A note on the G-FFT

Ulrich Haböck
uhaboeck@polygon.technology,

June 26, 2024

Abstract

For primes p with $p + 1$ being smooth, the G-FFT from Li and Xing [LX23] is an algebraic FFT, which at first glance seems equivalent to the circle FFT from [HLP24]: It also uses the circle curve over $\mathbb{F}_p$ (in other words the projective line) as underlying domain, and interpolates by low-degree functions with poles over the same set of points. However, their approach to control the degree of the FFT basis is fundamentally different. The G-FFT makes use of punctured Riemann-Roch spaces, and the construction works with the group doubling map only, no projection onto the x-axis involved.

In this note we give an elementary description of the G-FFT without using abstract algebra. We describe a variant which uses a simpler, and in our opinion more natural function space, and which treats the exceptional point of the domain (the group identity) differently. In comparison to the circle FFT, the G-FFT (both the original as well as our variant) has the following downsides. Interpolation and domain evaluation costs the double number of multiplications (the twiddle is not an "odd" function), and the function space is not invariant under the group action, causing additional overhead when applied in STARKs.

Contents

1 Intro

Algebraic FFTs [Can89, vzGG96, LCH14, BSCKL21, LX23, HLP24] are generalizations of the Fast Fourier Transform to finite fields $\mathbb{F}_q$ which do not have a smooth multiplicative group $\mathbb{F}_q^*$. (Here and in the sequel, q is a prime, or a power of a prime.) Instead, they work over suitable algebraic varieties over $\mathbb{F}_q$ (e.g. the line, or more generally a curve) with a sufficiently smooth subgroup G of automorphisms, which induces the necessary group structure on its non-degenerated orbits, the FFT domains. Similar to the multiplicative Fourier transform [CT65] based on the even-odd decomposition, algebraic FFTs are built from the following two main ingredients (for simplicity we restrict to the two-adic case):

1. A chain of 2-to-1 *reduction mappings*,
$$S_0 \xrightarrow{\pi_1} S_1 \xrightarrow{\pi_2} \ldots \xrightarrow{\pi_n} S_n,$$
which gradually halve the size of the FFT domain $D = S_0$, $|D| = 2^n$, until a singleton (or, small enough). These mappings stem from the group structure of D, and in most cases, they are group homomorphisms of algebraic degree 2.

2. For every $k = 0, \ldots, n-1$, a carefully selected *twiddle function*[1], i.e. a function
$$t_k : S_k \longrightarrow \mathbb{F}_q,$$
which distinguishes preimages under π_{k+1}. Typically, the algebraic degree of the twiddle is taken as small as possible. (In all the transforms we are aware of, they are either linear or linear fractional functions.)

The reduction chain, together with the twiddle functions, bootstrap a tensor-like basis of low-degree functions over the variety (often, polynomials), the *FFT basis*, and a divide-and-conquer algorithm for efficient interpolation with respect to that basis. (When run reversed, for domain evaluation[2].)

The main challenge in the construction is an appropriate choice of reduction mappings and twiddle functions. Foremost, the function spaces $\mathscr{F}_n$ spanned by the FFT bases of different two-adic sizes (for n up to the maximum supported order) need to build a bedrock for efficient arithmetics. Ideally, as in the case of the multiplicative FFT, the product of functions from $\mathscr{F}_n$ should be contained in $\mathscr{F}_{n+1}$, i.e.
$$\mathscr{F}_n \cdot \mathscr{F}_n \subseteq \mathscr{F}_{n+1},$$

[1] The naming is due to the final algorithm written down as a butterfly network. Then, the so-called twiddle factors of a butterfly are the values of t_k at the corresponding points of the domain.

[2] We stress the fact that we use the deprecated notions, FFT for interpolation and inverse FFT for evaluation.

but in general an efficient embedding from $\mathscr{F}_n \cdot \mathscr{F}_n$ into $\mathscr{F}_{n+1}$ is sufficient. The property is related to bounding the degree of the functions which, in terms of algebraic geometry, amounts to controlling their poles. Second, the specific choice of the twiddle function has impact on the concrete efficiency of the butterfly network. Again, ideally one would have the same computational cost as for the multiplicative FFT, which is

$$n \cdot 2^n \cdot \left(\frac{1}{2} \cdot \mathsf{M} + \mathsf{A}\right)$$

for a domain of size 2^n, where M denotes multiplications and A additions.

In this writeup we compare the *Galois FFT* (in short, G-FFT) from Li and Xing [LX23] with the recent circle FFT from [HLP24], both tailored to the case that $q+1$ is smooth. We highlight the G-FFT construction in term of the above described principle, and in doing this we keep the exposition as elementary as possible. That is, we do not use the theory of algebraic function fields, the reader is only assumed to be familiar with the concept of the projective closure of a curve.

This note is structured as follows. Section 2 surveys the circle curve, its univariate representation as projective line, and related function spaces. Then, in Section 3, we elaborate our variants of the G-FFT. These variants use a "tighter" function space than the original G-FFT, and treat the exceptional point of a subgroup domain (corresponding to the group identity) differently. The comparison with the circle FFT is then discussed in Section 4. Finally, in Appendix A we describe the original G-FFT from [LX23], and draw the connection between their notation and ours.

Throughout this writeup we restrict to the two-adic setting, in which the domain sizes are a power of two. The mixed radix case, as considered in full generality in [LX23], is beyond our scope.

2 Preliminaries

In this section we state elementary properties of the circle curve and its univariate description as projective line. For details we refer to [HLP24, Section 3]. As therein, we occasionally make use of algebraic geometry terms to address readers which are familiar with it. However, this is merely for connecting the dots between concrete and general. We demand no background in geometry beyond the concept of a projective space.

Throughout the note, we assume that $\mathbb{F}_q$ (where q is a prime, or a prime power) is a finite field with $q+1$ being divisible by 2^n a sufficiently large power of two, for some[3]$n \geq 2$, and F denotes a finite extension field of $\mathbb{F}_q$. The circle curve

$$C : x^2 + y^2 = 1$$

over $\mathbb{F}_q$, is a cyclic group of order $q + 1$, with the group law inherited from the rotation group $SO(2, \mathbb{F}_q)$, i.e.

$$(x, y) \cdot (x', y') = (x \cdot x' - y \cdot y', x \cdot y' + y \cdot x'). \tag{1}$$

Its neutral element is $e = (1, 0)$, the group squaring map is

$$\pi(x, y) = (x, y) \cdot (x, y) = (2 \cdot x^2 - 1, 2 \cdot xy),$$

and group inversion is given by the map $J(x, y) = (x, -y)$. For any integer m, $0 \leq m \leq n$ we shall denote by G_m the unique cyclic subgroup of order 2^m. The definition includes the trivial subgroup G_0 consisting of the neutral group element. The circle curve over $\mathbb{F}_q$ is affine, meaning it has no additional points in its projective closure. However, the picture changes when considering the curve over the algebraic closure, or any even degree extension of $\mathbb{F}_q$. In this case the circle curve has two points at infinity,

$$\infty = (1 : i : 0), \quad \bar{\infty} = (1 : -i : 0),$$

which are fixed points under the action of the rotation group. (Here $\pm i$ are the square roots of -1.)

