ABSTRACT

Title of dissertation: INTERPLAY OF CHAOS AND INTEGRABILITY: FROM SHOR'S ALGORITHM TO SOLITONS

Abu S Musa Patoary, Doctor of Philosophy, 2025

Dissertation directed by: Prof. Victor Galitski
Department of Physics, University of Maryland College Park

The RSA (Rivest–Shamir–Adleman) encryption is believed to be secure because there is no known classical algorithm which can calculate the prime factors of a number in polynomial time. Shor's algorithm can, in principle, solve this problem in polynomial time on a scalable quantum computer. Shor's algorithm is an application of quantum phase estimation where one factorizes a number by finding the periodicity of the modular multiplication operator. Quantum modular multiplication is related to classical Bernoulli map which is chaotic. However modular multiplication itself is periodic. It raises the question: is there any signature of chaos in modular multiplication? In this dissertation we show that the answer is yes. We prove that modular multiplication is a linear combination of chaotic quantized baker's maps. The periodicity of modular multiplication arises from 'destructive interference' of chaotic maps. Building on this result, we design a quantum circuit for modular multiplication whose complexity is on par with most of the available circuits. A novel feature of our circuit is that it is based entirely on discrete Fourier transform and its variants. In the last part of this dissertation we study integrability of discrete Gross-Neveu model. We show that the action of discrete Gross-Neveu model has a minimum

corresponding to soliton solutions. We further explore the connection between solitons and reflectionless potential using tools from discrete supersymmetry.

INTERPLAY OF CHAOS AND INTEGRABILITY: FROM SHOR'S ALGORITHM TO SOLITONS

by

Abu S Musa Patoary

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2025

Advisory Committee:
Prof. Victor Galitski, Chair/Advisor
Prof. Tom Cohen
Prof. Ian Spielman
Prof. Michael Gullans
Prof. Chris Jarzynski (Dean's Representative)

© Copyright by
Abu S Musa Patoary
2025

Dedication

To Ammu, Setu, Sejo Mama. And Sanjar and Haseen, who unknowingly, make everything worth it.

Acknowledgments

I would like to thank Victor Galitski, my advisor, for putting up with me through all these years. All my works are based on his ideas which he seems to have an infinite supply of. I thank all the agencies who funded my research: National Science Foundation, Department of Energy, Robust Quantum Simulation and Simons Foundation. I'm thankful to all my co-authors (Amit Vikram, Laura Shou, Shankar Balasubramanian), my group members and everyone I had a scientific discussion with.

I'm grateful to the administrative members of the physics department who diligently took care of all the paperwork. Special thanks to Josiland Chambers, Jessica Crosby, Tielia Bean, Sumerem Lehri.

Over the years I had Amitava Banerjee, Elizabeth Paul, Arthur Lin, Wonseok Hwang, Katelyn Rempe, Gautam Nambiar, Amit Vikram, Sagar Airen, Aritra Das, Aranya Chakrobarty, Vinay Kumar as roommates. They were the best roommates I could have asked for. Morning tea with Amitava and coffee with Katelyn has been a staple of my daily routine.

There are many friends who injected fun into the lonely life of a PhD student. Soccer is my most favorite thing in the world and it has gifted me a close-knit community of friends. Duc, Kassa, Zul, Johnny, Bihan, Aarun, Maddie, Oscar, Jay, Reint, Spandan, Mustafa, Alex and many others are part of that community. Sohitri and Sourav invited me to their place for dinner countless times. I will try to make an incomplete list of other friends who contributed in this PhD: Sharoon, Arinjoy, Tamoghna, Shubhayan, Naren, Navya, Cassidy, Grace, Jon, Bruno, Alireza, Djamil, Hemant, Shweta, Emily, Quincy. I am incredibly fortunate to have two amazing therapists: Kristen Regenauer and Kelly Carter. They helped me overcome the lowest of lows in this journey.

Finally I want to thank my family: my mom, sister, uncles, grandparents, brother-in law and my little nephew Sanjar and niece Haseen.

Table of Contents

Dedication ii

Acknowledgements iii

Table of Contents iii

List of Figures vi

1 Introduction 1

2 Chaotic Roots of the Modular Multiplication Dynamical System in Shor's Algorithm 7
- 2.1 Overview . . . 7
- 2.2 Overview of Shor's algorithm, Baker's map and its quantization . . . 9
  - 2.2.1 Shor's algorithm . . . 9
  - 2.2.2 Baker's map . . . 10
- 2.3 Results . . . 15
- 2.4 Semiclassical limit of the quantized baker's map . . . 19
- 2.5 Discussion . . . 28
- 2.6 Generalization to arbitrary N . . . 29
- 2.7 Quantum circuit of non-unitary A-baker's map . . . 33

3 A discrete Fourier transform based quantum circuit for modular multiplication in Shor's algorithm 36
- 3.1 Overview . . . 36
- 3.2 Outline of the circuit . . . 41
- 3.3 Breaking down the circuit into elementary gates . . . 42
  - 3.3.1 Construction of the resetting operator K_G and K_F . . . 44
- 3.4 Complexity . . . 47
- 3.5 Discussion . . . 48
- 3.6 On the order of modular multiplicative group . . . 49
- 3.7 Relevance of the theorems to prime factorization . . . 52

4 Solitons in lattice field theories via tight-binding supersymmetry 53
4.1 Overview . . . 53
4.2 Gross-Neveu model and Korteweg-de Vries equation . . . 57
4.2.1 Gross-Neveu (GN) model . . . 58
4.2.2 Korteweg-de Vries (KdV) equation . . . 60
4.2.3 Trace identities for Schrödinger equation . . . 61
4.2.4 Soliton solutions are reflectionless potentials . . . 63
4.2.5 Field theory hierarchy . . . 64
4.3 Solitons in a lattice Gross-Neveu model . . . 65
4.3.1 Trace identities for tight-binding Hamiltonians . . . 66
4.3.2 Lattice Gross-Neveu model . . . 71
4.3.3 Construction of field theory hierarchy . . . 80
4.4 Exact construction of saddle point solutions . . . 84
4.4.1 Continuous supersymmetry . . . 84
4.4.2 Discrete supersymmetry: formalism . . . 85
4.4.3 Construction of kink solitons . . . 88
4.4.4 Construction of kink-antikink solitons . . . 93
4.5 Chiral Gross-Neveu model and superconductivity . . . 96
4.5.1 Action in terms of scattering data . . . 97
4.5.2 Soliton solutions . . . 101
4.6 Relation to the Toda hierarchy . . . 103
4.7 Conclusions . . . 105

Bibliography 109

List of Figures

1.1 Schematic of a general communication system provided by Claude Shannon in [1]. An information source generates a message to send it to a destination. A transmitter converts the message into a signal which is carried by a channel to a receiver at the destination. The receiver converts the signal back to the original message. 1

1.2 Two categories of cryptographic algorithms have been depicted. Symmetric-key algorithms use one private key, where as public-key algorithms use one public-key and another private-key. 3

2.1 The A-baker's map transforms the unit square in the left to the one in the right. The unit square is divided into A rectangles which are marked by numbers from 1 to A. Each rectangle is stretched along x axis and contracted along p axis before being stacked on top of each other. 11

2.2 The density plot of the absolute value of the matrix elements of $B_3^{(1)}$ (left) and $\tilde{B}_3^{(1)}$(right) when $N = 52$. They are mostly identical except minor difference in the cuts between the 3 segments. Both of them resemble the classical A-baker's map for $A = 3$. This is necessary but not sufficient to claim that $\tilde{B}_3^{(1)}$ reduces to 3-baker's map in semi-classical limit. 20

2.3 Comparison of the quantum evolution under $\tilde{B}_3^{+(1)}$, and the classical evolution by the 3-baker map with cyclic shift $k = 1$. The time-evolved quantum state $\tilde{B}_3^{+(1)}|\Psi\rangle$ shown in (a) follows the classical action shown in (b), and also displays the stretching in x-direction and shrinking in p-direction characteristic of the classical A-baker map. 22

2.4 Plot of the fraction of singular values vs N. The fraction approaches 1 as $N \to \infty$ 35

3.1 The outline of the circuit for modular multiplication. There are two input registers. The first one contains the state one wants to apply modular multiplication on (state $|m\rangle_L$ in the figure) and the second one contains L ancilla qubits at $|0\rangle$. The gate S acts on the second register to create an equal superposition of the basis states. Then we apply two controlled phase gate $V_A^\dagger$ and V_1. After that we apply the operator K which swaps the two registers and reset the second register to $|0\rangle$. 42
3.2 The quantum circuit to create the equal superposition state $|\Psi_N\rangle$ following the psedudocode given above. One applies controlled-Hadamard (H) after rotating a qubit by the angle θ_i given in line 4 of the algorithm. 43
3.3 Diagram of the quantum circuit for operator K_G. The circuit essentially accomplishes phase estimation in reverse for the cyclic permutation $W = \sum |m\rangle \langle m+1|$. The inputs of the circuit are the state $|m\rangle$ in the first register and the state $G_N |m\rangle$, denoted by $|\tilde{m}_G\rangle$, in the second register The $F_{2^L}^A$ operator in the circuit is a DFT like transformation defined as $F_{2^L}^A |k\rangle = 1/\sqrt{2^L} \sum_{l=0}^{2^L-1} e^{-2\pi i A k l/2^L} |l\rangle$. Note that $F_{2^L}^A$ is unitary as long as A is odd. The H gates in the diagram refers to Hadamard gate. 45
3.4 Circuit diagram for the operator $F_{2^L}^A$. In the circuit, H denotes the Hadamard gate and $R_k^A = diag(1, e^{-2\pi i A/2^k})$ are phase gates with $k \in \{2,3 \ldots L\}$. 46
3.5 Schematic of the full circuit for modular multiplication. The operator S creates an equal superposition of the basis states (see Fig. 3.2 for details).V_A and V_1 denote phase gates. W is the cyclic permutation operator, H is Hadmard gate and F_{2^L} is QFT in 2^L dimensional Hilbert space. The circuit also contains SWAP gates in two different places. 47

4.1 A schematic depicting the sequence of steps used to generate a soliton hierarchy. We start with a hierarchy of field theories (the first of which is the Gross-Neveu field theory) or a hierarchy of dynamical systems/partial differential equations (the first in the Toda hierarchy is the Toda lattice, and the third in the KdV hierarchy is the KdV equation). The equations of motion of the GN field theory and a suitable change of variables for the KdV equation/Toda lattice map these seemingly unrelated systems to a one-dimensional scattering problem. With the help of trace identities derived in this scattering problem, we may rewrite either the action or the Hamiltonian in terms of scattering data, i.e. the reflection coefficient, the transmission coefficient, and the bound state energies of the scattering problem. There are also a hierarchy of trace identities, and each one uniquely maps onto one of the field theories or dynamical systems in the original hierarchies. The saddle point of the action corresponds to a reflectionless potential, and the equations of motion of the Hamiltonian systems imply the conservation of the magnitude of the reflection coefficient. In both cases, reflectionless potentials are either valid saddle points of the action or solutions to the dynamical system. These potentials are retrieved explicitly using supersymmetry methods, or more elaborately using the Gelfand-Levitan equation and the inverse scattering formalism. 58

4.2 In the left panel, a plot of the values of ϑ as a function of the filling n_0. Here, $g = 1$ and we have chosen $N = 100$ and varied u. Also plotted in black is the approximation $\sinh 2\vartheta \approx \frac{2N}{(N-n_0)}$, which is a valid in a regime where u is large compared to $\cosh\theta$ but small compared to N^2. We even see good accuracy of the approximation beyond the regime of validity. In the right panel, a plot of the bound state energy as a function of the filling n_0. The solid lines are the corresponding bound state energies obtained from the approximation. 81

4.3 A plot of the superpotential and the superhopping obtained from iterating discrete supersymmetry for four iterations starting with a constant potential. A constant shift is applied between iterations, and the corresponding solutions share the same spectrum apart from the constant shift and an additional bound state. These solutions correspond to one such hierarchy of kink solitons. 91

4.4 A plot of the superpotential and the superhopping obtained from the discrete hyperbolic secant potential given in Eqn. (4.102) for a variety of asymptotic values of t and u. The boundary condition $\Delta_0^2 = \Delta_\star^2$ was chosen, which results in non-topological soliton solutions shown. Note that the chain is cut off after 30 lattice sites due to the exponential numerical instability caused from small deviation from $\Delta_\star$. 95

List of Figures

Chapter 1: Introduction

The onset of information age is marked by the invention of germanium based point contact transistor in 1947 at Bell labs by John Bardeen, Walter Brattain and William Shockley [2]. On the theoretical side, Claude Shannon laid the groundwork of digital communication in his seminal paper entitled 'A Mathematical theory of communication' (1948) [1]. In this paper Shannon introduced the term 'bit' as a unit of information and provided diagram of a communication system. The diagram is sketched in Fig. 1.1. As shown in the figure, a source produces a message which is converted into a signal by a transmitter. The signal is carried by a channel to a receiver which converts the signal back to the original message for the intended party. These two works, along with the development of integrated

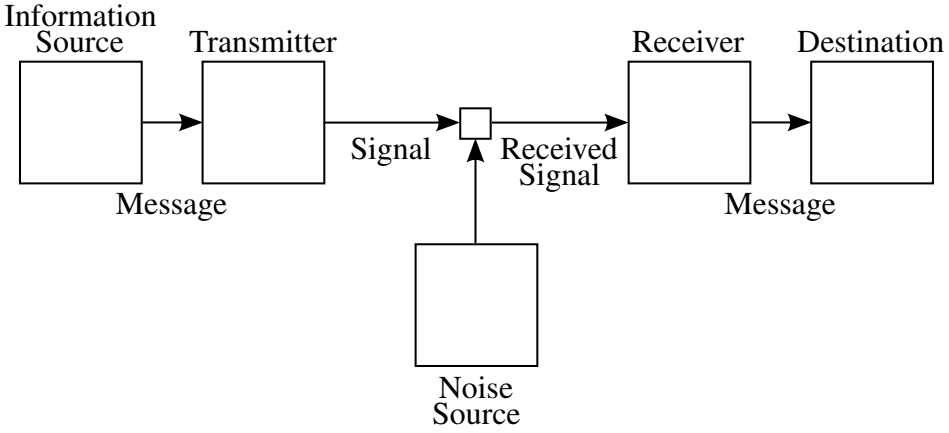
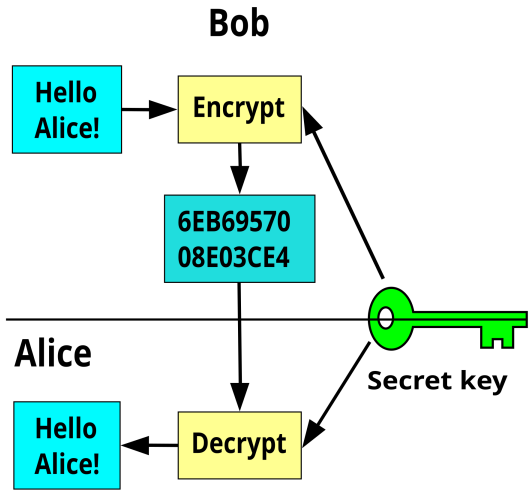


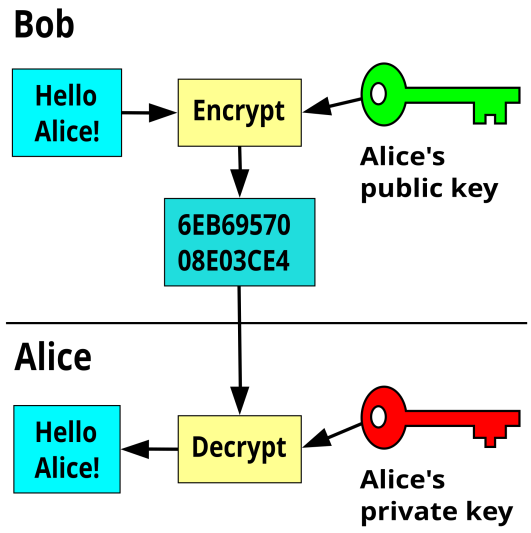
Figure 1.1: Schematic of a general communication system provided by Claude Shannon in [1]. An information source generates a message to send it to a destination. A transmitter converts the message into a signal which is carried by a channel to a receiver at the destination. The receiver converts the signal back to the original message.

circuit [3] (IC), set the stage for widespread use of digital computers. It was observed that the number density of transistors on an IC kept increasing in an exponential rate (Moore's law [4]). Consequently, modern communication system enabled transmission of unprecedented amount of information. It naturally increased interest in information security. The problem of developing protocols for secure communication, known as cryptography, has been discussed for a long time although not in a systematic way. The invention of digital computers necessitated rigorous study of cryptography. It was the same Claude Shannon who took the first step in this direction in the paper 'Communication theory of secrecy systems' [5]. As the available computational power increased, so does the need for more robust cryptographic protocols, also known as ciphers.

All ciphers can broadly be categorized into two categories: symmetric-key and asymmetric-key ciphers. Until 1976, all cryptographic protocols were of symmetric-key types. In these protocols, the same private key is used for both encryption and decryption. Some of the popular symmetric key algorithms are 3DES, Twofish, Serpent, IDEA etc. A big disadvantage of these algorithms are complexity of the key management in a communication system with many nodes. On the contrary, in asymmetric-key ciphers, information is encoded using a public key which is accessible to everyone. For decoding, one needs to use a different private key which is related to the public key in such a way that it is 'hard' to compute the private key from the public key. They key management in such protocols are less complex because the public key is the same for everyone. Fig. 1.2 depicts the basic working of the two types of protocols. The first asymmetric-key cipher was proposed by Diffe and Hellmann in 1976. One of the most commonly used public-key cryptosystem is known as RSA cryptosystem which is based on an algorithm published by Ron Rivest, Adi Shamir and Leonard Adleman [6]. In this algorithm the private-key is a pair of 'large' prime numbers and the public-key is their product. The security of this cryptosystem relies on the difficulty of finding the prime pair from their product, a problem known as prime



(a) Schematics of a symmetric-key algorithm. The sender ('Bob') and receiver ('Alice') use the same private key to encrypt and decrypt the message respectively.



(b) Schematics of an asymetric-key or public-key algorithm. Contrary to the case in 1.2a, there are two keys involved. The sender ('Bob') encrypts a message using a key, denoted by public key, which is accessible to everyone. The receiver ('Alice') decrypts the message using a separate private key.

Figure 1.2: Two categories of cryptographic algorithms have been depicted. Symmetric-key algorithms use one private key, where as public-key algorithms use one public-key and another private-key.

factorization. The problem of prime factorization belongs to the *NP* complexity class and there is no known classical algorithm which can solve it in polynomial time.

A more recent and ongoing field of research focuses on the development of a quantum computer [7–10]. Quantum computer attempts to use quantum resources like superposition, entanglement and non-deterministic measurements which are unavailable to the classical computers. In 1994, Peter Shor showed that, in theory, prime factorization can be solved efficiently on a quantum computer. Shor's algorithm boils down the prime factorization into finding the period of a unitary operator known as modular multiplication operator U_A. The operator acts on the computational basis states according to the following equation:

$$U_A \left|m\right\rangle = \left|mA \pmod N\right\rangle \tag{1.1}$$

where A, N are co-prime numbers and $m \in \{0, 1, 2 \ldots N-1\}$. The period of U_A can be calculated from the phases of the unitary. Finally the phases can be obtained efficiently on a quantum computer with the help of discrete Fourier transform and some entangling gates. In the next chapter we provide a detailed description of Shor's algorithm, which is at the heart of this dissertation.

Modern computers also influenced a different area of physics relevant to this dissertation: chaos. Similar to cryptography, the concept of chaos has been known long before the invention of computer. Most notably, while studying *n*-body problem Poincare noticed that dynamics can be strongly sensitive to initial condition. In his book 'New methods of Celestial Mechanics' Poincare stated that [11]:

"A very small cause, which eludes us, determines a considerable effect that we cannot fail to see, and so we say that this effect Is due to chance. If we knew exactly the laws of nature and the state of the universe at the initial moment, we could accurately predict the state of the same universe at a subsequent moment. But even If the natural laws no longer

held any secrets for us, we could still only know the state approximately. If this enables us to predict the succeeding state to the same approximation, that is all we require, and we say that the phenomenon has been predicted, that It Is governed by laws. But this is not always so, and small differences in the initial conditions may generate very large differences in the final phenomena. A small error in the former will lead to an enormous error In the latter. Prediction then becomes impossible, and we have a random phenomenon."

This observation, arguably, marks the birth of chaos theory. However, since the dynamics of chaotic systems are complex, many of them remained untractable until the invention of computers. With the help of computers, physicists and mathematicians were able to study intricate properties like fractal dimensions, strange attractors, density of periodic orbits etc. One of the canonical examples of chaotic sytems is Bernoulli map. Bernoulli map is defined as

$$f_A(x) = Ax \pmod 1 \tag{1.2}$$

where A is an integer and $x \in [0,1)$. Comparing it with Eq.(1.1) one can see that Bernoulli map is similar to the modular multiplication operator. **In Chapter 2 of this dissertation, we study the connection between quantum modular multiplication and Bernoulli map. We show that, modular multiplication can be written as a linear combination of quantized baker's map where the baker's map is a $2D$ analog of Bernoulli map.** Despite huge potential implications of Shor's algorithm it has not yet been implemented in any useful way. The experimental difficulties of its practical implementation are still insurmountable. Computationally, the most expensive part of Shor's algorithm is modular multiplication. **Based on our results in Chapter 2, we design a quantum circuit for modular multiplication in Chapter 3. A novel feature of our circuit is that it is constructed entirely in terms of discret Fourier transforms and its variants.**

Computers didn't only help with the analysis of chaotic systems. They are also re-

sponsible for some major breakthroughs in the dynamics of integrable systems. An early instance of such discovery is the so called Fermi-Pasta-Ulam-Tsingou problem [12, 13]. In the early 1950s, Enrico Fermi wanted to use the computer MANIAC-1 [14] at Los Alamos lab to study a physical system. After discussing with Stan Ulam and John Pasta, they decided to numerically analyze the equations of motion of a $1D$ harmonic chain of masses perturbed by non-linear force. The calculation was done by Mary Tsingou. The goal of this numerical experiment was to verify equi-partition of energy and Fermi's hypotheses that non-linearity leads to ergodicity. However the result showed a surprising recurrence in the dynamics which violated equipartition of energy. This apparent paradox was later resolved by showing that the system, in the continuum limit, reduces to Korteweg de-Vries(KdV) equation. This is an exactly solvable equation with dispersionless solutions called solitons. KdV equation can be solved using inverse scattering method where the solutions are constructed from scattering data. It turns out that solitons arise when the reflection coefficient is zero. Later it was proved that the action of Gross-Neveu model becomes minimum when the reflection coefficient vanishes. Consequently solitons minimizes the action of the system. **In the chapter 4 of this dissertation, we extend this result into discrete Gross-Neveu model. We find that in the case of discrete system, vanishing reflection coefficient is not the minimum but the saddle point of the action. We further construct a hierarchy of reflectionless potentials using tools from discrete supersymmetry.**

Chapter 2: Chaotic Roots of the Modular Multiplication Dynamical System in Shor's Algorithm

2.1 Overview

Shor's algorithm [15, 16] to factorize an integer N is a cornerstone of quantum computation [17], being exponentially faster than all known classical factorization algorithms and capable of breaking RSA encryption [18], a widely used scheme for secure data transmission. Interestingly, the success of this algorithm hinges on a foundational tension with the very notion of "quantum chaos" [19]: the quantum modular multiplication operator at the core of Shor's algorithm [15–17] belongs to a class of quantum systems that have a strongly chaotic classical limit, but violate several expected signatures of "chaos" on quantization.

The quantization of classically ergodic, chaotic systems [19, 20] is typically associated with spectral signatures such as non-degenerate energy levels and spectral rigidity, as supported by general theoretical arguments and numerical studies of several systems [19, 21–30]. Paradoxically, as indicated above, some quantizations [15, 31] of certain canonical textbook examples of classically ergodic and chaotic systems [20] – such as modular multiplication $f_A(x) = (Ax \mod N)$ on a 1D interval $x \in [0, N)$ (quantized in Shor's algorithm) and Arnold's cat map on the torus — are *exactly periodic* at long times with highly degenerate and orderly spectra [15, 32], which is at odds with ergodic quantum dynamics [30]. This is because quantization itself is not a uniquely defined procedure, and several distinct quantum systems can have the same classical limit (e.g., Refs. [15, 33–35] consider en-

tirely different quantizations of $f_2(x)$ with different spectral properties). In particular, the (conventionally) "standard" quantization of each of the above maps [15, 31] captures the dynamics of only a *measure-zero* subset of periodic orbits with a common (not necessarily fundamental) period [20, 36]. This gives the appearance of early-time "chaos" on quantization via the exponential divergence of typical nearby orbits, but completely misses out on the full ergodic and chaotic classical dynamics at late times in the bulk of the phase space.

On the one hand, the example of Shor's algorithm demonstrates a possibly generic need to eliminate "quantum chaos" in the quantization of even a classically chaotic map, for its successful utilization in certain quantum algorithms. On the other, it also suggests the more fundamental question of whether appropriate manifestations of quantum ergodicity and chaos can be hidden in some way even in such non-ergodic quantizations. Interestingly, a partial resolution to this question was noted in Refs. [37, 38], where it was shown [38] that the unitary operator implementing modular multiplication by $A = 2$ in Shor's algorithm can be expressed as a superposition of quantized baker's maps [34, 39], which may be regarded as "chaotic" quantizations of $f_2(x)$ [more precisely, of baker's maps [20] in a 2D phase space (x, p) whose action on the position coordinate $x \in [0, 1)$ is identical to $f_2(Nx)/N$] that by and large exhibit the expected signatures of quantum chaos and ergodicity [34, 35].

In this work, we show that this "embedding" of a superposition of "quantum chaotic" maps in the periodic modular multiplication map generalizes to an arbitrary multiplier A. The appropriate chaotic maps are direct generalizations of the 2D A-baker's maps (extensions of baker's maps whose 1D projection is $f_A(Nx)/N$), and these maps can be quantized in terms of certain combinations of discrete Fourier transforms [34], when either $N + 1$ or $N - 1$ is a multiple of A. This establishes a rigorous correspondence between specific "ergodic" and "non-ergodic" quantizations of $f_A(x)$ for arbitrary A, which may serve as a simple model for understanding the interplay of integrability, ergodicity and chaos in different quantizations of the same system. We will now present the details of this correspon-

dence, and subsequently discuss both its potential implications for studying the embedding of quantum chaos in Shor's algorithm, and in extending the quantization of A-baker's maps to arbitrary N.

2.2 Overview of Shor's algorithm, Baker's map and its quantization

In this section we will provide a brief overview of Shor's algorithm, Baker's map and its quantization. This will set the platform for our main result. Let us first recall the problem of prime factorization.

2.2.1 Shor's algorithm

Suppose N is a number obtained by multiplying two prime numbers p and q. The problem of interest is: Given the number N how to find its prime factors p and q? This problem belongs to NP and co-NP complexity classes. However it is not known if it belongs to either P or NP-complete complexity class. One can find the factors of N by finding the multiplicative order modulo N of another integer A which is co-prime to N. This follows from the following theorem:

Theorem 2.1. *If $A < N$ is co-prime to N with multiplicative order r modulo N and r is even then* $\gcd(A^{r/2}-1, N)$ *is either* 1 *or a prime factor of N.*

Proof. Since A is with multiplicative order r modulo N we know N divides $A^r - 1$ written as $N \mid A^r - 1$ and r is the smallest positive integer to do so. If r is even it further implies that $N|(A^{r/2}-1)(A^{r/2}+1)$. Now $N \nmid A^{r/2}-1$ because it contradicts r being the multiplicative order. So one must have either $\gcd(A^{r/2-1}, N) = 1$ or $\gcd(A^{r/2-1}, N) = p \vee q$. □

Shor's algorithm utilizes quantum phase estimation(QPE) procedure to find the multiplicative order of A. One can efficiently find the phase of a unitary operator using QPE.

The unitary used in Shor's algorithm is the modular multiplication operator U_A. Given two co-primes N and A $(A < N)$, U_A is defined in an N dimensional Hilbert space according to the equation:

$$U_A \left|m\right\rangle = \left|mA \pmod N\right\rangle, \text{ for } m \in \{0, 1 \ldots N-1\}, \tag{2.1}$$

where $\{\left|0\right\rangle, \left|1\right\rangle \ldots \left|N-1\right\rangle\}$ forms an orthonormal basis. Note that if r is the order of A then $U_A^r = \mathbb{1}$. So, the eigenvalues of U_A are $e^{2\pi i s/r}$ with $s \in \{0, 1 \ldots, r-1\}$. The output of Shor's algorithm is the fraction s/r from which the value of r is extracted.

The modular multiplication U_A has connection with chaos theory. U_A can be regarded as a quantization of $f_A(x)$, as a generic narrow wavepacket of width $w \ll N$ centered at some x_0 remains narrowly distributed around the classical trajectory of x_0 up to an Ehrenfest time [40, 41] $t_E \sim \ln(N/w)/\ln A$ determined by the Lyapunov exponent $\lambda = \ln A$. However, since N and A are co-primes, quantum modular multiplication is an exactly periodic unitary operator at longer time scales, which permutes the basis states according to Eq. (2.1).

2.2.2 Baker's map

The classical A-baker's map, a generalization of baker's map, is a canonical example of an ergodic and chaotic system [42]. It maps a unit square to itself by stretching in one direction and compressing in the perpendicular direction in such a way that the total area of the square is preserved, and rearranging the stretched square to fit inside the unit square. The map is defined by the following transformation:

$$x \to x' = Ax - \lfloor Ax \rfloor, \tag{2.2}$$

$$p \to p' = \frac{p + \lfloor Ax \rfloor}{A}. \tag{2.3}$$

Here $(x, p) \in [0,1) \times [0,1)$ are phase space coordinates and $\lfloor x \rfloor$ denotes the integer part of x. The map is illustrated in Fig. 2.1. The unit square is divided into A rectangles of equal area as shown in the left side of Fig. 2.1. Each of the rectangles is stretched by a factor of A along the horizontal direction and by $1/A$ along the vertical direction. Then the rectangles are stacked on top of each other as shown on the right side of Fig. 2.1. When $A = 2$ the

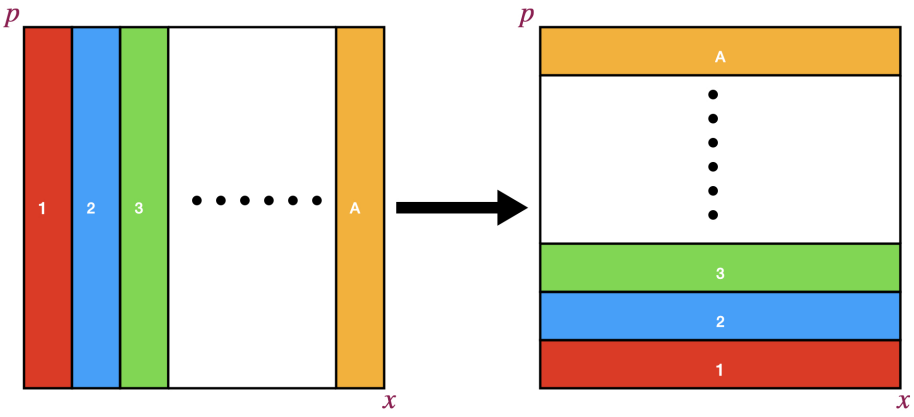


Figure 2.1: The A-baker's map transforms the unit square in the left to the one in the right. The unit square is divided into A rectangles which are marked by numbers from 1 to A. Each rectangle is stretched along x axis and contracted along p axis before being stacked on top of each other.

A-baker's map reduces to the standard baker's map [43].

