GFFT on the projective line

Ariel Gabizon
Aztec Labs

FFT Reminder

$$S = \left\{ g, g^2, \ldots, g^n = 1 \right\}, n = 2^k$$

FFT Reminder

$S = \{g, g^2, \ldots, g^n = 1\}, n = 2^k$

Want to evaluate $f(X) \in \mathbb{F}[X]$ of deg $< n$ on S.

FFT Reminder

$S = \{g, g^2, \ldots, g^n = 1\}, n = 2^k$

Want to evaluate $f(X) \in \mathbb{F}[X]$ of deg $< n$ on S.Use recursive formula

$$f(X) = f_e(X^2) + X \cdot f_o(X^2)$$

Since the map $x \to x^2$ is 2-to-1 on S, this reduces n evals of f to $n/2$ evals of two deg $n/2$ polys.

FFT Reminder

$S = \{g, g^2, \ldots, g^n = 1\}, n = 2^k$

Want to evaluate $f(X) \in \mathbb{F}[X]$ of deg $< n$ on S.Use recursive formula

$$f(X) = f_e(X^2) + X \cdot f_o(X^2)$$

Since the map $x \to x^2$ is 2-to-1 on S, this reduces n evals of f to $n/2$ evals of two deg $n/2$ polys.

Requires $n|p-1$, where $p = |\mathbb{F}|$.
Can we do something when $n|(p+1)$ instead??

GFFT idea: All you need is cyclic operation

$$S = \left\{ g, g^2, \ldots, g^n = 1 \right\}, n = 2^k$$

GFFT idea: All you need is cyclic operation

$S = \{g, g^2, \ldots, g^n = 1\}, n = 2^k$

The map $\sigma(x) = g \cdot x$ goes over S as a cycle.

GFFT idea: All you need is cyclic operation

$S = \{g, g^2, \ldots, g^n = 1\}, n = 2^k$
The map $\sigma(x) = g \cdot x$ goes over S as a cycle.

- Let $\tau = \sigma^{n/2}$. So $\tau(x) = -x$, and $\tau^2(x) = x$.

GFFT idea: All you need is cyclic operation

$S = \{g, g^2, \ldots, g^n = 1\}, n = 2^k$
The map $\sigma(x) = g \cdot x$ goes over S as a cycle.

- Let $\tau = \sigma^{n/2}$. So $\tau(x) = -x$, and $\tau^2(x) = x$.
- S splits into disjoint pairs $(a, \tau(a))$.

GFFT idea: All you need is cyclic operation

$S = \{g, g^2, \ldots, g^n = 1\}, n = 2^k$
The map $\sigma(x) = g \cdot x$ goes over S as a cycle.

- Let $\tau = \sigma^{n/2}$. So $\tau(x) = -x$, and $\tau^2(x) = x$.
- S splits into disjoint pairs $(a, \tau(a))$.
- Let $N(X) := X \cdot \tau(X)$.

GFFT idea: All you need is cyclic operation

$S = \{g, g^2, \ldots, g^n = 1\}, n = 2^k$
The map $\sigma(x) = g \cdot x$ goes over S as a cycle.

- Let $\tau = \sigma^{n/2}$. So $\tau(x) = -x$, and $\tau^2(x) = x$.
- S splits into disjoint pairs $(a, \tau(a))$.
- Let $N(X) := X \cdot \tau(X)$.
  2-1 on S: $N(a) = a \cdot \tau(a) = N(\tau(a))$.

GFFT idea: All you need is cyclic operation

$S = \{g, g^2, \ldots, g^n = 1\}, n = 2^k$
The map $\sigma(x) = g \cdot x$ goes over S as a cycle.

- Let $\tau = \sigma^{n/2}$. So $\tau(x) = -x$, and $\tau^2(x) = x$.
- S splits into disjoint pairs $(a, \tau(a))$.
- Let $N(X) := X \cdot \tau(X)$.
  2-1 on S: $N(a) = a \cdot \tau(a) = N(\tau(a))$.

  Can we find a set of size $p + 1$ with a cyclical σ?

The Projective line and fractional transformations

Look at *projective line* $\mathbb{P} := \mathbb{F} \cup \infty$

The Projective line and fractional transformations

Look at *projective line* $\mathbb{P} := \mathbb{F} \cup \infty$

Take fractional map: $\sigma(x) = \frac{1}{ax+b}$
Define: $\sigma(-b/a) = \infty, \sigma(\infty) = 0$.

