Complexidade Computacional De Problemas de Curvas Elípticas

Thomas Michael Bartlett

DCA-FEEC-UNICAMP
Seminário CAta

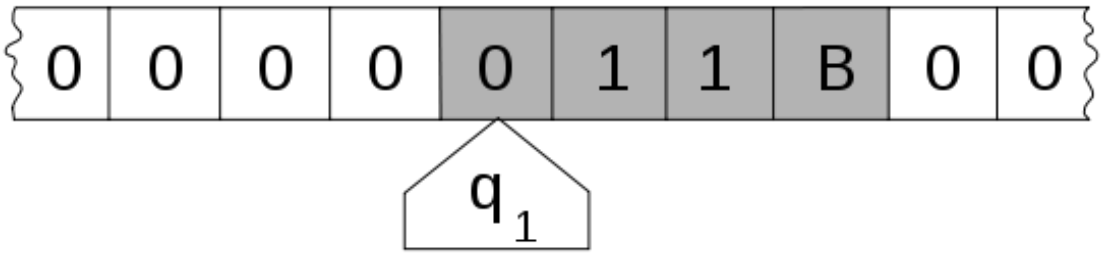
th.m.bartlett@gmail.com

19 de junho de 2015

Conteúdo

1. Teoria da Computação
   - Máquina de Turing
   - Complexidade Computacional
2. Complexidade de Códigos Algebro-Geométricos
   - Problemas NP-díficeis
   - Distância de Hamming
   - MLDP

Máquina de Turing



- Q is a finite, non-empty set of states
- Γ is a finite, non-empty set of tape alphabet symbols
- $B \in \Gamma$ is the blank symbol
- $\Sigma \subseteq \Gamma \setminus \{B\}$ is the set of input symbols
- $\delta : (Q \setminus F) \times \Gamma \to Q \times \Gamma \times \{L, R\}$ is a partial function called the transition function, where L is left shift, R is right shift.
- $q_0 \in Q$ is the initial state
- $F \subseteq Q$ is the set of final or accepting states.

Classes de Complexidade Computacional

P é classe dos algoritmos tal que $DTIME(n^{O(1)})$.
NP é classe dos algoritmos tal que $NTIME(n^{O(1)})$.
Um algoritmo é RP se o algoritmo permite uma escolha aleatória durante sua execução em tempo polinomial. O único caso em que o algoritmo retorna "SIM"se é a resposta é realmente "SIM"mas pode retornar "NÃO"sem ser correta a resposta.

Problema de Soma de Subconjunto

Instância: Um conjunto $A = \{a_1, a_2, ..., a_n\}$ de n inteiros positivos, um inteiro positivo b e um inteiro positivo $k < n$.
Questão: Existe um subconjunto não-vazio $\{a_{i_1}, a_{i_2}, ..., a_{i_k}\} \subset A$ de cardinalidade k tal que

$$a_{i_1} + a_{i_2} + ... + a_{i_k} = b \ ?$$

Enunciado dos Problemas

Problema da distância de Hamming do código
Instância: Um código Álgebro-Geométrico $[n,k]_p$.
Questão: Esse código é máxima distância separável, i.e. $d = n-k+1$ com d sendo a distância de Hamming do código?

Problema da Decodificação de Máxima Verossemelhança
Instância: Um código Álgebro-Geométrico $[n,k]_p$ e uma palavra-código $y \in \mathbb{F}_p^n$.
Questão: Ache a palavra-código que minimiza a distância de Hamming a y?

Problema de Soma de Subconjunto em Curvas Elípticas

Problema de Soma de Subconjunto em Curvas Elípticas
Instância: Um primo p , uma curva elíptica C sobre $\mathbb{F}_p$, um conjunto de pontos $A = \{P_1, P_2..., P_n, Q\}$ na curva e um inteiro positivo $k < n$.
Questão: Existe um subconjunto não-vazio $\{P_{i_1}, P_{i_2}, ..., P_{i_k}\} \subset A$ de cardinalidade k tal que

$$P_{i_1} + P_{i_2} + ... + P_{i_k} = Q \ ?$$

Teorema

O Problema de Soma de Subconjunto em Curvas Elípticas é NP-Difícil.

O seguinte teorema de [4] será usado na demonstração.

Teorema

Dado um N inteiro positivo, existe um algoritmo randomizado que encontra um primo $p > N$, uma curva elíptica C sobre $\mathbb{F}_p$ e um ponto G na curva de ordem de grupo elíptico maior que N. Esse algoritmo tem em média número de passos polinomialmente em $\log N$.

Prova:

O problema de Soma de Subconjunto será reduzido ao PSSCE, dessa forma PSSCE é NP-díficil pois no mínimo tem a mesma complexidade de PSS.