As with any classical dynamical system, there is no unique way to quantize the A-baker's map. By convention, the basic requirements are that the quantum map is unitary and it reduces to the classical map in the semi-classical limit. Several quantization procedures satisfying these requirements have been developed for A-baker's map [34, 35, 42, 44–46]. In this paper, we will use the quantization procedure developed by Balazs and Voros (BV)[34]. In BV quantization, one replaces the phase space of the classical map with a D dimensional Hilbert space. Suppose $\{|x_n\rangle\}_{n=0}^{D-1}$ and $\{|p_m\rangle\}_{m=0}^{D-1}$ are two different complete

basis. We assume that they satisfy the following boundary conditions:

$$|x_{n+D}\rangle = e^{-2\pi i\beta}\,|x_n\rangle\,, \tag{2.4}$$

$$|p_{n+D}\rangle = e^{2\pi i\alpha}\,|p_n\rangle\,. \tag{2.5}$$

When $\alpha = \beta = 0$ it becomes periodic boundary condition. Physically one can think of these two basis as the eigenbasis of discrete position and momentum operator. The inner product of them is

$$\langle p_m|x_n\rangle = \frac{1}{\sqrt{D}} e^{-\frac{2\pi i(n+\alpha)(m+\beta)}{D}} = [F_D^{\alpha,\beta}]_{nm}, \tag{2.6}$$

where $F_D^{\alpha,\beta}$ is a $D\times D$ DFT matrix with phase α and β. Let's look at an arbitrary state $|\psi\rangle$ in the Hilbert space. We write the state as

$$\begin{aligned}
|\psi\rangle &= \sum_{n=0}^{D-1} |x_n\rangle\langle x_n|\psi\rangle \\
&= \sum_{n=0}^{\frac{D}{A}-1} |x_n\rangle\langle x_n|\psi\rangle + \sum_{n=\frac{D}{A}}^{\frac{2D}{A}-1} |x_n\rangle\langle x_n|\psi\rangle \ldots \sum_{n=\frac{D(A-1)}{A}}^{D-1} |x_n\rangle\langle x_n|\psi\rangle \\
&= \sum_{l=1}^{A} |\psi_l\rangle\,,
\end{aligned} \tag{2.7}$$

where $|\psi_l\rangle = \sum_{n=D(l-1)/A}^{Dl/A-1} |x_n\rangle\langle x_n|\psi\rangle$. Essentially we have partitioned the state in such a way that the projection of each partition into position basis can have non-zero value only inside a region. The regions are obtained from the equation

$$\langle x_n|\psi_l\rangle = 0 \;\text{ for }\; 0 \le n \le \frac{D(l-1)}{A} - 1 \;\text{ and }\; \frac{Dl}{A} \le n \le D-1. \tag{2.8}$$

The quantized A-baker's map is the unitary operator $B_A^{(0)}$ such that

$$B_A^{(0)}|\psi_l\rangle = |\phi_l\rangle \quad \text{for} \quad l = 1,2\ldots A. \tag{2.9}$$

Eq. (2.9) implies that $B_A^{(0)}|\psi\rangle = \sum_{l=1}^{A}|\phi_l\rangle \equiv |\phi\rangle$. The states $|\phi_l\rangle$ are defined in a similar way as Eq. (2.7) but in momentum basis i.e. $|\phi_l\rangle = \sum_{n=\frac{D(l-1)}{A}}^{\frac{Dl}{A}-1}|p_n\rangle\langle p_n|\phi\rangle$. Furthermore $|\phi_l\rangle$ satisfies

$$\langle x_{An}|\phi_l\rangle = \frac{1}{\sqrt{A}}\langle x_n|\psi_l\rangle \quad \text{for} \quad \frac{D(l-1)}{A} \leq n \leq \frac{Dl}{A} - 1, \tag{2.10}$$

$$\langle p_n|\phi_l\rangle = \sqrt{A}\langle p_{An}|\psi_l\rangle \quad \text{for} \quad \frac{D(l-1)}{A} \leq n \leq \frac{Dl}{A} - 1. \tag{2.11}$$

Eqs. (2.10) and (2.11) are analogous to expansion and contraction in the classical map. We insert a resolution of identity in Eq. (2.11) and use the inner product of $|x_n\rangle$ and $|p_m\rangle$ to write

$$\begin{aligned}
\langle p_n|\phi_l\rangle &= \sqrt{A}\sum_{m=0}^{D-1}\langle p_{An}|x_m\rangle\langle x_m|\psi_l\rangle \qquad \text{for} \quad \frac{D(l-1)}{A} \leq n \leq \frac{Dl}{A} - 1 \\
&= \sqrt{\frac{A}{D}}\sum_{m=0}^{D-1} e^{-\frac{2\pi i A(n+\alpha)(m+\beta)}{D}}\langle x_m|\psi_l\rangle \\
&= \sum_{m=\frac{D(l-1)}{A}}^{\frac{Dl}{A}-1}(F_{\frac{D}{A}}^{\alpha,\beta})_{nm}\langle x_m|\psi_l\rangle\,. \qquad \text{[using Eq. (2.8)]}
\end{aligned} \tag{2.12}$$

Note that $|\phi_l\rangle$ is defined in such a way that $\langle p_n|\phi_l\rangle$ when $\leq n \leq \frac{D(l-1)}{A} - 1$ and $\frac{Dl}{A} \leq n \leq D-1$. Combining it with Eq. (2.12) we get a relation between $|\phi_l\rangle$ and $|\psi_l\rangle$. However, in Eq. (2.12) they are in different representation. One can show that $\langle p_n|\phi_l\rangle =$

$\sum_{m=0}^{D-1}(F_D^{\alpha,\beta})_{mn}\langle x_m|\phi_l\rangle$. Consequently we can rewrite Eq. (2.12) as

$$\langle x_n|\phi_l\rangle = \sum_{k=0}^{D-1}\sum_{m=\frac{D(l-1)}{A}}^{\frac{Dl}{A}-1}(F_D^{\alpha,\beta})^{-1}_{nk}(F_{\frac{D}{A}}^{\alpha,\beta})_{km}\langle x_m|\psi_l\rangle\,. \tag{2.13}$$

We compare Eq. (2.13) with Eq. (2.9) to get an expression for quantized A-baker's map $B_A^{(0)}$:

$$B_A^{(0)} = (F_D^{\alpha,\beta})^{-1}\begin{bmatrix} F_{\frac{D}{A}}^{\alpha,\beta} & 0 & 0 & \dots & 0 \\ 0 & F_{\frac{D}{A}}^{\alpha,\beta} & 0 & \dots & 0 \\ 0 & 0 & F_{\frac{D}{A}}^{\alpha,\beta} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & F_{\frac{D}{A}}^{\alpha,\beta} \end{bmatrix}. \tag{2.14}$$

We have derived the matrix form of B_A^0 without using Eq. (2.10) . But one can check that $B_A^{(0)}$ is consistent with Eq. (2.10). For periodic boundary conditions ($\alpha=\beta=0$), $F_D^{\alpha,\beta}$ reduces to the standard DFT matrix. For notational convenience we will denote the standard DFT matrix simply by F_D. Note that D/A in Eq. (2.14) should be an integer which requires D to be a multiple of A.

One can modify the A-baker's map so that the rectangles in the right side of Fig. 2.1 are stacked differently, and then use the same BV procedure to quantize this modified map. For example, if all the rectangles in the right side of Fig. 2.1 are cyclically permuted by one step so that now 1 goes to A, 2 goes to 1 ... 3 goes to 2, we get a different quantized map $B_A^{(1)}$. Similarly one can construct other quantum maps $B_A^{(2)}, B_A^{(3)} \dots B_A^{(A-1)}$ by cyclically permuting the horizontal rectangles by 2, 3,...,$A-1$ steps respectively. The general

equation for the A-baker's map $B_A^{(k)}$ is

$$B_A^{(k)} = [F_D^{\alpha,\beta}]^{-1} \begin{array}{c} \begin{array}{cccccc} 0 & \dots & k-1 & k & \dots & A-1 \end{array} \\ \begin{bmatrix} 0 & \dots & 0 & F_{\frac{D}{A}}^{\alpha,\beta} & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & F_{\frac{D}{A}}^{\alpha,\beta} \\ F_{\frac{D}{A}}^{\alpha,\beta} & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & F_{\frac{D}{A}}^{\alpha,\beta} & 0 & \dots & 0 \end{bmatrix} \end{array}, \tag{2.15}$$

where $k \in \{0, 1, ...A-1\}$. When $k = 0$ it reduces to Eq. (2.14).

2.3 Results

Now we've all the tools required to derive the main result of our paper. Given two co-prime integers N and A such that $N = Aq \pm 1$ where q is an integer, the corresponding modular multiplication operator $U_A^{\pm}$ can written to act instead on $D = Aq$ states (rather than on $N = Aq \pm 1$ as usual). This operator is obtained in the case $N = Aq + 1$ by removing the state $|0\rangle$ which is always a fixed point, $U_A^{+}|0\rangle = |0\rangle$, and in the case $N = Aq - 1$ by adding a Dth state $|D-1\rangle$, with the extension $U_A^{-}|D-1\rangle = |D-1\rangle$ which agrees with the original map defined in Eq. (2.1). The modular multiplication map dynamics are thus preserved, but the advantage is the number of states is now a multiple of A. With these conventions,

the $Aq \times Aq$ representation of the modular multiplication operator $U_A^{\pm}$ can be expressed as

$$U_A^{\pm} = F_{Aq}^{-1} \begin{bmatrix} F_q & F_q^{0,\mp\frac{1}{A}} & F_q^{0,\mp\frac{2}{A}} & \dots & F_q^{0,\mp\frac{A-1}{A}} \\ F_q & F_q^{0,\mp\frac{1}{A}} & F_q^{0,\mp\frac{2}{A}} & \dots & F_q^{0,\mp\frac{A-1}{A}} \\ F_q & F_q^{0,\mp\frac{1}{A}} & F_q^{0,\mp\frac{2}{A}} & \dots & F_q^{0,\mp\frac{A-1}{A}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ F_q & F_q^{0,\mp\frac{1}{A}} & F_q^{0,\mp\frac{2}{A}} & \dots & F_q^{0,\mp\frac{A-1}{A}} \end{bmatrix} \odot \tilde{F}_{Aq}^{\mp}. \tag{2.16}$$

Here $\odot$ denotes Hadamard or entry-wise product of two matrices defined as $(A \odot B)_{ij} = A_{ij}B_{ij}$ and $\tilde{F}_{Aq} = F_A^{\mp} \otimes J_q$ with J_q being a $q \times q$ matrix with all elements equal to 1, F_A^+ the $A \times A$ DFT matrix with no phase, F_A^- the conjugate of F_A^+ and $\otimes$ denoting tensor product. The derivation is slightly different for two cases of $N = qA \pm 1$. We will do the calculation for $N = Aq + 1$ and point out the differences with $N = Aq - 1$ case.

Let's recall the definition of modular multiplication U_A:

$$U_A |m\rangle = |mA \pmod N\rangle \text{ for } m = 0, 1 \dots, N-1. \tag{2.17}$$

From the definition one can see that the state $|0\rangle$ is always a fixed point of the modular multiplication. When $N = Aq+1$ we remove the $|0\rangle$ state such that the number of remaining states is a multiple of A. We denote this operator of dimension $Aq \times Aq$ as U^+. Using Eq. (2.1) we find that

$$\langle n| U_A^+ |m\rangle = \delta_{n,Am-lN} \quad \text{for} \quad lq+1 \leq m \leq (l+1)q \quad \text{and} \quad l = 0, 1 \dots, A-1. \tag{2.18}$$

Here $\delta_{n,m}$ denotes Kronecker delta function. Since we have removed the $|0\rangle$ state all the

blocks with same l have the same size. The Kronecker delta function can be written as

$$\begin{aligned}
\delta_{n,Am-lN} &= \frac{1}{Aq}\sum_{k=1}^{Aq} e^{\frac{2\pi ik(n-Am+lN)}{Aq}} \\
&= \frac{1}{Aq}\sum_{k=1}^{Aq} e^{\frac{2\pi ikn}{Aq}} e^{\frac{-2\pi ik(m-\frac{l}{A})}{q}} \\
&= \frac{1}{Aq}[\sum_{k=1}^{q} e^{\frac{2\pi ikn}{Aq}} e^{\frac{-2\pi ik(m-\frac{l}{A})}{q}} + \sum_{k=q+1}^{2q} e^{\frac{2\pi ikn}{Aq}} e^{\frac{-2\pi ik(m-\frac{l}{A})}{q}} \cdots + \sum_{k=(A-1)q+1}^{Aq} e^{\frac{2\pi ikn}{Aq}} e^{\frac{-2\pi ik(m-\frac{l}{A})}{q}}] \\
&= \frac{1}{Aq}[\sum_{k=1}^{q} e^{\frac{2\pi ikn}{Aq}} e^{\frac{-2\pi ik(m-\frac{l}{A})}{q}} + \sum_{k=1}^{q} e^{\frac{2\pi i(k+q)n}{Aq}} e^{\frac{-2\pi ik(m-\frac{l}{A})}{q}} e^{\frac{-2\pi il}{A}} \cdots + \sum_{k=1}^{q} e^{\frac{2\pi i[k+(A-1)q]n}{Aq}} e^{\frac{-2\pi ik(m-\frac{l}{A})}{q}} e^{\frac{-2\pi il(A-1)}{A}}] \\
&= \frac{1}{\sqrt{A}}\sum_{k=1}^{q} [(F_{Aq})^{-1}_{nk}(F_q^{0,-\frac{l}{A}})_{km} + (F_{Aq})^{-1}_{n(k+q)}\omega_A^l(F_q^{0,-\frac{l}{A}})_{km} \cdots + (F_{Aq})^{-1}_{n[k+(A-1)q]}\omega_A^{l(A-1)}(F_q^{0,-\frac{l}{A}})_{km}]
\end{aligned} \tag{2.19}$$

Here $\omega_A = e^{\frac{2\pi i}{A}}$ is the A^{th} root of unity. We have expressed the elements of modular multiplication in terms of DFT matrices. Using Eq. (2.19) we can write modular multiplication as

$$U_A^+ = \frac{1}{\sqrt{A}}F_{Aq}^{-1}\begin{bmatrix}
F_q & F_q^{0,-\frac{1}{A}} & F_q^{0,-\frac{2}{A}} & \dots & F_q^{0,-\frac{A-1}{A}} \\
F_q & \omega_A^1 F_q^{0,-\frac{1}{A}} & \omega_A^2 F_q^{0,-\frac{2}{A}} & \dots & \omega_A^{A-1} F_q^{0,-\frac{A-1}{A}} \\
F_q & \omega_A^2 F_q^{0,-\frac{1}{A}} & \omega_A^4 F_q^{0,-\frac{2}{A}} & \dots & \omega_A^{2(A-1)} F_q^{0,-\frac{A-1}{A}} \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
F_q & \omega_A^{A-1} F_q^{0,-\frac{1}{A}} & \omega_A^{2(A-1)} F_q^{0,-\frac{2}{A}} & \dots & \omega_A^{(A-1)^2} F_q^{0,-\frac{A-1}{A}}
\end{bmatrix}. \tag{2.20}$$

We can utilize Hadamard product to rewrite Eq. (2.20) as

$$U_A^+ = F_{Aq}^{-1} \begin{bmatrix} F_q & F_q^{0,-\frac{1}{A}} & F_q^{0,-\frac{2}{A}} & \dots & F_q^{0,-\frac{A-1}{A}} \\ F_q & F_q^{0,-\frac{1}{A}} & F_q^{0,-\frac{2}{A}} & \dots & F_q^{0,-\frac{A-1}{A}} \\ F_q & F_q^{0,-\frac{1}{A}} & F_q^{0,-\frac{2}{A}} & \dots & F_q^{0,-\frac{A-1}{A}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ F_q & F_q^{0,-\frac{1}{A}} & F_q^{0,-\frac{2}{A}} & \dots & F_q^{0,-\frac{A-1}{A}} \end{bmatrix} \odot \frac{1}{\sqrt{A}} \begin{bmatrix} \omega_A^0 & \omega_A^0 & \omega_A^0 & \dots & \omega_A^0 \\ \omega_A^0 & \omega_A & \omega_A^2 & \dots & \omega_A^{A-1} \\ \omega_A^0 & \omega_A^2 & \omega_A^4 & \dots & \omega_A^{2(A-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \omega_A^0 & \omega_A^{A-1} & \omega_A^{2(A-1)} & \dots & \omega_A^{(A-1)^2} \end{bmatrix} \otimes J_q$$

$$= F_{Aq}^{-1} \begin{bmatrix} F_q & F_q^{0,-\frac{1}{A}} & F_q^{0,-\frac{2}{A}} & \dots & F_q^{0,-\frac{A-1}{A}} \\ F_q & F_q^{0,-\frac{1}{A}} & F_q^{0,-\frac{2}{A}} & \dots & F_q^{0,-\frac{A-1}{A}} \\ F_q & F_q^{0,-\frac{1}{A}} & F_q^{0,-\frac{2}{A}} & \dots & F_q^{0,-\frac{A-1}{A}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ F_q & F_q^{0,-\frac{1}{A}} & F_q^{0,-\frac{2}{A}} & \dots & F_q^{0,-\frac{A-1}{A}} \end{bmatrix} \odot [F_A^{-1} \otimes J_q]. \tag{2.21}$$

When $N = Aq - 1$ we add the state $|N\rangle$, which is a fixed state, so that the total number of states is a multiple of A. After adding the extra state we denote the operator as U^- and perform a similar calculation as above to find

$$U_A^- = F_{Aq}^{-1} \begin{bmatrix} F_q & F_q^{0,\frac{1}{A}} & F_q^{0,\frac{2}{A}} & \dots & F_q^{0,\frac{A-1}{A}} \\ F_q & F_q^{0,\frac{1}{A}} & F_q^{0,\frac{2}{A}} & \dots & F_q^{0,\frac{A-1}{A}} \\ F_q & F_q^{0,\frac{1}{A}} & F_q^{0,\frac{2}{A}} & \dots & F_q^{0,\frac{A-1}{A}} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ F_q & F_q^{0,\frac{1}{A}} & F_q^{0,\frac{2}{A}} & \dots & F_q^{0,\frac{A-1}{A}} \end{bmatrix} \odot [F_A \otimes J_q]. \tag{2.22}$$

To extract the quantized A-baker's maps embedded in Eq. (2.16), we rewrite it as:

$$U_A^{\pm} = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} \tilde{B}_A^{\pm(k)}, \tag{2.23}$$

where $\tilde{B}_A^{\pm(k)}$ are quantized maps similar to the ones obtained in Eq. (2.15) but with some differences. Let us write the explicit form of $\tilde{B}_A^{\pm(k)}$ to identify the differences:

$$\tilde{B}_A^{\pm(k)} = F_{Aq}^{-1} \begin{array}{c} \begin{matrix} 0 & \dots & k-1 & k & \dots & A-1 \end{matrix} \\ \begin{bmatrix} 0 & \dots & 0 & F_q^{0,\mp\frac{k}{A}} & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & \dots & F_q^{0,\mp\frac{A-1}{A}} \\ F_q & \dots & 0 & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & F_q^{0,\mp\frac{k-1}{A}} & 0 & \dots & 0 \end{bmatrix} \end{array} \odot \tilde{F}_{Aq}^{\mp}. \tag{2.24}$$

Comparing Eq. (2.24) with Eq. (2.15) we notice two main differences: (i) In $\tilde{B}_A^{\pm(k)}$, the inverse of F_{Aq} has no phase and the phases of each $q \times q$ DFT matrices are different but in $B_A^{(k)}$ all of them have same phase, (ii) The Hadamard product in Eq. (2.24) is absent in Eq. (2.15). Despite these differences, the evolution of states under the operators $\tilde{B}_A^{\pm(k)}$ is very similar to that of $B_A^{(k)}$ in the semi-classical limit, and we will call $\tilde{B}_A^{\pm(k)}$ *quantum A-baker's maps*. We note that if we plot the matrix elements of $\tilde{B}_A^{\pm(k)}$ they resemble classical Bernoulli maps in the same way as the $B_A^{(k)}$ do (Fig. 2.2), although as we explain shortly this is not a sufficient criterion.

2.4 Semiclassical limit of the quantized baker's map

To justify calling $\tilde{B}_A^{\pm(k)}$ a quantum A-baker's map, we previously noted that the matrix elements of $\tilde{B}_A^{\pm(k)}$ in the position basis (and momentum basis) trace out the classical 1D action of the position (momentum) coordinate in the A-baker map defined in Eqs. (2.2-2.3). However, this is not sufficient to conclude that $\tilde{B}_A^{\pm(k)}$ has the correct semi-classical behavior,

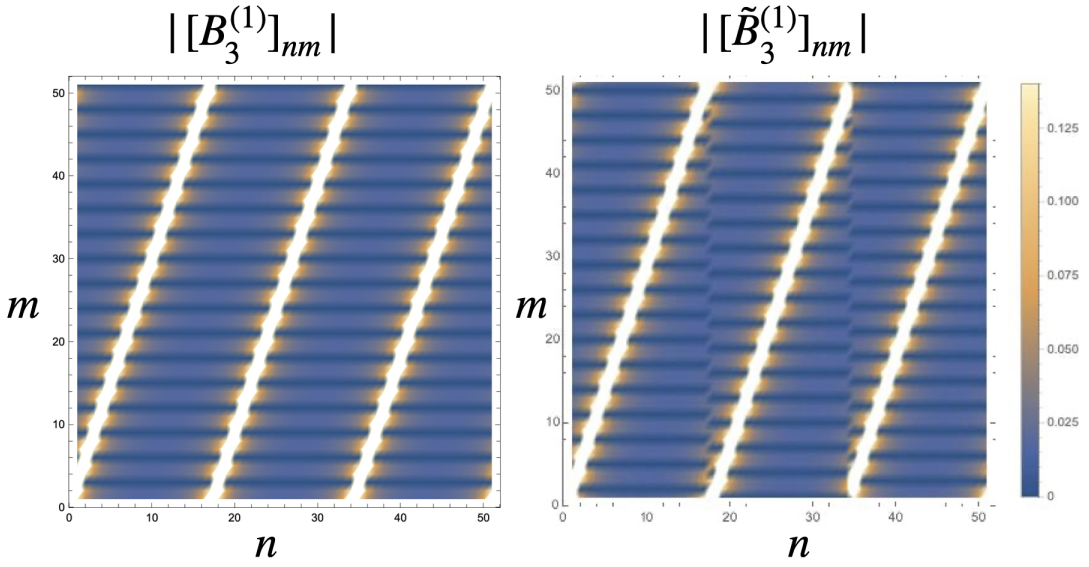


Figure 2.2: The density plot of the absolute value of the matrix elements of $B_3^{(1)}$ (left) and $\tilde{B}_3^{(1)}$(right) when $N = 52$. They are mostly identical except minor difference in the cuts between the 3 segments. Both of them resemble the classical A-baker's map for $A = 3$. This is necessary but not sufficient to claim that $\tilde{B}_3^{(1)}$ reduces to 3-baker's map in semi-classical limit.

as the Walsh baker quantizations considered in [42] also display this behavior, but as shown in [47] are not quantizations of the baker map. Instead the semi-classical limit there has to be interpreted as a "stochastic" or "multi-valued" baker map. One explanation for this is that even if the maps look classically correct in pure position or pure momentum basis, they may not entwine position and momentum together correctly. For a more rigorous analysis, we determine the action of $\tilde{B}_A^{\pm(k)}$ on Gaussian states ("coherent states") maximally localized at a point (x, p) in phase space. We show that $\tilde{B}_A^{\pm(k)}$ sends such a state to another coherent state localized close to the classical evolution location $(Ax - \lfloor Ax \rfloor, \frac{p+(\lfloor Ax \rfloor - k) \bmod A}{A})$. We only do this for (x, p) away from the discontinuities of the classical A-baker map, otherwise there can be diffraction effects [44, 48, 49]. The action on coherent states can be interpreted in terms of the Wigner or Husimi function in phase space: A state whose Wigner/Husimi function is localized near (x, p) is transformed by $\tilde{B}_A^{\pm(k)}$ to a state localized near the classical

trajectory point $(Ax - \lfloor Ax \rfloor, \frac{p+(\lfloor Ax \rfloor - k) \bmod A}{A})$. This correspondence between quantum and classical evolution is shown visually in Fig. 2.3.

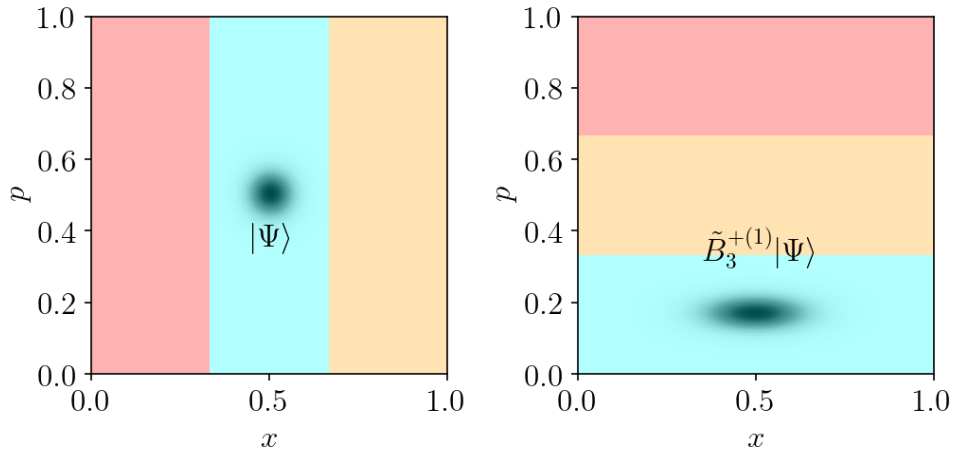
Such an action on Gaussian states was used in [49] to prove a rigorous classical-quantum correspondence (Egorov-type theorem [49, Theorem 12]) for the original Balazs–Voros quantization of the baker map. In the case here, we will be content with just analyzing the behavior of $\tilde{B}_A^{\pm(k)}$ on Gaussian states. Due to the varying phases in the DFT matrices in Eq. (2.24), the action on Gaussian states will be more complicated than in the original Balazs–Voros quantization. In particular, the quantum evolved state here is actually centered a distance $\mathscr{O}_A(D^{-1})$ away from the classical trajectory point, though this will still be close enough for our purposes to the Gaussian state actually centered at the classical trajectory.

The computations here will be very similar to those in [49, Prop. 5], though the addition of the phases α and β in the generalized DFT matrices will require some additional consideration, e.g. Eq. (2.31).

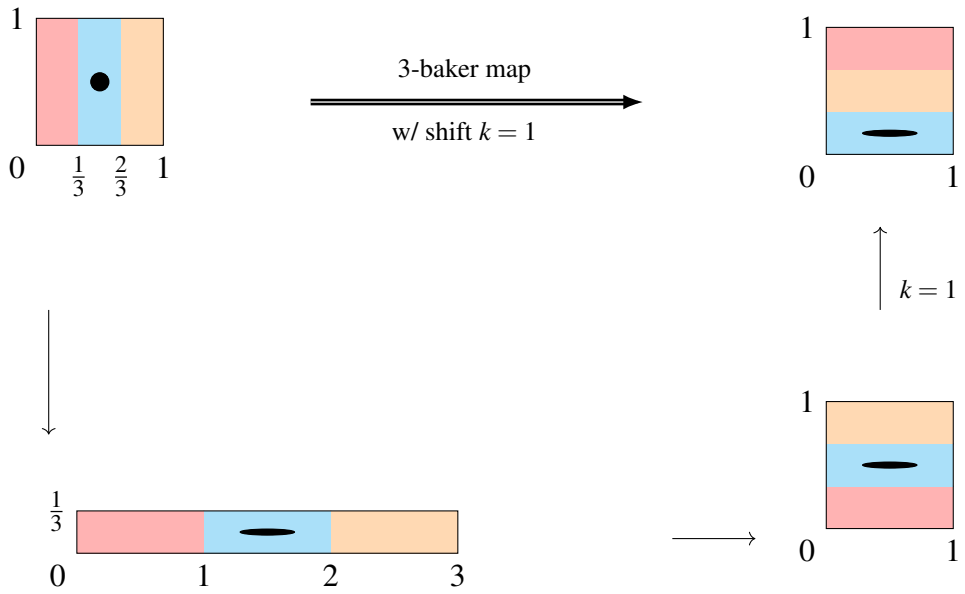
Besides cyclic shifts by k elements, we will allow any permutation of blocks in $\tilde{B}_A^{+(0)}$ in Eq. (2.24). To this end, let $\Pi : \{0,\ldots,A-1\} \to \{0,\ldots,A-1\}$ be a permutation on A elements, and let P_Π be the $A \times A$ permutation matrix corresponding to Π. To make this permutation act on blocks, define the $D \times D$ matrix $P_{D,\Pi} := P_\Pi \otimes I_{D/A}$, where $I_{D/A}$ is the $D/A \times D/A$ identity matrix. Then for $D \in A\mathbb{N}$, define

$$\tilde{B}_A^{(\Pi)} := F_D^{-1} P_{D,\Pi} \begin{bmatrix} \omega_0 F_{D/A}^{\alpha_0,\beta_0} & 0 & \cdots & 0 \\ 0 & \omega_1 F_{D/A}^{\alpha_1,\beta_1} & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & \omega_{A-1} F_{D/A}^{\alpha_{A-1},\beta_{A-1}} \end{bmatrix}, \tag{2.25}$$

where ω_j are arbitrary phase factors, $\alpha_j, \beta_j \in [-1,1]$, and $P_{D,\Pi}$ acts by permuting row



(a) Phase space plots (Husimi functions) of the quantum evolution of a Gaussian state $|\Psi\rangle$ by $\tilde{B}_3^{+(1)}$, for $D = 150$. The state $|\Psi\rangle$ is localized at $(x,p) = (\frac{1}{2},\frac{1}{2})$, and its time evolved state $\tilde{B}_3^{+(1)}|\Psi\rangle$ is localized near the classical trajectory point $(3x-1, \frac{p+(1-1)}{3}) = (\frac{1}{2},\frac{1}{6})$. The colored rectangles are overlayed for easier comparison to the classical map in (b).



(b) Classical evolution of the unit square by the 3-baker map with cyclic shift $k = 1$, which sends $(x,p) \mapsto (3x - \lfloor 3x \rfloor, \frac{p+(\lfloor Ax \rfloor - 1) \bmod A}{A})$. The total classical transformation is shown in the top row, while the intermediate components of stretching, cutting and stacking, and cyclic permutation are shown through the two stages in the bottom row. The action on a disk is also shown for comparison to part (a).

Figure 2.3: Comparison of the quantum evolution under $\tilde{B}_3^{+(1)}$, and the classical evolution by the 3-baker map with cyclic shift $k = 1$. The time-evolved quantum state $\tilde{B}_3^{+(1)}|\Psi\rangle$ shown in (a) follows the classical action shown in (b), and also displays the stretching in x-direction and shrinking in p-direction characteristic of the classical A-baker map.

blocks on the block matrix to the right according to Π. In this notation, $\tilde{B}_A^{\pm(k)}$ from the main text corresponds to the special case of $\tilde{B}_A^{(\Pi)}$, where Π is the cyclic shift by k elements $\Pi^{(k)} : n \mapsto n-k \bmod A$, $\alpha_j = 0$, $\beta_j = \mp j/A$, and $\omega_j = e^{\pm 2\pi i j(j-k \bmod A)/D}$. For later use it will also be useful to define $\tilde{B}_A^{(\Pi)}$ in a mixed position-momentum basis,

$$\tilde{B}_{A,\mathrm{mix}}^{(\Pi)} := F_D \tilde{B}_A^{(\Pi)}. \tag{2.26}$$

The associated classical map on the torus will be

$$S_A^{(\Pi)}(x,p) := \Big(Ax - \lfloor Ax \rfloor, \frac{p+\Pi(\ell)}{A}\Big), \quad \text{for } x \in \Big[\frac{\ell}{A}, \frac{\ell+1}{A}\Big),\ \ell = 0,\dots,A-1. \tag{2.27}$$

This is just the classical A-baker map with the permutation Π applied to the stacking of the blocks shown on the right side of Figure 2.1. Note that for $x \in [\frac{\ell}{A}, \frac{\ell+1}{A})$, that $\ell = \lfloor Ax \rfloor$.

We work on the D-dimensional Hilbert space of periodic states. Usually one would associate $F_{D/A}^{\alpha_j,\beta_j}$ with the Hilbert space of *quasi*-periodic states corresponding to phase factors α, β, but since we work with several different α_j, β_j, there is no single particularly favored choice of phase conditions, and so we pick the periodic (no phase) boundary conditions for simplicity. We first consider the $\mathbb{R}^2$-Gaussian state (also called "coherent state") localized at a point $F_0 = (x_0, p_0) \in \mathbb{R}^2$ with squeezing parameter $\sigma > 0$,

$$\Psi_{F_0,\sigma}(x) = (2D\sigma)^{1/4} e^{-\pi i D x_0 p_0} e^{2\pi i D p_0 x} e^{-\sigma D \pi (x-x_0)^2}, \quad x \in \mathbb{R}.$$

The corresponding torus coherent state $\Psi_{F,\sigma,\mathbb{T}^2} \in \mathbb{C}^D$ is obtained by periodicizing the $\mathbb{R}^2$-state in position and momentum, resulting in

$$\langle m | \Psi_{F_0,\sigma,\mathbb{T}^2} \rangle = \sum_{v \in \mathbb{Z}} \Psi_{F_0,\sigma}\Big(\frac{m}{D} + v\Big), \quad m \in \mathbb{Z}/D\mathbb{Z}. \tag{2.28}$$

For further details, see [49, 50].

The main properties we will use, in addition to the explicit formula for a Gaussian state, are the following.

1. For $0 < \delta < \frac{1}{2}$ and $x_0 \in (\delta, 1-\delta)$, the torus coherent state $\Psi_{(x_0,p_0),\sigma,\mathbb{T}^2}$ is well-approximated by the $\mathbb{R}^2$-coherent state $\Psi_{(x_0,p_0),\sigma}$: For $(\sigma D) \geq 1$ and $j = 0, \ldots, D-1$,

$$\sqrt{D}\langle j|\Psi_{F_0,\sigma,\mathbb{T}^2}\rangle = \Psi_{F_0,\sigma}\left(\frac{j}{D}\right) + \mathcal{O}((\sigma D)^{1/4} e^{-\pi\sigma D\delta^2}), \tag{2.29}$$

with a uniform implied constant in the error term. This is due to the rapid decay of thet $\mathbb{R}^2$-Gaussian states, and is useful so we can apply the Gaussian transformation properties of the $\mathbb{R}^2$-states,

$$\begin{aligned}
\psi_{(x_0,p_0),\sigma}(x+s) &= \psi_{(x_0-s,p_0),\sigma}(x) e^{\pi i D p_0 s} \\
\psi_{(x_0,p_0),\sigma}(rx) &= \psi_{(x_0/r,p_0 r),r^2\sigma}(x)\frac{1}{\sqrt{r}} \\
\psi_{(x_0,p_0),\sigma}(x) &= \psi_{(x_0,p_0+g),\sigma}(x) e^{i\pi D g x_0} e^{-2\pi i D g x}.
\end{aligned}$$

2. The Fourier transform action on $\mathbb{R}^2$-Gaussian states translates to the torus Gaussian states through the DFT matrix,

$$F_D \Psi_{F_0,\sigma,\mathbb{T}^2} = \Psi_{FF_0,1/\sigma,\mathbb{T}^2},$$

where $FF_0 := (p_0, -x_0)$. We will have to show the generalized DFT matrices $F_D^{\alpha,\beta}$ act in a similar enough way in the semiclassical limit. For later use, we will use the following identity to relate $F_{D/A}^{\alpha,\beta}$ to F_D: For $j \in \{0, \ldots, A-1\}$ and $m - jD/A, \xi -$

$\ell D/A \in \{0,\dots,D/A-1\}$,

$$\langle m - jD/A | F_{D/A}^{\alpha,\beta} | \xi - \ell D/A \rangle = \sqrt{A} \langle Am - jD | F_D | \xi \rangle \, e^{-2\pi i \left(\beta \frac{A}{D} m + \alpha \frac{A}{D} \xi - j\beta - \alpha\ell + \alpha\beta \frac{A}{D}\right)}. \tag{2.30}$$

3. If $\Gamma_0, \Gamma_1 \in \mathbb{T}^2$ are close enough, then the coherent states centered at Γ_0 and Γ_1 are close up to an overall phase factor: If $\eta, \varepsilon = o(D^{-1/2})$ and $\sigma > 0$ is fixed, then for $x_0 \in (\delta, 1-\delta)$ with $\delta \gg D^{-1/2}(\log D)^{-1/2}$, there is a phase factor $e^{i\Theta_{D,\eta,\varepsilon,\Gamma_0}}$ so that

$$\left\| \Psi_{(x_0,p_0),\sigma,\mathbb{T}^2} - e^{i\Theta_{D,\eta,\varepsilon,\Gamma_0}} \Psi_{(x_0+\eta,p_0+\varepsilon),\sigma,\mathbb{T}^2} \right\| = o(1), \quad \text{as } D \to \infty. \tag{2.31}$$

   One can check this by estimating the euclidean norm directly, by going to the $\mathbb{R}^2$ Gaussian states and performing estimates depending on the index's distance from Dx_0. The requirements on η, ε are intuitive, as the state $\Psi_{\Gamma_0,\sigma,\mathbb{T}^2}$ is a Gaussian state with standard deviation of order $D^{-1/2}$ in position or momentum space, and so a state centered at $\Gamma_0 + o(D^{-1/2})$ eventually overlaps strongly with one at Γ_0. The requirement on δ is for convenience so we can interchange the torus states with the $\mathbb{R}^2$ Gaussian states according to (2.29).

   This property is needed to handle the varying phases α_j, β_j in the DFT matrices; it is not required for the Balazs–Voros quantization with no phase factors.