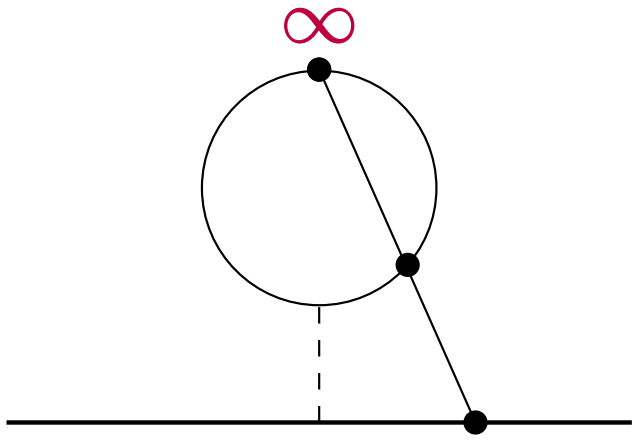
The Projective line and fractional transformations

Look at *projective line* $\mathbb{P} := \mathbb{F} \cup \infty$

Take fractional map: $\sigma(x) = \frac{1}{ax+b}$
Define: $\sigma(-b/a) = \infty, \sigma(\infty) = 0$.

claim: For the right choice of a, b, σ makes a cycle over all of $\mathbb{P}$.

Detour: The projective line as a circle in the plane



See Circle STARK paper [HLP24] for this approach

Let's try to proceed as before:
The map $\boldsymbol{\sigma(x) = \frac{1}{ax+b}}$ goes over $\mathbb{P}$ as a cycle.

Let's try to proceed as before:

The map $\sigma(x) = \frac{1}{ax+b}$ goes over $\mathbb{P}$ as a cycle.

- Let $\tau = \sigma^{n/2}$.
- $\mathbb{P}$ splits into disjoint pairs $(a, \tau(a))$.

Let's try to proceed as before:

The map $\sigma(x) = \frac{1}{ax+b}$ goes over $\mathbb{P}$ as a cycle.

- Let $\tau = \sigma^{n/2}$.
- $\mathbb{P}$ splits into disjoint pairs $(a, \tau(a))$.
- Let $N(X) := X \cdot \tau(X)$.

Let's try to proceed as before:

The map $\sigma(x) = \frac{1}{ax+b}$ goes over $\mathbb{P}$ as a cycle.

- Let $\tau = \sigma^{n/2}$.
- $\mathbb{P}$ splits into disjoint pairs $(a, \tau(a))$.
- Let $N(X) := X \cdot \tau(X)$.
  2-1 on $\mathbb{P}$: $N(a) = ?$

Let's try to proceed as before:
The map $\sigma(x) = \frac{1}{ax+b}$ goes over $\mathbb{P}$ as a cycle.

- Let $\tau = \sigma^{n/2}$.
- $\mathbb{P}$ splits into disjoint pairs $(a, \tau(a))$.
- Let $N(X) := X \cdot \tau(X)$.
  2-1 on $\mathbb{P}$: $N(a) = ?$

  $\mathbb{P}$ *is not a group, so* $N(a)$ *is not defined!*

The point α as a "place"

Let $K = \mathbb{F}(X)$.

The point α as a "place"

Let $K = \mathbb{F}(X)$.

Given $\alpha \in \mathbb{F}$, let $P_\alpha = \{r(X) \in K | r(\alpha) = 0\}$.

The point α as a "place"

Let $K = \mathbb{F}(X)$.

Given $\alpha \in \mathbb{F}$, let $P_\alpha = \{r(X) \in K | r(\alpha) = 0\}$.

P_α is called a *place* of K.

The point α as a "place"

Let $K = \mathbb{F}(X)$.

Given $\alpha \in \mathbb{F}$, let $P_\alpha = \{r(X) \in K | r(\alpha) = 0\}$.

P_α is called a *place* of K.

(P_α is the unique maximal ideal of the subring of elements r with $r(\alpha) \neq \infty$.)

Evaluating at α with P_α

Fix poly $f = \sum_{i=0}^{n} b_i X^i$.

Evaluating at a with P_a

Fix poly $f = \sum_{i=0}^{n} b_i X^i$.
Write $f(X) = c + \sum_{i=1}^{n} c_i (X - a)^i$.

Evaluating at a with P_a

Fix poly $f = \sum_{i=0}^{n} b_i X^i$.
Write $f(X) = c + \sum_{i=1}^{n} c_i (X - a)^i$.

Let $g := \sum_{i=1}^{n} c_i (X - a)^i$.

