A Discrete Fourier Transform on Lattices with Quantum Applications

(full version on arXiv: 1703.02515)

Lior Eldar[*] Peter W. Shor[†]

April 5, 2017

Abstract

In this work, we introduce a definition of the Discrete Fourier Transform (DFT) on Euclidean lattices in $\mathbb{R}^n$, that generalizes the n-th fold DFT of the integer lattice $\mathbb{Z}^n$ to arbitrary lattices. This definition is not applicable for every lattice, but can be defined on lattices known as Systematic Normal Form (SysNF) introduced in [ES16]. Systematic Normal Form lattices are sets of integer vectors that satisfy a single homogeneous modular equation, which itself satisfies a certain number-theoretic property. Such lattices form a dense set in the space of n-dimensional lattices, and can be used to approximate efficiently any lattice. This implies that for every lattice L a DFT can be computed efficiently on a lattice near L.

Our proof of the statement above uses arguments from quantum computing, and as an application of our definition we show a quantum algorithm for sampling from discrete distributions on lattices, that extends our ability to sample efficiently from the discrete Gaussian distribution [GPV08] to any distribution that is sufficiently "smooth". We conjecture that studying the eigenvectors of the newly-defined lattice DFT may provide new insights into the structure of lattices, especially regarding hard computational problems, like the shortest vector problem.

1 Introduction

The Fourier Transform is ubiquitous in the study of lattices in mathematics, and in recent years has led to breakthroughs in our understanding of the complexity of lattice problems [AR05, Reg09]. The Fourier Transform on Euclidean lattices is usually associated with the Fourier series of lattice-periodic functions: Let $L \subseteq \mathbb{R}^n$ denote some full-rank n-dimensional lattice, $L = \mathrm{Span}_{\mathbb{Z}}(B)$, where $B \in GL(n, \mathbb{R})$. Consider the set of bounded complex-valued continuous functions $f : \mathbb{R}^n \to \mathbb{C}$ that are periodic in L, i.e.

$$\forall x \in \mathbb{R}^n, z \in L, \quad f(x) = f(x+z).$$

Then the Fourier series of f, $\hat{f} : L^* \mapsto \mathbb{C}$, supported on the dual lattice L^* is defined as follows:

$$\forall z \in L^*, \quad \hat{f}(z) := \frac{1}{\det(B)} \cdot \int_{\mathcal{P}(L)} f(x) e^{-2\pi i \langle x,z \rangle} dx,$$

where $\mathcal{P}(L)$ is the basic parallelotope of the lattice defined by the image of $[0,1)^n$ under B. Hence, in this respect, the FT on n-dimensional lattices is defined as the n-dimensional generalization of the Fourier Series of functions defined on the unit interval.

[*] Center for Theoretical physics, MIT

[†] Department of Mathematics and Center for Theoretical physics, MIT

The Discrete Fourier Transform (DFT) of a sequence of N complex numbers $X_0, \ldots, X_{N-1}$ is defined as

$$\forall k \in \mathbb{Z}_N \quad \hat{x}_k = \sum_{z=0}^{N-1} X_z e^{-2\pi i x \cdot z / N}.$$

It is a map between discrete sequences that can be thought of as a discretization of the Fourier Transform to regularly spaced-grids in the following sense: the Fourier-Transform of a function f that is periodic on the interval $[0, N] \subseteq \mathbb{R}$, sampled at integer points $[0, \ldots, N-1]$, corresponds to the DFT of the sequence derived by sampling f at the points $[0, \ldots, N-1]$. The DFT has proven to be extremely useful in both engineering and computer science.

Given the interpretation of the DFT as a regularly-spaced sampling of the continuous FT it is then natural to consider whether one can define the DFT on an arbitrary lattice. Specifically, it would be desirable to have a definition of the DFT which inherits the inner-product between lattice vectors. Such is the case for the trivial lattice $\mathbb{Z}^n$: for any integer N one can consider the ring of integers modulo N, $\mathbb{Z}_N$ and define for any function $f : \mathbb{Z}_N^n \to \mathbb{C}$:

$$\forall x \in \mathbb{Z}_N^n \;\; \hat{f}(x) = \sum_{z \in \mathbb{Z}_N^n} f(z) e^{-2\pi i \langle x, z \rangle / N}.$$

In this case, the DFT at each point corresponds to sampling the continuous FT of f at the points of $L = \mathbb{Z}^n$. Furthermore, this definition corresponds to the Fourier Transform of the finite group $\mathbb{Z}_N^n$ with entry-wise addition modulo N.