We consider $\Gamma_0 = (x_0, p_0)$ away from the discontinuities of the classical A-baker map; specifically for any $0 < \gamma < \frac{1}{2}$ and $0 < \delta < \frac{1}{2A}$, we consider

$$\mathscr{G}_{A,\delta,\gamma} = \left\{ (x_0,p_0) : \left| x_0 - \frac{k}{A} \right| > \delta \ \ \forall k = 0,\dots,A, \text{ and } p_0 \in (\gamma, 1-\gamma) \right\}.$$

This partitions $[0,1]^2$ into A disjoint rectangles, $I_\ell \times \Gamma := \{x_0 \in (\frac{\ell}{A} + \delta, \frac{\ell+1}{A} - \delta)\} \times \{p_0 \in$

$(\gamma, 1-\gamma)\}$ for $\ell = 0, \ldots, A-1$. For each rectangle $I_\ell \times \Gamma$, we consider a coherent state centered at some $F_0 \in I_\ell \times \Gamma$, and compute its evolution under $\tilde{B}_A^{(\Pi)}$.

Suppose $F_0 \in I_\ell \times \Gamma$, and let $j = \Pi(\ell)$. Since the coherent state $\Psi_{F_0,\sigma,\mathbb{T}^2}$ is localized at F_0, it is small for coordinates away from I_ℓ, in particular, using (2.29), then

$$\langle \xi | \Psi_{F_0,\sigma,\mathbb{T}^2} \rangle = \frac{1}{\sqrt{D}} \mathscr{O}((\sigma D)^{1/4} e^{-\pi\sigma D\delta^2})), \quad \xi \notin \left[\ell\frac{D}{A}, (\ell+1)\frac{D}{A} - 1 \right], \tag{2.32}$$

since $|\frac{\xi}{D} - x_0| \geq \delta$. Thus the main contributions in $\tilde{B}^{(\Pi)}_{A,\mathrm{mix}} |\Psi_{F_0,\sigma,\mathbb{T}^2}\rangle$ will come from the ℓth-block $\omega_\ell F^{\alpha_\ell,\beta_\ell}_{D/A}$ in $\tilde{B}^{(\Pi)}_{A,\mathrm{mix}}$, since this block acts on the large elements of $|\Psi_{F_0,\sigma,\mathbb{T}^2}\rangle$ which correspond to the indices $\xi \in [\ell\frac{D}{A}, (\ell+1)\frac{D}{A} - 1]$. This block has been permuted to the jth row block, and so we start with computing $\langle m | \tilde{B}^{(\Pi)}_{A,\mathrm{mix}} | \Psi_{F_0,\sigma,\mathbb{T}^2} \rangle$ for $m \in [j\frac{D}{A}, (j+1)\frac{D}{A} - 1]$. We are not concerned with phase factors that depend on j, ℓ, α_ℓ, β_ℓ, D, A, or F_0 since these just become an overall phase factor, so we will accumulate them in a phase factor $e^{i\phi_{\Pi,F_0}}$ which may change from line to line. We will have to keep track of phase factors depending on m. Using (2.30), (2.32), and Gaussian transformation properties, we compute,

$$\begin{aligned}
\langle m | \tilde{B}^{(\Pi)}_{A,\mathrm{mix}} | \Psi_{F_0,\sigma,\mathbb{T}^2} \rangle &= \omega_j \sum_{\xi=\ell\frac{D}{A}}^{(\ell+1)\frac{D}{A}-1} \langle m - jD/A | F^{\alpha_\ell,\beta_\ell}_{D/A} | \xi - \ell D/A \rangle \langle \xi | \Psi_{F_0,\sigma,\mathbb{T}^2} \rangle \\
&= e^{i\phi_{\Pi,F_0}} e^{-2\pi i \beta_\ell \frac{A}{D} m} \sqrt{A} \sum_{\xi=0}^{D-1} \langle Am - jD | F_D | \xi \rangle e^{-2\pi i \alpha_\ell \xi \frac{A}{D}} \langle \xi | \Psi_{F_0,\sigma,\mathbb{T}^2} \rangle + \mathscr{O}(\sqrt{A}(\sigma D)^{1/4} e \\
&= e^{i\phi_{\Pi,F_0}} e^{-2\pi i \beta_\ell \frac{A}{D} m} \sqrt{A} \langle Am - jD | \Psi_{F(x_0, p_0 - \alpha_\ell A/D), 1/\sigma, \mathbb{T}^2} \rangle + \mathscr{O}(\sqrt{A}(\sigma D)^{1/4} e^{-\pi D\sigma\delta^2}),
\end{aligned} \tag{2.33}$$

where in the second line, we used (2.32) to freely (at the cost of the error term $\mathscr{O}((\sigma D)^{1/4} e^{-\pi D\sigma\delta^2})$) add in the terms involving $\langle \xi | \Psi_{F_0,\sigma,\mathbb{T}^2} \rangle$ for $\xi \notin [\frac{\ell D}{A}, \frac{(\ell+1)D}{A} - 1]$, and in the third line we used $e^{-2\pi i \alpha_\ell \xi \frac{A}{D}} \langle \xi | \Psi_{F_0,\sigma,\mathbb{T}^2} \rangle = e^{-i\pi\alpha_\ell A x_0} \langle \xi | \Psi_{(x_0, p_0 - \alpha_\ell A/D),\sigma,\mathbb{T}^2} \rangle + \frac{1}{\sqrt{D}} \mathscr{O}((\sigma D)^{1/4} e^{-\pi\sigma D\delta^2})$ as well as the DFT action on the torus states.

By Gaussian state transformation properties, for $F = (x_1, p_1)$,

$$\sqrt{A}\Psi_{FF,1/\sigma}(Ax - j) = \Psi_{((p_1+j)/A,-(Ax_1-\ell),A^2/\sigma}(x)e^{i\pi D\ell(p_1+j)/A}e^{-\pi iDjx_1}e^{-2\pi iD\ell x}.$$

Then taking $x = m/D$ and D large enough so $\gamma - A/D \geq \gamma/2$ (so that $p_0 - \alpha_\ell A/D \in (\gamma/2, 1 - \gamma/2)$ and $\frac{p_0+j}{A} - \frac{\alpha_\ell}{D} \in (\frac{\gamma}{2A}, 1 - \frac{\gamma}{2A})$), then

$$\sqrt{A}\langle Am - jD|\Psi_{F(x_0,p_0-\alpha_\ell A/D),1/\sigma,\mathbb{T}^2}\rangle = \langle m|\Psi_{(\frac{p_0+j}{A}-\frac{\alpha_\ell}{D},-(Ax_0-\ell)),A^2/\sigma,\mathbb{T}^2}\rangle e^{i\phi_{\Pi,F}0} + \mathscr{O}(\sigma^{-1/4}e^{-\pi D\gamma^2/(4\sigma)}).$$

Using this in (2.33) and taking into account the phase factor $e^{-2\pi i\frac{\beta_\ell A}{D}m}$, we obtain, for $m \in [j\frac{D}{A}, (j+1)\frac{D}{A} - 1]$,

$$\langle m|\tilde{B}^{(\Pi)}_{A,\mathrm{mix}}|\Psi_{F_0,\sigma,\mathbb{T}^2}\rangle = e^{i\phi_{\Pi,F}0}\langle m|\Psi_{(\frac{p_0+j}{A}-\frac{\alpha_\ell}{D},-(Ax_0-\ell)-\frac{\beta_\ell A}{D}),A^2/\sigma,\mathbb{T}^2}\rangle + \mathscr{O}(\max(\sigma,1/\sigma)^{1/4}D^{1/2}e^{-\pi D\theta}), \tag{2.34}$$

where $\theta := \max(\sigma\delta^2, \gamma^2/(4\sigma))$.

The same estimate holds for $m \notin [j\frac{D}{A}, (j+1)\frac{D}{A} - 1]$, essentially because everything on the right side of (2.34) is just $\mathscr{O}(\max(\sigma,1/\sigma)^{1/4}D^{1/2}e^{-\pi D\theta})$ as $|\frac{m}{D} - \frac{p_0+j}{A}| \geq \gamma/A$, and also so is the equivalent of the first line of (2.33) by (2.32). Then adding a factor $\sqrt{D}$ to go to the euclidean norm, we obtain,

$$\|\tilde{B}^{(\Pi)}_{A,\mathrm{mix}}\Psi_{(x_0,p_0),\sigma,\mathbb{T}^2} - e^{i\phi_{\Pi,F}0}\Psi_{(\frac{p_0+j}{A}-\frac{\alpha_\ell}{D},-(Ax_0-\ell)-\frac{\beta_\ell A}{D}),A^2/\sigma,\mathbb{T}^2}\| = \mathscr{O}(\max(\sigma,1/\sigma)^{1/4}De^{-\pi D\theta}).$$

Since the inverse DFT matrix F_D^{-1} is unitary, then also

$$\|\tilde{B}^{(\Pi)}_{A}\Psi_{(x_0,p_0),\sigma,\mathbb{T}^2} - e^{i\phi_{\Pi,F}0}\Psi_{(Ax_0-\ell+\frac{\beta_\ell A}{D},\frac{p_0+j}{A}-\frac{\alpha_\ell}{D}),\sigma/A^2,\mathbb{T}^2}\| = \mathscr{O}(\max(\sigma,1/\sigma)^{1/4}De^{-\pi D\theta}), \tag{2.35}$$

for $\theta = \max(\sigma\delta^2, \gamma^2/(4\sigma))$. The above bound is $o(1)$ if for example, $\sigma \sim c$, $\gamma \sim c$, $\delta \sim \frac{c}{A}$, and $A = o(D^{1/2}(\log D)^{-1/2})$. Finally, using (2.31) with $\eta = \frac{\beta_\ell A}{D}$ and $\varepsilon = -\frac{\alpha_\ell}{D}$, yields,

$$\|\tilde{B}_A^{(\Pi)}\Psi_{(x_0,p_0),\sigma,\mathbb{T}^2} - e^{i\tilde{\phi}_{\Pi,f}}{}_0\Psi_{(Ax_0-\ell,\frac{p_0+j}{A}),\sigma/A^2,\mathbb{T}^2}\| = o(1), \quad \text{as } D \to \infty. \tag{2.36}$$

2.5 Discussion

We have illustrated a specific "embedding" of quantum chaotic behavior in the periodic orbits of a classically ergodic, chaotic map via quantum superposition, by deriving an exact correspondence between the periodic modular-multiplication-by-A maps and "chaotic" A-baker's maps, for N such that either of $N \pm 1$ is a multiple of A. As will be shown in the next section, this result generalizes to other values of N albeit via a more complicated construction with two important implications.

Firstly, in any practical implementation of Shor's algorithm, it is N that is given while A is chosen as per convenience, in contrast to the dynamical systems approach, in which a fixed A specifies the modular multiplication map while $N \to \infty$ through any subsequence of $\mathbb{N}$ gives the classical limit. This means that a general result for N would be crucial if one is to understand the implications of this "embedding of quantum chaos" for Shor's algorithm (otherwise, choosing an A that is a factor of either of $N \pm 1$ would require the output of Shor's algorithm as applied to $N \pm 1$, introducing a circular element). Conversely, achieving such a generalization may provide a fuller picture of how certain perturbations affect the dynamics of Shor's algorithm, along the lines of the analysis in Ref. [38].

Secondly, from a fundamental quantum dynamical systems viewpoint, the study of quantized A-baker's maps has generally been restricted to Hilbert space dimensions that are multiples of A, due to a need to consider A copies of discrete Fourier transforms in, e.g., the Balazs–Voros quantization [34]. Approaching the quantization of such maps through

the above connection to Shor's algorithm, on the other hand, provides a promising avenue to generalize A-baker's maps to a wider set of Hilbert space dimensions (or chocies of N) with the use of *generalizations* of Fourier transforms, in particular for any coprime pair of (A,N). This also opens avenues for studying the semiclassical behavior of such generalized quantum A-baker's maps to explore atypicalities and any N-dependence in their "quantum chaos" signatures, noting that such atypicalities were observed for N a multiple of A in the Balazs-Voros quantization [34]. Further, A-baker's maps can be directly realized in quantum simulators using quantum Fourier transforms [51, 52], which may allow the experimental detection of such atypical spectral signatures using recently developed measurement protocols for signatures of "quantum chaos" [53, 54].

Finally, classical results in ergodic theory indicate that the above results relating different quantizations of the modular multiplication map $f_A(x)$ may generalize in some form to *arbitrary* sufficiently chaotic systems. This is due to Sinai's factor theorem [55, 56], which implies that any ergodic and chaotic system, whose Kolmogorov-Sinai entropy [57] (sum of positive Lyapunov exponents) is at least $\ln A$, contains $f_A(x)$ as a factor (i.e. can be coarse grained to yield a system equivalent to $f_A(x)$); a direct illustration is provided by the x-coordinate action of the A-baker's map (coarse-graining over p) being $f_A(x)$. Successfully implementing such a generalization in practice would depend on identifying suitable quantizations of a given chaotic system that capture the appropriate properties of its modular multiplication factor(s), and may provide further avenues for future work.

2.6 Generalization to arbitrary N

We have shown that when $N \pmod A = \pm 1$ then U_A can be expressed as a superposition of chaotic and ergodic quantum A-baker's maps. As promised in the discussion, now

we extend the result to arbitrary values of N and A. One can always write N as

$$N = Aq + b \tag{2.37}$$

where $q = Quotient[N,A]$ and $b = Mod[N,A]$. We know that U_A is defined on an N dimensional Hilbert space as

$$U_A |m\rangle = |mA \pmod N\rangle \quad \text{for} \quad m \in \{0,1,\ldots,N-1\}. \tag{2.38}$$

The value of $mA \pmod N$ depends on the value of m. We find that

$$\begin{aligned} mA \pmod N &= mA \quad \text{for} \quad 0 \le m < q_1 \\ &= mA - N \quad \text{for} \quad q_1 \le m < q_2 \\ &\vdots \\ &= mA - kN \quad \text{for} \quad q_k \le m < q_{k+1} \\ &\vdots \\ &= mA - (A-1)N \quad \text{for} \quad q_{A-1} \le m < q_A. \end{aligned} \tag{2.39}$$

We note that $q_1 = q+1$ and $q_A = N$. Even though the exact values of all other q_is depend on A and b we always have $q_{i+1} - q_i = q$ or $q+1$. Furthermore $q_{i+1} - q_i = q+1$ for b values of q_i. We define an interval I_l and a conditional function $\bar{\Theta}(x)$ as followed

$$I_l = [q_l, q_{l+1}) \tag{2.40}$$

$$\bar{\Theta}(x) = \begin{cases} 1, \text{if } x \text{ is } true \\ 0, \text{if } x \text{ is } false \end{cases}. \tag{2.41}$$

Furthermore $|I_l|$ denotes the number of integer elements in the interval I_l. Now we can write the matrix elements of U_A as

$$\langle n|\, U_A\, |m\rangle = \delta_{n,Am-lN}\bar{\Theta}(m \in I_l). \tag{2.42}$$

Here $\delta_{a,b}$ denotes the Kronecker delta function and $l \in \{0,1,\ldots A-1\}$. One can write Kronecker delta as

$$\begin{aligned}
\delta_{n,Am-lN} &= \frac{1}{N}\sum_{k=0}^{N-1} e^{\frac{2\pi ik(n-Am)}{N}} \\
&= \frac{1}{N}\sum_{k=0}^{N-1} e^{\frac{2\pi ink}{N}} e^{-2\pi ik\frac{m}{N/A}} \\
&= \frac{1}{N}\sum_{k=0}^{N-1}\sum_{j=0}^{A-1} e^{\frac{2\pi ink}{N}} e^{-2\pi ik\frac{m}{N/A}} \bar{\Theta}(k \in I_j).
\end{aligned} \tag{2.43}$$

We substitute Eq.(2.43) into Eq. (2.42) to get

$$\begin{aligned}
\langle n|\, U_A\, |m\rangle &= \frac{1}{N}\sum_{k=0}^{N-1}\sum_{j=0}^{A-1} e^{\frac{2\pi ink}{N}} e^{-2\pi ik\frac{m}{N/A}} \bar{\Theta}(k \in I_j)\bar{\Theta}(m \in I_l) \\
&= \frac{1}{\sqrt{A}}\sum_{k=0}^{N-1}\sum_{j=0}^{A-1} [F_N^{-1}]_{nk}[\tilde{F}_{jl}]_{km}
\end{aligned} \tag{2.44}$$

where F_N^{-1} is the inverse DFT and $[\tilde{F}_{jl}]$ is a modified DFT of dimension $|I_j|\times|I_l|$ whose elements are

$$[\tilde{F}_{jl}]_{nm} = \frac{1}{\sqrt{N/A}} e^{-2\pi in\frac{m}{N/A}} \bar{\Theta}(n \in I_j)\bar{\Theta}(m \in I_l). \tag{2.45}$$

We can write Eq. (2.44) in the following matrix form:

$$U_A = \frac{1}{\sqrt{A}} F_N^{-1} \begin{bmatrix} \tilde{F}_{00} & \tilde{F}_{01} & \cdots & \tilde{F}_{0(A-1)} \\ \tilde{F}_{10} & \tilde{F}_{11} & \cdots & \tilde{F}_{1(A-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{F}_{(A-1)0} & \tilde{F}_{(A-1)1} & \cdots & \tilde{F}_{(A-1)(A-1)} \end{bmatrix} \tag{2.46}$$

Now we can decompose U_A into a superposition of quantum A-baker maps. We define N dimensional A-baker map $B_A^{(k)}$ as

$$B_A^{(k)} = F_N^{-1} \begin{bmatrix} 0 & \cdots & \tilde{F}_{0k} & 0 & \cdots \\ 0 & \cdots & 0 & \tilde{F}_{1(k+1)} & \cdots \\ \vdots & \ddots & \vdots & \vdots & \ddots \\ \tilde{F}_{(A-k)0} & \cdots & 0 & 0 & \cdots \\ \vdots & \ddots & \vdots & \vdots & \ddots \end{bmatrix}. \tag{2.47}$$

We can write Eq. (2.46) using the A-baker maps as

$$U_A = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} B_A^{(k)}. \tag{2.48}$$

The standard definitions of quantum A-baker maps are valid only for dimension N which is a multiple of A. We provide a definition for an arbitrary dimension N. One interesting consequence of that is now the map is non-unitary for a finite N. However unitarity emerges in the classical limit of $N \to \infty$. That means the corresponding classical dynamics is symplectic as it should be. Now we will focus on the non-unitarity of $B_A^{(k)}$s in Eq. (2.47).

Let's first look at the case of $B_A^{(0)}$. We find that

$$B_A^{(0)\dagger} B_A^{(0)} = \begin{bmatrix} \tilde{F}_{00}^\dagger \tilde{F}_{00} & 0 & \dots & 0 \\ 0 & \tilde{F}_{11}^\dagger \tilde{F}_{11} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \tilde{F}_{(A-1)(A-1)}^\dagger \tilde{F}_{(A-1)(A-1)} \end{bmatrix}. \tag{2.49}$$

One can calculate all these block matrices using Eq. (2.45). We get that

$$[\tilde{F}_{xx}^\dagger \tilde{F}_{xx}]_{nm} = e^{2\pi i \frac{q_x(n-m)}{N/A}} \frac{1 - e^{2\pi i \frac{|I_x|(n-m)}{N/A}}}{1 - e^{2\pi i \frac{(n-m)}{N/A}}}. \tag{2.50}$$

Since $A|I_x|/N$ is, in general, not an integer, Eq. (2.50) implies that $B_A^{(0)}$ is not unitary. Comparing the absolute values of Eq. (2.50) we get

$$|[\tilde{F}_{xx}^\dagger \tilde{F}_{xx}]_{nm}| = \frac{\sin\left[\pi \frac{|I_x|(n-m)}{N/A}\right]}{\sin\left[\pi \frac{(n-m)}{N/A}\right]}. \tag{2.51}$$

2.7 Quantum circuit of non-unitary A-baker's map

Although the generalized A-baker's map defined in Eq. (2.47) is non-unitary, one can design a quantum circuit to implement it. We factorize the map using the singular value decomposition (SVD) to write

$$B_A^{(k)} = V_A^{(k)} D_A^{(k)}(d_1, d_2, \dots, d_N) S_A^{(k)}, \tag{2.52}$$

where $V_A^{(k)}$ and $S_A^{(k)}$ are unitary matrices and $D_A^{(k)}(d_1, d_2, \dots, d_N)$ is a diagonal matrix with non-negative diagonal elements d_is. One can design circuits for $V_A^{(k)}$ and $S_A^{(k)}$ using a uni-

versal quantum gate set. It is more complicated to realize the diagonal matrix. We will first discuss it for $N = 4$ and then generalize it for $N = 2^n$. In the context of factorization, N is not a power of 2. However one can increase the dimension of $B_A^{(k)}$ to the nearest power of 2 by direct summing it with identity matrix. When $N = 4$ the diagonal matrix is (we have removed the subscript and superscript for brevity)

$$D = \begin{bmatrix} d_1 & 0 & 0 & 0 \\ 0 & d_2 & 0 & 0 \\ 0 & 0 & d_3 & 0 \\ 0 & 0 & 0 & d_4 \end{bmatrix}. \tag{2.53}$$

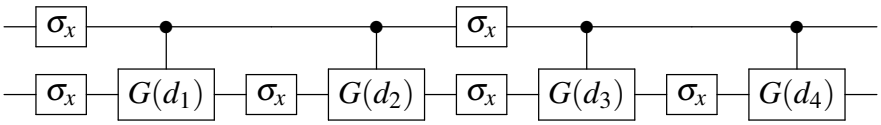
We note that it can alternately be written as

$$D = \begin{bmatrix} \sigma_x G(d_1)\sigma_x G(d_2) & 0 \\ 0 & \mathbb{1} \end{bmatrix} \begin{bmatrix} \mathbb{1} & 0 \\ 0 & \sigma_x G(d_3)\sigma_x G(d_4) \end{bmatrix}, \tag{2.54}$$

where $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the Pauli-X gate and $G(d_i) = \begin{pmatrix} 1 & 0 \\ 0 & d_i \end{pmatrix}$ is a non-unitary 2×2 matrix. We can further simplify Eq. (2.54) into

$$D = \sigma_x \otimes \sigma_x \begin{bmatrix} \mathbb{1} & 0 \\ 0 & G(d_1) \end{bmatrix} \mathbb{1} \otimes \sigma_x \begin{bmatrix} \mathbb{1} & 0 \\ 0 & G(d_2) \end{bmatrix} \sigma_x \otimes \sigma_x \begin{bmatrix} \mathbb{1} & 0 \\ 0 & G(d_3) \end{bmatrix} \mathbb{1} \otimes \sigma_x \begin{bmatrix} \mathbb{1} & 0 \\ 0 & G(d_4) \end{bmatrix}. \tag{2.55}$$

We recognize that $\begin{bmatrix} \mathbb{1} & 0 \\ 0 & G(d_i) \end{bmatrix}$ is the controlled-$G(d_i)$ gate. Now we can design the following circuit to implement D:



(2.56)

The size of this circuit is at least the number of singular values which is exponential in the number of qubits. So this circuit doesn't seem to be efficient unless a significant fraction of the singular values are 1. In Fig. 2.4 we plot the fraction of unitary singular values versus N. From the plot, one can see that, numerically, the fraction approaches unity with increasing N.

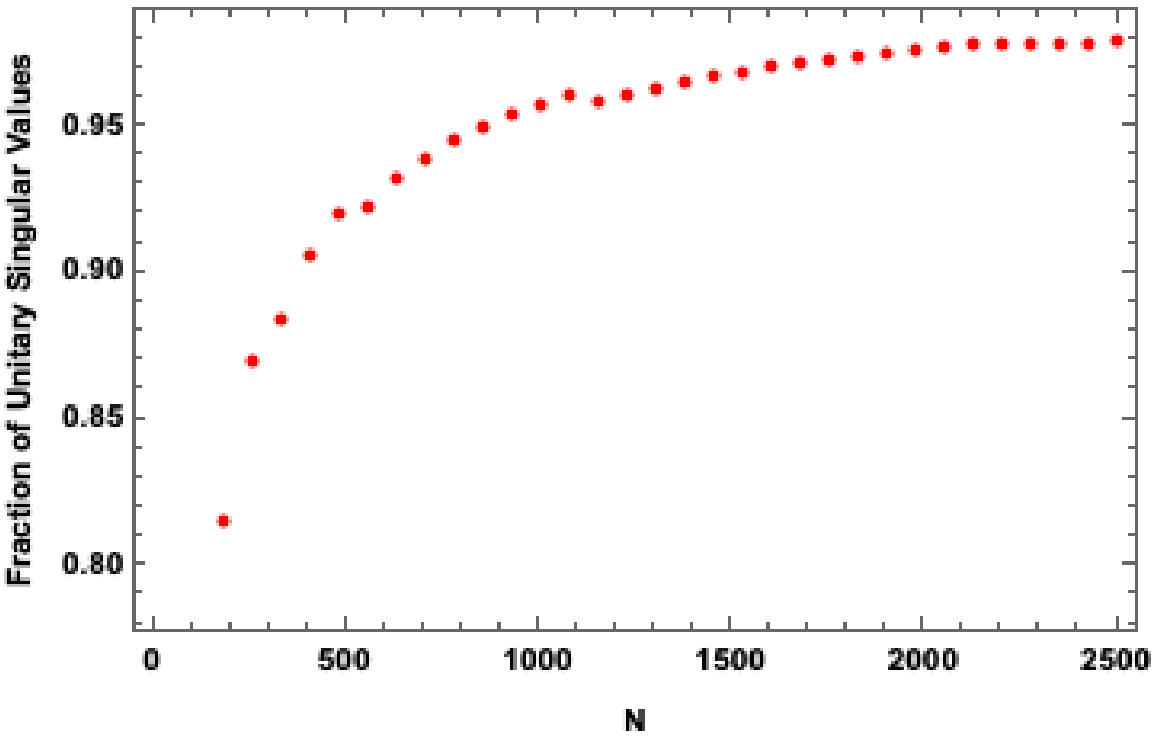


Figure 2.4: Plot of the fraction of singular values vs N. The fraction approaches 1 as $N \to \infty$

Chapter 3: A discrete Fourier transform based quantum circuit for modular multiplication in Shor's algorithm

3.1 Overview

Shor's algorithm [15] for the prime factorization of numbers provides an exponential speedup over the best known classical algorithm, the general number field sieve [58]. For a number with L bits, the complexity of Shor's algorithm is polynomial in L whereas the complexity of the general number field sieve is $O(e^{L^{1/3}(\log L)^{2/3}})$ [59]. As one of the few algorithms believed to show quantum advantage, Shor's algorithm has particularly received attention for its potential to break RSA encryption, which relies on the perceived difficulty of factorization [6]. However, nontrivial practical applications have remained out of reach due to experimental limitations: for example, the largest number successfully factorized in an experimental implementation of Shor's algorithm is 21 [60], which can be stored in 5 qubits, whereas the representation of numbers used in RSA typically require around $2048-4096$ classical bits [61] (and therefore, qubits).

To eventually achieve a practical advantage of Shor's algorithm, one would require: i) the successful processing of more qubits than currently available, ii) better error correcting codes, and iii) improved efficiency in all the modules of the algorithm. The primary bottleneck for the latter is the modular exponentiation component of the algorithm, for which the most straightforward implementations require $O(L^3 \log L)$ number of elementary gates for L qubits [62, 63]. While multiplication algorithms with better complexity exist [64], it

is not clear how they may be efficiently implemented in practice. When it comes to such implementations, the circuits used in experiments conducted so far [60, 65–68] are not generic, as the experimental implementation of modular multiplication is often simplified based on a classical foreknowledge of the factors the algorithm is meant to compute.

The challenging nature of experimental implementations has led to some alternative proposals for factorization that aim to be easier to implement for present-day demonstrations [69–72], though these are often specialized and not expected to be an improvement over Shor's algorithm for large L. In contrast, a recent proposal by Regev [73] (and relevant extensions [74]) is in fact superior to Shor's algorithm for asymptotically large L, though its practical advantage for classically relevant values of L (such as 2048) remains unclear. Further, Kahanamoku-Meyer and Yao have proposed an algorithm for modular multiplication itself which, asymptotically, requires $O(L^{2+\varepsilon})$ gates [75].

In this paper, we propose a quantum circuit with $O(L^3)$ elementary gates for the modular exponentiation operation. Though less efficient than the one proposed in [75], an interesting feature of our circuit is that it is composed only of Discrete Fourier Transforms (DFTs) and their closely related variants. It is also logarithmically more efficient than the "straightforward" circuits for modular multiplication based on the standard multiplication algorithm [7]. We note that the DFT operator is already an essential component of the *phase estimation* protocol in Shor's algorithm [7]. Our circuit therefore provides an implementation of Shor's algorithm entirely in terms of DFTs (specifically, the Quantum Fourier Transform (QFT) circuit [76]) and their variants, without requiring additional specialized implementations of modular exponentiation. Moreover, our circuit is generic because it doesn't require any specialization depending on the number to be factorized. Given that the experimental implementation of the algorithms discussed above is not clear-cut, a circuit such as ours may provide a more feasible route towards short term *generic* implementations of Shor's algorithm depending on the platform of choice.

The quantum part of Shor's algorithm is about finding the multiplicative order r of a number A which is co-prime to N, the number being factorized. The multiplicative order r is the smallest positive natural number which satisfies

$$A^r \pmod{N} = 1. \tag{3.1}$$

If r is even then the prime factors of N are $\gcd(A^{r/2} \pm 1, N)$ where gcd denotes the 'greatest common divisor' of two integers. Alternatively, one can consider the Bernoulli map $f(x) = Ax \pmod{N}$. Then the period of the orbit starting at $x = 1$ is equal to the multiplicative order r. In Shor's algorithm a unitary quantization of this Bernoulli map, namely the quantum modular multiplication operator U_A, is utilized. The action of this operator U_A on the computational basis states is given by

$$U_A |m\rangle = |mA \pmod{N}\rangle, \tag{3.2}$$

where $|m \in \{0, 1 \ldots N-1\}\rangle$ are computational basis states. Eq. (3.1) implies that $U_A^r = \mathbb{1}$. Since r can be as large as $N-1$, it is not efficient to find r by repeated multiplication of A or U_A. However the eigenvalues of U_A are of the form $e^{2\pi i s/r}$ where s is an integer. Consequently, a quantum phase estimation (QPE) algorithm [7] can be used to extract the value of the multiplicative order r. Shor's algorithm is an application of QPE where instead of repeatedly multiplying U_A, one uses modular exponentiation, which is the successive application of the gates $U_A^{2^k}$ controlled by auxiliary qubits, where $k \in \{0, 1, \ldots, k_{\max}\}$. It is notable that modular multiplication satisfies $U_A^{2^k} = U_{A^{2^k}}$. Consequently, an efficient strategy is to apply $k_{\max}$ different modular emultiplication operators with different values of A — which is particularly suitable for our circuit proposed below. Since $k_{\max}$, the maximum value of k, is typically of the order of L where L is the number of bits in which N is stored,

in this method one needs $O(L)$ controlled unitary modules. Each unitary module has the gate complexity $O(M(L))$ where $M(L)$ is the number of gates required to apply modular multiplication. Apart from modular exponentiation, Shor's algorithm also needs to apply the quantum Fourier transform (QFT) for completing the phase estimation step. However, for currently known implementations, the cost of modular exponentiation is far greater than the $O(L^2)$ cost of the standard QFT circuit [7, 77], making the overall gate complexity of Shor's algorithm $O(LM(L))$.

It is worth comparing our circuit to the existing literature. There are many works on the construction of a quantum circuit for modular multiplication [62, 75, 78–81]. All of these circuits, except the one in [75], use the quantum adder circuit by Draper [82] and an approximate QFT [83] to implement modular multiplication. These circuits require $O(M(L)) = O(L^2 \log L)$ gates. However, Ref. [75] utilizes the Toom-Cook algorithm [84] for fast multiplication to reduce the gate complexity of the circuit. In this approach, modular multiplication can be performed with $O(L^{1+\varepsilon})$ gates in the asymptotic limit for arbitrarily small ε (and a comparable simplification is possible for the QFT component), which leads to the overall $O(L^{2+\varepsilon})$ complexity mentioned above, for successive applications of modular multiplication. While our proposal for modular multiplication is $O(L^2)$, the fact that it can be be implemented in a similar way to the standard QFT circuit may simplify the real-world aspects of experimental implementation.

The core intuition behind our circuit is that the operator U_A generates a permutation of the computational basis states. We know that the discrete Fourier transform (DFT) matrix consists of the orthonormal states obtained by applying DFT to the computational basis states. We further observe that rows or columns of the DFT matrix, $[F_N]_{nm} \propto e^{-2\pi inm/N}$, can be permuted by rescaling the phases by an integer. Consequently, it is possible to write the modular multiplication operator U_A as the product of DFT matrix and a modified DFT matrix with rescaled phases. We will now illustrate these statements quantitatively. From

Eq. (3.2) we find that the elements of U_A in the computational basis are

$$\langle n|\, U_A\, |m\rangle \equiv [U_A]_{nm} = \delta_{n,Am-lN} \tag{3.3}$$

where $\delta_{a,b}$ denotes the Kronecker delta function and $l \in \{0,1\ldots,A-1\}$. We can use an identity of the Kronecker delta function to rewrite Eq. (3.3) as

$$[U_A]_{nm} = \frac{1}{N}\sum_{k=0}^{N-1} e^{\frac{2\pi ik(n-Am)}{N}} \equiv [F_N^{-1}.G_N]_{nm}, \tag{3.4}$$

where F_N and G_N denote two matrices whose elements are

$$[F_N]_{nm} = \frac{1}{\sqrt{N}} e^{\frac{-2\pi inm}{N}}, \tag{3.5}$$

$$[G_N]_{nm} = \frac{1}{\sqrt{N}} e^{\frac{-2\pi iAnm}{N}}. \tag{3.6}$$

Note that F_N is the DFT matrix and G_N is a modified DFT matrix whose phases have been rescaled. In our context, this expression was motivated by generalizing certain relations between modular multiplication and quantum maps involving DFTs [38, 85][1].

We will implement U_A by designing a circuit for these two matrices. If N is a power of 2, then the circuit for the DFT requires only the Hadamard and the phase gates [7]. However, in general we can not use that circuit here because N, the number to be factorized, is typically not a power of 2. Instead one can use Kitaev's algorithm for applying the DFT operator over an arbitrary Abelian group [76]. For our application, the Abelian group is the cyclic group of integers $\mathbb{Z}_N \in \{0,1\ldots,N-1\}$ together with the operation of addition modulo N. One restriction in our circuit is that it requires the coprime A to be an odd

[1] Specifically, given the setup of [38, 85], the generalization is from N being related to multiples of A to arbitrary N, and proceeds from Eq. (3.4) by splitting G_N into different terms, each with a block structure resembling the permuted A-baker's quantum maps, which are thereby also generalized to arbitrary N. between modular multiplication and quantum maps involving DFTs [38, 85]

number. The reason behind this will be clear when we describe the circuit in detail. One should be able to incorporate even coprimes with some modifications, but we do not discuss such modifications here. In section 3.2, we will provide a general structure of our circuit, and in section 3.3, we break down the circuit into elementary gates.

