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

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

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??

Reflection - why does FFT work?

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

Reflection - why does FFT work?

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

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

Reflection - why does FFT work?

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

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

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

Reflection - why does FFT work?

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

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

- Let $\tau = \sigma^{n/2}$. So $\tau(x) = -x$, and $\tau^2(x) = x$.
- The elements of S split into disjoint pairs $(a, -a)$.
- Define $N(X) = X \cdot \tau(X) = -X^2$. N maps elements of a pair to the same output.

Reflection - why does FFT work?

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

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

- Let $\tau = \sigma^{n/2}$. So $\tau(x) = -x$, and $\tau^2(x) = x$.
- The elements of S split into disjoint pairs $(a, -a)$.
- Define $N(X) = X \cdot \tau(X) = -X^2$. N maps elements of a pair to the same output.

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

The Projective line and fractional transformations

How to get set $\mathbb{P}$ of size $\mathbf{2^k}$? Look at *projective line* $\mathbb{P} := \mathbb{F} \cup \infty$

The Projective line and fractional transformations

How to get set $\mathbb{P}$ of size 2^k? 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

How to get set $\mathbb{P}$ of size $\mathbf{2^k}$? Look at *projective line* $\mathbb{P} := \mathbb{F} \cup \infty$

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

claim: For the right choice of $\mathbf{a}, \mathbf{b}$ $\boldsymbol{\sigma}$ makes a cycle over all of $\mathbb{P}$!

How do people formally represent the projective line?

Projective coordinates: Represent $a \in F$ by (c, d) with $a = c/d$ e.g. $(a, 1)$.

So $\infty = (1, 0)$.

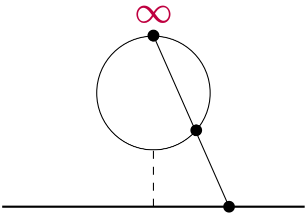
How do people formally represent the projective line?

Projective coordinates: Represent $a \in \mathbf{F}$ by (c, d) with $a = c/d$ e.g. $(a, 1)$.

So $\infty = (1, 0)$.

How do people formally represent the projective line?

As a circle in the plane:



See Circle STARK paper [HLP24] for this approach

How do people formally represent the projective line?

As places of the field $\mathbf{K} = \mathbb{F}(\mathbf{X})$:

How do people formally represent the projective line?

As places of the field $\mathbf{K} = \mathbb{F}(\mathbf{X})$:

Dfn: A *valuation ring* of $\mathbf{R} \subset \mathbb{F}(\mathbf{X})$ is a subring such that $\forall \mathbf{y} \in \mathbf{K}\ \mathbf{y} \in \mathbf{R}$ or $\mathbf{1}/\mathbf{y} \in \mathbf{R}$ (or both).

How do people formally represent the projective line?

As places of the field $K = \mathbb{F}(X)$:

Dfn: A *valuation ring* of $R \subset \mathbb{F}(X)$ is a subring such that $\forall y \in K \; y \in R$ or $1/y \in R$ (or both).

Example: Choose $a \in F$, take $R_a = \{f(X)/g(X) | f, g \in \mathbb{F}[X], g(a) \neq 0\}$.

How do people formally represent the projective line?

As places of the field $K = \mathbb{F}(X)$:

Dfn: A *valuation ring* of $R \subset \mathbb{F}(X)$ is a subring such that $\forall y \in K\ y \in R$ or $1/y \in R$ (or both).

Example: Choose $a \in F$, take
$R_a = \{f(X)/g(X) | f, g \in \mathbb{F}[X], g(a) \neq 0\}$.

Valuation rings in K, are also called "places" of K.

The infinity point in the algebraic representation

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

The infinity point in the algebraic representation

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

$\mathbf{R}_\infty =$ "the set of functions that can be evaluated at infinity"

Regular FFT via GFFT

1. Applying the map $\tau(x) = -x$.
2. Applying 2-1 map $x \to x^2$.

Regular FFT via GFFT

1. Applying the map $\tau(x) = -x$.
2. Applying 2-1 map $x \to x^2$.

How do these operations look in the framework of places?

Applying $\boldsymbol{\tau}$

1. Define $\boldsymbol{\tau}$ as operation on $\mathbf{K}$:
   $\boldsymbol{\tau}(\mathbf{r}(\mathbf{X})) := \mathbf{r}(-\mathbf{X})$.

Applying τ

1. Define τ as operation on K:
   $\tau(r(X)) := r(-X)$.
2. Apply τ on place R_a element-wise:
   $\tau(R_a) := \{\tau(r)\}_{r \in R_a}$
   $= \left\{ \frac{f(-X)}{g(-X)} | g(a) \neq 0 \right\} = R_{-a}$

Galois subfields

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

Galois subfields

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

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

Places splitting in extensions

Let $\mathbf{b} = \alpha^2$. Look at place $\mathbf{R}'_{\mathbf{b}}$ of $\mathbb{F}(\mathbf{X}^2)$.

Places splitting in extensions

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

For $r \in R'_b$

$r = f(X^2)/g(X^2)$ with $g(b) \neq 0$.
So $r(X) = f'(X)/g'(X)$ with $g'(a), g'(-a) \neq 0$.

Places splitting in extensions

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

For $r \in R'_b$

$r = f(X^2)/g(X^2)$ with $g(b) \neq 0$.
So $r(X) = f'(X)/g'(X)$ with $g'(a), g'(-a) \neq 0$.

Implies $R'_b \subset R_a$ and $R'_b \subset R_{-a}$.

Places splitting in extensions

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

For $\mathbf{r} \in \mathbf{R}'_{\mathbf{b}}$

$\mathbf{r} = \mathbf{f}(\mathbf{X}^2)/\mathbf{g}(\mathbf{X}^2)$ with $\mathbf{g}(\mathbf{b}) \neq \mathbf{0}$.
So $\mathbf{r}(\mathbf{X}) = \mathbf{f}'(\mathbf{X})/\mathbf{g}'(\mathbf{X})$ with $\mathbf{g}'(\mathbf{a}), \mathbf{g}'(-\mathbf{a}) \neq \mathbf{0}$.

Implies $\mathbf{R}'_{\mathbf{b}} \subset \mathbf{R}_{\mathbf{a}}$ and $\mathbf{R}'_{\mathbf{b}} \subset \mathbf{R}_{-\mathbf{a}}$.

We say $\mathbf{R}'_{\mathbf{b}}$ *splits* in $\mathbf{K}$ into $\mathbf{R}_{\mathbf{a}}$ and $\mathbf{R}_{-\mathbf{a}}$.

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