q. Hai đỉnh $\boldsymbol{a} = (a_1,\, a_2)$ và $\boldsymbol{b} = (b_1,\, b_2) \in V(RS_q)$ được nối với nhau bởi một cạnh khi và chỉ khi $p^\alpha = (a_2 - b_2,\, p^r) = ((a_1 - b_1) - (a_2^2 - b_2^2),\, p^r)$. Cố định đỉnh $\boldsymbol{a} = (a_1,\, a_2)$, đỉnh $\boldsymbol{b} = (b_1,\, b_2)$ được nối với đỉnh $\boldsymbol{a}$ bởi một cạnh khi và chỉ khi

$$2(a_2 - b_2) = t_1 p^\alpha \text{ với } t_1 \in \mathbb{Z}_{r-\alpha}^\times \text{ và } (a_1 - b_1) - (a_2^2 - b_2^2) = t_2 p^\alpha \text{ với } t_1 \in \mathbb{Z}_{r-\alpha}^\times.$$

Lập luận tương tự, ta cũng có F_α là một đồ thị $(p^{r-\alpha} - p^{r-\alpha-1})^2$ - chính quy.

Do RS_q là đồ thị $(p^r - p^{r-1})$ - chính quy nên ma trận A có một giá trị riêng $\lambda = p^r - p^{r-1}$ với vectơ riêng tương ứng là $\mathbf{1}$. Gọi θ là một giá trị riêng của ma trận A và $\theta \neq \lambda$. Giả sử $\boldsymbol{v}_\theta$ là vectơ riêng ứng với giá trị riêng θ, ta có $\boldsymbol{v}_\theta \in \mathbf{1}_\lambda^\perp$.

Do đó, ta có $(\theta^2 - p^r + p^{r-1} + 1)v_\theta = (-\sum_{\alpha=0}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1}(p^\alpha - 1)F_\alpha)v_\theta$. Từ đó, v_θ cũng là một vectơ riêng của ma trận $-\sum_{\alpha=0}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1}(p^\alpha - 1)F_\alpha$. Suy ra:

$$\theta^2 \leq p^r - p^{r-1} - 1 + \sum_{\alpha=0}^{r-1}(p^{r-\alpha} - p^{r-\alpha-1})(p^r - p^{r-\alpha} + p^{r-\alpha-1}) +$$

$$\sum_{\alpha=1}^{r-1}(p^\alpha - 1)(p^{r-\alpha} - p^{r-\alpha-1})^2.$$

Từ đó ta thu được $\theta^2 < (2r-1)p^{2r-1}$, suy ra điều phải chứng minh. □

2.2. Đồ thị tổng - tích

2.2.1. Đồ thị tổng - tích trên trường hữu hạn

Cho $\lambda \in \mathbb{F}_q$, đồ thị tổng - tích $\mathcal{FP}_q(\lambda)$ được định nghĩa như sau: Tập đỉnh của đồ thị tổng - tích $\mathcal{FP}_q(\lambda)$ là tập $\mathbb{F}_q \times \mathbb{F}_q$. Hai đỉnh $\boldsymbol{a} = (a_1, a_2)$ và $\boldsymbol{b} = (b_1, b_2) \in V(\mathcal{FP}_q(\lambda))$ được nối với nhau bởi một cạnh $\{\boldsymbol{a}, \boldsymbol{b}\} \in E(\mathcal{FP}_q(\lambda))$ khi và chỉ khi $a_1 + b_1 + a_2 b_2 = \lambda$. Ta có định lí sau:

Định lí 2.2.1. *Đồ thị $\mathcal{FP}_q(\lambda)$ là một*

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

Chứng minh. Trước hết, ta nhận xét rằng $\mathcal{FP}_q(\lambda)$ là đồ thị q - chính quy và có q^2 đỉnh. Bây giờ chúng ta tìm chặn trên cho giá trị riêng thứ hai của đồ thị tổng - tích $\mathcal{FP}_q(\lambda)$. Với $\boldsymbol{a} = (a_1, a_2) \neq \boldsymbol{b} = (b_1, b_2) \in V(\mathcal{FP}_q(\lambda))$ ta đếm số nghiệm của hệ phương trình

$$a_1 + x_1 + a_2 x_2 = b_1 + x_1 + b_2 x_2 = \lambda,\ \boldsymbol{x} = (x_1, x_2) \in V(\mathcal{FP}_q(\lambda)).$$

Hệ có nghiệm duy nhất

$$x_1 = \lambda - \frac{a_2 b_1 - a_1 b_2}{a_2 - b_2},$$
$$x_2 = \frac{b_1 - a_1}{a_2 - b_2},$$

nếu $a_2 \neq b_2$ và không có nghiệm trong trường hợp khác. Nói cách khác, hai đỉnh khác nhau $\boldsymbol{a} = (a_1, a_2)$ và $\boldsymbol{b} = (b_1, b_2)$ có duy nhất một đỉnh chung nếu $a_2 \neq b_2$ và không có đỉnh chung trong trường hợp khác.

Gọi M là ma trận kề của đồ thị $\mathcal{FP}_q(\lambda)$. Khi đó ta có:

$$M^2 = J + (q-1)I - E,$$

trong đó J là ma trận có tất cả các phần tử đều bằng một, I là ma trận đơn vị và E là ma trận kề của đồ thị $\mathcal{S}_E$, $V(\mathcal{S}_E) = \mathbb{F}_q \times \mathbb{F}_q$, hai đỉnh $\boldsymbol{a}, \boldsymbol{b} \in V(\mathcal{S}_E)$ được nối với nhau bởi một cạnh $\{\boldsymbol{a}, \boldsymbol{b}\} \in V(\mathcal{S}_E)$ khi và chỉ khi $a_2 = b_2$. Từ đó, ta có $\mathcal{S}_E$ là một đồ thị $(q-1)$ - chính quy.

Do đồ thị $\mathcal{FP}_q(\lambda)$ là một đồ thị q - chính quy nên q là một giá trị riêng của M với vectơ riêng tương ứng là $\mathbf{1}$. Đồ thị $\mathcal{FP}_q(\lambda)$ liên thông, do đó giá trị riêng q có bội một. Tương tự chứng minh của Định lí 2.1.1, gọi θ là một giá trị riêng khác q của $\mathcal{FP}_q$. Ta có $\theta^2 < 2q - 1$, suy ra điều cần chứng minh. □

Chúng ta cũng định nghĩa đồ thị tổng - tích $\mathcal{F}_{q,d}$ như sau: Tập đỉnh của đồ thị tổng - tích $\mathcal{F}_{q,d}$ là tập $\mathbb{F}_q \times \mathbb{F}_q^d$. Hai đỉnh $U = (a, \boldsymbol{b})$ và $V = (c, \boldsymbol{d}) \in V(\mathcal{F}_{q,d})$ được nối với nhau bởi một cạnh $\{U, V\} \in E(\mathcal{F}_{q,d})$ khi và chỉ khi $a + c = \boldsymbol{b} \cdot \boldsymbol{d}$. Vinh [59] thu được kết quả sau:

Định lí 2.2.2. *([59, Bổ đề 9.1]) Cho d là một số tự nhiên lớn hơn 1, đồ thị tổng - tích $\mathcal{F}_{q,d}$ là một $(q^{d+1}, q^d, q^{d/2})$- đồ thị.*

2.2.2. Đồ thị tổng - tích trên vành hữu hạn

Đồ thị tổng - tích $\mathcal{RP}_q$ trên vành hữu hạn được định nghĩa như sau: Tập đỉnh của đồ thị tổng - tích $\mathcal{RP}_q$ là tập $\mathbb{Z}_q \times \mathbb{Z}_q$. Hai đỉnh $\boldsymbol{a} = (a_1, a_2)$ và $\boldsymbol{b} = (b_1, b_2) \in V(\mathcal{RP}_q)$ được nối với nhau bởi một cạnh $\{\boldsymbol{a}, \boldsymbol{b}\} \in E(\mathcal{RP}_q)$ khi và chỉ khi $a_1 + b_1 = a_2 b_2$. Vinh [56] thu được kết quả sau:

Định lí 2.2.3. *([56, Định lí 2.3]) Đồ thị $\mathcal{RP}_q$ là một*

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

Tương tự, đồ thị tổng - tích $\mathcal{R}_{q,d}$ được định nghĩa như sau: Tập đỉnh của đồ thị tổng - tích $\mathcal{R}_{q,d}$ là tập $V(\mathcal{R}_{q,d}) = \mathbb{Z}_q \times \mathbb{Z}_q^d$. Hai đỉnh $U = (a, \boldsymbol{b})$ và $V = (c, \boldsymbol{d}) \in V(\mathcal{R}_{q,d})$ được nối với nhau bởi một cạnh $\{U, V\} \in E(\mathcal{R}_{q,d})$ khi và chỉ khi $a + c = \boldsymbol{b} \cdot \boldsymbol{d}$. Ta có định lí sau:

Định lí 2.2.4. *Cho d là một số tự nhiên lớn hơn 1, đồ thị tổng - tích $\mathcal{R}_{q,d}$ là một*

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

Chứng minh. Trước hết, ta nhận xét rằng $\mathcal{R}_{q,d}$ là một đồ thị q^d - chính quy và có q^{d+1} đỉnh. Bây giờ chúng ta đi tìm chặn trên cho giá trị trị riêng thứ hai của đồ thị $\mathcal{R}_{q,d}$. Với $U = (a, \boldsymbol{b}) \neq V = (c, \boldsymbol{d}) \in V(\mathcal{R}_{q,d})$ ta đếm số nghiệm của hệ phương trình

$$a + u = \boldsymbol{b} \cdot \boldsymbol{v},\ c + u = \boldsymbol{d} \cdot \boldsymbol{v} \text{ với } W = (u, \boldsymbol{v}) \in V(\mathcal{R}_{q,d}). \tag{2.2.1}$$

Với mỗi nghiệm $\boldsymbol{v}$ của phương trình

$$(\boldsymbol{b} - \boldsymbol{d}) \cdot \boldsymbol{v} = a - c \tag{2.2.2}$$

tồn tại duy nhất u thỏa mãn (2.2.1). Vì vậy, chúng ta chỉ cần đếm số nghiệm của phương trình (2.2.2). Giả sử p^α là ước lớn nhất của q ($0 \leq \alpha \leq r$) sao cho tất cả các tọa độ của $\boldsymbol{b} - \boldsymbol{d}$ đều chia hết cho p^α. Nếu $p^\alpha \nmid a - c$ khi đó phương trình (2.2.2) vô nghiệm. Giả sử $p^\alpha \mid a - c$. Đặt $\gamma = \frac{a-c}{p^\alpha} \in \mathbb{Z}_{p^{r-\alpha}}$ và $\boldsymbol{x} = \frac{\boldsymbol{b}-\boldsymbol{d}}{p^\alpha} \in \mathbb{Z}_{p^{r-\alpha}}^d$. Bây giờ chúng ta đếm số nghiệm $\boldsymbol{v} \in \mathbb{Z}_{p^{r-\alpha}}^d$ của

$$\boldsymbol{x} \cdot \boldsymbol{v} = \gamma. \tag{2.2.3}$$

Do p^α là ước lớn nhất của q sao cho tất cả các tọa độ của $\boldsymbol{b} - \boldsymbol{d}$ chia hết cho p^α, tồn tại chỉ số x_j không là ước của p. Với mỗi cách chọn $v_k \in \mathbb{Z}_{p^{r-\alpha}}$, $k \neq j$, ta có duy nhất một $v_j \in \mathbb{Z}_{p^{r-\alpha}}$ thỏa mãn phương trình (2.2.3). Có nghĩa là số nghiệm của phương trình (2.2.3) là $p^{(d-1)(r-\alpha)}$. Với mỗi nghiệm của phương trình (2.2.3), thay vào phương trình (2.2.2) ta được $p^{d\alpha}$ nghiệm. Do đó, phương trình (2.2.2) có $q^{d-1}p^\alpha$ nghiệm nếu $p^\alpha \mid a - c$.

Từ đó ta có, với hai đỉnh bất kì $U = (a, \boldsymbol{b})$ và $V = (c, \boldsymbol{d}) \in V(\mathcal{R}_{q,d})$. Giả sử p^α là ước lớn nhất của q sao cho tất cả các tọa độ của $\boldsymbol{b} - \boldsymbol{d}$ cũng chia hết

cho p^α, khi đó U và V có $q^{d-1}p^\alpha$ đỉnh chung nếu $p^\alpha \mid a-c$ và không có đỉnh chung trong trường hợp còn lại.

Giả sử A là ma trận kề của $\mathcal{R}_{q,d}$. Khi đó ta có:

$$A^2 = q^{d-1}J + (q^d - q^{d-1})I - q^{d-1}\sum_{0\le\alpha<r} E_\alpha + \sum_{0<\alpha<r}(q^{d-1}p^\alpha - q^{d-1})F_\alpha, \quad (2.2.4)$$

trong đó J là ma trận có tất cả các phần tử đều bằng một, I là ma trận đơn vị, E_α là ma trận kề của đồ thị $B_{E,\alpha}$. Hai đỉnh bất kì $U = (a, \boldsymbol{b})$ và $V = (c, \boldsymbol{d}) \in V(\mathcal{R}_{q,d})$, $\{U, V\}$ là một cạnh của $B_{E,\alpha}$ khi và chỉ khi p^α là ước lớn nhất của q sao cho tất cả các tọa độ của $\boldsymbol{b}-\boldsymbol{d}$ chia hết cho p^α nhưng $c-a$ không chia hết cho p^α. F_α là ma trận kề của đồ thị $B_{F,\alpha}$, với hai đỉnh bất kì $U = (a, \boldsymbol{b})$ và $V = (c, \boldsymbol{d}) \in V(\mathcal{R}_{q,d})$, $\{U, V\}$ là một cạnh của $B_{F,\alpha}$ khi và chỉ khi p^α là ước lớn nhất của q sao cho tất cả các tọa độ của $\boldsymbol{b}-\boldsymbol{d}$ chia hết cho p^α và $c-a$ cũng chia hết cho p^α. Với $\alpha > 0$ bất kì, khi đó $B_{E,\alpha}$ là đồ thị chính quy, bậc của mỗi đỉnh nhỏ hơn $p^{(r-\alpha)d}$ và $B_{F,\alpha}$ là đồ thị chính quy, bậc của mỗi đỉnh nhỏ hơn $p^{(r-\alpha)(d+1)}$. Do đó, tất cả các giá trị riêng của E_α bị chặn bởi $p^{(r-\alpha)d}$ và tất cả các giá trị riêng của F_α bị chặn bởi $p^{(r-\alpha)(d+1)}$. E_0 là ma trận có tất cả các phần tử đều bằng không.

Do $\mathcal{R}_{q,d}$ là một đồ thị q^d - chính quy nên q^d là một giá trị riêng của A với vectơ riêng tương ứng là $\mathbf{1}$. Đồ thị $\mathcal{R}_{q,d}$ là đồ thị liên thông nên q^d có bội một. Bên cạnh đó, chọn $\boldsymbol{b}, \boldsymbol{d} \in \mathbb{Z}_q^d$ sao cho $\boldsymbol{b}\cdot\boldsymbol{d} = 2a \neq 0$ khi đó $\mathcal{R}_{q,d}$ có chứa tam giác với ba đỉnh là $(-a, \mathbf{0})$, $(a, \boldsymbol{b})$ và $(a, \boldsymbol{d})$, có nghĩa là đồ thị $\mathcal{R}_{q,d}$ không phải là đồ thị hai phần. Gọi θ là giá trị riêng khác q^d của A thì $|\theta| < q^d$. Giả sử $\boldsymbol{v}_\theta$ là vectơ riêng ứng với giá trị riêng θ. Ta có $\boldsymbol{v}_\theta \in \mathbf{1}^\perp$, suy ra $J\boldsymbol{v}_\theta = 0$. Từ (2.2.4) ta có

$$(\theta^2 - q^d + q^{d-1})\boldsymbol{v}_\theta = \left(q^{d-1}\sum_{0\le\alpha<r} E_\alpha + \sum_{0<\alpha<r}(q^{d-1}p^\alpha - q^{d-1})F_\alpha\right)\boldsymbol{v}_\theta.$$

Do đó, $\boldsymbol{v}_\theta$ là một vectơ riêng của $q^{d-1}\sum_{0\le\alpha<r} E_\alpha + \sum_{0<\alpha<r}(q^{d-1}p^\alpha - q^{d-1})F_\alpha$. Suy ra

$$\begin{aligned}\theta^2 &\le q^d - q^{d-1} + q^{d-1}\sum_{0\le\alpha<r} qp^{(r-\alpha)d} + \sum_{0<\alpha<r}(q^{d-1}p^\alpha - q^{d-1})p^{(r-\alpha)(d+1)}\\ &< q^d + 2q^{2d}\sum_{0<\alpha<r} p^{-rd} < 2rp^{(2r-1)d},\end{aligned}$$

từ đó ta có điều phải chứng minh. □

2.3. Đồ thị tích - tổng

2.3.1. Đồ thị tích - tổng trên trường hữu hạn

Cho $\lambda \in \mathbb{F}_q^*$ bất kì, đồ thị tích - tổng $\mathcal{PS}_q(\lambda)$ được định nghĩa như sau: Tập đỉnh của đồ thị tích - tổng $\mathcal{PS}_q(\lambda)$ là tập $\mathbb{F}_q^* \times \mathbb{F}_q$. Hai đỉnh $\boldsymbol{a} = (a_1, a_2)$ và $\boldsymbol{b} = (b_1, b_2) \in V(\mathcal{PS}_q(\lambda))$ được nối với nhau bởi một cạnh $\{\boldsymbol{a}, \boldsymbol{b}\} \in E(\mathcal{PS}_q(\lambda))$ khi và chỉ khi $a_1b_1(a_2 + b_2) = \lambda$. Vinh [58] đã thu được kết quả sau:

Định lí 2.3.1. *([58, Định lí 3.6]) Đồ thị $\mathcal{PS}_q(\lambda)$ là một*

$$\left((q-1)q,\ q-1,\ \sqrt{3q}\right) - \text{ đồ thị.}$$

2.3.2. Đồ thị tích - tổng trên vành hữu hạn

Đồ thị tích - tổng $\mathcal{PSR}_q$ được định nghĩa như sau: Tập đỉnh $V(\mathcal{PSR}_q) = \mathbb{Z}_q^\times \times \mathbb{Z}_q$. Hai đỉnh $\boldsymbol{a} = (a_1, a_2)$ và $\boldsymbol{b} = (b_1, b_2) \in V(\mathcal{PSR}_q)$ được nối với nhau bởi một cạnh khi và chỉ khi $a_1b_1(a_2 + b_2) = 1$. Ta có định lí sau:

Định lí 2.3.2. *Đồ thị tích - tổng $\mathcal{PSR}_q$ là một*

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

Chứng minh. Trước hết, ta nhận xét rằng đồ thị tích - tổng $\mathcal{PSR}_q$ là một đồ thị $(p^r - p^{r-1})$ - chính quy và có $p^{2r} - p^{2r-1}$ đỉnh. Với $\boldsymbol{a} = (a_1, a_2) \neq \boldsymbol{b} = (b_1, b_2) \in V(\mathcal{PSR}_q)$ ta đếm số nghiệm của hệ phương trình sau:

$$a_1x_1(a_2 + x_2) = 1 \text{ và } b_1x_1(b_2 + x_2) = 1 \text{ với } \boldsymbol{x} = (x_1, x_2) \in V(\mathcal{PSR}_q).$$

Điều đó tương đương với

$$x_2 = \frac{1}{a_1x_1} - a_2, \tag{2.3.1}$$

$$x_1 = (a_2 - b_2) = \frac{1}{a_1} - \frac{1}{b_1}. \tag{2.3.2}$$

Với mỗi x_1 thỏa mãn phương trình (2.3.2) tồn tại duy nhất x_2 thỏa mãn phương trình (2.3.1). Suy ra số nghiệm của hệ phương trình trên là số nghiệm của

phương trình (2.3.2). Giả sử $0 \leq \alpha \leq r-1$ thỏa mãn $p^\alpha = (a_2 - b_2,\ p^r)$. Ta xét hai trường hợp sau:

Trường hợp 1. Nếu $(\frac{1}{a_1} - \frac{1}{b_1},\ p^r) \neq p^\alpha$ thì phương trình (2.3.2) vô nghiệm.