The circle curve over $\mathbb{F}_q$ is algebraically isomorphic to the projective line $P^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$, and the isomorphism is given via chordal projection through the neutral group element[4],

$$t = \frac{y}{x - 1},$$

and

$$(x, y) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2 \cdot t}{t^2 + 1} \right).$$

The isomorphism extends to any extension field of $\mathbb{F}_q$, and whenever present, the points at infinity ∞ and $\bar{\infty}$ are mapped to $t = \pm i$ on the projective line. We advise the reader to internalize this one-to-one correspondence, as we will frequently jump between bivariate and univariate representation, thinking of the projective line and the circle as one and the same geometric object.

For example, the circle group law in univariate coordinates is

$$t \odot t' = \frac{t \cdot t' - 1}{t + t'}, \tag{2}$$

[3] The condition $n \geq 2$ guarantees that $q - 1 = 2 \cdot t$ for some odd number t, and hence -1 does not have a square root in $\mathbb{F}_q$.

[4] Note that we use a different convention as in [HLP24], with the neutral group element $(1, 0)$ instead of $(-1, 0)$ being mapped to $t = \infty$ of the projective line.

with $\infty \in P^1(F)$ as the neutral element satisfying $t \odot \infty = t$ for all $t \in F$. (We overload notation here by using the same notation for the point at infinity of the projective line. As the environmental space is clear from the context, this should not cause confusion.) By means of the group operation, $P^1(\mathbb{F}_p)$ acts on itself via the translation map $T_\tau(t) = \tau \odot t$, the group squaring map is

$$\pi(t) = t \odot t = \frac{t^2 - 1}{2 \cdot t}, \tag{3}$$

and $(-1, 0)$ the unique circle element of order 2 corresponds to $\tau = 0$ on the line, with translation map $T_0(t) = -1/t$.

The circle FFT from [HLP24] is expressed in bivariate coordinates, and its function spaces $\mathscr{F}_m$, $m \geq 1$, are closely related to the spaces

$$\mathscr{L}_M(F) = \left\{ p \in F[x, y]/(x^2 + y^2 + 1) \; : \; \deg p \leq \frac{M}{2} \right\}, \tag{4}$$

for any extension field F of $\mathbb{F}_q$, where $M = 2^m$, and $\deg p$ means the smallest total degree amongst all representatives modulo the circle relation $x^2 + y^2 - 1 = 0$. In terms of algebraic geometry, this is the space of all F-rational functions in the Riemann-Roch space of the divisor

$$\frac{M}{2} \cdot \infty + \frac{M}{2} \cdot \bar{\infty}.$$

Even though restricted to F, not necessarily the algebraic closure of $\mathbb{F}_q$, we simply refer to $\mathscr{L}_M(F)$ as *Riemann-Roch space.* In univariate coordinates, the space corresponds to

$$\mathscr{L}_M(F) = \left\{ \frac{p(t)}{(1 + t^2)^{M/2}} \; : \; p(t) \in F[t]^{\leq M} \right\}, \tag{5}$$

consisting of all rational functions of degree at most M, and having poles only at $t = \pm i$. As for points and group operations, we override notation here and identify the two representations of the Riemann-Roch space.

On the other hand, we mainly express the G-FFT in univariate coordinates. Its function spaces $\mathscr{F}_m$, $m \geq 1$, are related to the *punctured Riemann-Roch spaces*

$$\mathscr{L}_M(F)' = \mathscr{L}_M(F) \cap \mathcal{V}(G_0)^5 = \left\{ \frac{p(t)}{(1 + t^2)^{M/2}} \; : \; p(t) \in F[t]^{< M} \right\}, \tag{6}$$

corresponding to all functions in $\mathscr{L}_M(F)$ which evaluate to zero at $t = \infty$, the neutral group element constituting the trivial subgroup G_0. (Note the strict degree bound in (6).) The dimension of $\mathscr{L}'_M(F)$ is $\dim \mathscr{L}'_M(F) = M$, one less than the entire Riemann-Roch space $\mathscr{L}_M(F)$.[6]

[5] Here and in the sequel, $\mathcal{V}(S) = \bigcap_{P \in S} \{p \in F[x, y]/(x^2 + y^2 - 1) \; : \; p(P) = 0\}$, for any set $S \subseteq C(\mathbb{F}_q)$.

[6] We deviate here from the notation in [HLP24], where $\mathscr{L}_M(F)'$ is the circle FFT space.

3 The G-FFT

We keep with the notation of the previous section, and assume that q be a prime (or more generally, a prime power) so that 2^n divides $q+1$, for some $n \geq 2$. For any $0 \leq m \leq n$, G_m is the unique cyclic subgroup of the circle $C(\mathbb{F}_q)$, having order $M = 2^m$, and P_m denotes a generator of G_m. In particular, P_0 is the neutral group element, and P_1 the unique point of order two.

Compared to the circle FFT, the Galois FFT is closer to the regular multiplicative FFT. It works over *arbitrary cosets* D_m of G_m, $m \leq n$, and it uses the chain of domains obtained throughout from the group doubling map π,

$$D_m \xrightarrow{\pi} D_{m-1} \xrightarrow{\pi} D_{m-2} \xrightarrow{\pi} \dots \tag{7}$$

where in each step the domain sizes are halved. However, in stark contrast to other FFTs, the Galois FFT takes a twiddle function which has a pole *outside* the set of fixed points of the group action, and thus is not contained in the Riemann-Roch space: The linear fractional function

$$t_0(t) = \frac{1}{t} = \frac{x-1}{y}$$

has a pole at $t = 0$ corresponding to P_1 the unique element of order two. We will see that this pole however does not harm, if one works with the punctured Riemann-Roch spaces

$$\mathscr{L}'_M(F) = \mathscr{L}_M(F) \cap \mathcal{V}(G_0).$$

The vanishing constraint at the neutral element P_0 assures that the pull-back $f \circ \pi$ of functions from the punctured Riemann-Roch space have a zero at P_1, cancelling out the pole of the twiddle.

For the sake of simplicity we first describe the *coset FFT*, in Section 3.1, where the interpolation domain is a *non-trivial* coset of G_m and thus does not contain the exceptional point P_0, the neutral group element. The remaining case, which we call the *group position FFT*, is then discussed in Section 3.2. We note that the algorithms in Section 3.1 and 3.2 are minor modifications of the one in [LX23]. Our variant takes the punctured Riemann-Roch space $\mathscr{L}'_M(F)$ as the function space $\mathscr{F}_m$, whereas Li and Xing choose the space of double dimension, and then size it down by additional vanishing constraints. We postpone a description of their original algorithm to Appendix A.