We would like to have this behavior for any arbitrary lattice $L \subseteq \mathbb{R}^n$. But to relate to finite groups we need to relate to a finite subset of L. Let $N = \det(L)$. Then L is periodic in N in each direction, i.e. for any $v \in L$ we have $v + Ne_i \in L$ for all $i \in [n]$. Therefore, it is sufficient to consider the finite lattice L_N as an additive subgroup of the finite vector space $\mathbb{Z}_N^n$ with addition modulo N, instead of L as an additive subgroup of $\mathbb{R}^n$ with real addition. We define lattice DFT as follows:

Definition 1. ***Lattice DFT***
Let $L \subseteq \mathbb{R}^n$ be an n-dimensional integer lattice, $N = \det(L)$. A Discrete Fourier Transform of L (DFT) is a Fourier Transform of the finite group L_N, for which the characters $\chi_x(z)$ for $x, z \in L_N$ satisfy:

$$\forall x, z \in L_N \;\; \chi_x(z) = e^{-2\pi i \langle x, z \rangle / N}.$$

and so the main question is

Question 1. *Does there exist a lattice DFT for every lattice?*

A natural place to look for a DFT is in the context of finite Abelian groups. Given a lattice L with determinant $N = \det(L)$, one can restrict his attention to the set of lattice points with entries in $\mathbb{Z}_N$, and consider this as a finite sub-group L_N of the cube $\mathbb{Z}_N^n$ with entry-wise addition modulo N. Since L_N is a finite Abelian group then by the fundamental theorem of classification of finite Abelian groups L_N is isomorphic to a product of primary cyclic groups. Hence, one can define the DFT of L_N by considering the DFT of the individual prime-power factors $\mathbb{Z}_p^k$ for prime p and integer k. Yet, one can check that generically, the resulting DFT would have an inner-product which is very different from the integer inner-product modulo N between lattice points.

In this work we answer the question above by showing that one can define the DFT for a certain dense set of lattices. Furthermore, we show that this DFT can be computed efficiently, albeit with a quantum computer. This dense set of lattices corresponds to lattices of a special form called *Systematic Normal Form* (or SysNF for short) introduced by Eldar and Shor in [ES16]:

Definition 2. ***Systematic Normal Form (SysNF)*** *[ES16]*

An integer matrix B is said to be SysNF if $B_{i,i} = 1$ for all $i > 1$, $B_{i,j} = 0$ for all $i > 1, i \neq j$, and $B_{1,1} = N$ satisfies

$$\sum_{i>1} B_{1,i}^2 + 1 \neq 0(mod\ N). \tag{1}$$

Specifying only the non-zero entries of B - it can be written as:

$$B = \begin{bmatrix} N & b_2 & b_3 & \dots & b_n \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{bmatrix} \tag{2}$$

These lattices form a dense set in the space of lattices in terms of the Euclidean distance, in the sense that for every $\varepsilon > 0$ and arbitrary lattice L, there exists an efficiently computable linear map σ, a large integer T, and a SySNF lattice L' such that for every $x \in L$ $\sigma(x) \in L'$ and $\|x - \sigma(x)/T\| \leq \varepsilon \|x\|$.

By its definition, a SysNF lattice is the set of integer vectors that satisfy a certain homogeneous modular equation (modulo a number N) where, in addition, this equation satisfies an extra number-theoretic condition. Defining lattices as the set of solutions of modular equations is a def-facto standard in the study of lattices (see e.g. [Pei15]), especially in the context of random lattices due to Ajtai [Ajt96]. However, the extra number-theoretic condition in Equation 1 wasn't defined prior to [ES16] and, in fact, is used crucially to establish that such lattices have a DFT. We discuss this further in sub-section 1.1.

