

Fourier aplicado al algoritmo de Schönhage-Strassen

Lucía Mielgo

May 11, 2023

Contents

1	Introducción	3
1.1	Contexto y motivación	3
1.2	Objetivos del trabajo	3
2	Fundamentos teóricos	3
2.1	Aritmética de enteros y multiplicación clásica	3
2.2	Transformada rápida de Fourier (FFT)	3
2.3	Aritmética modular	3
3	Descripción del algoritmo de Schönhage-Strassen	3
3.1	Explicación general del enfoque y estrategia	3
3.2	Descomposición en polinomios	3
3.3	Multiplicación de polinomios mediante FFT	3
3.4	Manejo de la aritmética modular	3
4	Análisis de complejidad	3
4.1	Complejidad asintótica del algoritmo	3
4.2	Comparación con la multiplicación clásica	3
4.3	Estudio de las constantes ocultas y su impacto práctico	3
5	Implementación y consideraciones prácticas	3
5.1	Detalles de implementación del algoritmo	3
5.2	Optimizaciones y mejoras posibles	3
5.3	Evaluación experimental de rendimiento	3
6	Aplicaciones y casos de uso	3
6.1	Escenarios en los que el algoritmo es particularmente útil	3
6.2	Ejemplos de aplicaciones prácticas	3
7	Avances y variantes del algoritmo	3
7.1	Desarrollos posteriores al algoritmo original	3
7.2	Variantes y mejoras propuestas por otros investigadores	3
8	Limitaciones y consideraciones adicionales	3
8.1	Tamaño de los números en los que el algoritmo es efectivo	3
8.2	Casos en los que otros enfoques pueden ser más adecuados	3
8.3	Desafíos y obstáculos para su implementación y uso	3
9	Conclusiones y perspectivas futuras	3
9.1	Resumen de los hallazgos clave	3
9.2	Reflexiones sobre las fortalezas y debilidades del algoritmo	3
9.3	Posibles direcciones para futuras investigaciones relacionadas	3

1 Introducción

1.1 Contexto y motivación

1.2 Objetivos del trabajo

2 Fundamentos teóricos

2.1 Aritmética de enteros y multiplicación clásica

2.2 Transformada rápida de Fourier (FFT)

2.3 Aritmética modular

3 Descripción del algoritmo de Schönhage-Strassen

3.1 Explicación general del enfoque y estrategia

3.2 Descomposición en polinomios

3.3 Multiplicación de polinomios mediante FFT

3.4 Manejo de la aritmética modular

4 Análisis de complejidad

4.1 Complejidad asintótica del algoritmo

4.2 Comparación con la multiplicación clásica

4.3 Estudio de las constantes ocultas y su impacto práctico

5 Implementación y consideraciones prácticas

5.1 Detalles de implementación del algoritmo

5.2 Optimizaciones y mejoras posibles

5.3 Evaluación experimental de rendimiento

6 Aplicaciones y casos de uso

6.1 Escenarios en los que el algoritmo es particularmente útil

6.2 Ejemplos de aplicaciones prácticas

7 Avances y variantes del algoritmo

7.1 Desarrollos posteriores al algoritmo original

7.2 Variantes y mejoras propuestas por otros investigadores

8 Limitaciones y consideraciones adicionales

8.1 Tamaño de los números en los que el algoritmo es efectivo

8.2 Casos en los que otros enfoques pueden ser más adecuados

8.3 Desafíos y obstáculos para su implementación y uso

9 Conclusiones y perspectivas futuras