Mathematisches Forschungsinstitut Oberwolfach

Report No. ??/2024

DOI: 10.4171/OWR/2024/??

AG: Quantum Signal Processing and Nonlinear Fourier Analysis

Organized by
András Gilyén, Budapest
Lin Lin, Berkeley
Christoph Thiele, Bonn

6 October – 11 October 2024

Abstract.

Mathematics Subject Classification (2010): 42B20.

Introduction by the Organizers

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1641185, "US Junior Oberwolfach Fellows".

Workshop: AG: Quantum Signal Processing and Nonlinear Fourier Analysis

Table of Contents

Abstracts

Orthogonal polynomials and Geronimus's theorem

Cade Ballew

This talk is based on [1].

A Schur function $f(z)$ is an analytic function defined in the open unit disk $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$ such that $|f(z)| \leq 1$ for all $z \in \mathbb{D}$. For a given Schur function, Schur's algorithm generates a sequence of Schur functions and so-called Schur parameters. It is defined by the recurrence

$$f_0 = f, \quad f_{n+1} = \frac{f_n(z) - f_n(0)}{z(1 - \overline{f_n(0)} f_n(z))}, \quad n \in \mathbb{N}.$$

Provided that f is not a finite Blaschke product, this algorithm generates an infinite sequence of Schur functions $\{f_n\}_{n=0}^{\infty}$ and Schur parameters $\{\gamma_n\}_{n=0}^{\infty}$ where $\gamma_n = f_n(0)$ satisfies $|\gamma_n| < 1$. It turns out that given any sequence $\{\gamma_n\}_{n=0}^{\infty} \subset \mathbb{C}$ such that $|\gamma_n| < 1$, there exists a unique Schur function with these Schur parameters.

A Carathéodory function F is an analytic function defined in the open unit disk $\mathbb{D} = \{z \in \mathbb{C} : |z| < 1\}$ such that $\mathrm{Re} F(z) \geq 0$ for all $z \in \mathbb{D}$. Given a Schur function f with Schur parameters $\{\gamma_n\}_{n=0}^{\infty}$, define

$$F(z) = \frac{1 + zf(z)}{1 - zf(z)}. \tag{1}$$

For $z \in \mathbb{D}$

$$\mathrm{Re} F(z) = \frac{1 - |zf(z)|^2}{|1 - zf(z)|^2} > 0,$$

and $F(z)$ is analytic, so F defines an associated Carathéodory function. By the Herglotz representation theorem, for any Carathéodory function F such that $F(0) = 1$, there exists some Borel probability measure $\frac{1}{2\pi} \mathrm{d}\sigma$ defined on $[0, 2\pi)$ such that

$$F(z) = \frac{1}{2\pi} \int_0^{2\pi} \frac{\mathrm{e}^{\mathrm{i}\theta} + z}{\mathrm{e}^{\mathrm{i}\theta} - z} \mathrm{d}\sigma(\theta). \tag{2}$$

For a Carathéodory function F associated to a Schur function f, The support of $\mathrm{d}\sigma$ is infinite except in the case where f is a finite Blaschke product. Conversely, given any Borel probability measure $\frac{1}{2\pi} \mathrm{d}\sigma$ defined on $[0, 2\pi)$, there exists some Carathéodory function F satisfying (2) and therefore an associated Schur function f satisfying (1).

On the other hand, orthogonal polynomials on the unit circle can be defined for a Borel probability measure $\frac{1}{2\pi} \mathrm{d}\sigma$ on $[0, 2\pi)$. To ensure that an infinite sequence of orthogonal polynomials exists, we assume that the support of $\mathrm{d}\sigma$ is an infinite set. Consider the inner product

$$\langle f, g \rangle_\sigma = \int_0^{2\pi} f\left(\mathrm{e}^{\mathrm{i}\theta}\right) \overline{g\left(\mathrm{e}^{\mathrm{i}\theta}\right)} \mathrm{d}\sigma(\theta),$$

defined for functions of the unit circle $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$. Given the restriction that $\varphi_n(z) = \chi_n z^n + \dots$ where $\chi_n > 0$, there exists a unique system of orthonormal polynomials $\{\varphi_n\}_{n=0}^{\infty}$ on $\mathbb{U} = \{z \in \mathbb{C} : |z| = 1\}$ such that

$$\langle \varphi_n, \varphi_m \rangle_\sigma = \delta_{n,m},$$

for all $n, m \in \mathbb{N}$, where $\delta_{n,m}$ is the Kronecker delta. Such polynomials can be generated through, say, the Gram–Schmidt algorithm applied to the set $\{\diamond^n\}_{n=0}^{\infty}$, starting of course from $n = 0$. The monic orthogonal polynomials $\{\Phi_n\}_{n=0}^{\infty}$ are defined by normalizing the orthonormal polynomials to have leading coefficient 1. That is,

$$\Phi_n(z) = \frac{1}{\chi_n}\varphi_n(z) = z^n + \dots, \quad n \in \mathbb{N}.$$

The reverse polynomials (and more broadly the * operation) are defined by reversing and conjugating the orthogonal polynomial coefficients. That is,

$$\Phi_n^*(z) = z^n \overline{\Phi_n\left(\frac{1}{\overline{z}}\right)}.$$

The monic orthogonal polynomials and their reverse satisfy a the following pair of recurrence formulae:

$$\begin{aligned} \Phi_{n+1}(z) &= z\Phi_n(z) - \overline{a}_n \Phi_n^*(z), \quad n \in \mathbb{N}, \\ \Phi_{n+1}^*(z) &= \Phi_n^*(z) - a_n z \Phi_n(z), \quad n \in \mathbb{N}, \end{aligned} \tag{3}$$

where $a_n = -\overline{\Phi_{n+1}(0)}$. The parameters $\{a_n\}_{n=0}^{\infty}$ are known as Verblunsky coefficients, and $|a_n| < 1$ for all $n \in \mathbb{N}$. Note that $\Phi_0 = \Phi_0^* = 1$, so the monic orthogonal polynomials and their reverse are uniquely generated by their Verblunsky coefficients. It turns out that this construction goes both ways. Favard's theorem says that given any sequence $\{a_n\}_{n=0}^{\infty} \subset \mathbb{C}$ such that $|a_n| < 1$ for all $n \in \mathbb{N}$, there exists a Borel probability measure $\frac{1}{2\pi}\mathrm{d}\sigma$ on $[0, 2\pi)$ such that the corresponding system of orthogonal polynomials $\{\Phi_n\}_{n=0}^{\infty}$ satifies (3) and $a_n = -\overline{\Phi_{n+1}(0)}$ for all $n \in \mathbb{N}$.

The connection between Schur functions and orthogonal polynomials on the unit circle is the following:

Theorem 1 (Geronimus)**.** *It holds that $a_n = \gamma_n$ for all $n \in \mathbb{N}$.*

We will prove this theorem. In a sense, it says that Schur functions and orthogonal polynomials on the unit circle are equivalent. Through the theory presented above, both Schur functions and orthogonal polynomials on the unit circle are associated with a set of parameters and a probability measure which can each be derived from the other. Geronimus's theorem tells us that when the measures agree, so do the parameters and vice versa. This allows us to appeal to the theory of orthogonal polynomials to derive properties of Schur functions, yielding theorems that guarantee decay rates of Schur parameters given smoothness properties of their associated Schur functions and vice versa. We will discuss (and prove if time permits) the following theorems via orthogonal polynomial theory.

Theorem 2. *Let f be a Schur function with boundary values $f(\mathrm{e}^{\mathrm{i}\theta})$. It is said to be regular if its boundary values are continuous and $\sup_{\theta\in\mathbb{R}} |f(\mathrm{e}^{\mathrm{i}\theta})| < 1$. If f is regular and*

$$\sum_{n=1}^{\infty} \frac{1}{\sqrt{n}} \sup_{0<\tau<\frac{1}{n}} \sup_{\theta\in\mathbb{R}} |f(\mathrm{e}^{\mathrm{i}(\theta+\tau)}) - f(\mathrm{e}^{\mathrm{i}\theta})| < \infty,$$

then its associated Schur parameters satisfy

$$\sum_{n=0}^{\infty} |\gamma_n| < \infty.$$

Conversely, if $\{\gamma_n\}_{n=0}^{\infty}$ are absolutely summable, then their associated Schur function is regular.

Theorem 3. *Schur coefficients $\{\gamma_n\}_{n=0}^{\infty}$ satisfy*

$$\limsup_{n\to\infty} |\gamma_n|^{1/n} < 1,$$

if and only if their associated Schur function is analytic in a region containing the closed unit disk $\overline{\mathbb{D}}$ and $\sup_{z\in\overline{\mathbb{D}}} |f(z)| < 1$.

References

[1] L. B. Golinskii. Schur Functions, Schur Parameters and Orthogonal Polynomials on the Unit Circle *Zeitschrift für Analysis und ihre Anwendungen*, 12(3):457–469, 1993.

The postulates of quantum computing

Tiklung Chan

In this talk we will discuss the basics of quantum computing based on chapter 1 of Ronald de Wolf's notes [1]. Classical computing is based on classical physics, including the important notions of locality and that systems can only exist in one state at a time, and bits, the basic objects of study, behave accordingly by taking on one of two states (0 or 1) and only changing when acted upon by a classical operation. On the other hand, quantum computing is based on quantum physics, which allows for nonlocal operations and superpositions of states, and qubits reflect these differences by taking on a superposition of states (0 and 1) and can be operated on by more complex operations. This leads to a richer theory of computing - in particular, quantum computing algorithms can work much faster and accomplish more complicated tasks than classical algorithms, for example Shor's algorithm for integer factorization. With this being said, much of the work on quantum computing is still theoretical as there are still many serious obstacles to effectively constructing physical quantum computers.

First, we introduce the notation and basic ideas of quantum mechanics as they relate to quantum computing. We use Dirac's bra-ket notation where a "bra" $\langle\cdot|$ represents a $1 \times n$ row vector and a "ket" $|\cdot\rangle$ represents an $n \times 1$ column vector. The point is that a "braket" ("bracket") correctly represents the inner product of two vectors. We will be intentionally ambiguous about exactly what we put in

place of the $\cdot$'s as we will often have to deal with complicated states and may need to abuse notation to simplify computations.

Typically we will use kets to represent states - for example, if we have N states we may denote them by $|0\rangle$, $|1\rangle$, ..., and $|N-1\rangle$ which are orthonormal basis vectors in some N-dimensional Hilbert space. Clasically, a system would only exist in one of these states at a given time but as we allow for superpositions in quantum mechanics, the state of a quantum system would be represented by:

$$|\Phi\rangle = \sum_{n=0}^{N-1} \alpha_n |n\rangle$$

Per the rules of quantum mechanics, the complex amplitudes $\alpha_n \in \mathbb{C}$ must represent a probability distribution in the sense that $\sum_{n=0}^{N-1} |\alpha_n|^2 = 1$. When we have multiple systems, we represent the state by the tensor product of these vectors. In particular, recall that if $\{|0\rangle, ..., |N-1\rangle\}$ is an orthonormal basis of the Hilbert space $\mathcal{H}_A$ and $\{|0\rangle, ..., |M-1\rangle\}$ is an orthonormal basis of the Hilbert space $\mathcal{H}_B$ then $\{|0\rangle \otimes |0\rangle, ..., |N-1\rangle \otimes |M-1\rangle\}$ is an orthonormal basis of the NM-dimensional Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

In quantum mechanics there are two basic operations that can be applied to a state. We can either measure the state, which yields a single classical state $|n\rangle$ with probability $|\alpha_n|^2$, or we can unitarily evolve the state, which yields a new quantum state. By the laws of quantum mechanics, only linear operations are allowed, i.e. matrix multiplication, and the probability must be preserved, i.e. unitary matrix multiplication.

For the purposes of computing, we will focus on systems of qubits where the state of each qubit is represented by a vector in a 2-complex-dimensional Hilbert space where the basis vectors are represented by $|0\rangle$ and $|1\rangle$. For shorthand, we will represent the tensor product of n of these basis vectors by:

$$|b_1\rangle \otimes |b_2\rangle ... \otimes |b_n\rangle = |b_1\rangle |b_2\rangle ... |b_n\rangle = |b_1 b_2 ... b_n\rangle$$

depending on the context, where $b_i \in \{0, 1\}$. It can also be useful to instead represent each of these basis vectors by an integer in $\{0, ..., 2^n - 1\}$. A key phenomenon in quantum computing is quantum entanglement, where the probabilities of each qubit being in state 0 or 1 are entangled with each other in the sense that as soon as one qubit is measured and it collapses into an observable classical state, the state of another qubit is immediately known as well. An example of this is an Einstein-Podolsky-Rosen (EPR) pair:

$$|\Phi\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

Here, if the first qubit is measured and found to be in the 0-state then the second qubit is immediately known to be in the 0-state as well (and similarly for the 1-state). These pairs are named after Einstein, Podolsky, and Rosen who studied their properties extensively. Formally, the state of a 2-qubit system is "entangled" if it cannot be writen as a tensor product $|\Phi_A\rangle \otimes |\Phi_B\rangle$.