Trường hợp 2. Nếu $(\frac{1}{a_1} - \frac{1}{b_1},\ p^r) = p^\alpha$, ta đặt $\beta = a_2 - b_2/p^\alpha$, $\gamma = (\frac{1}{a_1} - \frac{1}{b_1})/p^\alpha$, khi đó $x_1 = \gamma/\beta$. Thay vào phương trình (2.3.2) ta được p^α nghiệm x_1 thỏa mãn phương trình (2.3.2). Suy ra hai đỉnh $\boldsymbol{a} = (a_1,\ a_2)$ và $\boldsymbol{b} = (b_1,\ b_2) \in V(\mathcal{PSR}_q)$ bất kì thỏa mãn $p^\alpha = (a_2 - b_2,\ p^r) = (\frac{1}{a_1} - \frac{1}{b_1},\ p^r)$ thì có p^α đỉnh chung và không có đỉnh chung trong trường hợp khác.

Gọi A là ma trận kề của đồ thị $\mathcal{PSR}_q$, khi đó ta có:

$$A^2 = J + (p^r - p^{r-1} - 1)I - \sum_{\alpha=0}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1} (p^\alpha - 1)F_\alpha,$$

trong đó I là ma trận đơn vị, J là ma trận có tất cả các phần tử đều bằng một. Đồ thị E_α có tập đỉnh trùng với tập đỉnh của $\mathcal{PSR}_q$. Hai đỉnh $\boldsymbol{a} = (a_1,\ a_2)$ và $\boldsymbol{b} = (b_1,\ b_2) \in V(\mathcal{PSR}_q)$ được nối với nhau bởi một cạnh khi và chỉ khi p^α=$(a_2 - b_2,\ p^r) \neq (\frac{1}{a_1} - \frac{1}{b_1},\ p^r)$. Cố định đỉnh $\boldsymbol{a} = (a_1,\ a_2)$, đỉnh $\boldsymbol{b} = (b_1,\ b_2)$ được nối với đỉnh $\boldsymbol{a}$ bởi một cạnh khi và chỉ khi

$$a_2 - b_2 = p^\alpha t_1 \text{ với } t_1 \in \mathbb{Z}_{r-\alpha}^\times \text{ và } \frac{1}{a_1} - \frac{1}{b_1} \neq p^\alpha t_2 \text{ với } t_2 \in \mathbb{Z}_{r-\alpha}^\times.$$

Từ đó ta suy ra E_α là một đồ thị $(p^{r-\alpha} - p^{r-\alpha-1})(p^r - p^{r-\alpha} + p^{r-\alpha-1})$ - chính quy. Đồ thị F_α có tập đỉnh trùng với tập đỉnh của $\mathcal{PSR}_q$. Hai đỉnh $\boldsymbol{a} = (a_1,\ a_2)$ và $\boldsymbol{b} = (b_1,\ b_2) \in V(F_\alpha)$ được nối với nhau bởi một cạnh khi và chỉ khi $p^\alpha = (a_2 - b_2,\ p^r) = (\frac{1}{a_1} - \frac{1}{b_1},\ p^r)$. Cố định đỉnh $\boldsymbol{a} = (a_1,\ a_2)$, đỉnh $\boldsymbol{b} = (b_1,\ b_2)$ được nối với đỉnh $\boldsymbol{a}$ bởi một cạnh khi và chỉ khi

$$a_2 - b_2 = p^\alpha t_1 \text{ với } t_1 \in \mathbb{Z}_{r-\alpha}^\times \text{ và } \frac{1}{a_1} - \frac{1}{b_1} = p^\alpha t_2 \text{ với } t_2 \in \mathbb{Z}_{r-\alpha}^\times.$$

Từ hệ phương trình trên, ta suy ra F_α là một đồ thị $(p^{r-\alpha} - p^{r-\alpha-1})^2$ - chính quy.

Ta có $\mathcal{PSR}_q$ là đồ thị $(p^r - p^{r-1})$ - chính quy nên ma trận A có một giá trị riêng bằng $\lambda = p^r - p^{r-1}$, với vectơ riêng tương ứng là $\mathbf{1}$. Gọi θ là một giá trị riêng của A khác λ, ta có $|\theta| < \lambda$. Giả sử $\boldsymbol{v}_\theta$ là vectơ riêng ứng với giá trị riêng θ thì $\boldsymbol{v}_\theta \in \mathbf{1}^\perp$.

Do đó ta có $(\theta^2 - p^r + p^{r-1} + 1)v_\theta = (-\sum_{\alpha=0}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1}(p^\alpha - 1)F_\alpha)v_\theta$. Từ đó, $\boldsymbol{v}_\theta$ cũng là một vectơ riêng của ma trận $-\sum_{\alpha=0}^{r-1} E_\alpha + \sum_{\alpha=1}^{r-1}(p^\alpha - 1)F_\alpha$.

Vì vậy $\theta^2 \leq p^r - p^{r-1} - 1 + \sum_{\alpha=0}^{r-1}(p^{r-\alpha} - p^{r-\alpha-1})(p^r - p^{r-\alpha} + p^{r-\alpha-1})$

$$+\sum_{\alpha=1}^{r-1}(p^\alpha - 1)(p^{r-\alpha} - p^{r-\alpha-1})^2.$$

Từ đó suy ra điều phải chứng minh. □

2.4. Đồ thị tích

2.4.1. Đồ thị tích trên trường hữu hạn

Cho dạng song tuyến tính không suy biến $B(\cdot, \cdot)$ trên $\mathbb{F}_q^d$, với $\lambda \in \mathbb{F}$ bất kì, đồ thị tích $B_{q,d}(\lambda)$ được định nghĩa như sau: Tập đỉnh của đồ thị tích $B_{q,d}(\lambda)$ là tập $V(B_{q,d}(\lambda)) = \mathbb{F}^d \backslash (0, \ldots, 0)$. Hai đỉnh $\boldsymbol{a}$ và $\boldsymbol{b} \in V(B_{q,d}(\lambda))$ được nối với nhau bởi một cạnh $\{\boldsymbol{a}, \boldsymbol{b}\} \in E(B_{q,d}(\lambda))$ khi và chỉ khi $B(\boldsymbol{a}, \boldsymbol{b}) = \lambda$. Khi $\lambda = 0$, đồ thị tích trở thành đồ thị Erdős - Rényi, đồ thị này đã được tính giá trị riêng trong [3]. Với $\lambda \neq 0$, Vinh [59] có định lí sau:

Định lí 2.4.1. *([59, Bổ đề 9.2]) Cho d là một số tự nhiên lớn hơn 1 và $\lambda \in \mathbb{F}^*$, đồ thị tích $B_{q,d}(\lambda)$ là một*

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

2.4.2. Đồ thị tích trên vành hữu hạn

Với $\lambda \in \mathbb{Z}_q$ tùy ý, đồ thị tích $B_q(d, \lambda)$ được định nghĩa như sau: Tập đỉnh của đồ thị $B_q(d, \lambda)$ là tập $\mathbb{Z}_{p^r}^d \backslash (\mathbb{Z}_{p^r}^0)^d$. Hai đỉnh $\boldsymbol{a}$ và $\boldsymbol{b} \in V(B_q(d, \lambda))$ được nối với nhau bởi một cạnh $\{\boldsymbol{a}, \boldsymbol{b}\} \in E(B_q(d, \lambda))$ khi và chỉ khi $\boldsymbol{a} \cdot \boldsymbol{b} = \lambda$. Khi $\lambda = 0$, đồ thị tích $B_q(d, \lambda)$ cũng trở thành đồ thị Erdős - Rényi. Với $\lambda \neq 0$, Vinh [56] thu được định lí sau:

Định lí 2.4.2. *([56, Định lí 2.4]) Cho d là một số tự nhiên lớn hơn 1 và $\lambda \in \mathbb{Z}_{p^r}^{\times}$, đồ thị tích $B_q(d, \lambda)$ là một*

$$\left(p^{rd} - p^{(r-1)d},\ p^{r(d-1)},\ \sqrt{2rp^{(d-1)(2r-1)}}\right) - \textit{đồ thị.}$$

2.5. Đồ thị Euclid hữu hạn

Cho Q là một dạng toàn phương không suy biến trên $\mathbb{F}_q^d$. Với $t \in \mathbb{F}_q$ bất kì, đồ thị Euclid hữu hạn $E_q(d, Q, t)$ được định nghĩa như sau: Tập đỉnh là tập $\mathbb{F}_q^d$ và tập cạnh là

$$E = \left\{\{\boldsymbol{x}, \boldsymbol{y}\} \in \mathbb{F}_q^d \times \mathbb{F}_q^d \mid \boldsymbol{x} \neq \boldsymbol{y},\ Q(\boldsymbol{x} - \boldsymbol{y}) = t\right\}.$$

Bannai và đồng nghiệp [8] và Kwok [38] thu được định lí sau:

Định lí 2.5.1. *([8, 38]) Cho Q là một dạng toàn phương không suy biến trên $\mathbb{F}_q^d$. Với $t \in \mathbb{F}_q^*$ bất kì, đồ thị $E_q(d, Q, t)$ là một*

$$\left(q^d,\ (1 + o(1))q^{d-1},\ 2q^{(d-1)/2}\right) - \textit{đồ thị.}$$

Chương 3

Đánh giá lực lượng của một số tập hợp trên trường và vành hữu hạn

3.1. Giới thiệu về phương pháp phổ của đồ thị

Đối tượng nghiên cứu đầu tiên chúng tôi quan tâm là bài toán mở cổ điển trong hình học tổ hợp, bài toán về khoảng cách của Erdős [20]. Bài toán yêu cầu chúng ta tìm số các khoảng cách khác nhau tối thiểu được xác định bởi một tập gồm N điểm trên mặt phẳng Euclid. Có nghĩa là chúng ta cần đánh giá lực lượng cho tập khoảng cách được xác định bởi tập điểm này. Có liên quan đến đánh giá lực lượng của các tập hợp cũng được nhiều người quan tâm là đánh giá lực lượng của tập tích vô hướng, đánh giá tổng - tích, đánh giá lực lượng của tập thể tích khối, đi tìm các hàm nở...

Trong mặt phẳng, bài toán khoảng cách của Erdős, đánh giá tổng - tích có thể sử dụng nhiều tính chất hình học để giải quyết. Tuy nhiên, trên không gian hữu hạn nhiều tính chất hình học không còn đúng. Vì thế, không thể áp dụng phương pháp trên mặt phẳng cho không gian hữu hạn và dẫn đến nhiều phương pháp nghiên cứu được ra đời. Điển hình như phương pháp sử dụng giải tích Fourier được phát triển rất mạnh mẽ bởi nhóm nghiên cứu của Iosevich. Cách tiếp cận bằng giải tích Fourier kế thừa được những công cụ mạnh từ giải tích và có lợi hơn phương pháp tiếp cận bằng đồ thị là có sử dụng các cấu trúc của bài toán trên một không gian vectơ. Ngoài ra, gần đây xuất hiện phương pháp sử dụng liên thuộc điểm và đường thẳng của Rudnev [46] để nghiên cứu một số bài toán tổ hợp cộng tính cho các tập nhỏ.

Năm 2008, Vũ Hà Văn và Lê Anh Vinh đã đồng thời sử dụng (n, d, λ) - đồ

thị và Bổ đề trộn nở để nghiên cứu về một số bài toán tổ hợp cộng tính. Cụ thể, Vu [54] nghiên cứu về bài toán đánh giá tổng - tích và Vinh [55] nghiên cứu về bài toán khoảng cách của Erdős. Trong Luận án này nhóm chúng tôi sẽ tiếp tục sử dụng (n, d, λ) - đồ thị và Bổ đề trộn nở để nghiên cứu các bài toán nêu trên. Chúng tôi gọi phương pháp này là "phương pháp phổ của đồ thị".

Phương pháp phổ của đồ thị:

- *Bước 1:* Xây dựng một (n, d, λ) - đồ thị trên không gian R chúng ta đang nghiên cứu bài toán ($R = \mathbb{F}_q$ hoặc $\mathbb{Z}_q$).
  - Tập đỉnh thường là $V = R \times R \times .... \times R$ hoặc $R^\times \times R^\times \times .... \times R^\times$.
  - Hai đỉnh $\boldsymbol{a}, \boldsymbol{b}$ của đồ thị được nối với nhau bởi một cạnh khi và chỉ khi $f(\boldsymbol{a}, \boldsymbol{b}) = t$, trong đó $t \in R$ và $f : V \times V \to R$ là một hàm số. Trong mỗi bài toán chúng ta sẽ chọn một hàm f phù hợp.
- *Bước 2:* Tìm các tham số (n, d, λ) của đồ thị trên.
- *Bước 3:* Áp dụng Bổ đề trộn nở:
  - Đếm số nghiệm của phương trình $f(\boldsymbol{a}, \boldsymbol{b}) = t$ với $\boldsymbol{a} \in \mathcal{A}, \boldsymbol{b} \in \mathcal{B}$.
  - Đồng nhất số nghiệm của phương trình này với số cạnh giữa hai tập đỉnh $\mathcal{A}, \mathcal{B}$ của đồ thị trên.
  - Sử dụng Bổ đề trộn nở để đưa ra đánh giá về số cạnh của đồ thị, tương ứng với những đánh giá cho tập hợp mà chúng ta quan tâm.

Phương pháp phổ của đồ thị mặc dù có thể sử dụng để chứng minh lại và cải thiện được một số kết quả gần đây của nhiều nhà nghiên cứu và đưa ra một số kết quả khá thú vị khác nhưng lại yêu cầu rất ít cấu trúc trong bài toán. Từ quan điểm hình học, sử dụng phương pháp này chúng ta rất ít khi quan tâm đến lợi thế rằng bài toán của chúng ta có cấu trúc trên một không gian vectơ. Điều này giải thích tại sao phương pháp đó được ứng dụng vào rất nhiều bài toán khác nhau nhưng nó cũng chỉ rõ cho chúng ta thấy sự khó khăn để cải thiện các kết quả này là do sự phức tạp của hình học trên trường

hay vành hữu hạn. Trong chương này của Luận án, chúng tôi sẽ sử dụng phương pháp phổ của đồ thị để nghiên cứu một số bài toán đang được rất nhiều người quan tâm: tập khoảng cách, tập tích, tập thể tích khối, tập tổng - tỉ số và đi tìm các hàm nở hai biến.

