Une implémentation de la multiplication rapide des polynômes binaires

Joris van der Hoeven, Robin Larrieu and Grégoire Lecerf

CNRS & École polytechnique

JNCF 2018
24 Janvier, Luminy

Objectif

Multiplication dans $\mathbb{F}_2[X]$, grand degré ($\geqslant 10^6$).
Multiplication rapide par évaluation-interpolation (FFT).

Objectif

Multiplication dans $\mathbb{F}_2[X]$, grand degré ($\geqslant 10^6$).
Multiplication rapide par évaluation-interpolation (FFT).

Problème

Peu de points d'évaluation dans $\mathbb{F}_2 \Rightarrow$ travail dans une extension de corps.
Comment minimiser le surcoût?

Librairies de référence

1. Algorithme de Schönhage-Strassen (GF2X – Brent, Gaudry, Thomé, Zimmermann)

Librairies de référence

1. Algorithme de Schönhage-Strassen (GF2X – Brent, Gaudry, Thomé, Zimmermann)
2. FFT dans $\mathbb{F}_{2^{60}}$ (Harvey, van der Hoeven, Lecerf – 2016)

Librairies de référence

1. Algorithme de Schönhage-Strassen (GF2X – Brent, Gaudry, Thomé, Zimmermann)
2. FFT dans $\mathbb{F}_{2^{60}}$ (Harvey, van der Hoeven, Lecerf – 2016)
3. FFT additive dans $\mathbb{F}_{2^{128}}$ ou $\mathbb{F}_{2^{256}}$ (Chen, Cheng, Kuo, Li, Yang – 2017)

Nouvelle idée

Frobenius FFT (van der Hoeven, L. – 2017)

Une FFT dans $\mathbb{F}_{q^d}$ peut être calculée $\sim d$ fois plus vite si l'entrée est en fait dans $\mathbb{F}_q$. $\Rightarrow$ Surcoût *en théorie* nul.

Nouvelle idée

Frobenius FFT (van der Hoeven, L. – 2017)

Une FFT dans $\mathbb{F}_{q^d}$ peut être calculée $\sim d$ fois plus vite si l'entrée est en fait dans $\mathbb{F}_q$. $\Rightarrow$ Surcoût *en théorie* nul.

Nouvelle implémentation

Faire fonctionner le Frobenius FFT *en pratique* dans $\mathbb{F}_{2^{60}}$.
Accélération d'un facteur 2 par rapport aux librairies existantes.

Pourquoi $\mathbb{F}_{2^{60}}$?

Bonne arithmétique dans $\mathbb{F}_{2^{60}}$

- Taille légèrement $<$ mot machine
- $\mu(X) := \frac{X^{61}-1}{X-1}$ irréductible sur $\mathbb{F}_2$

FFT efficace

Racines d'unité d'ordre

$$2^{60} - 1 = 3^2 \times 5^2 \times 7 \times 11 \times 13 \times 31 \times 41 \times 61 \times 151 \times 1321$$

Pourquoi $\mathbb{F}_{2^{60}}$?

Bonne arithmétique dans $\mathbb{F}_{2^{60}}$

- Taille légèrement $<$ mot machine
- $\mu(X) := \frac{X^{61}-1}{X-1}$ irréductible sur $\mathbb{F}_2$

FFT efficace

Racines d'unité d'ordre

$$2^{60} - 1 = 3^2 \times 5^2 \times 7 \times 11 \times 13 \times 31 \times 41 \times 61 \times 151 \times 1321$$

Bonus

- 61 divise $2^{60} - 1$. (Fermat)
- 2 génère $(\mathbb{Z}/61\mathbb{Z})^\times$ ($\Leftrightarrow \mu(X)$ irréductible)

Table des matières

Extensions de corps

Version naïve $\mathbb{F}_2[X]_{<n} \hookrightarrow \mathbb{F}_{2^{60}}[X]_{<n}$

$$\begin{array}{l} A \in \mathbb{F}_2[X] \longrightarrow \tilde{A} \in \mathbb{F}_{2^{60}}[X] \\ B \in \mathbb{F}_2[X] \longrightarrow \tilde{B} \in \mathbb{F}_{2^{60}}[X] \end{array} \longrightarrow \tilde{AB} \in \mathbb{F}_{2^{60}}[X] \longrightarrow AB \in \mathbb{F}_2[X]$$

Extensions de corps

Version naïve $\mathbb{F}_2[X]_{<n} \hookrightarrow \mathbb{F}_{2^{60}}[X]_{<n}$

$$\begin{array}{l} A \in \mathbb{F}_2[X] \longrightarrow \tilde{A} \in \mathbb{F}_{2^{60}}[X] \\ B \in \mathbb{F}_2[X] \longrightarrow \tilde{B} \in \mathbb{F}_{2^{60}}[X] \end{array} \longrightarrow \tilde{AB} \in \mathbb{F}_{2^{60}}[X] \longrightarrow AB \in \mathbb{F}_2[X]$$

Segmentation de Kronecker $\mathbb{F}_2[X]_{<n} \hookrightarrow \mathbb{F}_2[X]_{<30}[Z]_{<n/30} \hookrightarrow \mathbb{F}_{2^{60}}[Z]_{<n/30}$

$$\begin{array}{l} A \in \mathbb{F}_2[X] \longrightarrow \tilde{A} \in \mathbb{F}_2[X]_{<30}[Z] \\ B \in \mathbb{F}_2[X] \longrightarrow \tilde{B} \in \mathbb{F}_2[X]_{<30}[Z] \end{array} \longrightarrow \tilde{AB} \in \mathbb{F}_2[X]_{<60}[Z] \xrightarrow{\boxed{Z = X^{30}}} AB \in \mathbb{F}_2[X]$$