We can then define and use gates, which are named in analogy with the same notion in classical computing. We will focus on gates used for systems of a small number of qubits (say 2 or 3 qubits). Each gate is a unitary matrix which acts upon quantum systems in particular ways. For example, the NOT gate which negates the state of a 1-qubit system is represented by the matrix:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

There are many interesting gates which we will discuss in more detail.

In particular, we will use these gates to demonstrate the process of quantum teleportation, which allows users to send qubits across space without measuring the state (which would destroy the superposition that it is in). Note that in this process, classical information still has to be sent so it is not the instantaneous teleportation depicted in science-fiction. This process combines lots of the ideas introduced previously and represents one of the many fascinating new possibilities of quantum computing as compared to classical computing.

References

[1] R. de Wolf, *Quantum Computing: Lecture Notes*, https://arxiv.org/abs/1907.09415

Jacobi matrices and Schrödinger operators

Rubén de la Fuente Fernández

We study an application of Schur's algorithm to prove spectral properties of Jacobi matrices that can be used to show results about the spectrum of Schrödinger operators on the discrete half-line.

In particular, we will focus our attention on the paper [DK04], which is devoted to studying spectral properties of half-line discrete Schrödinger operators with a Dirichlet boundary condition at the origin. Those operators take the form

$$[h_V\psi](n) = \psi(n+1) + \psi(n-1) + V(n)\psi(n) \tag{1}$$

with $\psi \in l^2(\mathbb{Z}^+)$, $\mathbb{Z}^+ = \{1, 2, ...\}$ and $\psi(0)$=0.

In the free case ($V = 0$), the spectrum of h_0 is $[-2, 2]$ and it is purely absolutely continuous. In [DK04] the authors give two results regarding the spectrum of h_V.

Theorem 1. [DK04, Theorem 1] *A discrete half-line Schrödinger operator h_V with spectrum contained in $[-2, 2]$ has purely absolutely continuous spectrum.*

Theorem 2. [DK04, Theorem 3] *If a discrete half-line Schrödinger operator h_V has only finitely many eigenvalues outside $[-2, 2]$, then it has purely absolutely continuous spectrum on $[-2, 2]$.*

In order to prove these theorems, the authors mainly use one result about the spectrum on Jacobi operators [DK04, Theorem 5], which will be the object of our attention. The proof of it strongly relies on the Schur algorithm and orthogonal polynomials in order to give a relation between the coefficients defining a Jacobi

operator and Schur's coefficients. They also prove natural analogues to Theorems 1 and 2 for the continuous setting, but we will focus on the discrete case.

Jacobi matrices and Schur coefficients

A Jacobi Matrix acting on the disrete half-line is an operator of the form

$$[J\psi](n) = a_n\psi(n+1) + a_{n-1}\psi(n-1) + b_n\psi(n)$$

with $\psi \in l^2(\mathbb{Z}^+)$, a_n positive and b_n real. Both coefficient sequences are assumed to be bounded, therefore J defines a bounded self-adjoint operator. Note that in the case $a_n = 1$, $b_n = V(n)$ this is just a Schrödinger operator of the form (1).
The result we will focus on, which corresponds to Section 2 in [DK04], is the following

Theorem 3. [DK04, Theorem 5] *A Jacobi matrix with coefficients a_n and b_n has spectrum $\sigma(J) \subseteq [-2, 2]$ if and only if there is a sequence $\gamma_n \in (-1, 1)$, $n \in \{0, 1, ...\}$, that obeys*

$$b_{n+1} = (1 - \gamma_{2n-1})\gamma_{2n} - (1 + \gamma_{2n-1})\gamma_{2n-2} \tag{2}$$

$$a_{n+1}^2 = (1 - \gamma_{2n-1})(1 - \gamma_{2n})^2(1 + \gamma_{2n+1}) \tag{3}$$

(Here $\gamma_{-1} = -1$, and the value of γ_{-2} is irrelevant since it is multiplied by zero.)

This sequence γ_n comprises exactly the coefficients of a Schur algorithm starting from a function which is constructed using a spectral measure of J. The authors of [DK04] devote Sections 3, 4, and 5 to prove bounds for the Schur coefficients associated with Jacobi matrices and use them together with Theorem 3 to show properties of the spectrum of Schrödinger operators and, in particular, Theorems 1 and 2.

Sketch of the proof of Theorem 3

The strategy of the proof starts with constructing the spectral measure of J associated with the vector $\delta_{1,n} \in l^2(\mathbb{Z}^+)$, the Kronecker delta function at 1, which we will denote $d\mu$. This vector is cyclic with respect to J, so the support of $d\mu$ coincides with the spectrum of J. From cyclicity we can also derive that J is unitarily equivalent to $g(x) \mapsto xg(x)$ in $L^2(d\mu)$. As $l^2(\mathbb{Z}^+)$ is infinite dimensional, $L^2(d\mu)$ is as well, therefore $d\mu$ must be supported in an infinite set.
We can also write the m-function of J using $d\mu$

$$m_0(z) = \int \frac{1}{t - z} d\mu(t).$$

First we assume $\sigma(J) \subseteq [-2, 2]$. Then, we can use $d\mu$ to define a measure on $\mathbf{S}^1$

$$\int g(t)d\mu(t) = \int g(\zeta + \zeta^{-1})d\rho(\zeta).$$

Next step is to construct a Schur function f_0 using the Carathéodory function F_0 associated with ρ

$$F_0(\xi) = \int \frac{\zeta + \xi}{\zeta - \xi} d\rho(\zeta) = (\xi - \xi^{-1})m_0(\xi + \xi^{-1}) \quad ; \quad f_0 = \frac{1}{\xi}\frac{F_0(\xi) - 1}{F_0(\xi) + 1}.$$

The fact that $d\mu$ is supported on an infinite set implies that f_0 cannot be written as a Blaschke product, allowing us to set up Schur's algorithm to construct the Schur coefficients for f_0

$$f_{n+1}(\xi) = \frac{1}{\xi}\frac{f_n(\xi) - \gamma_n}{1 - \bar{\gamma}_n f_n(\xi)},$$

with $\gamma_n = f_n(0)$ and $|\gamma_n| < 1$. The key observation is that the step in which we defined f_0 using $d\rho$ can be inverted, so we can define a different measure on $\mathbf{S}^1$ for each f_n we produce. These measures are then used to construct Carathéodory functions F_n, m-functions m_n and Jacobi matrices J_n. Relations (2) and (3) are obtained by computing the coefficients of J_{2n}.

For the converse direction of Theorem 3 we assume that the coefficients of J fulfill (2) and (3). Then we can construct a Schur function with these coefficients γ_n. With this function we construct a probability measure $d\tilde{\rho}$ on $\mathbf{S}^1$, which induces a probability measure on $[-2, 2]$, and therefore a Jacobi matrix $\tilde{J}$ with spectrum contained in $[-2, 2]$. But as the coefficients of $\tilde{J}$ are also determined by (2) and (3), then $\tilde{J} = J$ and $\sigma(J) = \sigma(\tilde{J}) \subseteq [-2, 2]$.

Theorem 3 is not new to [DK04], it already appeared in [G54]. However, the authors of [DK04] present a short, clear and self-contained proof that explicitly relies on the Schur algorithm and the shape of Jacobi operators.

References

[DK04] D. Damanik and R. Killip, *Half line Schrödinger operators with no bound states.* Acta Math., 193(1):31–72, 2004.

[G54] Ya. L. Geronimus, *Polynomials Orthogonal on a Circle and Their Applications.* Amer. Math. Soc. Translation **104**, AMS, Providence, RI, 1954.

The Nonlinear Fourier Transform on $\ell^2(\mathbf{Z})$

Max Giessler

In this talk we extend the definition of the NLFT to square summable sequences on the full line and discuss some of its properties, following lecture 3 of Tao's and Thiele's lecture notes [2]. In particular, we are concerned with its invertibility properties.

For a sequence $F \in \ell^2(\mathbf{Z}_{\leq -1}, D)$ supported on the negative integers and taking values in the complex disc D we define its NLFT to be

$$\widehat{F}(z) := (a^*(z^{-1}), b(z^{-1})), \quad z \in \mathbf{T},$$

where (a, b) is the NLFT of the reflected sequence in $\ell^2(\mathbf{Z}_{\geq 1}, D)$ as defined in the previous talk. Recall that the NLFT is a homeomorphism from $\ell^2(\mathbf{Z}_{\geq 0}, D)$ to $\mathbf{H}$, defined to be the space of all $SU(1,1)$-valued functions (a, b) such that a satisfies an outerness condition and a normalization condition at ∞, and b/a^* satisfies a holomorphicity condition (see [1] for details on the underlying complex analysis). Analogously, we define $\mathbf{H}_0^*$, replacing the holomorphicity condition with one for

b/a and additionally requiring that $b(\infty) = 0$. By the shifting property (Lemma 1 (5) in [2]) one can deduce that the NLFT extends to a homeomorphism from $\ell^2(\mathbf{Z}_{\leq -1}, D)$ to $\mathbf{H}_0^*$. Intuitively, the NLFT is a bijection on both half-lines.

Now we define the NLFT of a sequence $F \in \ell^2(\mathbf{Z}, D)$ to be the $SU(1,1)$-valued measurable function on $\mathbf{T}$ given by the matrix product

$$\overbrace{F}(z) := \overbrace{F^{\leq -1}}(z)\,\overbrace{F^{\geq 0}}(z), \tag{1}$$

where $F^{\leq -1} \in \ell^2(\mathbf{Z}_{\leq -1}, D)$ and $F^{\geq 0} \in \ell^2(\mathbf{Z}_{\geq 0}, D)$ denote the truncations of the sequence F to its negative and non-negative entries, respectively. In line with the earlier notation, we also write $(a, b) = (a_- b_-)(a_+ b_+)$ for (1). Observe that we modified the definition of the NLFT on the half-line in accordance with Lemma 1 in [2] to gain a definition for the full-line. Therefore by construction, the NLFT on the full-line still satisfies Lemma 1 and is consistent with the definition of the NLFT on $\ell^p(\mathbf{Z})$ for $1 \leq p < 2$. In a way, until now we have only harvested the fruit from our work on the half-line.

Further investigation shows that the NLFT maps $\ell^2(\mathbf{Z}, D)$ into the space $\mathbf{L}$ and is continuous. The Plancherel identity

$$\int_{\mathbf{T}} \log|a(z)| = -\frac{1}{2} \sum_{z \in \mathbf{Z}} \log(1 - |F_n|^2)$$

carries over. However, bijectivity is lost: Indeed, the NLFT in *not* injective on $\ell^2(\mathbf{Z}, D)$.

This insight leads the way to the inverse problem with which we shall concern ourselves for the remainder of the talk. We want to find a (not necessarily unique) preimage for a given function $(a, b) \in \mathbf{L}$, i.e. a sequence $F \in \ell^2(\mathbf{Z}, D)$ with NLFT (a, b). By the half-line theory, this boils down to finding a matrix factorization

$$(a, b) = (a_- b_-)(a_+ b_+) \quad \text{with } (a_- b_-) \in \mathbf{H}_0^* \text{ and } (a_+ b_+) \in \mathbf{H}. \tag{2}$$

That is because any such factorization is the NLFT of uniquely determined truncations $F^{\leq -1}$ and $F^{\geq 0}$ of a sequence $F \in \ell^2(\mathbf{Z}, D)$ as the NLFT is a bijection on the half-lines. Keeping in mind this equivalence between finding a preimage for the NLFT and finding a factorization as in (2) is worth it.

The factorization problem (2) of a matrix-valued function on $\mathbf{T}$ is called *Riemann-Hilbert problem*. It is possible to rewrite it as a product of functions on D and D^*, respectively, obtaining the classical formulation of the R-H problem modulo outerness, normalization, and holomorphicity constraints (this is done in [2]).

We can recover injectivity of the NLFT or, equivalently, prove the uniqueness of any R-H factorization if we additionally assume a to be bounded:

Theorem 1 ([2], Lemma 18)**.** *For a function $(a, b) \in \mathbf{L}$ where a is bounded there is a* unique *$F \in \ell^2(\mathbf{Z}, D)$ such that $\overbrace{F} = (a, b)$.*

The proof relies upon the Banach fixed-point theorem. W.l.o.g. we can assume that a_+, b_+^*, a_-, b_- lie in the Hardy space of square-integrable functions $H^2(D^*)$.

