

به نام خدا

اعضاء گروه : سیدعلی اسیائی، علی رضوی

توضیحات پروژه پایانی جبر خطی

روش حذفی گاوس جردن : پیچیدگی زمانی از مرتبه $O(N^3)$ و پیچیدگی مکانی از مرتبه $O(N^2)$

روش بسط لاپلاس : پیچیدگی زمانی از مرتبه $O(N!)$ و پیچیدگی مکانی از مرتبه $O(N^3)$

روش امید رضایی فر : پیچیدگی زمانی از مرتبه $O(4^N)$ و پیچیدگی مکانی از مرتبه $O(N^3)$

در ادامه دقت و کارایی سه روش را در ماتریس های با ابعاد مختلف مقایسه میکنیم و در نهایت بهترین روش را انتخاب میکنیم :

1) روش گاوس-جردن

دقت

- روش گاوس-جردن با استفاده از عملیات های خطی و ضرب ماتریس ها، دقت بالایی دارد. اما در صورتی که اعداد موجود در ماتریس بسیار بزرگ یا بسیار کوچک باشند، ممکن است به دلیل خطاهای عددی دقت کاهش یابد

کارایی

- زمان اجرا : $O(N^3)$

- برای ماتریس های کوچک و متوسط (تا حدود $100 * 100$) کارایی بسیار خوبی دارد
- برای ماتریس های بزرگتر، زمان اجرا به دلیل پیچیدگی $O(N^3)$ ممکن است طولانی شود

فضای مورد نیاز

- فضای ذخیره سازی : $O(N^2)$

- نیاز به فضای N^2 برای ذخیره سازی ماتریس اصلی و ماتریس های میانی

2) روش گسترش لاپلاس

دقت

- گسترش لاپلاس یکی از روش‌های کلاسیک و دقیق برای محاسبه دترمینان است. اما در ماتریس‌های بزرگ به دلیل تعداد زیاد محاسبات، خطاهای عددی ممکن است افزایش یابد

کارایی

- زمان اجرا : $O(N!)$

- برای ماتریس‌های کوچک (تا حدود $10 * 10$) مناسب است
- برای ماتریس‌های بزرگتر، پیچیدگی فاکتوریل باعث می‌شود که زمان اجرا به شدت افزایش یابد و این روش عملاً غیرقابل استفاده شود

فضای مورد نیاز

- فضای ذخیره‌سازی : $O(N^3)$

- برای هر زیرماتریس نیاز به فضای ذخیره‌سازی جدید دارد، اما به دلیل بازگشت به عقب، فضای مورد نیاز تا حدی کاهش می‌یابد

3) روش امید رضایی فر

دقت

- این روش دقت بالایی دارد، اما مانند دیگر روش‌ها، ممکن است در اعداد بسیار بزرگ یا کوچک خطاهای عددی رخ دهد

کارایی

- زمان اجرا : $O(4^N)$

- برای ماتریس‌های کوچک تا متوسط (تا حدود $10 * 10$) مناسب است.
- برای ماتریس‌های بزرگتر، پیچیدگی نمایی باعث می‌شود که زمان اجرا به شدت افزایش یابد و این روش عملاً غیرقابل استفاده شود

فضای مورد نیاز

- فضای ذخیره‌سازی : $O(N^3)$

- نیاز به فضای N^2 برای ذخیره‌سازی ماتریس اصلی و فضای اضافی برای ذخیره‌سازی گراف و ماتریس‌های میانی

مقایسه کلی

- برای ماتریس‌های کوچک (تا حدود $10 * 10$) :

- روش گسترش لاپلاس : دقیق و مناسب، اما زمان اجرا بالا

- روش گاوس-جردن : دقیق و کارا
- روش امید رضایی فر : دقیق، اما زمان اجرا بالا
- برای ماتریس‌های متوسط (تا حدود $50 * 50$) :
- روش گاوس-جردن : دقیق و کارا، پیچیدگی $O(N^3)$ نسبت به سایر روش‌ها بهتر است
- روش امید رضایی فر : زمان اجرا بالا
- روش گسترش لاپلاس : زمان اجرا بسیار بالا
- برای ماتریس‌های بزرگتر (بیشتر از $50 * 50$) :
- روش گاوس-جردن : دقیق و کارا، مناسب‌ترین روش از نظر زمان اجرا
- روش امید رضایی فر و روش گسترش لاپلاس : زمان اجرا بسیار بالا و عملاً غیرقابل استفاده

بهترین روش

روش گاوس جردن به دلیل پیچیدگی زمانی $O(N^3)$ و فضای ذخیره‌سازی $O(N^2)$ ، به ویژه برای ماتریس‌های بزرگ، از نظر کارایی برتری دارد و همچنان دقت بالایی را حفظ می‌کند. روش بسط لاپلاس تنها برای ماتریس‌های بسیار کوچک مناسب است و روش امید رضایی فر برای موارد خاص و ماتریس‌های کوچک تا متوسط کاربرد دارد.

در نتیجه ما روش گاوس جردن را برای محاسبه دترمینان در الگوریتم hill cipher استفاده می‌کنیم لازم به ذکر است برای قسمت hill cipher رابط کاربری هم پیاده سازی شده است. جهت استفاده از رابط کاربری فایل main.py در پوشه Code را اجرا کنید.

ضمناً از گیت هاب در توسعه این پروژه استفاده شده است. لینک ریپوی گیت هاب:

Github Repository : <https://github.com/paranism0/HillCipher>