Our proof that DFT can be defined on SysNF lattices is quantum. Concretely, we provide a quantum circuit implementing the character map for each lattice point. To do this, we first define a quantum analog of the map above:

Definition. ***Quantum Fourier Transform on SysNF lattices***
Let $L \subseteq \mathbb{R}^n$ be a SysNF lattice, $N = \det(L)$. The Quantum Fourier Transform on L_N is defined for basis states as follows:

$$\forall x \in L_N, \mathcal{F}_{L,N}(|x\rangle) = \frac{1}{\sqrt{N^{n-1}}} \sum_{z \in L_N} e^{-2\pi i \langle x,z \rangle / N} |z\rangle. \tag{3}$$

The normalization by $\sqrt{N^{n-1}}$ follows from the fact that there are precisely N^{n-1} points in L_N. We then show that this map is unitary (and in particular, efficiently computable) thereby establishing that the $|L_N|$ characters $\chi_x(z) = e^{-2\pi i \langle x,z \rangle / N}$ for $x \in L_N$ are orthogonal, and hence form a complete set of inequivalent irreducible representations of L_N - i.e. a Fourier Transform of the group L_N.

Theorem 1. ***A Quantum Circuit for lattice DFT***
Given is a lattice $L = L(B)$, where B is an $n \times n$ SysNF matrix. There exists a quantum circuit Q of size poly(n)*, that implements $\mathcal{F}_{L,N}$. In particular, L can be assigned a lattice DFT.*

As an application of our new definition, the above circuit gives rise to an efficient way to sample from any discrete distribution on a lattice, for sufficiently "nice" functions:

Theorem 2. *(sketch) Let f be a complex-valued function on $\mathbb{R}^n$, and $L \subseteq \mathbb{R}^n$ some lattice, generated by matrix B. Suppose that $\mathcal{F}$, the FT of f, can be generated as a superposition on $\mathbb{Z}^n$*

$$\sum_{x \in \mathbb{Z}^n} f(x)|x\rangle$$

and $\mathcal{F}$ is approximately bounded in $\lambda_1(L^*)/2^{n/2}$ then one can approximately sample from the following discrete distribution efficiently quantumly:

$$\forall x \in L \quad \mathsf{P}(x) \propto |f(x)|^2.$$

1.1 Discussion and Previous Work

To the best of our knowledge, a Discrete Fourier Transform that inherits the Euclidean inner-product and generalizes the DFT of the integer lattice $\mathbb{Z}^n$ to arbitrary n-dimensional lattices has not been defined before. The standard notion of the Fourier Transform on arbitrary n-dimensional lattices relates to the Fourier Series of lattice-periodic functions, and thus behaves quite differently - and in particular, is not a map from the lattice onto itself. Our definition of DFT for lattices cannot be defined for general lattices. Luckily, however, SysNF lattices form an efficiently computable dense group in the space of lattices, hence for every lattice, there exists a "nearby" efficiently-computable lattice for which the DFT can be defined.

The Discrete Fourier Transform we define can be viewed as a Fourier Transform of the discrete group $L_N \subseteq \mathbb{Z}_N^n$ with entry-wise addition modulo N, where the set of irreducible representations used are the 1-dimensional characters of the cyclic group of order N. We note that given any lattice L with $\det(L) = N$ one can define a Fourier Transform on the finite group L_N using the Fundamental Theorem of Finite Abelian Groups, but in general this does not give rise to the DFT with the inner-product between lattice points as in our definition. Hence, our claim is not that perturbing a lattice to SysNF is necessary to define a finite-group FT, but rather that perturbing it is sufficient to define a DFT - a FT that inherits the inner-product over integer vectors modulo N. As an added bonus, the DFT on SysNF lattices can be computed on a quantum computer in time which is polynomial in the dimension of the lattice.

Perturbing lattices to nearby lattices with special structure is not new and has been investigated by Paz and Schnorr in [PS87]. In that reduction, one perturbs a given lattice L to a nearby lattice L' in which the quotient $\mathbb{Z}^n/L$ is cyclic. The authors then characterize a lattice L as the set of vectors satisfying a homogeneous modular equation if and only if the quotient $\mathbb{Z}^n/L$ is cyclic. Hence the Paz-Schnorr reduction reduces any lattice to the set of solutions of a homogeneous equation modulo some large integer N. However, the structure of the reduction generates lattices in which N does not generally satisfy our extra co-primality condition. Hence the lattices produced by the Paz-Schnorr reduction cannot be assigned a lattice DFT as in our case.

In terms of the quantum implementation of the Fourier Transform, we note that effectively, it is a reduction from the definition of the DFT on L_N to the standard DFT on $\mathbb{Z}^{n-1}$. That said, it is only because of the extra number-theoretic condition, namely that $\sum_{i>1} B_{1,i}^2 \neq (-1)(\text{mod } N)$ that such a reduction is possible. The quantum implementation of the DFT on the ring of integers modulo N is well-known by now [NC11], and has been studied for other groups as well [Bea97].