We can show that the factor (a_+, b_+) in any R-H factorization must be a fixed point of the map

$$(A, B) \mapsto (c + P_{D^*}(Bb^*/a^*), P_D(Ab/a)) \tag{3}$$

mapping $L^2(\mathbf{T}) \times L^2(\mathbf{T})$ into itself. Here, P_D and P_{D^*} are the orthogonal projections from the Hilbert space $L^2(\mathbf{T})$ to $H^2(D)$ and $H_0^2(D^*)$, respectively, and c is a uniquely determined constant. Crucially, to prove that (3) is a contraction we need that a is bounded. Then we obtain as the unique fixed point (a_+, b_+) and the corresponding factor (a_-, b_-) by rewriting (2):

$$(a_-, b_-) = (a, b)(a_+^*, -b_+). \tag{4}$$

This shows the uniqueness of the R-H factorization and therefore of the inverse.

The general case of unbounded a is more complicated. In particular, we cannot prove the uniqueness of the preimage anymore. Let us fix a function $(a, b) \in \mathbf{L}$. Instead of using the Banach fixed-point theorem, we apply the Riesz representation theorem to the functional $\lambda : (A, B) \mapsto \mathrm{Re}[A(\infty)]$ on the Hilbert spaces H_{min} and H_{max}. These are nested in between

$$H^2(D^*) \times H^2(D) \subseteq H_{min} \subsetneq H_{max} \subseteq aH^2(D^*) \times a^* H^2(D)$$

and equipped with the scalar product $\langle (A', B'), (A, B) \rangle := \int_{\mathbf{T}} \mathrm{Re}[A'(A^* - \frac{b}{a}B^*) + (B')^*(B - \frac{b}{a}A)]$. Let (A_{min}, B_{min}) be the unique element in H_{min} which represents λ in this scalar product and likewise (A_{max}, B_{max}). In this setting, we can prove the following general result for the inverse problem:

Theorem 2 ([2], Theorem 7)**.** *Let $(a, b) \in \mathbf{L}$. Then there exists a R-H factorization (2). Two possible choices are given by*

$$(a_+, b_+) = (A_{min}, B_{min}) A_{min}(\infty)^{-1/2} \quad \textit{and}$$
$$(a_+, b_+) = (A_{max}, B_{max}) A_{max}(\infty)^{-1/2}$$

where in each case (a_-, b_-) is determined as in (4).

While we approached the proof of Theorem 1 from the point of view of the R-H problem, here we take the perspective of finding a preimage for the NLFT. We sketch the proof for H_{min}. Let H_n for all $n \in \mathbf{Z}$ be a particular family of Hilbert spaces such that $H_0 = H_{min}$ and $H_{n+1} \subseteq H_n$ (see [2] for details). For each integer n let (A_n, B_n) be the Riesz representer of the functional λ in H_n. Then we can deduce the relation

$$(A_{n+1}, B_{n+1}) = (A_n, B_n) - F_n(B_n^* z^n, A_n^* z^n)$$

for uniquely determined complex numbers F_n in the unit disc D. It remains to verify that the sequence $F := (F_n)_{n \in \mathbf{Z}}$ is indeed in $\ell^2(\mathbf{Z}, D)$ and that its NLFT is (a, b). Finally, the NLFT of its truncation $\overbrace{F^{\geq 0}} = (a_+, b_+)$ is of the required form. Note that we can imitate this proof for H_{max} and thus obtain another, different sequence $\tilde{F}$ with NLFT (a, b).

Taking the point of view of the R-H problem again the underlying reason for the loss of uniqueness in Theorem 2 turns out the be the following:

Theorem 3 ([2], Theorem 8)**.** *Let* $(a,b) \in \mathbf{L}$*. Then there exists a* unique *factorization*

$$(a,b) = (a_{--},b_{--})(a_o,b_o)(a_{++},b_{++})$$

with $(a_{--},b_{--}) \in \mathbf{H}_0^*$, $(a_o,b_o) \in \mathbf{H}_0^* \cap \mathbf{H}$, $(a_{++},b_{++}) \in \mathbf{H}$*. Furthermore,* (a_{--},b_{--}) *and* (a_{++},b_{++}) *only admit the trivial R-H factorizations* $(a_{--},b_{--}) = (a_{--},b_{--})(1,0)$ *and* $(a_{++},b_{++}) = (1,0)(a_{++},b_{++})$*.*

Because the factor (a_o,b_o) is in both the spaces $\mathbf{H}_0^* \cap \mathbf{H}$ we can multiply it with either factor (a_{--},b_{--}) or (a_{++},b_{++}) and stay within the spaces $\mathbf{H}_0^*$ or $\mathbf{H}$ by the group structure of $SU(1,1)$. In this way, we obtain different R-H factorizations (2) and consequently different preimages for (a,b).

References

[1] J.B. Garnett, *Bounded Analytic Functions*, Springer New York (2007).
[2] T. Tao and C. Thiele, *Nonlinear Fourier Analysis*, arXiv: 1201.5129 [math.CA] (2012).

The circuit model of quantum computing

Massimiliano Incudini

In quantum computing, the de facto standard model of computation is the circuit model, which can be derived by generalizing the classical circuit model.

A *Boolean circuit* is a directed acyclic graph where each vertex is either an input, an output, or a computational node representing the logical gates AND, OR, NOT, or COPY, and it computes a function $f : \{0,1\}^n \to \{0,1\}^m$. Using these gates, we can implement any Boolean function, making this set of gates *universal* for Boolean computation. A sequence of such circuits, one for each input size n, is called a *circuit family* $\mathcal{C} = \{C_n : \{0,1\}^n \to \{0,1\}\}$, and it is denoted as *uniformly polynomial* if there exists a deterministic Turing machine that outputs the description of C_n using $\mathcal{O}(\log n)$ space. The condition of being uniformly polynomial ensures that there is an efficient way to construct each circuit C_n based on the input size, avoiding the need to manually specify each circuit for different sizes; the requirement of $\log n$ space ensures that the Turing machine generates circuits running in poly n time.

In the context of computational complexity, a *decision problem* L is a subset of $\{0,1\}^* = \cup_{n=0}^{\infty}\{0,1\}^n$, where each binary string represents an instance of the problem. A decision problem L is in the class P if there exists a uniformly polynomial circuit family $\mathcal{C} = \{C_n\}$ such that for every input $x \in \{0,1\}^n$, the circuit C_n outputs 1 if $x \in L$ and 0 otherwise.

Extending this concept, a *randomized circuit family* is a circuit family $\mathcal{C} = \{C_n\}$ where each circuit C_n is provided with $\mathcal{O}(\text{poly}(n))$ random bits in addition to its input. A decision problem L is in the class BPP if there exists a uniformly polynomial randomized circuit family such that for all $x \in \{0,1\}^n$, the probability that $C_n(x) = 1$ is at least $\frac{2}{3}$ if $x \in L$, and at most $\frac{1}{3}$ if $x \notin L$.

In the quantum setting, a *quantum circuit family* $\mathcal{C} = \{C_n\}$ consists of circuits where each gate corresponds to a unitary transformation on a few qubits. Notable quantum gates include

$$X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \qquad Y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right) \qquad Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \qquad H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$$
$$S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right) \qquad T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{smallmatrix}\right) \qquad \text{CNOT} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) \otimes \mathbb{I} + \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \otimes X$$

The set $\{H, S, \text{CNOT}\}$ is universal for quantum computation. The Solovay-Kitaev theorem guarantees that any m-qubit unitary transformation can be approximated up to precision ϵ with $\text{poly}(m \log(m\epsilon^{-1}))$ gates from any universal set. The operations are composed in parallel via the tensor product and in sequence via matrix multiplication. The computation ends with a measurement on the computational basis, yielding a probabilistic result. A decision problem L is in the class BQP if there exists a uniformly polynomial family of quantum circuits $\mathcal{C} = \{Q_n\}$ such that for all $x \in \{0,1\}^n$, the probability that $Q_n(x) = 1$ is at least $\frac{2}{3}$ if $x \in L$, and at most $\frac{1}{3}$ if $x \notin L$.

We can now present some quantum algorithms outperforming their classical analog. These algorithms are best analyzed in the *query model*.

The query model differs from the standard model: the input $x \in \{0,1\}^N$, with $N = 2^n$, is provided as a black-box oracle O_x. This oracle is a unitary operator over $n+1$ qubits, whose action is given by $O_x |i\rangle |b\rangle = |i\rangle |b \oplus x_i\rangle$. A single application of the oracle is called a query, and it is represented in the quantum circuit similarly to other gates. The query complexity model conveniently illustrates an *exponential separation* between classical and quantum computation in certain tasks. For instance, any (uniformly polynomial) classical circuit would require exponentially many queries (in the input size n), whereas its quantum analog would require only a polynomial number of queries. A slightly different form of the oracle, implementing $O_x^{\pm} |i\rangle = (-1)^{x_i} |i\rangle$, is sometimes used and referred to as a phase oracle.

Two problems exemplify a significant separation between classical and quantum computational capabilities. The first is the Deutsch-Jozsa problem, which involves determining whether a function f, defined over n bits (represented as a lookup table $x \in \{0,1\}^N$, with $N = 2^n$), is either balanced (where half the outputs are zero and the other half are one) or constant, under the promise that it is one of the two [1]. The Deutsch-Jozsa algorithm is a quantum algorithm that begins with the state $|0^n\rangle$, applies the unitary operation $H^{\otimes n} O_x^{\pm} H^{\otimes n}$, and then performs a measurement in the computational basis. The state just before measurement is:

$$\begin{aligned} H^{\otimes n} O_x^{\pm} H^{\otimes n} |0^n\rangle &= H^{\otimes n} 2^{-n/2} \sum_{i \in \{0,1\}^n} (-1)^{f(i)} |i\rangle \\ &= 2^{-n/2} \sum_{i \in \{0,1\}^n} (-1)^{f(i)} \sum_{j \in \{0,1\}^n} (-1)^{i \cdot j} |j\rangle \end{aligned}$$

The amplitude of the state $|0\rangle$ reveals the result: zero for balanced functions and ± 1 for constant functions. Thus, only a single query is needed. In contrast, classical computation would require at least $2^{n/2}+1$ queries. However, a randomized classical algorithm can find the result with a small error probability using a constant number of queries.

The second example is the Bernstein-Vazirani problem. Here, for $N = 2^n$ and $x \in \{0,1\}^N$, there exists an $a \in \{0,1\}^n$ such that $x_i = (i \cdot a) \mod 2$ [2]. The Bernstein-Vazirani algorithm uses the same quantum circuit as the Deutsch-Jozsa algorithm, where $x_i = i \cdot a$. Consequently, the second application of $H^{\otimes n}$ leads to the computational state $|a\rangle$:

$$H^{\otimes n} O_x^{\pm} H^{\otimes n} |0^n\rangle = 2^{-n/2} \sum_{i,j \in \{0,1\}^n} (-1)^{i \cdot a + i \cdot j} |j\rangle = |a\rangle$$

For this problem, it has been proven that any classical or randomized algorithm requires at least $\mathcal{O}(n)$ queries to obtain the result with a small error probability, whereas the quantum algorithm achieves the result with only a single query.

References

[1] D. Deutsch and R. Jozsa *Rapid solution of problems by quantum computation*, Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences **439.1907** (1992), 553–558.

[2] E. Bernstein and U. Vazirani, *Quantum complexity theory*, SIAM Journal on Computing, 26.5 (1997), 1411–1473.

Simon's algorithm

Miriam Kosik

1. Introduction

Simon's algorithm, invented by Daniel Simon in 1994, was the first quantum algorithm to show an exponential speed-up over the best classical algorithm for a given problem (in this case - for Simon's problem). Its importance also stems from the fact that it served as direct inspiration for Peter Shor to create his famous quantum factoring algorithm.

2. Simon's problem statement

Let us start by presenting the problem considered by Simon. A black box (oracle) is given which implements a function from n-bit binary strings into n-bit binary strings, i.e. $f : \{0,1\}^n \to \{0,1\}^n$ such that for all $x, y \in \{0,1\}^n$:

$$f(x) = f(y) \quad \text{iff} \quad x = y \ \text{ or } \ x = y \oplus s. \tag{1}$$

Here, s denotes an n-bit binary string which is considered to be a hidden property of the oracle and $\oplus$ denotes addition modulo 2.

Note that f can either be 2-to-1 (if $s \neq 000...0$) or 1-to-1 (if $s = 000...0$). The essence of Simon's problem is to determine whether $s = 000...0$ is the only solution

that fulfils condition (1), querying the oracle as few times as possible. If the trivial all-zero solution is not the only one, the goal is also to find a non-trivial solution s.