3.1 Coset case

Let D_m be a *non-trivial* coset of the cyclic subgroup G_m, $m \geq 1$, and F any extension field of $\mathbb{F}_q$. Given a set of values $f \in F^{D_m}$ the coset FFT computes the coefficients of $\hat{f} \in \mathscr{L}'_M(F)$ with respect to a specific basis $\mathcal{B}_m$ of $\mathscr{L}'_M(F)$, defined below, so that $\hat{f}(P) = f(P)$ for every $P \in D_m$. The variant described in this section takes the chain

$$D_m \xrightarrow{\pi} D_{m-1} \xrightarrow{\pi} \ldots \xrightarrow{\pi} D_1, \tag{8}$$

down to the *two-point* domain D_1, each of which are again non-trivial cosets of the subgroups G_m, G_{m-1}, $\ldots$, G_1, respectively. (The reason why we do not continue down to a singleton domain is that the definition of $\mathscr{L}_M$ fits our purpose only for even degree bounds $M = 2^m$, $m \geq 1$.)

Given the function $f \in F^{D_m}$ to be interpolated, the FFT is as follows. In the first step, $k = 1$, the function $f \in F^{D_m}$ is decomposed into $f_0, f_1 \in F^{D_{m-1}}$ over the "projected" domain, via

$$f(t) = f_0(\pi(t)) + \frac{1}{t} \cdot f_1(\pi(t)), \tag{9}$$

where

$$f_1(\pi(t)) = \frac{t}{1+t^2} \cdot \left(f(t) - f\left(-\frac{1}{t}\right)\right), \tag{10}$$

$$f_0(\pi(t)) = f(t) - \frac{1}{t} \cdot f_1(\pi(t)) = \frac{t}{1+t^2} \cdot \left(t \cdot f(t) + \frac{1}{t} \cdot f\left(-\frac{1}{t}\right)\right). \tag{11}$$

Note that the right-hand sides of Equation (10) and (11) are well-defined and invariant with respect to $T_0(t) = -\frac{1}{t}$, i.e. the group translation with respect to the generator P_1 of G_1. In fact, denoting the right-hand side of Equation (10) by $F_1(t)$, we obtain that

$$F_1\left(-\frac{1}{t}\right) = -\frac{t}{1+t^2} \cdot \left(f\left(-\frac{1}{t}\right) - f(t)\right) = F_1(t)$$

and likewise the right-hand side $F_0(t)$ of Equation (11) satisfies

$$F_0\left(-\frac{1}{t}\right) = -\frac{t}{1+t^2} \cdot \left(-\frac{1}{t} \cdot f\left(-\frac{1}{t}\right) - t \cdot f(t)\right) = F_0(t).$$

By invariance with respect to G_1, both F_0 and F_1 are of the claimed form $f_0 \circ \pi$ and $f_1 \circ \pi$ with $f_0, f_1 \in F^{D_{m-1}}$, respectively.

In the further steps, $k = 2, \ldots, m-1$, corresponding to the domains $D_{m-1}, \ldots$, D_2, one proceeds with each of the functions $f_{i_1,\ldots,i_{k-1}} \in F^{D_{m-k+1}}$ from the previous step, $(i_1, \ldots, i_{k-1}) \in \{0,1\}^{k-1}$, in the same manner as with f in the first step, decomposing them into $f_{i_1,\ldots,i_{k-1},0}$ and $f_{i_1,\ldots,i_{k-1},1} \in F^{D_{m-k}}$ by means of Equation (9), (10) and (11).

In the last step $k = m$, corresponding to the two-point coset D_1, each of the functions $f_{i_1,\ldots,i_{m-1}} \in F^{D_1}$, $(i_1, \ldots, i_{m-1}) \in \{0,1\}^{m-1}$, is interpolated by

$(c_1 + c_0 \cdot t)/(1+t^2) \in \mathscr{L}_2'(F)$ using the explicit formulas[7]

$$c_1 = f(t) + f\left(-\frac{1}{t}\right), \tag{12}$$

$$c_0 = t \cdot f(t) - \frac{1}{t} \cdot f\left(-\frac{1}{t}\right). \tag{13}$$

The obtained coefficients $c_{i_1,\dots,i_m} \in F$, $(i_1, \dots, i_m) \in \{0,1\}^m$, two for each of the $f_{i_1,\dots,i_{m-1}}$, are the output of the algorithm.

The coefficients output by the algorithm are in fact the coordinates with respect to the basis as described in the following main theorem.

Theorem 1 (Coset FFT)**.** *Given $f \in F^{D_m}$ a function over a non-trivial coset D_m of the subgroup G_m, where $1 \leq m \leq n$, the above described algorithm determines the coefficients $c_{i_1,\dots,i_m} \in F$, $(i_1, \dots, i_m) \in \{0,1\}^m$, of $\hat{f} = \sum_{i \in \{0,1\}^m} c_i \cdot b_{m,i}$ with respect to the family $\mathcal{B}_m$ of functions from $\mathscr{F}_m = \mathscr{L}_M'(F)$ defined by*

$$\mathcal{B}_m = \{b_{m,i}\} = \left\{ v_{G_m} \cdot \prod_{k=0}^{m-1} (t_0 \circ \pi^k)^{i_{k+1}} \ : \ i = (i_1, \dots, i_m) \in \{0,1\}^m \right\}, \tag{14}$$

where $t_0(t) = 1/t$, $v_{G_1}(t) = \frac{t}{1+t^2}$ and $v_{G_m} = v_{G_1} \circ \pi^{m-1}$. In particular, the functions from $\mathcal{B}_m$ form a basis of $\mathscr{F}_m$.

Remark 2. Together with the constant function, $\mathcal{B}_m \cup \{1\}$ is a basis of the non-punctured Riemann-Roch space $\mathscr{L}_M(F)$. Up to non-zero scaling factors, this is the same basis as in [LX23, Lemma 4.4], see Appendix A.

Proof of Theorem 1. We prove the theorem by induction on m. In the case $m = 1$, Equation (12) and Equation (13) yield the coefficients c_1 and c_0 of

$$b_{0,i_0}(t) = \frac{v_{G_1}(t)}{t^{i_0}} = \begin{cases} \frac{t}{1+t^2} & i_1 = 0, \\ \frac{1}{1+t^2} & i_0 = 1, \end{cases}$$

which form a basis of the punctured space $\mathscr{L}_2'(F) = \mathscr{L}_2(F) \cap \mathcal{V}(G_0)$.