Evaluating at a with P_a

Fix poly $f = \sum_{i=0}^{n} b_i X^i$.
Write $f(X) = c + \sum_{i=1}^{n} c_i (X - a)^i$.

Let $g := \sum_{i=1}^{n} c_i (X - a)^i$.

So $f(a) = c$ and $g(X) \in P_a$.

Evaluating at a with P_a

Fix poly $f = \sum_{i=0}^{n} b_i X^i$.
Write $f(X) = c + \sum_{i=1}^{n} c_i (X - a)^i$.

Let $g := \sum_{i=1}^{n} c_i (X - a)^i$.

So $f(a) = c$ and $g(X) \in P_a$.

I.e. - taking f mod P_a gives $f(a)$.

The infinity point in the algebraic representation

There is *one more* place of degree one in $\mathbf{K}$:
$\mathbf{P_\infty = \{f(X)/g(X) | deg(f) < deg(g)\}}$.

The infinity point in the algebraic representation

There is *one more* place of degree one in $\mathbf{K}$:
$\mathbf{P_\infty = \{f(X)/g(X) | deg(f) < deg(g)\}}$.

$\mathbf{P_\infty}$ = "the set of functions that are zero at infinity"

To exemplify ideas focus from now on map $\boldsymbol{\tau}(\boldsymbol{x}) = -\boldsymbol{x}$ *from regular FFT.*

Defining τ on places:

Defining τ on places:

1. Define τ as operation on K:
   $\tau(r(X)) := r(-X)$.

Defining $\boldsymbol{\tau}$ on places:

1. Define $\boldsymbol{\tau}$ as operation on $\mathbf{K}$:
   $\boldsymbol{\tau}(\mathbf{r}(\mathbf{X})) := \mathbf{r}(-\mathbf{X})$.
2. Define $\boldsymbol{\tau}$ on place $\mathbf{P_a}$ element-wise:
   $\boldsymbol{\tau}(\mathbf{P_a}) := \{\boldsymbol{\tau}(\mathbf{r})\}_{\mathbf{r}\in\mathbf{P_a}}$

Defining $\boldsymbol{\tau}$ on places:

1. Define $\boldsymbol{\tau}$ as operation on $\mathbf{K}$:
   $\boldsymbol{\tau}(\mathbf{r}(\mathbf{X})) := \mathbf{r}(-\mathbf{X})$.
2. Define $\boldsymbol{\tau}$ on place $\mathbf{P}_{\mathbf{a}}$ element-wise:
   $\boldsymbol{\tau}(\mathbf{P}_{\mathbf{a}}) := \{\boldsymbol{\tau}(\mathbf{r})\}_{\mathbf{r}\in\mathbf{P}_{\mathbf{a}}}$
   $= \{\mathbf{r}(-\mathbf{X}) | \mathbf{r}(\mathbf{a}) = \mathbf{0}\} = \mathbf{P}_{-\mathbf{a}}$

Galois subfields

Look at the *subfield* of $\mathbf{K}$ fixed by $\boldsymbol{\tau}$ - $\{\mathbf{r} \in \mathbf{K} | \boldsymbol{\tau}(\mathbf{r}) = \mathbf{r}\}$.

Galois subfields

Look at the *subfield* of $\mathbf{K}$ fixed by $\boldsymbol{\tau}$ -
$\{\mathbf{r} \in \mathbf{K} | \boldsymbol{\tau}(\mathbf{r}) = \mathbf{r}\}$.

This is exactly $\mathbb{F}(\mathbf{X^2})$.
e.g. $\boldsymbol{\tau}(\mathbf{X^2}) = (-\mathbf{X})^{\mathbf{2}} = \mathbf{X^2}$.

Places "splitting" in extensions:

Let $\mathbf{b} = \mathbf{a^2}$. Look at place $\mathbf{P'_b}$ of $\mathbb{F}(\mathbf{X^2})$.

Places "splitting" in extensions:

Let $\mathbf{b} = \mathbf{a}^2$. Look at place $\mathbf{P}'_{\mathbf{b}}$ of $\mathbb{F}(\mathbf{X}^2)$.
$\mathbf{P}'_{\mathbf{b}} = \{\mathbf{r}(\mathbf{X}^2) | \mathbf{r}(\mathbf{b}) = \mathbf{0}\}$.

Places "splitting" in extensions:

Let $b = a^2$. Look at place P'_b of $\mathbb{F}(X^2)$.
$P'_b = \{r(X^2) | r(b) = 0\}$.