2.1. **Example of Simon's oracle with s equals 101.** Let us look at an example of a function $f(x)$ which satisfies Eq. (1). It is presented as a table of values on the left side in Table 1.

Input: x	Output: $f(x)$
000	000
001	001
010	010
011	011
100	001
101	000
110	011
111	010

Input: $\|x\rangle$	Output: $U_f \|x\rangle$
$\|000\,000\rangle$	$\|000\,000\rangle$
$\|001\,000\rangle$	$\|001\,001\rangle$
$\|010\,000\rangle$	$\|010\,010\rangle$
$\|011\,000\rangle$	$\|011\,011\rangle$
$\|100\,000\rangle$	$\|100\,001\rangle$
$\|101\,000\rangle$	$\|101\,000\rangle$
$\|110\,000\rangle$	$\|110\,011\rangle$
$\|111\,000\rangle$	$\|111\,010\rangle$

TABLE 1. On the left: the action of a classical Simon's oracle $f(x)$ with the hidden string $s = 101$. On the right: the action of a quantum counterpart of f, denoted as U_f.

Let us consider how one could create a quantum oracle that implements $f(x)$. We need to keep in mind one important fact - quantum operations must be reversible. To ensure this, we make the quantum oracle act on one input register (denoted $|x_i\rangle$) but store the output in a separate register (denoted $|x_o\rangle$):

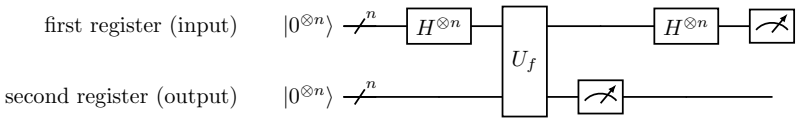
$$f(x) = y \quad \longrightarrow \quad U_f \,|x_i\rangle\,|x_o\rangle = |x_i\rangle\,|x_o \oplus y\rangle\,. \tag{2}$$

In this way, the input qubits are never changed and we are guaranteed to get different outputs for different input values. On the right in Table 1, we can see the action of the quantum counterpart of f on a selected subset of all possible inputs. In general, the action on U_f is defined for all possible binary strings as input values in the second register but for simplicity we will always assume that the second register is initialized in an all-zero state.

3. Solving Simon's problem

3.1. **Classical approach.** How would one approach the problem in a classical setting? A simple idea is to query the oracle by providing it with random strings as input, store the input-output pairs and repeat this procedure until you find a repeating output. This is analogous to the *birthday problem* since finding any pair of matching outputs is enough to determine the answer. Hence, on average $\Omega(\sqrt{2^n})$ queries are needed to recover s. One can also show that this is the best classically achievable complexity for this problem (see [1]).

3.2. **Quantum algorithm (Simon's algorithm).** The quantum circuit to solve Simon's problem is presented below.



The initial state of the system consists of all qubits in state $|0\rangle$. First, a Hadamard transform is applied to all qubits in the first register:

$$\left|0^{\otimes n}\right\rangle \left|0^{\otimes n}\right\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)^{\otimes n} \left|0^{\otimes n}\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \left|0^{\otimes n}\right\rangle \tag{3}$$

Next, the query to the oracle is made, which causes the second register to change:

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \left|0^{\otimes n}\right\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle |f(x)\rangle \tag{4}$$

Next, we measure the second register. This will yield some particular value of $f(x)$ as a result. Let us denote the possible arguments that yield that value x_m and $x_m \oplus s$, and the measured result is then $f(x_m)$.

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle |f(x)\rangle \xrightarrow[\text{2nd register}]{\text{measurement of}} \frac{1}{\sqrt{2}}(|x_m\rangle + |x_m \oplus s\rangle) |f(x_m)\rangle \tag{5}$$

We will now ignore the second register and again apply Hadamard transforms to the first n qubits:

$$\begin{aligned}
&\frac{1}{\sqrt{2}}(|x_m\rangle + |x_m \oplus s\rangle) |f(x_m)\rangle \xrightarrow{H^{\otimes n}} \\
&\qquad \frac{1}{\sqrt{2^{n+1}}} \left(\sum_{j\in\{0,1\}^n} (-1)^{x_m\cdot j} |j\rangle + \sum_{j\in\{0,1\}^n} (-1)^{(x_m\oplus s)\cdot j} |j\rangle \right) = \\
&\qquad = \frac{1}{\sqrt{2^{n+1}}} \sum_{j\in\{0,1\}^n} (-1)^{x_m\cdot j} \left(1 + (-1)^{s\cdot j}\right) |j\rangle \,. \qquad (6)
\end{aligned}$$

As a result, we obtain a superposition of states labelled $|j\rangle$, which have a non-zero amplitude if and only if $s \cdot j \bmod 2 = 0$. Hence, measuring state $|j\rangle$ and receiving as a result the some value j gives information about s. Precisely, it gives a random element from the set $\{j \mid s \cdot j \bmod 2 = 0\}$ - we get a linear equation that involves s.

We repeat the quantum part multiple times until we get a system of $n-1$ linear equations. This system will have either one or two solutions. If $f(x)$ is 1-to-1, the only solution will be the all-zero string 000....0. If it is 2-to-1, there will be another non-trivial for solution s. Such a system of linear equations can be solved efficiently using a classical algorithm, e.g. Gaussian elimination, which has runtime $\mathrm{O}(n^3)$ for an $n \times n$ system of equations. Hence, the overall complexity

of the quantum algorithm is $O(n)$ oracles queries and polynomially many other operations.

References

[1] R. de Wolf, *Quantum Computing: Lecture Notes* [v5], arXiv:1907.09415v5, 2023.
[2] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, 2011.

Appendix A. Appendix - Simon's oracle implementation

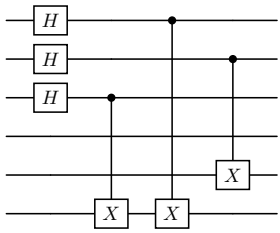
In the oracle computation model, an oracle is an operation that has some property which is hidden from the rest of the world. The term *black box* is also often used equivalently. It is an object that takes some input, returns an output but you have no access or information about what is happening inside. The goal of most quantum algorithms is to query the black box, analyze its outputs and in this way - retrieve the hidden information.

In reality, we cannot look into the oracle. However, to simulate quantum algorithms, one needs to implement a model of the oracle. Below, the implementation steps, an exemplary circuit and an a Qiskit implementation of Simon's oracle are given.

Implementation steps:

- copy the contents of first register onto the second one (using CNOT gates),
- if s is not all equal zero, find the smallest index j for which $s_j = 1$. If $x_j = 0$, then XOR the second register with s. Otherwise, do not do anything.

Circuit for the Simon's oracle hiding string $s = 101$.



Qiskit implementation of the Simon's oracle hiding string s.

```python
from qiskit import QuantumCircuit

def simon_oracle(s):

    qc = QuantumCircuit(2*len(s))
    least_1_found = False
    for idx, i in enumerate(s):

        # find the smallest index j for which s_j is 1
        if i == "1" and not least_1_found:
            least_1_idx = idx
            least_1_found = True

        # copy contents of 1st register onto second
        qc.cx(idx, idx + len(s))

    for idx, i in enumerate(s):
        if i == "1" and least_1_found:
            qc.cx(least_1_idx, idx + len(s))

    return qc
```

Quantum Singular Value Transformation

James Berkeley Larsen

1. Introduction

In this report, we introduce the quantum singular value transformation (QSVT). We mainly base the content on these notes by András Gilyén and §3.1-3.3 of [1].

The basic idea of QSVT is to combine methods from quantum signal processing (QSP) with block-encoding to construct a quantum circuit that can perform polynomial transformations of the singular values of arbitrary rectangular matrices. This seemingly abstract task has been shown to provide a unifying framework for all major quantum algorithms, somehow capturing the speedups present in search, phase estimation, and Hamiltonian simulation [2].

2. The Heart of the QSVT

Let $U \in \mathbb{C}^{N\times N}$ be a block-encoding of A as follows:

$$U = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where A and D may be rectangular with different dimensions. Let Π and Π' be the orthogonal projectors such that $A = \Pi' U \Pi$ and $D = (I - \Pi')U(I - \Pi)$. Let us also define the following operators:

$$Z_\Pi(\phi) := e^{i\phi}\Pi + e^{-i\phi}(I - \Pi), \tag{1}$$

$$U_\Phi := Z_{\Pi^{(\prime)}}(\phi_d) \cdots U^\dagger \cdot Z_{\Pi'}(\phi_3) \cdot U \cdot Z_\Pi(\phi_2) \cdot U^\dagger \cdot Z_{\Pi'}(\phi_1) \cdot U \cdot Z_\Pi(\phi_0), \tag{2}$$

where $\Phi = (\phi_0, \phi_1, \phi_2, \ldots, \phi_d)$. Note that Eq. (1) has a straightforward implementation on a quantum computer using Z rotation gates on an ancillary qubit. The heart of the QSVT is the fact that Eq. (2) applies a polynomial transformation to the singular values of A and D. More concretely,

$$U_\Phi = \begin{cases} \begin{pmatrix} AP(A^\dagger A) & BQ^*(D^\dagger D) \\ CQ(A^\dagger A) & DP^*(D^\dagger D) \end{pmatrix} & \text{for } d \text{ odd} \\ \begin{pmatrix} P(A^\dagger A) & C^\dagger DQ^*(D^\dagger D) \\ B^\dagger AQ(A^\dagger A) & P^*(D^\dagger D) \end{pmatrix} & \text{for } d \text{ even,} \end{cases} \tag{3}$$

for some $P, Q \in \mathbb{C}[x]$ with $\deg(P) \leq \frac{d}{2}$ and $\deg(Q) \leq \frac{d-1}{2}$. In §3, we will provide an inductive derivation of Eq. (3) to reveal a recurrence relation that defines the polynomials P and Q. We will then conclude in §4 by showing how to choose the angles Φ given some polynomial P.

3. Derivation of Polynomial Recurrence Relations

For the base case of our inductive derivation, notice that when $d = 0$,

$$U_{(\phi_0)} = Z_\Pi(\phi_0) = \begin{pmatrix} e^{i\phi_0} I & 0 \\ 0 & e^{-i\phi_0} I \end{pmatrix},$$

i.e., $P \equiv e^{i\phi_0}$ and $Q \equiv 0$. These (constant) polynomials will also serve as the base case for our recurrence relations.

We let $[P(x)|x = M^{(SV)}]$ denote the application of a polynomial P to the singular values of a matrix $M = \sum_i \sigma_i |\phi_i\rangle\langle\psi_i|$, i.e., $P(M^\dagger M) = [P(x^2)|x = M^{(SV)}]$ and $MP(M^\dagger M) = [xP(x^2)|x = M^{(SV)}]$. We only treat the case for even d, the odd case can be derived using the same steps. Let $P_\Phi(x) := P(x^2)$ and $Q_\Phi(x) := xQ(x^2)$. By the assumed unitarity of U,

$$I = UU^\dagger = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \begin{pmatrix} A^\dagger & C^\dagger \\ B^\dagger & D^\dagger \end{pmatrix} = \begin{pmatrix} AA^\dagger + BB^\dagger & AC^\dagger + BD^\dagger \\ CA^\dagger + DB^\dagger & CC^\dagger + DD^\dagger \end{pmatrix}. \tag{4}$$

We then can derive that

$$Z_{\Pi'}(-\phi_{d+1}) \cdot U_{(\phi_0,\phi_1,\cdots,\phi_d,\phi_{d+1})} = U \cdot U_\Phi$$

$$= \begin{pmatrix} A & B \\ C & D \end{pmatrix} \cdot \begin{pmatrix} [P_\Phi(x)|x = A^{(SV)}] & C^\dagger \cdot [Q^*_\Phi(x)|x = D^{(SV)}] \\ B^\dagger \cdot [Q_\Phi(x)|x = A^{(SV)}] & [P^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix} \tag{5}$$

$$= \begin{pmatrix} [xP_\Phi(x) + (1-x^2)Q_\Phi(x)|x = A^{(SV)}] & B \cdot [P^*_\Phi(x) - xQ^*_\Phi(x)|x = D^{(SV)}] \\ C \cdot [P_\Phi(x) - xQ_\Phi(x)|x = A^{(SV)}] & [xP^*_\Phi(x) + (1-x^2)Q^*_\Phi(x)|x = D^{(SV)}] \end{pmatrix}, \tag{6}$$

where $\Phi = (\phi_0, \cdots, \phi_d)$, Eq. (5) invokes the inductive hypothesis, and Eq. (6) uses the four matrix identities provided by Eq. (4).

