GFFT on projective line

Ariel Gabizon
Zeta Function Technologies

FFT Reminder

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

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??

Reflection - why does FFT work?

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

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

claim: For the right choice of $\mathbf{a, b}$ $\boldsymbol{\sigma}$ 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 $\infty = (1, 0)$.

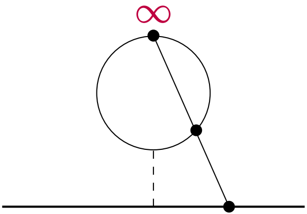
How do people formally represent the projective line?

Projective coordinates: Represent $a \in F$ 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 $\alpha \in F$, take $R_\alpha = \{f(X)/g(X) | f, g \in \mathbb{F}[X], g(\alpha) \neq 0\}$.

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 $\alpha \in F$, take $R_\alpha = \{f(X)/g(X) | f, g \in \mathbb{F}[X], g(\alpha) \neq 0\}$.

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

The unique maximal ideal of $\mathbf{R}_a$ is
$\mathbf{I}_a = \{(\mathbf{X} - \mathbf{a}) \cdot \mathbf{r} | \mathbf{r} \in \mathbf{R}\}$

The unique maximal ideal of $\mathbf{R}_\alpha$ is
$\mathbf{I}_\alpha = \{(\mathbf{X} - \alpha) \cdot \mathbf{r} | \mathbf{r} \in \mathbf{R}\}$

Cool thing: $\mathbf{R}_\alpha / \mathbf{I}_\alpha = \mathbb{F}$*. And we can evaluate*
$\mathbf{r} \in \mathbf{R}_\alpha$ *at* α *by taking* $\mathbf{r} \mod \mathbf{I}_\alpha$

The unique maximal ideal of $\mathbf{R}_\alpha$ is
$\mathbf{I}_\alpha = \{(\mathbf{X} - \alpha) \cdot \mathbf{r} | \mathbf{r} \in \mathbf{R}\}$

Cool thing: $\mathbf{R}_\alpha / \mathbf{I}_\alpha = \mathbb{F}$. *And we can evaluate* $\mathbf{r} \in \mathbf{R}_\alpha$ *at* α *by taking* $\mathbf{r} \mod \mathbf{I}_\alpha$

This gives the same result as “normal” evaluation!

The infinity point in the algebraic representation

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

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"

What does this last part have to do with FFT?

Like in regular FFT - we'll end up needing to represent $\mathbf{f(X)}$ as a combination of two functions $\mathbf{f_e(N(X)), f_o(N(X))}$ of half the "degree"; where $\mathbf{N}$ will be a degree two rational function.

What does this last part have to do with FFT?

Like in regular FFT - we'll end up needing to represent $\mathbf{f(X)}$ as a combination of two functions $\mathbf{f_e(N(X)), f_o(N(X))}$ of half the "degree"; where $\mathbf{N}$ will be a degree two rational function.

Working within the function field gives us convenient tools to construct the right bases for representing $\mathbf{f, f_e, f_o}$, and defining degree in the right way.