Next, suppose that the statement of the theorem is true for some m, $1 \leq m \leq n-1$, and let $f \in F^{D_{m+1}}$. Then for each of the functions $f_0, f_1 \in F^{D_m}$ defined by decomposition

$$f(t) = f_0(\pi(t)) + \frac{1}{t} \cdot f_1(\pi(t))$$

the algorithm outputs the coefficients $(c_{0,i_1,\dots,i_m})$ and $(c_{1,i_1,\dots,i_m})$ with respect to $\mathcal{B}_m$, and this family is a basis of $\mathscr{L}_M'(F)$, for $M = 2^m$. Combining them into

[7] Notice that these formulas are normalized and sign-switched variants of (10) and (11).

a single vector $(c_{i_0,i_1,\dots,i_m})$ of size 2^{m+1} yields the coefficients of f with respect to the family of functions defined by

$$b_{m+1,i}(t) = \frac{1}{t^{i_0}} \cdot b_{m,i_1,\dots,i_m}(\pi(t)),$$

where $i = (i_0, \dots, i_m) \in \{0,1\}^{m+1}$. Since each $b_{m,i_1,\dots,i_m}$ is from $\mathscr{L}_M$ and vanishes over G_0, their pull-backs $b_{m,i_1,\dots,i_m} \circ \pi$ belong to $\mathscr{L}_{2M}$ and they vanish over G_1. In particular, multiplication by the twiddle $t_0(t) = 1/t$, which has a single simple pole at P_1, does change neither the membership to $\mathscr{L}_{2M}$, nor the value zero at P_0. This shows that the functions from $\mathcal{B}_{m+1}$ belong to $\mathscr{L}'_{2\cdot M}(F) = \mathscr{L}_{2\cdot M}(F) \cap \mathcal{V}(G_0)$, and their linear combination using the coefficient vector $(c_{i_0,\dots,i_{m+1}})$ interpolate the given function $f \in F^{D_{m+1}}$. Since f was arbitrary, the span of $\mathcal{B}_{m+1}$ is 2^{m+1}-dimensional, which equals the dimension of the punctured space $\mathscr{L}'_{2\cdot M}(F)$. In other words, $\mathcal{B}_{m+1}$ is a basis of $\mathscr{L}'_{2\cdot M}(F)$, proving the statement of the theorem for $m+1$. □

Remark 3. The coset FFT can be implemented as a butterfly network, which modifies the values over D_m pairwise and in-place by means of Equation (10) and (11), and in the last step via Equation (12) and (13). Counting subtractions as additions, each butterfly costs two additions over F and two multiplications by precomputed elements of $\mathbb{F}_q$, yielding an overall cost of

$$m \cdot 2^m \cdot (\mathsf{M} + \mathsf{A})$$

for the entire algorithm, where M are multiplications of elements from F by scalars of $\mathbb{F}_q$, and A additions in F.

The inverse FFT for domain evaluation reverses each of the decomposition steps of the FFT. Given the coefficient vector $(c_{i_1,\dots,i_{m-1},i_m})$, each of the functions $f_{i_1,\dots,i_{m-1}} = c_{i_1,\dots,i_{m-1},0} \cdot b_{1,0} + c_{i_1,\dots,i_{m-1},1} \cdot b_{1,1}$ is evaluated over D_1 via the inverse butterfly of Equation (12) and Equation (13),

$$f(t) = \frac{1}{1+t^2} \cdot c_1 + \frac{t}{1+t^2} \cdot c_0, \tag{15}$$

$$f\left(-\frac{1}{t}\right) = \frac{t^2}{1+t^2} \cdot c_1 - \frac{t}{1+t^2} \cdot c_0 = c_1 - f(t). \tag{16}$$

In the other steps, one takes

$$f(t) = f_0(\pi(t)) + \frac{1}{t} \cdot f_1(\pi(t)), \tag{17}$$

$$f\left(-\frac{1}{t}\right) = f_0(\pi(t)) - t \cdot f_1(\pi(t)), \tag{18}$$

to combine the values of $f_{i_1,\dots,i_{i_{m-k}},0}$, $f_{i_1,\dots,i_{m-k},1} \in F^{D_{m-k}}$ into the values of $f_{i_1,\dots,i_{m-k},i_{m-k+1}}$ over D_{m-k+1}. Both butterflies again cost two additions in F and two multiplications by elements from $\mathbb{F}_q$. We summarize the result by the following theorem.

Theorem 4 (Evaluation over cosets)**.** *Given the coefficients $c_i \in F$, $i = (i_1, \dots, i_m) \in \{0,1\}^m$, with respect to $\mathcal{B}_m = \{b_{m,i}\}$ as in Theorem 1, the above sketched algorithm computes the values of*

$$f(t) = \sum_{i \in \{0,1\}^m} c_i \cdot b_{m,i}(t)$$

over the non-trivial coset D_m, within $m \cdot 2^m$ additions in F and $m \cdot 2^m$ multiplications of elements in F with (precomputed) elements from $\mathbb{F}_q$.

3.2 Group position

For the exceptional case that the coset D_m is in group position, i.e. $D_m = G_m$, the FFT from Section 3.1 can be easily modified to solve the generalized interpolation problem over the domain.

Definition 5. Given values $f \in F^{G_m}$, the *generalized interpolation problem* asks for a function $\hat{f}$ from the punctured Riemann-Roch space $\mathscr{F}_m = \mathscr{L}'_M(F)$ such that $\hat{f}(t) = f(t)$ for every $t \in G_m \setminus G_0$, and $t \cdot \hat{f}(t) = f(t)$ at the exceptional point $t = \infty$.

The function $f \in F^{D_m}$ is decomposed into $f_0, f_1 \in F^{D_{m-1}}$ in the usual way, using Equation (10) and (11) for $t \in D_m \setminus G_1$, yielding their values over $D_{m-1} \setminus G_0$. To determine f_0 and f_1 at the exceptional point, one takes

$$f_1(\infty) = -\frac{f(0)}{2}, \tag{19}$$

$$f_0(\infty) = \frac{f(\infty)}{2}. \tag{20}$$

The rationale behind these formulas is taken from the observation that their low-degree extensions satisfy

$$t' \cdot \hat{f}_1(t')\Big|_{t'=\infty} = \frac{t^2-1}{2 \cdot t} \cdot \frac{t}{1+t^2} \cdot \left(\hat{f}(t) - \hat{f}\left(-\frac{1}{t}\right)\right)\Big|_{t=\infty},$$

$$t' \cdot \hat{f}_0(t')\Big|_{t'=\infty} = \frac{t^2-1}{2 \cdot t} \cdot \frac{t}{1+t^2} \cdot \left(t \cdot \hat{f}(t) + \frac{1}{t} \cdot \hat{f}\left(-\frac{1}{t}\right)\right)\Big|_{t=\infty},$$

where in both formulas $t' = \pi(t)$. This procedure is applied to all the other steps $k = 2, \dots, m-1$ which correspond to domain sizes larger than two. In the final step, $k = m$, determining the coefficients of $f := f_{i_1,\dots,f_{m-1}} \in F^{G_1}$ with respect to $\mathcal{B}_1 = \{b_{1,0}, b_{1,1}\}$ is trivial: Taking

$$c_1 = f(0), \tag{21}$$

$$c_0 = f(\infty), \tag{22}$$

gives $\hat{f}(t) = c_0 \cdot b_{1,0}(t) + c_1 \cdot b_{1,1}(t)$ which solves the generalized interpolation problem over G_1.

