

THÔNG TIN VỀ LUẬN ÁN TIẾN SĨ

1. Họ và tên: Lê Quang Hàm
2. Giới tính: Nam
3. Ngày sinh: 17/11/1979
4. Nơi sinh: Thanh Hóa
5. Quyết định công nhận nghiên cứu sinh: Số 4860/QH - ĐHKHTN, ngày 24/11/2014 của Hiệu trưởng Trường Đại học Khoa học Tự nhiên - ĐHQGHN
6. Các thay đổi trong quá trình đào tạo: Không.
7. Tên đề tài luận án: Xây dựng các lớp hàm nở trên trường và vành hữu hạn.
8. Chuyên ngành: Cơ sở Toán học cho tin học
9. Mã số: 9460117.02.
10. Cán bộ hướng dẫn khoa học: GS.TS. Lê Anh Vinh.
11. Tóm tắt các kết quả mới của luận án:

Với hàm hai biến. Chứng minh một số kết quả về hàm nở hai biến dưới dạng tổng - tích.

Cụ thể:

- Với hàm $f(x, y) = g(x)(h(x) + y)$ ta có

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

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

- Với hàm $f(x, y) = g(x)h(y)(x + y)$, ta có

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

- Với hàm $f(x, y) = xy(g(x) + y)$, ta có

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

Với hàm ba biến. Chứng minh đa thức $axy + g(x) + s(y) + t(z)$ là hàm nở. Bên cạnh đó, cũng đưa ra được một số kết quả dạng tổng-tích sau đây.

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

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

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

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

Với hàm bốn biến. Chứng minh được các lớp hàm $F(u, v, y, z) := f(Q(u, v), y, z)$, trong đó f không có dạng $g(h(x) + k(y) + l(z))$,

$Q(u, v) = m(u) + u^k n(v)$ là nở vừa với ngưỡng $5/13$ trên trường nguyên tố và ngưỡng $3/8$ trên trường hữu hạn bất kỳ.

Trên vành định giá hữu hạn, chúng tôi cũng chứng minh rằng các hàm $u(u+v)y+z$, $u(u+v)+yz$, $u(u+v)(y+z)$, $y(u(u+v)+z)$, $(u(u+v)-y)^2+z$, và $(y-z)^2+u(u+v)$ là nở.

Với các tập tích trên nhóm Heisenberg.

- Trên $\mathcal{H}_1(\mathbb{F}_q)$, trong trường hợp tập lớn, với một tập con A của \mathbb{F}_q có năng lượng cộng tính nhỏ, luận án chứng minh được một kết quả cải thiện $|[A, A, 0][A, A, 0]| \gg Kq|[A, A, 0]|$, và tổng quát trên $\mathcal{H}_n(\mathbb{F}_q)$ cho ta kết quả $|[E, E, 0][E, E, 0]| \gg q|[E, E, 0]|$ với $|E| \gg q^{\frac{n+1}{4}}$.

- Trên $\mathcal{H}_2(\mathbb{F}_p)$, luận án chứng minh được $|[E, E, 0][E, E, 0]| \gg |[E, E, 0]|^{\frac{19}{15}}$, trong đó $|E| \ll p^{8/5}$.

- Trên $\mathcal{H}_1(\mathbb{F}_p)$ luận án chứng minh được $|[A, A, 0][A, A, 0]| \gtrsim |[A, A, 0]|^{\frac{151}{80}}$, với $|A| \lesssim p^{1/2}$.

- Trên $\mathcal{H}_1(\mathbb{C})$, luận án chứng minh được $|[A, A, 0][A, A, 0]| \gtrsim |[A, A, 0]|^{\frac{29}{16}}$ với $|A| \geq 2$,

đây cũng là một mở rộng kết quả của Hegyvári và Hennecart trên trường số thực \mathbb{R} .

12. Khả năng ứng dụng thực tiễn:

Có khả năng ứng dụng vào giải quyết các bài toán thuộc các lĩnh vực như khoa học máy tính lý thuyết, lý thuyết số, mật mã.

13. Các hướng nghiên cứu tiếp theo:

Tập trung nghiên cứu tiếp các bài toán tổ hợp cộng tính, hình học tổ hợp và các bài toán có ứng dụng cho lĩnh vực khoa học máy tính lý thuyết.