Extensions de corps

Version naïve $\mathbb{F}_2[X]_{<n} \hookrightarrow \mathbb{F}_{2^{60}}[X]_{<n}$

$$\begin{array}{l} A \in \mathbb{F}_2[X] \longrightarrow \tilde{A} \in \mathbb{F}_{2^{60}}[X] \\ B \in \mathbb{F}_2[X] \longrightarrow \tilde{B} \in \mathbb{F}_{2^{60}}[X] \end{array} \longrightarrow \tilde{AB} \in \mathbb{F}_{2^{60}}[X] \longrightarrow AB \in \mathbb{F}_2[X]$$

Segmentation de Kronecker $\mathbb{F}_2[X]_{<n} \hookrightarrow \mathbb{F}_2[X]_{<30}[Z]_{<n/30} \hookrightarrow \mathbb{F}_{2^{60}}[Z]_{<n/30}$

$$\begin{array}{l} A \in \mathbb{F}_2[X] \longrightarrow \tilde{A} \in \mathbb{F}_2[X]_{<30}[Z] \\ B \in \mathbb{F}_2[X] \longrightarrow \tilde{B} \in \mathbb{F}_2[X]_{<30}[Z] \end{array} \longrightarrow \tilde{AB} \in \mathbb{F}_2[X]_{<60}[Z] \overset{\boxed{Z = X^{30}}}{\longrightarrow} AB \in \mathbb{F}_2[X]$$

Frobenius FFT

Soit ω racine d'unité, $\phi : x \to x^2$ agit sur $\{1, \omega, \omega^2, \omega^3, \dots\}$. La FFT naïve $A \to [A(1), A(\omega), A(\omega^2), \dots]$ est redondante:

$$A \in \mathbb{F}_2[X], x \in \mathbb{F}_{2^{60}} \Rightarrow A(x^2) = A(x)^2$$

Notre variante du Frobenius FFT

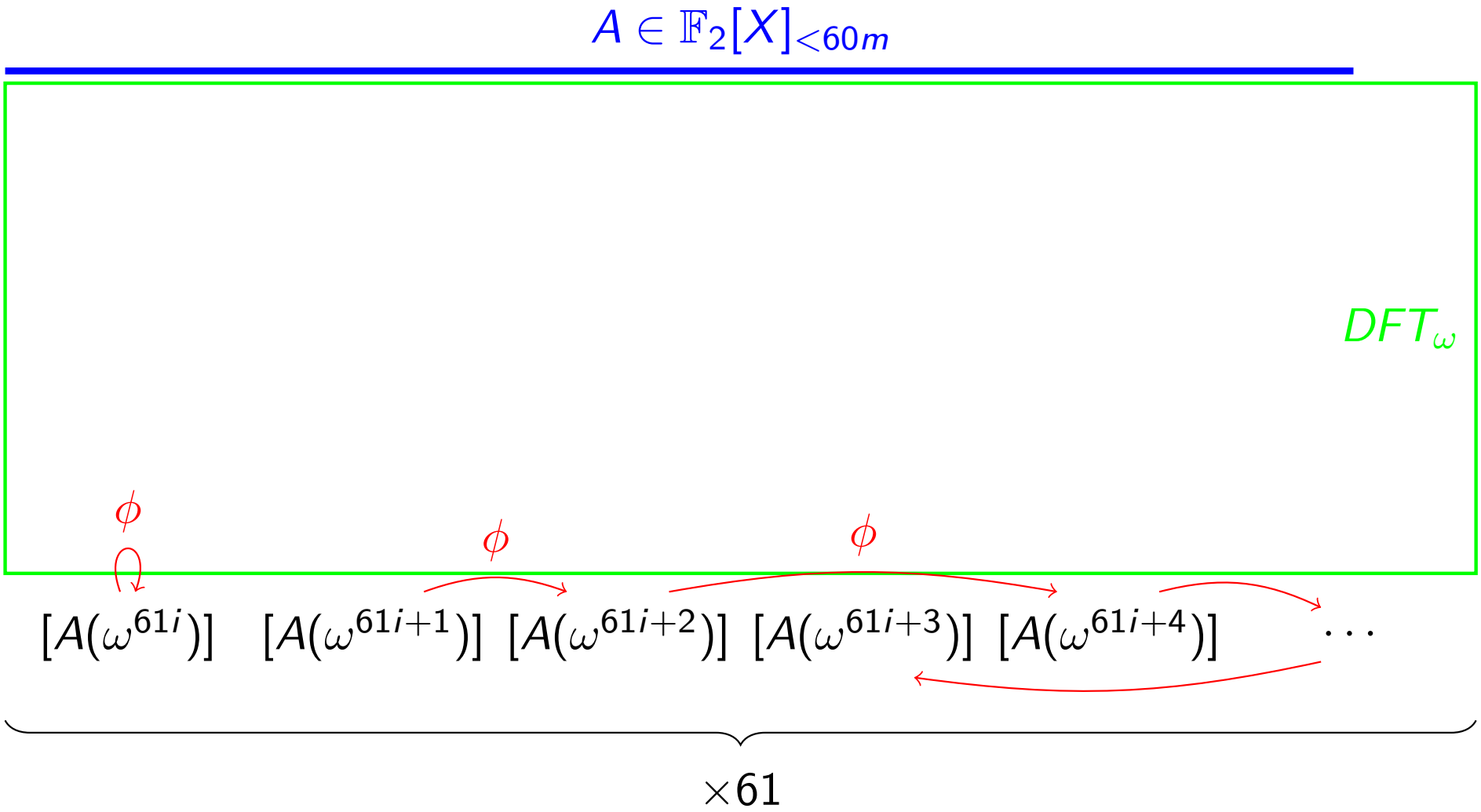
$$A \in \mathbb{F}_2[X]_{<60m}$$

DFT_ω

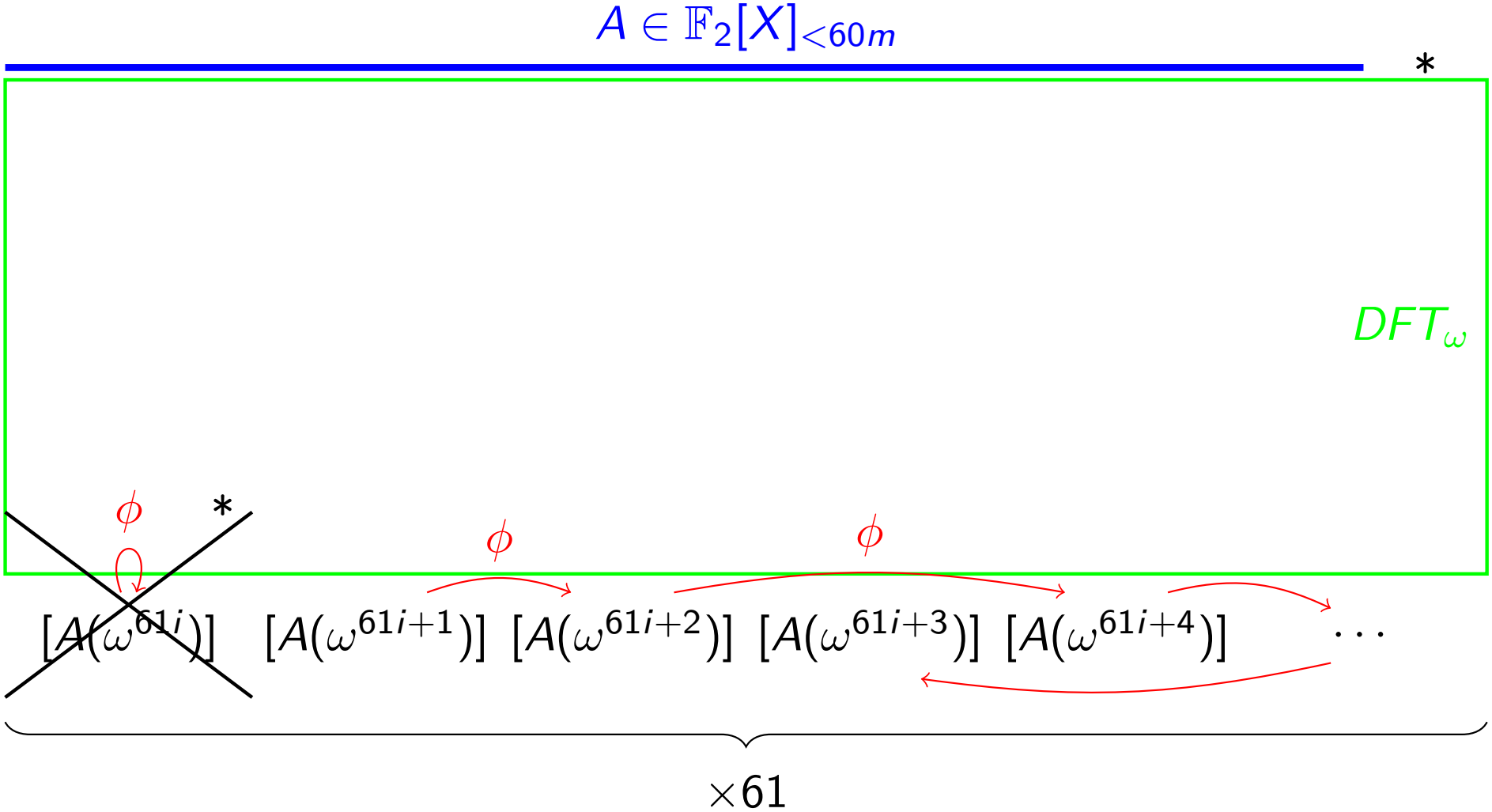
$$[A(\omega^{61i})] \quad [A(\omega^{61i+1})] \; [A(\omega^{61i+2})] \; [A(\omega^{61i+3})] \; [A(\omega^{61i+4})] \qquad \cdots$$