3.2. Tập khoảng cách, tập tích

3.2.1. Giới thiệu tổng quan về bài toán tập khoảng cách và tập tích

Sử dụng giải tích Fourier trên trường hữu hạn, Iosevich và Rudnev [34] chứng minh rằng nếu $|\mathcal{E}| \geq 2q^{(n+1)/2}$ thì $\Delta(\mathcal{E}) = \mathbb{F}_q$. Hart và Iosevich [30] đã tìm điều kiện của tập $\mathcal{E}$ để $|\Delta(\mathcal{E})| \gtrsim q$. Cụ thể, họ thu được định lí sau:

Định lí 3.2.1. *([30, Định lí 1.1, Hệ quả 1.2]) Với $\mathcal{E} = E_1 \times \ldots \times E_n$, trong đó $E_1, \ldots, E_n \subset \mathbb{F}_q$ thỏa mãn $|\mathcal{E}| \gtrsim q^{\frac{n^2}{2n-1}}$. Khi đó $|\Delta(\mathcal{E})| \gtrsim q$.*

Hart, Iosevich, Koh và Rudnev [28] cũng thu được các kết quả tương tự cho tập tích trong không gian vectơ trên trường hữu hạn, được cụ thể trong định lí sau:

Định lí 3.2.2. *([28, Định lí 2.5]) Với $\mathcal{E} = E_1 \times \ldots \times E_n$, trong đó $E_1, \ldots, E_n \subset \mathbb{F}_q$ thỏa mãn $|\mathcal{E}| \gtrsim q^{\frac{n^2}{2n-1}}$. Khi đó $|\Pi(\mathcal{E})| \gtrsim q$.*

Từ Định lí 3.2.1 và Định lí 3.2.2, nếu $A \subset \mathbb{F}_q$ có lực lượng $|A| \gtrsim q^{\frac{n}{2n-1}}$ thì

$$|\Delta(A^n)|,\ |\Pi(A^n)| \gtrsim q.$$

Sử dụng phương pháp phổ của đồ thị, chúng tôi chỉ ra một cách chứng minh khác ngắn gọn hơn cho các kết quả trên. Cụ thể, chúng tôi [31] đã thu được kết quả sau:

Định lí 3.2.3. *([31, Định lí 2.3]) Với $A \subset \mathbb{F}_q$ thỏa mãn $|A| \gtrsim q^{1/2}$. Khi đó, ta có:*

$$|\Delta_{\mathbb{F}}(A^n)| \gtrsim \min\left\{q,\ \frac{|A|^{2n-1}}{q^{n-1}}\right\}.$$

Định lí 3.2.4. *([31, Định lí 2.4]) Với $A \subset \mathbb{F}_q$ thỏa mãn $|A| \gtrsim q^{1/2}$. Khi đó, ta có:*

$$|\Pi_{\mathbb{F}}(A^n)| \gtrsim \min\left\{q,\ \frac{|A|^{2n-1}}{q^{n-1}}\right\}.$$

Covert, Iosevich và Pakianathan [16] sử dụng giải tích Fourier cũng đã thu được kết quả tương tự trên vành hữu hạn.

Định lí 3.2.5. *([16, Định lí 1.3.1]) Với $\mathcal{E} \subset \mathbb{Z}_q^n$ thỏa mãn*

$$|\mathcal{E}| \gtrsim r(r+1)q^{\frac{(2r-1)n}{2r}+\frac{1}{2r}},$$

ta có:

$$\mathbb{Z}_q^\times \subset \Delta_{\mathbb{Z}_q}(\mathcal{E}).$$

Định lí 3.2.6. *([16, Định lí 1.3.2]) Với $\mathcal{E} \subset \mathbb{Z}_q^n$ thỏa mãn*

$$|\mathcal{E}| \gtrsim rq^{\frac{(2r-1)n}{2r}+\frac{1}{2r}},$$

ta có:

$$\mathbb{Z}_q^\times \subset \Pi_{\mathbb{Z}_q}(\mathcal{E}).$$

Sử dụng phương pháp phổ của đồ thị, chúng tôi [31] đã đưa ra điều kiện của tập $A \subset \mathbb{Z}_q$ để $|\Delta_{\mathbb{Z}_q}(A^n)|$, $|\Pi_{\mathbb{Z}_q}(A^n)| \gtrsim q$.

Định lí 3.2.7. *([31, Định lí 2.7]) Với $A \subset \mathbb{Z}_q$ thỏa mãn $|A| \gtrsim q^{1-\frac{1}{2r}}$, ta có:*

$$|\Delta_{\mathbb{Z}_q}(A^n)| \gtrsim \min\left\{q, \frac{|A|^{2n-1}}{(rq^{2-1/r})^{n-1}}\right\}.$$

Định lí 3.2.8. *([31, Định lí 2.8]) Với $A \subset \mathbb{Z}_q$ thỏa mãn $|A| \gtrsim q^{1-\frac{1}{2r}}$, ta có:*

$$|\Pi_{\mathbb{Z}_q}(A^n)| \gtrsim \min\left\{q, \frac{|A|^{2n-1}}{(rq^{2-1/r})^{n-1}}\right\}.$$

Lưu ý, từ Định lí 3.2.5 và Định lí 3.2.6, với $A \subset \mathbb{Z}_q$ có lực lượng

$$|A| \gtrsim r^{2/n}q^{1+\frac{1}{2rn}-\frac{1}{2r}}$$

thì

$$\mathbb{Z}_q^\times \subset \Delta_{\mathbb{Z}_q}(A^n) \text{ và } \mathbb{Z}_q^\times \subset \Pi_{\mathbb{Z}_q}(A^n).$$

Từ Định lí 3.2.7 và Định lí 3.2.8, với $A \subset \mathbb{Z}_q$ có lực lượng

$$|A| \gtrsim r^{\frac{n-1}{2n-1}}q^{1+\frac{1}{2r(2n-1)}-\frac{1}{2r}}$$

thì

$$|\Delta_{\mathbb{Z}_q}(A^n)|, \ |\Pi_{\mathbb{Z}_q}(A^n)| \gtrsim q.$$

3.2.2. Đánh giá tập khoảng cách trên trường và vành hữu hạn

Đánh giá tập khoảng cách trên trường hữu hạn

Trong phần này, chúng ta sẽ chứng minh Định lí 3.2.3. Trước hết, sử dụng phương pháp phổ của đồ thị cho đồ thị tổng - bình phương, ta có bổ đề sau:

Bổ đề 3.2.9. *Với $A, B, C \subset \mathbb{F}_q$, ta có:*

$$\left|\left\{a+(b-c)^2 : a \in A, b \in B, c \in C\right\}\right| \gtrsim \min\left\{q, \frac{|A||B||C|}{q}\right\}.$$

Chứng minh. Giả sử $D = \left\{a+(b-c)^2 : a \in A, b \in B, c \in C\right\} \subset \mathbb{F}_q$. Gọi N là số nghiệm của phương trình $-d+a+(b-c)^2 = 0$, $(a, b, c, d) \in A \times B \times C \times D$. Với mỗi $a \in A$, $b \in B$, $c \in C$ ta có duy nhất một giá trị $d \in D$ thỏa mãn phương trình trên nên $N = |A||B||C|$. Mặt khác, N là số cạnh giữa hai tập đỉnh $(-D) \times B$ và $A \times (-C)$ của đồ thị tổng - bình phương $\mathcal{FS}_q$. Từ Bổ đề 1.3.1 và Định lí 2.1.1, ta có:

$$\left||A||B||C| - \frac{|A||B||C||D|}{q}\right| \leq \sqrt{2q|A||B||C||D|},$$

tương đương với

$$|A||B||C| \leq \frac{|A||B||C||D|}{q} + \sqrt{2q|A||B||C||D|}.$$

Đặt $t = \sqrt{|D|} \geq 0$, ta được:

$$\frac{\sqrt{|A||B||C|}}{q}t^2 + \sqrt{2q}t - \sqrt{|A||B||C|} \geq 0,$$

suy ra

$$\begin{aligned}\sqrt{|D|} &\geq \frac{-\sqrt{2q}+\sqrt{2q+4|A||B||C|/q}}{2\sqrt{|A||B||C|}/q} \\ &= \frac{2\sqrt{|A||B||C|}}{\sqrt{2q}+\sqrt{2q+4|A||B||C|/q}} \\ &\gtrsim \min\left\{\sqrt{q}, \sqrt{\frac{|A||B||C|}{q}}\right\}.\end{aligned}$$

Bình phương hai vế suy ra điều phải chứng minh. □

Tiếp theo chúng ta chứng minh Định lí 3.2.3 bằng phương pháp quy nạp theo n.

Chứng minh. Với $n = 2$ tập $X = \{(a-b)^2 : a, b \in A\}$, $Y = Z = A$. Do $|X| \geq |A|/2$, từ Bổ đề 3.2.9 ta có:

$$\begin{aligned} |\Delta_{\mathbb{F}}(A^2)| &= \left|\left\{x + (y-z)^2 : x \in X, y \in Y, z \in Z\right\}\right| \\ &\gtrsim \min\left\{q, \frac{|X||Y||Z|}{q}\right\} \\ &\gtrsim \min\left\{q, \frac{|A|^3}{q}\right\}. \end{aligned}$$

Giả sử định lí đúng với n. Chúng ta chứng minh định lí cũng đúng với $n+1$. Tập $X = \Delta_{\mathbb{F}}(A^n)$, $Y = Z = A$. Theo giả thiết quy nạp, ta có:

$$|X| \gtrsim \min\left\{q, \frac{|A|^{2n-1}}{q^{n-1}}\right\}. \tag{3.2.1}$$

Áp dụng Bổ đề 3.2.9 và sử dụng điều kiện (3.2.1), ta thu được:

$$\begin{aligned} |\Delta_{\mathbb{F}}(A^{n+1})| &= \left|\left\{x + (y-z)^2 : x \in X, y \in Y, z \in Z\right\}\right| \\ &\gtrsim \min\left\{q, \frac{|X||Y||Z|}{q}\right\} \\ &\gtrsim \min\left\{q, \frac{|A|^{2n+1}}{q^n}\right\}, \end{aligned}$$

suy ra điều cần chứng minh. □

Đánh giá tập khoảng cách trên vành hữu hạn

Trong phần này, chúng ta sẽ chứng minh Định lí 3.2.7. Tương tự đánh giá tập khoảng cách trên trường hữu hạn, trước hết chúng ta cần chứng minh bổ đề sau:

Bổ đề 3.2.10. *Với $A, B, C \subset \mathbb{Z}_q$, ta có:*

$$\left|\left\{a + (b-c)^2 : a \in A, b \in B, c \in C\right\}\right| \gtrsim \min\left\{q, \frac{|A||B||C|}{rq^{2-1/r}}\right\}.$$

Chứng minh. Giả sử $D = \left\{a + (b-c)^2 : a \in A, b \in B, c \in C\right\} \subset \mathbb{Z}_q$. Gọi N là số nghiệm của phương trình $-d + a + (b-c)^2 = 0$, $(a, b, c, d) \in A \times B \times C \times D$. Với mỗi $a \in A$, $b \in B$, $c \in C$ ta có duy nhất một giá trị $d \in D$ thỏa mãn phương trình trên nên $N = |A||B||C|$. Mặt khác, N là số cạnh giữa hai tập đỉnh $(-D) \times B$ và $A \times (-C)$ của đồ thị tổng - bình phương trên vành hữu hạn. Từ Bổ đề 1.3.1 và Định lí 2.1.2, ta có:

$$\left| |A||B||C| - \frac{|A||B||C||D|}{q} \right| \leq \sqrt{2rq^{2-1/r}|A||B||C||D|},$$

tương đương với

$$|A||B||C| \leq \frac{|A||B||C||D|}{q} + \sqrt{2rq^{2-1/r}|A||B||C||D|}.$$

Đặt $t = \sqrt{|D|} \geq 0$, khi đó

$$\frac{\sqrt{|A||B||C|}}{q}t^2 + \sqrt{2rq^{2-1/r}}t - \sqrt{|A||B||C|} \geq 0,$$

từ đó ta có:

$$\begin{aligned}
\sqrt{|D|} &\geq \frac{-\sqrt{2rq^{2-1/r}} + \sqrt{2rq^{2-1/r} + 4|A||B||C|/q}}{2\sqrt{|A||B||C|}/q} \\
&= \frac{2\sqrt{|A||B||C|}}{\sqrt{2rq^{2-1/r}} + \sqrt{2rq^{2-1/r} + 4|A||B||C|/q}} \\
&\gtrsim \min\left\{\sqrt{q}, \sqrt{\frac{|A||B||C|}{rq^{2-1/r}}}\right\}.
\end{aligned}$$

Bình phương hai vế ta suy ra điều phải chứng minh. □

Tiếp theo, chúng ta chứng minh Định lí 3.2.7 bằng phương pháp quy nạp theo n.

Chứng minh. Với $n = 2$. Tập $X = \{(a-b)^2 : a, b \in A\}$, $X' = X \cap \mathbb{Z}_q^\times$ và $Y = Z = A$. Do $a, b \in \mathbb{Z}_q^\times$, $a^2 = b^2$ khi đó $a = \pm b$, ta có:

$$|X| \geq |X'| \geq \frac{|A - A| - |\mathbb{Z}_q^0|}{2} \geq \frac{|A| - p^{r-1}}{2} \gtrsim |A|.$$

Từ Bổ đề 3.2.10, ta có

$$\begin{aligned}|\Delta_{\mathbb{Z}_q}(A^2)| &= \left|\left\{x+(y-z)^2 : x\in X, y\in Y, z\in Z\right\}\right| \\ &\gtrsim \min\left\{q, \frac{|X||Y||Z|}{rq^{2-1/r}}\right\} \\ &\gtrsim \min\left\{q, \frac{|A|^3}{rq^{2-1/r}}\right\}.\end{aligned}$$

Giả sử định lí đúng với n. Chúng ta chứng minh cũng đúng với $n+1$. Tập $X=\Delta_{\mathbb{Z}_n}(A^n)$, $Y=Z=A$. Theo giả thiết quy nạp, ta có:

$$|X| \gtrsim \min\left\{q, \frac{|A|^{2n-1}}{(rq^{2-1/r})^{n-1}}\right\}. \tag{3.2.2}$$

Áp dụng Bổ đề 3.2.10 và sử dụng điều kiện (3.2.2), ta được:

$$\begin{aligned}|\Delta_{\mathbb{Z}_q}(A^{n+1})| &= \left|\left\{x+(y-z)^2 : x\in X, y\in Y, z\in Z\right\}\right| \\ &\gtrsim \min\left\{q, \frac{|X||Y||Z|}{rq^{2-1/r}}\right\} \\ &\gtrsim \min\left\{q, \frac{|A|^{2n+1}}{(rq^{2-1/r})^{n}}\right\},\end{aligned}$$

suy ra điều phải chứng minh. □

3.2.3. Đánh giá tập tích trên trường và vành hữu hạn

Trong phần này, chúng ta sẽ chứng minh Định lí 3.2.4 và Định lí 3.2.8. Tương tự chứng minh của đánh giá tập khoảng cách trên trường và vành hữu hạn, sử dụng phương pháp phổ của đồ thị và các Định lí 2.2.1, Định lí 2.2.3, ta có các bổ đề sau:

Bổ đề 3.2.11. *Với $A, B, C \subset \mathbb{F}_q$, ta có:*

$$|\{a+bc : a\in A, b\in B, c\in C\}| \gtrsim \min\left\{q, \frac{|A||B||C|}{q}\right\}.$$

Bổ đề 3.2.12. *Với $A, B, C \subset \mathbb{Z}_q$, ta có:*

$$|\{a+bc : a\in A, b\in B, c\in C\}| \gtrsim \min\left\{q, \frac{|A||B||C|}{rq^{2-1/r}}\right\}.$$

Định lí 3.2.4 và Định lí 3.2.8 được suy ra từ Bổ đề 3.2.11 và Bổ đề 3.2.12 tương ứng.

3.3. Tập thể tích khối

3.3.1. Giới thiệu tổng quan về tập thể tích khối

Cho $A \subset \mathbb{F}_q$, tập thể tích khối $\mathcal{V}_n(A)$ của tập A được định nghĩa như sau:

$$\mathcal{V}_n(A) = \underbrace{(A-A)\cdot(A-A)\cdots(A-A)}_{n}.$$

Sử dụng giải tích Fourier, Hart, Iosevich và Solymosi [29] thu được kết quả sau:

Định lí 3.3.1. *([29, Định lí 1.4]) Với $A \subset \mathbb{F}_q$ thỏa mãn $|A| \gtrsim q^{\frac{1}{2}+\frac{1}{2n}}$, ta có:*

$$\mathcal{V}_n(A) = \mathbb{F}_q.$$

Sử dụng bất đẳng thức tam giác Ruzsa, Balog [7] đã cải thiện kết quả trên.

Định lí 3.3.2. *([7, Định lí 1.1]) Với $A \subset \mathbb{F}_q$ thỏa mãn $|A| \geq q^{\frac{1}{2}+\frac{1}{2k}}$, trong đó k là số tự nhiên và $k > 1$. Khi A là một nhóm con cộng của $\mathbb{F}_q$ chúng ta cần thêm điều kiện $|A| \geq q^{\frac{1}{2}} + 1$. Khi đó, ta có:*

$$\mathcal{V}_{2k+1}(A) = \mathbb{F}_q.$$

Hệ quả 3.3.3. *([7, Hệ quả 1]) Với $A \subset \mathbb{F}_q$ thỏa mãn $|A| \geq q^{\frac{1}{2}}$. Nếu A là một nhóm con cộng của $\mathbb{F}_q$ thỏa mãn $|A| \geq q^{\frac{1}{2}} + 1$. Khi đó, ta có:*

$$|\mathcal{V}_k(A)| \geq q^{1-\frac{1}{2^k}}.$$

Sử dụng phương pháp phổ của đồ thị và Hệ quả 3.3.3, chúng tôi [32] cũng thu được kết quả về tập thể tích khối.

Định lí 3.3.4. *([32, Định lí 1.4]) Với $A \subset \mathbb{F}_q$ thỏa mãn $|A| \gtrsim q^{\frac{1}{2}}$, ta có:*

$$|\mathcal{V}_n(A)| \gtrsim \min\left\{q, \frac{|A|^2}{q^{\frac{1}{2^{n-1}}}}\right\}.$$

Trong trường hợp đặc biệt, từ Định lí 3.3.4 dẫn đến nếu $A \subset \mathbb{F}_q$ thỏa mãn

$$|A| \gtrsim q^{\frac{1}{2}+\frac{1}{2^n}}$$

thì

$$|\mathcal{V}_n(A)| \gtrsim q.$$

Với $A \subset \mathbb{Z}_q$ chúng ta định nghĩa tập thể tích khối tương tự như trên trường hữu hạn. Khi sử dụng phương pháp phổ của đồ thị cho đồ thị tích - tổng trên vành hữu hạn, chúng ta cũng thu được kết quả tương tự cho tập thể tích khối trên vành hữu hạn. Cụ thể, chúng tôi [32] chứng minh được kết quả sau:

Định lí 3.3.5. *([32, Định lí 1.5]) Với $A \subset \mathbb{Z}_q$ thỏa mãn $|A| \gtrsim q^{1-\frac{1}{2r}}$, ta có:*

$$|\mathcal{V}_n(A)| \gtrsim \min\left\{p^r, \frac{|A|^2}{2rp^{r-1+\frac{1}{2^{n-1}}}}\right\}.$$

Sử dụng phương pháp phổ của đồ thị và Định lí 3.3.4, chúng tôi [32] đã cải thiện được kết quả của Định lí 3.3.2.