We have thus arrived at the following recurrence relations for the polynomials P_Φ and Q_Φ:

$$d = 0: \quad P_{(\phi_0)} = e^{i\phi_0},\ Q_{(\phi_0)} = 0,$$

$$d \to d+1:$$

$$\begin{cases} P_{(\phi_0,\phi_1,\cdots,\phi_d,\phi_{d+1})} = e^{i\phi_{d+1}} \left[xP_{(\phi_0,\phi_1,\cdots,\phi_d)}(x) + (1-x^2)Q_{(\phi_0,\phi_1,\cdots,\phi_d)}(x) \right], \\ Q_{(\phi_0,\phi_1,\cdots,\phi_d,\phi_{d+1})} = e^{-i\phi_{d+1}} \left[P_{(\phi_0,\phi_1,\cdots,\phi_d)}(x) - xQ_{(\phi_0,\phi_1,\cdots,\phi_d)}(x) \right]. \end{cases}$$

Note that P_Φ and Q_Φ have opposite but well-defined parity. Note that for even d, the original P and Q polynomials from Eq. (3) satisfy $P(x) = P_\Phi(\sqrt{x})$ and $Q(x) = \frac{1}{\sqrt{x}} Q_\Phi(\sqrt{x})$ (the case for odd d is similar).

4. Choosing Angles for a Polynomial

In §3, we derived what polynomial transforms would be accomplished by Eq. (3) given some angles Φ. It is important to note that the angles determine the polynomials independent of the choice or dimensions of sub-blocks of U. Specifically, QSP considers the simple case when U is 2×2. For example, if $U =$

$\begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix}$, we have that $U_\Phi = \begin{pmatrix} P_\Phi(x) & \sqrt{1-x^2}Q^*_\Phi(-x) \\ \sqrt{1-x^2}Q_\Phi(x) & P^*_\Phi(-x) \end{pmatrix}$. Enforcing unitarity of U_Φ in this case gives us an additional requirement that

$$|P_\Phi(x)|^2 + (1-x^2)|Q_\Phi(x)|^2 = 1 \quad \forall x \in [-1,1]. \tag{7}$$

We can now try to reverse the process and derive the angles given two polynomials P and Q with $\deg(P) = \deg(Q) + 1$. Given the recurrence relations P_Φ and Q_Φ must eventually satisfy, the leading coefficients p_d and q_{d-1} must have the same magnitude, so let $\phi_d := \frac{1}{2i}(\ln p_d - \ln q_{d-1})$ (i.e. $e^{2i\phi_d} = p_d/q_{d-1}$). Next, let $\tilde{P}(x)$ and $\tilde{Q}(x)$ be defined as follows:

$$\begin{pmatrix} \tilde{P}(x) \\ \sqrt{1-x^2}\tilde{Q}(x) \end{pmatrix} = \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix} \cdot \begin{pmatrix} e^{-i\phi_d} & 0 \\ 0 & e^{i\phi_d} \end{pmatrix} \cdot \begin{pmatrix} P(x) \\ \sqrt{1-x^2}Q(x) \end{pmatrix}.$$

A straightforward matrix computation reveals that the leading coefficients cancel out, resulting in $\deg(\tilde{P}) = \deg(P) - 1$ and $\deg(\tilde{Q}) = \deg(Q) - 1$. Therefore, the process can be iterated d times to find $\phi_{d-1}, ..., \phi_0$, with each iteration decreasing the degree of the target polynomials.

Often, a practitioner only cares about applying a real polynomial transformation $P \in \mathbb{R}[x]$ to the singular values of the A block of U. In this case, one can find a corresponding $\hat{P}_\Phi$ with $\mathcal{R}(\hat{P}_\Phi) = P_\Phi$ and $\hat{Q}_\Phi$ satisfying the stringent form of the recurrence relations if and only if:

$$|P_\Phi(x)| \leq 1 \quad \forall x \in [-1,1]. \tag{8}$$

Therefore, one need only check the condition from Eq. (8) to guarantee that suitable angles can be found for the desired transformation.

References

[1] A. Gilyén, Y. Su, G. Low, and N. Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC '19. ACM, June 2019.

[2] J. Martyn, Z. Rossi, A. Tan, and I. Chuang. Grand unification of quantum algorithms. *PRX Quantum*, 2(4), December 2021.

The nonlinear Fourier transform, square integrable on half line

Ricardo Motta

1. Introduction

As established in [1, Lecture 1], given $F = \{F_n\}_{n\in\mathbb{Z}}$ a finite sequence, we recursively define $\begin{pmatrix} a_n & b_n \end{pmatrix} := \begin{pmatrix} a_{n-1} & b_{n-1} \end{pmatrix} T_n$, where

$$T_n = \frac{1}{\sqrt{1-|F_n|^2}} \begin{pmatrix} 1 & F_n z^n \\ \overline{F_n} z^{-n} & 1 \end{pmatrix} \tag{1}$$

and[1] $\begin{pmatrix} a_{-\infty} & b_{-\infty} \end{pmatrix} = \begin{pmatrix} 1 & 0 \end{pmatrix}$. The nonlinear Fourier transform of this sequence F is the pair of functions $(a(z), b(z))$ in the parameter $z \in \mathbb{T}$, where a_n and b_n are equal to a and b for sufficiently large positive n. We denote the NLFT of F as

$$\overbrace{F}(z) = (a(z), b(z)).$$

The goal of [1, Lecture 2] is to extend the nonlinear Fourier transform (NLFT) to square-summable sequences supported on the right half-line, with values in $\mathbb{D}$, and to prove that it defines a homeomorphism between this space and another space $\mathbf{H}$, which can be explicitly described.

The challenge arises from the fact that this transform for finite sequences is an infinite product of transfer matrices (1), whose pointwise convergence is not guaranteed here. To overcome this, we proceed by approximation arguments using Cauchy sequences and some tools of complex analysis.

2. Extension to half-line square summable sequences

The authors' approach is to draw parallels with classical Fourier analysis, and the first ingredient is the extension of Plancherel's Theorem to this context.

Lemma 1. *Let $F = \{F_n\}_{n\in\mathbb{Z}}$ be a finite sequence of elements in the unit disc. Consider the nonlinear transform of F, denoted by $\overbrace{F} = (a, b)$. Then,*

$$\frac{1}{2}\int_{\mathbb{T}} \log\big(1 + |b(z)|^2\big)\, dz = \int_{\mathbb{T}} \log|a(z)|\, dz = -\frac{1}{2}\sum_n \log\big(1 - |F_n|^2\big). \tag{2}$$

Similar to the linear Fourier Transform in L^2, the Plancherel identity in (2) will be a fundamental key to define the NLFT of $F \in \ell^2(\mathbb{Z}_{\geq 0}, \mathbb{D})$ as a limit of a Cauchy sequence in some appropriate space $\mathbf{H}$.

To construct this space, we first consider $\mathbf{K}$ to be the space of all measurable functions $(a(z), b(z)) \in SU(1,1)$ on the circle with $\log|a(z)| \in L^1(\mathbb{T})$. We can embed this space into the space $L^1(\mathbb{T}) \times L^2(\mathbb{T}) \times L^2(\mathbb{T})$ by mapping the function (a, b) to the function $(\log|a|, b/|a|, a/|a|)$ and this embedding is indeed injective. We endow the space $\mathbf{K}$ with the inherited metric, so that the distance between (a, b) and (a', b') is given by

$$\left(\int_{\mathbb{T}} \log|a| - \log|a'|\right) + \left(\int_{\mathbb{T}} |b/|a| - b'/|a'||^2\right)^{1/2} + \left(\int_{\mathbb{T}} |a/|a| - a'/|a'||^2\right)^{1/2}.$$

This makes $\mathbf{K}$ a complete metric space.

Furthermore, we also need to construct $\mathbf{H}$ and $\mathbf{L}$, two subspaces of $\mathbf{K}$. To achieve this, we must introduce the concept of an outer function.

[1]Here $a_{-\infty}$ and $b_{-\infty}$ need to be interpreted as a_n and b_n for sufficiently small n.

Definition 2. *We say g is an outer function in $\mathbb{D}$ if g belongs to the Nevanlinna class*[2] *and there exists a function $G : \mathbb{T} \to [0, \infty)$, with $G \in L^1(\mathbb{T})$, such that*

$$g(z) = \exp\left(\int_0^{2\pi} \frac{e^{i\theta} + z}{e^{i\theta} - z} G(e^{i\theta})\, d\theta\right)$$

for $z \in \mathbb{D}$.

Let $\mathbf{L} \subset \mathbf{K}$ be the subspace of pairs (a, b) where a is the boundary value of an outer function a^* on the unit disk $\mathbb{D}$ that is positive at 0, and $\mathbf{H}$ be the subspace of $\mathbf{L}$ where b/a^* is the boundary value of an analytic function in the Hardy space $H^2(\mathbb{D})$. The space $\mathbf{H}$ is closed in $\mathbf{L}$, and $\mathbf{L}$ is closed in $\mathbf{K}$. Moreover, if F is a finite sequence supported on $\mathbb{Z}_{\geq 0}$, then $(a, b) \in \mathbf{H}$.

Lemma 3. *Let F be a sequence in $\ell^2(\mathbb{Z}_{\geq 0}, \mathbb{D})$ and let $F^{(\leq N)}$ denote the truncations to $[0, N]$. Then $(a_N, b_N) = \overbrace{F^{(\leq N)}}$ is a Cauchy sequence in $\mathbf{H}$.*

Given that $\overbrace{F^{(\leq N)}}$ form a Cauchy sequence in $\mathbf{H}$, we define $\overbrace{F}$ as the limit of this sequence. The distance between the NLFT of the truncated sequence and the NLFT of the full sequence converges to 0, ensuring that the Plancherel identity (2) holds on all of $\ell^2(\mathbb{Z}_{\geq 0}, \mathbb{D})$. The theorem below follows from several technical results in [1, Lecture 2].

Theorem 4. *The NLFT is a homeomorphism from $\ell^2(\mathbb{Z}_{\geq 0}, \mathbb{D})$ to $\mathbf{H}$.*

Sketch of Proof. For the continuity of the NLFT, the strategy relies on truncating the sequences and controlling the error introduced by this truncation. One term of this approximation is controlled by using the equivalence of norms in finite-dimensional spaces. Therefore, this proof does not guarantee uniform continuity due to the lack of control over the sequence's length when switching from ℓ^2 to ℓ^1 norms.

On the other hand, the proof shows that each term F_n in the inverse NLFT depends continuously on (a, b). This is true for F_0 by the mean formula, and using induction for higher-order terms, continuity is shown via Möbius transformation, which induces a Lipschitz distortion that depends on F_0. To finish, we combine this with an approximation argument and the Plancherel identity. □

Finally, there are higher-order identities of Plancherel type, which arise from calculating higher derivatives of $\log(a^*)$ at 0.

Lemma 5. *For $F = \{F_n\}_n$ in $\ell^2(\mathbb{Z}_{\geq 0}, \mathbb{D})$, we have*

$$2 \int_{\mathbb{T}} z^{-1} \log |a|(z) = \sum_n \overline{F_n} F_{n+1}$$

[2] We define the Nevanlinna class as

$$N = \left\{ f \in \mathrm{Hol}(\mathbb{D}) \mid \sup_{r<1} \int_{\mathbb{T}} \log_+ |f(rs)|\, ds < \infty \right\}.$$

and

$$4\int_{\mathbb{T}} z^{-2}\log|a|(z) = -\sum_n (\overline{F_n}F_{n+1})^2 + 2\sum_n \overline{F_n}(1-|F_{n+1}|^2)F_{n+2}.$$

References

[1] T. Tao and C. Thiele, *Nonlinear Fourier Analysis*, arXiv:1201.5129 [math.CA] (2012)

Riemann-Hilbert problem for rational functions

Speaker: Kristina Oganesyan

1. Definitions

Let us define the following classes:

$\mathbf{L} := \{SU(1,1) - \text{valued measurable } (a,b) :\ a \text{ has outer extension to } \mathbb{D}^*,\ a(\infty) > 0\}$,

$\mathbf{H} := \{(a,b) \in \mathbf{L} :\ b/a^* \text{ has a holomorphic extension to } \mathbb{D} \text{ which is in } H^2(\mathbb{D})\}$,

$\mathbf{H}^* := \{(a,b) \in \mathbf{L} :\ b/a \text{ has a holomorphic extension to } \mathbb{D}^* \text{ which is in } H^2(\mathbb{D}^*)\}$,

and let $\mathbf{H}_0 := \{(a,b) \in \mathbf{H} :\ b(0) = 0\}$, $\mathbf{H}_0^* := \{(a,b) \in \mathbf{H}^* :\ b(\infty) = 0\}$. Note that $\mathbf{L}$ is exactly the class of nonlinear Fourier transforms of ℓ^2 sequences.

