3. Đa thức và các kỹ thuật liên quan

Ngày 22 tháng 7 năm 2025

1 Đa thức cơ bản

Một đa thức là biểu thức dạng:

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \ldots + a_dx^d$$

trong đó a_i là các hệ số hằng số và x là biến.

Nếu đa thức chỉ có một biến, gọi là đa thức đơn biến (univariate polynomial).

Một điểm quan trọng: Nếu $p(x)$ là đa thức và $p(a) = 0$, thì $(x-a)$ là một thừa số của $p(x)$. Tức là tồn tại đa thức $q(x)$ sao cho:

$$p(x) = (x-a)q(x), \quad \deg(p) = \deg(q) + 1$$

2 Đa thức và điểm nghiệm

Schwartz-Zippel Lemma:
Hai đa thức khác nhau chỉ có thể bằng nhau tại rất ít điểm. Cụ thể, nếu $p(x)$ và $q(x)$ là hai đa thức bậc tối đa d, thì số điểm x sao cho $p(x) = q(x)$ không quá d.

Ý nghĩa: Giúp kiểm tra hai đa thức có bằng nhau không bằng cách so sánh giá trị tại vài điểm ngẫu nhiên.

3 Nội suy Lagrange (Lagrange Interpolation)

Cho tập hợp các điểm $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$, ta có thể tìm một đa thức bậc $n-1$ duy nhất đi qua các điểm này.

Ví dụ:

- 2 điểm xác định đường thẳng.
- 3 điểm xác định parabol bậc 2.
- n điểm xác định đa thức bậc $n-1$.

Nội suy là cơ sở để biểu diễn đa thức dưới dạng các điểm giá trị thay vì hệ số.

4 Hai cách biểu diễn đa thức

Dạng hệ số (Coefficient form):

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_dx^d$$

Dạng điểm giá trị (Point value form):
Là tập các điểm (x_i, y_i) với $y_i = f(x_i)$.

Hai dạng này có thể chuyển đổi qua lại bằng phương pháp nội suy và đánh giá.

5 Các sơ đồ cam kết đa thức (Polynomial Commitment Schemes)

Cam kết đa thức là giao thức giữa:

- **Người cam kết (Prover):** cam kết đa thức P.
- **Người kiểm chứng (Verifier):** kiểm tra giá trị $P(z) = a$ tại một điểm z mà không biết toàn bộ P.

Yêu cầu:

- **Ràng buộc (Binding):** Không thể mở cam kết thành giá trị khác.
- **Bí mật (Hiding):** Không tiết lộ thông tin gì về P.

Một số sơ đồ phổ biến:

- **FRI:** nền tảng cho STARKs.
- **KZG:** dựa trên elliptic curve và pairing, dùng trong SNARKs.
- **IPA:** dẫn đến Bulletproofs.

6 Sơ lược về KZG Commitment

Ý tưởng: Cam kết đa thức thông qua điểm trong nhóm elliptic với SRS dựa trên giá trị bí mật s.

Tạo SRS:

$$\{G, sG, s^2G, \ldots, s^dG\}$$

trong đó G là phần tử sinh của nhóm elliptic.

Cam kết cho $f(x) = f_0 + f_1x + f_2x^2 + \ldots + f_dx^d$:

$$\text{com}(f) = f_0G + f_1sG + f_2s^2G + \ldots + f_ds^dG = f(s)G$$

Prover cung cấp bằng chứng $f(z) = a$ mà không tiết lộ f.

Cam kết có kích thước và bằng chứng nhỏ, độc lập với bậc đa thức.

7 Mã sửa lỗi và chia sẻ bí mật

Reed-Solomon codes:
Dùng đa thức để mã hóa dữ liệu bằng cách đánh giá tại nhiều điểm — giúp sửa lỗi.

Shamir Secret Sharing:
Dùng đa thức bậc $k-1$ để chia bí mật thành n phần, cần ít nhất k phần để khôi phục bí mật.
Bí mật là hệ số tự do a_0 của đa thức. Mỗi phần là điểm $(i, f(i))$.

8 Kỹ thuật đa thức trong ZKP

Dùng đa thức để biểu diễn các ràng buộc logic trong chứng minh:

Ví dụ: ràng buộc đầu ra chỉ là 0 hoặc 1:

$$C(x) = x(x-1)$$

Nếu đầu ra $P(x)$ thỏa mãn ràng buộc, tồn tại $P'(x)$ sao cho:

$$C(P(x)) = P'(x) \cdot V(x)$$

với $V(x)$ là đa thức có nghiệm tại các điểm được kiểm tra.

Nếu $P(x)$ không thỏa mãn, thì không tồn tại $P'(x)$ phù hợp.

Tóm lại

Mục này giới thiệu các khái niệm và công cụ đa thức quan trọng như nội suy, cam kết đa thức và ứng dụng trong chia sẻ bí mật, sửa lỗi, cũng như cách biểu diễn ràng buộc bằng đa thức phục vụ cho chứng minh không tiết lộ.