Theorem 6 (Group position FFT)**.** *Given $f \in F^{G_m}$, the above sketched modified FFT computes the coefficients of $\hat{f} \in \mathscr{F}_m$ with respect to the basis $\mathcal{B}_m$ as in Theorem 1, so that $\hat{f}(t) = f(t)$ for $t \in G_m \setminus G_0$, and $t \cdot \hat{f}(t) = f(t)$ at $t = \infty$.*

Proof. The proof is similar to that of Theorem 1. For $m = 1$, the function $\hat{f}(t) = c_0 \cdot b_{1,0}(t) + c_1 \cdot b_{1,1}(t)$ with c_1, c_0 as in Equation (21) and (22) obviously satisfies the generalized interpolation problem over $G_1 = \{0, \infty\}$, since

$$\hat{f}(t) = c_0 \cdot \frac{t}{1+t^2} + c_1 \cdot \frac{1}{1+t^2}\Big|_{t=0} = c_1,$$

and

$$t \cdot \hat{f}(t) = c_0 \cdot \frac{t^2}{1+t^2} + c_1 \cdot \frac{t}{1+t^2}\Big|_{t=\infty} = c_0.$$

For the induction step, if $\hat{f}_0, \hat{f}_1 \in \mathscr{L}'_M(F)$ satisfy the generalized interpolation problem for $f_0, f_1 \in F^{G_m}$ as defined by Equation (10) and (11) for $t \in G_{m+1} \setminus G_1$, and Equation (19) and (20) at the exceptional point, then

$$\hat{f}(t) = \hat{f}_0(\pi(t)) + \frac{1}{t} \cdot \hat{f}_1(\pi(t))$$

satisfies the generalized interpolation problem for $f \in F^{G_{m+1}}$: For the regular points $t \in D_{m+1} \setminus G_1$ we have $\hat{f}(t) = f(t)$ for the usual reasons, and over G_1 we get

$$\hat{f}(t) = \hat{f}_0(\pi(t)) + \frac{1}{t} \cdot \hat{f}_1(\pi(t))\Big|_{t=0} = \hat{f}_0(t') - 2 \cdot t' \cdot \hat{f}_1(t')\Big|_{t'=\infty} = f(0),$$

since $t \cdot t' = t \cdot \frac{t^2-1}{2 \cdot t}\Big|_{t=0} = -1/2$ and $\hat{f}_0(\infty) = 0$, whereas

$$t \cdot \hat{f}(t) = t \cdot \hat{f}_0(\pi(t)) + \hat{f}_1(\pi(t))\Big|_{t=\infty} = 2 \cdot t' \cdot \hat{f}_0(t') + \hat{f}_1(t')\Big|_{t=\infty} = f(\infty),$$

since $t/t' = t \cdot \frac{2 \cdot t}{t^2-1}\Big|_{t=\infty} = 2$ and $\hat{f}_1(\infty) = 0$. □

Likewise, the inverse FFT can be modified to compute the generalized evaluation of a function $\hat{f} \in \mathscr{L}'_M(F)$ over the group position domain G_m.

Definition 7. The *generalized evaluation* of a function $\hat{f} \in \mathscr{F}_m$ over G_m outputs the value of $\hat{f}(t)$ for every $t \in G_m \setminus G_0$ and the value of $t \cdot \hat{f}(t)$ at $t = \infty$.

In the first step $k = 1$, generalized evaluation of each $f_{i_1,\dots,i_{m-1}}$ over D_1 is directly read off the coefficients $c_{i_1,\dots,i_{m-1},0}$ and $c_{i_1,\dots,i_{m-1},1}$ using Equation (21) and Equation (22), and in the other steps $2 \leq k \leq m$, corresponding to the larger domains $G_2, \dots, G_m$, the values of $\hat{f}_{i_1,\dots,i_{m-k},0}$ and $\hat{f}_{i_1,\dots,i_{m-k},1}$ are combined into those of $\hat{f}_{i_1,\dots,i_{m-k},i_{m-k+1}}$ in the usual manner at the regular points $t \in G_k \setminus G_1$, and by Equation (19) and Equation (20) at the exceptional point.

Theorem 8 (Evaluation over subgroups)**.** *Given coefficients $c_i \in F$, $i \in \{0,1\}^m$, the above sketched inverse FFT computes the generalized evaluation of $\hat{f} = \sum_i c_i \cdot b_{m,i} \in \mathscr{F}_m$ over G_m.*

In terms of group operations, the cost of both the group position FFT and its inverse is essentially that of the coset FFT.

3.3 Explicit form of the basis

For an explicit form of the basis $\mathcal{B}_m$ of the FFT space $\mathscr{F}_m = \mathscr{L}'_M(F)$, an alternative representation based on vanishing functions is more useful than the one from Theorem 1. For $1 \leq k < n$, let $v_{G_k} = v_{G_1} \circ \pi^{k-1}$ and $v_{G'_k} = v_{G'_1} \circ \pi^{k-1}$, where

$$v_{G_1} = y = \frac{2 \cdot t}{t^2 + 1}, \quad v_{G'_1} = x = \frac{t^2 - 1}{t^2 + 1}.$$

(Note that, compared to the previous sections we use a scaled variant of v_{G_1} here. This is for more elegant expressions.) It follows from their definition that v_{G_k} and $v_{G'_k}$ have simple zeros over G_k and its complementing coset G'_k, respectively, and poles at $t = \pm i$ of order 2^k each. (No other poles and zeros present.) Thus they belong to $\mathscr{L}_{2^k}(\mathbb{F}_q)$. Their explicit representation

$$v_{G_k}(t) = \frac{u_k(t)}{(t^2+1)^{2^{k-1}}}, \quad v_{G'_k}(t) = \frac{v_k(t)}{(t^2+1)^{2^{k-1}}},$$

with polynomials $u_k(t), v_k(t) \in \mathbb{F}_q[t]$, where $\deg u_k = 2^k - 1$ and $\deg v_k = 2^k$, can be obtained recursively via the same law

$$u_{k+1}(t) = (2 \cdot t)^{2^k} \cdot u_k\left(\frac{t^2-1}{2 \cdot t}\right), \quad v_{k+1}(t) = (2 \cdot t)^{2^k} \cdot v_k\left(\frac{t^2-1}{2 \cdot t}\right),$$

starting with $u_1(t) = 2 \cdot t$ and $v_1(t) = t^2 - 1$, respectively. Alternatively, they can be derived from the circle polynomials v_{G_k} and $v_{G'_k}$, which are recursively given by

$$v_{G'_{k+1}}(x) = v_{G'_k}(2 \cdot x^2 - 1),$$
$$v_{G_{k+1}} = 2 \cdot v_{G_k} \cdot v_{G'_k},$$

starting with $v_{G'_1} = x$ and $v_{G_1} = y$.