Poly $f \in P'_b$ looks like:
$f = \sum_{i=1}^{n} c_i (X^2 - b)^i$

Places "splitting" in extensions:

Let $b = a^2$. Look at place P'_b of $\mathbb{F}(X^2)$.
$P'_b = \{r(X^2) | r(b) = 0\}$.

Poly $f \in P'_b$ looks like:
$f = \sum_{i=1}^{n} c_i (X^2 - b)^i$
$= \sum_{i=1}^{n} c_i (X + a)^i (X - a)^i$.

Places "splitting" in extensions:

Let $b = a^2$. Look at place P'_b of $\mathbb{F}(X^2)$.
$P'_b = \{r(X^2) | r(b) = 0\}$.

Poly $f \in P'_b$ looks like:
$f = \sum_{i=1}^{n} c_i (X^2 - b)^i$
$= \sum_{i=1}^{n} c_i (X + a)^i (X - a)^i$.

So $P'_b \subset P_a$ and $P'_b \subset P_{-a}$.

Places "splitting" in extensions:

Let $b = a^2$. Look at place P'_b of $\mathbb{F}(X^2)$.
$P'_b = \{r(X^2) | r(b) = 0\}$.

Poly $f \in P'_b$ looks like:
$f = \sum_{i=1}^{n} c_i (X^2 - b)^i$
$= \sum_{i=1}^{n} c_i (X + a)^i (X - a)^i$.

So $P'_b \subset P_a$ and $P'_b \subset P_{-a}$.

We say P'_b *splits* in K into P_a and P_{-a}.

Tying it together

Let's try to define $\mathbf{N}$ *again:*

$\mathbb{P} := \{\mathbf{P}_{\mathbf{a}}\}_{\mathbf{a} \in \mathbb{F}} \cup \mathbf{P}_{\infty}$.

Tying it together

Let's try to define $\mathbf{N}$ *again:*

$\mathbb{P} := \{\mathbf{P_a}\}_{\mathbf{a}\in\mathbb{F}} \cup \mathbf{P}_\infty$.

The map $\boldsymbol{\sigma(x) = \frac{1}{ax+b}}$ goes over $\mathbb{P}$ as a cycle.

- Let $\boldsymbol{\tau = \sigma^{n/2}}$.
- $\mathbb{P}$ splits into disjoint pairs $\boldsymbol{(\mathbf{P}, \tau(\mathbf{P}))}$.

Tying it together

Let's try to define $\mathbf{N}$ *again:*

$\mathbb{P} := \{\mathbf{P_a}\}_{\mathbf{a}\in\mathbb{F}} \cup \mathbf{P}_\infty$.

The map $\boldsymbol{\sigma(x) = \frac{1}{ax+b}}$ goes over $\mathbb{P}$ as a cycle.

- Let $\boldsymbol{\tau = \sigma^{n/2}}$.
- $\mathbb{P}$ splits into disjoint pairs $\boldsymbol{(\mathbf{P}, \tau(\mathbf{P}))}$.
- Let $\mathbf{K'}$ be the subfield of $\mathbf{K}$ fixed by $\boldsymbol{\tau}$. Define $\mathbf{N(P)}$ to be the place of $\mathbf{K'}$ splitting in $\mathbf{K}$ into $\mathbf{P}, \boldsymbol{\tau}(\mathbf{P})$.

For more details see:

FAST FOURIER TRANSFORM VIA AUTOMORPHISM GROUPS OF RATIONAL FUNCTION FIELDS

SONGSONG LI AND CHAOPING XING

Abstract. The Fast Fourier Transform (FFT) over a finite field $\mathbb{F}_q$ computes evaluations of a given polynomial of degree less than n at a specifically chosen set of n distinct evaluation points in $\mathbb{F}_q$. If q or $q-1$ is a smooth number, then the divide-and-conquer approach leads to the fastest known FFT algorithms. Depending on the type of group that the set of evaluation points forms, these algorithms are classified as multiplicative (Math of Comp. 1965) and additive (FOCS 2014) FFT algorithms. In this work, we provide a unified framework for FFT algorithms that include both multiplicative and additive FFT algorithms as special cases, and beyond: our framework also works when $q+1$ is smooth, while all known results require q or $q-1$ to be smooth. For the new case where $q+1$ is smooth (this new case was not considered before in literature as far as we know), we show that if n is a divisor of $q+1$ that is B-smooth for a real $B > 0$, then our FFT needs $O(Bn \log n)$ arithmetic operations in $\mathbb{F}_q$. Our unified framework is a natural consequence of introducing the algebraic function fields into the study of FFT.

1. Introduction

For more elementary approach with better final constants see Circle STARK[HLP24]