$\times 61$

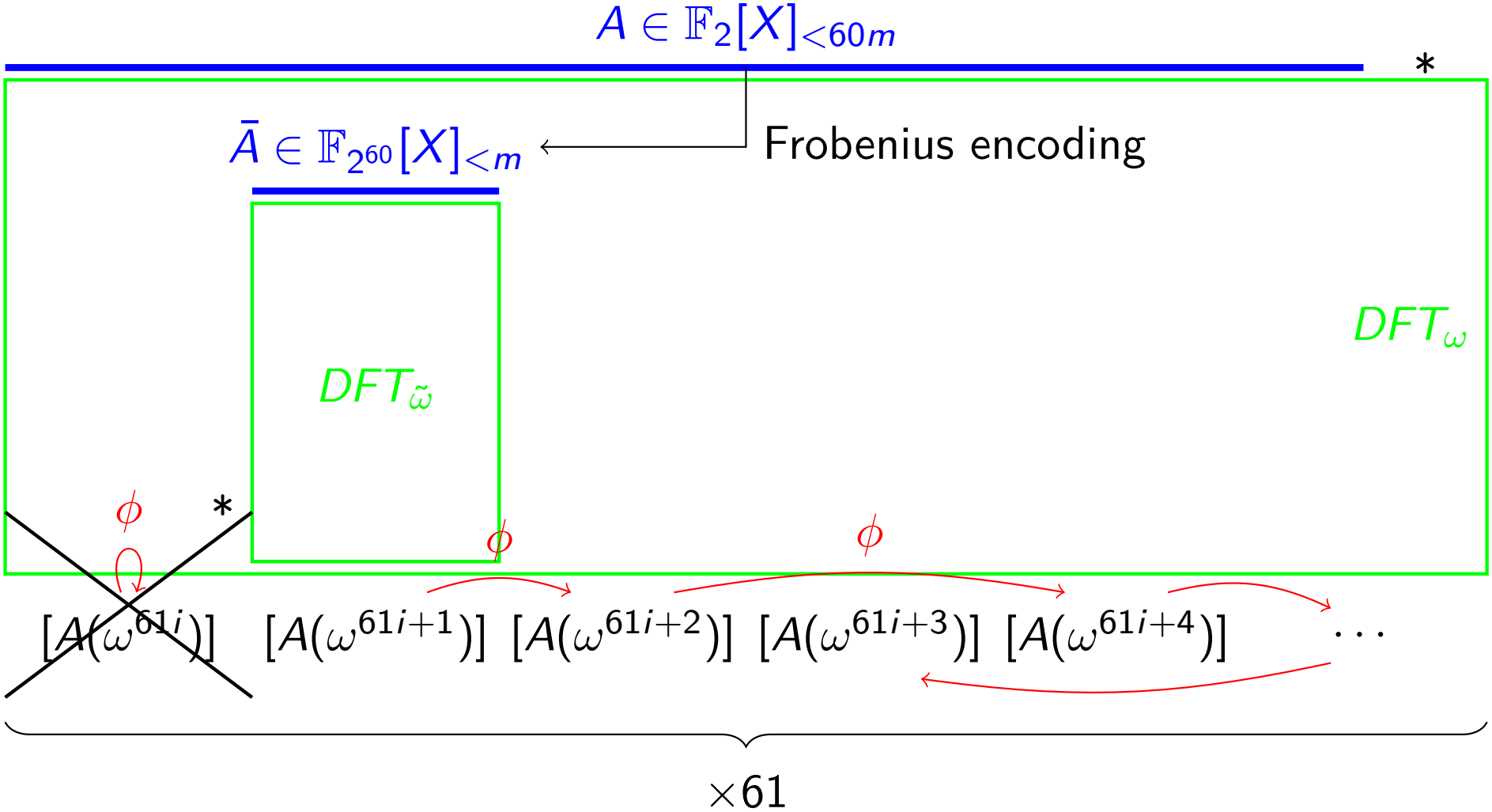
Notre variante du Frobenius FFT



Notre variante du Frobenius FFT



Notre variante du Frobenius FFT



Multiplication polynomiale

$$A \in \mathbb{F}_2[X]_{<a}$$
$$\downarrow \text{Frobenius Encoding}$$
$$\bar{A} \in \mathbb{F}_{2^{60}}[X]_{<a/60}$$
$$\downarrow DFT_{\tilde{\omega}}$$
$$E_\omega(A) \in \mathbb{F}_{2^{60}}^m$$

$a + b < 60m$
$61m$ divise $2^{60} - 1$

Multiplication polynomiale

$$A \in \mathbb{F}_2[X]_{<a} \qquad\qquad B \in \mathbb{F}_2[X]_{<b}$$
$$\downarrow \text{Frobenius Encoding} \qquad\qquad \text{Frobenius Encoding} \downarrow$$
$$\bar{A} \in \mathbb{F}_{2^{60}}[X]_{<a/60} \qquad\qquad \bar{B} \in \mathbb{F}_{2^{60}}[X]_{<b/60}$$
$$\downarrow DFT_{\tilde{\omega}} \qquad\qquad DFT_{\tilde{\omega}} \downarrow$$
$$E_\omega(A) \in \mathbb{F}_{2^{60}}^m \qquad\qquad E_\omega(B) \in \mathbb{F}_{2^{60}}^m$$

$a + b < 60m$
$61m$ divise $2^{60} - 1$

Multiplication polynomiale

$A \in \mathbb{F}_2[X]_{<a}$ $\qquad$ $B \in \mathbb{F}_2[X]_{<b}$

$\downarrow$ Frobenius Encoding $\qquad$ Frobenius Encoding $\downarrow$

$\bar{A} \in \mathbb{F}_{2^{60}}[X]_{<a/60}$ $\qquad$ $\bar{B} \in \mathbb{F}_{2^{60}}[X]_{<b/60}$

$\downarrow DFT_{\tilde{\omega}}$ $\qquad$ $DFT_{\tilde{\omega}} \downarrow$

$E_\omega(A) \in \mathbb{F}_{2^{60}}^m$ $\qquad$ $E_\omega(B) \in \mathbb{F}_{2^{60}}^m$

Produit 1 à 1

$E_\omega(AB) \in \mathbb{F}_{2^{60}}^m$

$\downarrow DFT_{\tilde{\omega}}^{-1}$

$\bar{AB} \in \mathbb{F}_{2^{60}}[X]_{<m}$

$\downarrow$ Frobenius Decoding

$AB \in \mathbb{F}_2[X]_{<a+b}$

$a + b < 60m$
$61m$ divise $2^{60} - 1$

Frobenius encoding

Cooley-Tukey FFT

$$A(\omega^{61i+1}) = \sum_{k<m} \omega^k \left(\sum_{l<61} a_{k+ml} \omega^{ml} \right) \omega^{61ki}$$

Frobenius encoding

Cooley-Tukey FFT

$$A(\omega^{61i+1}) = \sum_{k<m} \omega^k \left(\sum_{l<61} a_{k+ml} \omega^{ml} \right) \omega^{61ki}$$

- $\theta := \omega^m, \tilde{\omega} := \omega^{61}$
- $\tilde{A}_k := \sum_{l<61} a_{k+ml} X^l \in \mathbb{F}_2[X]_{<60} \quad (A \in \mathbb{F}_2[X]_{<60m})$
- $\bar{A} = \sum_{k<m} \omega^k \tilde{A}_k(\theta) Z^k \in \mathbb{F}_{2^{60}}[Z]_{<m}$

$$A(\omega^{61i+1}) = \bar{A}(\tilde{\omega})$$

Frobenius encoding

Cooley-Tukey FFT

$$A(\omega^{61i+1}) = \sum_{k<m} \omega^k \left(\sum_{l<61} a_{k+ml}\omega^{ml} \right) \omega^{61ki}$$

- $\theta := \omega^m, \tilde{\omega} := \omega^{61}$
- $\tilde{A}_k := \sum_{l<61} a_{k+ml} X^l \in \mathbb{F}_2[X]_{<60} \quad (A \in \mathbb{F}_2[X]_{<60m})$
- $\bar{A} = \sum_{k<m} \omega^k \tilde{A}_k(\theta) Z^k \in \mathbb{F}_{2^{60}}[Z]_{<m}$

$$A(\omega^{61i+1}) = \bar{A}(\tilde{\omega})$$

Hypothèse technique

On suppose ω choisi tel que $\theta = z \bmod \mu(z)$ avec $\mu(z) := \frac{z^{61}-1}{z-1}$