Lemma 1. *For $1 \leq k < n$, it holds that $v_{G_k} \cdot v_{G'_k} = 2 \cdot v_{G_{k+1}}$. In particular $v_{G_m} = 2^{m-1} \cdot v_{G_1} \cdot v_{G'_1} \cdot \ldots \cdot v_{G'_{m-1}}$, for $1 \leq m \leq n$.*

Proof. The first assertion follows from $v_{G_k} = v_{G_1} \circ \pi^{k-1}$ and $v_{G'_k} = v_{G'_1} \circ \pi^{k-1}$, and that

$$v_{G_2} = v_{G_1} \circ \pi = 4 \cdot t \cdot \frac{t^2 - 1}{(t^2-1)^2 + 4 \cdot t^2} = 2 \cdot \frac{2 \cdot t \cdot (t^2 - 1)}{(t^2+1)^2} = 2 \cdot v_{G_1} \cdot v_{G'_1}.$$

The second assertion is obtained by repeated application of the first. □

Proposition 1. *In terms of the vanishing functions v_{G_k} and $v_{G'_k}$ we have*

$$b_{m,i} = 2^{m-2} \cdot \frac{v_{G_1}}{t^{i_1}} \cdot \prod_{k=1}^{m-1} \left(i_{k+1} \cdot v_{G_k} + (1 - i_{k+1}) \cdot v_{G'_k} \right). \tag{23}$$

Therefore, by means of the univariate vanishing polynomials u_k and v_k, we obtain the representation $b_{m,i} = p_{m,i}(t)/(1+t^2)^{2^{m-1}}$, with polynomials

$$p_{m,i} = 2^{m-2} \cdot t^{1-i_1} \cdot \prod_{k=1}^{m-1} \left(i_{k+1} \cdot u_k + (1 - i_{k+1}) \cdot v_k \right), \tag{24}$$

These polynomials form a basis of $\mathbb{F}_q[t]^{<M}$.

Proof. Using Lemma 1, and $t_0 \circ \pi^k = \frac{v_{G_k}}{v_{G'_k}}$ for $1 \leq k \leq m-1$, we obtain

$$b_{m,i} = \frac{1}{2} \cdot 2^{m-1} \cdot \frac{v_{G_1}}{t^{i_1}} \cdot v_{G'_1} \cdot \ldots \cdot v_{G'_{m-1}} \cdot \prod_{k=1}^{m-1} \left(\frac{v_{G_k}}{v_{G'_k}} \right)^{i_{k+1}}.$$

(The leading factor $1/2$ is for the different convention of v_{G_m} in Theorem 1.) Thus the bit i_{k+1} effectively selects between $v_{G'_k}$ and v_{G_k}, for $k = 1, \ldots, m-1$, yielding

$$b_{m,i} = 2^{m-1} \cdot \frac{v_{G_1}}{t^{i_1}} \cdot \prod_{k=1}^{m-1} \left(i_{k+1} \cdot v_{G_k} + (1 - i_{k+1}) \cdot v_{G'_k} \right),$$

from which the univariate representation follows. □

In bivariate coordinates, the first four vanishing polynomials are

$$\begin{aligned}
v_{G'_1} &= x, & v_{G_1} &= y, \\
v_{G'_2} &= 2\,x^2 - 1, & v_{G_2} &= y \cdot x, \\
v_{G'_3} &= 8\,x^4 - 8\,x^2 + 1, & v_{G_3} &= y \cdot (2\,x^3 - x), \\
v_{G'_4} &= 128\,x^8 - 256\,x^6 + 160\,x^4 - 32\,x^2 + 1, & v_{G_4} &= y \cdot (16\,x^7 - 24\,x^5 + 10\,x^3 - x),
\end{aligned}$$

whereas in univariate coordinates we obtain the numerator polynomials

$$
\begin{aligned}
v_1 &= t^2 - 1, & u_1 &= 2\,t,\\
v_2 &= t^4 - 6\,t^2 + 1, & u_2 &= 2\,t \cdot (t^2 - 1),\\
v_3 &= t^8 - 28\,t^6 + 70\,t^4 - 28\,t^2 + 1, & u_3 &= 2\,t \cdot (t^6 - 7\,t^4 + 6\,t^2 - 1),
\end{aligned}
$$

and

$$
\begin{aligned}
v_4 &= t^{16} - 120\,t^{14} + 1820\,t^{12} - 8008\,t^{10} + 12870\,t^8 - 8008\,t^6 + 1820\,t^4 - 120\,t^2 + 1,\\
u_4 &= 2\,t \cdot (t^{14} - 35\,t^{12} + 273\,t^{10} - 715\,t^8 + 715\,t^6 - 273\,t^4 + 35\,t^2 - 1).
\end{aligned}
$$

4 Comparison with the circle FFT

The circle FFT from [HLP24] uses a fundamentally different strategy for bounding the degree of the function spaces $\mathscr{F}_m$. Instead of working with the group squaring map π alone, the first step of the FFT is with respect to the quotient map

$$\phi_J : C(\mathbb{F}_q) \longrightarrow C(\mathbb{F}_q)/J$$

of the group inversion automorphism $J(x, y) = (x, -y)$, which is a linear (and not quadratic) algebraic map. The subsequent steps are then performed with respect to the group squaring map π, which uniquely translates to a map on the quotient $C(\mathbb{F}_q)/J$, since J and π commute, i.e. $J \circ \pi = \pi \circ J$. This leads to the reduction chain

$$D_m \xrightarrow{\phi_J} D_m/J \xrightarrow{\pi} D_{m-1}/J \xrightarrow{\pi} \ldots \xrightarrow{\pi} D_m/J,$$

whereas the quotient sets may be also regarded as subset of the x-axis, and ϕ_J as projection onto it. Considering the domain D_m being the *standard position cosets* of G_m (i.e. $D_m = G'_m$ with G'_m being the unique coset of G_m such that $G'_m \cap G_m = G_{m+1}$) all maps are 2-to-1, halving the domains in each of the steps. In the first step, the twiddle function y is taken, and in the other steps x. The resulting function space $\mathcal{F}_m$ is the subspace of $\mathscr{L}_M(F)$ spanned by the basis

$$b_{m,i} = y^{i_1} \cdot \prod_{k=1}^{m-1} (x \circ \pi^{k-1})^{i_{k+1}} = y^{i_1} \cdot \prod_{k=1}^{m-1} v_{G'_k}^{i_{k+1}},$$

where $i = (i_1, \ldots, i_m) \in \{0, 1\}^m$. The complete Riemann-Roch space $\mathscr{L}_M(F)$ decomposes as

$$\mathscr{L}_M(F) = \mathscr{F}_m(F) + \langle v_{D_m} \rangle,$$

and this decompositions is orthogonal in a certain sense [HLP24, Section 4.3].

Overall, the circle FFT has the following advantages over the G-FFT:

1. *Concrete performance.* The twiddle functions of the circle FFT are alternating under the action of the kernel group (which acts transitively on the fibers of the projections), and thus yield a butterfly network which consumes only the half number of multiplications (by pre-computed twiddle values) than additions, yielding the usual computational cost

   $$\mathsf{FFT}(2^m) = m \cdot 2^{m-1} \cdot \mathsf{M} + m \cdot 2^m \cdot \mathsf{A},$$

   as for a regular multiplicative FFT. The G-FFT instead (both the variants from Section 3.1 and 3.2, as well as the original described in Appendix A) costs the double amount of multiplications

   $$\mathsf{FFT}(2^m) = m \cdot 2^m \cdot \mathsf{M} + m \cdot 2^m \cdot \mathsf{A},$$

   cf. Remark 3 of Theorem 1, and Theorem 4. This double multiplication cost is due to the fact that the twiddle function t_0 does not alternate under action of the kernel group[8] G_1, i.e. $t_0(-1/t) \neq -t_0(t)$.