We will call a pair (a,b) *rational* if both a and b are rational functions. We also say that a rational function g is *subordinate* to a rational function f on a certain domain if for all points z in the domain with $ord(g,z) > 0$ we have $ord(f,z) \geq ord(g,z)$.

For $(a,b) \in \mathbf{L}$, the factorization

$$(a,b) = (a_-,b_-)(a_+,b_+)$$

is called *a Riemann-Hilbert factorization* if $(a_-,b_-) \in \mathbf{H}_0^*$ and $(a_+,b_+) \in \mathbf{H}$.

2. Properties of rational pairs

First of all, we establish the following important properties of rational pairs (a,b) and their factorizations.

Lemma 1. (Parametrization by b). For a rational function b, there is a unique rational function a such that $aa^* = 1 + bb^*$, a has no zeros and poles in $\mathbb{D}^*$, and $a(\infty) > 0$. This is the unique function a such that $(a,b) \in \mathbf{L}$.

For rational $(a,b) \in \mathbf{L}$, we have $(a,b) \in \mathbf{H}$ if and only if b has no poles in $\mathbb{D}$, and $(a,b) \in \mathbf{H}_0$ if and only if in addition $b(0) = 0$. (Similarly, we have $(a,b) \in \mathbf{H}^*$ if and only if b has no poles in $\mathbb{D}^*$, and $(a,b) \in \mathbf{H}_0^*$ if and only if in addition $b(\infty) = 0$.)

Lemma 2. (Preservation of the class of rational functions). Let $(a,b) \in \mathbf{L}$ be rational. Given a Riemann-Hilbert factorization

$$(a,b) = (a_-,b_-)(a_+,b_+),$$

we have that (a_-,b_-) and (a_+,b_+) are also rational.

Lemma 3. (Subordination). Let $(a, b) \in \mathbf{L}$ be rational. Then a is subordinate to bb^*. For a Riemann-Hilbert factorization

$$(a, b) = (a_-, b_-)(a_+, b_+),$$

the functions b_- and b_+ are subordinate to b.

In light of the results above, we can reduce the Riemann-Hilbert problem for rational functions to a finite dimensional algebraic problem.

3. Existence and uniqueness of the Riemann-Hilbert factorization for rational functions

With Lemmas 1-3 in hand, we are able to prove our main result.

Theorem 1. Let $(a, b) \in \mathbf{L}$ be rational. There exists a unique Riemann-Hilbert factorization

$$(a, b) = (a_-, b_-)(a_+, b_+)$$

with either a) b_+ or b) b_- having no poles on $\mathbb{T}$.

Recall that, according to the triple factorization theorem, for any $(a, b) \in \mathbf{L}$, there is a unique factorization

$$(a, b) = (a_{--}, b_{--})(a_0, b_0)(a_{++}, b_{++})$$

such that $(a_{--}, b_{--}) \in \mathbf{H}_0^*$, $(a_0, b_0) \in \mathbf{H}_0^* \cap \mathbf{H}$, $(a_{++}, b_{++}) \in \mathbf{H}$, and (a_{--}, b_{--}) and (a_{++}, b_{++}) do not have nontrivial Riemann-Hilbert factorizations. Moreover, one can show that for a pair $(a, b) \in \mathbf{H}$, the factor (a_-, b_-) in its Riemann-Hilbert factorization also belongs to $\mathbf{H}$. It therefore follows that the factor (a_+, b_+) in part a) of Theorem 1 coincides with (a_{++}, b_{++}) (and similarly, the factor (a_-, b_-) in part b) of Theorem 1 coincides with (a_{--}, b_{--})).

4. Factorization of the middle factor in the triple factorization for rational functions

For the sake of completeness, we comment (without proof) also on the description of the factorizations of the middle term in the triple factorization.

Theorem 2. Consider a rational $(a, b) \in \mathbf{H} \cap \mathbf{H}_0^*$. Let $z_j \in \mathbb{T}$, $j = 1, ..., N$ be the distinct poles of a and let n_j be the order of the pole z_j. Let the nonnegative numbers $n_j^+, n_j^- \leq n_j$, $j = 1, ..., N$ be such that for each j either

$$n_j^+ + n_j^- = n_j \quad \text{(split case)}$$

or

$$n_j^+ + n_j^- - 1 = n_j \quad \text{(shared case)}.$$

Assume also that for each j in the shared case we are given positive numbers μ_j^+, μ_j^- such that

$$\mu_j^+ \mu_j^- = \mu_j,$$

where μ_j is defined by

$$\frac{1}{aa^*}(\zeta) = \mu_j(\zeta - z_j)^{n_j}\Big(\frac{1}{\zeta} - \frac{1}{z_j}\Big)^{n_j} + \mathcal{O}(\zeta - z_j)^{2n_j+1}.$$

Then there exists a unique Riemann-Hilbert factorization

$$(a, b) = (a_-, b_-)(a_+, b_+)$$

satisfying

$$ord(a_+, z_j) = n_j^+, \quad ord(a_-, z_j) = n_j^-,$$

and, for j in the shared case,

$$A_+ := \frac{a_-^*}{a_+a^*} = -\mu_j^+ z_j(\zeta - z_j)^{n_j^+-1}\Big(\frac{1}{\zeta} - \frac{1}{z}\Big)^{n_j^+} + \mathcal{O}((\zeta - z_j)^{2n_j^+}),$$

$$A_- := \frac{a_+}{a_-^* a} = -\mu_j^- z_j^*(\zeta - z_j)^{n_j^-}\Big(\frac{1}{\zeta} - \frac{1}{z}\Big)^{n_j^- - 1} + \mathcal{O}((\zeta - z_j)^{2n_j^-}).$$

Moreover, all Riemann-Hilbert factorizations are obtained in this way.

References

[1] T. Tao, C. Thiele, *Nonlinear Fourier analysis*, arXiv:1201.5129.

Alternative and multivariable quantum signal processing

Zane Marius Rossi
(joint work with Isaac Chuang)

1. Overview

Quantum algorithms remain difficult to design and interpret; correspondingly, great effort has been spent to not only generate algorithms but formalize the motifs of quantum advantage. These desires have been partially addressed with quantum signal processing (QSP) [1, 2], which allows one to transform the spectrum of large linear operators by tunable polynomial functions using a simple alternating ansatz, in turn unifying and simplifying most known quantum algorithms.

QSP's success follows from a thorough understanding of the permitted maps of type $\mathbb{T} \to \mathrm{SU}(2)$ (from the complex unit circle to the two-dimensional special unitary group) affiliated with QSP's ansatz. A natural extension promotes this study to the multivariable setting, i.e., maps of type $\mathbb{T}^{\otimes n} \to \mathrm{SU}(2)$. Physically, here the computing parity is allowed access to not just one but multiple independent oracles, between which one is allowed to intersperse their own unitaries.

The work of [3] considers the simplest instance of this extension—two commuting, single-qubit oracles—showing that the necessary and sufficient conditions under which a given *multivariable* polynomial transform is achievable are far from obvious, and entangled with results in functional analysis and analytic geometry.

This talk centers on [3] but is steered by insights accumulated over the two years since its publication. Here we briefly place this work in the context of a larger research program on extensions to QSP/QSVT:

(a) **Tethering circuit ansätze and function classes:** The standard map between QSP circuit parameterizations and polynomial transforms is degenerate and awkward. Later work has removed unnecessary d.o.f's, allowing performant phase-finding algorithms. Do similar techniques extend to the multivariable setting? *More broadly, how are constraints on circuit parameterizations taken to constraints on achieved polynomials?*

(b) **Novel constructive and non-constructive theorems for the existence of good circuit parameterizations:** QSP ansatz specifications rely on constructive, inductive proof methods to show the achieveability of specific classes of polynomials.[1] As such, modifying the ansatz, i.e., moving to the multivariable setting, requires overhauling the constructive proof. *Do there exist non-constructive methods to only* ***indirectly*** *show density of ansätze in wider function classes?*

(c) **An *algorithmic resource theory* built around the block-encoding data type:** One way to interpret the incomplete results of [3] is that a given multivariable polynomial transformation of block encodings may require a certain ciruit depth, width, and query-complexity. With the advent of 'generalized polynomial methods' for matrix functions [18], *can we provide tighter upper and lower bounds for general algebraic manipulation of commuting/non-commuting block encodings?*

It stands that 'solutions' to the problems raised by multivariable variants of QSP can take multiple forms. Of greatest benefit would be a better understanding of how precisely various naïve extensions of QSP fail, and more diverse techniques for expressing structured products of unitaries. In this way, recent work on QSP as a form of nonlinear Fourier analysis is exciting progress: useful analytic properties of the QSP ansatz related to iterative phase-finding methods are connected to at-first-glance un-physical properties of the analytic extension of the induced polynomial transforms at infinity!

2. Main statements

Multivariable quantum signal processing (M-QSP) as introduced considered in [3] allows the use (in any order) of two possible signal unitaries $W(x_1), W(x_2)$: rotations about a fixed axis on the Bloch sphere by different, unknown angles. As such, while suppressing some underlying complexity discussed afterwards, M-QSP's characterization theorem looks superficially similar to that of standard QSP.

[1] While in practice QSP phases are found by iterative, optimization-based methods.

Theorem 1 (M-QSP in the Laurent picture)**.** *Let* $\Phi = \{\phi_0, \ldots, \phi_k\} \in \mathbb{R}^{k+1}$ *and* $s = \{s_1, \ldots, s_k\} \in \{0,1\}^k$*. Then the M-QSP unitary for* (Φ, s) *has form*

$$U_{M\text{-}QSP}(x_1, x_2; \Phi, s) \equiv \Phi[W(x_1), W(x_2)]$$
$$= e^{i\phi_0\sigma_z} \prod_{j=1}^{k} W(x_1)^{s_j} W(x_2)^{1-s_j} e^{i\phi_j\sigma_z} = \begin{pmatrix} P & Q \\ -Q^* & P^* \end{pmatrix} \tag{1}$$

where $W(x) = (1/2)(x + x^{-1})I + (1/2)(x - x^{-1})\sigma_x$ *for* $(x_1, x_2) \in \mathbb{T}^2$ iff $P, Q \in \mathbb{C}[x_1, x_2]$ *are Laurent polynomials in* x_1 *and* x_2 *satisfying the following conditions:*

(1) $deg(P) \preccurlyeq (m, n-m)$ *and* $deg(Q) \preccurlyeq (m, n-m)$ *with* $n = |s|$*, the Hamming weight of* s*.*
(2) P *has even parity under* $(x_1, x_2) \mapsto (x_1^{-1}, x_2^{-1})$ *and* Q *has odd parity under* $(x_1, x_2) \mapsto (x_1^{-1}, x_2^{-1})$*.*
(3) P *has parity* m *mod* 2 *under* $x_1 \mapsto -x_1$ *and parity* $(m-n)$ *mod* 2 *under* $x_2 \mapsto -x_2$*.* Q *has parity* m *mod* 2 *under* $x_1 \mapsto -x_1$ *and parity* $(m-n)$ *mod* 2 *under* $x_2 \mapsto -x_2$*.*
(4) For all $(x_1, x_2) \in \mathbb{T}^2$*, we have* $|P|^2 + |Q|^2 = 1$*.*
(5) A statement of equivalent strength to the FRT = QSP condition,[2] *given in* [3]*, holds.*

The difficulty in the above statement is the last condition, namely recovering the inductive property that allows any M-QSP unitary to be written as the product of two unitaries—one with the form $W(x_k)e^{i\phi_j\sigma_z}$ for some k, ϕ_j, and the other an M-QSP unitary with strictly lower degree.

The difficulty in M-QSP comes from two places: (1) ensuring that a given polynomial as a matrix element can be suitably 'completed' and embedded in a unitary satisfying the first four conditions of the theorem, and (2) ensuring completions satisfying the first four conditions always permit decompositions into products of oracles and σ_z-generated rotations.

Problem (1) can be answered, albeit opaquely, by appealing to *multivariable Fejér-Riesz theorems* (FRTs) [19]; such theorems specify when positive (or non-negative) multivariable trigonometric polynomials can be expressed as squares.[3] Problem (2), however, originally left up to 'FRT = QSP' conjecture in [3], has proven more obstinate; currently there is not even a non-trivial *sufficient* condition for when such unitary completions permit factorizations into products of only oracles and SU(2) rotations.

Against these difficulties, we can either (a) give more abilities to the computing party in an attempt to broaden the set of achievable functions, or (b) provide sufficient conditions such that a given polynomial function permits both (1) unitary

[2]A counterexample to the original conjecture has since been given in [4]. Think of this as a statement guaranteeing that polynomials with unitary extensions permit, at each degree, the inductive step required to iteratively compute QSP phases.