3.2 Outline of the circuit

In quantum computation, a system of multiple qubits grouped together is called a register [86]. We have two input registers each containing L qubits. Define a unitary V_A which multiplies a state by a phase proportional to A, according to the following equation

$$V_A \left|m\right\rangle_1 \left|n\right\rangle_2 = \left|m\right\rangle_1 e^{\frac{2\pi i A m n}{N}} \left|n\right\rangle_2 . \tag{3.7}$$

Here $m,n \in \{0,1 \ldots N-1\}$ are computational basis states and the subscripts denote their register index. This is the order of registers we will stick to even if we do not explicitly mention the register number for brevity. From Eq. (3.7), we can evaluate the action of V_A on an arbitrary state. Let us calculate the output of V_A when the state $\left|n\right\rangle_2$ in Eq. (3.7) is an equal superposition of all the basis states. We denote the equal superposition state as $\left|\Psi_N\right\rangle$ i.e.

$$\left|\Psi_N\right\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \left|l\right\rangle . \tag{3.8}$$

We replace the state $\left|n\right\rangle$ in Eq. (3.7) with the state $\left|\Psi_N\right\rangle$ to get

$$V_A \left|m\right\rangle \left|\Psi_N\right\rangle = \left|m\right\rangle \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} e^{\frac{2\pi i A m l}{N}} \left|l\right\rangle = \left|m\right\rangle G_N^{-1} \left|m\right\rangle . \tag{3.9}$$

We further note that

$$V_1 \left|m\right\rangle \left|\Psi_N\right\rangle = \left|m\right\rangle F_N^{-1} \left|m\right\rangle . \tag{3.10}$$

Now we can use Eq. (3.9) and (3.10) to design the circuit for modular multiplication. The outline is given in Fig. 3.1.

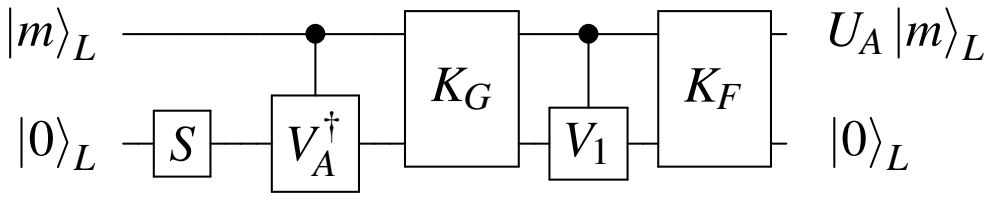


Figure 3.1: The outline of the circuit for modular multiplication. There are two input registers. The first one contains the state one wants to apply modular multiplication on (state $|m\rangle_L$ in the figure) and the second one contains L ancilla qubits at $|0\rangle$. The gate S acts on the second register to create an equal superposition of the basis states. Then we apply two controlled phase gate $V_A^\dagger$ and V_1. After that we apply the operator K which swaps the two registers and reset the second register to $|0\rangle$.

In Fig. 3.1, the gate denoted by S converts the second register at the state $|0\rangle_L$ into the equal superposition state $|\Psi_N\rangle$ i.e.

$$S|0\rangle_L = |\Psi_N\rangle\,. \tag{3.11}$$

After that one applies the operator $V_A^\dagger$ which produces the state $G_N|m\rangle$ in the second register. Then the operator K_G swap the two registers and reset the second register to the state $|0\rangle$. In the next step, one applies the operator S and V_1 to get the state $U_A|m\rangle$. Finally, similar to the previous sequence, one applies the operator K_F to reset the second register to the state $|0\rangle$. This is necessary for further applications of U_A with the same auxiliary register.

3.3 Breaking down the circuit into elementary gates

In this section we will break down the gates in Fig. 3.1 into simpler gates. First we want to perform the operation which transforms the state $|0\rangle_L$ into the equal superposition state $|\Psi_N\rangle_L$. We can create $|\Psi_N\rangle$ using a series of recursive rotations on the state $|0\rangle_L$. Let's say $N_1N_2\ldots N_L$ is the binary representation of the number N. Then the equal superposition

state can be prepared using the following algorithm [76]:

Algorithm for preparing the equal superposition state

The following pseudocode outlines the procedure to create the equal superposition state $|\Psi_N\rangle$:

1: Initialize $\bar{N} \leftarrow N$
2: **for** $i = 1$ to L **do**
3: **if** $N_i = 1$ **then**
4: Rotate qubit i by $\theta_i = \tan^{-1}(\sqrt{\bar{N}/2^{L-i} - 1})$
5: **if** the ith ancilla is in $|0\rangle$ **then**
6: Apply Hadamard gate H on qubits $i+1$ through L
7: **else**
8: **break**
9: **end if**
10: $\bar{N} \leftarrow \bar{N} - 2^{L-i}$
11: **end if**
12: **end for**

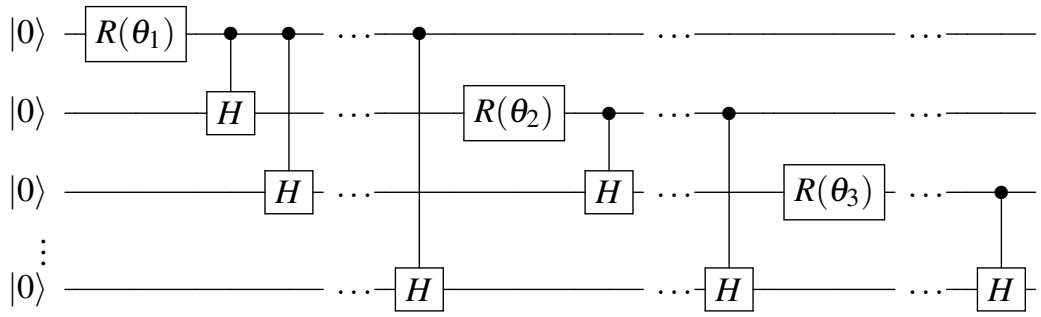


Figure 3.2: The quantum circuit to create the equal superposition state $|\Psi_N\rangle$ following the pseudocode given above. One applies controlled-Hadamard (H) after rotating a qubit by the angle θ_i given in line 4 of the algorithm.

From the pseudocode given above we recognize that the operator S can be implemented using single qubit rotation and the Hadamard gate. The circuit to realize this algorithm is shown in Fig. 3.2. The operators V_1 and $V_A^\dagger$ can be constructed from the phase shift gates $\Lambda(k)$ of the form [76]

$$\Lambda(k) = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i \frac{2^k}{N}} \end{bmatrix}, \tag{3.12}$$

where $k \in \{0, 1, \ldots, L-1\}$. We break down the resetting operators K_G and K_F into elementary gates using the method presented by Kitaev in [76]. The main idea is to apply inverse phase estimation for a cyclic permutation, $W = \sum |m\rangle \langle m+1|$. Since the DFT basis states are the eigenvectors of the cyclic permutation operation, this step resets the state $|m\rangle$ to $|0\rangle$. In the following subsection we elaborate on this method.

3.3.1 Construction of the resetting operator K_G and K_F

In this section we construct the resetting operators K_G and K_F using Kitaev's algorithm in [76]. We will explicitly describe the circuit for K_G only and show that K_F is a special case of K_G. The circuit for applying the operator K_G is drawn in Fig. 3.3. From Fig. 3.1 we see that K_G is applied after applying the controlled phase gate $V_A^\dagger$. As a result, the inputs are the state $|m\rangle$ in the first register and the state $G_N |m\rangle$, denoted as $|\tilde{m}_G\rangle$ for brevity, in the second register. Now, we apply a DFT like operator $F_{2^L}^{A\dagger}$ on the state $|m\rangle = |m_1 m_2 \ldots m_L\rangle$. The action of $F_{2^L}^A$ on the computational basis states is

$$F_{2^L}^A |k\rangle = \frac{1}{\sqrt{2^L}} \sum_{l=0}^{2^L-1} e^{\frac{-2\pi i A k l}{2^L}} |l\rangle . \tag{3.13}$$

We note that $F_{2^L}^A$ is unitary when A is odd. We can realize $F_{2^L}^A$ using the circuit in Fig. 3.4. After applying $F_{2^L}^{A\dagger}$ on the first register we get the the state

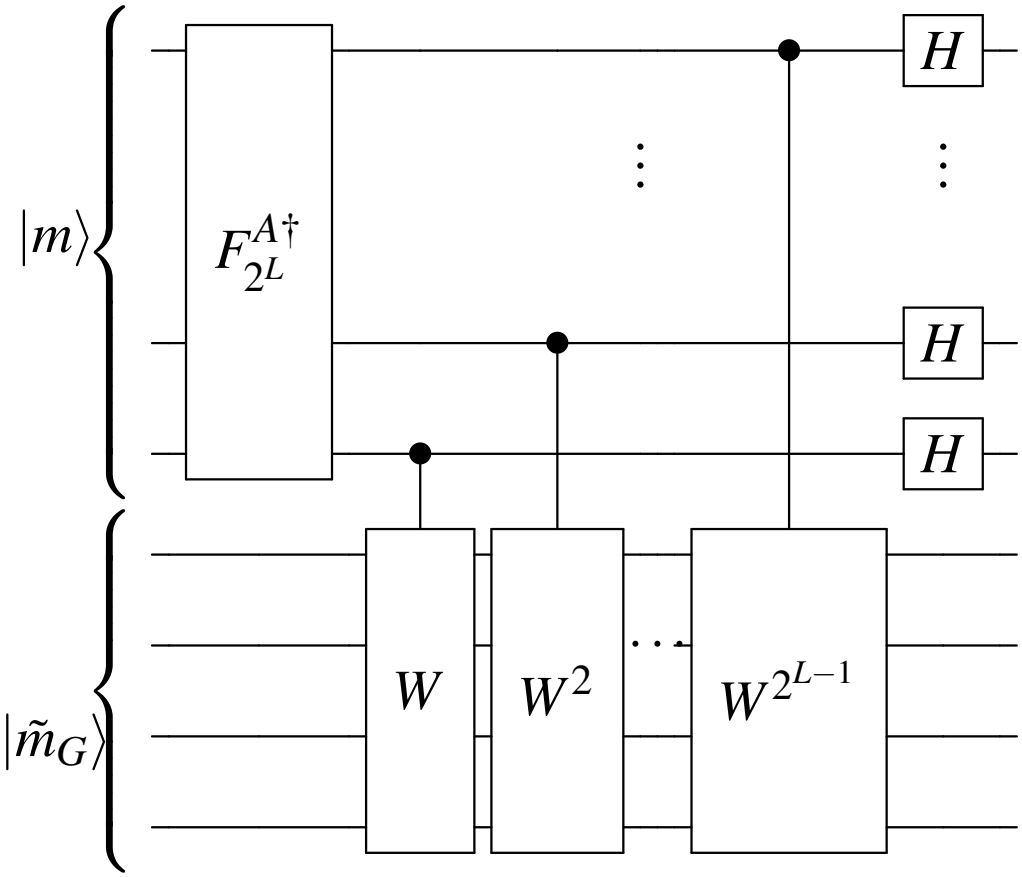


Figure 3.3: Diagram of the quantum circuit for operator K_G. The circuit essentially accomplishes phase estimation in reverse for the cyclic permutation $W = \sum |m\rangle \langle m+1|$. The inputs of the circuit are the state $|m\rangle$ in the first register and the state $G_N|m\rangle$, denoted by $|\tilde{m}_G\rangle$, in the second register The $F_{2^L}^A$ operator in the circuit is a DFT like transformation defined as $F_{2^L}^A|k\rangle = 1/\sqrt{2^L}\sum_{l=0}^{2^L-1} e^{-2\pi iAkl/2^L}|l\rangle$. Note that $F_{2^L}^A$ is unitary as long as A is odd. The H gates in the diagram refers to Hadamard gate.

$$F_{2^L}^{A\dagger}|m_1 m_2 \ldots m_L\rangle = \frac{1}{\sqrt{2^L}}(|0\rangle + e^{2\pi Ai 0.m_L}|1\rangle)(|0\rangle + e^{2\pi Ai 0.m_{L-1}m_L}|1\rangle)\ldots(|0\rangle + e^{2\pi Ai 0.m_1 m_2 \ldots m_L}|1\rangle), \tag{3.14}$$

where $.m_j \ldots m_L = \sum_{k=j}^{L} m_k 2^{j-k-1}$ is the binary representation of fraction. Then we apply a series of $controlled - W$ gates, denoted as cW. For this operation, the control and target qubits are the qubits in the first and second register respectively. After some calculation we

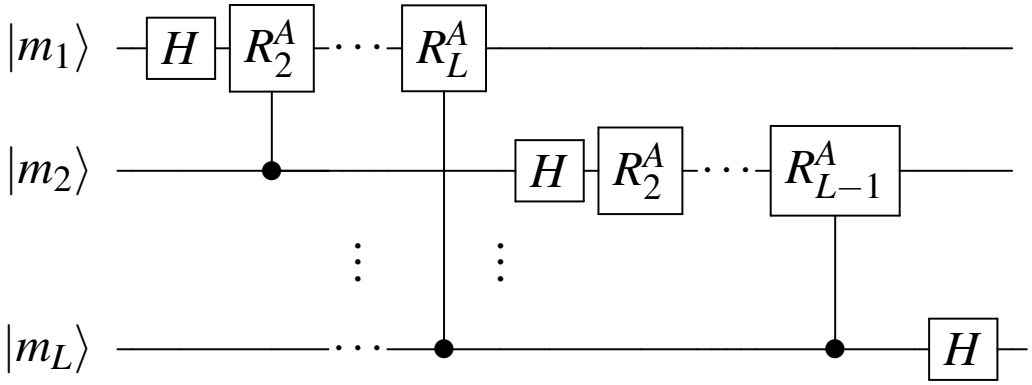


Figure 3.4: Circuit diagram for the operator $F_{2^L}^A$. In the circuit, H denotes the Hadamard gate and $R_k^A = diag(1, e^{-2\pi iA/2^k})$ are phase gates with $k \in \{2,3\ldots L\}$.

find that

$$cW(|0\rangle + e^{2\pi Ai 0.m_1 m_2 \ldots m_L}|1\rangle)|\tilde{m}_G\rangle = (|0\rangle + e^{2\pi Ai(0.m_1 m_2 \ldots m_L - \frac{m}{N})}|1\rangle)|\tilde{m}_G\rangle \tag{3.15}$$

$$cW^2(|0\rangle + e^{2\pi Ai 0.m_2 m_3 \ldots m_L}|1\rangle)|\tilde{m}_G\rangle = (|0\rangle + e^{2\pi Ai(0.m_2 m_3 \ldots m_L - \frac{2m}{N})}|1\rangle)|\tilde{m}_G\rangle \tag{3.16}$$

$$\vdots = \vdots$$

$$cW^{2^{L-1}}(|0\rangle + e^{2\pi Ai 0.m_L}|1\rangle)|\tilde{m}_G\rangle = (|0\rangle + e^{2\pi Ai(0.m_L - \frac{2^{L-1}m}{N})}|1\rangle)|\tilde{m}_G\rangle\,. \tag{3.17}$$

We define the phases θ_k for $k \in \{1,2\ldots,L\}$ as $\theta_k = 0.m_k m_{k+1}\ldots m_L - \frac{2^{k-1}m}{N}$. This allows us to succinctly write Eqn. (3.15) - (3.17) as

$$cW^{2^{k-1}}(|0\rangle + e^{2\pi i 0.m_k m_{k+1}\ldots m_L}|1\rangle)|\tilde{m}_G\rangle = (|0\rangle + e^{2\pi Ai\theta_k}|1\rangle)|\tilde{m}_G\rangle\,. \tag{3.18}$$

It means that now the second register is in the state $|\tilde{m}_G\rangle$ and the first register is in the product state

$$\prod_{k=1}^{L}(|0\rangle + e^{2\pi iA\theta_k}|1\rangle). \tag{3.19}$$

Then we apply Hadamard gate on each of the qubits in the first register. It produces the state

$$\prod_{k=1}^{L}[(1+e^{2\pi Ai\theta_k})\,|0\rangle+(1-e^{2\pi Ai\theta_k})\,|1\rangle]\,|\tilde{m}_G\rangle\,. \tag{3.20}$$

Note that $\theta_k \approx 0$ which means that the two registers are approximately in the state $|0\rangle\,|\tilde{m}_G\rangle$. Finally we swap the first and the second register to get the desired output $|\tilde{m}_G\rangle\,|0\rangle$ and completes the application of K_G. Interestingly, we can apply the other resetting operator K_F just by replacing $F_{2^L}^{A\dagger}$ with the standard quantum Fourier transform F_{2^L}. Now we put everything together to expand the circuit in Fig. 3.1 into Fig. 3.5

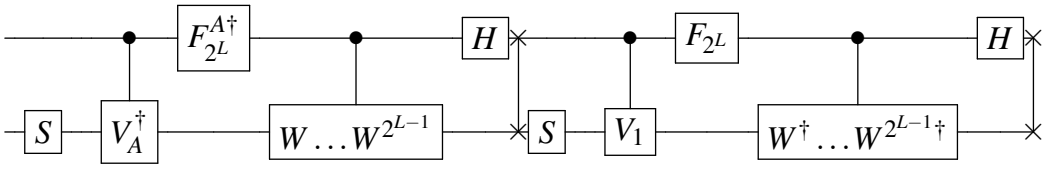


Figure 3.5: Schematic of the full circuit for modular multiplication. The operator S creates an equal superposition of the basis states (see Fig. 3.2 for details).V_A and V_1 denote phase gates. W is the cyclic permutation operator, H is Hadmard gate and F_{2^L} is QFT in 2^L dimensional Hilbert space. The circuit also contains SWAP gates in two different places.

3.4 Complexity

The complexity of the circuit can be calculated from Fig. 3.5. We note that the realization of the S gate using the circuit in Fig 3.2 requires $L(L+1)/2$ elementary gates. The gates V_1 and V_A each can be implemented using $O(L^2)$ phase-shift gates [76]. The QFT operators $F_{2^L}^{A}$ and F_{2^L} each require $O(L^2)$ gates. Finally, we note that the operators W, W^2, W^4, ... are modular addition by a constant number. The controlled modular additions can be done in sub-quadratic time following the method in [75]. Consequently, the complexity of our full circuit for modular multiplication is $O(L^2)$. In Shor's algorithm, one needs to apply upto L such modular multiplication for different powers of A which makes the complexity of the modular exponentiation module in Shor's algorithm $O(L^3)$.

3.5 Discussion

We have presented a quantum circuit for performing modular exponentiation, which is computationally the most expensive part of Shor's algorithm. A distinctive feature of our circuit is that it consists entirely of the QFT circuit and its variants. This is accomplished by utilizing Kitaev's algorithm for Fourier transform on the Abelian group $\mathscr{Z}_N$ with some modifications. Our approach is different from other proposals [62, 75, 78–81] where the circuit is constructed by combining quantum adder circuits. For Shor's algorithm to be useful in breaking RSA encryption, the algorithm must be able to factorize large numbers N that can be stored in about 2048 bits. The complexity of our circuit is $O(L^3)$ where L is the number of bits of the number being factorized. While this is larger by $O(L^\alpha)$, where $\alpha < 1$, compared to the best known proposal for Shor's algorithm [75], its advantages in reusing the structure of a single QFT implementation for modular multiplication may allow near-term experimental implementations for generic values of N, depending on the platform. Further, if one can adapt more efficient circuits for the QFT [87], which are only logarithmically worse than $O(L)$, to the matrix G_N, it may be possible to realize Shor's algorithm with a complexity only logarithmically worse than $O(L^2)$.

We conclude with some general comments. It is noteworthy that the complexity of any circuit depends on the order of the coprime A, where smaller values are more favorable. The circuit would be significantly simplified if one can a priori choose A with small order. Alternatively, it may be possible to run the circuit for a superposition of different As and extract the smallest order.

3.6 On the order of modular multiplicative group

Definition 3.1. *The set of all integers a such that* $(a,N) = 1$ *and* $1 \leq a < N$ *form a group under multiplication modulo N. The group is called modulo multiplication group and is henceforth denoted by* Π_N.

Definition 3.2. *If* $(a,N) = 1$ *and r is the smallest positive exponent such that*

$$a^r \equiv 1 \pmod{N}, \tag{3.21}$$

one says that a is of order r modulo N.

The number of elements of the group Π_N is $\phi(N) = (p-1)(q-1)$ where $\phi()$ denotes Euler's totient function. We know that for every group with number of elements n, $a^n = I$ for all elements a. This implies that for the group Π_N

$$a^{\phi(N)} \equiv 1 \pmod{N} \forall a \in \Pi_N. \tag{3.22}$$

However $\phi(N)$ is not always the smallest exponent satisfying Eqn. (3.22). The smallest exponent is called Carmichael function $\lambda(N)$.

Definition 3.3. *Carmichael function is the smallest positive exponent* $\lambda(N)$ *such that*

$$a^{\lambda(N)} \equiv 1 \pmod{N} \forall a \in \Pi_N. \tag{3.23}$$

The value of $\lambda(n)$ for any integer n can be calculated using the following recurrence

relation

$$\lambda(n) = \begin{cases} p^{r-1}(p-1) & \text{if } n = 2, 4, p^r \text{where } p \text{ is an odd prime,} \\ 2^{r-2} & \text{if } n = 2^r \text{where } r \geq 3, \\ \text{lcm}(\lambda(p_1^{\beta_1}), \lambda(p_2^{\beta_2}) \ldots \lambda(p_k^{\beta_k})) & \text{if } n = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k} \text{ where } p_i \text{ are the prime factors of } n. \end{cases} \tag{3.24}$$

From Eq. (3.24) one can deduce the following properties of λ:

1. For any prime exponent p^α

$$p^\alpha \leq 4\lambda(p^\alpha). \tag{3.25}$$

2. $\lambda(p^\alpha)$ is at most 3 to 1 when p is a prime.

We are interested to know how large is $\lambda(N)$ compared to N. There are two important theorems relevant to the size of $\lambda(N)$.

Theorem 3.1. *For any increasing sequence* $< n_i >_{i \in \mathbb{N}}$ *of natural numbers one has*

$$\lambda(n_i) > (\log n_i)^{(1/\log 2 + o(1)) \log\log\log n_i} \tag{3.26}$$

for i sufficiently large.

[88]

Proof. From the definition of $\lambda(n)$ we have

$$\lambda(n) = \text{lcm}\{\lambda(p^\alpha) : p^\alpha | n\}. \tag{3.27}$$

This implies

$$n = \prod_{p^\alpha | n} p^\alpha \leq \prod_{\lambda(p^\alpha) | \lambda(n)} p^\alpha. \tag{3.28}$$

Since $p^\alpha \leq 4\lambda(p^\alpha)$

$$n \leq \prod_{\lambda(p^\alpha)|\lambda(n)} 4\lambda(p^\alpha). \tag{3.29}$$

Furthermore λ is at most 3 to 1 when restricted to powers of prime. Hence

$$n \leq \prod_{d|\lambda(n)} (4\lambda(n))^3 \leq (4\lambda(n))^{3d(\lambda(n))} \tag{3.30}$$

where $d(k)$ denotes the number of divisors of k with k being an integer. It is known that[89]

$$d(k) \leq 2^{(1+o(1))\log k/\log\log k} \tag{3.31}$$

where k is an integer. Substituting this one gets

$$\lambda(n) > (\log n)^{(1/\log 2+o(1))\log\log\log n}. \tag{3.32}$$

□

Before stating the second theorem we need to define asymptotic density of a set of integers.

Definition 3.4. *If S is a set of positive integers, its asymptotic density $\rho(S)$ is defined as*

$$\rho(S) = \lim_{n\to\infty} \frac{|S \cap \{1,2,\ldots n\}|}{n}, \tag{3.33}$$

where $|\ldots|$ denotes the number of elements in a set.

Theorem 3.2. *There is a set S of positive integers with asymptotic density 1 such that for all $n \in S$*

$$\lambda(n) = \frac{n}{\log n^{(\log\log\log n+A+o(1/\log\log\log n))}} \tag{3.34}$$

where $A = -1 + \sum_{q \in \mathbb{P}} \log q/(q-1)^2 \approx .23$ *and* $\mathbb{P}$ *denotes the set of prime numbers.*

[88]

3.7 Relevance of the theorems to prime factorization

The numbers used in NSA encryption are generated by multiplying two large primes. One can construct an increasing sequence from the products of two distinct prime numbers. We denote this sequence as $\langle PQ_i \rangle_{i \in \mathbb{N}}$. We can use Theorem 3.1 to claim that for sufficiently large i

$$\lambda([PQ]_i) > (\log[PQ]_i)^{(1/\log 2 + o(1)) \log\log\log[PQ]_i}. \tag{3.35}$$

This gives us a lower bound on the value of λ for a composite number N consists of two large prime factors. However, this sequence doesn't necessarily have an overlap with the set S of Theorem 3.2. As a result, we can't use that to establish an upper bound on the value of $\lambda(PQ)$.

Chapter 4: Solitons in lattice field theories via tight-binding supersymmetry

4.1 Overview

Solitons are ubiquitous in nature and occur in a plethora of classical and quantum systems, among which include water waves [90–93], optical fibers [94], magnets [95], superfluids [96–98] and superconductors [99–102] - an incomplete list. While solitons have been observed for centuries, the elegant mathematical structure behind them, known as the inverse scattering method, is comparatively recent. The development of the inverse scattering method was highly influenced by the Fermi–Pasta–Ulam–Tsingou (FPUT) problem - numerical experiments carried out by Fermi et al. in 1954-1955 [103]. Fermi and co-workers were interested in the question of thermalization and sought to observe it in a discrete chain of non-linear oscillators. However, they numerically observed a recurrent, almost periodic behavior instead, which became known as the Fermi–Pasta–Ulam–Tsingou paradox [104]. This paradox motivated the work by Kruskal and Zabusky ten years later, who showed that the FPUT problem maps onto the Korteweg–de Vries (KdV) equation in the continuum limit [91]. They performed their own simulations of the dynamics of the KdV equation, which showed a number of features, surprising at the time, but understood now in terms of integrable dynamics. Kruskal and Zabusky coined the term "soliton" and their work on the KdV equation gave impetus to the development of the inverse scattering method. The inverse scattering method eventually provided complete understanding of the nature

of integrable solutions in both the KdV equations and other continuous classical integrable theories [105–109]. At the heart of the method is a mapping of the KdV equation to an auxiliary quantum scattering problem, whose time-evolved potential is a solution to the KdV equation.

This link between the purely classical problem of waves in shallow water and quantum mechanics has led to a number of other unexpected discoveries. Notably, Dashen, Hasslacher, Neveu, Shei and others [110–112] showed in the 1970s that inverse scattering methods can be used to construct non-perturbative soliton solutions to saddle-point equations of $1+1$ dimensional quantum field theories (justified in the large-N limit). The saddle point equations of the Gross-Neveu (GN) model are mathematically equivalent to the auxiliary scattering problem in the KdV equation. It was also shown, using trace identities for the scattering problem, that the saddle points are achieved for reflectionless potentials.

These results further propagated to condensed matter physics. In particular, Brazovsky and others recognized that the chiral Gross-Neveu model is equivalent to the problem of interacting electrons in one dimension and therefore the (classical) solitons of the chiral GN model represent static solitons in either Peierels-insulating charge-density-wave states (for repulsive fermions) or superconducting states (for attractive fermions) [100–102, 113–119]. In these cases too, the solitons originated from the reflectionless self-consistent solutions of the Bogoliubov-de Gennes (BdG) equations – the classical saddle point of the action describing the superconductor/Peierels insulator. More recently, these methods were applied to Larkin-Ovchinnikov-Fulde-Ferrel superconducting phases [120, 121] and time-dependent superconductors, featuring a solitonic lattice and periodic-in-time soliton trains of the superconducting order parameter correspondingly [99, 119, 122–130]. Moving solitons have also been considered in both high-energy context [131] and for cold-atom superfluids [96–98, 107, 132, 133]. Another more controversial example has been the attempt to construct soliton trains in imaginary time (to represent hypothetical at this stage

imaginary-time crystals) [134–136]. In all these cases however, the mathematical construction of solitons hinges on the reflectionless potentials of the underlying scattering problem.

A useful method for constructing such potentials is supersymmetric quantum mechanics (for a comprehensive review, see [137]). Continuous quantum-mechanical supersymmetry involves writing the Schrödinger operator - the Hamiltonian - as a product of two operators $H = A^\dagger A$ and constructing another Schrödinger operator $\widetilde{H} = AA^\dagger$. It can be shown that the two corresponding Hamiltonians/potentials are (almost) isospectral and share the same scattering data. This allows for the construction of non-trivial reflectionless potentials. The simplest example is to start with the transparent constant potential and find its superpartner, which happens to be related to the simplest KdV single-soliton solution. The process can be iterated and a series of reflectionless potentials can be constructed including multi-soliton solutions.

All in all, the combination of the inverse scattering method and quantum-mechanical supersymmetry (SUSY) allows to build exact analytic non-linear soliton solutions to a variety of diverse problems from bound states in large-N field theories to non-linear excitations in superfluids and superconductors, with both static and dynamic solitons recently of interest.

The resolution of the Fermi-Pasta-Ulam paradox has been understood through both KdV limit and the Toda lattice – a fully integrable classical lattice model, which gives rise to the FPUT problem as its Taylor expansion [138]. The first appearance of inverse scattering methods applied to a lattice field theory is in the Ablowitz-Ladik model [139]. However, surprisingly the lattice field theoretical and superconducting analogies of the Toda lattice have not been fully explored. A large number of integrable lattice models have been considered using more modern methods in quantum integrability that go beyond classical inverse scattering [140, 141]. However, it appears that the role of reflectionless potentials and their explicit construction have not been fully investigated in the context of

interacting tight-binding models. This paper fills this gap and develops a general framework to study solitons in a family of large-N lattice field theories.

In particular, we first introduce a lattice variant of the Gross-Neveu model that has site dependent hoppings. With the aid of previously known trace identities relating scattering data of the equations of motion and parameters of the Lagrangian, we rewrite the action of the Gross-Neveu model in terms of scattering data (using the first few trace identities) and compute the saddle points of this action. This gives us both the bound state spectrum for non-topological lattice solitons and the result that the saddle point corresponds to reflectionless potentials associated with the equations of motion. We use the remaining trace identities to construct a hierarchy of lattice field theories which admit exact soliton solutions also corresponding to reflectionless potentials.

Next, we construct these reflectionless potentials directly from lattice supersymmetry (also called the *Darboux transformation*). We show that local tight-binding models in an onsite potential map under discrete SUSY onto the same class of models, but with site-dependent hoppings. This observation had been previously made and exact albeit restricted soliton hierarchies were previously constructed (see *Note Added* section). However, we present a formalism where the onsite potential and hopping can be iteratively obtained by evaluating a continued fraction – this generalizes the topological soliton solutions previously obtained. We also describe a novel recipe for constructing non-topological solitons under this continued fraction formalism. This approach can be easily extended to more exotic soliton solutions with non-uniform boundary conditions.

We finally consider the chiral Gross-Neveu model, whose equations of motion coincide with the BdG equations for a lattice superconductor. We derive a previously unknown set of trace identities for this system and use these identities to show that the saddle point of this lattice field theory corresponds to reflectionless potentials of the associated equations of motion. The simplest non-trivial class of solutions can be obtained directly from super-

symmetry methods, which describe solitons exhibiting a nontrivial phase slip (also known as twisted-kinks) – since such solitons should have nontrivial dynamics, this motivates the pursuit of the theory of dynamical solitons for such lattice systems. We end by discussing the similarities of these lattice field theories to coupled Toda chains.

4.2 Gross-Neveu model and Korteweg-de Vries equation

We start with a review of soliton solutions in continuum systems. The simplest model which exhibits such solutions is the Korteweg-de Vries equation, which was first used to describe shallow water waves [90]. The KdV equation can be generalized to construct a hierarchy of nonlinear differential equations, each of which also supports soliton solutions. A seemingly unrelated system is the Gross-Neveu model, which is field theory of N flavors of massless fermions subject to an attractive potential. When N is large, the Gross-Neveu model is a toy model of quantum chromodynamics: it is asymptotically free, and spontaneously breaks chiral symmetry, which results in the fermions acquiring a mass, therefore gapping the theory. The mean field theory of a chiral version of the Gross-Neveu model, also known as the Nambu-Jona-Lasinio model, can be shown to be equivalent to BCS superconductivity in 1D [102, 119]. Both the Gross-Neveu and the chiral Gross-Neveu model have nontrivial saddle point solutions which correspond to solitons.

It turns out that the construction of soliton solutions for the KdV equation and the Gross-Neveu field theories are nearly identical. This is because both the KdV equation as well as the equations of motion for the Gross-Neveu model can be mapped onto a 1D quantum scattering problem. Based on a series of *trace identities* that connect the potential of the scattering problem to the scattering properties of plane wave solutions, it can be shown that soliton solutions correspond to reflectionless potentials of the scattering problem. Constructing these reflectionless potentials can be achieved through several methods,

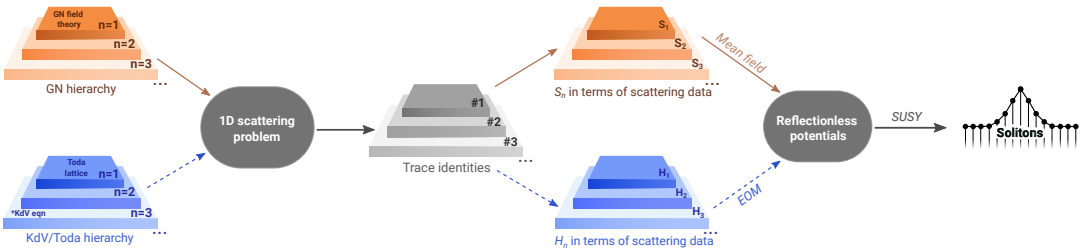


Figure 4.1: A schematic depicting the sequence of steps used to generate a soliton hierarchy. We start with a hierarchy of field theories (the first of which is the Gross-Neveu field theory) or a hierarchy of dynamical systems/partial differential equations (the first in the Toda hierarchy is the Toda lattice, and the third in the KdV hierarchy is the KdV equation). The equations of motion of the GN field theory and a suitable change of variables for the KdV equation/Toda lattice map these seemingly unrelated systems to a one-dimensional scattering problem. With the help of trace identities derived in this scattering problem, we may rewrite either the action or the Hamiltonian in terms of scattering data, i.e. the reflection coefficient, the transmission coefficient, and the bound state energies of the scattering problem. There are also a hierarchy of trace identities, and each one uniquely maps onto one of the field theories or dynamical systems in the original hierarchies. The saddle point of the action corresponds to a reflectionless potential, and the equations of motion of the Hamiltonian systems imply the conservation of the magnitude of the reflection coefficient. In both cases, reflectionless potentials are either valid saddle points of the action or solutions to the dynamical system. These potentials are retrieved explicitly using supersymmetry methods, or more elaborately using the Gelfand-Levitan equation and the inverse scattering formalism.

one of which is quantum mechanical supersymmetry. In this section, we will briefly review these results, which have been summarized in Figure 4.1.