Định lí 3.3.6. *([32, Định lí 1.6]) Với $A \subset \mathbb{F}_q$ thỏa mãn $|A| \gtrsim q^{\frac{1}{2}+\frac{2}{3}\frac{1}{2^k}}$, trong đó $k > 1$, ta có:*

$$\mathcal{V}_{2k+1}(A) = \mathbb{F}_q.$$

Chúng tôi [32] cũng có kết quả tương tự trên vành hữu hạn.

Định lí 3.3.7. *([32, Định lí 1.7]) Với $A \subset \mathbb{Z}_q$ thỏa mãn*

$$|A| \gtrsim \sqrt{2r}q^{1-\frac{1}{2r}+\frac{1}{3/2\cdot r2^k}},$$

ta có:

$$\mathbb{Z}_q^\times \subset \mathcal{V}_{2k+1}(A).$$

3.3.2. Một số kết quả cần dùng

Để chứng minh Định lí 3.3.7, chúng ta cần một số kết quả sau:

Bổ đề 3.3.8. *Với A, $B \subset \mathbb{Z}_q$ thỏa mãn $|A||B| > q^{2-\frac{1}{r}}$, ta có:*

$$\mathbb{Z}_q^\times \subset \frac{A-A}{(B-B)\setminus \mathbb{Z}_q^0}.$$

Chứng minh. Với $x \in \mathbb{Z}_q^\times$ bất kì, xét tập $A - xB \subset \mathbb{Z}_q$. Do $|A - xB| \leq p^r < \frac{|A||B|}{p^{r-1}}$ nên tồn tại p^{r-1} cặp phân biệt $(a_1, b_1), (a_2, b_2), \ldots, (a_{p^{r-1}}, b_{p^{r-1}})$ sao cho $a_i - xb_i = a_j - xb_j$, tương đương với $x(b_i - b_j) = a_i - a_j$. Nếu $a_i = a_j$ thì $b_i = b_j$ nên $a_j \neq a_j$ với mọi $i \neq j$. Đặt $M = \{a_1, a_2, \ldots, a_{p^{r-1}}\}$. Do $|M - M| > |M| = p^{r-1}$, nên tồn tại i_o, j_o sao cho $a_{i_o} - a_{j_o} \in \mathbb{Z}_q^\times$, suy ra $x = \frac{b_{i_o} - b_{j_o}}{a_{i_o} - a_{j_o}} \in \frac{A-A}{(B-B)\setminus \mathbb{Z}_q^0}$, dẫn tới điều phải chứng minh. □

Bổ đề dưới đây được gọi là Bất đẳng thức tam giác Ruzsa, đây là một kết quả rất quan trọng trong tổ hợp.

Bổ đề 3.3.9. *([47]) Cho U, V, W là các tập con hữu hạn của nhóm G bất kì. Khi đó, ta có:*

$$|UV^{-1}||W| \leq |UW||VW|.$$

Từ Bổ đề 3.3.8 và Bổ đề 3.3.9 chúng ta thu được được kết quả sau trên vành hữu hạn:

Bổ đề 3.3.10. *Với $A \subset \mathbb{Z}_q$ thỏa mãn $|A| \geq q^{1-\frac{1}{2r}}$. Khi đó, ta có:*

$$|\mathcal{V}_n(A)| \gtrsim q^{1-\frac{1}{r2^n}}.$$

Chứng minh. Đặt $U = V = (A - A) \setminus \mathbb{Z}_q^0$ và $W = V^n$. Áp dụng Bổ đề 3.3.9 với $G = \mathbb{Z}_q$ ta được:

$$|UV^{-1}||V^n| \leq |V^{n+1}|^2.$$

Từ Bổ đề 3.3.8, nếu $|A| > p^{r-\frac{1}{2}}$ thì $\mathbb{Z}_q^\times \subset \frac{A-A}{(A-A)\setminus \mathbb{Z}_q^0}$. Vì $\mathbb{Z}_q^\times$ là tập các phần tử khả nghịch của $\mathbb{Z}_q$ nên suy ra $\mathbb{Z}_q^\times \subset \frac{(A-A)\setminus \mathbb{Z}_q^0}{(A-A)\setminus \mathbb{Z}_q^0}$. Từ đó, ta có $|UV^{-1}| \geq p^r - p^{r-1}$, kéo theo

$$(p^r - p^{r-1})|V^n| \leq |V^{n+1}|^2.$$

Sử dụng phương pháp quy nạp ta thu được:

$$(p^r - p^{r-1})^{2^n-1}|V| \leq |V^{n+1}|^{2^n}.$$

Mặt khác, dễ thấy $|V| = |(A - A) \setminus \mathbb{Z}_q^0| > p^{r-\frac{1}{2}} - p^{r-1}$, vì thế

$$|\mathcal{V}_n(A)| \geq |V^n| \gtrsim q^{1-\frac{1}{r2^n}},$$

ta có điều phải chứng minh. □

Sử dụng phương pháp phổ của đồ thị, ta có bổ đề sau:

Bổ đề 3.3.11. *Với $A, B \subset \mathbb{F}_q^*$ và $C, D \subset \mathbb{F}_q$ thỏa mãn $|A||B||C||D| \geq 3q^3$. Khi đó, ta có:*

$$AB(C-D) = \mathbb{F}_q.$$

Chứng minh. Đặt $H = \{(a, b, c, d) \in A \times B \times C \times D : \ ab(c-d) = \lambda\}$, với $\lambda \in \mathbb{F}_q^*$ bất kì. Ngoài ra, $|H|$ là số cạnh giữa hai tập đỉnh $A \times C$ và $B \times D$ của đồ thị tích - tổng $\mathcal{PS}_q(\lambda)$. Từ Bổ đề 1.3.1 và Định lí 2.3.1, ta có:

$$\left| |H| - \frac{|A||B||C||D|}{q} \right| \leq \sqrt{3q|A||B||C||D|},$$

tương đương với

$$|H| \geq \frac{|A||B||C||D|}{q} - \sqrt{3q|A||B||C||D|}.$$

Nếu $|A||B||C||D| > 3q^3$ khi đó $|H| > 0$, từ đó suy ra

$$AB(C-D) = \mathbb{F}_q,$$

đây là điều phải chứng minh. □

Tương tự, chúng ta cũng chứng minh được bổ đề sau trên vành hữu hạn:

Bổ đề 3.3.12. *Với $A, B \subset \mathbb{Z}_q^\times$ và $C, D \subset \mathbb{Z}_q$ thỏa mãn $|A||B||C||D| \geq 2rq^{4-\frac{1}{r}}$. Khi đó, ta có:*

$$\mathbb{Z}_q^\times \subset AB(C-D).$$

Chứng minh. Đặt $H = \{(a, b, c, d) \in A \times B \times C \times D : \ ab(c-d) = \lambda\}$, với $\lambda \in \mathbb{Z}_q^\times$ bất kì. Ngoài ra, $|H|$ là số cạnh giữa hai tập đỉnh $A \times C$ và $B \times D$ của đồ thị tích - tổng $\mathcal{PSR}_q$. Từ Bổ đề 1.3.1 và Định lí 2.3.2, ta có:

$$\left| |H| - \frac{|A||B||C||D|}{p^r} \right| \leq \sqrt{2rp^{2r-1}|A||B||C||D|},$$

tương đương với

$$|H| \geq \frac{|A||B||C||D|}{p^r} - \sqrt{2rp^{2r-1}|A||B||C||D|}.$$

Nếu $|A||B||C||D| > 2rp^{4r-1}$, khi đó $|H| > 0$, từ đó suy ra

$$\mathbb{Z}_q^\times \subset AB(C-D),$$

điều phải chứng minh. □

3.3.3. Đánh giá tập thể tích khối trên trường hữu hạn

Trong phần này, chúng ta sẽ chứng minh Định lí 3.3.4 và Định lí 3.3.6 bằng phương pháp phổ của đồ thị. Trước hết, ta sẽ chứng minh Định lí 3.3.4.

Chứng minh. Với $A \subset \mathbb{F}_q^*$ và B, $C \subset \mathbb{F}_q$, ta đặt

$$D = \{a(b-c) : a \in A,\, b \in B,\, c \in C\} \cap \mathbb{F}_q^*.$$

Giả sử N là số nghiệm của phương trình $ad(b-c) = 1$, $(a, b, c, d) \in A \times B \times C \times D^{-1}$. Với mỗi $a \in A$, $b \in B$, $c \in C$ và $b \neq c$ thì có duy nhất một $d \in D$ thỏa mãn phương trình $ad(b-c) = 1$ nên $N = |A||B||C| - |A||B \cap C|$. Mặt khác, N là số cạnh giữa hai tập đỉnh $A \times B$ và $D^{-1} \times (-C)$ của đồ thị tích - tổng $\mathcal{PS}_q$. Từ Bổ đề 1.3.1 và Định lí 2.3.1, ta có:

$$\left| |A||B||C| - |A||B \cap C| - \frac{|A||B||C||D|}{q} \right| \leq \sqrt{3q|A||B||C||D|},$$

tương đương với

$$|A||B||C| - |A||B \cap C| \leq \frac{|A||B||C||D|}{q} + \sqrt{3q|A||B||C||D|}.$$

Đặt $t = \sqrt{|D|} \geq 0$, ta được:

$$\frac{\sqrt{|A||B||C|}}{q}\, t^2 + \sqrt{3q}\, t - \sqrt{|A||B||C|} + \sqrt{\frac{|A|}{|B||C|}}|B \cap C| \geq 0,$$

suy ra

$$\begin{aligned}
\sqrt{|D|} &\geq \frac{-\sqrt{3q} + \sqrt{3q + 4|A||B||C|/q - 4|A||B \cap C|/q}}{2\sqrt{|A||B||C|}/q} \\
&\geq \frac{-\sqrt{3q} + \sqrt{3q + |A||B||C|/q}}{2\sqrt{|A||B||C|}/q} \\
&= \frac{2^{-1}\sqrt{|A||B||C|}}{\sqrt{3q} + \sqrt{3q + |A||B||C|/q}} \\
&\gtrsim \min\left\{\sqrt{q}, \sqrt{\frac{|A||B||C|}{q}}\right\}.
\end{aligned}$$

Thay $A = \mathcal{V}_{n-1}(A)$, $B = C = A$ và từ Hệ quả 3.3.3, ta có:

$$|\mathcal{V}_n(A)| \gtrsim \min\left\{q, \frac{|A|^2}{q^{\frac{1}{2^{n-1}}}}\right\},$$

điều phải chứng minh. □

Tiếp theo, chúng ta chứng minh Định lí 3.3.6. Chúng ta sẽ tìm điều kiện cho tập A để tập thể tích khối chiếm toàn bộ không gian $\mathbb{F}_q$.

Chứng minh. Áp dụng Bổ đề 3.3.11 với $A = \mathcal{V}_k(A)$, $B = \mathcal{V}_k(A)$, $C = D = A$ và sử dụng kết quả của Định lí 3.3.4 ta có, nếu $|A| \geq cq^{\frac{1}{2}+\frac{1}{3/2\cdot 2^k}}$ thì

$$\mathcal{V}_{2k+1}(A) = \mathbb{F}_q,$$

điều phải chứng minh. □

3.3.4. Đánh giá tập thể tích khối trên vành hữu hạn

Trong phần này, chúng ta cũng sử dụng phương pháp phổ của đồ thị để chứng minh Định lí 3.3.5 và Định lí 3.3.7. Các kĩ thuật ở đây tương tự với chứng minh của Định lí 3.3.4 và Định lí 3.3.6. Trước hết, chúng ta sẽ chứng minh Định lí 3.3.5.

Chứng minh. Với $A \subset \mathbb{Z}_q^\times$ và $B, C \subset \mathbb{Z}_q$, ta đặt

$$D = \{a(b-c) : \ a \in A, b \in B, c \in C\} \cap \mathbb{Z}_q^\times.$$

Giả sử N là số nghiệm của phương trình $ad(b-c) = 1$, $(a, b, c, d) \in A \times B \times C \times D^{-1}$. Với mỗi $a \in A$, $b \in B$, $c \in C$ và $b - c \notin \mathbb{Z}_q^0$ thì có duy nhất một $d \in D$ thỏa mãn phương trình trên nên số nghiệm của phương trình trên là:

$$N = |A||B||C| - |A| \sum_{t \in \mathbb{Z}_q^0} |B \cap (C+t)|.$$

Mặt khác, N là số cạnh giữa hai tập đỉnh $A \times B$ và $D^{-1} \times (-C)$ của đồ thị tích - tổng $\mathcal{PSR}_q$. Từ Bổ đề 1.3.1 và Bổ đề 2.3.2, ta có:

$$\left| |A||B||C| - |A| \sum_{t \in \mathbb{Z}_q^0} |B \cap (C+t)| - \frac{|A||B||C||D|}{p^r} \right| \leq \sqrt{2rp^{2r-1}|A||B||C||D|},$$

tương đương với

$$\frac{\sqrt{|A||B||C|}|D|}{p^r} + \sqrt{2rp^{2r-1}|D|} - \sqrt{|A||B||C|} + \sqrt{\frac{|A|}{|B||C|}} \sum_{t \in \mathbb{Z}_q^0} |B \cap (C+t)| \geq 0.$$

Đặt $x = \sqrt{|D|} \geq 0$, ta được:

$$\frac{\sqrt{|A||B||C|}}{p^r} x^2 + \sqrt{2rp^{2r-1}}\, x - \sqrt{|A||B||C|} + \sqrt{\frac{|A|}{|B||C|}} \sum_{t \in \mathbb{Z}_q^0} |B \cap (C+t)| \geq 0,$$

từ đó ta có:

$$\sqrt{|D|} \geq \frac{-\sqrt{2rp^{2r-1}} + \sqrt{2rp^{2r-1} + |A||B||C|p^{-r}}}{2\sqrt{|A||B||C|}\, p^{-r}}$$

$$= \frac{\sqrt{|A||B||C|}}{2(\sqrt{2rp^{2r-1}} + \sqrt{2rp^{2r-1} + |A||B||C|\, p^{-r}})}$$

$$\gtrsim \min\left\{\sqrt{p^r}, \sqrt{\frac{|A||B||C|}{2rp^{2r-1}}}\right\}.$$

Thay $A = \mathcal{V}_{n-1}(A)$, $B = C = A$ và sử dụng kết quả của Bổ đề 3.3.10 ta thu được:

$$|\mathcal{V}_n(A)| \gtrsim \min\left\{p^r, \frac{|A|^2}{2rp^{r-1+\frac{1}{2^{n-1}}}}\right\},$$

điều phải chứng minh. □

Tiếp theo, chúng ta sẽ chứng minh Định lí 3.3.7. Chúng ta tìm điều kiện cho tập A để tập thể tích khối chiếm toàn bộ các phần tử khả nghịch của vành hữu hạn $\mathbb{Z}_q$.

Chứng minh. Áp dụng Bổ đề 3.3.12 với $A = \mathcal{V}_k(A)$, $B = \mathcal{V}_k(A)$, $C = D = A$ và sử dụng kết quả của Định lí 3.3.5, ta có nếu $|A| \geq c\sqrt{2r}q^{1-\frac{1}{2r}+\frac{1}{3/2\cdot r2^k}}$ thì

$$\mathbb{Z}_q^\times \subset \mathcal{V}_{2k+1}(A),$$

đây là điều phải chứng minh. □

3.4. Tập tổng - tỉ số

3.4.1. Giới thiệu tổng quan về bài toán tổng - tỉ số

Với $A \subset \mathbb{F}_q^*$, tập tỉ số được định nghĩa như sau:

$$A : A = \{a/b : \ a, b \in A\}.$$

Khi thay tập tích AA bằng tập tỉ số $A : A$, Roche - Newton [43] sử dụng bất đẳng thức tam giác Ruzsa đã thu được các kết quả sau:

Định lí 3.4.1. *([5, Định lí 2]) Giả sử $A \subset \mathbb{F}_q$ thỏa mãn*

$$|A \cap cG| \leq \max\{|G|^{1/2}, \frac{|A|}{8}\}$$

với G là một trường con của $\mathbb{F}_q$ và $c \in \mathbb{F}_q$. Khi đó ta có:

$$|A + A|^7 |A : A|^4 \gtrsim |A|^{12},$$

hoặc

$$|A + A|^6 |A : A|^5 \gtrsim |A|^{12}.$$

Dẫn đến

$$\max\{|A + A|, |A : A|\} \gtrsim |A|^{12/11}.$$

Định lí 3.4.2. *([5, Định lí 4.1]) Giả sử $A \subset \mathbb{F}_q$ thỏa mãn*

$$|A \cap cG| \leq \max\{|G|^{1/2}, \frac{|A|}{8}\}$$

với G là trường con của $\mathbb{F}_q$ và $c \in \mathbb{F}_q$. Khi đó ta có:

$$|A + A + A + A|^5 |A : A|^4 \gtrsim |A|^{10},$$

hoặc

$$|A + A + A + A|^4 |A : A|^5 \gtrsim |A|^{10}.$$

Dẫn đến

$$\max\{|A + A + A + A|, |A : A|\} \gtrsim |A|^{10/9}.$$

Trong chương này, chúng tôi sử dụng phương pháp phổ của đồ thị để đánh giá lực lượng của tập tổng - tỉ số cho trường hợp tập A có kích thước lớn. Cụ thể, ta có định lí sau:

Định lí 3.4.3. *Với $A, B, C \subset \mathbb{F}_q$ và $0 \notin B$, ta có:*

$$|\underbrace{A + \ldots + A}_{d} + C||A \cdot B|^d \gtrsim \min\left\{q|A|^d, \frac{|A|^{2d}|B|^d|C|}{q^d}\right\}.$$

Thay B bằng A^{-1} và thay C bằng A ta thu được hệ quả sau:

Hệ quả 3.4.4. *Với $A \subset \mathbb{F}_q^*$, ta có:*

$$|\underbrace{A+\ldots+A}_{d+1}||A:A|^d \gtrsim \min\left\{q|A|^d, \frac{|A|^{3d+1}}{q^d}\right\}.$$

Dẫn đến

$$\max\{|\underbrace{A+\ldots+A}_{d+1}|, |A:A|\} \gtrsim \min\left\{\sqrt[d+1]{q|A|^d}, \frac{|A|^{\frac{3d+1}{d+1}}}{\sqrt[d+1]{q^d}}\right\}.$$

Từ Hệ quả 3.4.4, ta có:

- Nếu $d = 1$ và $A \subset \mathbb{F}_q$ thỏa mãn

$$|A| \gtrsim q^{\frac{11}{20-22\epsilon}}$$

thì

$$\max\{|A+A|, |A:A|\} \gtrsim |A|^{12/11+\epsilon}.$$

- Nếu $d = 3$ và $A \subset \mathbb{F}_q$ thỏa mãn

$$|A| \gtrsim q^{\frac{27}{50-36\epsilon}}$$

thì

$$\max\{|A+A+A+A|, |A:A|\} \gtrsim |A|^{10/9+\epsilon}.$$

Tương tự, với $A \subset \mathbb{Z}_q^\times$ chúng ta cũng có định nghĩa tập tỉ số tương tự như trên trường hữu hạn. Sử dụng phương pháp phổ của đồ thị chúng tôi cũng thu được kết quả tương tự cho tập tổng - tỉ số trên vành hữu hạn.