In terms of the sampling algorithm our result generalizes, in the quantum setting, the result of Gentry et al. [GPV08] to arbitrary distributions with "nice" FT's. In that result the authors showed how to sample from the discrete Gaussian distribution with a variance comparable to the length of the lattice basis $\|B\|$, and here we provide a quantum routine that can perform this task for essentially any distribution that can be "sampled quantumly". We note that one can also distill a quantum sampling routine from the work of Regev [Reg09], but the SysNF structure makes our scheme advantageous compared to that scheme: we can sample quantumly from functions which are not known to be accessible via the work of [Reg09].

Finally, the question of sampling from general distributions on lattices has been also investigated by Lyubashevsky and Wichs [LW15] in the context of cryptographic efficiency. There, the authors show how to sample classically from arbitrary distributions on lattices defined by a system of modular equations, but they also require the knowledge of a secret trapdoor in addition to the lattice basis, in order to do that.

1.2 Open Questions

We believe there are several important open questions that arise from our new definition, and its quantum implementation, that pertain to the problem of solving hard lattice problems. One such question is trying to characterize the eigenvectors of the lattice DFT unitary:

Question 2. *Let $L \subseteq \mathbb{R}^n$ be some SysNF lattice, and $\mathcal{F}_{L,N}$ denote its corresponding DFT. Find the eigenvectors of $\mathcal{F}_{L,N}$.*

The interest in the above question stems from the fact that using quantum phase estimation w.r.t. $\mathcal{F}_{L,N}$ and, say a randomly chosen quantum state, it may be possible to find such eigenvectors efficiently. On the other hand, it is known that the eigenvectors of the standard n-dim. DFT are Gaussian, up to multiplying by a Hermite polynomial. Hence it is possible that the eigenvectors of $\mathcal{F}_{L,N}$ are discrete Gaussian superpositions on L_N. Could it be that one of these eigenvectors is a Gaussian that is computationally "interesting"? say with variance $s = \text{poly}(n)$?

References

[Ajt96] M. Ajtai. Generating hard instances of lattice problems (extended abstract). pages 99–108, 1996. doi:10.1145/237814.237838.

[AR05] Dorit Aharonov and Oded Regev. Lattice problems in NP intersect coNP. *J. ACM*, 52(5):749–765, September 2005. doi:10.1145/1089023.1089025.

[Bab86] L. Babai. On Lovász' lattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986. doi:10.1007/BF02579403.

[Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–636, 1993.

[Bea97] Robert Beals. Quantum computation of fourier transforms over symmetric groups. In *Proceedings of the Twenty-ninth Annual ACM Symposium on Theory of Computing*, STOC '97, pages 48–53, New York, NY, USA, 1997. ACM. doi:10.1145/258533.258548.

[ES16] Lior Eldar and Peter W. Shor. The systematic normal form of lattices. 2016. URL: arxiv.org/abs/1604.07800.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, pages 197–206, New York, NY, USA, 2008. ACM. doi:10.1145/1374376.1374407.

[Iwa78] H. Iwaniec. On the problem of jacobsthal. *Demonstratio Mathematica*, 11(1):225–231, 1978.

[KB79] Ravindran Kannan and Achim Bachem. Polynomial algorithms for computing the smith and hermite normal forms of an integer matrix. *SIAM Journal on Computing*, 8(4):499–507, 1979. doi:10.1137/0208040.

[LW15] Vadim Lyubashevsky and Daniel Wichs. *Simple Lattice Trapdoor Sampling from a Broad Class of Distributions*, pages 716–730. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015. doi:10.1007/978-3-662-46447-2_32.

[NC11] Michael A. Nielsen and Isaac L. Chuang. Quantum computation and quantum information: 10th anniversary edition. 2011.

[Pei15] Chris Peikert. A decade of lattice cryptography. Cryptology ePrint Archive, Report 2015/939, 2015. http://eprint.iacr.org/2015/939.

[PS87] A. Paz and C. P. Schnorr. Approximating integer lattices by lattices with cyclic factor groups. pages 386–393, 1987. doi:10.1007/3-540-18088-5_33.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, September 2009. `doi:10.1145/1568318.1568324`.