14. Các công trình công bố liên quan đến luận án:

- L. Q. Ham, P. V. Thang and L. A. Vinh (2017), “Conditional expanding bounds for two-variable functions over finite valuation rings”, *European Journal of Combinatorics*, 60(2), pp. 114-123.

- Le Quang Ham, Nguyen Van The, Phuc D. Tran and Le Anh Vinh (2020), “On three-variable expanders over finite valuation rings”, *Forum Math*, 33(1), pp. 17–27.

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

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

NGƯỜI HƯỚNG DẪN

GS.TS. Lê Anh Vinh

Ngày 20 tháng 01 năm 2022

NGHIÊN CỨU SINH

Lê Quang Hàm

INFORMATION ON DOCTORAL THESIS

1. Full name: Lê Quang Hàm
2. Gender: Male
3. Date of birth: 17th November 1979
4. Place of birth: Thanh Hóa
5. Admission decision number: 4860/QD – DHKHTN, date on 24th November 2014 by Rector of VNU University of Science
6. Changes in academic process: No.
7. Official thesis title: *Expanding polynomials over finite rings.*
8. Major: Mathematical foundation for Computers
9. Code: 9460117.02.
10. Supervisor: Prof.Dr. Lê Anh Vinh.
11. Summary of the new findings of the thesis:

Two - variable functions. several two-variable expanders having sum - product form.

- For $f(x, y) = g(x)(\square(x) + y)$,

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

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

- For $f(x, y) = g(x)\square(y)(x + y)$,

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

- For $f(x, y) = xy(g(x) + y)$,

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

Three - variable functions. The polynomials $axy + g(x) + s(y) + t(z)$ are expanders and several sum - product type results.

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

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

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

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

Four - variable functions. $F(u, v, y, z) := f(Q(u, v), y, z)$, where f does not have form of $g(\square(x) + k(y) + l(z))$, $Q(u, v) = m(u) + u^k n(v)$ are expanders with threshold of $5/13$ over finite prime fields and threshold $3/8$

over finite fields. Additionally, we established the expanders $u(u+v)y+z$, $u(u+v)+yz$, $u(u+v)(y+z)$, $y(u(u+v)+z)$, $(u(u+v)-y)^2+z$, and $(y-z)^2+u(u+v)$ over finite valuation rings \square .

The product - set over Heisenberg groups.

- Over $\square_1(\mathbb{F}_q)$, let $A \subset \mathbb{F}_q$, we have $|[A, A, 0][A, A, 0]| \gg Kq|[A, A, 0]|$, and in general, we have $|[E, E, 0][E, E, 0]| \gg q|[E, E, 0]|$ where $|E| \gg q^{\frac{n+1}{2}}$ over $\square_n(\mathbb{F}_q)$.

- Let $E \subset \square_2(\mathbb{F}_p)$, $|[E, E, 0][E, E, 0]| \gg |[E, E, 0]|^{\frac{19}{15}}$, where $|E| \ll p^{8/5}$.

- Let $A \subset \square_1(\mathbb{F}_p)$, $|[A, A, 0][A, A, 0]| \gtrsim |[A, A, 0]|^{\frac{151}{80}}$, where $|A| \lesssim p^{1/2}$.

- Let $A \subset \square_1(\square)$, $|[A, A, 0][A, A, 0]| \gtrsim |[A, A, 0]|^{\frac{29}{16}}$ where $|A| \geq 2$.

12. Potential applications:

These results can be applied to some areas such as incidence geometry, combinatorics, expanders, extractors, dispersers, complexity theory, pseudorandomness, property testing, hardness amplification, probabilistic checkable proofs (PCPs), and cryptography.

13. Further works: Discrete Combinatorial Geometry and Additive Combinatorics.

14. Thesis-related publications:

- L. Q. Ham, P. V. Thang and L. A. Vinh (2017), “Conditional expanding bounds for two-variable functions over finite valuation rings”, *European Journal of Combinatorics*, 60(2), pp. 114-123.

- Le Quang Ham, Nguyen Van The, Phuc D. Tran and Le Anh Vinh (2020), “On three-variable expanders over finite valuation rings”, *Forum Math*, 33(1), pp. 17–27.

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

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

Thursday, 20th January 2022

SUPERVISOR

PhD STUDENT

Prof.Dr. Lê Anh Vinh

Lê Quang Hàm