Resolución de sistemas de Toeplitz sobre cuerpos finitos

VIII Jornadas de Matemática Discreta y Algorítmica

N. Busom, J.M. Miret, F. Sebé

Departament de Matemàtica
Universitat de Lleida

Almería, 12 de Julio de 2012

Índice

Sección 1 | Introducción

Definición

Una matriz de Toeplitz T de orden $n+1$, cuyos elementos pertenecen a un cuerpo $\mathbb{K}$, es una matriz cuadrada en la que cada diagonal descendiente de izquierda a derecha es constante. Esto es:

$$T = \begin{pmatrix} t_0 & t_{-1} & t_{-2} & \dots & t_{-n} \\ t_1 & t_0 & t_{-1} & \dots & t_{-n+1} \\ t_2 & t_1 & t_0 & \dots & t_{-n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_n & t_{n-1} & t_{n-2} & \dots & t_0 \end{pmatrix}.$$

Ejemplo: Matriz de Toeplitz 4×4

$$T_4 = \begin{pmatrix} 1 & 3 & 7 & 9 \\ 2 & 1 & 3 & 7 \\ 8 & 2 & 1 & 3 \\ 4 & 8 & 2 & 1 \end{pmatrix}.$$

Estado del arte

Sistema de Toeplitz

$$\begin{pmatrix} t_0 & t_{-1} & t_{-2} & \dots & t_{-n} \\ t_1 & t_0 & t_{-1} & \dots & t_{-n+1} \\ t_2 & t_1 & t_0 & \dots & t_{-n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_n & t_{n-1} & t_{n-2} & \dots & t_0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

Complejidad

- El método de Gauss resuelve cualquier sistema lineal de ecuaciones de orden $n+1$ en $O(n^3)$.
- El método de Levinson resuelve un sistema de Toeplitz de orden $n+1$ sobre los reales en $O(n^2)$.
- El método de Kumar resuelve un sistema de Toeplitz de orden $n+1$ **sobre los reales** en $O(n \log^2 n)$.

Objetivo

Solucionar sistemas de Toeplitz sobre cuerpos finitos en $O(n \log^2 n)$.

Sección 2 Transformada de Fourier

Discrete Fourier Transform (DFT)

- Entrada: secuencia de N números complejos $x_0, x_1, \ldots, x_{N-1}$.
- Salida: secuencia de N números complejos $X_0, X_1, \ldots, X_{N-1}$.

DFT

$$X_j = \sum_{k=0}^{N-1} x_k e^{-\frac{2\pi i}{N} jk}, \qquad j = 0, 1, \ldots, N-1.$$

donde i es la unidad imaginaria y $e^{\frac{2\pi i}{N}}$ es una raíz N-ésima primitiva de la unidad.

Inverse Discrete Fourier Transform (IDFT)

- Entrada: secuencia de N números complejos $X_0, \ldots, X_{N-1}$.
- Salida: secuencia de N números complejos $x_0, \ldots, x_{N-1}$.

IDFT

$$x_j = \frac{1}{N} \sum_{k=0}^{N-1} X_k e^{\frac{2\pi i}{N} jk} \qquad j = 0, 1, \cdots, N-1.$$

donde i es la unidad imaginaria y $e^{\frac{2\pi i}{N}}$ es una raíz N-ésima primitiva de la unidad.

Number Theoretic Transform (NTT)

- Entrada: secuencia de N números $x_0, x_1, \ldots, x_{N-1}$ sobre $\mathbb{F}_p$.
- Salida: secuencia de N números $X_0, X_1, \ldots, X_{N-1}$ sobre $\mathbb{F}_p$.

NTT

$$X_j \equiv \sum_{k=0}^{N-1} x_k (\omega^\zeta)^{jk} \pmod{p} \quad j = 0, 1, \ldots, N-1,$$

donde ω^ζ es una raíz N-ésima primitiva de la unidad.

Condición necesaria y suficiente

Necesitamos que $N \mid (p-1)$, esto es $p = \zeta N + 1$ para algún entero positivo ζ.