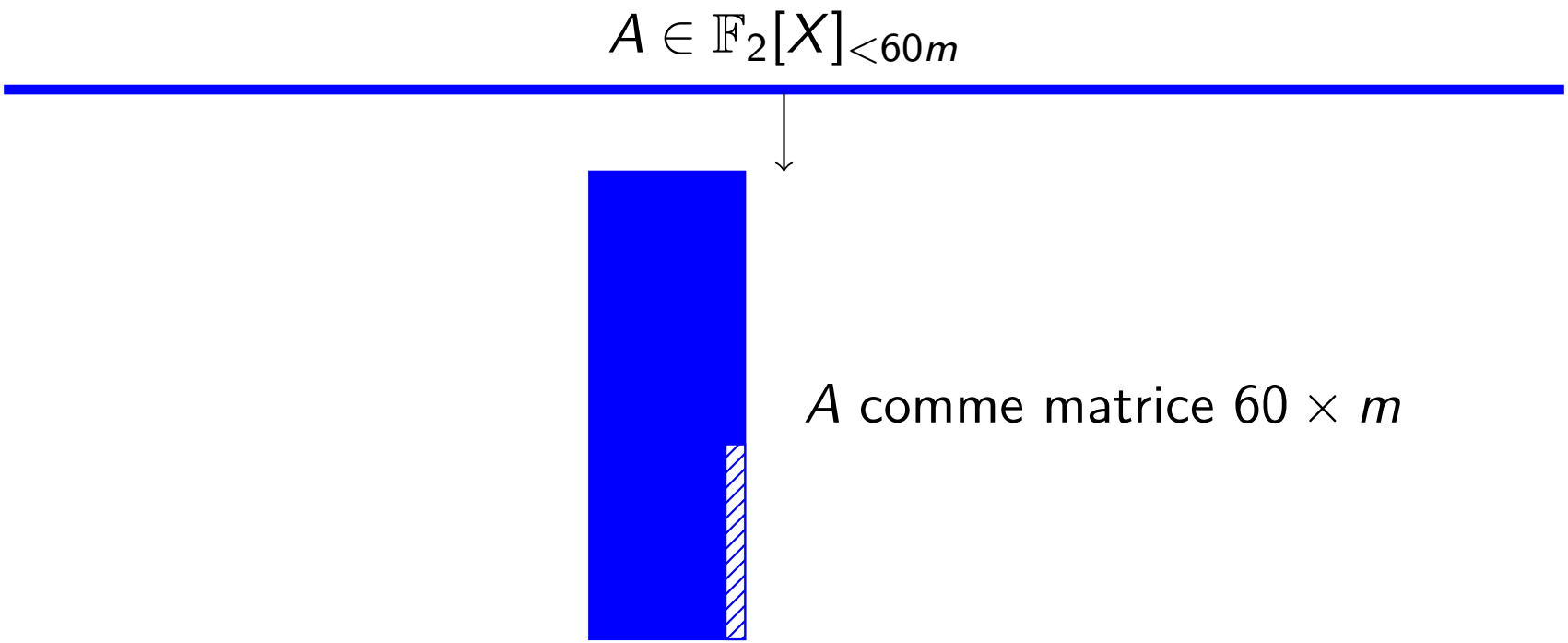
Table des matières

Représentation de données

- Polynômes sur $\mathbb{F}_2$ en représentation compacte.
- Éléments de $\mathbb{F}_{2^{60}}$ dans un mot machine ; polynômes sur $\mathbb{F}_{2^{60}}$ en un vecteur de mots.
- Matrices sur $\mathbb{F}_2$ en représentation compacte par colonnes.