2. *Rotation invariance.* Contrary to the punctured Riemann-Roch space $\mathscr{L}'_M(F)$, the circle FFT space $\mathscr{F}_m$ is invariant under rotations by elements from G_m [HLP24, Section 4.3], which makes it more suitable for the proving algebraic intermediate representations (AIR) [BSBHR18, BSGKS20, Sta23], or more generally Plonk-ish arithmetization [GWC19].

References

[BSBHR18] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. In *IACR ePrint Archive 2018/046*, 2018. https://eprint.iacr.org/2018/046.

[BSCKL21] Eli Ben-Sasson, Dan Carmon, Swastik Kopparty, and David Levit. Elliptic Curve Fast Fourier Transform (ECFFT) Part I: Fast polynomial algorithms over all finite fields. In *Electronic Colloquium on Compputational Complexity*, volume TR21-103, 2021. https://eccc.weizmann.ac.il/report/2021/103/.

[BSGKS20] Eli Ben-Sasson, Lior Goldberg, Swastik Kopparty, and Shubhangi Saraf. DEEP-FRI: Sampling outside the box improves soundness. In *ITCS 2020*, 2020. Full paper: https://eprint.iacr.org/2019/336.

[Can89] David G. Cantor. On arithmetical algorithms over finite fields. In *Journal of Combinatorial Theory*, volume Series A 50, 1989.

[8] The kernel group parametrizes the fibers of the 2-to-1 mappings, hence the name.

[CT65] James W. Cooley and John W. Tukey. An algorithm for the machine calculation of complex Fourier series. In *Mathematics of Computation*, volume 19 (90), pages 297–301, 1965.

[GWC19] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. PLONK: Permutations over Lagrange-bases for oecumenical noninteractive arguments of knowledge. In *IACR ePrint Archive 2019/953*, 2019. `https://eprint.iacr.org/2019/953`.

[HLP24] Ulrich Haböck, David Levit, and Shahar Papini. Circle STARKs. In *IACR preprint archive*, 2024. `https://eprint.iacr.org/2024/278`.

[LCH14] Sian-Jheng Lin, Wei-Ho Chung, and Yunghsiang S. Han. Novel polynomial basis and its application to Reed-Solomon erasure codes. In *FOCS 2014*, 2014.

[LX23] Songsong Li and Chaoping Xing. Fast Fourier transform via automorphicsm groups of rational function fields. In *arXiv:2310.14462*, 2023. `https://arxiv.org/abs/2310.14462`.

[Sta23] StarkWare Team. ethSTARK documentation – version 1.2. In *IACR preprint archive 2021/582*, 2023. `https://eprint.iacr.org/2021/582`.

[vzGG96] Joachim von zur Gathen and Jürgen Gerhard. Arithemtic and factorization of polynomials over F_2. In *ISSAC'96*, 1996.

A Appendix

We describe the original G-FFT from Li and Xing, restricted to the two-adic case, and domains of size smaller than $q + 1$.

As before, q is a prime (or a prime power) so that $q + 1 = 2^n \cdot t$ for some integer $n \geq 0$ and odd $t \geq 1$. Given domain size $M = 2^m$, where we assume that $m \leq n - 1$ in our description, the authors construct a function basis of the Riemann-Roch space from the G_k-invariant functions[9]

$$x_k = \sum_{\tau \in G_k} \tau(t), \quad y_k = \prod_{\tau \in G_k} \tau\left(\frac{1}{1+t^2}\right), \tag{25}$$

where $0 \leq k \leq m$, which (up to scaling factors) is the basis from Theorem 1. This can be seen from their definition of the basis functions as

$$\frac{x_{m-1} \cdot y_{m-1}}{x_0^{i_0} \cdots x_{m-1}^{i_{m-1}}},$$

[9] The group action of G_k on the space of rational functions is given by $\tau(f)(t) := f(\tau^{-1} \odot t)$ for $\tau \in G_k$.

and the following two lemmas.

Lemma 2. *For any $0 \leq k \leq n$ the G_k-invariant function x_k is equal to*

$$x_k = 2^k \cdot \pi^k(t), \tag{26}$$

where π is the group squaring map. The function has simple poles over G_k, and whenever $k < n$ it has simple zeros over the complementing coset $G'_k = \sigma \odot G_k$, where σ is of order 2^{k+1}.

Proof. We proof Equation (26) by induction. Taking π^0 as the identity map, Equation (26) is trivially true for $k = 0$. Assume that it holds for some $0 \leq k < n$. Taking the decomposition $G_{k+1} = G_k \cup \sigma \odot G_k$, where σ is an element of order 2^{k+1}, we obtain

$$\begin{aligned} x_{k+1} &= \sum_{\tau \in G_{k+1}} \tau(t) = \sum_{\tau \in G_k} \tau(t) + \sum_{\tau \in G_k} \tau(\sigma(t)) \\ &= 2^k \cdot \left(\pi^k(t) + \pi^k(\sigma(t))\right). \end{aligned}$$

Note that π^k is a group endomorphism which maps σ to $P_1 = 0$, the generator of the two-point subgroup G_1. Hence for every point t on the projective line $\pi^k(\sigma(t)) = \pi^k(\sigma^{-1} \odot t) = 0 \odot \pi^k(t) = -1/\pi^k(t)$, which by degree holds as a formal identity. Therefore,

$$\begin{aligned} x_{k+1} &= 2^k \cdot \left(\pi^k(t) - \frac{1}{\pi^k(t)}\right) = 2^{k+1} \cdot \frac{\pi^k(t)^2 - 1}{2 \cdot \pi^k(t)} \\ &= 2^{k+1} \cdot \pi(\pi^k(t)) = 2^{k+1} \cdot \pi^{k+1}(t), \end{aligned}$$

which proves the claim for $k + 1$. The assertion on the poles and zeros of x_k follows from Equation (26). □

Lemma 3. *For any $0 \leq k \leq n$ the G_k-invariant function y_k is equal to*

$$y_k = \frac{1}{4^{2^k - 1}} \cdot \frac{1}{\pi^k(t)^2 + 1} \tag{27}$$

where π is the group squaring map. The function has zeros over G_k, each of order 2, and poles at $t = \pm i$, each of order $|G_k|$.

Proof. Since the action of G_k leaves $\pm i$ fixed, and lets ∞ visit every point from G_k, the product y_k has poles at $t = \pm i$, each of order $|G_k|$, and zeros over G_k, each of order 2. No other poles and zeros present. The same is true for $1/(\pi^k(t)^2 + 1)$ which shows that $y_k = c_k \cdot 1/(\pi^k(t)^2 + 1)$ for some constant $c_k \neq 0$.