Định lí 3.4.5. *Với $A, C \subset \mathbb{Z}_q$ và $B \subset \mathbb{Z}_q^\times$, ta có:*

$$|\underbrace{A+\ldots+A}_{d}+C||A\cdot B|^d \gtrsim \min\left\{p^r|A|^d, \frac{|A|^{2d}|B|^d|C|}{2rp^{(2r-1)d}}\right\}.$$

Thay B bằng A^{-1} và thay C bằng A chúng ta thu được hệ quả sau:

Hệ quả 3.4.6. *Với $A \subset \mathbb{Z}_q^\times$, ta có:*

$$|\underbrace{A+\ldots+A}_{d+1}||A:A|^d \gtrsim \min\left\{p^r|A|^d, \frac{|A|^{3d+1}}{2rp^{(2r-1)d}}\right\}.$$

Dẫn đến

$$\max\{|\underbrace{A+\ldots+A}_{d+1}|, |A:A|\} \gtrsim \min\left\{\sqrt[d+1]{p^r|A|^d}, \frac{|A|^{\frac{3d+1}{d+1}}}{\sqrt[d+1]{2rp^{(2r-1)d}}}\right\}.$$

3.4.2. Đánh giá tổng - tỉ số trên trường hữu hạn

Trong phần này, chúng ta sẽ sử dụng phương pháp phổ của đồ thị để chứng minh Định lí 3.4.3.

Chứng minh. Giả sử N là số nghiệm của phương trình

$$s_1 \cdot b_1^{-1} + s_2 \cdot b_2^{-1} + \ldots + s_d \cdot b_d^{-1} + c = t,\ (s_i, b_j, c, t) \in S \times B \times C \times T,$$

với

$$S = A \cdot B,\ T = A + A + \ldots + A + C.$$

Ta có $N \geq |A|^d|B|^d|C|$. Mặt khác, N là số cạnh giữa hai tập đỉnh $U = C \times B^{-1} \times \ldots \times B^{-1}$ và $V = (-T) \times S \times \ldots \times S$ của đồ thị tổng - tích $\mathcal{F}_{q,d}$. Từ Bổ đề 1.3.1 và Định lí 2.2.2, ta có:

$$\left|N - \frac{|S|^d|B|^d|C||T|}{q}\right| \leq \sqrt{q^d|S|^d|B|^d|C||T|},$$

tương đương với

$$|A|^d|B|^d|C| \leq N \leq \frac{|S|^d|B|^d|C||T|}{q} + \sqrt{q^d|S|^d|B|^d|C||T|}.$$

Đặt $t = \sqrt{|S|^d|T|} \geq 0$, ta được:

$$\frac{\sqrt{|B|^d|C|}}{q}t^2 + \sqrt{q^d}t - |A|^d\sqrt{|B|^d|C|} \geq 0,$$

từ đó suy ra

$$\begin{aligned}\sqrt{|S|^d|T|} &\geq \frac{-\sqrt{q^d}+\sqrt{q^d+4|A|^d|B|^d|C|/q}}{2\sqrt{|B|^d|C|}/q}\\ &= \frac{2|A|^d\sqrt{|B|^d|C|}}{\sqrt{q^d}+\sqrt{q^d+4|A|^d|B|^d|C|/q}}\\ &\gtrsim \min\left\{\sqrt{q|A|^d}, \sqrt{\frac{|A|^{2d}|B|^d|C|}{q^d}}\right\},\end{aligned}$$

suy ra điều phải chứng minh. □

3.4.3. Đánh giá tổng - tỉ số trên vành hữu hạn

Trong phần này, chúng ta sẽ chứng minh Định lí 3.4.5, chúng ta mở rộng kết quả về tập tổng - tỉ số trên vành hữu hạn.

Chứng minh. Đặt N là số nghiệm của phương trình

$$s_1 \cdot b_1^{-1} + s_2 \cdot b_2^{-1} + \ldots + s_d \cdot b_d^{-1} + c = t,\ (s_i,\ b_j,\ c,\ t) \in S \times B \times C \times T,$$

với $S = A \cdot B$, $T = A + A + \ldots + A + C$.
Dễ thấy $N \geq |A|^d|B|^d|C|$. Ngoài ra, N là số cạnh giữa hai tập đỉnh $U = C \times B^{-1} \times \ldots \times B^{-1}$ và $V = (-T) \times S \times \ldots \times S$ của đồ thị tổng - tích $\mathcal{R}_{q,d}$. Từ Bổ đề 1.3.1 và Định lí 2.2.4, ta có:

$$\left|N - \frac{|S|^d|B|^d|C||T|}{p^r}\right| \leq \sqrt{2rp^{(2r-1)d}|S|^d|B|^d|C||T|}.$$

Tương tự chứng minh của Định lí 3.4.3 ta suy ra điều cần chứng minh. □

3.5. Hàm nở hai biến

3.5.1. Giới thiệu tổng quan về hàm nở hai biến

Trong phần lớn các trường hợp nếu một hàm số chứa nhiều phép toán và có đầy đủ cả phép cộng và phép nhân thì tập ảnh của hàm số có tính giãn nở mạnh. Vì vậy, việc đi tìm các lớp hàm nở hai biến sẽ khó khăn hơn rất nhiều so với việc đi tìm các hàm nở nhiều biến hơn. Garaev và Shen [23] đã chứng

minh $f = x(y+1)$ là một hàm nở hai biến với x, $y \in A$ và tập A có kích thước lớn. Cụ thể, ta có định lí sau:

Định lí 3.5.1. *([23, Định lí 2]) Với $A \subset \mathbb{F}_p^*$, ta có:*

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

Từ Định lí 3.5.1, chúng ta thấy rằng $f = x(y+1)$ là một hàm nở hai biến với x, $y \in A$ và $|A| \gg p^{1/2}$. Sử dụng bất đẳng thức tam giác Ruzsa, Timothy, Jones và Roche - Newton [52] đã chứng minh được $f = x(y+1)$ là một hàm nở hai biến với x, $y \in A$ và $|A| < p^{1/2}$.

Định lí 3.5.2. *([52, Định lí 1]) Với $A \subset \mathbb{F}_q$ thỏa mãn $|A| < p^{1/2}$, ta có:*

$$|A(A+1)| \geq |A|^{57/56}.$$

Trong Luận án này, sử dụng phương pháp phổ của đồ thị chúng tôi cũng thu được kết quả tương tự cho trường hợp tập A có kích thước lớn. Cụ thể, ta có định lí sau:

Định lí 3.5.3. *Với $A \subset \mathbb{F}_q \setminus \{0, q-1\}$, ta có:*

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

Sử dụng phương pháp phổ của đồ thị cho đồ thị tích trên vành hữu hạn $\mathbb{Z}_q$, chúng ta cũng thu được kết quả tương tự.

Định lí 3.5.4. *Với $A \subset \mathbb{Z}_q \setminus \{p\mathbb{Z}_{p^{r-1}}, p\mathbb{Z}_{p^{r-1}} - 1\}$, ta có:*

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

Bằng những kĩ thuật tương tự, khi sử dụng đồ thị tổng - bình phương chúng tôi cũng chứng minh được $g = x + y^2$ là một hàm nở hai biến trên trường và vành hữu hạn với x, $y \in A$ và $|A| \gg q^{1/2}$. Cụ thể, ta có các định lí sau:

Định lí 3.5.5. *Với $A \subset \mathbb{F}_q$, ta có:*

$$|A + A^2| \gtrsim \min\left\{\sqrt{q|A|}, \frac{|A|^2}{\sqrt{q}}\right\},$$

trong đó $A^2 = \{a^2 : a \in A\}$.

Kết quả tương tự trên vành hữu hạn.

Định lí 3.5.6. *Với $A \subset \mathbb{Z}_q$ thỏa mãn $|A| \gtrsim q^{\frac{1}{2}}$, khi đó ta có:*

$$|A + A^2| \gtrsim \min\left\{\sqrt{p^r|A|}, \frac{|A|^2}{\sqrt{2rp^{2r-1}}}\right\},$$

trong đó $A^2 = \{a^2 : a \in A\}$.

3.5.2. Hàm nở $f = x(y+1)$

Hàm nở $f = x(y+1)$ trên trường hữu hạn

Bây giờ chúng ta sẽ chứng minh Định lí 3.5.3. Chúng ta chứng minh $f = x(y+1)$ là một hàm nở hai biến với $x, y \in A$ và $|A| \gg q^{1/2}$.

Chứng minh. Giả sử N là số nghiệm của phương trình

$$(s \cdot b^{-1} + 1)c = t,\ (s, b, c, t) \in S \times B \times C \times T,$$

với

$$S = A(D+1),\ B = D+1,\ T = C(A+1).$$

Ta có $N \geq |A||B||C|$. Ngoài ra, N là số cạnh giữa hai tập đỉnh $C^{-1} \times B^{-1}$ và $T \times (-S)$ của đồ thị Tích $B_{q,2}(1)$. Từ Bổ đề 1.3.1 và Định lí 2.4.1, ta có:

$$\left|N - \frac{|S||B||C||T|}{q - 1/q}\right| \leq \sqrt{q|S||B||C||T|},$$

tương đương với

$$|A||B||C| \leq N \leq \frac{|S||B||C||T|}{q-1/q} + \sqrt{q|S||B||C||T|} < \frac{|S||B||C||T|}{q-1} + \sqrt{q|S||B||C||T|}.$$

Đặt $t = \sqrt{|S||T|} \geq 0$, ta được:

$$\frac{\sqrt{|B||C|}}{q-1}t^2 + \sqrt{q}t - |A|\sqrt{|B||C|} \geq 0,$$

suy ra

$$\begin{aligned}\sqrt{|S||T|} &\geq \frac{-\sqrt{q}+\sqrt{q+4|A||B||C|/(q-1)}}{2\sqrt{|B||C|}/(q-1)} \\ &= \frac{2|A|\sqrt{|B||C|}}{\sqrt{q}+\sqrt{q+4|A||B||C|/(q-1)}} \\ &\gtrsim \min\left\{\sqrt{q|A|}, \sqrt{\frac{|A|^2|B||C|}{q}}\right\} \\ &= \min\left\{\sqrt{q|A|}, \sqrt{\frac{|A|^2|D||C|}{q}}\right\}.\end{aligned}$$

Thay C và D bằng A, ta suy ra điều phải chứng minh. □

Hàm nở $f = x(y+1)$ trên vành hữu hạn

Bây giờ chúng ta sẽ chứng minh Định lí 3.5.5.

Chứng minh. Giả sử N là số nghiệm của phương trình

$$(sb^{-1}+1)c = t,\ (s,\ b,\ c,\ t) \in S \times B \times C \times T,$$

với

$$S = A(D+1),\ B = D+1,\ T = C(A+1).$$

Ta có $N \geq |A||B||C|$. Mặt khác, N là số cạnh giữa hai tập đỉnh $C^{-1} \times B^{-1}$ và $T \times (-S)$ của đồ thị Tích $B_q(2,\ 1)$. Từ Bổ đề 1.3.1 và Định lí 2.4.2, ta có:

$$\left|N - \frac{|S||B||C||T|}{p^r(1-1/p^2)}\right| \leq \sqrt{2rp^{2r-1}|S||B||C||T|},$$

tương đương với

$$|A||B||C| \leq N \leq \frac{|S||B||C||T|}{p^r(1-1/p^2)} + \sqrt{2rp^{2r-1}|S||B||C||T|},$$

điều này kéo theo

$$|A||B||C| < \frac{|S||B||C||T|}{p^r/2} + \sqrt{2rp^{2r-1}|S||B||C||T|},$$

Đặt $t = \sqrt{|S||T|} \geq 0$, ta được:

$$\frac{2\sqrt{|B||C|}}{p^r}t^2 + \sqrt{2rp^{2r-1}}t - |A|\sqrt{|B||C|} \geq 0,$$

dẫn đến

$$\begin{aligned}\sqrt{|S||T|} &\geq \frac{-\sqrt{2rp^{2r-1}}+\sqrt{2rp^{2r-1}+8|A||B||C|/p^r}}{4\sqrt{|B||C|}/p^r}\\ &= \frac{2|A|\sqrt{|B||C|}}{\sqrt{2rp^{2r-1}}+\sqrt{2rp^{2r-1}+8|A||B||C|/p^r}}\\ &\gtrsim \min\left\{\sqrt{p^r|A|}, \sqrt{\frac{|A|^2|B||C|}{2rp^{2r-1}}}\right\}\\ &= \min\left\{\sqrt{p^r|A|}, \sqrt{\frac{|A|^2|D||C|}{2rp^{2r-1}}}\right\}.\end{aligned}$$

Thay C và D bằng A, suy ra điều phải chứng minh. □

3.5.3. Hàm nở $g = x + y^2$

Hàm nở $g = x + y^2$ trên trường hữu hạn

Chứng minh. Đặt N là số nghiệm của phương trình

$$(s-d)^2 + c = t,\ (s,\ d,\ c,\ t) \in S \times D \times C \times T,$$

với

$$S = A + B^2,\ D = B^2,\ T = A^2 + C.$$

Dễ thấy $N \geq |A||B||C|/2$. Ngoài ra, N là số cạnh giữa hai tập đỉnh $(-C) \times (-B)$ và $T \times S$ của đồ thị tổng - bình phương $\mathcal{FS}_q$. Từ Bổ đề 1.3.1 và Định lí 2.1.1, ta có:

$$\left|N - \frac{|S||B^2||C||T|}{p^r}\right| \leq \sqrt{2p^{2r-1}|S||B^2||C||T|}.$$

Biến đổi tương tự phần trước, ta được:

$$\sqrt{|S||T|} \gtrsim \min\left\{\sqrt{q|A|}, \sqrt{\frac{|A|^2|B||C|}{q}}\right\}.$$

Thay B và C bằng A, suy ra điều phải chứng minh. □

Hàm nở $g = x + y^2$ trên vành hữu hạn

Chứng minh. Đặt N là số nghiệm của phương trình

$$(s-d)^2 + c = t,\ (s,\ d,\ c,\ t) \in S \times D \times C \times T,$$

với

$$S = A + B^2,\ D = B^2,\ T = A^2 + C.$$

Dễ thấy $N \geq |A||B||C|/2$. Ngoài ra, N là số cạnh giữa hai tập đỉnh $(-C) \times (-B)$ và $T \times S$ của đồ thị tổng - bình phương $\mathcal{SR}_q$. Từ Bổ đề 1.3.1 và Định lí 2.1.2, ta có:

$$\left| N - \frac{|S||B^2||C||T|}{q} \right| \leq \sqrt{q|S||B^2||C||T|}.$$

Biến đổi tương tự phần trước, ta được:

$$\sqrt{|S||T|} \gtrsim \min\left\{ \sqrt{p^r|A|}, \sqrt{\frac{|A|^2|D||C|}{2rp^{2r-1}}} \right\}.$$

Thay B và C bằng A, suy ra điều phải chứng minh. □

Chương 4

Tập khoảng cách trên đa tạp chính quy

4.1. Giới thiệu tổng quan về bài toán tập khoảng cách trên đa tạp chính quy

Trong chương này của Luận án, chúng tôi nghiên cứu bài toán khoảng cách tổng quát trong trường hợp $\mathcal{E}$ là một tập con của một đa tạp chính quy. Chúng ta bắt đầu bằng định nghĩa sau:

Định nghĩa 4.1.1. *([18, Định nghĩa 2.1]) Với $\mathcal{E} \subset \mathbb{F}_q^d$, kí hiệu $\mathbf{1}_\mathcal{E}$ là hàm đặc trưng của tập $\mathcal{E}$. Cho $F(\mathbf{x}) \in \mathbb{F}_q[x_1, \ldots, x_d]$ là một đa thức. Đa tạp $\mathcal{V} = \{\mathbf{x} \in \mathbb{F}_q^d \colon F(\mathbf{x}) = 0\}$ được gọi là đa tạp chính quy nếu $|\mathcal{V}| = \Theta(q^{d-1})$ và $\widehat{\mathbf{1}_\mathcal{V}(\mathbf{m})} \lesssim q^{-(d+1)/2}$ với mọi $\mathbf{m} \in \mathbb{F}_q^d \setminus \mathbf{0}$, trong đó*

$$\widehat{\mathbf{1}_\mathcal{V}(\mathbf{m})} = \frac{1}{q^d} \sum_{\mathbf{x} \in \mathbb{F}_q^d} \chi(-\mathbf{m} \cdot \mathbf{x}) \mathbf{1}_\mathcal{V}(\mathbf{x}).$$

Chúng ta có một số ví dụ về đa tạp chính quy:

1. Hình cầu với bán kính khác 0:

$$S_j = \left\{ \mathbf{x} \in \mathbb{F}_q^d \colon \|\mathbf{x}\| = j \right\}, \ j \in \mathbb{F}_q^*.$$

2. Paraboloid:

$$P = \left\{ \mathbf{x} \in \mathbb{F}_q^d \colon x_1^2 + \cdots + x_{d-1}^2 = x_d \right\}.$$

3. Hình cầu được định nghĩa "khoảng cách Minkowski" với bán kính khác 0:

$$M_j = \left\{ \mathbf{x} \in \mathbb{F}_q^d \colon x_1 \cdot x_2 \cdots x_d = j \right\}, \ j \in \mathbb{F}_q^*.$$

Năm 2007, Iosevich và Rudnev [34] sử dụng biến đổi Fourier đã thu được kết quả đầu tiên của tập khoảng cách trên hình cầu đơn vị trên trường hữu hạn $\mathbb{F}_q^d$. Cụ thể, họ thu được kết quả sau:

Định lí 4.1.1 ([34]). *Cho $\mathcal{E} \subset S_1$ trong $\mathbb{F}_q^d$ với $d \geq 3$.*

1. *Nếu $|\mathcal{E}| \geq Cq^{\frac{d}{2}}$ với hằng số C đủ lớn, khi đó tồn tại $c > 0$ sao cho $|\Delta(\mathcal{E})| \geq cq$.*
2. *Nếu d là một số chẵn và $|\mathcal{E}| \geq Cq^{\frac{d}{2}}$ với hằng số C đủ lớn, khi đó $\Delta(\mathcal{E}) = \mathbb{F}_q$.*
3. *Nếu d là một số chẵn, tồn tại $c > 0$ và $\mathcal{E} \subset S_1$ sao cho $|\mathcal{E}| \geq cq^{\frac{d}{2}}$ và $\Delta(\mathcal{E}) \neq \mathbb{F}_q$.*
4. *Nếu d là một số lẻ và $|\mathcal{E}| \geq Cq^{\frac{d+1}{2}}$ với hằng số $C > 0$ đủ lớn, khi đó $\Delta(\mathcal{E}) = \mathbb{F}_q$.*
5. *Nếu d là số lẻ, tồn tại $c > 0$ và $\mathcal{E} \subset S_1$ sao cho $|\mathcal{E}| \geq cq^{\frac{d+1}{2}}$ và $\Delta(\mathcal{E}) \neq \mathbb{F}_q$.*

Cho $\mathcal{V} \subset \mathbb{F}_q^d$ và $\mathcal{E} \in \mathcal{V}$. Chúng ta nhắc lại định nghĩa tập $\Delta_{k,D}(\mathcal{E})$

$$\Delta_{k,D}(\mathcal{E}) = \left\{ D(\mathbf{x}^1 + \cdots + \mathbf{x}^k) \colon \mathbf{x}^i \in \mathcal{E},\, 1 \leq i \leq k \right\}. \tag{4.1.1}$$

Covert, Koh và Pi [18] đã đưa ra kết quả tổng quát cho Định lí 4.1.1. Cụ thể, các kết quả đó trả lời cho câu hỏi sau: Tập con $\mathcal{E}$ của đa tạp chính quy $\mathcal{V}$ phải có độ lớn như thế nào để $\Delta_{k,D}(\mathcal{E}) = \mathbb{F}_q$ hoặc $|\Delta_{k,D}(\mathcal{E})| \gtrsim q$?

Ý tưởng chính của chứng minh Định lí 4.1.1 là chúng ta suy ra kết quả bài toán đánh giá tập tích thông qua bài toán khoảng cách, với hai điểm $\mathbf{x}$ và $\mathbf{y}$ thuộc S_1 thì ta có khoảng cách giữa hai điểm đó là $2 - 2\mathbf{x} \cdot \mathbf{y}$ (trong đó $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_d y_d$). Do đó

$$|\Delta(\mathcal{E})| = |\Pi_2(\mathcal{E})| = |\{\mathbf{x} \cdot \mathbf{y} \colon \mathbf{x},\, \mathbf{y} \in \mathcal{E}\}|. \tag{4.1.2}$$

Trong trường hợp $k \geq 3$ và $\mathcal{E} \subset S_1$, dễ thấy

$$|\Delta_{k,D}(\mathcal{E})| = |\Pi_k(\mathcal{E})| = \left| \left\{ \sum_{i=1}^{k} \sum_{j=1}^{k} a_{ij} \cdot b_{ij} \cdot \mathbf{x}^i \cdot \mathbf{x}^j \colon \mathbf{x}^l \in \mathcal{E},\, 1 \leq l \leq k \right\} \right|,$$

với $a_{ij} = 1$ nếu $i < j$ và 0 trong trường hợp ngược lại, $b_{ij} = 1$ nếu $i = 1$ và -1 trong trường hợp ngược lại.

Tuy nhiên, rất khó có một đánh giá tốt cho tập $|\Pi_k(\mathcal{E})|$ khi $k \geq 3$ và nếu chúng ta thay hình cầu đơn vị S_1 bằng một đa tạp chính quy tổng quát $\mathcal{V}$,

nó sẽ không đảm bảo dấu bằng ở phương trình (4.1.2) có thể xảy ra. Do đó, chúng ta không thể áp dụng chứng minh của Định lí 4.1.1 để đánh giá lực lượng cho tập $\Delta_{k,D}(\mathcal{E})$.

Covert, Koh và Pi [18] sử dụng biến đổi Fourier đã cải thiện được điều kiện của $\mathcal{E}$ trong Định lí 4.1.1 để $\Delta_{k,D}(\mathcal{E}) = \mathbb{F}_q$ với $k \geq 3$. Cụ thể, họ đã chứng minh được kết quả sau:

Định lí 4.1.2. *([18, Định lí 2.2]) Giả sử $\mathcal{V} \subset \mathbb{F}_q^d$ là một đa tạp chính quy và $k \geq 3$ là một số nguyên. Với $\mathcal{E} \subset \mathcal{V}$ thỏa mãn $|\mathcal{E}| \gtrsim q^{\frac{d-1}{2}+\frac{1}{k-1}}$, ta có:*

$$\Delta_{k,D}(\mathcal{E}) \supseteq \mathbb{F}_q^* \text{ với } d \text{ chẵn}, d \geq 2$$

và

$$\Delta_{k,D}(\mathcal{E}) = \mathbb{F}_q \text{ với } d \text{ lẻ}, d \geq 3.$$

Từ Định lí 4.1.1, ta có $\Delta_{2,D}(\mathcal{E}) = \mathbb{F}_q$, số mũ của tập $\mathcal{E} \subset S_1$ lớn hơn hoặc bằng $d/2$ với d chẵn, $d \geq 4$ và $(d+1)/2$ với d lẻ, $d \geq 3$. Từ Định lí 4.1.2 suy ra số mũ $d/2$ có thể giảm xuống thành $\frac{d-1}{2} + \frac{1}{k-1}$ với $k \geq 3$ và đa tạp chính quy $\mathcal{V} \subset \mathbb{F}_q^d$ tùy ý.

Sử dụng phương pháp phổ của đồ thị, chúng tôi thu được các kết quả tổng quát sau:

Định lí 4.1.3. *([33, Định lí 1.4]) Cho Q là một dạng toàn phương không suy biến trên $\mathbb{F}_q^d$. Giả sử $\mathcal{V} \subset \mathbb{F}_q^d$ là một đa tạp chính quy và $k \geq 3$ là một số nguyên. Với $\mathcal{E} \subset \mathcal{V}$ thỏa mãn $q^{\frac{d-1}{2}+\frac{1}{k-1}} = o(|\mathcal{E}|)$, khi đó với $t \in \mathbb{F}_q^*$ bất kì, ta có:*

$$\left|\left\{(\mathbf{x}_1, \ldots, \mathbf{x}_k) \in \mathcal{E}^k \colon Q(\mathbf{x}_1 + \cdots + \mathbf{x}_k) = t\right\}\right| = (1 - o(1))\frac{|\mathcal{E}|^k}{q}.$$

Hệ quả 4.1.4. *([33, Hệ quả 1.5]) Cho Q là một dạng toàn phương không suy biến trên $\mathbb{F}_q^d$. Giả sử $\mathcal{V} \subset \mathbb{F}_q^d$ là một đa tạp chính quy và $k \geq 3$ là một số nguyên. Với $\mathcal{E} \subset \mathcal{V}$ thỏa mãn $q^{\frac{d-1}{2}+\frac{1}{k-1}} = o(|\mathcal{E}|)$, ta có:*

$$\Delta_{k,Q}(\mathcal{E}) \supseteq \mathbb{F}_q^*.$$

Đặt $P(\boldsymbol{x}) = \sum_{j=1}^{d} a_j x_j^s$, trong đó $s \geq 2$ và $a_j \neq 0$ với mọi $j = 1, \ldots, d$ là một đa thức trong $\mathbb{F}_q[x_1, \ldots, x_d]$. Chúng tôi cũng chứng minh được kết quả tổng

quát cho tập $\Delta_{k,D}(\mathcal{E})$ khi ta thay hàm D bằng đa thức $P(\boldsymbol{x})$. Cụ thể, ta có kết quả sau:

Định lí 4.1.5. *([33, Định lí 1.6]) Giả sử $\mathcal{V} \subset \mathbb{F}_q^d$ là một đa tạp chính quy và $k \geq 3$ là một số nguyên. Với $\mathcal{E} \subset \mathcal{V}$ và $X \subset \mathbb{F}_q$ thỏa mãn $|X||\mathcal{E}|^{2k-2} \gtrsim q^{(d-1)(k-1)+2}$, ta có:*

$$|X + \Delta_{k,P}(\mathcal{E})| \gtrsim q.$$

Hệ quả 4.1.6. *([33, Hệ quả 1.7]) Giả sử $\mathcal{V} \subset \mathbb{F}_q^d$ là một đa tạp chính quy và $k \geq 3$ là một số nguyên. Với $\mathcal{E} \subset V$ thỏa mãn $|\mathcal{E}| \gtrsim q^{\frac{d-1}{2}+\frac{1}{k-1}}$, ta có:*

$$|\Delta_{k,P}(\mathcal{E})| \gtrsim q.$$

4.2. Đánh giá cho dạng toàn phương không suy biến

Cho H là một nhóm cộng Abel hữu hạn và $S \subset H$. Chúng ta định nghĩa đồ thị Cayley C_S như sau: Tập đỉnh của C_S là H. Giữa hai đỉnh x, y có một cạnh (x, y) khi và chỉ khi $y - x \in S$. Dễ thấy, mỗi đỉnh của C_S có bậc đi ra là $|S|$. Với $\alpha \in H$, giả sử χ_α là hàm đặc trưng của H. Với $\alpha \in H$ bất kì, ta có $\sum_{s\in S} \chi_\alpha(s)$ là một giá trị riêng của C_S với vectơ riêng tương ứng là $(\chi_\alpha(x))_{x\in H}$.

Chúng ta định nghĩa đồ thị Cayley $C_\mathcal{V}$ như sau: Tập đỉnh $H = \mathbb{F}_q^d$ và $S = \mathcal{V}$ với $\mathcal{V}$ là một đa tạp chính quy. Tập cạnh của đồ thị $C_\mathcal{V}$ là

$$E(C_\mathcal{V}) = \{(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{F}_q^d \times \mathbb{F}_q^d \colon \mathbf{y} - \mathbf{x} \in \mathcal{V}\}.$$

Với hai đỉnh $\mathbf{x}$ và $\mathbf{y}$ bất kì của đồ thị H, ta có:

$$|N^+(\mathbf{x}, \mathbf{y})| = |N^-(\mathbf{x}, \mathbf{y})| = |(\mathbf{x} + \mathcal{V}) \cap (\mathbf{y} + \mathcal{V})|.$$

Khi đó $C_\mathcal{V}$ là đồ thị chuẩn tắc. Chúng ta sẽ nghiên cứu tính chất (n, d, λ) của đồ thị có hướng $C_\mathcal{V}$ trong định lí sau:

Định lí 4.2.1. *Đồ thị Cayley $C_\mathcal{V}$ là một $(q^d, |\mathcal{V}|, cq^{(d-1)/2})$ - đồ thị, với hằng số $c > 0$ nào đó.*

Chứng minh. Dễ thấy $C_{\mathcal{V}}$ có q^d đỉnh. Với mỗi đỉnh bất kì của $C_{\mathcal{V}}$ thì bậc đi vào và bậc đi ra đều bằng $|\mathcal{V}|$. Bây giờ chúng ta sẽ đánh giá giá trị riêng của đồ thị $C_{\mathcal{V}}$. Do $C_{\mathcal{V}}$ là đồ thị Cayley nên ma trận kề của $C_{\mathcal{V}}$ có vectơ riêng là

$$\chi_m(\mathbf{x}) = \chi(\mathbf{x} \cdot \mathbf{m}), \tag{4.2.1}$$

với $\mathbf{x}, \mathbf{m} \in \mathbb{F}_q^d$, ứng với giá trị riêng

$$\begin{aligned} \lambda_{\mathbf{m}} &= \sum_{\mathbf{x} \in \mathcal{V}} \chi_{\mathbf{m}}(\mathbf{x}) \\ &= \sum_{\mathbf{x} \in \mathcal{V}} \chi(\mathbf{x} \cdot \mathbf{m}) \\ &= q^d \widehat{\mathbf{1}_{\mathcal{V}}(-\mathbf{m})} \\ &\lesssim q^{(d-1)/2}, \end{aligned}$$

khi $\mathbf{m} \neq \mathbf{0}$. Nếu $\mathbf{m} = \mathbf{0}$ thì $\lambda_{\mathbf{0}} = |\mathcal{V}|$ là giá trị riêng lớn nhất của $C_{\mathcal{V}}$. Như vậy, $C_{\mathcal{V}}$ là một đồ thị $(q^d, |\mathcal{V}|, cq^{(d-1)/2})$ với c là hằng số. □

Để chứng minh Định lí 4.1.3, chúng ta cần lưu ý sau:

Với số tự nhiên chẵn $k = 2m \geq 2$ và $\mathcal{E} \subset \mathbb{F}_q^d$, chúng ta định nghĩa $\Lambda_k(\mathcal{E})$ như sau:

$$\Lambda_k(\mathcal{E}) = \left| \left\{ (\mathbf{x}^1, \ldots, \mathbf{x}^k) \in \mathcal{E}^k \colon \mathbf{x}^1 + \cdots + \mathbf{x}^m = \mathbf{x}^{m+1} + \cdots + \mathbf{x}^k \right\} \right|.$$

Với $\mathcal{E} \subset \mathbb{F}_q^d$, chúng ta định nghĩa

$$\nu_k(t) = \left| \left\{ (\mathbf{x}^1, \ldots, \mathbf{x}^k) \in \mathcal{E}^k \colon Q(\mathbf{x}^1 + \cdots + \mathbf{x}^k) = t \right\} \right|.$$

Chúng ta sẽ đánh giá độ lớn của $\nu_k(t)$ trong các bổ đề sau:

Bổ đề 4.2.2. *Với $\mathcal{E} \subset \mathbb{F}_q^d$ và $k \geq 2$ là số chẵn, ta có:*

$$\left| \nu_k(t) - (1 + o(1)) \frac{|\mathcal{E}|^k}{q} \right| \leq 2q^{(d-1)/2} \Lambda_k(\mathcal{E}).$$

Chứng minh. Giả sử $k = 2m$. Cho $\mathcal{A}$ và $\mathcal{B}$ là các đa tập với các phần tử thuộc $\mathbb{F}_q^d$ được định nghĩa như sau:

$$\mathcal{A} = \{\mathbf{x}_1 + \cdots + \mathbf{x}_m \colon \mathbf{x}_i \in \mathcal{E},\ 1 \leq i \leq m\},$$

$$\mathcal{B} = \{-\mathbf{x}_{m+1} - \cdots - \mathbf{x}_k \colon \mathbf{x}_i \in \mathcal{E},\ m+1 \le i \le k\}.$$

Từ đó ta có:

$$\sum_{\mathbf{a}\in\mathcal{A}} m_{\mathcal{A}}(\mathbf{a})^2 = \Lambda_k(\mathcal{E}), \quad \sum_{\mathbf{b}\in\mathcal{B}} m_{\mathcal{B}}(\mathbf{b})^2 = \Lambda_k(\mathcal{E}).$$

Mặt khác, $\nu_k(t)$ là số cạnh giữa hai tập đỉnh $\mathcal{A}$ và $\mathcal{B}$ trong đồ thị $E_q(d, Q, t)$ nên từ Bổ đề 1.3.2 và Định lí 2.5.1 ta có:

$$\left|\nu_k(t) - \frac{(1+o(1)q^{d-1})|\mathcal{A}||\mathcal{B}|}{q^d}\right| \le 2q^{(d-1)/2}\sqrt{\sum_{\mathbf{a}\in\mathcal{A}} m_{\mathcal{A}}(\mathbf{a})^2}\sqrt{\sum_{\mathbf{b}\in\mathcal{B}} m_{\mathcal{B}}(\mathbf{b})^2}.$$

Điều này tương đương với

$$\left|\nu_k(t) - (1+o(1))\frac{|\mathcal{A}||\mathcal{B}|}{q}\right| \le 2q^{(d-1)/2}\Lambda_k(\mathcal{E}).$$

Do $|\mathcal{A}||\mathcal{B}| = |\mathcal{E}|^k$, ta có điều phải chứng minh. □

Tương tự, ta có kết quả cho trường hợp k là số lẻ.