4.2.1 Gross-Neveu (GN) model

The Lagrangian for the Gross-Neveu model in $(1+1)$ dimensions is given by [110]:

$$\mathscr{L} = \sum_{k=1}^{N} i\overline{\psi}^{(k)} \partial\!\!\!/ \psi^{(k)} + \frac{g^2}{2}\left(\sum_{k=1}^{N} \overline{\psi}^{(k)}\psi^{(k)}\right)^2, \tag{4.1}$$

where $\psi^{(k)}(x,t)$ is a two-component fermionic field and k, which ranges from 1 to N, labels fermion flavor. Throughout the analysis, we assume that N is large, which justifies the use of mean field theory. We also adopt the standard definitions $\overline{\psi}^{(k)} = \psi^{\dagger(k)}\gamma_0$ and $\partial\!\!\!/ = \gamma_\mu \partial^\mu$ with γ_μ being the Dirac matrices in (1+1) dimension. Throughout the text, we will choose

the representation where $\gamma_0 = -\sigma_x$, $\gamma_1 = -i\sigma_z$, and $\gamma_5 = \gamma_0\gamma_1 = \sigma_y$. For the sake of brevity, we also introduce the following notations:

$$\overline{\psi}\partial\!\!\!/\psi \equiv \sum_{k=1}^{N} \overline{\psi}^{(k)}\partial\!\!\!/\psi^{(k)}, \tag{4.2}$$

$$\overline{\psi}\psi \equiv \sum_{k=1}^{N} \overline{\psi}^{(k)}\psi^{(k)}. \tag{4.3}$$

In the path integral formulation the real time functional can be written as

$$Z = \int \mathscr{D}\psi\mathscr{D}\overline{\psi}\exp\left[i\int d^2x\left(-i\overline{\psi}\partial\!\!\!/\psi - \frac{g^2}{2}\left(\overline{\psi}\psi\right)^2\right)\right] \tag{4.4}$$

We introduce a Hubbard-Stratonovich field $\Delta(x,t)$, so that the path integral becomes

$$Z = \int \mathscr{D}\psi\mathscr{D}\overline{\psi}\mathscr{D}\Delta\exp\left[i\int d^2x\left(-i\overline{\psi}\partial\!\!\!/\psi - g\Delta\overline{\psi}\psi - \frac{\Delta^2}{2}\right)\right], \tag{4.5}$$

Following a standard mean field assumption, we assume that the Hubbard-Stratonovich field possesses no dynamics, and we search for static solutions which correspond to the saddle point of the action. We further restrict our search of saddle point solutions to those that satisfy $\lim_{|x|\to\infty}\Delta(x) = \Delta_0$. Due to the time independence of the HS field, the equations of motion for the fermionic fields map onto a one-dimensional scattering problem for each component of the fermionic field; the effective scattering problem is equivalent to the time independent Schrödinger equation

$$-\partial_x^2\psi_{1,2} + u_{1,2}(x)\psi_{1,2} = k^2\psi_{1,2}. \tag{4.6}$$

where ψ_1 and ψ_2 are two components of the fermion, k^2 is the energy and the effective potential

$$u_{1,2}(x) \triangleq u_{\pm}(x) = g^2(\Delta^2 - \Delta_0^2) \pm g\frac{d\Delta}{dx} \tag{4.7}$$

vanishes asymptotically. The saddle point solutions can therefore be constructed by recasting the action in terms of scattering data of this scattering problem.

4.2.2 Korteweg-de Vries (KdV) equation

The KdV equation is a non-linear partial differential equation used to describe a wide range of phenomena from waves on a shallow water surface [90, 142, 143] to ion-acoustic waves in plasma [144, 145]. For a function $u(x,t)$ the KdV equation is

$$\frac{\partial u}{\partial t} - 6u\frac{\partial u}{\partial x} + \frac{\partial^3 u}{\partial x^3} = 0. \tag{4.8}$$

At first sight, Eqn. (4.8) does not seem to have anything in common with Gross-Neveu model discussed in the previous subsection. However, the KdV equation can also be mapped onto a time independent Schrödinger equation, whose effective potential coincides with the function $u(x,t)$. To explicitly see this mapping, define a function $v(x,t)$ which satisfies

$$u = v^2 + \frac{\partial v}{\partial x}. \tag{4.9}$$

Substituting $v = \frac{\partial \log \psi}{\partial x}$ into Eqn. (4.9) one finds

$$u = \frac{\partial_x^2 \psi}{\psi}. \tag{4.10}$$

Note that if $u(x,t)$ is a solution of KdV equation then so is $\bar{u}(x,t) = u(x+6\lambda t,t) + \lambda$. This foreshadows the fact that the KdV equation possesses soliton solutions which move without

changing shape. Thus, we can replace u in Eqn. (4.10) with $u-\lambda$ to write it as

$$-\partial_x^2\psi + u\psi = \lambda\psi. \tag{4.11}$$

If we set $\lambda = k^2$ then Eqn. (4.11) is same as Eqn. (4.6) derived for the GN model [1]. In the KdV equation, propagating solitons are described by the time-evolved potential $u(x,t)$; under the mean field assumption, solitons are static in the GN model and are described by $\Delta(x)$, which is related to $u(x,t=0)$ via Eqn. (4.7).

4.2.3 Trace identities for Schrödinger equation

Both the GN model and the KdV equation map onto a time independent Schrödinger equation. Solutions to the Schrödinger equation can be both bound as well as scattering, and the scattering data must account for both types of states. In the asymptotic limit $x \to \pm\infty$, scattering states have the form

$$\lim_{x\to-\infty}\psi(x,k) = e^{ikx} + r(k)e^{-ikx} \tag{4.12}$$

$$\lim_{x\to\infty}\psi(x,k) = t(k)e^{ikx}, \tag{4.13}$$

where $r(k)$ and $t(k)$ are the momentum-dependent reflection and transmission coefficients respectively. For a bound state with energy $-\kappa_\ell^2$, the wavefunction has the asymptotic form

$$\lim_{|x|\to\infty}\psi_\ell(x) = N_\ell e^{-\kappa_\ell|x|}, \tag{4.14}$$

[1] The reader should note that the appearance of Schrödinger equation in both the GN and the KdV models does not imply their equivalence – the Schrödinger equation and soliton solutions emerge as a result of linearizing the GN model, while the soliton solutions in the KdV equation are exact.

where N_ℓ is a normalization. We now define the scattering data as the set $\{r(k), t(k), \kappa_\ell\}$. Remarkably, there exists a hierarchy of *trace identities* that relates integrals of powers and derivatives of the potential to the reflection coefficient and the bound state energies [146–149]. Suppose the potential we are given has N bound states. Then, the trace identities are given by

$$\frac{1}{2\pi i}\int_{-\infty}^{\infty} q^{2n}\log\left[1-|r(q)|^2\right]\,dq-\frac{2}{2n+1}\sum_{\ell=1}^{N}(i\kappa_\ell)^{2n+1}=-\frac{1}{(2i)^{2n+1}}\int_{-\infty}^{\infty}\beta_{2n+1}(x)\,dx, \tag{4.15}$$

where n is a non-negative integer and β_n are functions of the potential which are recursively determined from the coupled differential equations

$$\beta_{n+1}(x)=-\frac{d}{dx}\beta_n(x)-\sum_{m=1}^{n-1}\beta_m(x)\beta_{n-m}(x) \tag{4.16}$$

$$\beta_1(x)=u(x). \tag{4.17}$$

For clarity and convenience, we explicitly reproduce the first three identities below:

$$-\frac{1}{2i}\int_{-\infty}^{\infty}u\,dx=\frac{1}{2\pi i}\int_{-\infty}^{\infty}\log\left(1-|r(q)|^2\right)dq-2\sum_{\ell}(i\kappa_\ell), \tag{4.18}$$

$$-\frac{1}{8i}\int_{-\infty}^{\infty}u^2\,dx=\frac{1}{2\pi i}\int_{-\infty}^{\infty}q^2\log\left(1-|r(q)|^2\right)dq-\frac{2}{3}\sum_{\ell}(i\kappa_\ell)^3, \tag{4.19}$$

$$-\frac{1}{32i}\int_{-\infty}^{\infty}(2u^3+u_x^2)\,dx=\frac{1}{2\pi i}\int_{-\infty}^{\infty}q^4\log\left(1-|r(q)|^2\right)dq-\frac{2}{5}\sum_{\ell}(i\kappa_\ell)^5. \tag{4.20}$$

In particular, the first identity relates the integral of the potential to the reflection coefficient and bound state energies; this will be useful for performing a change of variables in the Gross-Neveu action.

4.2.4 Soliton solutions are reflectionless potentials

One can formulate both the Gross-Neveu mean field action and the KdV equation in terms of scattering data using the trace identities of section 4.2.3. For the GN model, the Lagrangian in Eqn. (4.5) is quadratic in the fermion fields ψ and $\overline{\psi}$. Consequently the fermions can be integrated out, yielding an effective action for the HS field

$$S_{\text{eff}}(\Delta) = -\log\left[\int \mathscr{D}\psi\mathscr{D}\overline{\psi}\exp\left(-\int_{-\infty}^{\infty}dx\int_0^T dt\,\overline{\psi}\left(i\partial\!\!\!/ - g\Delta\right)\psi\right)\right] - \frac{1}{2}\int_{-\infty}^{\infty}dx\int_0^T dt\,\Delta^2. \tag{4.21}$$

Using the first trace identity given by Eqn. (4.18) and other standard results from path integration and scattering theory one can write the effective action as a function of scattering data [110] as

$$\begin{aligned} S_{\text{eff}} \propto \frac{1}{g^2}\int_{-\infty}^{\infty}\log\left[1-|r(k)|^2\right]dk + \frac{4\pi}{g^2}k_0 \\ -\frac{1}{\pi}\int_0^{\infty}\frac{kdk}{\sqrt{k^2+g^2\sigma_0^2}}\left(\log\left(1-|r(k)|^2\right)+4\pi\tan^{-1}\frac{k_0}{k}\right)+\text{const.} \end{aligned} \tag{4.22}$$

where it has been assumed that there is only one bound state with energy $-k_0^2$. The saddle point of the effective action can be determined by first extremizing over the reflection coefficient; we see that the minimum corresponds to a reflectionless potential, i.e the choice of $\Delta(x)$ such that the reflection coefficient $r(k) = 0$.

A similar connection to reflectionless potentials can be made for the KdV equation. It has been has shown that the KdV equation is a Hamiltonian system and arises from the Hamiltonian $H[u] = \int_{-\infty}^{\infty}dx\left[u^3(x)+\frac{u_x^2}{2}\right]$ [150]. One can check that the Hamiltonian H yields the KdV equation in the form

$$\frac{\partial u}{\partial t} = \frac{\partial}{\partial x}\frac{\delta H}{\delta u}, \tag{4.23}$$

where $\frac{\delta H}{\delta u}$ indicates a functional derivative of H. Using the third non-trivial trace identity (Eqn. (4.20)), this Hamiltonian can be written solely in terms of scattering data as

$$H_{\mathrm{KdV}} = -\frac{8}{\pi}\int_{-\infty}^{\infty} k^4 \log\left(1-|r(k)|^2\right) dk - \frac{32}{5}\sum_{i=1}^{N} k_i^5, \tag{4.24}$$

where N is the number of bound states and $-k_i^2$ is the energy of the ith bound state. However, one must argue that the scattering data can be rewritten as pairs of canonically conjugate variables. This was first verified by Faddeev and Zakharov, and the corresponding Hamilton's equations of motion imply that one class of solutions to the KdV equation are time-dependent reflectionless potentials. In fact, a particular combination of the scattering data turns out to be action-angle coordinates for the KdV Hamiltonian, which manifestly indicates the integrable nature of the system (see [146, 151]).

The remaining question left is how to construct such potentials, which correspond to soliton solutions. One such method utilizes supersymmetric quantum mechanics, which is briefly summarized in section 4.4.1. In particular, applying the supersymmetry transformation to a constant potential results in a nontrivial reflectionless potential for the Schrödinger equation; this corresponds to a kink soliton.

Note that for the KdV equation the third trace identity serves as the Hamiltonian. However, in general, one can consider any of the trace identities as a candidate Hamiltonian and construct equations of motion; each such equation of motion corresponds to a nonlinear higher-order differential equation for $u(x,t)$, each of which is integrable. The set of equations constructed in this manner form the KdV hierarchy [93, 152].

4.2.5 Field theory hierarchy

While the KdV hierarchy is a celebrated concept in classical integrability theory, it is possible to construct a similar hierarchy for the Gross-Neveu field theories. Note that only

the first trace identity given by Eqn. (4.18) has been used to write the action of GN model as a function of the scattering data. We may similarly use the other trace identities to construct a hierarchy of field theories whose saddle point corresponds to reflectionless potential. To construct the field theory after the Gross-Neveu model in the hierarchy, we replace the first trace identity by hand with the second trace identity, obtaining the action

$$\mathscr{L}_2 = i\overline{\psi}\partial\!\!\!/\psi - g\Delta\overline{\psi}\psi - \left(g^4\Delta^4 + g^2\Delta\frac{\partial^2\Delta}{\partial x^2}\right). \tag{4.25}$$

One can integrate out the HS field to write the Lagrangian only in terms of the fermions as

$$\mathscr{L}_2 = i\overline{\psi}\partial\!\!\!/\psi - \log\left(\int d\Delta \exp\left[\int dx\left(ig\Delta\overline{\psi}\psi - g^2\Delta\frac{\partial^2\Delta}{\partial x^2} - g^4\Delta^4\right)\right]\right). \tag{4.26}$$

This is the second field theory in the hierarchy. In principle, one can construct one such field theory per trace identity; however, each higher order field theory is intractable and non-local when one attempts to integrate out the HS field.

4.3 Solitons in a lattice Gross-Neveu model

In the continuum Gross-Neveu field theory, it was argued that stationary solutions to the action correspond to choices of $\Delta(x)$ such that the equations of motion describe a particle in a reflectionless potential. In lattice systems, which are currently achievable in cold atom experiments, there are several differences that may result in exotic soliton solutions. Firstly, there exist non-unique discretization schemes of placing fermions on a lattice that give rise to different microscopic dynamics even if they reduce to the same theory in the continuum limit. Secondly, if a lattice theory possesses soliton solutions, then a solitonic texture may arise in both the onsite potential and the hopping, which is not seen in the continuum limit. And lastly, at the scale of the lattice spacing, the dispersion relation looks like a

band structure, thus differing markedly from the dispersion in the continuum limit; this may result in different characteristic soliton spectra and propagation velocities (the latter of which we do not consider in this paper). The aforementioned reasons therefore make it enticing to study solitons in discretized field theories.

For lattice systems we will adopt a reverse engineering approach, starting with known discrete trace identities due to Toda [138] and using these identities to subsequently construct lattice models whose saddle points correspond to reflectionless potentials. In Section 4.5, we perform the same analysis for the chiral Gross-Neveu model which is an effective description for a lattice superconductor. In the process, we derive previously unknown trace identities for the discrete Dirac operator.

4.3.1 Trace identities for tight-binding Hamiltonians

Before introducing the lattice Gross-Neveu model, we first set out to derive trace identities for discrete scattering problems. To define the scattering problem we consider a generic tight binding Hamiltonian with nearest neighbour hopping, written out explicitly as

$$\mathscr{H} = \sum_{n=-\infty}^{\infty} \left(-t_{n+1}|n\rangle\langle n+1| + \text{h.c.} + u_n|n\rangle\langle n|\right), \tag{4.27}$$

The Hamiltonian describes a particle in a discrete Schrödinger equation, which we write as

$$-(t_{n+1}\psi_{n+1} + t_n\psi_{n-1}) + u_n\psi_n = \lambda\,\psi_n, \tag{4.28}$$

where n is the site number, t_n is a site-dependent hopping which is absent in the continuum case, and u_n is a discrete onsite potential. Both t_n and u_n will later be shown to be expressible in terms of the HS parameter. The energy λ is independent of n, and we can determine it by constructing eigenfunctions in the asymptotic limit when $n \to \infty$; these eigenfunctions

satisfy

$$-(\psi_{n+1}+\psi_{n-1})+u\psi_n=\lambda\psi_n, \tag{4.29}$$

where we have used that $\lim_{n\to\pm\infty}u_n=u$ and $\lim_{n\to\pm\infty}t_n=1$. The solution for Eqn. (4.29) is $\psi_n=e^{i\phi n}\equiv z^n$ where ϕ is a quasi-momentum constrained to lie within the interval $[0,2\pi)$; this gives the dispersion $\lambda=2\cos\phi+u$.

Next, we will reproduce the trace identities analogous to Eqn. (4.15) that relate the potential u_n to the scattering data of the discrete Schrödinger equation, which were previously known to Toda *et al.* [138, 153]. We first make a choice of two independent basis functions of Eqn. (4.56). We denote those two bases as $\{f_n(z),f_n(\frac{1}{z})\}$ and $\{g_n(z),g_n(\frac{1}{z})\}$; their asymptotic behavior is given by

$$\lim_{n\to\infty}f_n(z)=z^n, \tag{4.30}$$

$$\lim_{n\to-\infty}g_n(z)=z^{-n}. \tag{4.31}$$

These are known as the *Jost functions*, which is a frequently used representation in scattering theory. This choice of basis is necessary in order to derive well-behaved trace identities. Since both f_n and g_n independently form a basis, one may be written as a linear combination of the other. Thus, we have the relation

$$f_n(z)=b(z)g_n(z)+a(z)g_n\left(\frac{1}{z}\right), \tag{4.32}$$

where we have introduced coefficients a and b which can be shown to be related to the reflection and transmission coefficients of the original discrete scattering problem. A valid scattering eigenstate for the discrete Schrödinger equation in terms of the Jost functions is $\psi_n(z)=\frac{f_n(z)}{a(z)}$; the asymptotic behavior of this solution assumes a form familiar from

scattering theory:

$$\psi_n(z) = \begin{cases} z^n + \frac{b(z)}{a(z)} z^{-n}, & \text{for } n \to -\infty \\ \\ \frac{1}{a(z)} z^n, & \text{for } n \to \infty \end{cases} \tag{4.33}$$

From Eqn. (4.33) we find that the reflection coefficient $r(z)$ and the transmission coefficient $t(z)$ are related to $a(z)$ and $b(z)$ according to the relations $r(z) = \frac{b(z)}{a(z)}$ and $t(z) = \frac{1}{a(z)}$. Since the reflection and transmission coefficients satisfy $|r|^2 + |t|^2 = 1$ we have

$$|a(z)|^2 = \frac{1}{1 - |r(z)|^2}. \tag{4.34}$$

So far, we have considered the scattering states for the discrete Schrödinger operator; it may consist of discrete bound states as well, which are necessary for a complete characterization of the scattering data. The location of the bound states occur at $z = z_j$ for which $a(z_j) = 0$; these correspond to eigenstates which scale as z_j^n for large n. We also require the physical constraint that $|z_j| < 1$ in order for the wavefunction to be normalizable and decay exponentially at infinity. Thus, we require the following constraints on $a(z)$:

$$|a(z)|^2 = \frac{1}{1 - |r(z)|^2} \text{ when } |z| = 1, \tag{4.35}$$

$$a(z_j) = 0 \text{ for some discrete } |z_j| < 1. \tag{4.36}$$

Appealing to the theory of meromorphic functions, the properties of $a(z)$ allow us to uniquely define $\log|a(z)|$ within the unit disk $|z| < 1$ via the Poisson-Jensen theorem:

$$\log|a(z)| = \sum_{j=1}^{M} \log\left|\frac{z - z_j}{1 - z_j z}\right| - \frac{1}{4\pi}\int_0^{2\pi} \Re\left(\frac{e^{i\phi} + z}{e^{i\phi} - z}\right) \log\left[1 - |r(e^{i\phi})|^2\right] d\phi, \tag{4.37}$$

where M is the number of bound states and $\Re[z]$ means the real part of z. We can expand

the right hand side of the equation above using the following series expansions:

$$\log \frac{z-z_j}{1-z_j z} = \log z_j + \sum_{p=1}^{\infty} \frac{z_j^p - z_j^{-p}}{p} z^p, \tag{4.38}$$

$$\Re\left(\frac{e^{i\phi}+z}{e^{i\phi}-z}\right) = 1 + 2\sum_{p=1}^{\infty} \cos(p\phi - p\theta)|z|^p. \tag{4.39}$$

where $z = |z|e^{i\theta}$. Substituting these expansions, we may write

$$\log \frac{|a(z)|}{|a(0)|} = \sum_{p=1}^{\infty} \left[\sum_{j=1}^{M} \Re\left(\frac{z_j^p - z_j^{-p}}{p} z^p\right) - \frac{|z|^p}{2\pi} \int_0^{2\pi} \log\left[1 - |r(e^{i\phi})|^2\right] \cos(p\phi - p\theta) d\phi \right]. \tag{4.40}$$

One can write $\log(a(z)/a(0))$ to the onsite potential via the following relation:

$$-\log \frac{a(z)}{a(0)} = \sum_{n=1}^{\infty} \frac{(-1)^n \mathrm{Tr}\,(H^n - (H_0)^n)}{n(z+\frac{1}{z})^n}, \tag{4.41}$$

where H and H_0 are tridiagonal matrices; H is the Hamiltonian for the Schrödinger operator with elements $H_{n,n-1} = -t_n, H_{n,n+1} = -t_{n+1}$, and $H_{n,n} = u_n$, and H_0 is the asymptotic form of the Hamiltonian with matrix elements $(H_0)_{n,n-1} = (H_0)_{n,n+1} = -1$ and $(H_0)_{n,n} = u$. The derivation of the Eqn. (4.41) is given in Appendix **??**. In section 4.5, we derive similar identities for the Dirac operator in the case of the chiral Gross Neveu model.

We can expand the right hand side of Eqn. (4.41) as a power series of z to write

$$\sum_{p=1}^{\infty} K_p z^p = \sum_{n=1}^{\infty} \frac{(-1)^{n+1} \mathrm{Tr}\,(H^n - (H_0)^n)}{n(z+\frac{1}{z})^n}, \tag{4.42}$$

where K_p are real coefficients that depend on the potential and the hopping. We have already derived an alternate expression for $\log(|a(z)|/|a(0)|)$ in Eqn. (4.40) which we can

compare with Eqn. (4.42) to write

$$\sum_{p=1}^{\infty} K_p |z|^p \cos p\theta = \sum_{p=1}^{\infty} \left[-\frac{|z|^p}{2\pi} \int_0^{2\pi} \log\left(1-|r(e^{i\phi})|^2\right) \cos(p\phi - p\theta)\, d\phi \right. \\ \left. + \sum_{j=1}^{M} \Re\left(\frac{z_j^p - z_j^{-p}}{p} z^p \right) \right]. \quad (4.43)$$

In general, and for the cases we will consider, the Hamiltonian is real; thus the eigenstates can be chosen to be real and we expect the bound states to monotonically decay at infinity without spatial oscillations. This implies that z_j is real. With this simplification, we set $\theta = 0$ and compare the coefficients of z^p in the above equation to get

$$K_p = -\frac{1}{2\pi} \int_0^{2\pi} \log\left(1-|r(e^{i\phi})|^2\right) \cos(p\phi)\, d\phi + \sum_{j=1}^{M} \frac{z_j^p - z_j^{-p}}{p}. \quad (4.44)$$

Matching to the series expansion in terms of the onsite potential and hopping yields a discrete version of the trace identities discussed in Dashen et al. [110]. For convenience, we write the first two identities associated with matching the two lowest order terms in both series expansions:

$$\sum_{n=-\infty}^{\infty} u_n = -\frac{1}{2\pi} \int_0^{2\pi} \log\left(1-|r(e^{i\phi})|^2\right) \cos(\phi)\, d\phi + \sum_{j=1}^{M} \left(z_j - \frac{1}{z_j} \right), \quad (4.45)$$

$$\sum_{n=-\infty}^{\infty} u_n^2 + 2t_n^2 = -\frac{1}{2\pi} \int_0^{2\pi} \log\left(1-|r(e^{i\phi})|^2\right) \cos(2\phi)\, d\phi + \frac{1}{2} \sum_{j=1}^{M} \left(z_j^2 - \frac{1}{z_j^2} \right). \quad (4.46)$$

Much like in the continuous case, sums of the hopping and onsite potentials can be related directly to the reflection coefficient of the scattering problem and the locations of the bound states.

4.3.2 Lattice Gross-Neveu model

Motivated by the continuous case we can formulate the discrete version of the Gross-Neveu model. For a discrete two-component fermionic field $\Psi_n(t)$, where n is the lattice site index, the action $S = \sum_n \mathscr{L}_n$ can be specified by the lattice Lagrangian

$$\mathscr{L}_n = \sum_{k=1}^{N} \Psi_n^{\dagger(k)}(t) \begin{pmatrix} i\frac{\partial}{\partial t} & \partial_n \\ \partial_n^\dagger & i\frac{\partial}{\partial t} \end{pmatrix} \Psi_n^{(k)}(t) + \frac{g^2}{2}\left(\Psi_n^{\dagger(k)}(t)\gamma_0\Psi_n^{(k)}(t)\right)^2, \tag{4.47}$$

where N is the number of flavors of fermions and $\Psi_n^{(k)}(t) = \left(\psi_n^{(1,k)}(t), \psi_n^{(2,k)}(t)\right)^T$ can be written as a two-component field. Throughout the text, we will assume that N is large in order to justify subsequent saddle point computations. The operators ∂_n and $\partial_n^\dagger$ the analogues of derivative operators in the continuum limit but will be represented as discrete "shift" operators with matrix elements $\partial_n f_n \triangleq \tau_{n+1} f_{n+1}$. The fermionic field is always assumed to be time dependent but for the sake of brevity we will not explicitly write it. We also suppress the sum over flavors by introducing the following notation:

$$\Psi_n^\dagger \mathbf{M} \Psi_n \equiv \sum_{k=1}^{N} \Psi_n^{\dagger(k)} \mathbf{M} \Psi_n^{(k)}, \tag{4.48}$$

where $\mathbf{M}$ is a 2×2 matrix. We introduce a discrete Hubbard-Stratonovich (HS) field $\Delta_n(t)$ to write an equivalent Lagrangian:

$$\mathscr{L}_n = \Psi_n^\dagger \begin{pmatrix} i\frac{\partial}{\partial t} & \partial_n + g\Delta_n(t) \\ \partial_n^\dagger + g\Delta_n(t) & i\frac{\partial}{\partial t} \end{pmatrix} \Psi_n - \frac{\Delta_n^2(t)}{2}. \tag{4.49}$$

As in the continuous case, we may recover the original Lagrangian after integrating out the HS field. We work in the large-N/mean field limit, and thus assume that the HS parameter is

time-independent. The Lagrangian is quadratic in the fermionic field, so we may integrate out the fermions to get the effective action for Δ:

$$S_{\text{eff}}(\Delta) = S_1(\Delta) - \log \int \mathscr{D}\Psi \mathscr{D}\Psi^\dagger \exp\left[-S_2\left(\Psi,\Delta\right)\right], \tag{4.50}$$

where

$$S_1(\Delta) = -\frac{T}{2}\sum_n \Delta_n^2 \tag{4.51}$$

$$S_2(\Psi,\Delta) = \sum_n \int_0^T dt\, \Psi_n^\dagger \begin{pmatrix} i\frac{\partial}{\partial t} & \partial_n + g\Delta_n \\ \partial_n^\dagger + g\Delta_n & i\frac{\partial}{\partial t} \end{pmatrix} \Psi_n. \tag{4.52}$$

Note that the integration measure in the path integral is defined as $\mathscr{D}\psi = \prod_n d\psi_n$. We will show that the effective action can be written as a function of the scattering data according to the following equation:

$$\frac{S_{\text{eff}}}{T} = \frac{1}{4\pi g^2}\int_0^{2\pi} \log\left(1 - |r(e^{i\phi})|^2\right)\cos(\phi)\, d\phi - \frac{1}{g^2}\sum_{j=1}^{M}\left(z_j + z_j^{-1}\right) + 2N\int_0^{2\pi}\frac{d\phi}{2\pi}\frac{\sin(\phi)}{\sqrt{u-2\cos\phi}}\delta_t(\phi), \tag{4.53}$$

where r is the reflection coefficient of the scattering problem associated with the equations of motion, z_j is related to the energy of the bound states, M is the number of bound states and $\delta_t(\phi)$ is the phase of the transmission coefficient. In the rest of this subsection, we will derive the above equation and analyze its saddle point solutions. First note that from the

action in Eqn. (4.49), the equations of motion for the fermionic fields ψ_n^1 and $\psi_n^{(2)}$ are

$$i\frac{\partial \psi_n^{(1)}}{\partial t} = -g\Delta_n \psi_n^{(2)} - \partial_n \psi_n^{(2)} \triangleq \left(-A\psi^{(2)}\right)_n, \tag{4.54}$$

$$i\frac{\partial \psi_n^{(2)}}{\partial t} = -g\Delta_n \psi_n^{(1)} - \partial_n^\dagger \psi_n^{(1)} \triangleq \left(-A^\dagger\psi^{(1)}\right)_n, \tag{4.55}$$

where A and $A^\dagger$ are matrices whose actions on the fields are encoded in the relations above. Note that there are a total of N pairs of equations of the above form, one for each flavor of fermion. If Δ_n is time-independent, taking a time derivative of Eqn. (4.54) and (4.55) gives the equations of motion $\ddot{\psi}^{(1)} = -AA^\dagger\psi^{(1)}$ and $\ddot{\psi}^{(2)} = -A^\dagger A\psi^{(1)}$. These equations of motion have a supersymmetric structure, which will be further used to construct soliton solutions in the next section. We may map these equations onto a discrete time-independent Schrödinger equation of the form

$$-(t_{n+1}^{(i)}\psi_{n+1}^{(i)} + t_n^{(i)}\psi_{n-1}^{(i)}) + u_n^{(i)}\psi_n^{(i)} = \omega^2\psi_n^{(i)}, \tag{4.56}$$

where $i = 1,2$ indicates the index of fermions. Due to the supersymmetric structure, the hoppings have the form

$$t_n^{(1)} = g\tau_n\Delta_{n-1}, \quad t_n^{(2)} = g\tau_n\Delta_n, \tag{4.57}$$

and the onsite potentials have the form

$$u_n^{(1)} = \tau_n^2 + g^2\Delta_n^2, \quad u_n^{(2)} = \tau_{n+1}^2 + g^2\Delta_n^2. \tag{4.58}$$

From now on we will perform the calculation for $i = 1$ and drop the superscript (i) in Eqn. (4.56). This is because the associated scattering problems for $i = 1$ and $i = 2$ have nearly identical scattering data and it does not matter which data we choose to write the action in terms of.

