MACY projekt 10

15 maj 2025

Bartłomiej Miłkowski, Jan Sosnowski, Ignacy Prugarewicz

Problemy kratowe są ważnym elementem wykorzystywanym w informatyce w budowie systemów kryptograficznych. W projekcie przedstawione zostało 5 algorytmów aproksymacyjnych dla trzech przypadków:

* SVP (Shortest Vector Problem)
* CVP (Closest Vector Problem)
* SIVP (Shortest Independent Vectors Problem)

Spis treści

1. LLL
2. AKS
3. Hill Climbing SVP
4. ENUM
5. Gauss Sieve

Pierwszym zaimplementowanym algorytmem jest LLL (algorytm Lenstra-Lenstra-Lovasz). Jest to algorytm aproksymacyjny rozwiązujący problem najkrótszego wektora. Algorytm znajduje taką bazę jakiejś kraty, w której wektory są krótsze i ortogonalne. Warunkiem działania programu jest podanie wektorów wejściowych, które są oczywiście liniowo niezależne. Do implementacji dołączona jest funkcja ortogonalizująca wektory wejściowe.

Algorytm Ajati-Kumar-Sivakumar jest probabilistycznym algorytmem aproksymacyjnym rozwiązującym problem najkrótszego wektora. W przeciwieństwie do powyższego algorytmu LLL, wykorzystuje on losowe próbkowanie w kracie i jest oparty na teorii siatek losowych. Przeważnie pozwala na uzyskanie lepszej aproksymacji niż algorytm LLL, jednak sama złożoność obliczeniowa algorytmu jest większa.

Różnice w algorytmach LLL oraz AKS polegają na tym, że LLL zwraca całą zredukowaną bazę kratową, natomiast AKS zwraca jedynie jeden najkrótszy wektor.

Hill Climbing to heurystyczny algorytm poszukiwania lokalnego minimum długości wektora w kracie. Algorytm zaczyna od losowego wektora kratowego i próbuje go lokalnie poprawić poprzez dodawanie lub odejmowanie wektorów bazy (lub ich wielokrotności). Jeśli nowy wektor ma mniejszą normę euklidesową, staje się aktualnym kandydatem. Proces ten jest powtarzany, aż osiągnięty zostanie punkt, którego nie można dalej poprawić przy zadanym kroku — czyli znajduje lokalne minimum. Skuteczny głównie w małych wymiarach lub przy wielu losowych restartach.

ENUM, czyli metoda enumeracji, to dokładny algorytm przeszukujący przestrzeń wszystkich możliwych kombinacji wektorów kratowych w zadanym promieniu od zera. Wykorzystuje ortogonalizację Grama-Schmidta do ograniczania przestrzeni przeszukiwania i poruszania się po drzewie rozgałęzień z odcinaniem gałęzi, które nie mogą prowadzić do lepszego rozwiązania. Wysoka złożoność obliczeniowa, rosnąca wykładniczo z wymiarem.

Sito Gaussa to heurystyczny algorytm inspirowany redukcją Gaussa w 2D, rozszerzony na wyższe wymiary. Algorytm iteracyjnie tworzy listę krótkich wektorów kratowych. Każdy nowy wektor jest redukowany względem istniejących elementów listy, a następnie sam może posłużyć do redukcji tych wektorów. Tylko wektory, których nie da się bardziej zredukować, zostają dodane do listy. Heurystyczny, ale efektywny w praktyce dla wymiarów do ~80.

Implementacja: <https://github.com/jansosna7/MACY>

Przykład działania:

Obraz zawierający tekst, zrzut ekranu, Czcionka, dokument

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna. Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Zawartość wygenerowana przez sztuczną inteligencję może być niepoprawna.

Źródła:

<https://en.wikipedia.org/wiki/Lenstra%E2%80%93Lenstra%E2%80%93Lov%C3%A1sz_lattice_basis_reduction_algorithm>

<https://www.sciencedirect.com/science/article/pii/S0304397508009316>