Cálculo de la convolución circular $a \circledast b$

1. Calcular las NTT de a y b

$$A = NTT(a);\ B = NTT(b)$$

2. Multiplicar las secuencias elemento a elemento

$$C = A \cdot B$$

3. Calcular la NTT^{-1} de C

$$a \circledast b = NTT^{-1}(C)$$

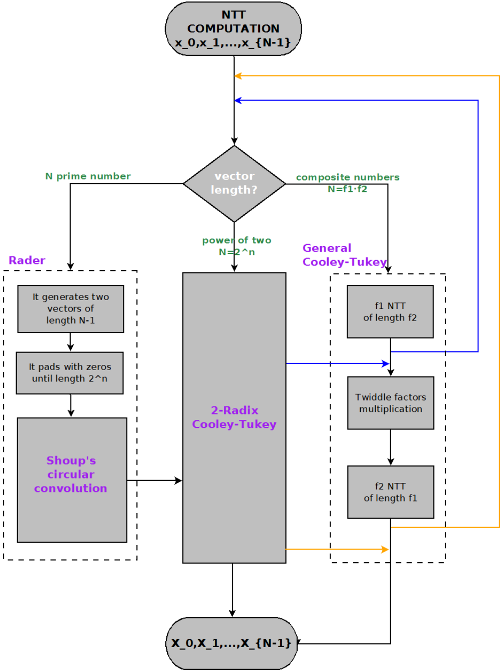
Convolución lineal y circular

Si dos secuencias de m elementos son extendidas añadiendo m ceros al final, entonces la convolución circular es equivalente a la lineal.

Fast Fourier Transform (FFT)

Definición

Una Fast Fourier Transform (FFT) es un algoritmo eficiente que calcula la NTT así como su inversa en tiempo $O(n \log n)$.


NTT COMPUTATION x_0,x_1,...,x_{N-1}
vector length?
N prime number
composite numbers N=f1·f2
power of two N=2^n
Rader
It generates two vectors of length N-1
It pads with zeros until length 2^n
Shoup's circular convolution
2-Radix Cooley-Tukey
General Cooley-Tukey
f1 NTT of length f2
Twiddle factors multiplication
f2 NTT of length f1
X_0,X_1,...,X_{N-1}

Sección 3 | Algoritmo de Kumar

Algoritmo de Kumar

$$\begin{pmatrix} t_0 & t_{-1} & t_{-2} & \dots & t_{-n} \\ t_1 & t_0 & t_{-1} & \dots & t_{-n+1} \\ t_2 & t_1 & t_0 & \dots & t_{-n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ t_n & t_{n-1} & t_{n-2} & \dots & t_0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}, t_i, x_i, y_i \in \mathbb{R}$$

Pasos

1. Construir una matriz circulante C a partir de una matriz de Toeplitz T. Calcular la matriz inversa de C.
2. Calcular la primera fila y la primera columna de la matriz inversa de T, a partir de la primera fila y columna de C^{-1}.
3. Resolver el sistema de Toeplitz en términos de la primera fila y la primera columna de T^{-1}.

Paso 1

1.1 Construir una matriz circulante C a partir de una matriz de Toeplitz T.

$$C=\begin{pmatrix} t_0 & t_{-1} & \dots & t_{-n} & t_n & \dots & t_2 & t_1 \\ t_1 & t_0 & \dots & t_{-n+1} & t_{-n} & \dots & t_3 & t_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_n & t_{n-1} & \dots & t_0 & t_{-1} & \dots & t_{-n+1} & t_{-n} \\ t_{-n} & t_n & \dots & t_1 & t_0 & \dots & t_{-n+2} & t_{-n+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{-2} & t_{-3} & \dots & t_{n-1} & t_{n-2} & \dots & t_0 & t_{-1} \\ t_{-1} & t_{-2} & \dots & t_n & t_{n-1} & \dots & t_1 & t_0 \end{pmatrix}$$

$$C_{(1)} = (t_0, t_{-1}, \dots, t_{-n}, t_n, \dots, t_2, t_1).$$

Paso 1

... $C_{(1)} = (t_0, t_{-1}, \ldots, t_{-n}, t_n, \ldots, t_2, t_1)$.