Conforme o teorema acima em tem polinomial, seja um primo $p > a_1 + ... + a_n - b$,uma curva elíptica C sobre $\mathbb{F}_p$ e G um ponto de ordem $q > a_1 + ... + a_n - b$. Então, defina

$$Q = bG,\ P_1 = a_1 G,\ P_2 = a_2 G, ...,\ P_n = a_n G\ .$$

Então,

$$P_{i_1} + P_{i_2} + ... + P_{i_k} = Q$$

se e somente se

$$a_{i_1} + a_{i_2} + ... + a_{i_k} \equiv b\ (mod\ q) \Leftrightarrow a_{i_1} + a_{i_2} + ... + a_{i_k} = b\ .$$

Distância de Hamming é NP-difícil

Teorema

Dada a instância do problema de Problema de Soma de Subconjunto em Curvas Elípticas, podemos construir, em tempo polinomial randomizado, um código algebro geométrico $[n,k]_p$ com tal que se a resposta para o PSSCE é "SIM"então o código tem distância mínima de $n-k$. Se a resposta para o PSSCE é "NÃO"então o código tem distância mínima de $n-k+1$

Corolário

Decidir se um código AG é separável por máxima distância é NP-díficil sob uma redução randomizada.

Vamos usar os seguintes resultados:

Proposição

(De [5]) Seja $P_1, P_2, ..., P_n, P$ elementos de $E(F_q)$ distintos de O. Se $m_1P_1 + m_2P_2 + ... + m_nP_n = P$ com $m_1 \in \mathbb{Z}_+$, então existe uma função tendo zeros em $P_1, P_2, ..., P_n$ com multiplicidade $m_1, m_2, ...m_n$ resp., um pólo em P com mult. 1 e um pólo em O com mult. $m_1 + m_2 + ... + m_n - 1$. Podemos computar essa função em tempo polinomial em $m_1 + m_2 + ... + m_n$ e $\log q$.

Proposição

Existe um algoritmo randomizado que calcula a base de $L(\alpha O)$ e $L(Q + \alpha O)$ polinomial em α e $\log q$

Prova:
Seja $f_1, f_2, ..., f_k$ uma base para $L(Q+(k-1)O)$, então considere o código C cuja matriz geradora é conforme abaixo:

$$\begin{bmatrix} f_1(P_1) & f_1(P_2) & \cdots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \cdots & f_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_k(P_1) & f_k(P_2) & \cdots & f_k(P_n) \end{bmatrix}$$

Pela limitação de Singleton, sabemos que a distância de Hamming $d = min_{x \neq y \in C} d(x,y) \leq n-k+1$. Pela construção do código, sabemos que $d \geq n-k$, então $d \in \{n-k, n-k+1\}$.

Se a resposta do PSSCE é "SIM"então existe $\{P_{i_1}, P_{i_2}, \cdots, P_{i_k}\} \subset P_1, P_2, \cdots, P_n$ tal que $P_{i_1} + P_{i_2} + \cdots + P_{i_k} = Q$.
Então, pela Proposição acima, existe $f \in L(-P_{i_1} - P_{i_2} - \cdots - P_{i_k} + Q + (k-1)O) \Rightarrow f \in L(Q + (k-1)O)$.
A palavra código correspondente a f tem peso $n-k$ pois $(f(P_1), f(P_2), ..., f(P_n))$ tem k zeros. Então $d = n-k$.
Na outra direção, se $d = n-k$ então existe $f \in L(Q + (k-1)O)$ tal que tem k zeros em $\{P_1, ..., P_n\}$. Denote esses zeros por $P_{i_1}, P_{i_2}, \cdots, P_{i_k}$. Como f não tem mais de k pólos contando multiplicidades, f tem exatamente k zeros com multiplicidade um. Então $(f) = -P_{i_1} - P_{i_2} - \cdots - P_{i_k} + Q + (k-1)O$ e

$$P_{i_1} + P_{i_2} + \cdots + P_{i_k} = Q$$

Se a resposta do PSSCE é "NÃO"então $d = n-k+1$.

Decodificação de Máxima Verossemelhança é NP-difícil

Lema

Considere o código gerado por aplicar função de $L((k-1)O)$ *em* $P_1, P_2, ..., P_n$. *Supõe que* $f' \in L(Q+(k-1)O) - L((k-1)O)$ *e que a palavra recebida é* $R = ((f'(P_1), f'(P_2), ..., f'(P_n)))$. *Então,*
1)A distância entre R e o código é $n-k+1$ *ou* $n-k$;
2)A distância entre R e o código é $n-k$ *se e só se existe* $\{P_{i_1}, P_{i_2}, \cdots, P_{i_k}\} \subset P_1, P_2, \cdots, P_n$ *tal que*

$$P_{i_1} + P_{i_2} + \cdots + P_{i_k} = Q$$

Teorema

Dado um vetor recebido, computar a distância desse vetor ao código elíptico é NP-Hard sobre uma redução randomizada. Então, o MLDP para código algebro geométricos é NP-Hard sobre uma redução randomizada.

CHENG, Qi. Hard problems of algebraic geometry codes. Information Theory, IEEE Transactions on, v. 54, n. 1, p. 402-406, 2008.

COOPER, S. Barry. Computability theory. CRC Press, 2003.

MULMULEY, Ketan D.; SOHONI, Milind. Geometric complexity theory I: An approach to the P vs. NP and related problems. SIAM Journal on Computing, v. 31, n. 2, p. 496-526, 2001.

GOLDWASSER, Shafi; KILIAN, Joe. Primality testing using elliptic curves. Journal of the ACM (JACM), v. 46, n. 4, p. 450-472, 1999.

HUANG, Ming-Deh; IERARDI, Doug. Efficient algorithms for the Riemann-Roch problem and for addition in the

Jacobian of a curve. Journal of Symbolic Computation, v. 18, n. 6, p. 519-539, 1994.