Bổ đề 4.2.3. *Với $\mathcal{E} \subset \mathbb{F}_q^d$ và $k \ge 3$ là số lẻ, ta có:*

$$\left|\nu_k(t) - (1+o(1))\frac{|\mathcal{E}|^k}{q}\right| \le 2q^{(d-1)/2}\left(\Lambda_{k-1}(\mathcal{E})\right)^{1/2}\left(\Lambda_{k+1}(\mathcal{E})\right)^{1/2}.$$

Chứng minh. Giả sử $k = 2m+1$. Cho $\mathcal{A}$ và $\mathcal{B}$ là các đa tập với các phần tử thuộc $\mathbb{F}_q^d$ được định nghĩa như sau:

$$\mathcal{A} = \{\mathbf{x}_1 + \cdots + \mathbf{x}_m \colon \mathbf{x}_i \in \mathcal{E},\ 1 \le i \le m\},$$

$$\mathcal{B} = \{-\mathbf{x}_{m+1} - \cdots - \mathbf{x}_k \colon \mathbf{x}_i \in \mathcal{E},\ m+1 \le i \le k\}.$$

Từ đó ta có:

$$\sum_{\mathbf{a}\in\mathcal{A}} m_{\mathcal{A}}(\mathbf{a})^2 = \Lambda_{k-1}(\mathcal{E}), \quad \sum_{\mathbf{b}\in\mathcal{B}} m_{\mathcal{B}}(\mathbf{b})^2 = \Lambda_{k+1}(\mathcal{E}).$$

Mặt khác, $\nu_k(t)$ là số cạnh giữa hai tập đỉnh $\mathcal{A}$ và $\mathcal{B}$ trong đồ thị $E_q(d, Q, t)$ nên từ Bổ đề 1.3.2 và Định lí 2.5.1, ta có:

$$\left|\nu_k(t) - \frac{(1+o(1)q^{d-1})|\mathcal{A}||\mathcal{B}|}{q^d}\right| \leq 2q^{(d-1)/2}\sqrt{\sum_{\mathbf{a}\in\mathcal{A}} m_{\mathcal{A}}(\mathbf{a})^2}\sqrt{\sum_{\mathbf{b}\in\mathcal{B}} m_{\mathcal{B}}(\mathbf{b})^2}.$$

Điều này tương đương với

$$\left|\nu_k(t) - (1+o(1))\frac{|\mathcal{A}||\mathcal{B}|}{q}\right| \leq 2q^{(d-1)/2}(\Lambda_{k-1}(\mathcal{E}))^{1/2}(\Lambda_{k+1}(\mathcal{E}))^{1/2}.$$

Do $|\mathcal{A}||\mathcal{B}| = |\mathcal{E}|^k$, ta có điều phải chứng minh. □

Từ Bổ đề 4.2.2 và Bổ đề 4.2.3, ta có định lí sau:

Định lí 4.2.4. *Với $\mathcal{E} \subset \mathbb{F}_q^d$, ta có:*

1. *Nếu $q^{\frac{d+1}{2}}\Lambda_k(\mathcal{E}) = o(|\mathcal{E}|^k)$ và k là số chẵn, khi đó*

$$\left|\left\{(\mathbf{x}_1, \ldots, \mathbf{x}_k) \in \mathcal{E}^k \colon Q(\mathbf{x}_1 + \cdots + \mathbf{x}_k) = t\right\}\right| = (1+o(1))\frac{|\mathcal{E}|^k}{q}.$$

2. *Nếu $q^{\frac{d+1}{2}}(\Lambda_{k-1}(\mathcal{E}))^{1/2}(\Lambda_{k+1}(\mathcal{E}))^{1/2} = o(|\mathcal{E}|^k)$ và k là số lẻ, khi đó*

$$\left|\left\{(\mathbf{x}_1, \ldots, \mathbf{x}_k) \in \mathcal{E}^k \colon Q(\mathbf{x}_1 + \cdots + \mathbf{x}_k) = t\right\}\right| = (1+o(1))\frac{|\mathcal{E}|^k}{q}.$$

Từ Định lí 4.2.4, dễ thấy để chứng minh Định lí 4.1.3, chúng ta cần đánh giá độ lớn của $\Lambda_k(\mathcal{E})$.

Bổ đề 4.2.5. *Cho một đa tạp chính quy $\mathcal{V} \subset \mathbb{F}_q^d$. Nếu $k \geq 4$ là số chẵn và $\mathcal{E} \subset \mathcal{V}$. Ta có:*

$$\Lambda_k(\mathcal{E}) \lesssim \frac{|\mathcal{E}|^{k-1}}{q} + q^{(d-1)/2}(\Lambda_{k-2}(\mathcal{E}))^{1/2}(\Lambda_k(\mathcal{E}))^{1/2}.$$

Chứng minh. Do $\mathcal{E}$ là tập con của $\mathcal{V}$ nên ta có đánh giá sau:

$$\Lambda_k(\mathcal{E}) \leq \sum_{\mathbf{x}_1,\ldots,\mathbf{x}_{k-1}\in\mathcal{E}} \mathbf{1}_{\mathcal{V}}(\mathbf{x}_1 + \cdots + \mathbf{x}_{k/2} - \mathbf{x}_{k/2+1} - \cdots - \mathbf{x}_{k-1}).$$

Đặt

$$N = \sum_{\mathbf{x}_1,\ldots,\mathbf{x}_{k-1}\in\mathcal{E}} \mathbf{1}_{\mathcal{V}}(\mathbf{x}_1 + \cdots + \mathbf{x}_{k/2} - \mathbf{x}_{k/2+1} - \cdots - \mathbf{x}_{k-1}).$$

Chúng ta định nghĩa hai đa tập $\mathcal{A}$ và $\mathcal{B}$ như sau:

$$\mathcal{A} = \{\mathbf{x}_1 + \cdots + \mathbf{x}_{k/2} \colon \mathbf{x}_i \in \mathcal{E},\ 1 \le i \le k/2\}$$

và

$$\mathcal{B} = \{-\mathbf{x}_{k/2+1} - \cdots - \mathbf{x}_{k-1} \colon \mathbf{x}_i \in \mathcal{E},\ k/2+1 \le i \le k-1\}.$$

Dễ thấy

$$\sum_{\mathbf{a}\in\mathcal{A}} m_{\mathcal{A}}(\mathbf{a})^2 = \Lambda_k(\mathcal{E}), \quad \sum_{\mathbf{b}\in\mathcal{B}} m_{\mathcal{B}}(\mathbf{b})^2 = \Lambda_{k-2}(\mathcal{E}).$$

Mặt khác, $\sum_{\mathbf{x}_1,\ldots,\mathbf{x}_{k-1}\in\mathcal{E}} \mathbf{1}_{\mathcal{V}}(\mathbf{x}_1 + \cdots + \mathbf{x}_{k/2} - \mathbf{x}_{k/2+1} - \cdots - \mathbf{x}_{k-1})$ bằng số cạnh giữa hai tập đỉnh $\mathcal{A}$ và $\mathcal{B}$ của đồ thị Cayley $C_{\mathcal{V}}$ nên từ Bổ đề 1.3.4 và Định lí 4.2.1 ta có:

$$\left| N - \frac{|\mathcal{V}||\mathcal{E}|^{k-1}}{q^d} \right| \lesssim q^{(d-1)/2} (\Lambda_{k-2}(\mathcal{E}))^{1/2} (\Lambda_k(\mathcal{E}))^{1/2}.$$

Điều này tương đương với

$$N \lesssim \frac{|\mathcal{V}||\mathcal{E}|^{k-1}}{q^d} + q^{(d-1)/2} (\Lambda_{k-2}(\mathcal{E}))^{1/2} (\Lambda_k(\mathcal{E}))^{1/2}.$$

Theo định nghĩa đa tạp chính quy ta có $|\mathcal{V}| = \Theta(q^{d-1})$. Từ đó ta có:

$$N \lesssim \frac{|\mathcal{E}|^{k-1}}{q} + q^{(d-1)/2} (\Lambda_{k-2}(\mathcal{E}))^{1/2} (\Lambda_k(\mathcal{E}))^{1/2}.$$

Từ đó suy ra điều cần chứng minh. □

Cho $\mathcal{E} \subset \mathcal{V}$ và $k \ge 4$ là số chẵn, từ Bổ đề 4.2.5 ta có:

$$\Lambda_k(\mathcal{E}) \lesssim \frac{|\mathcal{E}|^{k-1}}{q} + q^{(d-1)/2} (\Lambda_{k-2}(\mathcal{E}))^{1/2} (\Lambda_k(\mathcal{E}))^{1/2}.$$

Từ đó suy ra

$$\Lambda_k(\mathcal{E}) \lesssim q^{d-1} \Lambda_{k-2}(\mathcal{E}) + \frac{|\mathcal{E}|^{k-1}}{q}.$$

Sử dụng phương pháp quy nạp toán học, chúng ta thu được đánh giá cho tập $\Lambda_k(\mathcal{E})$ như sau:

$$\Lambda_k(\mathcal{E}) \lesssim q^{\frac{(d-1)(k-2)}{2}} \Lambda_2(\mathcal{E}) + \frac{|\mathcal{E}|^{k-1}}{q} \sum_{j=0}^{(k-4)/2} \left(\frac{q^{d-1}}{|\mathcal{E}|^2} \right)^j, \tag{4.2.2}$$

trong đó $\mathcal{E} \subset \mathcal{V}$ và $k \ge 4$ là một số chẵn.

Giả sử $|\mathcal{E}| > q^{(d-1)/2}$, từ Bất đẳng thức (4.2.2) ta có định lí sau:

Định lí 4.2.6. *Với $\mathcal{E}$ là một tập con của đa tạp chính quy $\mathcal{V}$ trong $\mathbb{F}_q^d$ thỏa mãn $|\mathcal{E}| > q^{(d-1)/2}$. Khi đó*

1. *Nếu $k \geq 2$ chẵn, ta có:*

$$\Lambda_k(\mathcal{E}) \lesssim q^{\frac{(d-1)(k-2)}{2}}|\mathcal{E}| + \frac{|\mathcal{E}|^{k-1}}{q}.$$

2. *Nếu $k \geq 3$ lẻ, ta có:*

$$\Lambda_{k-1}(\mathcal{E})\Lambda_{k+1}(\mathcal{E}) \lesssim q^{(d-1)(k-2)}|\mathcal{E}|^2 + q^{\frac{(d-1)(k-3)-2}{2}}|\mathcal{E}|^{k+1} + \frac{|\mathcal{E}|^{2k-2}}{q^2}.$$

Để ý rằng nếu kết hợp Bất đẳng thức (4.2.2) với điều kiện $\Lambda_2(\mathcal{E}) = |\mathcal{E}|$ và $\frac{q^{d-1}}{|\mathcal{E}|^2} < 1$, ta sẽ suy ra được bất đẳng thức đầu tiên trong Định lí 4.2.6. Bất đẳng thức thứ hai là kết quả được suy ra từ bất đẳng thức đầu. Tiếp theo chúng ta sẽ chứng minh Định lí 4.1.3.

Chứng minh. Chúng ta xét hai trường hợp sau:
Trường hợp 1: Nếu $k \geq 2$ chẵn và $q^{\frac{d-1}{2}+\frac{1}{k-1}} = o(|\mathcal{E}|)$. Khi đó, từ Định lí 4.2.6 suy ra

$$q^{\frac{d+1}{2}}\Lambda_k(\mathcal{E}) = o(|\mathcal{E}|^k).$$

Trường hợp 2: Nếu $k \geq 3$ lẻ và $q^{\frac{d-1}{2}+\frac{1}{k-1}} = o(|\mathcal{E}|)$. Khi đó, từ Định lí 4.2.6 suy ra

$$q^{\frac{d+1}{2}}(\Lambda_{k-1}(\mathcal{E}))^{1/2}(\Lambda_{k+1}(\mathcal{E}))^{1/2} = o(|\mathcal{E}|^k).$$

Kết hợp với Định lí 4.2.4, ta có điều phải chứng minh. □

4.3. Đánh giá cho đa thức chéo $P(\mathbf{x}) = \sum_{j=1}^{d} a_j x_j^s$

Để chứng minh Định lí 4.1.5, trước hết chúng ta cần xây dựng đồ thị Cayley như sau: Cho $P(\mathbf{x}) = \sum_{j=1}^{d} a_j x_j^s \in \mathbb{F}_q[x_1, \ldots, x_d]$ trong đó $s \geq 2$ và $a_j \neq 0$ với mọi $j = 1, \ldots, d$. Đặt

$$P'(x_1, \ldots, x_{2d}) = P(x_1, \ldots, x_d) - P(x_{d+1}, \ldots, x_{2d}) \in \mathbb{F}_q[x_1, \ldots, x_{2d}].$$

Chúng ta định nghĩa đồ thị Cayley $C_{P'}(\mathbb{F}_q^{2d+1})$ như sau: Tập đỉnh $H = \mathbb{F}_q \times \mathbb{F}_q^{2d}$ và $S = \{(x_0, \mathbf{x}) \in \mathbb{F}_q \times \mathbb{F}_q^{2d} \mid x_0 + P'(\mathbf{x}) = 0\}$. Tập cạnh là

$$E(C_{P'}(\mathbb{F}_q^{2d+1})) = \left\{((x_0, \mathbf{x}), (y_0, \mathbf{y})) \in H \times H \colon y_0 - x_0 + P'(\mathbf{y} - \mathbf{x}) = 0\right\}.$$

Đồ thị $C_{P'}(\mathbb{F}_q^{2d+1})$ đã được nghiên cứu trong [57]. Cụ thể, ta có bổ đề sau:

Bổ đề 4.3.1 ([57]). *Cho d là một số tự nhiên và $d \geq 1$, khi đó $C_{P'}(\mathbb{F}_q^{2d+1})$ là một*

$$(q^{2d+1}, q^{2d}, q^d) - \textit{đồ thị có hướng}.$$

Với $\mathcal{E} \subset \mathbb{F}_q^d$, $X \subset \mathbb{F}_q$ và $t \in \mathbb{F}_q^*$, chúng ta định nghĩa $\nu_{P,k}(t)$ như sau:

$$\nu_{P,k}(t) = \left|\{(a, \mathbf{x}_1, \ldots, \mathbf{x}_k) \in X \times \mathcal{E}^k \colon a + P(\mathbf{x}_1 + \cdots + \mathbf{x}_k) = t\}\right|.$$

Để chứng minh Định lí 4.1.5, chúng ta cần các bổ đề sau:

Bổ đề 4.3.2. *Cho $\mathcal{E} \subset \mathbb{F}_q^d$ với k là một số chẵn và $k \geq 2$. Ta có:*

$$\sum_{t \in \mathbb{F}_q} \nu_{P,k}(t)^2 \leq \frac{|\mathcal{E}|^{2k}|X|^2}{q} + q^d |X| \Lambda_k(\mathcal{E})^2.$$

Chứng minh. Cho $\mathcal{A}$ và $\mathcal{B}$ là các đa tập được định nghĩa như sau:

$$\mathcal{A} = \{(a, -\mathbf{x}_1 - \cdots - \mathbf{x}_{k/2}, -\mathbf{y}_1 - \cdots - \mathbf{y}_{k/2}) \colon a \in X, \mathbf{x}_i, \mathbf{y}_i \in \mathcal{E}\}$$

và

$$\mathcal{B} = \{(b, \mathbf{x}_{k/2+1} + \cdots + \mathbf{x}_k, \mathbf{y}_{k/2+1} + \cdots + \mathbf{y}_{k/2+1}) \colon b \in X, \mathbf{x}_i, \mathbf{y}_i \in \mathcal{E}\}.$$

Ta có:

$$\sum_{\mathbf{x} \in \mathcal{A}} m_{\mathcal{A}}(\mathbf{x})^2 = |X| \Lambda_k(\mathcal{E})^2, \sum_{\mathbf{x} \in \mathcal{B}} m_{\mathcal{B}}(\mathbf{x})^2 = |X| \Lambda_k(\mathcal{E})^2, |\mathcal{A}| = |\mathcal{B}| = |X||\mathcal{E}|^k.$$

Mặt khác $\sum_{t \in \mathbb{F}_q} \nu_{P,k}^2$ là số cạnh từ tập đỉnh $\mathcal{A}$ vào tập đỉnh $\mathcal{B}$ trong đồ thị $C_{P'}(\mathbb{F}_q^{2d+1})$. Do đó, từ Bổ đề 1.3.4 và Định lí 4.3.1 suy ra

$$\sum_{t \in \mathbb{F}_q} \nu_{P,k}(t)^2 \leq \frac{|\mathcal{E}|^{2k}|X|^2}{q} + q^d |X| \Lambda_k(\mathcal{E})^2,$$

từ đó ta suy ra điều phải chứng minh. □

Sử dụng kĩ thuật tương tự, ta cũng có kết quả tương tự cho trường hợp k là một số lẻ và $k \geq 3$.

Bổ đề 4.3.3. *Cho $\mathcal{E} \subset \mathbb{F}_q^d$ với k là một số lẻ và $k \geq 3$. Ta có:*

$$\sum_{t \in \mathbb{F}_q} \nu_{P,k}(t)^2 \leq \frac{|\mathcal{E}|^{2k}|X|^2}{q} + q^d |X| \Lambda_{k-1}(\mathcal{E}) \Lambda_{k+1}(\mathcal{E}).$$

Bây giờ chúng ta chứng minh Định lí 4.1.5.