1.2 Calcular la DFT de $C_{(1)}$, $\mathcal{U} = DFT(C_{(1)})$.

1.3 Calcular $\mathcal{V}(i) = 1/\mathcal{U}(i)$, para cada $i = 0, \ldots, 2n$,

1.4 Calcular la primera fila de C^{-1} como $DFT^{-1}(\mathcal{V})$.

Sección 4 | Adaptación de algoritmo de Kumar

Adaptación de algoritmo de Kumar

Algoritmo de Kumar sobre cuerpos finitos

1. Tomar la primera fila y la primera columna de la matriz de Toeplitz y **generar la primera fila de** C:

$$C_{(1)} = \begin{pmatrix} t_0 & t_{-1} & \dots & t_{-n} & t_n & t_{n-1} & \dots & t_1 \end{pmatrix}.$$

2. **Calcular la NTT de** $C_{(1)}, \mathcal{U} = NTT(C_{(1)})$.
3. **Calcular** $\mathcal{V}(i) = 1/\mathcal{U}(i)$, para cada $i = 0, \dots, 2n$.
4. **Calcular la primera fila de** C^{-1}**,** $C^{-1}_{(1)} = NTT^{-1}(\mathcal{V})$.

Recordar

Necesitamos que $N \mid (p-1)$, esto es $p = \zeta N + 1$ para algún entero positivo ζ.

Qué pasa si no hay elementos del orden deseado?

(a) Insertar ceros entre la primera fila y la primera columna de T:

$$C_{(1)} = (t_0, \ldots, \; t_{-n}, \; t_n, \quad \underbrace{0 \; \ldots \; 0}_{\textbf{ceros adicionales}} \quad t_{n-1}, \ldots, \; t_1).$$

(b) Extender el cuerpo $\mathbb{F}_p$.

(c) Utilizar una combinación de (a) y (b).

Ejemplo (1/2)

Calcular la NTT de x en $\mathbb{F}_{11}$:

$$x = \boxed{1 \mid 2 \mid 3 \mid 5 \mid 9 \mid 6 \mid 4}$$

- $N = 7$, $p = 11$
- $N \nmid p - 1$, qué hacemos? Añadimos ceros. Cuántos?

$$C_{(1)} = \boxed{1 \mid 2 \mid 3 \mid 5 \mid 0 \mid 0 \mid 0 \mid 9 \mid 6 \mid 4}$$

- Calcular la NTT de x

Ejemplo (1/2)

Calcular la NTT de x en $\mathbb{F}_{11}$:

$$x = \boxed{1 \mid 2 \mid 3 \mid 5 \mid 9 \mid 6 \mid 4}$$

- $N = 7$, $p = 11$
- $N \nmid p - 1$, qué hacemos? Añadimos ceros. Cuántos?

$$C_{(1)} = \boxed{1 \mid 2 \mid 3 \mid 5 \mid 0 \mid 0 \mid 0 \mid 9 \mid 6 \mid 4}$$

- Calcular la NTT de x

Trabajando con cuerpos extendidos

Ejemplo (1/3)

Calcular la NTT de x en $\mathbb{F}_5$:

$$x = \begin{array}{|c|c|c|}\hline 3 & 2 & 1 \\ \hline\end{array}$$

- $N = 3$, $p = 5$
- $N \nmid p - 1$, qué hacemos?
- $N \mid p^2 - 1$
- $\mathbb{F}_{5^2} = \mathbb{F}_5[\alpha]$, $\alpha^2 + 4\alpha + 2 = 0 \mod 5$
- Calcular la NTT de x

Trabajando con cuerpos extendidos

Ejemplo (1/3)

Calcular la NTT de x en $\mathbb{F}_5$:

$$x = \boxed{3} \boxed{2} \boxed{1}$$

- $N = 3$, $p = 5$
- $N \nmid p - 1$, qué hacemos?
- $N \mid p^2 - 1$
- $\mathbb{F}_{5^2} = \mathbb{F}_5[\alpha]$, $\alpha^2 + 4\alpha + 2 = 0 \mod 5$
- Calcular la NTT de x