For the concrete value of c_k we use a similar trick as in the proof of Lemma 2. For $k \leq n-1$ we write

$$\begin{aligned} y_{k+1} &= \prod_{\tau \in G_k} \frac{1}{1+\tau(t)^2} \cdot \prod_{\tau \in G_k} \frac{1}{1+\tau(\sigma(t))^2} \\ &= c_k^2 \cdot \frac{1}{\pi^k(t)^2+1} \cdot \frac{1}{\pi^k(\sigma(t))^2+1}, \end{aligned}$$

where σ is an element of order 2^{k+1}, and therefore $\pi^k(\sigma(t)) = -1/\pi^k(t)$. Thus

$$y_{k+1} = c_k^2 \cdot \frac{\pi^k(t)^2}{(\pi^k(t)^2+1)^2},$$

but also

$$y_{k+1} = c_{k+1} \cdot \frac{1}{\pi^{k+1}(t)^2+1} = c_{k+1} \cdot \frac{4 \cdot \pi^k(t)^2}{\left(\pi^k(t)^2+1\right)^2},$$

where we have used that $\pi^{k+1}(t) = \left(\pi^k(t)^2 - 1\right)/(2 \cdot \pi^k(t))$. This yields the recursive law

$$c_k^2 \cdot \frac{1}{4} = c_{k+1},$$

for any $0 \leq k \leq n-1$, where the starting value is $c_0 = 1$. Writing $c_k = 4^{e_k}$ we get $e_{k+1} = 2 \cdot e_k - 1$, where $e_0 = 0$, which has the solution $e_k = -(2^k - 1)$. The assertion on the poles and zeros of y_k follows from Equation (27). □

Corollary 1. *For $m \leq n-1$, and up to non-zero scaling factors from $\mathbb{F}_q$, the set of functions*

$$\tilde{\mathcal{B}}_m = \left\{ \frac{x_{m-1} \cdot y_{m-1}}{x_0^{i_0} \cdots x_{m-1}^{i_{m-1}}} \; : \; (i_0, \ldots, i_{m-1}) \in \{0,1\}^m \right\} \tag{28}$$

equals the basis $\mathcal{B}_m$ from Theorem 1.

Proof. Lemma 2 implies that $1/x_k$ is a (non-zero) scalar multiple of $t_0 \circ \pi^k$, since they have the same set of poles and zeros. For the same reason, Lemma 2 and 3 imply that the product $x_{m-1} \cdot y_{m-1}$ is a non-zero scalar multiple of the vanishing function v_{G_m}. In other words, up to a non-zero scaling factor, the functions from Equation (28) equal $b_{m,i_0,\ldots,i_{m-1}}$ as defined in Theorem 1. □

Let us turn to the FFT. For domain size $M = 2^m$, where $m \leq n-1$, Li an Xing use the function space

$$\mathscr{F}_m = \mathscr{L}_{2\cdot M}(F)' \cap \mathcal{V}(G'_m) = \mathscr{L}_{2\cdot M}(F) \cap \mathcal{V}(G_0) \cap \mathcal{V}(G'_m) \tag{29}$$

consisting of all functions from $\mathscr{L}_{2\cdot M}(F)'$ which also vanish over G'_m the unique coset of G_m so that $G_m \cup G'_m = G_{m+1}$. (By our assumption $m \leq n-1$ such a coset exists.) Contrary to $\mathscr{L}'_M(F)$ the space $\mathscr{F}_m$ is also well-defined in the case $m = 0$, where

$$\mathscr{F}_0 = \mathscr{L}_2(F) \cap \mathcal{V}(G_0) \cap \mathcal{V}(G'_0) = \mathscr{L}_2(F) \cap \mathcal{V}(G_1), \tag{30}$$

spanned by the vanishing function $v_{G_1}(t) = t/(1+t^2)$. For $m \geq 1$ it has the univariate representation

$$\mathscr{F}_m = \left\{ v_{G'_m}(t) \cdot \frac{p(t)}{(1+t^2)^{M/2}} \ : \ p(t) \in F[t]^{<M} \right\}, \tag{31}$$

where $v_{G'_m}(t)$ is the vanishing function of G'_m. In other words,

$$\mathscr{F}_m = \frac{u_m(t)}{(1+t^2)^M} \cdot F[t]^{<M},$$

where $u_m(t) = v_{G'_m}(t) \cdot (1+t^2)^{M/2}$ is the univariate vanishing *polynomial* of G'_m. Up to a non-zero scaling factor, this is the polynomial $u_{m,0}$ from [LX23, Lemma 4.2].

Both the coset FFT from Section 3.1 and the group position FFT from Section 3.2 apply to the function spaces $\mathscr{F}_m$ from (29) with as good as no changes, assuming that the FFT domain D_m is disjoint to the vanishing set G'_m. The only difference is that the double-sized Riemann-Roch spaces allow a reduction chain down to a singleton domain. Given domain D_m, a coset of G_m the subgroup of size $M = 2^m$, the reduction chain is

$$D_m \xrightarrow{\pi} D_{m-1} \xrightarrow{\pi} \ldots \xrightarrow{\pi} D_1 \xrightarrow{\pi} D_0, \tag{32}$$

using the same decomposition also in the last step, leading again to Equation (10) and (11) whenever $t \notin G_1$, and Equation (19) and (20) in the case $t \in G_1$. With $\{v_{G_1}\}$ as the basis for $\mathscr{F}_0$, the resulting basis of $\mathscr{F}_m$ is

$$\mathcal{B}'_{m+1} = \left\{ v_{G_{m+1}} \cdot \prod_{k=0}^{m-1} (t_0 \circ \pi^k)^{i_{k+1}} \ : \ i = (i_1, \ldots, i_m) \in \{0,1\}^m \right\},$$

where $t_0(t) = 1/t$. This is the sub-basis of $\mathcal{B}_{m+1}$ from Theorem 1 when taking the last index entry zero,

$$\mathcal{B}'_{m+1} = \left\{ b_{m+1,i_1,\ldots,i_m,0} \ : \ (i_1, \ldots, i_m) \in \{0,1\}^m \right\}.$$

We leave the details to the reader, and only state the main result [LX23, Theorem 4.6].

Theorem 9 (G-FFT, two-adic case)**.** *Let D_m be a coset of G_m the subgroup of size $M = 2^m$, where $0 \leq m \leq n-1$, and such that $D_m \neq G'_m$, the unique coset of G_m with $G_m \cup G'_m = G_{m+1}$. Given a function f over D_m with values in an extension field F of $\mathbb{F}_q$, the above algorithm outputs the coefficients $c_{i_1,\ldots,i_m}$ of the unique low-degree extension $\hat{f}(t) = \sum c_{i_1,\ldots,i_m} \cdot b_{m+1,i_1,\ldots,i_m,0}(t)$ from $\mathscr{F}_m$ as defined in (29), which solves the (generalized, in case that $D_m = G_m$) interpolation problem for f over G_m.*

Remark 10. There are still some minor differences of our description of the G-FFT to that in [LX23]. Therein, the authors use group position domains $D_m = G_m$ only in the edge case $M = q + 1$, which we do not handle for the sake of interpreting $\mathscr{F}_m$ as a vanishing subspace of $\mathscr{L}_{2 \cdot M}(F)$. Whenever $M < q + 1$ they take coset domains but miss to exclude the choice $D_m = G'_m$, over which the function space $\mathscr{F}_m$ throughout evaluates to zero. Besides, their group position FFT only serves usual domain evaluation, not in the generalized sense as in Section 3.2.