For the discrete Gross-Neveu model we will need only the first identity with $p = 1$:

$$\sum_{n=-\infty}^{\infty} u_n = -\frac{1}{2\pi}\int_0^{2\pi} \log\left[1 - |r(e^{i\phi})|^2\right] \cos(\phi)\, d\phi + \sum_{j=1}^{M}\left(z_j - \frac{1}{z_j}\right). \tag{4.59}$$

For the Gross-Neveu model with the potential $u_n = \tau_n^2 + g^2\Delta_n^2$, we find that $\sum_{n=-\infty}^{\infty} u_n = g^2\sum_{n=-\infty}^{\infty}\Delta_n^2 + \Upsilon$, where $\Upsilon = \sum_n \tau_n^2$ is a fixed constant that we will henceforth ignore (more precisely, it can be compensated by an appropriate renormalization of the vacuum energy in the original field theory). Thus, we can write the first term of the effective action S_1 given by Eqn. (4.50) as a function of the scattering data:

$$S_1 = -\frac{T}{2}\sum_n \Delta_n^2 = -\frac{T}{2g^2}\left[-\frac{1}{2\pi}\int_0^{2\pi} \log\left[1 - |r(e^{i\phi})|^2\right] \cos(\phi)\, d\phi + \sum_{j=1}^{M}\left(z_j - \frac{1}{z_j}\right)\right]. \tag{4.60}$$

Now we will express the remaining part of the action as a function of the scattering data. We first need to evaluate the following path integral which is quadratic in the fermions:

$$\mathscr{I}_N(\Delta) = \int \mathscr{D}\Psi\mathscr{D}\Psi^\dagger \exp\left[-S_2(\Psi,\Delta)\right], \tag{4.61}$$

where again, N is the number of flavors of fermions and S_2 is given by Eqn. (4.52). The fermionic fields $\psi^{(1,2)}$ satisfy the anti-periodic boundary conditions in time: $\psi^{(1,2)}(t+T) = -\psi^{(1,2)}(t)$. Following Dashen *et al.* [110], the path integral can be written down as

$$\mathscr{I}_N(\Delta) = [\mathscr{I}_1(\Delta)]^N = \mathscr{I}_1(0)\prod_{m,k}\frac{\varepsilon_{m,k}(\Delta)}{\varepsilon_{m,k}(0)}, \tag{4.62}$$

where $\varepsilon_{m,k}$ are the eigenvalues of the following matrix relation:

$$\begin{pmatrix} i\frac{\partial}{\partial t} & \partial_n + g\Delta_n \\ \partial_n^\dagger + g\Delta_n & i\frac{\partial}{\partial t} \end{pmatrix}\begin{pmatrix} \xi_{m,k}^{(1)} \\ \xi_{m,k}^{(2)} \end{pmatrix} = \varepsilon_{m,k}\begin{pmatrix} \xi_{m,k}^{(1)} \\ \xi_{m,k}^{(2)} \end{pmatrix}. \tag{4.63}$$

and $\mathscr{I}_1(0) = \prod_{m,k} \varepsilon_{m,k}(0)$ is independent of the onsite potential and hopping. Suppose $\phi_k^{(1,2)}$ satisfies Eqn. (4.63) where the right hand side is 0. For a time-independent Δ_n, we may choose $\phi_k^{(1,2)}$ such that it satisfies $\phi_k^{(1,2)}(t+T) = e^{-i\alpha_k(\Delta)}\phi_k^{(1,2)}(t)$ where $\alpha_k(\Delta) = \omega_k(\Delta)T$ and ω_k^2 is the energy. In general, for $\Delta_n(t)$ time periodic with period T, α_k label the Floquet indices; however, when Δ_n is time independent, the Floquet indices coincide with the energy. One can show that the function $\xi_{m,k}^{(1,2)}(t) = \exp\left(i(2m+1)\pi t/T + i\alpha_k t/T\right)\phi_k^{1,2}(t)$ satisfies the anti-periodic boundary condition and is an eigenfunction of Eqn. (4.63) with eigenvalue:

$$\varepsilon_{m,k} = -\frac{(2m+1)\pi}{T} - \frac{\alpha_k}{T} \tag{4.64}$$

We substitute Eqn. (4.64) into Eqn. (4.62) and simplify it using the standard infinite product identity for cosine to get:

$$\mathscr{I}_1(\Delta) = \mathscr{I}_1(0)\prod_k (e^{i\alpha_k/2} + e^{-i\alpha_k/2}) \tag{4.65}$$

$$= \mathscr{I}_1(0)\exp\left(i\sum_k |\alpha_k|\right)\prod_{\alpha_k>0}(1+e^{-i\alpha_k})^2 \tag{4.66}$$

$$= \mathscr{I}_1(0)\exp\left(i\sum_k |\alpha_k|\right)\sum_{\{n_i\}} e^{-i\sum_{\alpha_i>0} n_i\alpha_i}\prod_i q_{n_i} \tag{4.67}$$

where $0 \le n_i \le 2N$ is the population of the ith energy mode, $q_{n_i} = \frac{2N!}{n_i!(2N-n_i)!}$, and in the second line we have used the fact that the energies come in pairs with opposite sign to restrict the summation to positive energy modes. In general, we may assume that the set of Floquet indices are comprised of a set of isolated, discrete states and a continuum of scattering states. The N fermions and N anti-fermions may occupy these states, and we will assume that the saddle point corresponds to n_0 fermions occupying a single discrete state α_0. Thus, we may replace the summation over n_i with a constant n_0 and write the

action as:

$$S_{\text{eff}} = S_1 + N\sum_k |\alpha_k| - n_0\alpha_0 + \text{const.} \tag{4.68}$$

We have already written the second term S_1 as a function of the scattering data. Now we want to do the same for the first term $\sum_k |\alpha_k|$. We have noticed that for time-independent potentials $\alpha_k = \omega_k T$ where $\omega_k^2 = u - 2\cos k$ is the energy as a function of quasi-momentum. In Appendix **??** we show that for a system with N sites the quasi-momentum k is quantized as $k_n^{\pm} = \frac{2\pi n - \lambda^{\pm}}{N}$ where $\lambda^{\pm}$ are the eigenvalues of the scattering matrix. Then, one may show, as derived in the appendix:

$$\sum_k |\alpha_k| = 2T\int_0^{2\pi} \frac{d\phi}{2\pi} \frac{\sin(\phi)}{\sqrt{u-2\cos\phi}} \delta_t(\phi) + \omega_0 T + \Lambda, \tag{4.69}$$

where $\delta_t(\phi)$ is the phase of the transmission coefficient and Λ is a divergent constant and can be tamed by a suitable vacuum energy shift. We have also accounted for the presence of the single bound state $\alpha_0 = \omega_0 T$. The transmission coefficient is the inverse of $a(z)$, and so the phase of the the transmission coefficient is the imaginary part of $\log a^{-1}(z)$. Using the Jensen formula like before, we can write an equation for $\log a(z)$ similar to Eqn. (4.37):

$$\delta_t(\theta) = -\sum_{j=1}^{N} \Im\left(\log\frac{z-z_j}{1-z_j z}\right) + \frac{1}{4\pi}\int_0^{2\pi} \Im\left(\frac{e^{i\phi}+z}{e^{i\phi}-z}\right) \log\left[1-|r(\phi)|^2\right] d\phi, \tag{4.70}$$

where $z = e^{i\theta}$ and z_i are the zeros of $a(z)$. Note that $\Im(z)$ denotes the imaginary part of z. Combining all the results together we get an equation for effective action as a function of

the scattering data:

$$\frac{S_{\text{eff}}}{T} = \frac{1}{4\pi g^2}\int_0^{2\pi} \log\left(1-|r(e^{i\phi})|^2\right)\cos(\phi)d\phi - \frac{1}{2g^2}\sum_{j=1}^{N}\left(z_j - \frac{1}{z_j}\right) + 2N\int_0^{2\pi}\frac{d\phi}{2\pi}\frac{\sin(\phi)}{\sqrt{u-2\cos\phi}}\delta_t(\phi) + (N-n_0)\omega_0. \quad (4.71)$$

Upon varying the action with respect to scattering data, we obtain the saddle point solutions for the HS parameter, which correspond to solitonic textures. Setting $\delta S_{\text{eff}}/\delta r = 0$ gives the solution $r(\phi) = 0$, which implies that the effective onsite potential $u_n = \tau_n^2 + g^2\Delta_n^2$ must admit reflectionless scattering solutions. However there is an additional subtlety in the discrete case that does not appear in the continuous case. We note that in Eqn. (4.71) there is a $\cos\phi$ multiplying $\log\left(1-|r(e^{i\phi})|^2\right)$ in the integrand which was absent in the continuous case. Consequently, one can construct a potential which, in principle, has a smaller contribution to the action than a reflectionless potential. However, there are no physical potentials that we are aware of that have such scattering properties, so we deem that such kinds of potentials are likely unphysical.

One obvious example of a reflectionless potential is a constant; however, it is well known that there are many nontrivial candidates which are also reflectionless and give rise to kink solitons. To construct such nontrivial solutions, we will utilize a version of supersymmetric quantum mechanics for tight binding models, which will be discussed in the next section. We will show that we can construct a hierarchy of reflectionless soliton solutions by iterating the supersymmetric transformation starting from a constant onsite potential.

Furthermore, we must also vary the action with respect to the bound state energy; this results in the mass/energy spectrum for semiclassical bound states in the Gross-Neveu/lattice superconductor model. There are two separate cases that we must consider, both of which

give rise to physically distinct soliton solutions.

- In the first case, we assume that the HS parameter and the hopping converge to the constant values Δ_∞ and τ_∞ at both $\pm\infty$; the value of the potential and hopping is related to these asymptotic values via $u = g^2\Delta_\infty^2 + \tau_\infty^2$ and $t = g\Delta_\infty\tau_\infty$, the latter of which has been set to one. For simplicity, we follow same assumption as in Dashen *et al.* [110] that there is a single, isolated bound state occupied by n_0 fermions (the general case in which we allow for multiple bound states is a straightforward extension of the analysis presented). We calculate the energy of that bound state at the saddle point, which is given by setting $\delta S_{\text{eff}}/\delta z_1 = 0$ with the reflection coefficient $r(\phi) = 0$. From Eqn. (4.71) we get

$$\frac{1}{T}\frac{\delta S_{\text{eff}}}{\delta z_1} = -\frac{1}{2g^2}\left(1+\frac{1}{z_1^2}\right) - 4N\int_0^{2\pi}\frac{d\phi}{2\pi}\frac{\sin^2\phi}{\sqrt{u-2\cos\phi}}\frac{1}{1+z_1^2-2z_1\cos\phi} + (N-n_0)\frac{1-z_1^2}{2z_1^2\sqrt{u-(z_1+1/z_1)}}. \quad (4.72)$$

We may perform a convenient change of variables $2\cosh\vartheta = 1/z_1 + z_1$ and $2\sinh\vartheta = 1/z_1 - z_1$. Then, the condition $\delta S_{\text{eff}}/\delta z_1 = 0$ becomes

$$-\frac{1}{g^2}\cosh\vartheta - 2N\int_0^{2\pi}\frac{d\phi}{2\pi}\frac{\sin^2\phi}{\sqrt{u-2\cos\phi}}\frac{1}{\cosh\vartheta-\cos\phi} + (N-n_0)\frac{\sinh\vartheta}{\sqrt{u-2\cosh\vartheta}} = 0. \quad (4.73)$$

The integral has a closed form in terms of elliptic functions, but the subsequent implicit equation for $\cosh\vartheta$ is difficult to analyze analytically. We have evaluated the integral numerically and found that for a wide range of parameters there is only one solution where $\cosh\vartheta > 1$. To make progress analytically, we proceed by assuming that $\cosh\vartheta \gg 1$, which physically assumes that the bound state is strongly bound;

then, the equation above can be simplified to

$$-\frac{1}{g^2}\cosh\vartheta - \frac{N}{\cosh\vartheta}I(u) + (N-n_0)\frac{\sinh\vartheta}{\sqrt{u-2\cosh\vartheta}} = 0, \tag{4.74}$$

where

$$I(u) = 2\int_0^{2\pi}\frac{d\phi}{2\pi}\frac{\sin^2\phi}{\sqrt{u-2\cos\phi}}. \tag{4.75}$$

This may be reduced to a fifth order polynomial equation in $\cosh\vartheta$ which is still not analytically tractable. In the limit where $u \gg 2\cosh\vartheta$ and $\sqrt{u} \ll g^2N$, we may neglect the first term and utilize the simplification $I(u) = 1/\sqrt{u}$. Then, we obtain that $\sinh 2\vartheta \approx \frac{2N}{(N-n_0)}$, which is an approximately valid solution for moderate values of the filling n_0/N. We plot both the approximation and exact values of θ in Figure 4.2, and it is clear that the approximation holds even beyond the regime of validity described.

The corresponding reflectionless potentials with these bound state energies are non-topological solitons which are kink-antikink solitons. These solitons are strongly dependent on the number of trapped fermions; intuitively, this is because repulsion due to the n_0 fermions trapped in the kink and antikink will cause them to separate; the calculation above self consistently determines the stable value for the separation distance, which is also related to the bound state energy.

- In the second case, we assume that the HS parameter and the hopping converge to different values $\Delta_{\pm\infty}$ and $\tau_{\pm\infty}$ at $\pm\infty$; we find that these solitons are topological, and are associated with the Callan-Coleman-Gross-Zee (CCGZ) kink solitons first discovered famously in the φ^4-field theory. If we assume that n_0 of the fermions are trapped in a single bound state, we arrive at a slightly different result assuming kink boundary conditions. First, we note that the scattering problems for both components

of the fermion differ by a bound state. This can be seen by computing

$$\sum_n (u_n^{(2)} - u_n^{(1)}) = \sum_n (\tau_{n+1}^2 - \tau_n^2) = \tau_\infty^2 - \tau_{-\infty}^2, \tag{4.76}$$

and therefore the right hand side of the trace identity in Eqn. (4.59) will differ between the two scattering problems. We will show in the next section that the reflection coefficient of the scattering problems are the same, and so the two scattering problems must differ in the number of bound states. For there to be a single bound state, the scattering problem for the first component of the fermion must have no bound states and must be reflectionless. The action reduces drastically to $S_{\text{eff}} = (N - n_0)\omega_0$, which is minimized for $\omega_0 = 0$ regardless of the value of n_0. The intuition for this is rather simple. The theory possesses a topological zero-mode, the Jackiw-Rebbi mode, which is insensitive to the number of occupied fermions; therefore, the nature of this kink soliton should not depend on the filling.

We also know that the bound state energies are given by the explicit formula

$$\omega_0 = \sqrt{u - z_1 - \frac{1}{z_1}}. \tag{4.77}$$

Using the formulae $u = g^2\Delta_\infty^2 + \tau_\infty^2 = g^2\Delta_{-\infty}^2 + \tau_{-\infty}^2$ and $t = 1 = g\Delta_\infty\tau_\infty = g\Delta_{-\infty}\tau_{-\infty}$, we find that $z_1 = \tau_\infty^2$. Substitution into ω_0 also gives $\omega_0 = 0$, consistent with the saddle point solution obtained directly from minimizing the action.

4.3.3 Construction of field theory hierarchy

The lattice Gross-Neveu model presented in the previous section can be considered to be the first such model in a hierarchy of field theories that admit soliton solutions. First note that we rather naturally divided the action for the lattice GN model into two pieces

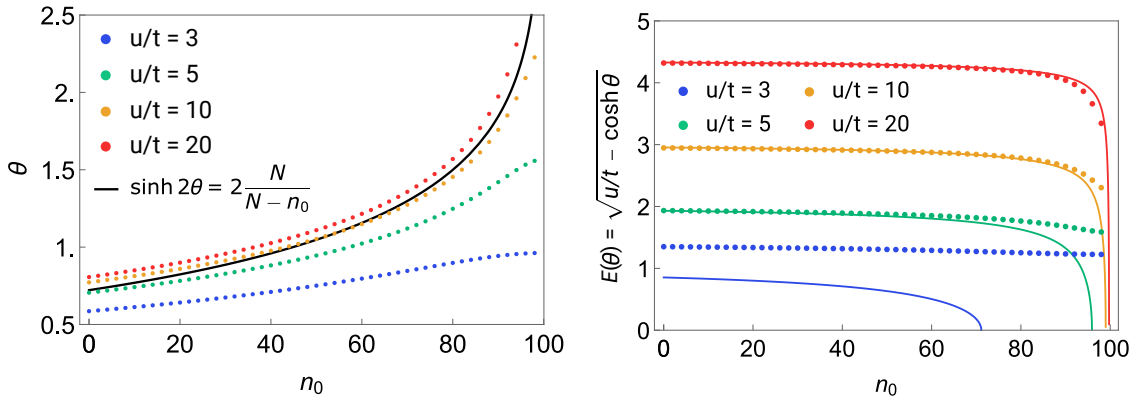


Figure 4.2: In the left panel, a plot of the values of ϑ as a function of the filling n_0. Here, $g = 1$ and we have chosen $N = 100$ and varied u. Also plotted in black is the approximation $\sinh 2\vartheta \approx \frac{2N}{(N-n_0)}$, which is a valid in a regime where u is large compared to $\cosh\theta$ but small compared to N^2. We even see good accuracy of the approximation beyond the regime of validity. In the right panel, a plot of the bound state energy as a function of the filling n_0. The solid lines are the corresponding bound state energies obtained from the approximation.

given by Eqns. (4.51) and (4.52). The first part of the action was rewritten using the first trace identity, while no trace identities were required for the second part of the action. To generalize, we write the first part of the action as a trace identity of our choice; the form of such an action is

$$S = -\sum_n \int_0^T dt\, F(\Delta_n(t), \tau_n) + \sum_n \int_0^T dt\, \Psi_n^\dagger \begin{pmatrix} i\frac{\partial}{\partial t} & \partial_n + g\Delta_n(t) \\ \partial_n^\dagger + g\Delta_n(t) & i\frac{\partial}{\partial t} \end{pmatrix} \Psi_n, \qquad (4.78)$$

where $F(\Delta_n, \tau_n)$ is constructed from the trace identities, and can be written as a linear combination of traces of powers of the Hamiltonian. If we utilize the first trace identity and the potential given by Eqn. (4.58) to write $F(\Delta_n, \tau_n) = u_n = g^2\Delta_n^2$ then we get back the lattice GN model. In general if we use any trace identity, the action will have a saddle point corresponding to a reflectionless potential because the trace identities have a $\log(1-|r|^2)$ dependence on the reflection coefficient r; thus a solution to $\delta S_{\text{eff}}/\delta r = 0$ will always be $r = 0$. To exemplify this process, we will construct an action using the second trace identity.

In this case we choose $F(\Delta_n, \tau_n)$ to be

$$F(\Delta_n, \tau_n) = u_n^2 + 2t_n^2 = \tau_n^4 + g^4\Delta_n^4 + 2g^2\Delta_n^2\left(\tau_n^2 + \tau_{n+1}^2\right), \tag{4.79}$$

where we have used Eqn. (4.58) and (4.57) to write down the form of the onsite potential and hopping. Substituting Eqn. (4.79) into the action we get a new field theory with a background field τ and the Hubbard-Stratonovich field Δ. First we assume that the HS field is time-independent as before. Then, we may integrate out the HS field to construct a local theory in the fermions. Upon performing the integration, the action becomes

$$S = \sum_n \int_0^T dt\, \Psi_n^\dagger(t) \begin{pmatrix} i\frac{\partial}{\partial t} & \partial_n \\ \partial_n^\dagger & i\frac{\partial}{\partial t} \end{pmatrix} \Psi_n(t) + \log(Z), \tag{4.80}$$

where Z is obtained by taking the path integral of the remaining part of the action with respect to the HS field:

$$Z = \prod_n \int_{-\infty}^{\infty} d\Delta_n \exp\left[\Psi_n^\dagger \begin{pmatrix} 0 & g\Delta_n \\ g\Delta_n & 0 \end{pmatrix} \Psi_n - g^4\Delta_n^4 - 2g^2\Delta_n^2\left(\tau_n^2 + \tau_{n+1}^2\right)\right], \tag{4.81}$$

where we have ignored the constant term coming from τ_n^4. The functional Z can be further simplified to the following form

$$Z \propto \exp\left(\sum_n \frac{\zeta\left(\tau_n^2 + \tau_{n+1}^2\right)}{2g^2}\left(\overline{\Psi}_n\Psi_n\right)^2\right). \tag{4.82}$$

Therefore, the full action is a Gross-Neveu model where the interaction has site-dependence and can be treated as a background field. The function ζ is given by

$$\zeta\left(\tau_n^2+\tau_{n+1}^2\right)=\frac{\int_{-\infty}^{\infty}dx\,x^2e^{-x^4-\left(\tau_n^2+\tau_{n+1}^2\right)x^2}}{\int_{-\infty}^{\infty}dx\,e^{-x^4-\left(\tau_n^2+\tau_{n+1}^2\right)x^2}}, \tag{4.83}$$

which may be expressible in terms of special functions. In principle, one can treat τ as a scalar field in the path integral formulation; in this case, the full theory is obtained by integrating over τ_n. Unfortunately, since the dependence of the effective interaction on the τ_n's does not decouple, the resulting theory will look quite non-local. This is analogous to what happens in the continuum limit, except there the non-locality of the theory arises when integrating out the HS parameter.

If one continues to construct more such field theories using higher order trace identities, the corresponding actions will take the generic form

$$S=\int_0^T dt\,\left[\sum_n\Psi_n^\dagger(t)\begin{pmatrix}i\frac{\partial}{\partial t} & \partial_n\\ \partial_n^\dagger & i\frac{\partial}{\partial t}\end{pmatrix}\Psi_n(t)+\zeta_k\left(\tau_n,\tau_{n+1},\cdots,\tau_{n+k-1}\right)\left(\overline{\Psi}_n(t)\Psi_n(t)\right)^2\right], \tag{4.84}$$

where k indexes the action constructed using the kth trace identity. It is a rather elegant feature that nontrivial field theories with soliton solutions may be reverse engineered from a series of trace identities; however, for each of these models the mass spectrum (or equivalently the bound state/soliton spectrum) will vary depending on which trace identity is used. Such a calculation is a simple modification of the procedure developed in the previous subsection.

4.4 Exact construction of saddle point solutions

In the previous sections, we justified that a saddle point of the action for the lattice Gross-Neveu model corresponds to reflectionless potentials with a particular spectrum of bound states. To obtain the original potential corresponding to a particular set of scattering data, the inverse scattering method is applied, which involves solving the Gelfand-Levitan equation. Since this formulation can be rather bulky, in this section we introduce an alternate formalism based on a generalization of supersymmetric quantum mechanics to tight binding models, and use this method to construct the kink soliton and kink-antikink solutions described in the previous section, without resorting to using the Gelfand-Levitan equation.

4.4.1 Continuous supersymmetry

Here, we briefly review the well-established field of supersymmetric (SUSY) quantum mechanics [137]. We start with the Schrödinger operator factorized as $\mathscr{H} = -\partial_x^2 + V(x) = A^\dagger A$, where $A^\dagger = -\partial_x + W(x)$ and $A = \partial_x + W(x)$. By convention, $W(x)$ is known as the superpotential, and is related to the original potential via the Riccati equation $W^2(x) - W'(x) = V(x)$. We then construct a new Hamiltonian $\widetilde{\mathscr{H}} = AA^\dagger$, which is also a valid Schrödinger operator with a new potential $\widetilde{V}(x) = W^2(x) + W'(x)$. The Hamiltonian $\widetilde{\mathscr{H}}$ has the same spectrum as the Hamiltonian $\mathscr{H}$, apart from the removal of a zero energy eigenstate, if any, which solves $A\psi = 0$. Furthermore, if $\psi(x)$ is an eigenstate of $\mathscr{H}$ with energy E, then $A\psi(x)$ is an eigenstate of $\widetilde{\mathscr{H}}$ with the same energy.

The canonical example of continuous soliton solutions can be obtain by repeated application of the SUSY method to a constant potential. In particular, if we consider the

Schrödinger equation

$$\left(-\frac{\partial^2}{\partial x^2} - N(N+1)\,\mathrm{sech}^2 x\right)\psi(x) = E\,\psi(x), \tag{4.85}$$

we may find that the system at N can be related to the system at $N+1$ via a supersymmetry transformation with $A = -\partial_x - N\tanh x$; the case $N = 0$ corresponds to a constant potential. One can show that the number of bound states exactly equals N and that their energies are given by $E_n = -(n-N)^2$. The scattering states where $E > 0$ are reflectionless. This is an example of an N-soliton solution with the property that the number of solitons coincides with the number of bound states.

4.4.2 Discrete supersymmetry: formalism

We would like to extend the formalism of continuous supersymmetry to tight binding models. The simplest structure of a Hamiltonian which is amenable to supersymmetry is a tridiagonal matrix, equivalent to the one from Eqn. (4.27), with t_n the hopping amplitudes and u_n the onsite potentials. We factor $\mathscr{H} = A^\dagger A$, and select an ansatz for A to be

$$A^\dagger = \sum_{n=-\infty}^{\infty} \tau_{n+1}|n\rangle\langle n+1| + \Delta_n|n\rangle\langle n|, \tag{4.86}$$

which is a discrete version of $A^\dagger = -\partial_x + W(x)$; we will call τ the superhopping and Δ the superpotential. Note that the matching notation with the previous section is no coincidence: indeed, the matrix $A^\dagger$ is equal to $\partial_n^\dagger + \Delta_n$ (we will set $g = 1$ for convenience). The equations of motion of the Gross-Neveu model decouple into independent equations of motion for the effective Hamiltonians $\mathscr{H} = A^\dagger A$ and $\widetilde{\mathscr{H}} = AA^\dagger$, both of which are tridiagonal and have nearly identical spectra because they are superpartners. Crucially, knowing $\mathscr{H}$, one may extract the superhopping and superpotential and use it to compute $\widetilde{\mathscr{H}}$.

We can iterate this process to create a family of nearly isospectral Hamiltonians, which gives us a hierarchy of saddle point solutions to the Gross-Neveu model. For example, at the kth iteration, we construct the Hamiltonian $\mathscr{H}_k = A_k A_k^\dagger$ and solve the matching condition $A_k A_k^\dagger = A_{k+1}^\dagger A_{k+1}$ to obtain a new set of superpotentials and superhoppings. The Hamiltonian at the $(k+1)$st iteration can then be constructed via $\mathscr{H}_{k+1} = A_{k+1} A_{k+1}^\dagger$. In this hierarchy, any pair of consecutive Hamiltonians can be considered to be a valid saddle point solution for the Gross-Neveu model. The matching condition can be obtained from Eqns. (4.57) and (4.58):

$$\tau_n^{(k-1)} \Delta_{n-1}^{(k-1)} = \tau_n^{(k)} \Delta_n^{(k)}, \tag{4.87}$$

$$\tau_n^{(k-1)^2} + \Delta_n^{(k-1)^2} = \tau_{n+1}^{(k)\ 2} + \Delta_n^{(k)^2}. \tag{4.88}$$

Note that the subscripts denote the location on the lattice while the superscripts indicate the level of the hierarchy. The Hamiltonians $\mathscr{H}_k$ and $\mathscr{H}_{k+1}$ have the same spectrum and differ by a possible zero-energy state that appears only in the limit of an infinitely long chain with open boundary conditions; this zero-energy state is analogous to the one in continuous supersymmetry. Using this method, one can create a Hamiltonian with arbitrarily placed energy levels for the bound states: one only needs to introduce the constant shift $\mathscr{H}_k \to \mathscr{H}_k + \delta_k$ after each iteration. The corresponding bound state energy levels after the kth iteration will be $E_m = \sum_{i=1}^m \delta_i$ for $m \leq k$. As a result, this iterative method can be used to obtain saddle point solutions given a sequence of bound state energies; we need only prove that the corresponding potentials are reflectionless. To see this, first note the eigenstates of the Hamiltonian after k levels are given by

$$|\psi\rangle_k \propto A_k A_{k-1} \ldots A_1 |\psi\rangle_1, \tag{4.89}$$

so that due to the local properties of the matrix A, bound states remain bound and scattering states remain scattering. Next, we consider a scattering process that occurs in the base Hamiltonian $\mathscr{H}_1$; assuming the potential and hopping are asymptotically constants u and t and the incident scattering particles come from the left, we may write the wavefunction using $z = e^{ik}$ as

$$\psi_n(z) = \begin{cases} z^n + r(z)z^{-n}, & \text{for } n \to -\infty \\ t(z)z^n, & \text{for } n \to \infty \end{cases} \tag{4.90}$$

where $t(z)$ and $r(z)$ are the transmission and reflection coefficients. Upon supersymmetry, the new scattering eigenstates in $\mathscr{H}_2$ are $\overline{\psi}_n(z) = \Delta_n \psi_n(z) + \tau_{n+1}\psi_{n+1}(z)$, which can be written as

$$\overline{\psi}_n(z) = \begin{cases} z^n + r(z)\frac{z\Delta_- + \tau_-}{z(\Delta_- + \tau_- z)}z^{-n}, & \text{for } n \to -\infty \\ t(z)\frac{\Delta_+ + \tau_+ z}{\Delta_- + \tau_- z}z^n, & \text{for } n \to \infty \end{cases} \tag{4.91}$$

where the subscripts $+$ and $-$ denote the asymptotic values of the superpotential and superhopping at positive and negative infinity respectively. which allows us to identify the modified reflection and transmission coefficients $\bar{r}(z)$ and $\bar{t}(z)$. In particular, we find that

$$|\bar{r}|^2 = \frac{|r|^2}{|z|^2}\frac{(\tau_- + \Delta_-\cos\phi)^2 + \Delta_-^2\sin^2\phi}{(\Delta_- + \tau_-\cos\phi)^2 + \tau_-^2\sin^2\phi} = |r|^2, \tag{4.92}$$

and

$$|\bar{t}|^2 = |t|^2\frac{(\Delta_+ + \tau_+\cos\phi)^2 + \tau_+^2\sin^2\phi}{(\Delta_- + \tau_-\cos\phi)^2 + \tau_-^2\sin^2\phi} = |t|^2\frac{{\Delta_+}^2 + {\tau_+}^2 + 2\Delta_+\tau_+\cos\phi}{{\Delta_-}^2 + {\tau_-}^2 + 2\Delta_-\tau_-\cos\phi} = |t|^2, \tag{4.93}$$

where we have used the supersymmetry relations ${\Delta_\pm}^2 + {\tau_\pm}^2 = u$ and $\Delta_\pm\tau_\pm = t$. Thus, the superpartner Hamiltonian preserves the magnitude of the reflection and transmission coefficients, and induction proves that this holds for all subsequent Hamiltonians in the

hierarchy. We also note that the poles of $\bar{t}$ are the poles of t along with an additional pole at $z_* = -\Delta_-/\tau_-$. This additional pole corresponds to a normalizable bound state at zero energy if z_* lies within the unit disk, or if $|\Delta_-/\tau_-| < 1$.

4.4.3 Construction of kink solitons

In continuous supersymmetry, a soliton hierarchy is achieved by starting with a reflectionless constant potential and iterating the supersymmetry procedure. In analogy to the continuous case, let us assume a tight binding Hamiltonian given by

$$\mathscr{H} = \sum_{n=-\infty}^{\infty} \left(-t|n\rangle\langle n+1| + \text{h.c.} + u|n\rangle\langle n|\right). \tag{4.94}$$

We iterate the supersymmetric process once. For this, we will need to solve the equations $t = \tau_i\Delta_{i-1}$ and $u = \tau_i^2 + \Delta_i^2$. We need to first determine the asymptotic behavior for the superhopping and the superpotential, which implies solving $\tau^2 + \Delta^2 = u$ and $\tau\Delta = t$. This yields two solutions

$$\Delta_\pm^2 = \frac{u}{2}\left(1 \pm \sqrt{1 - \frac{4t^2}{u^2}}\right), \tag{4.95}$$

and $\tau_\pm = t/\Delta_\pm$. Thus, our kink solution will transition from one of these solutions at $-\infty$ to the other solution at $+\infty$. To solve for the intermediate values, we choose the origin as a seed with $\Delta_0 = \Delta$, determine Δ_n for $n > 0$ and $n < 0$ separately, and self-consistently determine constraints on Δ for the existence of a solution. We may solve for the superpotential

and find that it takes the form of a continued fraction:

$$\Delta_N^2 = u - \cfrac{t^2}{u - \cfrac{t^2}{u - \cfrac{t^2}{u - \cfrac{t^2}{\ddots - \cfrac{t^2}{\Delta^2}}}}} \qquad \Delta_{-N}^2 = \cfrac{t^2}{u - \cfrac{t^2}{u - \cfrac{t^2}{u - \cfrac{t^2}{\ddots - \Delta^2}}}} \tag{4.96}$$

where the number of repetitions in continued fraction is N. We use a well-known result for the finite continuants of a continued fraction. Given a continued fraction of the form

$$F(\eta,\gamma) = \eta_0 + \cfrac{\gamma_1}{\eta_1 + \cfrac{\gamma_2}{\eta_2 + \cfrac{\gamma_3}{\eta_3 + \cdots}}}, \tag{4.97}$$

the finite continuants can be expressed in the form $F_N(\eta,\gamma) = p_N/q_N$, where p_n satisfies the recurrence

$$p_n = \eta_n p_{n-1} + \gamma_n p_{n-2} \tag{4.98}$$

with $p_0 = \eta_0$ and $p_{-1} = 1$, and q_n satisfies the same recurrence with $q_0 = 1$ and $q_{-1} = 0$. In the present case, focusing on the equation for W_N, we find that $\eta_N = \Delta^2$ and $\gamma_N = -t^2$ as well as $\eta_i = u$ and $\gamma_i = -t^2$ for $i < N$. We then find the following solution for the recurrence for p:

$$\begin{pmatrix} p_N \\ p_{N-1} \end{pmatrix} = \begin{pmatrix} \Delta^2 & -t^2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u & -t^2 \\ 1 & 0 \end{pmatrix}^{N-1} \begin{pmatrix} u \\ 1 \end{pmatrix}, \tag{4.99}$$

and similarly for q:

$$\begin{pmatrix} q_N \\ q_{N-1} \end{pmatrix} = \begin{pmatrix} \Delta^2 & -t^2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u & -t^2 \\ 1 & 0 \end{pmatrix}^{N-1} \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{4.100}$$

For Δ_{-N}, we find a similar series of expressions, but it can be shown that they are equivalent to an analytic continuation of the above expressions to negative N. Combining both branches, we find the following solution for Δ_N^2:

$$\Delta_N^2 = \frac{\Delta_-^{2N+2}(\Delta_+^2 - \Delta^2) + \Delta_+^{2N+2}(\Delta^2 - \Delta_-^2)}{\Delta_-^{2N}(\Delta_+^2 - \Delta^2) + \Delta_+^{2N}(\Delta^2 - \Delta_-^2)}. \tag{4.101}$$

Notice that $\lim_{N\to\infty} \Delta_N^2 = \Delta_+^2$ and $\lim_{N\to-\infty} \Delta_N^2 = \Delta_-^2$ as well as $\Delta_0^2 = \Delta^2$. Thus, this superpotential behaves like a discretized version of hyperbolic tangent, which is the superpotential in the continuous limit. However, we do want to enforce that the above equation does not become negative; an accordingly sufficient constraint on Δ^2 is that $\Delta_-^2 < \Delta^2 < \Delta_+^2$. The superhopping is correspondingly given by $\tau_N = t/\Delta_{N-1}$ and also behaves like a discrete hyperbolic tangent. Examples of these soliton profiles are plotted numerically in Figure 4.3. We may write expression for the new potential $\widetilde{u}_N = \tau_{N+1}^2 + \Delta_N^2$ and the new hopping $\widetilde{t}_N = \tau_N \Delta_N$ after one iteration of supersymmetry:

$$\widetilde{u}_N = t^2 \frac{\Delta_-^{2N}(\Delta_+^2 - \Delta^2) + \Delta_+^{2N}(\Delta^2 - \Delta_-^2)}{\Delta_-^{2N+2}(\Delta_+^2 - \Delta^2) + \Delta_+^{2N_2}(\Delta^2 - \Delta_-^2)} + \frac{\Delta_-^{2N+2}(\Delta_+^2 - \Delta^2) + \Delta_+^{2N+2}(\Delta^2 - \Delta_-^2)}{\Delta_-^{2N}(\Delta_+^2 - \Delta^2) + \Delta_+^{2N}(\Delta^2 - \Delta_-^2)}, \tag{4.102}$$

$$\widetilde{t}_N = t \frac{\left(\Delta_-^{2N}(\Delta_+^2 - \Delta^2) + \Delta_+^{2N}(\Delta^2 - \Delta_-^2)\right)^2}{\left(\Delta_-^{2N+2}(\Delta_+^2 - \Delta^2) + \Delta_+^{2N+2}(\Delta^2 - \Delta_-^2)\right)\left(\Delta_-^{2N-2}(\Delta_+^2 - \Delta^2) + \Delta_+^{2N-2}(\Delta^2 - \Delta_-^2)\right)}, \tag{4.103}$$

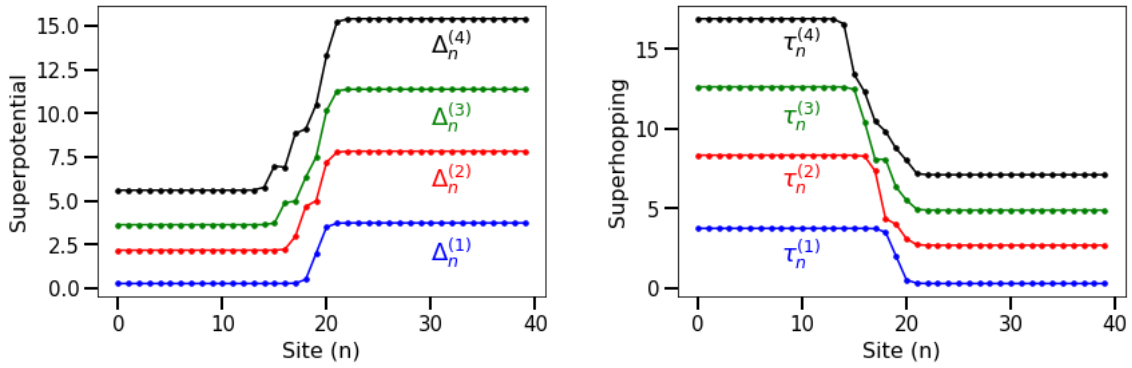


Figure 4.3: A plot of the superpotential and the superhopping obtained from iterating discrete supersymmetry for four iterations starting with a constant potential. A constant shift is applied between iterations, and the corresponding solutions share the same spectrum apart from the constant shift and an additional bound state. These solutions correspond to one such hierarchy of kink solitons.

both of which resemble a discretized version of hyperbolic secant. Furthermore, we may also formulate a condition for which a bound state will exist, given that $\tau_- = t/\Delta_-$. Setting $\Delta_-^2/t < 1$ gives

$$\frac{u}{2t}\left(1-\sqrt{1-\frac{4t^2}{u^2}}\right) < 1, \tag{4.104}$$

which always holds since we require $u > 2t$ (this can be seen because the left hand side is a decreasing function of $u/2t$ and equals 1 when $u = 2t$); this implies the existence of an additional bound state at zero energy. This is the discrete analogue of the Jackiw-Rebbi zero mode associated with the kink soliton solution.