Ejemplo (2/3)

1. Calcular dos nuevas secuencias a, b de longitud $N-1=2$

$$a = \boxed{2 \mid 1} \quad b = \boxed{2\alpha+1 \mid 3\alpha+3}$$

2. Realizar la convolución circular $a \circledast b$:

$$b = \boxed{2\alpha+1 \mid 3\alpha+3} \quad \nearrow \; b_0 = \boxed{1 \mid 3} \qquad \searrow \; b_1 = \boxed{2 \mid 3}$$

$$\left.\begin{array}{lcl} a & = & \boxed{2 \mid 1 \mid 0 \mid 0} \\ b_0 & = & \boxed{1 \mid 3 \mid 0 \mid 0} \end{array}\right\} \xrightarrow{\circledast} \boxed{2 \mid 2 \mid 3 \mid 0}$$

$$\left.\begin{array}{lcl} a & = & \boxed{2 \mid 1 \mid 0 \mid 0} \\ b_1 & = & \boxed{2 \mid 3 \mid 0 \mid 0} \end{array}\right\} \xrightarrow{\circledast} \boxed{4 \mid 3 \mid 3 \mid 0}$$

$$cl = a * b = \boxed{4\alpha+2 \mid 3\alpha+2 \mid 3\alpha+3 \mid 0}$$

Ejemplo (3/3)

3. Transformar la convolución lineal en una circular.

cl=

$4\alpha + 2$	$3\alpha + 2$	$3\alpha + 3$	0

cc=

2α	$3\alpha + 2$

4. Generar los resultados:

$$X_0 = \sum_{k=0}^{N-1} x_k = 1 \pmod 5$$
$$X_1 = x_0 + cc_0 = 2\alpha + 3$$
$$X_2 = x_0 + cc_3 = 3 + 3\alpha + 2 = 3\alpha$$

X=NTT(x)=

1	$2\alpha + 3$	3α

Observación

Aunque el resultado de la NTT sea una lista de elementos del cuerpo extendido, al hacer la NTT^{-1} se obtienen otra vez elementos del cuerpo base.

Cuando añadir ceros y cuando extender?

- Sistema de Toeplitz de 10×10, $n = 9$
- Sistema definido en $\mathbb{F}_p$, $p = 839$
- $p - 1 = 2 \cdot 419$
- Longitud de $C_{(1)}$ es $2n + 1 = 19$
- Qué número k de ceros debemos añadir hasta que $2n + 1 + k \mid p - 1$?
- $k = 400$

Coste

Dado un vector con $n' = 2n + 1 + k$ elementos en $\mathbb{F}_p$, p primo

- Coste FTT en $\mathbb{F}_p$: $O(n' \log n')$.
- Rader en $\mathbb{F}_{p^d}$: hasta d^2 convoluciones en $\mathbb{F}_p$.
- $O(d^2 n' \log n')$.

Cuando añadir ceros y cuando extender?

- Sistema de Toeplitz de 10×10, $n = 9$
- Sistema definido en $\mathbb{F}_p$, $p = 839$
- $p - 1 = 2 \cdot 419$
- Longitud de $C_{(1)}$ es $2n + 1 = 19$
- Qué número k de ceros debemos añadir hasta que $2n + 1 + k \mid p - 1$?
- $k = 400$

Coste

Dado un vector con $n' = 2n + 1 + k$ elementos en $\mathbb{F}_p$, p primo

- Coste FTT en $\mathbb{F}_p$: $O(n' \log n')$.
- Rader en $\mathbb{F}_{p^d}$: hasta d^2 convoluciones en $\mathbb{F}_p$.
- $O(d^2 n' \log n')$.

Estrategia

Estrategia

1. Para cada $d \in \{1, 2, \ldots, d'\}$, hallar el menor entero k_d tal que $n'_d = 2n + 1 + k_d$ divide $p^d - 1$.
2. Estimar la magnitud del número de operaciones necesarias en cada extensión como

$$t_d = d^2 n'_d \log n'_d,$$

y elegir la opción que genera el valor t_d más reducido.