[3]The statement of these theorems (and variants) is involved but, inspired by the univariate case, require that a Toeplitz matrix of Fourier coefficients of the intended function has low rank.

completion and (2) phase read-off automatically. Approaches toward this are more specifically enumerated in Sec. 4.

3. A brief guide to related works

While [3] posed initial questions on multivariable QSP variants, a greater impact of its publication manifests in companion papers which address its limitations, examine extensions, and push the theory of QSP/QSVT in new directions. We break these papers into categories for a new reader.

(a) **Restricted and extended ansätze:** Outside of the multivariable setting, numerous works investigate modifications to the QSP circuit, either by restricting the ansatz to improve numerical properties [14], investigating infinite-dimensional variants [13], or allowing larger gate sets to relax certain parity requirements [10].

(b) **Multivariable variants:** Insightful papers have since followed [3] providing counterexamples to the conjecture provided [4, 5] (along with alternative ansätze), as well as LCU-based variants using additional space to achieve similar block encodings [8].

(c) **General, modular block-encoding manipulation:** By relaxing resource models, multivariable polynomials in block-encoded operators can be achieved with incomparable complexities, e.g., through LCU-methods [8] mentioned, or black-box composition of QSP-protocols (first described in [11, 9]) or special supersets of the QSP ansatz (*gadgets*) [6].

(d) **QSP and NLFA:** Finally, recent works [16, 17] have recast QSP as a form of *nonlinear Fourier analysis*, wherein suitably modified results from standard Fourier analysis can be recovered for group-valued functions which, suitably discretized, allow clean proofs of convergence for iterative phase-finding algorithms for wide classes (e.g., Szegö) of target polynomials.

4. Discussion and open problems

Having reviewed some of the main statements of the original instantiation of M-QSP, as well as works since published addressing, extending, or circumventing its methods, we enumerate some open problems/promising avenues.

(a) **Adding abilities to the computing party:** To enable the recovery of the inductive step used for finding M-QSP phases, we could permit additional space, intervening measurement, disparate oracle types, etc. We know LCU and QSP-based techniques can, with additional space and query complexity, achieve arbitrary bounded multivariable matrix polynomials. *Can the required query complexity be lower bounded in terms of desired function class?*

(b) **Identifying a restricted sub-class of achievable functions:** just as symmetrized QSP usefully restricts the class of achievable functions to improve QSP's numerical properties, we can imagine identifying a more simply-describable, but non-trivial, subset of M-QSP-achievable functions. *We know that Chebyshev polynomials and certain algebraic relations among*

these polynomials are achievable without additional space; can the dictionary of permitted algebraic operations be diversified?

(c) **Identifying new iterative phase-finding algorithms and nonconstructive existence theorems:** Work in QSP as nonlinear Fourier analysis, as well as symmetrized QSP in general, has yielded exciting algorithms for QSP phase finding of new character, relying on solving structured linear systems. *Do similarly well-performing algorithms exist in the multivariable case, and do they suggest classes of functions in which a given ansatz is dense?*

Ultimately, in this author's opinion, the unifying character of QSP/QSVT seems less a statement of these algorithms generality, and more a suggestion that the quantum algorithmist's toolkit is narrow. The success of recent works rests on their ability to systematically break QSP's basic assumptions while still recovering QSP-like guarantees, in turn building broad families of analytically well-understood parameterized ansätze from well-understood techniques in functional analysis.

References

[1] G. H. Low and I. L. Chuang. *Optimal Hamiltonian simulation by quantum signal processing.* Phys. Rev. Lett., 118:010501, 2017.

[2] G. H. Low and I. L. Chuang. *Hamiltonian simulation by qubitization.* Quantum, 3:163, 2019.

[3] Z. M. Rossi, I. L. Chuang, *Multivariable quantum signal processing (M-QSP): prophecies of the two-headed oracle*, *Quantum* 6, 2022, 811.

[4] Balázs Németh and Blanka Kövér and Boglárka Kulcsár and Roland Botond Miklósi and András Gilyén, *On variants of multivariate quantum signal processing and their characterizations*, arXiv preprint (`arxiv:2312.09072`), 2023.

[5] Hitomi Mori, Keisuke Fujii, Kaoru Mizuta, *Comment on "Multivariable quantum signal processing (M-QSP): prophecies of the two-headed oracle"*. ArXiv preprint (`2310.00918`), 2023.

[6] Z. M. Rossi and J. L. Ceroni and I. L. Chuang, *Modular quantum signal processing in many variables*, arXiv preprint (`2309.16665`), 2023.

[7] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. *Quantum singular value transformation and be- yond: exponential improvements for quantum matrix arithmetics.* Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, 2019.

[8] Yonah Borns-Weil, Tahsin Saffat, and Zachary Stier. *A quantum algorithm for functions of multiple commuting Hermitian matrices.* arXiv preprint, (`2302.11139`), 2023.

[9] Zane M. Rossi and Isaac L. Chuang. *Semantic embedding for quantum algorithms.* Journal of Mathematical Physics, 64(12):122202, 12 2023.

[10] Danial Motlagh and Nathan Wiebe. *Generalized Quantum Signal Processing.* PRX Quantum 5, 020368, 2024.

[11] Kaoru Mizuta and Keisuke Fujii. *Recursive quantum eigenvalue and singular-value transformation: Analytic construction of matrix sign function by Newton iteration.* Phys. Rev. Research 6, 2024.

[12] Dong, Yulong and Lin, Lin and Ni, Hongkang and Wang, Jiasu. *Robust Iterative Method for Symmetric Quantum Signal Processing in All Parameter Regimes.* SIAM Journal on Scientific Computing 46 (5), 2024.

[13] Yulong Dong, Lin Lin, Hongkang Ni, and Jiasu Wang. *Infinite quantum signal processing.* arXiv preprint (`2209.10162`), 2022.

[14] Jiasu Wang, Yulong Dong, and Lin Lin. *On the energy landscape of symmetric quantum signal processing.* Quantum, 6:850, 2022.

[15] Yulong Dong, Xiang Meng, K. Birgitta Whaley, and Lin Lin. *Efficient phase-factor evaluation in quantum signal processing.* Phys. Rev. A, 103(4), 2021.
[16] Michel Alexis and Gevorg Mnatsakanyan and Christoph Thiele. *Quantum signal processing and nonlinear Fourier analysis.* ArXiv preprint, (2310.12683), 2024.
[17] Michel Alexis, Lin Lin, Gevorg Mnatsakanyan, Christoph Thiele, Jiasu Wang. *Infinite quantum signal processing for arbitrary Szegő functions.* ArXiv preprint (2407.05634), 2024.
[18] Ashley Montanaro, Changpeng Shao. *Quantum and classical query complexities of functions of matrices.* ArXiv preprint (2311.06999), 2023
[19] J. Geronimo and Hugo Woerdeman. *Positive extensions, Fejér-Riesz factorization and autoregressive filters in two variables.* Ann. Math. 160, 839–906 (2004).

QSP and NLFT

Miquel Saucedo

1. Connection between QSP and NLFT

1.1. Definition of QSP.

Proposition 1 (Pauli matrices and some of their properties)**.** *Set*

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ and } Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The following properties hold:

(1) The matrix

$$M = 2^{-\frac{1}{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

diagonalizes X and satisfies $M = M^{-1}$, that is,

$$MXM = Z.$$

(2) For $\theta \in \mathbb{R}$,

$$e^{i\theta X} = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix} \text{ and } e^{i\theta Z} = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}.$$

Let $\Psi = (\psi_k)_{k\in\mathbb{N}}$ with $\psi_k \in (-\frac{\pi}{2}, \frac{\pi}{2})$. We now define the QSP for Ψ.

Definition 2. *Set $x = \cos(\theta)$ with $\theta \in [0, \frac{\pi}{2}]$ and define recursively the symmetric QSP*

$$U_0(\Psi, x) = e^{i\psi_0 Z}, \quad U_d(\Psi, x) = e^{i\psi_d Z} e^{i\theta X} U_{d-1}(\Psi, x) e^{i\theta X} e^{i\psi_d Z}. \tag{1}$$

The QSP of Ψ is the limit imaginary part of the upper-left entry of U_d as $d \to \infty$.

1.2. **Definition of SU(2) NLFT and connection with QSP.** First we recall the definition of NLFT. Let $F = (F_n)_{n\in\mathbb{Z}}$ with $F_n \in \mathbb{C}$ and finite support (extensions to larger spaces have been discussed in previous lectures).

Definition 3 (NLFT)**.** *Define recursively*

$$G_k(z) = G_{k-1}(z)T_k(F_k, z)$$

with the initial condition $G_{-\infty} = I$, and where

$$T_k(F_k, z) = \frac{1}{\sqrt{1+|F_k|^2}} \begin{pmatrix} 1 & F_k z^k \\ -\overline{F_k} z^{-k} & 1 \end{pmatrix}.$$

We write $\overset{\frown}{F} = (a, b)$, where

$$G_\infty(z) = \begin{pmatrix} a(z) & b(z) \\ -b^*(z) & a^*(z) \end{pmatrix}.$$

We now describe the connection between QSP and NLFT.

Theorem 4. *Let $F = (F_n)_{n\in\mathbb{Z}} = (i\tan\psi_{|n|})_{n\in\mathbb{Z}}$. Set $x = \cos(\theta)$ and $z = e^{2i\theta}$. Then, for $n \in \mathbb{N}$*

$$G_n(F, z) = e^{-in\theta Z} M U_n(\Psi, x) M e^{-in\theta Z}.$$

Therefore $\overset{\frown}{F}(z) = (a(z), b(z))$ and , because of the symmetries of F_n,

$$b(z) = -b^*(z),$$

and

$$(a(z), b(z)) = (a^*(z^{-1}), -b^*(z^{-1})).$$

Hence, b is purely imaginary, even and $\lim_n \mathrm{Im}(U_n(\Psi, x)_{1,1}) = b(z)$.

Proof. Observe that

$$T_k(F_k, z) = \begin{pmatrix} \cos\psi_k & i\sin\psi_k e^{2ki\theta} \\ i\sin\psi_k e^{-2ki\theta} & \cos\psi_k \end{pmatrix} = e^{ik\theta Z} e^{i\psi_k X} e^{-ik\theta Z}.$$

Hence,

$$\begin{aligned} G_n(F, z) &= e^{-in\theta Z} e^{i\psi_n X} e^{in\theta Z} \cdots e^{-i2\theta Z} e^{i\psi_2 X} e^{i2\theta Z} e^{-i\theta Z} e^{i\psi_1 X} e^{i\theta Z} \times \\ &\times e^{i\psi_0 X} e^{i\theta Z} e^{i\psi_1 X} e^{-i\theta Z} e^{i2\theta Z} e^{i\psi_2 X} e^{-i2\theta Z} \cdots e^{in\theta Z} e^{i\psi_n X} e^{-in\theta Z} \\ &= e^{-in\theta Z} e^{i\psi_n X} e^{i\theta Z} \cdots e^{i\psi_0 X} e^{i\theta Z} e^{i\psi_1 X} e^{i\theta Z} e^{i\psi_2 X} e^{i\theta Z} \cdots e^{i\theta Z} e^{i\psi_n X} e^{-in\theta Z} \\ &= e^{-in\theta Z} M U_d(\Psi, x) M e^{-in\theta Z}. \end{aligned}$$

□

Hence, the problem of finding angles which encode f becomes finding F such that $\overset{\frown}{F} = (a, b)$ for a given even, imaginary b and some a.

2. Given b, find NLF coefficients

Recall that, by previous lectures, given *suitable* (a, b) (more precisely $|a^*|^2 + |b|^2 = 1$ on $\mathbb{T}$, $a^* \in H^2(\mathbb{D})$, $\inf_{z\in\mathbb{D}} |a^*(z)|^2 > \frac{1}{2}$ and $a^*(0) > 0$) we can find the NLF coefficients by applying layer-stripping to the Riemann Hilbert factorization. The problem is now for a given b to find such an a.