Chứng minh Định lí 4.1.5. Từ chứng minh của Định lí 2.6 trong [57], ta có:

$$|X + \Delta_{k,P}(\mathcal{E})| \gtrsim \frac{|X|^2 |\mathcal{E}|^{2k}}{\sum_{t \in \mathbb{F}_q} \nu_{P,k}(t)^2}.$$

Do đó, từ Bổ đề 4.3.2 và Bổ đề 4.3.3, chúng ta xét hai trường hợp sau

1. Với k chẵn và $k \geq 2$. Ta có:

$$|X + \Delta_{k,P}(\mathcal{E})| \gtrsim \min \left\{ \frac{|X||\mathcal{E}|^{2k}}{q^d \Lambda_k(\mathcal{E})^2}, q \right\}.$$

2. Với k lẻ và $k \geq 3$. Ta có:

$$|X + \Delta_{k,P}(\mathcal{E})| \gtrsim \min \left\{ \frac{|X||\mathcal{E}|^{2k}}{q^d \Lambda_k(\mathcal{E}) \Lambda_{k-1}(\mathcal{E})}, q \right\}.$$

Kết hợp với Định lí 4.2.6, chúng ta suy ra điều phải chứng minh. □

Kết luận

Trong Luận án này, chúng tôi đã sử dụng phương pháp phổ của đồ thị để thu được một số kết quả mới trong lý thuyết tổ hợp cộng tính. Cụ thể, chúng tôi đã thu được các kết quả sau:

- Trong Chương 3, sử dụng phương pháp phổ của đồ thị để nghiên cứu và cải thiện một số kết quả về tập khoảng cách, tập tích, tập thể tích khối, tập tổng - tỉ số, hàm nở hai biến trên trường và vành hữu hạn.
  - Luận án đã đưa ra chứng minh khác ngắn gọn hơn chứng minh của Hart và Iosevich cho tập khoảng cách và tập tích trên trường hữu hạn, tìm điều kiện để tập khoảng cách và tập tích trên trường hữu hạn có bậc lớn nhất có thể.
  - Đồng thời, chúng tôi cải thiện kết quả của tập thể tích khối trên trường hữu hạn, tìm điều kiện để tập thể tích khối có bậc lớn nhất có thể và mở rộng kết quả của tập thể tích khối trên vành hữu hạn.
  - Bên cạnh đó, chúng tôi đưa ra kết quả tổng quát cho tập tổng - tỉ số trên trường và vành hữu hạn.
  - Ngoài ra, chúng tôi xây dựng các hàm nở hai biến $f = x(y+1)$ và $g = x + y^2$ trên trường và vành hữu hạn.
- Trong Chương 4, sử dụng phương pháp phổ của đồ thị mở rộng để nghiên cứu và đưa ra kết quả tổng quát cho tập khoảng cách trên đa tạp chính quy khi thay hàm khoảng cách bằng dạng toàn phương không suy biến và đa thức chéo.

Các hướng nghiên cứu tiếp theo:

- *Cải thiện các kết quả đã đạt được:* Tuy khó có thể cải thiện được các kết quả đã đạt được trong trường hợp tổng quát, nhưng người ta có thể cải thiện trong các trường hợp đặc biệt về số chiều của không gian hoặc xét các tập trên các mặt đặc biệt như parabol, hyperbol, đường tròn, mặt cầu... Điển hình như: Năm 2007, Iosevich và Rudnev [34] sử dụng biến đổi Fourier đã cải thiện được kết quả của tập khoảng cách trên hình cầu đơn vị. Cụ thể, họ thu được kết quả sau: Cho $\mathcal{E} \subset S_1$ trong $\mathbb{F}_q^d$ với $d \geq 3$.

  1. Nếu $|\mathcal{E}| \geq Cq^{\frac{d}{2}}$ với hằng số C đủ lớn, khi đó tồn tại $c > 0$ sao cho $|\Delta(\mathcal{E})| \geq cq$.
  2. Nếu d là một số chẵn và $|\mathcal{E}| \geq Cq^{\frac{d}{2}}$ với hằng số C đủ lớn, khi đó $\Delta(\mathcal{E}) = \mathbb{F}_q$.
  3. Nếu d là một số chẵn, tồn tại $c > 0$ và $\mathcal{E} \subset S_1$ sao cho $|\mathcal{E}| \geq cq^{\frac{d}{2}}$ và $\Delta(\mathcal{E}) \neq \mathbb{F}_q$.
  4. Nếu d là một số lẻ và $|\mathcal{E}| \geq Cq^{\frac{d+1}{2}}$ với hằng số $C > 0$ đủ lớn, khi đó $\Delta(\mathcal{E}) = \mathbb{F}_q$.
  5. Nếu d là số lẻ, tồn tại $c > 0$ và $\mathcal{E} \subset S_1$ sao cho $|\mathcal{E}| \geq cq^{\frac{d+1}{2}}$ và $\Delta(\mathcal{E}) \neq \mathbb{F}_q$.

  Trong Chương 4, chúng tôi cũng đã nghiên cứu bài toán khoảng cách trên đa tạp chính quy. Tuy nhiên, hướng nghiên cứu khi xét các tập trên các mặt đặc biệt đến nay vẫn còn khá mới và có nhiều hướng mở. Trong thời gian tới, chúng tôi hy vọng sẽ có thêm nhiều kết quả tốt khi tiếp tục theo đuổi hướng nghiên cứu này.

- *Nghiên cứu các bài toán tổ hợp cộng tính trên các tập bé:* Phương pháp phổ của đồ thị mặc dù cách sử dụng khá đơn giản và nghiên cứu được nhiều bài toán tổ hợp cộng tính. Tuy nhiên, điểm yếu của phương pháp là chỉ nghiên cứu được các kết quả cho các tập lớn. Cụ thể, các kết quả khi sử dụng phương pháp phổ của đồ thị chỉ có ý nghĩa khi tập $A \subset \mathbb{F}_q$ (hoặc $\mathbb{Z}_q$) thỏa mãn điều kiện $|A| \gtrsim q^{1/2}$. Gần đây, có một số tác giả sử

dụng liên thuộc điểm - đường thẳng và bất đẳng thức tam giác Ruzsa để nghiên cứu một số bài toán tổ hợp cộng tính trên các tập nhỏ. Điển hình như: Roche-Newton, Rudnev và Shkredov [45] sử dụng [46] chứng minh với A, B, $C \in \mathbb{F}$ thỏa mãn $|A| = |B| = |C| = N \ll p^{2/3}$ thì

$$|AB + C| \gg N^{3/2}.$$

Trong thời gian tới, chúng tôi sẽ tiến hành nghiên cứu một số bài toán trên các tập bé với hy vọng sẽ thu được nhiều kết quả có ý nghĩa.

- *Sử dụng phương pháp khác:* Ngoài phương pháp đồ thị thì phương pháp sử dụng giải tích Fourier cũng được sử dụng rộng rãi. Chúng tôi cũng đã có những nghiên cứu ban đầu khi sử dụng phương pháp này. Cụ thể, khi sử dụng giải tích Fourier, chúng tôi cũng chứng minh được $f = x + y^{-1}$ là hàm nở hai biến trên trường và vành hữu hạn với x, $y \in A$ và $|A| \gg q^{1/2}$. Trong thời gian tới, chúng tôi sẽ tiếp tục tìm hiểu sâu hơn về giải tích Fourier và sử dụng phương pháp này để nghiên cứu một số bài toán tổ hợp cộng tính.

Công trình liên quan đến Luận án

- D. D. Hieu and P. V. Thang, Distinct distances on regular varieties over finite fields, *Journal of Number Theory*, **173** (2017), 602 - 613.
- D. D. Hieu and L. A. Vinh, On distance sets and product sets in vector spaces over finite rings, *Michigan Mathematical Journal*, **62** (2013), 779 - 792.
- D. D. Hieu and L. A. Vinh, On volume set of boxes in finite spaces, *Indiana University Mathematics Journal*, **65** (2016), 2125 - 2136.

Tài liệu tham khảo

[1] E. Aksoy Yazici, B. Murphy, M. Rudnev, and I. Shkredov, Growth estimates in positive characteristic via collisions, *International Mathematics Research Notices*, **23**(2017), 7148 - 7189.

[2] N. Alon and Fan R. K. Chung, *Explicit Constructions of linear sized tolerant networks*, *Discrete mathematics*, **2**(1988), 15 - 19.

[3] N. Alon and M. Krivelevich, Constructive bounds for a Ramsey-type problem, *Graphs and Combinatorics*, **13** (1997), 217 - 225.

[4] N. Alon and J. H. Spencer, The probabilistic method, 2nd ed., *Willey-Interscience*, 2000.

[5] A. Balog, K. A. Broughan, I. E. Shparlinski, *Sum-products estimates with several sets and applications*, *Integers*, **12** (5) (2010), 895 - 906.

[6] A. Balog, A note on sum-product estimates, *Publicationes Mathematicae, Debrecen*, **79**(3 - 4) (2011), 283 - 289.

[7] A. Balog, Another Sum-Product Estimate in Finite Fields, *Sovremennye Problemy Matematiki*, **16** (2012), 31 - 37.

[8] E. Bannai, O. Shimabukuro and H. Tanaka, Finite analogues of non-Euclidean spaces and Ramanujan graphs, *European Journal of Combinatorics*, **25** (2004), 243 - 259.

[9] B. Barak, R. Impagliazzo, and A. Wigderson, Extracting randomness using few inde- pendent sources, *SIAM Journal on Computing*, **36** (2006), 1095 - 1118.

[10] N. Biggs, Algebraic Graph Theory, *Cambridge Mathematical Library (2nd ed.), Cambridge University Press*, 1993.

[11] J. Bourgain and S. Konyagin Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order, *Comptes Rendus de l'Académie des Sciences*, **337**(2) (2003), 75 - 80.

[12] J. Bourgain, N. Katz, and T. Tao, A sum product estimate in finite fields and Applications, *Geometric and Functional Analysis,* **14** (2004), 27 - 57.

[13] J. Bourgain, Mordell's exponential sum estimate revisited, *Journal of the AMS - American Mathematical Society*, **18**(2) (2005), 477 - 499.

[14] J. Bourgain, A. Glibichuk, and S. Konyagin Estimates for the number of sums and products for exponentials sums in fields of prime order, *Journal of the London Mathematical Society*, **73** (2006), 380 - 398.

[15] M. Chang, Factorization in generalized arithmetic progressions and applications to the Erdős - Szemerédi sum - product problems, *Geometric and Functional Analysis*, **13** (2003), 720-736.

[16] D. Covert, A. Iosevich, and J. Pakianathan, Geometric configurations in the ring of integers modulo p^l, *Indiana University Mathematics Journal,* **61** (2012), 1949 - 1969.

[17] D. Covert, D. Koh, and Y. Pi, On the sums of any k points in finite fields, *SIAM Journal on Discrete Mathematics*, **30**(1) (2016), 367 - 382.

[18] D. Covert, D. Koh, Y. Pi, The k-resultant modulus set problem on algebraic varieties over finite fields, *Finite Fields and Their Applications,* **48** (2017), 68 - 86.

[19] P. Erdős and E. Szemerédi, On sums and products of integers. *In Studies in pure mathematics, Birkhäuser, Basel,* (1983), 213 - 218.

[20] P. Erdős, Integral distances, *Bulletin of the AMS - American Mathematical Society,* **51** (1945), 996.

[21] G. Elekes and I. Ruzsa, Few sums, many products, *Studia Scientiarum Mathematicarum Hungarica*, **40** (2003), 301 - 308.

[22] G. Elekes, On the number of sums and products, *Acta Arithmetica*, **81**(4) (1997), 365 - 367.

[23] M. Z. Garaev and C.-Y. Shen, On the size of the set A(A + 1),*Mathematische Zeitschrift*, **265** (1) (2010), 125 - 132.

[24] A. A. Glibichuk and S. V. Konyagin, Additive properties of product sets in fields of prime order, *Centre de Recherches Mathematiques, CRM Prceedings and Lecture Notes,* **43** (2007), 279 - 286.

[25] C. Godsil and G. Royle, Algebraic Graph Theory, *Springer (2001), ISBN 0 - 387 - 95241 - 1*, 2000.

[26] L. Guth and N. Katz, On the Erdős distinct distances problem in the plane, *Annals Of Mathematics*, **181** (2015), 155 - 190.

[27] B. Hanson, B. Lund, and O. Roche-Newton, On distinct perpendicular bisectors and pinned distances in finite fields, *Finite Fields and Their Applications*, **37** (2016), 240 - 264.

[28] D. Hart, A. Iosevich, D. Koh and M. Rudnev, Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős - Falconer distance conjecture, *Transactions of the AMS*, **363** (2011) 3255 - 3275.

[29] D. Hart, A. Iosevich, J. Solymosi, Sum-product Estimates in Finite Fields via Kloosterman Sums, *International Mathematics Research Notices* (2007) Vol. **2007**, article ID rmn007, 14 pages.

[30] D. Hart and A. Iosevich, Sum and products in finite fields: an integral geometric view - pint, *Contemporary Mathematics*, **464** (2008), 1 - 9.

[31] D. D. Hieu and L. A. Vinh, On distance sets and product sets in vector spaces over finite rings, *Michigan Mathematical Journal*, **62** (2013), 779 - 792.

[32] D. D. Hieu and L. A. Vinh, On volume set of boxes in finite spaces, *Indiana University Mathematics Journal*, **65** (2016), 2125 - 2136.

[33] D. D. Hieu and P. V. Thang, Distinct distances on regular varieties over finite fields, *Journal of Number Theory*, **173** (2017), 602 - 613.

[34] A. Iosevich and M. Rudnev, Erdős distance problem in vector spaces over finite fields, *Transactions of the American Mathematical Society*, **359** (2007), 6127 - 6142.

[35] D. Koh and C-Y. Shen, The generalized Erdős-Falconer distance problems in vector spaces over finite fields, *Journal of Number Theory,* **132**(11) (2012), 2455 - 2473.

[36] D. Koh and H. Sun, Distance sets of two subsets of vector spaces over finite fields, *Proceedings of the AMS - American Mathematical Society*, **143**(4) (2015), 1679 - 1692.

[37] Kevin Ford, Sums and products from a finite set of real numbers, *Ramanujan Journal*, **2**(1-2) (1998), 59 - 66.

[38] W.M. Kwok, Character tables of association schemes of affine type, *European Journal of Combinatorics*, **13** (1992), 167 - 185.

[39] L. Li and O. Roche-Newton, An improved sum-product estimate for general finite fields, *SIAM Journal on Discrete Mathematics*, **25** (3) (2011), 1285 - 1296.

[40] Mei-Chu Chang, A sum-product estimate in algebraic division algebras, *Israel Journal of Mathematics,* **150** (2005), 369 - 380.

[41] M. Nathanson, On sums and products of integers, *Proceedings of the AMS - American Mathematical Society,* **125**(1) (1997), 9 - 16.

[42] M. Nathanson and G. Tenenbaum, Inverse theorems and the number of sums and products, *Asterisque*, **258** (1999), 195 - 204.

[43] O. Roche-Newton, Sum-ratio estimates over arbitrary finite fields, *arxiv.org/abs*/1407.1654v1.

[44] O. Roche-Newton, M. Rudnev, and Shkredov, New sum-product type estimates over finite fields, *Advances in Mathematics,* **293** (2016), 589 - 605.

[45] O. Roche-Newton, M. Rudnev, and I.D. Shkredov, New sum-product type estimates over finite fields, *Advances in Mathematics,* **293** (2016), 589 - 605.

[46] M. Rudnev, On the number of incidences between points and planes in three dimensions, *Combinatorica*, **38** (1) (2018), 219 - 254.

[47] I. Z. Ruzsa, "On the cardinality of $A + A$ and $A - A$", *Combinatorics, Vol. II., Colloquia Mathematica Societatis János Bolyai, 18, North-Holland, Amsterdam,* (1978), 933 - 938.

[48] A. Sárközy, On sums and products of residues modulo p, *Acta Arithmetica*, **118** (2005), 403 - 409.

[49] A. Sárközy, On products and shifted products of residues modulo p, *Integers: Electronic Journal of Combinatorial Number Theory*, **8**(2)(2008), A9.

[50] I. E. Shparlinski, On the solvability of bilinear equation in finite fields, *Glassgow Mathematical Joernal,* **50** (2008), 523 - 529.

[51] J. Solymosi, On the number of sums and products, *Bulletin of the London Mathematical Society*, **37** (2005), 491 - 494.

[52] Timothy, G. F. Jones and O. Roche-Newton, Improved bounds on the set A(A+1), *Journal of Combinatorial Theory,* **120** (2013), 515 - 526.

[53] P. V. Thang, L. A. Vinh and F. d. Zeeuw, Three-variable expanding polynomials and higher-dimensional distinct distances, *arXiv:1612.09032v2* (2017).

[54] V. H. Van, Sum-product estimates via directed expanders, *Mathematical research letters*, **15**(2) (2008), 375 - 388.

[55] L. A. Vinh, Explicit Ramsey graphs and Erdős distance problem over finite Euclidean and non-Euclidean spaces, *Electronic Journal of Combinatorics*, **15** (2008), Article R5.

[56] L. A. Vinh, Sum and shifted - product subsets of product-sets over finite rings, *The Electronic Journal of Combinatorics*, **19**(2) (2012), P33.

[57] L.A. Vinh, On the generalized Erdős - Falconer distance problems over finite fields, *Journal of Number Theory,* **133** (2013), 2939 - 2947.

[58] L. A. Vinh, Graphs generated by Sidon sets and algebraic equations over finite fields, *Journal of Combinatorial Theory, Series B*, **103**(6) (2013), 651 - 794.

[59] L. A. Vinh, The solvability of norm, bilinear and quadratic equations over finite fields via spectral of graphs, *Forum Mathematicum*, **26** (2014), 141 - 175.