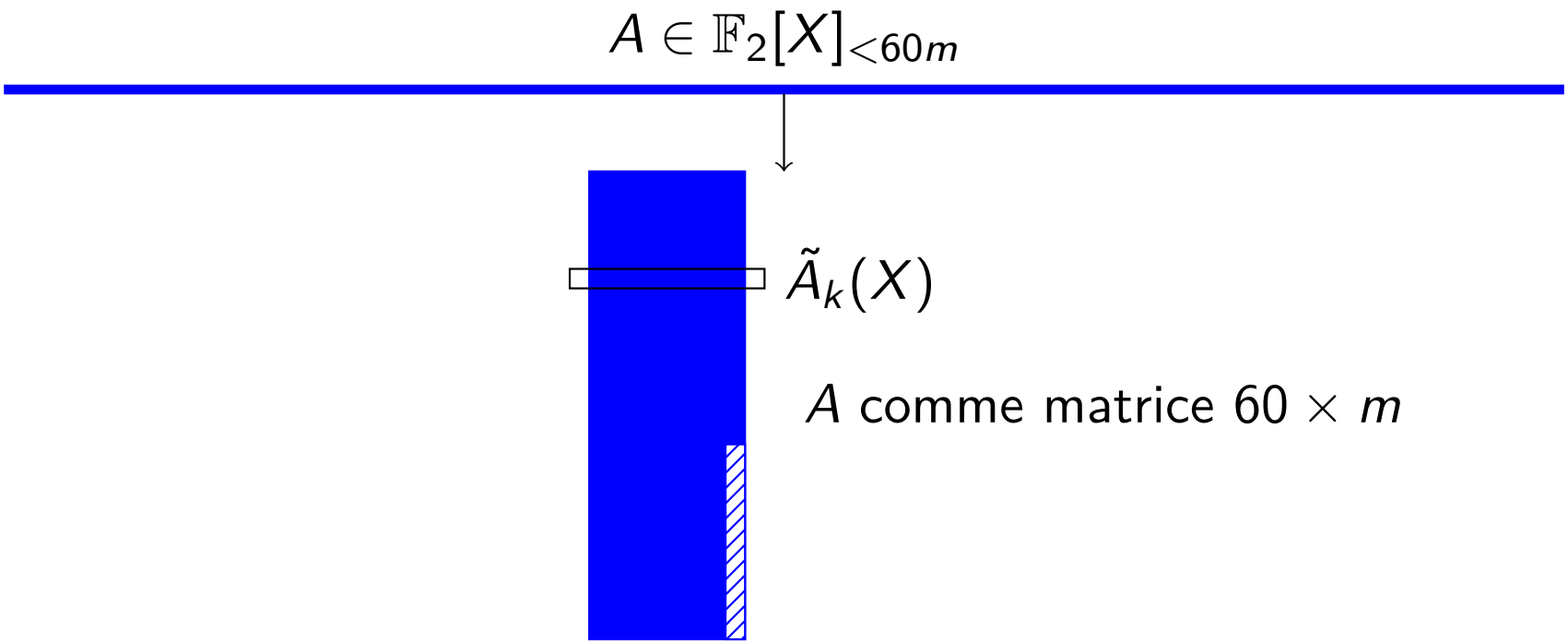
Représentation de données

- Polynômes sur $\mathbb{F}_2$ en représentation compacte.
- Éléments de $\mathbb{F}_{2^{60}}$ dans un mot machine ; polynômes sur $\mathbb{F}_{2^{60}}$ en un vecteur de mots.
- Matrices sur $\mathbb{F}_2$ en représentation compacte par colonnes.



Représentation de données

- Polynômes sur $\mathbb{F}_2$ en représentation compacte.
- Éléments de $\mathbb{F}_{2^{60}}$ dans un mot machine ; polynômes sur $\mathbb{F}_{2^{60}}$ en un vecteur de mots.
- Matrices sur $\mathbb{F}_2$ en représentation compacte par colonnes.



Frobenius encoding

Rappel

- $\tilde{A}_k := \sum_{l<61} a_{k+ml} X^l \in \mathbb{F}_2[X]_{<60} \quad (A \in \mathbb{F}_2[X]_{<60m})$
- $\bar{A} = \sum_{k<m} \omega^k \tilde{A}_k(\theta) Z^k \in \mathbb{F}_{2^{60}}[Z]_{<m}$
- $\theta = z \bmod \mu(z)$

Frobenius encoding

Rappel

- $\tilde{A}_k := \sum_{l<61} a_{k+ml} X^l \in \mathbb{F}_2[X]_{<60} \quad (A \in \mathbb{F}_2[X]_{<60m})$
- $\bar{A} = \sum_{k<m} \omega^k \tilde{A}_k(\theta) Z^k \in \mathbb{F}_{2^{60}}[Z]_{<m}$
- $\theta = z \bmod \mu(z)$

Phase d'encodage

- Voir A comme une matrice $60 \times m$ ($+$ 4 colonnes pour l'alignement).
- Transposer la matrice $64 \times m$ ($\Rightarrow [\tilde{A}_k(\theta)]_{k<m}$) .
- Multiplier par les twiddle factors ω^k($\Rightarrow \bar{A}$).

Frobenius encoding

Rappel

- $\tilde{A}_k := \sum_{l<61} a_{k+ml} X^l \in \mathbb{F}_2[X]_{<60} \quad (A \in \mathbb{F}_2[X]_{<60m})$
- $\bar{A} = \sum_{k<m} \omega^k \tilde{A}_k(\theta) Z^k \in \mathbb{F}_{2^{60}}[Z]_{<m}$
- $\theta = z \bmod \mu(z)$

Phase d'encodage

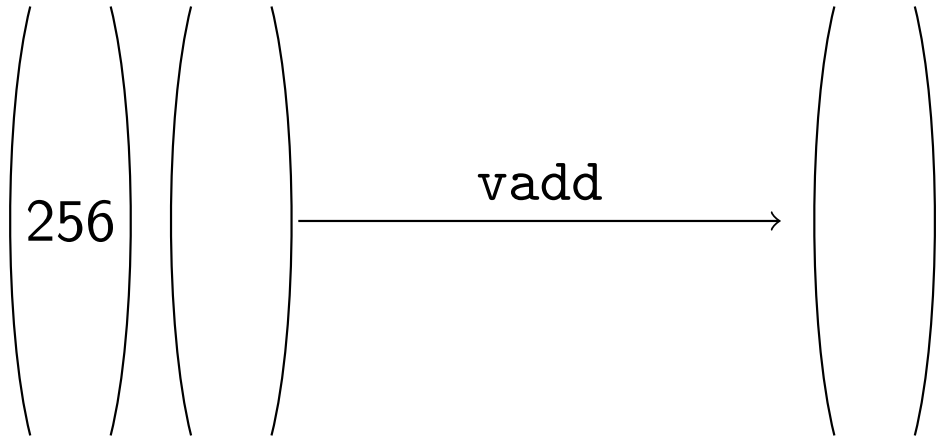
- Voir A comme une matrice $60 \times m$ ($+$ 4 colonnes pour l'alignement).
- Transposer la matrice $64 \times m$ ($\Rightarrow [\tilde{A}_k(\theta)]_{k<m}$) .
- Multiplier par les twiddle factors ω^k($\Rightarrow \bar{A}$).

Ensuite, appliquer la FFT sur $\bar{A}$.

Transposition de matrices

Instructions vectorielles (AVX2)

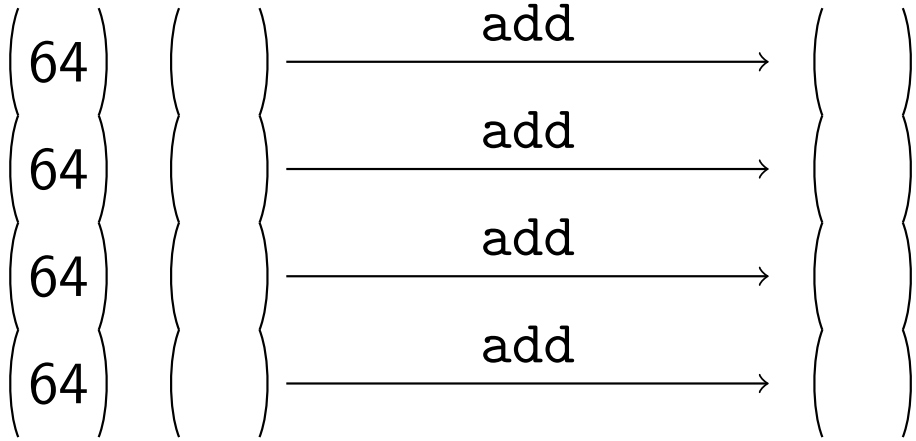
SIMD: Single Instruction Multiple Data



Transposition de matrices

Instructions vectorielles (AVX2)