Next, we may iterate this process to determine other reflectionless kink potentials with a given spectrum of bound states. One subtlety we must observe is that we cannot guarantee that the supersymmetry process can be iterated indefinitely; if the partial continued fraction expression for some Δ_N^2 is negative at a given iteration, then there does not exist a solution

to Eqns. (4.87) and (4.88). In the general case, we may write

$$\Delta^2_{-N} = \cfrac{t^2_{-N+1}}{u_{-N+1} - \cfrac{t^2_{-N+2}}{u_{-N+2} - \cfrac{t^2_{-N+3}}{\ddots - \cfrac{t_0^2}{\Delta^2}}}} \qquad \Delta^2_N = u_N - \cfrac{t^2_N}{u_{N-1} - \cfrac{t^2_{N-1}}{u_{N-2} - \cfrac{t^2_{N-2}}{\ddots - \Delta^2}}} \tag{4.105}$$

Alternatively, these continued fractions can be written in terms of the ratio of determinants of tridiagonal matrices:

$$\Delta^2_N = \frac{\det\begin{pmatrix} u_N & t_N & \dots & 0 & 0 \\ t_N & u_{N-1} & t_{N-1} & \dots & 0 \\ \vdots & t_{N-1} & \ddots & t_{-2} & \vdots \\ 0 & \vdots & t_{-2} & u_{-1} & t_{-1} \\ 0 & 0 & \dots & t_{-1} & u_0 - \Delta^2 \end{pmatrix}}{\det\begin{pmatrix} u_{N-1} & t_{N-1} & \dots & 0 & 0 \\ t_{N-1} & u_{N-2} & t_{N-2} & \dots & 0 \\ \vdots & t_{N-2} & \ddots & t_{-2} & \vdots \\ 0 & \vdots & t_{-2} & u_{-1} & t_{-1} \\ 0 & 0 & \dots & t_{-1} & u_0 - \Delta^2 \end{pmatrix}} \quad \frac{t^2_{-N+1}}{\Delta^2_{-N}} = \frac{\det\begin{pmatrix} u_{-N+1} & t_{-N+2} & \dots & 0 & 0 \\ t_{-N+2} & u_{-N+2} & t_{-N+3} & \dots & 0 \\ \vdots & t_{-N+3} & \ddots & t_{-1} & \vdots \\ 0 & \vdots & t_{-1} & u_{-1} & t_0 \\ 0 & 0 & \dots & t_0 & \Delta^2 \end{pmatrix}}{\det\begin{pmatrix} u_{-N+2} & t_{-N+3} & \dots & 0 & 0 \\ t_{-N+3} & u_{-N+3} & t_{-N+4} & \dots & 0 \\ \vdots & t_{-N+4} & \ddots & t_{-1} & \vdots \\ 0 & \vdots & t_{-1} & u_{-1} & t_0 \\ 0 & 0 & \dots & t_0 & \Delta^2 \end{pmatrix}} \tag{4.106}$$

The matrices in these equations resemble submatrices of the Hamiltonian (by submatrices we mean matrices formed by deleting some set of columns and corresponding rows in the Hamiltonian). Because the Hamiltonian is positive semi-definite and the zero-energy bound state has nonzero support at each site, all submatrices of the Hamiltonian are positive definite. Next, we note that adding a constant ε to each of the onsite potentials does not change the reflectionless property of the Hamiltonian and shifts the ground state energy to ε. Setting $u_N \to u_N + \varepsilon$, we find that a sufficient condition for both Δ^2_N and t^2_{-N+1}/Δ^2_{-N} to be

positive is $\varepsilon + \Delta^2 - u_0 > 0$ and $\varepsilon - \Delta^2 > 0$. This implies that $u_0 - \varepsilon < \Delta^2 < \varepsilon$. The resulting superpartner potential will have an additional bound state at zero energy, which does not coincide with the previous bound state now at energy ε. With an appropriate application of a shift at every iteration, we can generate a hierarchy of reflectionless potentials. Note that the bound on the shift ε that we derived is not tight, and in practice we find a much less restrictive bound.

4.4.4 Construction of kink-antikink solitons

Thus far we have described how to construct kink solutions, with asymptotically different boundary conditions at $\pm\infty$. These topological solitons correspond to a robust zero energy mode, which is present in one of the scattering problems and absent in the other. However, we argued that there should also be non-topological solitons – in the high-energy context, these correspond to fermion-antifermion bound states (and in the general case, multi-fermion bound states). In the previous section, we constructed the bound state spectrum of multi-fermion states as a function of the fermion/anti-fermion filling, but did not construct a satisfying solution for Δ_n and τ_n. Here, we discuss a method for constructing such solutions using discrete supersymmetry.

As described in the previous section, we seek a solution for Δ_n which converges to the same value at $\pm\infty$. Given an arbitrary onsite potential u_n and hopping t_n, we may evaluate the superpotential using the continued fraction method illustrated in Eqn. (4.105). Let us focus on the case where $n > 0$, for which Δ_n converges to Δ_+ as $n \to \infty$. We may first write the continued fraction as a ratio p_n/q_n, where, as discussed in the previous subsection, p_n can be determined via the following relation:

$$\begin{pmatrix} p_N \\ p_{N-1} \end{pmatrix} = \begin{pmatrix} \Delta^2 & -t_1^2 \\ 1 & 0 \end{pmatrix} \prod_{j=1}^{N} \begin{pmatrix} u_j & -t_{j+1}^2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \tag{4.107}$$

and q_N satisfies a similar relation but with $N \to N-1$. This transfer matrix method was used to obtain the exact solution for the kink soliton where both u_n and t_n were constant, but works equally well in the general case. For large N, the product is dominated by a product of the asymptotic form of the transfer matrix, assuming that $u_\infty = u$ and $t_\infty = t$. The eigenvalues of the asymptotic value of the transfer matrix are Δ_+ and $\Delta_- < \Delta_+$, so for generic values of the initial condition $\Delta_0 = \Delta$, $p_{N\to\infty} \sim \Delta_+^N$ while $q_{N\to\infty} \sim \Delta_+^{N-1}$ – this results in the asymptotic superpotential being Δ_+. A similar analysis shows that $\Delta_{-\infty} = \Delta_-$ and we recover a kink solution.

However, if Δ is chosen such that the eigenvector corresponding to eigenvalue Δ_+ is annihilated by the matrix product in Eqn. (4.107) (for N large), then the asymptotic superpotential will be Δ_-, and corresponding soliton solution will have the same boundary conditions at $\pm\infty$ – this corresponds to a non-topological soliton. The eigenvector of the transfer matrix corresponding to eigenvalue Δ_+ is $\lambda_+^T = (\Delta_+, 1)$, so the unique value of Δ that generates these solutions solves

$$\begin{pmatrix} \Delta_\star^2 & -t_1^2 \end{pmatrix} \prod_{j=1}^{\infty} \begin{pmatrix} u_j & -t_{j+1}^2 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \Delta_+ \\ 1 \end{pmatrix} = 0, \tag{4.108}$$

or equivalently using the notation $e_1^T = (1,0)$ and $e_2^T = (0,1)$,

$$\Delta_\star^2 = t_1^2 \frac{e_2^T Q \lambda_+}{e_1^T Q \lambda_+}, \qquad Q = \prod_{j=1}^{\infty} \begin{pmatrix} u_j & -t_{j+1}^2 \\ 1 & 0 \end{pmatrix}. \tag{4.109}$$

The corresponding non-topological solitons are unstable to perturbations in the initial condition $\Delta_\star$ and will revert to kink solitons. Now that a value for $\Delta_0 = \Delta_\star$ is specified, we must select an appropriate choice of u_n. Clearly, this choice of u_n must be reflectionless, but it also must have at least one bound state (a choice of u_n with no bound states such as

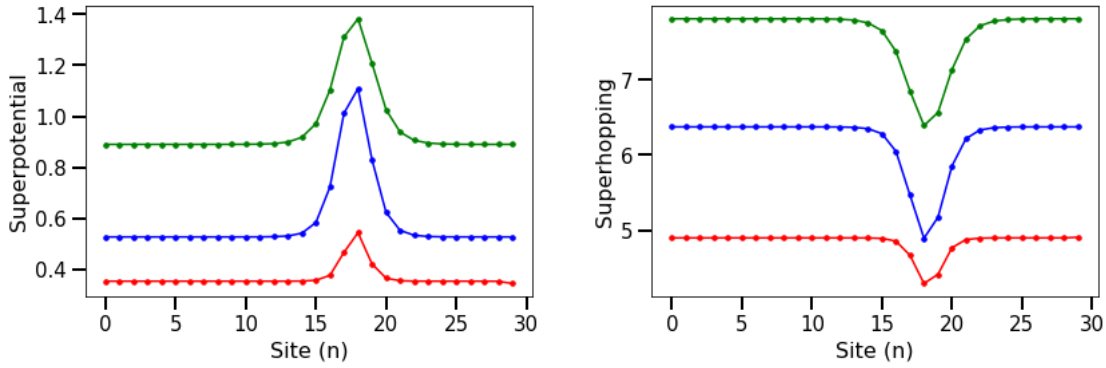


Figure 4.4: A plot of the superpotential and the superhopping obtained from the discrete hyperbolic secant potential given in Eqn. (4.102) for a variety of asymptotic values of t and u. The boundary condition $\Delta_0^2 = \Delta_\star^2$ was chosen, which results in non-topological soliton solutions shown. Note that the chain is cut off after 30 lattice sites due to the exponential numerical instability caused from small deviation from $\Delta_\star$.

$u_n = u$ will yield a trivial answer where Δ_n is constant everywhere). We have constructed an example of such a potential in the previous subsection (see Eqn. (4.102)), which is a discretized version of hyperbolic secant. The superpartner to this potential with the initial condition $\Delta^2 = \Delta_\star^2$ will not have additional bound state at zero energy as such a state is not normalizable; thus, the superpartner will have an identical spectrum. This describes the case where supersymmetry is broken, while supersymmetry was unbroken in the case of the kink soliton.

We verify that the choice of potential u_n and initial condition $\Delta_\star$ indeed generates non-topological solitons, as shown in Figure 4.4. As expected, these solitons can be viewed as a sum of a propagating kink and antikink topological soliton. Similar kinds of non-topological solitons can be constructed for potentials with more than a single bound state by an analogous procedure.

4.5 Chiral Gross-Neveu model and superconductivity

Thus far, we worked exclusively with the Gross-Neveu model, showing the correspondence between semiclassical saddle point solutions of the action and reflectionless potentials of the effective scattering problem. We were able to explicitly retrieve these reflectionless solutions using discrete supersymmetry. We analyzed both topological and non-topological soliton solutions, the former of which appears as a kink in the magnitude of the real scalar field Δ, and the latter of which occurs due to the merging of kink and antikink solutions. In superconductors, the order parameter is complex, and kink solitons can become dynamical. To reproduce this case, we consider a modification of the Gross-Neveu model, the chiral Gross-Neveu model (equivalently the Nambu-Jona-Lasinio model), which has an additional chiral term necessary for the order parameter to be complex. In this section, we perform a similar analysis of this model, and construct nontrivial soliton solutions in lattice superconductors, relevant for cold atom experimental platforms.

The chiral Gross-Neveu model, as first discussed by Shei [111], is a modification of the Gross-Neveu model that preserves chiral symmetry $\psi \to e^{i\theta\gamma_5}\psi$:

$$\mathscr{L} = \sum_{k=1}^{N} i\overline{\psi}^{(k)}\partial\!\!\!/\,\psi^{(k)} + \frac{g^2}{2}\left(\sum_{k=1}^{N}\overline{\psi}^{(k)}\psi^{(k)}\right)^2 - \frac{g^2}{2}\left(\sum_{k=1}^{N}\overline{\psi}^{(k)}\gamma_5\psi^{(k)}\right)^2. \tag{4.110}$$

As in the rest of the text, we use a representation of the gamma matrices where $\gamma_0 = -\sigma_x$, $\gamma_1 = -i\sigma_z$, and $\gamma_5 = \gamma_0\gamma_1 = \sigma_y$. As defined on a lattice, the chiral Gross-Neveu model is

$$\mathscr{L}_n = \sum_{k=1}^{N}\Psi_n^{\dagger(k)}(t)\begin{pmatrix} i\frac{\partial}{\partial t} & \partial_n \\ \partial_n^\dagger & i\frac{\partial}{\partial t}\end{pmatrix}\Psi_n^{(k)}(t) + \frac{g^2}{2}\left(\Psi_n^{\dagger(k)}(t)\gamma_0\Psi_n^{(k)}(t)\right)^2 - \frac{g^2}{2}\left(\Psi_n^{\dagger(k)}(t)\gamma_0\gamma_5\Psi_n^{(k)}(t)\right)^2. \tag{4.111}$$

We will follow Shei's analysis and determine the saddle point solutions of this lattice action.

In the continuum limit, the chiral GN model has saddle point equations which exactly corresponds to the BdG equation and self-consistency condition in superconductors and fermionic superfluids; the Lagrangian above therefore corresponds to analogous systems defined on a lattice.

4.5.1 Action in terms of scattering data

To map the action onto a scattering problem, we require the introduction of two Hubbard-Stratonovich fields, which we will call χ and η with the full order parameter $\Delta = \chi + i\eta$; suppressing the sum over flavors, the Lagrangian then becomes

$$\mathscr{L}_n = \Psi_n^\dagger \begin{pmatrix} i\frac{\partial}{\partial t} - g\eta_n(t) & \partial_n + g\chi_n(t) \\ \partial_n^\dagger + g\chi_n(t) & i\frac{\partial}{\partial t} + g\eta_n(t) \end{pmatrix} \Psi_n - \frac{\chi_n^2(t)}{2} - \frac{\eta_n^2(t)}{2}. \tag{4.112}$$

As before, we assume that the Hubbard-Stratonovich fields are static. Then, the action can be split into two pieces as in the case of the Gross-Neveu model:

$$S_1(\Delta) = -\frac{T}{2}\sum_n (\chi_n^2 + \eta_n^2), \tag{4.113}$$

$$S_2(\Psi, \Delta) = \sum_n \int_0^T dt\, \Psi_n^\dagger \begin{pmatrix} i\frac{\partial}{\partial t} - g\eta_n & \partial_n + g\chi_n \\ \partial_n^\dagger + g\chi_n & i\frac{\partial}{\partial t} + g\eta_n \end{pmatrix} \Psi_n. \tag{4.114}$$

The equations of motion now correspond to the following eigenvalue problem (assuming simple oscillatory time dependence for the fermionic fields)

$$\begin{pmatrix} -g\eta_n & \partial_n + g\chi_n \\ \partial_n^\dagger + g\chi_n & g\eta_n \end{pmatrix} \Psi_n = \omega \Psi_n. \tag{4.115}$$

Unlike in the original Gross-Neveu model, this equation cannot be factorized into two independent Schrödinger equations for each component of the fermionic field due to the presence of the chiral term. As a result, we must re-derive trace identities for the above Dirac operator and relate the action to suitably defined scattering data. As discussed in Appendix **??**, we may define the Jost functions for this scattering problem, which are written as $f_\pm$ and $g_\pm$ – the subscript $\pm$ is present due to the two-sheet structure of the Dirac equation, which supports both positive and negative energy modes. In the Dirac equation, the positive and negative sheets are decoupled, and so the action can be written in terms of two reflection coefficients $r_+(\phi)$ and $r_-(\phi)$, each of which corresponds to a scattering process involving the positive or negative modes separately. As in the Gross-Neveu model, we assume that both $a_+(\phi)$ and $a_-(\phi)$ have the same structure as in Eqns. (4.35) and (4.36). Therefore, by the Poisson-Jensen formula, we may write

$$\begin{aligned}\log|a_+(z)|+\log|a_-(z)| = &\sum_{j=1}^{M_+}\log\left|\frac{z-z_{j,+}}{1-z_{j,+}z}\right|+\sum_{j=1}^{M_-}\log\left|\frac{z-z_{j,-}}{1-z_{j,-}z}\right| \\ &-\frac{1}{4\pi}\int_0^{2\pi}\Re\left(\frac{e^{i\phi}+z}{e^{i\phi}-z}\right)\left[\log\left(1-|r_+(e^{i\phi})|^2\right)+\log\left(1-|r_-(e^{i\phi})|^2\right)\right]d\phi,\end{aligned} \tag{4.116}$$

where $M_\pm$ are the number of bound states in the scattering problems defined on the positive and negative sheets. On a technical note, we show in Appendix A that $a_+(z)$ and $a_-(z)$ are separately not meromorphic in the unit disk, but their product is; thus, the Poisson-Jensen formula must be applied to $\log(a_+(z)a_-(z))$. As a result, the left hand side of the above equation admits a Laurent series expansion as derived in Appendix **??**. In particular, like for the Schrodinger equation, we show that

$$-\log\frac{a_+(z)}{a_+(0)}-\log\frac{a_-(z)}{a_-(0)} = h_+(z)+h_-(z)+\sum_{k=0}^{\infty}\frac{\mathrm{Tr}(H^{2k})}{\omega^{2k}k}, \tag{4.117}$$

where $h_\pm$ are unimportant functions and

$$\omega^2(z) = \eta_\infty^2 + \left(\frac{\tau_\infty(z+z^{-1})}{2} + \chi_\infty\right)^2 - \frac{\tau_\infty^2(z-z^{-1})^2}{4}. \tag{4.118}$$

and the matrix H is the Dirac operator:

$$H = \begin{pmatrix} -g\eta_n & \partial_n + g\chi_n \\ \partial_n^\dagger + g\chi_n & g\eta_n \end{pmatrix}. \tag{4.119}$$

Henceforth, we shall set $g = 1$. As in the case of the Gross-Neveu model, we match the series expansion obtained via the trace identity with that obtained via the Poisson-Jensen formula. Matching to lowest order in z gives the first nontrivial trace identity:

$$-\frac{1}{2\pi}\int_0^{2\pi}\left[\log\left(1-|r_+(e^{i\phi})|^2\right)+\log\left(1-|r_-(e^{i\phi})|^2\right)\right]\cos(\phi)\,d\phi + \sum_{j=1}^{M_+}\left(z_{j,+}-\frac{1}{z_{j,+}}\right) + \sum_{j=1}^{M_-}\left(z_{j,-}-\frac{1}{z_{j,-}}\right) = C(N,\chi_\infty,\eta_\infty,\tau_\infty) + \frac{4}{\tau_\infty\chi_\infty}\sum_n(\eta_n^2+\chi_n^2+\tau_n^2), \tag{4.120}$$

where C is a constant that can be eliminated by an appropriate shift of the vacuum energy and will be ignored henceforth. Here, we have used the fact that $\mathrm{Tr}(H^2) = \sum_n(\eta_n^2+\chi_n^2+\tau_n^2)$. Using the assumption that $\tau_\infty\chi_\infty = 1$ and assuming that the sum of the squared values of τ_i are bounded and fixed, the second term in the action can be written in terms of the scattering data:

$$S_1 = -\frac{T}{2}\sum_n(\chi_n^2+\eta_n^2) = \frac{T}{2\pi}\int_0^{2\pi}\left[\log\left(1-|r_+(e^{i\phi})|^2\right)+\log\left(1-|r_-(e^{i\phi})|^2\right)\right]\cos(\phi)\,d\phi + \sum_{j=1}^{M_+}\left(z_{j,+}-\frac{1}{z_{j,+}}\right) + \sum_{j=1}^{M_-}\left(z_{j,-}-\frac{1}{z_{j,-}}\right). \tag{4.121}$$

Next, we must write the integration over the fermionic variables in terms of the scattering data. This can be done in a very similar way to what was done in the Gross-Neveu model. First, Eqn. (4.62) still holds. However, in this case we must distinguish the positive and negative sheets because the corresponding bound state spectra may not coincide. In the Gross-Neveu case, this was not necessary because the theory was invariant under charge conjugation. Therefore, we write

$$\mathscr{I}_1(\chi,\eta) = \mathscr{I}_1(0)\prod_k (e^{i\alpha_{+,k}/2} + e^{-i\alpha_{+,k}/2})\prod_{k'}(e^{i\alpha_{-,k'}/2} + e^{-i\alpha_{-,k'}/2}) \tag{4.122}$$

$$= \mathscr{I}_1(0)\exp\left(\frac{i}{2}\sum_k |\alpha_{+,k}| + |\alpha_{-,k}|\right)\prod_{\alpha_{+,k}>0}(1+e^{-i\alpha_{+,k}})\prod_{\alpha_{-,k}>0}(1+e^{-i\alpha_{-,k}}) \tag{4.123}$$

$$= \mathscr{I}_1(0)\exp\left(\frac{i}{2}\sum_k |\alpha_{+,k}| + |\alpha_{-,k}|\right)\sum_{\{n_i,m_j\}} e^{-i\sum_{\alpha_{+,i}>0} n_i\alpha_{+,i} - i\sum_{\alpha_{-,j}>0} m_j\alpha_{-,j}}\prod_{i,j} q_{n_i}q_{m_j}, \tag{4.124}$$

where the combinatorial coefficients are defined without an additional factor of two, $q_{n_i} = \frac{N!}{n_i!(N-n_i)!}$. Then, the full effective action can be written as

$$S_{\text{eff}} = S_1 + \frac{N}{2}\sum_k (|\alpha_{+,k}| + |\alpha_{-,k}|) - \sum_k n_{+,k}|\alpha_{+,k}| - \sum_k n_{-,k}|\alpha_{-,k}| + \text{const.} \tag{4.125}$$

Next, we make the assumption that there is only a single discrete bound state for each branch: that is, $n_{+,0}$ fermions occupy mode $\alpha_{+,0}$ and $n_{-,0}$ fermions occupy mode $\alpha_{-,0}$ (the rest fill the continuum Fermi sea). Next, we need to relate the second term in the equation above as a function of the scattering data. Again, note that in the time independent case, the Floquet indices are T times the corresponding energies. Because the positive and negative branches are independent from one another, the associated scattering problems are decoupled, and a similar analysis to that presented in Appendix **??** gives (up to an infinite

constant that is corrected by a suitable renormalization of the vacuum energy)

$$\sum_k (|\alpha_{+,k}|+|\alpha_{-,k}|) = 2T\int_0^{2\pi}\frac{d\phi}{2\pi}\frac{\sin\phi}{\sqrt{\eta_0^2+\chi_0^2+\tau_0^2-\cos\phi}}(\delta_+(\phi)+\delta_-(\phi)), \tag{4.126}$$

where $\eta_0^2+\chi_0^2+\tau_0^2$ is the value of $\eta_n^2+\chi_n^2+\tau_n^2$ at infinity. Using the imaginary part of the Jensen formula presented in Eqn. (4.70), the action in Eqn. (4.125) can be written in terms of the reflection coefficient as well as the energy of the bound state

$$\begin{aligned}\frac{S_{\text{eff}}}{T} = \frac{1}{2\pi}\int_0^{2\pi}&\left[\log\left(1-|r_+(e^{i\phi})|^2\right)+\log\left(1-|r_-(e^{i\phi})|^2\right)\right]\cos(\phi)\,d\phi\\ &+\sum_{j=1}^{M_+}\left(z_{j,+}-\frac{1}{z_{j,+}}\right)+\sum_{j=1}^{M_-}\left(z_{j,-}-\frac{1}{z_{j,-}}\right)-n_{+,0}|\omega_{+,0}|-n_{-,0}|\omega_{-,0}|\\ &+N\int_0^{2\pi}\frac{d\phi}{2\pi}\frac{\sin\phi}{\sqrt{\eta_0^2+\chi_0^2+\tau_0^2-\cos\phi}}(\delta_+(\phi)+\delta_-(\phi)).\end{aligned} \tag{4.127}$$

The saddle point corresponding to this action implies that the effective scattering problems for both the positive and negative sheets are reflectionless. Furthermore, the corresponding bound state energy can be constructed by finding a minimum of the action with respect to $z_{j,\pm}$. The corresponding bound state energies are similar to those computed in the case of the Gross-Neveu model, and like before, we have two types of soliton solutions, topological and non-topological solitons. However, because the HS parameter is complex, there is a richer structure of saddle point solutions with nontrivial phase slip.

4.5.2 Soliton solutions

We now proceed to find saddle point solutions corresponding to the action in Eqn. (4.127). As the saddle point corresponds to reflectionless potentials in both of the scattering processes in the Dirac equation, we need to utilize the inverse scattering approach to retrieve the most general form of such a solution, which we will not attempt to pursue here.

One such class of solutions corresponds to $\eta_n = 0$ and χ_n a reflectionless superpotential; in this case, the chiral Gross-Neveu model reduces to the Gross-Neveu model and our previous analysis applies. These solutions are likely to be of most relevance for experimental verification.

There is another saddle point solution which can be achieved through minimal additional effort. We square the Dirac operator H defined in Eqn. (4.119) to obtain

$$H^2 = \begin{pmatrix} \eta_n^2 + (\partial_n + \chi_n)(\partial_n^\dagger + \chi_n) & \overline{\partial}_n \\ \overline{\partial}_n^\dagger & \eta_n^2 + (\partial_n^\dagger + \chi_n)(\partial_n + \chi_n) \end{pmatrix}, \tag{4.128}$$

where $\overline{\partial}_n f_n = \tau_{n+1}(\eta_{n+1} - \eta_n) f_{n+1}$. If $\eta_n = \eta$ is a constant, then the off-diagonal blocks vanish and the operator has a supersymmetric structure apart from a shift η^2, which does not affect the energy eigenstates. The eigenstates of the square of the Dirac operator are those of the original Dirac operator, and if χ is chosen to be a reflectionless superpotential, then the eigenstates of H^2 are reflectionless. This implies that both the positive and negative scattering problems are reflectionless for the Dirac operator, therefore satisfying the saddle point condition.

For these solutions, the Hubbard-Stratonovich field has a non-zero albeit constant imaginary part. If χ is a non-topological soliton, then it may be expressed as a kink-antikink pair as was previously deduced (assuming occupation of only a single bound state). If χ is a topological kink soliton, then the Hubbard-Stratonovich field undergoes a phase slip by a nontrivial angle θ, given by

$$\tan\theta = -\frac{\eta(\chi_+ - \chi_-)}{\chi_+\chi_- + \eta^2} = -\frac{\eta\sqrt{u}}{t+\eta^2}\left[\left(\frac{1}{2} + \frac{1}{2}\sqrt{1 - \frac{4t^2}{u^2}}\right)^{1/2} - \left(\frac{1}{2} - \frac{1}{2}\sqrt{1 - \frac{4t^2}{u^2}}\right)^{1/2}\right], \tag{4.129}$$

where $\chi_\pm$ are given in Eqn. (4.95). In the continuum case, it has been shown that such

solitons experience dynamics if the phase slip does not equal π, and one would need to solve for time-dependent saddle point solutions. The velocity of propagation of the soliton strongly depends on the phase angle: as the propagation velocity increases, the phase angle decreases towards zero and vanishes at a critical velocity, at which the soliton becomes unstable in accordance to the Landau criterion [99]. The theory of a dynamical or moving soliton has not been pursued here, though the authors speculate that the time dependence simply can be constructed from replacing n with $n - vt$ in expressions for χ_n, η_n, and τ_n.

Finally, constructing reflectionless potentials of the Dirac equation is a rich problem, and there is no elegant method one may use to construct such potentials via *discrete supersymmetry*, unlike in the case of the Schrödinger equation. Classification of such soliton solutions would be a reasonable next step to pursue [154–156].

4.6 Relation to the Toda hierarchy

In Section 4.2.4 we discussed the KdV equation and the KdV hierarchy, which is a series of nonlinear differential equations that are integrable and possess soliton solutions. To construct the hierarchy, one considers each trace identity of the Schrödinger equation as a Hamiltonian and constructs the corresponding equations of motion in terms of the scattering data. As has been emphasized, the soliton solutions of the KdV equation are related to those appearing as saddle point solutions in the Gross-Neveu model.

In the discrete case, the lattice Gross-Neveu model turns out to analogously possess resemblance to the Toda hierarchy, a series of integrable dynamical systems. To illustrate the resemblance, we reconstruct the Toda lattice Hamiltonian by utilizing the discrete trace identities; the method that we discuss had been first developed by Faddeev [151]. However, there are two differences from the continuous case that we must reconcile. First, for discrete systems each trace identity given by K_n (via Eqn. (4.44)) cannot be treated as a

Hamiltonian system because the dynamics induced by such a system does not preserve the phase space measure. Instead, Faddeev has shown that one needs to consider the combination $K_n - K_{n-2}$ as the Hamiltonian. Second, unlike in the case of the KdV equation, both the potential and hopping are considered dynamical variables, and are related to the original canonically conjugate position and momentum variables of the Toda lattice by a Flaschka transformation. The first Hamiltonian of the hierarchy is

$$H_1 = K_2 = \sum_n u_n^2 + 2t_n^2, \tag{4.130}$$

where u_n is the potential and t_n is the hopping. If we identify them as the Flaschka variables defined as $u_n = -\frac{p_n}{2}$ and $t_n = \frac{1}{2}e^{-\frac{(q_{n+1}-q_n)}{2}}$ then the Hamiltonian corresponds to the Toda lattice [138]. The equations of motion of such a system therefore preserves the magnitude of the reflection coefficient, as observed in the KdV equation; soliton solutions correspond to time-dependent reflectionless potentials. Continuing in a similar manner generates all Hamiltonians in the Toda hierarchy.

One subtlety that we have ignored is the fact that the equations of motion of the Gross-Neveu model are those of a massless Dirac particle, which decouples into two Schrödinger equations. Thus, it is more accurate to draw the analogy between the Gross-Neveu model and two interrelated Toda lattices. The soliton solutions to an analogous dynamical system will correspond to propagating kinks or domain walls. To obtain this dynamical system, we utilize the Lax pair formalism: we construct two operators L (which is antisymmetric) and H such that $\dot{H} = [L,H]$. It is simple to show that this dynamical system has an infinite set of conserved quantities $K_p = \mathrm{Tr}(H^p)$, implying its integrability. We choose the operator H to be the Dirac Hamiltonian in Eqn. (4.119) with $\eta_n = 0$ and χ_n relabelled to be Δ_n. Therefore, the conserved quantities coincide with the right hand sides of the trace identities. We also choose the following ansatz for the block diagonal matrix $L = \mathrm{diag}(h,h')$, where

h and h' are the matrices with nonzero matrix elements $h'_{n,n+1} = -h'_{n+1,n} = \Delta_n \tau_{n+1}$ and $h_{n,n+1} = -h_{n+1,n} = \Delta_{n+1}\tau_{n+1}$. With this choice, H and L form a Lax pair, resulting in the dynamical system

$$\frac{d\Delta_n}{dt} = \Delta_n \left(\tau_n^2 - \tau_{n+1}^2\right) \qquad \frac{d\tau_n}{dt} = \tau_n \left(\Delta_{n-1}^2 - \Delta_n^2\right). \tag{4.131}$$

If we perform a Flaschka transformation $\Delta_n = e^{\frac{1}{2}(q_{n+1}-q_n)}$ and $\tau_n = e^{p_n}$, the equations of motion describe a Hamiltonian system with the Hamiltonian

$$H_1 = K_1 = \sum_n \tau_n^2 + \Delta_n^2 = \sum_n e^{2p_n} + \sum_n e^{q_{n+1}-q_n}, \tag{4.132}$$

which is similar to the Toda lattice Hamiltonian but with the quadratic kinetic energy replaced by the exponential of the momentum operator. For the case of the chiral Gross-Neveu model (with $\eta_n \neq 0$), the authors have no found a satisfying Lax pair L so we cannot deduce dynamical systems with complex soliton solutions. However, for a Dirac operator with a mass term,

$$H = \begin{pmatrix} -g\eta_n & \partial_n + g\chi_n \\ \partial_n^\dagger + g\chi_n & g\zeta_n \end{pmatrix}, \tag{4.133}$$

there exists a Lax pair matrix L with a similar block matrix structure, but with non-trivial off-diagonal blocks having the same matrix structure of ∂_n. We will not write down the associated dynamical system, as it possesses a different class of soliton solutions that we have not constructed.

4.7 Conclusions

In this paper, we describe a general formalism to construct soliton solutions corresponding to saddle points of a lattice quantum field theory, which is based on the semiclassical

method developed by Dashen, Hasslacher, and Neveu [110, 111]. We first focus our attention to a lattice generalization of the Gross-Neveu model with N flavors of fermions. The equations of motion decouple into two discrete Schrödinger equations, and utilizing trace identities for the Schrödinger equation, we rewrite the action in terms of scattering variables – namely, the reflection coefficient and the bound state spectrum. The saddle point solutions of this action functional correspond to the Hubbard-Stratonovich parameter being a reflectionless potential. Depending on the boundary conditions at $\pm\infty$, we derive the bound state spectrum for either topological or non-topoogical solitons, the former of which possesses a robust zero mode. To construct these potentials explicitly, we develop a discrete generalization of supersymmetry, in which we create a hierarchy of reflectionless tight-binding Hamiltonians with a bound state spectrum of our choice. We are able to retrieve both kink solitons and kink-antikink solitons using this formalism. Both such solitons are described by a site-dependent modulation in the onsite potential and the hopping, the latter of which is absent in the continuum limit.

We then proceed to applying the semiclassical method to the lattice chiral Gross-Neveu model. In doing so, we derive a set of trace identities for the Dirac operator, and show that the action can be written in terms of scattering data of the scattering problems of the positive and negative energy modes. In a similar way, the particle spectrum can be obtained, and saddle point solutions correspond to reflectionless potentials of the Dirac equation. We write down one such example, a kink soliton undergoing a non-π phase slip; these solitons likely have nontrivial dynamics that we have not accounted for. Finally, we relate the soliton solutions obtained from the saddle points to exact solitons in the Toda lattice. In the process, we write down dynamical systems whose solutions are propagating domain walls/kinks, in analogy to the static solutions derived in the field theories.