2.1. **Finding a from b.**

Theorem 5. *Let b be a measurable function on $\mathbb{T}$ with $\sup b^2 < \frac{1}{2}$. Then there exists an $a^* \in H^2(\mathbb{D})$ such that $a^*(0) > 0$, $|a^*|^2 + |b|^2 = 1$ on $\mathbb{T}$ and $\inf_{z\in\mathbb{D}} |a^*(z)|^2 > \frac{1}{2}$.*

Proof. Let, for $z \in \mathbb{T}$,

$$M(z) := \frac{1}{2} \log\big(1 - |b(z)|^2\big).$$

Since M is real,

$$N(z) := M(z) + iH(M)(z) \sim \hat{M}(0) + \sum_{n=1}^{\infty} 2\hat{M}(n) z^n \in L^2(\mathbb{T})$$

where the Hilbert transform $H(M)$ is also real. Thus, N can be extended to a holomorphic function in the disc via the formula (equivalently by convolution with the Poisson kernel)

$$N(re^{i\theta}) = P_r * N(\theta) = \hat{M}(0) + \sum_{n=1}^{\infty} 2\hat{M}(n)(re^{i\theta})^n.$$

Set

$$a^*(z) = \exp(N(z)),$$

it is a holomorphic function with radial limits at $z \in \mathbb{T}$ satisfying $|a^*(z)|^2 = 1 - |b(z)|^2$ almost everywhere and $a^*(0) = e^{\hat{M}(0)} > 0$. It is outer because

$$\log |a^*(re^{i\theta})| = \operatorname{Re} N(re^{i\theta}) = P_r * M(\theta) = P_r * \log |a^*(\theta)|.$$

Finally, by Jensen's inequality, for any real λ,

$$|a^*(re^{i\theta})|^\lambda \le P_r * |a^*(\theta)|^\lambda.$$

Since on the boundary $\frac{1}{2} + \varepsilon \le |a^*|^2 \le 1$, we have $a^* \in H^2(\mathbb{D})$ and $\inf_{z\in\mathbb{D}} |a^*(z)|^2 > \frac{1}{2}$.

□

Remark 6. *We have*

$$\begin{aligned} -\frac{1}{2} \sum_{n\in\mathbb{Z}} \log\left(1 + \tan^2(\psi_{|n|})\right) &= \log(a^*(0)) = \frac{1}{2} \int_{\mathbb{T}} \log\big(1 - |b(\theta)|^2\big) d\theta \\ &= \frac{1}{\pi} \int_0^\pi \log\big(1 - f(x)^2\big) \frac{dx}{\sqrt{1 - x^2}}. \end{aligned}$$

Hence the QSP of the truncated series converges in the

$$\int_0^\pi \log\bigl(1-f(x)^2\bigr)\frac{dx}{\sqrt{1-x^2}}$$

sense.

3. Summmary: how to find QSP angles

Given $f:[0,1]\to\mathbb{R}$ to find ψ: extend it to an even function, let $b(z)=if(x)$ with $x=\cos\theta$, $\theta\in[0,\pi]$ and $z=e^{2i\theta}$. Find the outer a as in Theorem 2.1. Let F be the NLF coefficients of (a,b), since b is imaginary and even, F_n is even and imaginary. The angles of the QSP are $\psi_n=\arctan(-iF_n)$.

References

[1] M. Alexis, G. Mnatsakanyan and C. Thiele, *Quantum signal processing and nonlinear Fourier analysis*, Rev. Mat. Complut (2024).

Nonlinear Fourier series for better than square summable

Mitchell Taylor

The content of this talk is based on Lecture 1 of [1].

1. Review of the (linear) Fourier transform

Before introducing the nonlinear Fourier transform, we set some conventions.

Given a sequence $F=(F_n)_{n\in\mathbb{Z}}$ of complex numbers, the *Fourier transform* of F is defined formally as:

$$\widehat{F}(\theta)=\sum_{n\in\mathbb{Z}}F_n e^{-2\pi i\theta n}.$$

As is well-known, the Fourier inversion formula

$$F_n=\int_0^1\widehat{F}(\theta)e^{2\pi i\theta n}d\theta$$

yields a correspondence between $F\in\ell^2(\mathbb{Z})$ and $\widehat{F}\in L^2(\mathbb{T})$.[1]

[1]Here, we are identifying 1-periodic functions in θ with functions in the variable $z\in\mathbb{T}$ via $z=e^{-2\pi i\theta}$.

2. The (discrete) nonlinear Fourier transform

The discrete nonlinear Fourier transform acts on sequences $F = (F_n)_{n\in\mathbb{Z}}$, where each F_n is in the unit disc D. The definition of this transform will be given in stages. As a first step, we assume that F is a finitely supported sequence, so that there exists $N \in \mathbb{N}$ such that $F_n = 0$ whenever $|n| \geq N$.

For a complex parameter z, we consider the formal infinite recursion:

$$\begin{bmatrix} a_n & b_n \end{bmatrix} = \frac{1}{\sqrt{1-|F_n|^2}} \begin{bmatrix} a_{n-1} & b_{n-1} \end{bmatrix} \begin{bmatrix} 1 & F_n z^n \\ \overline{F}_n z^{-n} & 1 \end{bmatrix}$$

with the initialization

$$a_{-\infty} = 1, \quad b_{-\infty} = 0. \tag{1}$$

Note that by the assumption that $(F_n)_{n\in\mathbb{Z}}$ is compactly supported, the *transfer matrix*

$$\frac{1}{\sqrt{1-|F_n|^2}} \begin{bmatrix} 1 & F_n z^n \\ \overline{F}_n z^{-n} & 1 \end{bmatrix}$$

is the identity matrix when $|n|$ is sufficiently large. For this reason, the initialization (1) can be interpreted as the condition that $a_n = 1$ and $b_n = 0$ for sufficiently negative n.

We define the *nonlinear Fourier transform* of the sequence $F = (F_n)_{n\in\mathbb{Z}}$ as the pair of functions (a_∞, b_∞) in the parameter $z \in \mathbb{T}$, which is again well-defined by the assumption that $(F_n)_{n\in\mathbb{Z}}$ is compactly supported. We will use the notation

$$\overbrace{F}(z) = (a_\infty(z), b_\infty(z))$$

to denote this function.

Remark: Note that $\overbrace{F}$ is a finite Laurent polynomial in z, so may be defined everywhere on the complex plane except at the origin. However, we will view the nonlinear Fourier transform as a function on the unit circle $\mathbb{T}$, as this will be necessary when we extend the definition of $\overbrace{F}$ to non-compactly supported F.

2.1. Interpretation as a map into a group.

Recall that the group $SU(1,1)$ consists of all complex matrices of the form

$$\begin{bmatrix} a & b \\ \overline{b} & \overline{a} \end{bmatrix}$$

which have determinant one. Note that for each $z \in \mathbb{T}$, the transfer matrix is in this group. Moreover, for $z \in \mathbb{T}$, it is easy to see that the functions (a_n, b_n) can be equivalently defined via the recursion

$$\begin{bmatrix} a_n & b_n \\ \overline{b}_n & \overline{a}_n \end{bmatrix} = \frac{1}{\sqrt{1-|F_n|^2}} \begin{bmatrix} a_{n-1} & b_{n-1} \\ \overline{b}_{n-1} & \overline{a}_{n-1} \end{bmatrix} \begin{bmatrix} 1 & F_n z^n \\ \overline{F}_n z^{-n} & 1 \end{bmatrix}$$

with

$$\begin{bmatrix} a_{-\infty} & b_{-\infty} \\ \overline{b}_{-\infty} & \overline{a}_{-\infty} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Hence, one may easily check that each matrix

$$\begin{bmatrix} a_n & b_n \\ \overline{b}_n & \overline{a}_n \end{bmatrix}$$

is in $SU(1,1)$; in particular, $|a_n|^2 = 1 + |b_n|^2$ and we may consider the nonlinear Fourier transform as a map

$$\ell_0(\mathbb{Z}; D) \to C(\mathbb{T}; SU(1,1)),$$

where $\ell_0(\mathbb{Z}; D)$ denotes the set of all finitely supported integer sequences with values in the open unit disc D. We will abuse notation and write

$$(a, b)(c, d) = (ac + b\overline{d}, ad + b\overline{c}),$$

which is consistent with the group law.

2.2. **Properties of the nonlinear Fourier transform.** For small values of F_n, the nonlinear Fourier transform can be approximated by the linear (inverse) Fourier transform. Indeed, this can be seen by linearizing in F. By Taylor expansion, we have $(1 - |F_n|^2)^{-1/2} \approx 1$ for F_n small. Otherwise, the remaining formula for (a_∞, b_∞) is polynomial in the variables F and $\overline{F}$. Collecting only the constant and linear terms, we have

$$(a_\infty, b_\infty) = (1, \sum_{n\in\mathbb{Z}} F_n z^n).$$

Thus, to leading order, $a_\infty = 1$ and b_∞ is the usual discrete Fourier transform. The following theorem summarizes various properties of the nonlinear Fourier transform. In it, for a function c defined on an open set E in the Riemann sphere, we use the notation $c^*(z) := \overline{c(\overline{z}^{-1})}$ which is defined on $E^* = \{z : \overline{z}^{-1} \in E\}$.

Theorem: The following properties hold.

(1) If $F_n = 0$ for $n \neq m$, then

$$\overbrace{(F_n)} = (1 - |F_m|^2)^{-\frac{1}{2}}(1, F_m z^m).$$

(2) If $\overbrace{(F_n)} = (a, b)$, then for the shifted sequence with n-th entry F_{n+1}, we have

$$\overbrace{(F_{n+1})} = (a, bz^{-1}).$$

(3) If the support of F is entirely to the left of the support of G, then

$$\overbrace{(F + G)} = \overbrace{F}\,\overbrace{G}.$$

(4) If $|c| = 1$ then

$$\overbrace{(cF_n)} = (a, cb).$$

(5) For the reflected sequence whose n-th entry is F_{-n}, we have

$$\overbrace{(F_{-n})}(z) = (a^*(z^{-1}), b(z^{-1})).$$

(6) For the complex conjugate sequence, we have

$$\widetilde{(\overline{F}_n)} = (a^*(z^{-1}), b^*(z^{-1})).$$

(7) The nonlinear Fourier transform is a bijection from $\ell_0(\mathbb{Z}; D)$ into the space of all pairs (a, b) with b an arbitrary Laurent polynomial and a the unique Laurent polynomial satisfying $aa^* = 1 + bb^*$, $a(\infty) > 0$, and a has no zeros in D^*.

Remark: Observe that statements (2)-(6) are consistent with the linearization $a \sim 1$ and $b \sim \sum F_n z^n$. Statement (7) is by far the most delicate to prove; it will be relevant later for identifying the mapping properties of the nonlinear Fourier transform on Hilbert spaces.

2.3. **The definition of the nonlinear Fourier transform, summabel sequences.** As with the classical Fourier transform, the extension of the nonlinear Fourier transform to absolutely summable sequences is relatively straightforward. To see this, we define a metric on the space $SU(1,1)$ by

$$\text{dist}(G, G') = \|G - G'\|_{op}.$$

Since $SU(1,1)$ is closed in $\mathbb{C}^4$, $SU(1,1)$ is a complete metric space. We define $L^\infty(\mathbb{T}; SU(1,1))$ to be the metric space of all essentially bounded functions $G : \mathbb{T} \to SU(1,1)$ with distance

$$\text{dist}(G, G') = \sup_z \text{dist}(G(z), G'(z)).$$

We also make $\ell^1(\mathbb{Z}; D)$ into a complete metric space by defining

$$\text{dist}(F, F') = \sum_n \|T_n - T'_n\|_{op},$$

where T_n and T'_n are the associated transfer matrices. We first observe that for every $\epsilon > 0$, the above metric is bi-Lipschitz equivalent to the usual ℓ^1 metric

$$\text{dist}'(F, F') = \sum_n |F_n - F'_n|$$

on $B_\epsilon = \{F_n : \sup_n |F_n| < 1 - \epsilon\}$ and $\cup_\epsilon (B_\epsilon \cap \ell^1(\mathbb{Z}; D)) = \ell^1(\mathbb{Z}; D)$. In particular, finitely supported sequences will be dense in $\ell^1(\mathbb{Z}; D)$. With this in mind, we have the following lemma.

Lemma: With the above metrics, the NLFT on $\ell_0(\mathbb{Z}; D)$ extends uniquely to a locally Lipschitz map from $\ell^1(\mathbb{Z}; D)$ to $L^\infty(\mathbb{T}; SU(1,1))$. Moreover, the NLFT of an $\ell^1(\mathbb{Z}; D)$ sequence can be written as the convergent infinite ordered product of the transfer matrices.

The proof is an application of Trotter's formula to obtain a Lipschitz estimate on bounded sets for finite sequences together with a standard approximation argument.

Remark: By somewhat more sophisticated arguments, the NLFT can be extended to ℓ^p sequences in a rather explicit fashion when $1 \leq p < 2$. However,

the extension to ℓ^2 is more delicate as certain multilinear expansions in the above definition of the NLFT will fail to converge. This will be discussed in the next lecture.

References

[1] T. Tao and C. Thiele, *Nonlinear Fourier Analysis*, Lect. Notes IAS Park City Summer School, July 2003.

Reporter: Christoph Thiele