Sección 5 | Resultados experimentales

Resultados

- Dificultad en predecir el tiempo de ejecución.

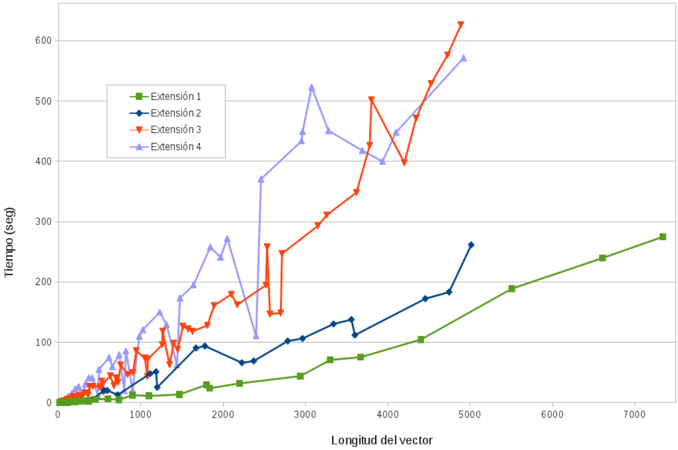


Figura : Tiempo de ejecución, $p = 660601$

Resultados

d	n'	Num. op.	T. (seg)
1	233	551.594	0.93936
2	24	**132.500**	**0.18647**
3	38	540.286	0.97135
4	24	530.001	0.61891

Cuadro : Sistema inicial de 9×9 con $p = 467$

- $p - 1 = 2 \cdot 233$
- $p^2 - 1 = 2^3 \cdot 3^2 \cdot 13 \cdot 233$
- $p^3 - 1 = 2 \cdot 19 \cdot 233 \cdot 11503$
- $p^4 - 1 = 2^4 \cdot 3^2 \cdot 5 \cdot 13 \cdot 113 \cdot 193 \cdot 233$

Resultados

d	n'	Num. op.	T. (seg)
1	641	1799.196	5.33719
2	107	868.576	0.99485
3	43	**632.152**	**0.94486**
4	40	1025.318	1.15282

Cuadro : Sistema inicial de 15×15 con $p = 1283$

- $p - 1 = 2 \cdot 641$
- $p^2 - 1 = 2^3 \cdot 3 \cdot 107 \cdot 641$
- $p^3 - 1 = 2 \cdot 7 \cdot 13 \cdot 43 \cdot 421 \cdot 641$
- $p^4 - 1 = 2^4 \cdot 3 \cdot 5 \cdot 97 \cdot 107 \cdot 641 \cdot 1697$

Resultados

d	n'	Num. op.	T. (seg)
1	7121	27433.944	401.64194
2	1187	14597.492	22.12164
3	73	1224.203	1.77473
4	26	**588.629**	**0.95086**

Cuadro : Sistema inicial de 12×12 con $p = 14243$

- $p - 1 = 2 \cdot 7121$
- $p^2 - 1 = 2^3 \cdot 3 \cdot 1187 \cdot 7121$
- $p^3 - 1 = 2 \cdot 73 \cdot 79 \cdot 127 \cdot 277 \cdot 7121$
- $p^4 - 1 = 2^4 \cdot 3 \cdot 5^2 \cdot 13 \cdot 461 \cdot 677 \cdot 1187 \cdot 7121$

Sección 6 | Conclusiones

Conclusiones

- El algoritmo de Kumar se puede adaptar para trabajar sobre cuerpos finitos.
- Se han expuesto tres opciones distintas para solucionar el problema de la divisibilidad de la longitud del vector y el orden del cuerpo.
- Se ha propuesto una heurística para determinar cuando añadir ceros o cuando considerar una extensión del cuerpo.

Resolución de sistemas de Toeplitz sobre cuerpos finitos

VIII Jornadas de Matemática Discreta y Algorítmica

N. Busom, J.M. Miret, F. Sebé

Departament de Matemàtica
Universitat de Lleida

Almería, 12 de Julio de 2012