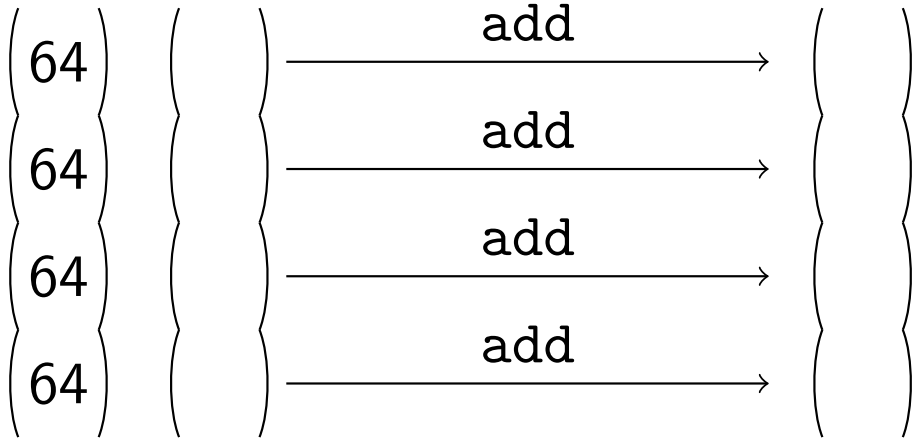
SIMD: Single Instruction Multiple Data



Transposition de matrices

Instructions vectorielles (AVX2)