There are multiple generalizations that are straightforward to consider given our formalism. First, we have exclusively considered a single-band model. To construct a two-

band (and in general, a multi-band) model, we simply set asymptotic conditions where $\Delta_{2n+1} = \Delta_1^{(\pm)}$ and $\Delta_{2n} = \Delta_2^{(\pm)}$ as $n \to \pm\infty$, which is in the spirit of the Su-Schrieffer-Heeger model [115, 116]. The action can be written in terms of scattering data by an appropriate modification of trace identities for the Schrödinger operator with staggered boundary conditions. Reflectionless soliton solutions can be computed easily using the discrete supersymmetry formalism. Another possible extension would be to apply a magnetic field, so that the hopping undergoes a phase slip from $-\infty$ to ∞. Second, it may be possible to pursue a similar analysis with long-range hopping. In this case, there may be multiple scatterers at a given energy, and the scattering data will consist of a potentially large scattering matrix. Depending on the structure of the hopping, discrete supersymmetry may still provide a means for obtaining classes of solutions with scattering properties prescribed by the saddle point solution. Finally, it is interesting to pursue an analogous analysis in 2+1 dimensions, where the inverse scattering method can still be formulated, though supersymmetry may not be a useful tool for extracting soliton solutions.

The original motivation for studying both the Gross-Neveu and the chiral Gross-Neveu model is that both models (especially the latter) are equivalent to the self-consistent Bogoliubov de-Genne Hamiltonians describing superconductors and/or fermionic superfluids [102]. As a result, it is possible that lattice soliton solutions presented in the text can be observed in cold atom experiments [96]. A more complete analysis should also include an analysis of the dynamics of such soliton solutions, where it is known that the velocity of propagation is related to the phase slip of a kink soliton [99]. Furthermore, the kink solitons that were presented for the chiral Gross-Neveu model are not the only family of reflectionless potentials; a complete classification of transparent potentials of the Dirac equation would be of importance to understanding the full saddle point structure of the action [154, 155].

Finally, discrete supersymmetry is itself a rich topic with many unexplored questions.

Though the application of the methodology in this paper was for obtaining soliton solutions, discrete symmetry can be applied to other kinds of 1D and quasi 1D systems to explore potentially interesting physics. A complete classification of what kinds of systems are closed under a discrete SUSY transformation has not been performed. Discrete SUSY may also have significance when applied to non-Hermitian or time-reversal symmetry breaking Hamiltonians. A potential application of discrete SUSY would be to probe topological properties of a system. Since a single iteration of supersymmetry removes or adds a zero mode, the topological (Witten) index of a system can itself be altered – it would be interesting to pursue an analysis in this direction [157].

Note added. After completion of this manuscript, the authors became aware of [158], which focuses on constructing exact hierarchies of discrete reflectionless potentials using a method similar to supersymmetric quantum mechanics (albeit more restrictive than ours). It would be interesting to understand whether more kinds of exact hierarchies can be constructed using our framework.

Bibliography

[1] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27(3):379–423, 1948. doi: 10.1002/j.1538-7305.1948.tb01338.x.

[2] Lillian Hoddeson. The discovery of the point-contact transistor. *Historical Studies in the Physical Sciences*, 12(1):41–76, 1981.

[3] Jack S Kilby. Invention of the integrated circuit. *IEEE Transactions on electron devices*, 23(7):648–654, 1976.

[4] Gordon E Moore et al. Cramming more components onto integrated circuits, 1965.

[5] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

[6] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978. ISSN 0001-0782. doi: 10.1145/359340.359342. URL `https://doi.org/10.1145/359340.359342`.

[7] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*, chapter 5, pages 218–219. Cambridge university press, 2010. doi: 10.1017/CBO9780511976667.

[8] Richard P Feynman. Simulating physics with computers, international journal of theoretical physics. 1982.

[9] Scott Aaronson. *Quantum Computing since Democritus*. Cambridge University Press, 2013.

[10] N. David Mermin. *Quantum Computer Science: An Introduction*. Cambridge University Press, 2007.

[11] Henri Poincaré. *New methods of celestial mechanics*. Number 450-451. National Aeronautics and Space Administration, 1967.

[12] Lapo Casetti, Monica Cerruti-Sola, Marco Pettini, and E. G. D. Cohen. The fermi-pasta-ulam problem revisited: Stochasticity thresholds in nonlinear hamiltonian systems. *Phys. Rev. E*, 55:6566–6574, Jun 1997. doi: 10.1103/PhysRevE.55.6566. URL https://link.aps.org/doi/10.1103/PhysRevE.55.6566.

[13] Giancarlo Benettin, Helen Christodoulidi, and Antonio Ponno. The fermi-pasta-ulam problem and its underlying integrable dynamics. *Journal of Statistical Physics*, 152(2):195–212, 2013.

[14] Tao Pang. *An introduction to computational physics*. Cambridge university press, 2006.

[15] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. IEEE, 1994. URL https://doi.org/10.1109/SFCS.1994.365700.

[16] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999. URL https://doi.org/10.1137/S0097539795293172.

[17] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010. doi: 10.1017/CBO9780511976667. URL https://doi.org/10.1017/CBO9780511976667.

[18] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978. URL https://doi.org/10.1145/359340.359342.

[19] Fritz Haake. *Quantum signatures of chaos*. Springer, Berlin, Heidelberg, 2001. URL https://doi.org/10.1007/978-3-662-04506-0.

[20] Edward Ott. *Chaos in dynamical systems*. Cambridge University Press, 2002. URL https://doi.org/10.1017/CBO9780511803260.

[21] Steven W McDonald and Allan N Kaufman. Spectrum and eigenfunctions for a Hamiltonian with stochastic trajectories. *Phys. Rev. Lett.*, 42(18):1189, 1979. URL https://doi.org/10.1103/PhysRevLett.42.1189.

[22] G Casati, F Valz-Gris, and I Guarnieri. On the connection between quantization of nonintegrable systems and statistical theory of spectra. *Lett. Nuovo Cimento*, 28(8):279–282, 1980. URL https://doi.org/10.1007/BF02798790.

[23] Michael V Berry. Quantizing a classically ergodic system: Sinai's billiard and the KKR method. *Ann. Phys.*, 131(1):163–216, 1981. URL https://doi.org/10.1016/0003-4916(81)90189-5.

[24] Oriol Bohigas, Marie-Joya Giannoni, and Charles Schmit. Characterization of chaotic quantum spectra and universality of level fluctuation laws. *Phys. Rev. Lett.*, 52(1):1, 1984. URL https://doi.org/10.1103/PhysRevLett.52.1.

[25] J H Hannay and A M Ozorio de Almeida. Periodic orbits and a correlation function for the semiclassical density of states. *J. Phys. A: Math. Gen.*, 17(18):3429, 1984. URL https://doi.org/10.1088/0305-4470/17/18/013.

[26] Michael Victor Berry. Semiclassical theory of spectral rigidity. *Proc. Roy. Soc. Lond. A*, 400(1819):229–251, 1985. URL https://doi.org/10.1098/rspa.1985.0078.

[27] Nathan Argaman, Yoseph Imry, and Uzy Smilansky. Semiclassical analysis of spectral correlations in mesoscopic systems. *Phys. Rev. B*, 47(8):4440, 1993. URL https://doi.org/10.1103/PhysRevB.47.4440.

[28] Sebastian Müller, Stefan Heusler, Petr Braun, Fritz Haake, and Alexander Altland. Semiclassical foundation of universality in quantum chaos. *Phys. Rev. Lett.*, 93(1): 014103, 2004. URL https://doi.org/10.1103/PhysRevLett.93.014103.

[29] Sebastian Müller, Stefan Heusler, Petr Braun, Fritz Haake, and Alexander Altland. Periodic-orbit theory of universality in quantum chaos. *Phys. Rev. E*, 72(4):046207, 2005. URL https://doi.org/10.1103/PhysRevE.72.046207.

[30] Amit Vikram and Victor Galitski. Dynamical quantum ergodicity from energy level statistics. *Phys. Rev. Res.*, 5(3):033126, 2023. URL https://doi.org/10.1103/PhysRevResearch.5.033126.

[31] JH Hannay and Michael V Berry. Quantization of linear maps on a torus-fresnel diffraction by a periodic grating. *Phys. D: Nonlinear Phenom.*, 1(3):267–290, 1980. URL https://doi.org/10.1016/0167-2789(80)90026-3.

[32] Jonathan P Keating. The cat maps: quantum mechanics and classical motion. *Nonlinearity*, 4(2):309, 1991. URL https://doi.org/10.1088/0951-7715/4/2/006.

[33] Prot Pakoński, Karol Życzkowski, and Marek Kuś. Classical 1D maps, quantum graphs and ensembles of unitary matrices. *J. Phys. A: Math. Gen.*, 34(43):9303, 2001. URL https://doi.org/10.1088/0305-4470/34/43/313.

[34] Nandor L Balazs and André Voros. The quantized baker's transformation. *Ann. Phys.*, 190(1):1–31, 1989. URL https://doi.org/10.1016/0003-4916(89)90259-5.

[35] Marcos Saraceno. Classical structures in the quantized baker transformation. *Ann. Phys.*, 199(1):37–60, 1990. URL https://doi.org/10.1016/0003-4916(90)90367-W.

[36] Freeman J Dyson and Harold Falk. Period of a discrete cat mapping. *The American Mathematical Monthly*, 99(7):603–614, 1992. URL https://doi.org/10.2307/2324989.

[37] Arul Lakshminarayan. Shuffling cards, factoring numbers and the quantum baker's map. *J. Phys. A: Math. Gen.*, 38(37):L597, 2005. URL https://doi.org/10.1088/0305-4470/38/37/L01.

[38] Arul Lakshminarayan. Modular multiplication operator and quantized baker's maps. *Phys. Rev. A*, 76(4):042330, 2007. URL https://doi.org/10.1103/PhysRevA.76.042330.

[39] NL Balazs and A Voros. The quantized baker's transformation. *Europhysics Letters*, 4(10):1089, 1987. URL https://doi.org/10.1209/0295-5075/4/10/001.

[40] B. V. Chirikov, F. M. Izrailev, and D. L. Shepelyansky. Dynamical stochasticity in classical and quantum mechanics. *Sov. Scient. Rev. C*, 2:209, 1981.

[41] D. Shepelyansky. Ehrenfest time and chaos. *Scholarpedia*, 15(9):55031, 2020. doi: 10.4249/scholarpedia.55031. URL https://doi.org/10.4249/scholarpedia.55031.

[42] Nalini Anantharaman and Stéphane Nonnenmacher. Entropy of semiclassical measures of the Walsh-quantized baker's map. *Ann. Henri Poincaré*, 8(1):37–74, 2007. URL https://doi.org/10.1007/s00023-006-0299-z.

[43] Alfréd Rényi. Representations for real numbers and their ergodic properties. *Acta Math. Acad. Sci. Hungar*, 8(3-4):477–493, 1957. URL https://doi.org/10.1007/BF02020331.

[44] Marcos Saraceno and André Voros. Towards a semiclassical theory of the quantum baker's map. *Phys. D: Nonlinear Phenom.*, 79(2-4):206–268, 1994. URL https://doi.org/10.1016/S0167-2789(05)80007-7.

[45] Ron Rubin and Nathan Salwen. A canonical quantization of the baker's map. *Ann. Phys.*, 269(2):159–181, 1998. URL https://doi.org/10.1006/aphy.1998.5845.

[46] Leonardo Ermann and Marcos Saraceno. Generalized quantum baker maps as perturbations of a simple kernel. *Phys. Rev. E*, 74(4):046205, 2006. URL https://doi.org/10.1103/PhysRevE.74.046205.

[47] Mark M. Tracy and A. J. Scott. The classical limit for a class of quantum baker's maps. *J. Phys. A*, 35(39):8341–8360, 2002. URL https://doi.org/10.1088/0305-4470/35/39/314.

[48] S. De Bièvre and M. Degli Esposti. Egorov theorems and equidistribution of eigenfunctions for the quantized sawtooth and baker maps. *Ann. Inst. H. Poincaré Phys. Théor.*, 69(1):1–30, 1998. URL http://www.numdam.org/item/AIHPA_1998__69_1_1_0/.

[49] M. Degli Esposti, S. Nonnenmacher, and B. Winn. Quantum variance and ergodicity for the baker's map. *Comm. Math. Phys.*, 263(2):325–352, 2006. URL https://doi.org/10.1007/s00220-005-1397-3.

[50] A. Bouzouina and S. De Bièvre. Equipartition of the eigenfunctions of quantized ergodic maps on the torus. *Comm. Math. Phys.*, 178(1):83–105, 1996. URL https://doi.org/10.1007/BF02104909.

[51] Todd A Brun and Rüdiger Schack. Realizing the quantum baker's map on a NMR quantum computer. *Phys. Rev. A*, 59(4):2649, 1999. URL https://doi.org/10.1103/PhysRevA.59.2649.

[52] Yaakov S Weinstein, Seth Lloyd, Joseph Emerson, and David G Cory. Experimental implementation of the quantum baker's map. *Phys. Rev. Lett.*, 89(15):157902, 2002. doi: https://doi.org/10.1103/PhysRevLett.89.157902.

[53] Denis V Vasilyev, Andrey Grankin, Mikhail A Baranov, Lukas M Sieberer, and Peter Zoller. Monitoring quantum simulators via quantum nondemolition couplings to atomic clock qubits. *PRX Quantum*, 1(2):020302, 2020. URL https://doi.org/10.1103/PRXQuantum.1.020302.

[54] Lata Kh Joshi, Andreas Elben, Amit Vikram, Benoît Vermersch, Victor Galitski, and Peter Zoller. Probing many-body quantum chaos with quantum simulators. *Phys. Rev. X*, 12(1):011018, 2022. URL https://doi.org/10.1103/PhysRevX.12.011018.

[55] Yakov Grigor'evich Sinai. A weak isomorphism of transformations with invariant measure. In *Dokl. Akad. Nauk SSSR*, volume 147, pages 797–800. Russian Academy of Sciences, 1962. URL https://www.mathnet.ru/eng/dan27300.

[56] Eli Glasner. *Ergodic theory via joinings*. Number 101. American Mathematical Soc., 2003.

[57] I. P. Cornfield, S. V. Fomin, and Yakov G. Sinai. *Ergodic theory*. Springer-Verlag New York, 1982. ISBN 978-1-4615-6927-5. URL https://doi.org/10.1007/978-1-4615-6927-5.

[58] Arjen K Lenstra and Hendrik W Lenstra. *The development of the number field sieve*, volume 1554. Springer Science & Business Media, 1993. doi: 10.1007/BFb0091534.

[59] Carl Pomerance. A tale of two sieves. *Notices of the American Mathematical Society*, 43(12):1473–1485, 1996.

[60] Enrique Martin-Lopez, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou, and Jeremy L O'brien. Experimental realization of shor's quantum factoring algorithm using qubit recycling. *Nature photonics*, 6(11):773–776, 2012. doi: 10.1038/nphoton.2012.259.

[61] Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid. Nist special publication 800-57. *NIST Special publication*, 800(57):1–142, 2007. doi: 10.6028/NIST.SP.800-57pt3r1.

[62] Stephane Beauregard. Circuit for shor's algorithm using 2n+3 qubits, 2003. URL https://arxiv.org/abs/quant-ph/0205095.

[63] XinJian Tan and Peng Gao. An efficient quantum circuit implementation of shor's algorithm for gpu accelerated simulation. *AIP Advances*, 14(2), 2024. doi: 10.1063/5.0186385.

[64] Arnold Schönhage and Volker Strassen. Fast multiplication of large numbers. *Computing*, 7:281–292, 1971.

[65] Alberto Politi, Jonathan C. F. Matthews, and Jeremy L. O'Brien. Shor's quantum factoring algorithm on a photonic chip. *Science*, 325(5945):1221–1221, 2009. doi: 10.1126/science.1173731. URL https://www.science.org/doi/abs/10.1126/science.1173731.

[66] John A. Smolin, Graeme Smith, and Alexander Vargo. Oversimplifying quantum factoring. *Nature*, 499:163–165, 2013. URL https://api.semanticscholar.org/CorpusID:4422110.

[67] Chao-Yang Lu, Daniel E. Browne, Tao Yang, and Jian-Wei Pan. Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits. *Phys. Rev. Lett.*, 99:250504, Dec 2007. doi: 10.1103/PhysRevLett.99.250504. URL https://link.aps.org/doi/10.1103/PhysRevLett.99.250504.

[68] B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James, A. Gilchrist, and A. G. White. Experimental demonstration of a compiled version of shor's algorithm with quantum entanglement. *Phys. Rev. Lett.*, 99:250505, Dec 2007. doi: 10.1103/PhysRevLett.99.250505. URL https://link.aps.org/doi/10.1103/PhysRevLett.99.250505.

[69] Eric R. Anschuetz, Jonathan P. Olson, Alán Aspuru-Guzik, and Yudong Cao. Variational quantum factoring, 2018. URL https://arxiv.org/abs/1808.08927.

[70] Bao Yan, Ziqi Tan, Shijie Wei, Haocong Jiang, Weilong Wang, Hong Wang, Lan Luo, Qianheng Duan, Yiting Liu, Wenhao Shi, Yangyang Fei, Xiangdong Meng, Yu Han, Zheng Shan, Jiachen Chen, Xuhao Zhu, Chuanyu Zhang, Feitong Jin, Hekang Li, Chao Song, Zhen Wang, Zhi Ma, H. Wang, and Gui-Lu Long. Factoring integers with sublinear resources on a superconducting quantum processor, 2022. URL https://arxiv.org/abs/2212.12372.

[71] Yanwu Gu, Yunheng Ma, Nicolò Forcellini, and Dong E. Liu. Noise-resilient phase estimation with randomized compiling. *Phys. Rev. Lett.*, 130:250601, Jun 2023. doi: 10.1103/PhysRevLett.130.250601. URL https://link.aps.org/doi/10.1103/PhysRevLett.130.250601.

[72] Debjyoti Biswas, Sourav Dutta, Shrikant Utagi, and Prabha Mandayam. A modified order-finding algorithm for nisq devices. In *2024 16th International Conference on COMmunication Systems and NETworkS (COMSNETS)*, pages 1064–1069, 2024. doi: 10.1109/COMSNETS59351.2024.10426927.

[73] Oded Regev. An efficient quantum factoring algorithm, 2024. URL https://arxiv.org/abs/2308.06572.

[74] Martin Ekerå and Joel Gärtner. Extending regev's factoring algorithm to compute discrete logarithms. In *International Conference on Post-Quantum Cryptography*, pages 211–242. Springer, 2024. URL https://doi.org/10.1007/978-3-031-62746-0_10.

[75] Gregory D. Kahanamoku-Meyer and Norman Y. Yao. Fast quantum integer multiplication with zero ancillas, 2024. URL https://arxiv.org/abs/2403.18006.

[76] Alexei Y. Kitaev. Quantum measurements and the abelian stabilizer problem. *Electron. Colloquium Comput. Complex.*, TR96, 1995. URL https://api.semanticscholar.org/CorpusID:17023060.

[77] Igor L. Markov and Mehdi Saeedi. Constant-optimized quantum circuits for modular multiplication and exponentiation, 2015. URL https://arxiv.org/abs/1202.6614.

[78] Vlatko Vedral, Adriano Barenco, and Artur Ekert. Quantum networks for elementary arithmetic operations. *Physical Review A*, 54(1):147–153, July 1996. ISSN 1094-1622. doi: 10.1103/physreva.54.147. URL http://dx.doi.org/10.1103/PhysRevA.54.147.

[79] David Beckman, Amalavoyal N. Chari, Srikrishna Devabhaktuni, and John Preskill. Efficient networks for quantum factoring. *Physical Review A*, 54(2):1034–1063, August 1996. ISSN 1094-1622. doi: 10.1103/physreva.54.1034. URL http://dx.doi.org/10.1103/PhysRevA.54.1034.

[80] Thomas Häner, Martin Roetteler, and Krysta M. Svore. Factoring using 2n+2 qubits with toffoli based modular multiplication, 2017. URL https://arxiv.org/abs/1611.07995.

[81] Yasuhiro Takahashi and Noboru Kunihiro. A quantum circuit for Shor's factoring algorithm using 2n+2 qubits. *Quant. Inf. Comput.*, 6(2):184–192, 2006. doi: 10.26421/QIC6.2-4.

[82] Thomas G. Draper. Addition on a quantum computer, 2000. URL https://arxiv.org/abs/quant-ph/0008033.

[83] D. Coppersmith. An approximate fourier transform useful in quantum factoring, 2002. URL https://arxiv.org/abs/quant-ph/0201067.

[84] Donald Ervin Knuth. *The art of computer programming*, volume 3. Pearson Education, 1997.

[85] Abu Musa Patoary, Amit Vikram, Laura Shou, and Victor Galitski. Chaotic roots of the modular multiplication dynamical system in Shor's algorithm. *Phys. Rev. Res.*, 6:L032046, 2024. URL https://doi.org/10.1103/PhysRevResearch.6.L032046.

[86] A. Ekert, P. M. Hayden, and H. Inamori. *Basic Concepts in Quantum Computation*, page 661–701. Springer Berlin Heidelberg. ISBN 9783540410478. doi: 10.1007/3-540-45338-5_10. URL http://dx.doi.org/10.1007/3-540-45338-5_10.

[87] Richard Cleve and John Watrous. Fast parallel circuits for the quantum fourier transform. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 526–536. IEEE, 2000. URL https://doi.org/10.48550/arXiv.quant-ph/0006004.

[88] P. Erdos, C. Pomerance, and E. Schmutz. Carmichael's lambda function. *Acta Arithmetica*, 58(4):363–385, 1991. URL http://eudml.org/doc/206359.

[89] G. H. Hardy and S. Ramanujan. On the normal number of prime factors of a number n. *Quarterly Journal of Mathematics*, s2-16(1):112–120, 1917. doi: 10.1112/plms/s2-16.1.112.

[90] D. J. Korteweg and G. de Vries. On the change of form of long waves advancing in a rectangular canal, and on a new type of long stationary waves. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 39(240):422–443, 1895. doi: 10.1080/14786449508620739. URL https://doi.org/10.1080/14786449508620739.

[91] Norman J. Zabusky and Martin D. Kruskal. Interaction of" solitons" in a collisionless plasma and the recurrence of initial states. *Physical review letters*, 15(6):240, 1965.

[92] Clifford S. Gardner, John M. Greene, Martin D. Kruskal, and Robert M. Miura. Method for solving the korteweg-devries equation. *Physical review letters*, 19(19): 1095, 1967.

[93] Peter D. Lax. Integrals of nonlinear equations of evolution and solitary waves. *Communications on pure and applied mathematics*, 21(5):467–490, 1968.

[94] Linn F. Mollenauer and James P. Gordon. *Solitons in optical fibers: fundamentals and applications*. Elsevier, 2006.

[95] A. M. Kosevich, B. A. Ivanov, and A. S. Kovalev. Magnetic solitons. *Physics Reports*, 194(3-4):117–238, 1990.

[96] Tarik Yefsah, Ariel T. Sommer, Mark J. H. Ku, Lawrence W. Cheuk, Wenjie Ji, Waseem S. Bakr, and Martin W. Zwierlein. Heavy solitons in a fermionic superfluid. *Nature*, 499(7459):426–430, 2013.

[97] J Denschlag, J. E. Simsarian, D. L. Feder, Charles W. Clark, L. A. Collins, J. Cubizolles, L. Deng, E. W. Hagley, K. Helmerson, W. P. Reinhardt, S. L. Rolston, B. I. Schneider, and W. D. Phillips. Generating solitons by phase engineering of a bose-einstein condensate. *Science*, 287(5450):97–101, 2000.

[98] L. Khaykovich, F. Schreck, G. Ferrari, T. Bourdel, J. Cubizolles, L. D. Carr, Y. Castin, and C. Salomon. Formation of a matter-wave bright soliton. *Science*, 296(5571):1290–1293, 2002.

[99] Dmitry K. Efimkin and Victor Galitski. Moving solitons in a one-dimensional fermionic superfluid. *Physical Review A*, 91(2):023616, 2015.

[100] Daisuke A. Takahashi and Muneto Nitta. On reflectionless nature of self-consistent multi-soliton solutions in bogoliubov–de gennes and chiral gross–neveu models. *Journal of Low Temperature Physics*, 175(1):250–257, 2014.

[101] Daisuke A. Takahashi, Shunji Tsuchiya, Ryosuke Yoshii, and Muneto Nitta. Fermionic solutions of chiral gross–neveu and bogoliubov–de gennes systems in nonlinear schrödinger hierarchy. *Physics Letters B*, 718(2):632–637, 2012.

[102] Daisuke A. Takahashi and Muneto Nitta. Self-consistent multiple complex-kink solutions in bogoliubov–de gennes and chiral gross-neveu systems. *Physical review letters*, 110(13):131601, 2013.

[103] Enrico Fermi, John Pasta, and Stanislaw M. Ulam. *Studies of Nonlinear Problems*. University of California Press, 2020.

[104] G. P. Berman and F. M. Izrailev. The fermi–pasta–ulam problem: fifty years of progress. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 15(1):015104, 2005.

[105] Mark J. Ablowitz and Harvey Segur. *Solitons and the inverse scattering transform*. SIAM, 1981.

[106] Yuri S. Kivshar and Boris A. Malomed. Dynamics of solitons in nearly integrable systems. *Reviews of Modern Physics*, 61(4):763, 1989.

[107] Yaroslav V. Kartashov, Boris A. Malomed, and Lluis Torner. Solitons in nonlinear lattices. *Reviews of Modern Physics*, 83(1):247, 2011.

[108] F. Calogero and A. Degasperis. Coupled nonlinear evolution equations solvable via the inverse spectral transform, and solitons that come back: the boomeron. *Lettere al Nuovo Cimento (1971-1985)*, 16(14):425–433, 1976.

[109] V. N. Serkin, A. Hasegawa, and T. L. Belyaeva. Nonautonomous solitons in external potentials. *Physical Review Letters*, 98(7):074102, 2007.

[110] Roger F. Dashen, Brosl Hasslacher, and Andre Neveu. Semiclassical bound states in an asymptotically free theory. *Physical Review D*, 12(8):2443, 1975.

[111] Sun-Sheng Shei. Semiclassical bound states in a model with chiral symmetry. *Physical Review D*, 14(2):535, 1976.

[112] M. Karowski and P. Weisz. Exact form factors in (1+ 1)-dimensional field theoretic models with soliton behaviour. *Nuclear Physics B*, 139(4):455–476, 1978.

[113] S. A. Brazovskii, S. A. Gordyunin, and N. N. Kirova. *Soviet Journal of Experimental and Theoretical Physics Letters*, 31:456, 1980.

[114] S. A. Brazovskii and N. N. Kirova. Excitons, polarons, and bipolarons in conducting polymers. *Soviet Journal of Experimental and Theoretical Physics Letters*, 33:4, 1981.

[115] W. P. Su, J. R. Schrieffer, and A. J. Heeger. Soliton excitations in polyacetylene. *Physical Review B*, 22(4):2099, 1980.

[116] D. K. Campbell and A. R. Bishop. Solitons in polyacetylene and relativistic-field-theory models. *Physical Review B*, 24(8):4859, 1981.

[117] A. I. Buzdin and V. V. Tugushev. Phase diagrams of electronic and superconducting transitions to soliton lattice states. *Sov. Phys. JETP*, 58:428, 1983.

[118] Baruch Horovitz. Soliton lattice in polyacetylene, spin-peierls systems, and two-dimensional sine-gordon systems. *Physical Review Letters*, 46(11):742, 1981.

[119] Gökçe Başar and Gerald V. Dunne. Self-consistent crystalline condensate in chiral gross-neveu and bogoliubov–de gennes systems. *Physical review letters*, 100(20): 200404, 2008.

[120] A. I. Larkin and Yu. N. Ovchinnikov. Nonuniform state of superconductors. *Soviet Physics-JETP*, 20(3):762–762, 1965.

[121] Peter Fulde and Richard A. Ferrell. Superconductivity in a strong spin-exchange field. *Physical Review*, 135(3A):A550, 1964.

[122] R. A. Barankov, L. S. Levitov, and B. Z. Spivak. Collective rabi oscillations and solitons in a time-dependent bcs pairing problem. *Physical review letters*, 93(16): 160401, 2004.

[123] Emil A. Yuzbashyan. Normal and anomalous solitons in the theory of dynamical cooper pairing. *Physical Review B*, 78(18):184507, 2008.

[124] A. I. Buzdin and S. V. Polonskii. Nonuniform state in quasi-1d superconductors. *Sov. Phys. JETP*, 66(422):8, 1987.

[125] Gökçe Başar and Gerald V. Dunne. Twisted kink crystal in the chiral gross-neveu model. *Physical Review D*, 78(6):065022, 2008.

[126] Gökçe Başar, Gerald V. Dunne, and Michael Thies. Inhomogeneous condensates in the thermodynamics of the chiral NJL_2 model. *Physical Review D*, 79(10):105012, 2009.

[127] Francisco Correa, Gerald V. Dunne, and Mikhail S. Plyushchay. The bogoliubov–de gennes system, the akns hierarchy, and nonlinear quantum mechanical supersymmetry. *Annals of Physics*, 324(12):2522–2547, 2009.

[128] Y. Tanaka. Soliton in two-band superconductor. *Physical review letters*, 88(1): 017002, 2001.

[129] Shi-Zeng Lin and Xiao Hu. Phase solitons in multi-band superconductors with and without time-reversal symmetry. *New Journal of Physics*, 14(6):063021, 2012.

[130] Julien Garaud, Johan Carlström, and Egor Babaev. Topological solitons in three-band superconductors with broken time reversal symmetry. *Physical review letters*, 107(19):197001, 2011.

[131] Erick J. Weinberg. *Classical solutions in quantum field theory: Solitons and Instantons in High Energy Physics*. Cambridge University Press, 2012.

[132] Stefan Burger, Kai Bongs, Stefanie Dettmer, Wolfgang Ertmer, Klaus Sengstock, Anna Sanpera, Gora V Shlyapnikov, and Maciej Lewenstein. Dark solitons in bose-einstein condensates. *Physical Review Letters*, 83(25):5198, 1999.

[133] Kevin E. Strecker, Guthrie B. Partridge, Andrew G. Truscott, and Randall G. Hulet. Formation and propagation of matter-wave soliton trains. *Nature*, 417(6885):150–153, 2002.

[134] Victor Galitski. Non-perturbative Quantum Dynamics of the Order Parameter in the Pairing Model. *Phys. Rev. B*, 82(5):054511, 2010. doi: 10.1103/PhysRevB.82.054511.

[135] Frank Wilczek. Quantum time crystals. *Physical review letters*, 109(16):160401, 2012.

[136] Grigory A. Starkov and Konstantin B. Efetov. Phase transition into an instanton crystal state. *Physical Review B*, 103(7):075121, 2021.

[137] Fred Cooper, Avinash Khare, and Uday Sukhatme. Supersymmetry and quantum mechanics. *Physics Reports*, 251(5-6):267–385, 1995.

[138] Morikazu Toda. *Theory of Nonlinear Lattices*, pages 42–97. Springer, 1989. ISBN 978-3-642-83219-2. doi: 10.1007/978-3-642-83219-2_3. URL https://doi.org/10.1007/978-3-642-83219-2_3.

[139] M. J. Ablowitz and J. F. Ladik. Nonlinear differential–difference equations and fourier analysis. *Journal of Mathematical Physics*, 17(6):1011–1018, 1976. doi: 10.1063/1.523009. URL https://doi.org/10.1063/1.523009.

[140] Vladimir E. Korepin, Nicholay M. Bogoliubov, and Anatoli G. Izergin. *Quantum inverse scattering method and correlation functions*, volume 3. Cambridge university press, 1997.

[141] L. D. Faddeev. Algebraic aspects of the bethe ansatz. *International Journal of Modern Physics A*, 10(13):1845–1878, 1995.

[142] D. G. Crighton. *Applications of KdV*, pages 39–67. Springer, 1995.

[143] Harvey Segur. The korteweg-de vries equation and water waves. solutions of the equation. part 1. *Journal of Fluid Mechanics*, 59(4):721–736, 1973.

[144] Noah Hershkowitz, Thomas Romesser, and David Montgomery. Multiple soliton production and the korteweg—de vries equation. *Physical Review Letters*, 29(24):1586, 1972.

[145] Noah Hershkowitz and Thomas Romesser. Observations of ion-acoustic cylindrical solitons. *Physical Review Letters*, 32(11):581, 1974.

[146] V. E. Zakharov and L. D. Faddeev. Korteweg-de vries equation: A completely integrable hamiltonian system. *Functional Analysis and Its Applications*, 5(4):280–287, 1971.

[147] V. E. Zakharov and S. V. Manakov. On the complete integrability of a nonlinear schrödinger equation. *Theoretical and Mathematical Physics*, 19(3):551–559, 1974.

[148] Leon Armenovich Takhtadzhyan and Lyudvig Dmitrievich Faddeev. Essentially nonlinear one-dimensional model of classical field theory. *Theoretical and Mathematical Physics*, 21(2):1046–1057, 1974.

[149] P. Deift and E. Trubowitz. Inverse scattering on the line. *Communications on Pure and Applied Mathematics*, 32(2):121–251, 1979. doi: https://doi.org/10.1002/cpa.3160320202. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/cpa.3160320202.

[150] Clifford S. Gardner. Korteweg-de vries equation and generalizations. iv. the korteweg-de vries equation as a hamiltonian system. *Journal of Mathematical Physics*, 12(8):1548–1551, 1971.

[151] Ludwig D. Faddeev and Leon A. Takhtajan. *Hamiltonian Methods in the Theory of Solitons*, pages 471–522. Springer, 2007. ISBN 978-3-540-69969-9. doi: 10.1007/978-3-540-69969-9_7. URL https://doi.org/10.1007/978-3-540-69969-9_7.

[152] P. G. Drazin and R. S. Johnson. *Solitons: An Introduction*, page 89–126. Cambridge Texts in Applied Mathematics. Cambridge University Press, 2nd edition, 1989. doi: 10.1017/CBO9781139172059.006.

[153] Hermann Flaschka. On the toda lattice. ii: inverse-scattering solution. *Progress of Theoretical Physics*, 51(3):703–716, 1974.

[154] Y. Nogami and F. M. Toyama. Supersymmetry aspects of the dirac equation in one dimension with a lorentz scalar potential. *Physical Review A*, 47(3):1708, 1993.

[155] Gerald V. Dunne and Michael Thies. Transparent dirac potentials in one dimension: The time-dependent case. *Physical Review A*, 88(6):062115, 2013.

[156] F. Correa and V. Jakubský. Twisted kinks, dirac transparent systems, and darboux transformations. *Phys. Rev. D*, 90:125003, Dec 2014. doi: 10.1103/PhysRevD.90.125003. URL https://link.aps.org/doi/10.1103/PhysRevD.90.125003.

[157] Gerard Queraltó, Mark Kremer, Lukas J Maczewsky, Matthias Heinrich, Jordi Mompart, Verònica Ahufinger, and Alexander Szameit. Topological state engineering via supersymmetric transformations. *Communications Physics*, 3(1):1–8, 2020.

[158] Vyacheslav Spiridonov and Alexei Zhedanov. Discrete reflectionless potentials, quantum algebras, and q-orthogonal polynomials. *Annals of physics*, 237(1):126–146, 1995.