Diviser pour régner: Transformée de Möbius .

Michaël Quisquater (Maître de Conférences, UVSQ)

Résultat classique d'interpolation.

Un résultat classique d'interpolation dit que pour n'importe quel ensemble de $n+1$ couples (x_i, y_i) (x_i distincts) dont les valeurs appartiennent à un corps commutatif il existe un unique polynôme à coefficients dans ce corps commutatif, de degré au maximum n et passant par ces points.

Appliqué à $\mathbb{F}_q$ ($q = p^k$ avec p premier), cela signifie qu'il existe un polynôme unique de degré maximum $q-1$ à coefficients dans $\mathbb{F}_q$ passant par les couples $(x, f(x))$ pour tout $x \in \mathbb{F}_q$ et pour une fonction f.
Ceci est évidemment généralisable aux polynômes multivariés.

L'ensemble des couples $(x, f(x))$ pour tout $x \in \mathbb{F}_q$ est appelée table de vérité de f.

Transformée de Möbius.

Considérons la fonction booléenne $f : \mathbb{F}_2^n \to \mathbb{F}_2 : x \mapsto f(x)$.

La théorie de l'interpolation nous dit qu'il existe des coefficients $a_u \in \mathbb{F}_2$ avec $u \in \mathbb{F}_2^n$ tel que :

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u \text{ . avec } x^u = \bigotimes_{i=1}^n x_i^{u_i} \text{ .}$$

Cette expression polynomiale est appelée *Forme algébrique normale (ANF)* de la fonction booléenne.

L'objet de la transformée de Möbius est le calcul rapide des coefficients a_u à partir de $f(x)$ pour $x \in \mathbb{F}_2^n$ et inversement.

Transformée de Möbius.

Considérons l'ensemble partiellement ordonné $(\mathbb{F}_2, \preceq)$:

$\preceq$	0	1
0	1	1
1	*	1

où 1 signifie que la relation est satisfaite et $*$ qu'elle ne l'est pas.

On peut étendre cet ordre partiel à $\mathbb{F}_2^n$ par :

$$(x_n, \cdots, x_1) \preceq (u_n, \cdots, u_1) \text{ ssi } x_i \preceq u_i \text{ pour tout } i = 1 \ldots n \text{ .}$$

Transformée de Möbius.

Soit $x \in \mathbb{F}_2^n$, nous avons que

$$x^u = \begin{cases} 1 & \text{si } u \preceq x; \\ 0 & \text{sinon.} \end{cases}$$

Par conséquent,

$$f(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u = \bigoplus_{u \preceq x} a_u .$$

Transformée de Möbius.
Principe d'interpolation
Transformée de Möbius
Transformée inverse

Transformée de Möbius (suite).

Notre but est à présent de montrer que la table de vérité peut se déduire de l'ANF via la formule :

$$f_n = \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \underline{a}_n ,$$

où $\bigotimes$ est le produit de Kronecker entre matrices.

A cette fin, nous allons montrer que pour tout $a_u \in \mathbb{F}_2$ avec $u \in \mathbb{F}_2^n$,

$$\left(\bigoplus_{u \preceq x} a_u \right)_{x \in \mathbb{F}_2^n} = \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \underline{a}_n .$$

Transformée de Möbius : cas de base (n=1)

Considérons

$$\left(\bigoplus_{u \preceq x} a_u\right)_{x \in \mathbb{F}_2}.$$

Il s'agit du vecteur

$$\begin{pmatrix} a_0 \\ a_0 \oplus a_1 \end{pmatrix}.$$

et nous avons bien :

$$\begin{pmatrix} a_0 \\ a_0 \oplus a_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}.$$

Transformée de Möbius : cas récurrent

Supposons que pour tous coefficients $a_u \in \mathbb{F}_2$ (avec $u \in \mathbb{F}_2^n$) la relation suivante est satisfaite :

$$\left(\bigoplus_{u \preceq x} a_u\right)_{x \in \mathbb{F}_2^n} = \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \underline{a}_n$$

où les coefficients a_u, représentés par le vecteur $\underline{a}_n$, sont énumérées suivant l'ordre naturel.

Considérons le vecteur

$$\left(\bigoplus_{(u_{n+1}, \underline{u}) \preceq (x_{n+1}, \underline{x})} a_{u_{n+1}, \underline{u}}\right)_{(x_{n+1}, \underline{x}) \in \mathbb{F}_2^{n+1}}$$

Transformée de Möbius : cas récurrent

Ce vecteur peut s'exprimer alternativement par

$$\begin{pmatrix} (\bigoplus_{\underline{u} \preceq \underline{x}} a_{0,\underline{u}})_{\underline{x} \in \mathbb{F}_2^n} \\ (\bigoplus_{\underline{u} \preceq \underline{x}} a_{0,\underline{u}} \oplus \bigoplus_{\underline{u} \preceq \underline{x}} a_{1,\underline{u}})_{\underline{x} \in \mathbb{F}_2^n} \end{pmatrix}$$

Par hypothèse de récurrence,

$$(\bigoplus_{\underline{u} \preceq \underline{x}} a_{0,\underline{u}})_{\underline{x} \in \mathbb{F}_2^n} = \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot a_{0,*} ,$$

et

$$(\bigoplus_{\underline{u} \preceq \underline{x}} a_{1,\underline{u}})_{\underline{x} \in \mathbb{F}_2^n} = \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot a_{1,*} .$$

Transformée de Möbius : cas récurrent

Par conséquent, le vecteur peut s'exprimer comme

$$\begin{pmatrix} \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot a_{0,*} \\ \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot a_{0,*} \oplus \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot a_{1,*} \end{pmatrix}$$

ou de façon équivalente

$$\begin{pmatrix} \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} & 0 \\ \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} & \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \end{pmatrix} \cdot \begin{pmatrix} a_{0,*} \\ a_{1,*} \end{pmatrix} = \bigotimes_{n+1} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \underline{a}_{n+1}$$

où $\underline{a}_{n+1} = \begin{pmatrix} a_{0,*} \\ a_{1,*} \end{pmatrix}$. Le pas récurrent est donc montré.

Transformée de Möbius

Nous avons donc montré que la table de vérité f_n d'une fonction booléenne $f : \mathbb{F}_2^n \to \mathbb{F}_2$ est liée aux coefficients a_u de sa forme algébrique normale par la relation

$$f_n = \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \underline{a}_n ,$$

où $\bigotimes$ est le produit de Kronecker entre matrices.

Ceci permet de construire un algorithme en $\mathcal{O}(n \cdot 2^n)$, ce qui est quasi-linéaire en la taille des données.

Transformée de Möbius : inverse

Comme nous venons de montrer que

$$f_n = \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \underline{a}_n ,$$

et en observant que

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} .$$

nous avons

$$\underline{a}_n = \bigotimes_n \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot f_n .$$

Il est donc possible de calculer rapidement les coefficients de la forme algébrique normale de f à partir de la table de vérité de f en $\mathcal{O}(n \cdot 2^n)$, ce qui est quasi-linéaire en la taille des données.