SIMD: Single Instruction Multiple Data

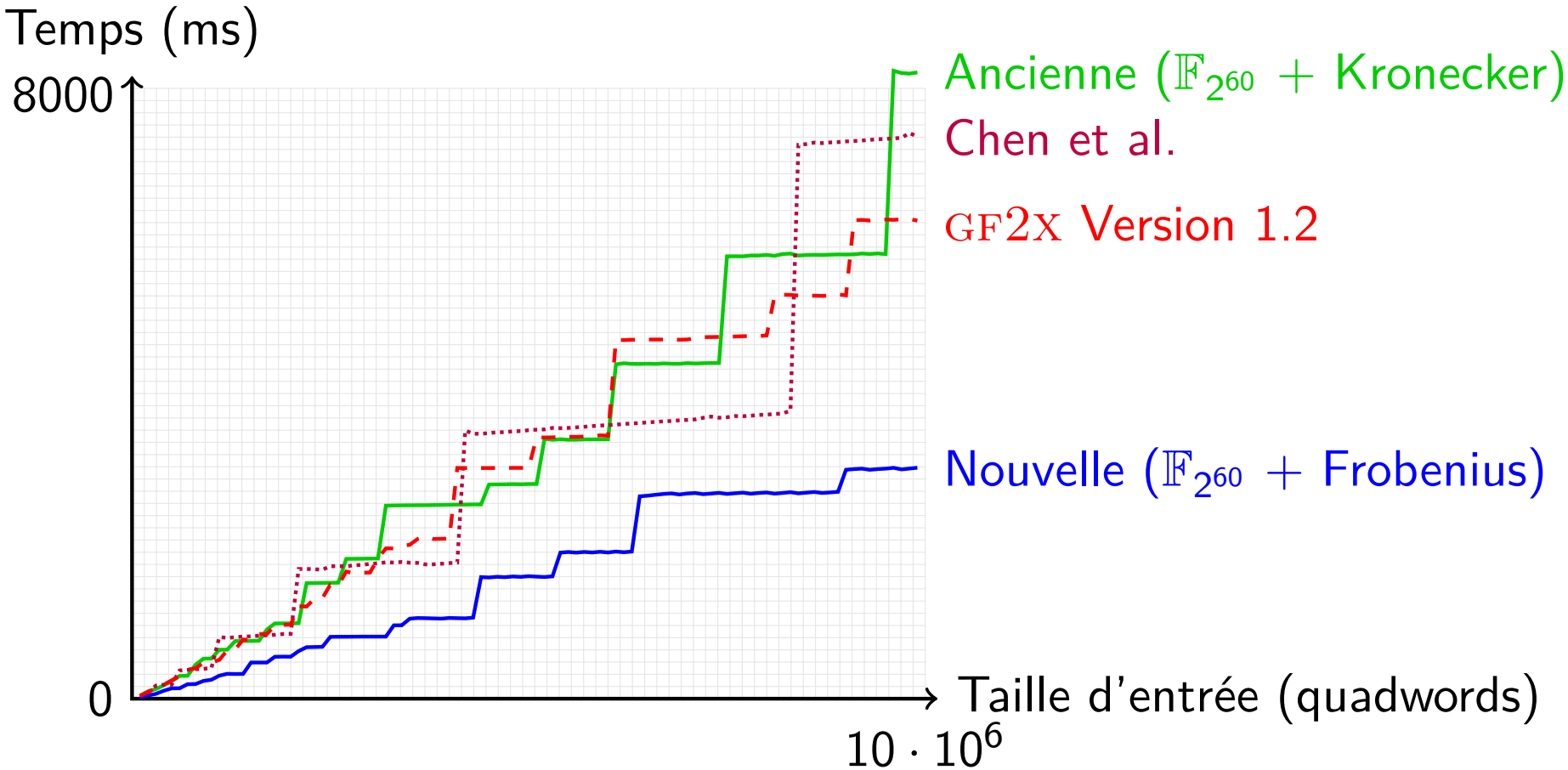


Méthode

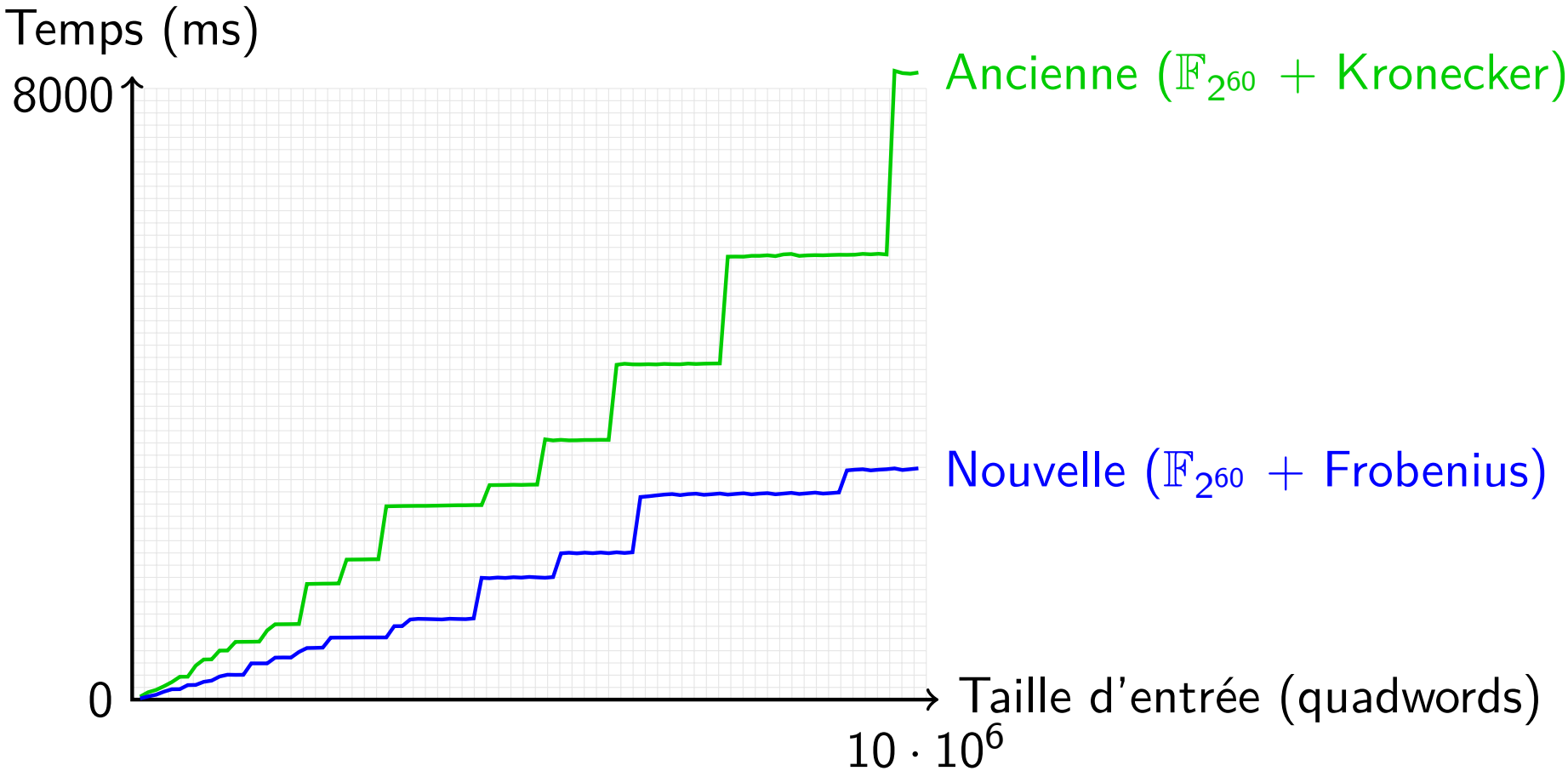
Exploiter les instructions AVX2

- Réduction $(64 \times m) \to (64 \times 256) \to (8 \times 8)$
- Transposer 4 matrices 8×8 (compactes 64 bits) à la fois.

Résultats


Temps (ms)
8000
0
Taille d'entrée (quadwords)
$10 \cdot 10^6$
Ancienne ($\mathbb{F}_{2^{60}}$ + Kronecker)
Chen et al.
GF2X Version 1.2
Nouvelle ($\mathbb{F}_{2^{60}}$ + Frobenius)

Résultats


Temps (ms)
8000
0
Taille d'entrée (quadwords)
$10 \cdot 10^6$
Ancienne ($\mathbb{F}_{2^{60}}$ + Kronecker)
Nouvelle ($\mathbb{F}_{2^{60}}$ + Frobenius)

Résumé

Nouveau record de multiplication sur $\mathbb{F}_2$. Facteur 2 par rapport aux autres implémentations.

Résumé

Nouveau record de multiplication sur $\mathbb{F}_2$. Facteur 2 par rapport aux autres implémentations.

Améliorations

- Optimiser les instructions vectorielles
  - Support pour AVX-512.
  - Vectoriser la routine de FFT sur $\mathbb{F}_{2^{60}}$.

Résumé

Nouveau record de multiplication sur $\mathbb{F}_2$. Facteur 2 par rapport aux autres implémentations.

Améliorations

- Optimiser les instructions vectorielles
  - Support pour AVX-512.
  - Vectoriser la routine de FFT sur $\mathbb{F}_{2^{60}}$.
- Autres
  - Transformée de Fourier Tronquée (réduire l'effet de saut)
  - Généralisation à d'autres corps finis

Résumé

Nouveau record de multiplication sur $\mathbb{F}_2$. Facteur 2 par rapport aux autres implémentations.

Améliorations

- Optimiser les instructions vectorielles
  - Support pour AVX-512.
  - Vectoriser la routine de FFT sur $\mathbb{F}_{2^{60}}$.
- Autres
  - Transformée de Fourier Tronquée (réduire l'effet de saut)
  - Généralisation à d'autres corps finis

Merci de votre attention