Interesting Eigenvectors of the Fourier Transform

Interesting Eigenvectors of the Fourier Transform

Berthold K.P. Horn*

***Abstract*—It is well known that a function can be decomposed uniquely into the sum of an odd and an even function. This notion can be extended to the unique decomposition into the sum of *four* functions — two of which are even and two odd. These four functions are eigenvectors of the Fourier Transform with four different eigenvalues. That is, the Fourier transform of each of the four components is simply that component multiplied by the corresponding eigenvalue. Some eigenvectors of the discrete Fourier transform of particular interest find application in coding, communication and imaging. Some of the underlying mathematics goes back to the times of Carl Friedrich Gauss.**

***Index Terms*—Function decomposition, Fourier transform, Discrete Fourier transform, Coded apertures, Coded aperture imaging, Gaussian Integers, Eisenstein Integers, Legendre symbol, Legendre sequence, Legendre symbol sequence, Bi-level auto-correlation, Ideal auto-correlaton, Flat power spectrum, Periodic phase sequences.**

I. Background

A function f can be uniquely decomposed into a sum of an even component, f_e, and an odd component, f_o:

$$f = f_e + f_o \quad \text{with} \quad Rf_e = f_e \quad \text{and} \quad Rf_o = -f_o \tag{1}$$

where R is an operator that reverses a function, i.e. $(Rf)(x) = f(-x)$. Noting that $R(f_e + f_o) = f_e - f_o$, we can easily find the even and odd components using

$$f_e = (f + Rf)/2 \quad \text{and} \quad f_o = (f - Rf)/2 \tag{2}$$

We can rewrite this as $f_e = P_e f$ and $f_o = P_o f$, where

$$P_e = (I + R)/2 \quad \text{and} \quad P_o = (I - R)/2 \tag{3}$$

are operators that project a function into the subspaces of even and odd functions respectively, with I being the identity operator.

As behooves projection operators, $P_e^2 = P_e$ and $P_o^2 = P_o$, — which can be seen by noting that $R^2 = I$. R has exactly two eigenvalues, namely $+1$ and -1, since, from $R^2 = I$, we get the equation $\lambda^2 = 1$ for the eigenvalues. Note that each of the projection operators is degenerate since it maps vectors that lie in the other subspace to zero, and so must have a zero eigenvalue.

There is a subspace of even functions and a subspace of odd functions and any function can be uniquely decomposed into the sum of two functions, one from each of these two subspaces. With respect to the operator R, all even functions have eigenvalue $+1$ and all odd functions have eigenvalue -1.

* Department of Electrical Engineering and Computer Science, MIT and CSAIL, MIT, Cambridge, MA 02139, USA, bkph@csail.mit.edu

While we are here, note that,

$$F(f_e) = F(f_e)^* \quad \text{and} \quad F(f_o) = -F(f_o)^* \tag{4}$$

if f_e and f_o are even and odd respectively, where F is the Fourier transform operator, and * denotes the complex conjugate. All this is well known. Now for the fun part.

II. Splitting a function into four components

First, recall that the inverse Fourier transform is pretty much the same as the forward Fourier transform, *except* for a sign change of the product in the exponent (for convenience we use the *unitary* Fourier transform here). As a result, if, "by mistake," we apply the forward Fourier transform, instead of the inverse Fourier transform to Ff, then, instead of getting back f, we get f *reversed*, i.e. $F(Ff) = F^2 f = Rf$. It follows from $F^2 = R$ that $F^4 = R^2 = I$. Hence F has exactly four eigenvalues, namely $+1$, -1, $-i$, and $+i$, since from $F^4 = I$ we get the equation $\lambda^4 = 1$ for the eigenvalues. Again, this is known [1], [2], although, the idea of eigenvalues of the Fourier transform may seem at bit odd at first.

Following the example of decomposition into even and odd components above, we note that there are four subspaces, each containing functions with one of these four eigenvalues w.r.t. F. Thus we might look for a unique decomposition of a function f into four components, one from each of the four subspaces:

$$f = f_{+1} + f_{-1} + f_{-i} + f_{+i} \tag{5}$$

with $Ff_{+1} = f_{+1}$, $Ff_{-1} = -f_{-1}$, $Ff_{-i} = -if_{-i}$, and $Ff_{+i} = if_{+i}$. We note that

$$F(f_{+1} + f_{-1} + f_{-i} + f_{+i}) = f_{+1} - f_{-1} - if_{-i} + if_{+i} \tag{6}$$

so that, if it should turn out that we could find this decomposition cheaply, then we would have a *really* cheap way of computing the Fourier transform!

III. Finding the four components

Using this last equation, and what we know about the properties of R and the even and odd components, we can show that the four components are given by:

$$f_{+1} = (f_e + Ff_e)/2, \quad \text{and} \quad f_{-1} = (f_e - Ff_e)/2, \tag{7}$$

$$f_{-i} = (f_o - iFf_o)/2, \quad \text{and} \quad f_{+i} = (f_o + iFf_o)/2, \tag{8}$$

or

$$f_{+1} = P_{+1} f \quad \text{and} \quad f_{-1} = P_{-1} f, \tag{9}$$

$$f_{-i} = P_{-i} f \quad \text{and} \quad f_{+i} = P_{+i} f, \tag{10}$$

where

$$P_{+1} = (I + F)(I + R)/4,\ P_{-1} = (I - F)(I + R)/4, \quad (11)$$

$$P_{-i} = (I - iF)(I - R)/4,\ P_{+i} = (I + iF)(I - R)/4, \quad (12)$$

are operators that project a function into the four subspaces. Again, as required of projection operators, $P_{+1}^2 = P_{+1}$, $P_{-1}^2 = P_{-1}$, $P_{-i}^2 = P_{-i}$, and $P_{+i}^2 = P_{+i}$, as can easily be verified using $F^2 = R$ and $R^2 = I$. Also note that,

$$P_e = P_{+1} + P_{-1} \quad \text{and} \quad P_o = P_{+i} + P_{-i} \qquad (13)$$

and that all four components of a function can be computed using a *single* Fourier transform (since $FR = F^*$).

Perhaps somewhat surprisingly, the four projections of a real function are also real, as can be seen by inspecting the projection operators. For example, in applying P_{+1}, only the even component of the function is used and the transform of an even (real) function is real (and even). Similarly, in applying P_{+i}, only the odd component of the function is used and the transform of an odd (real) function is imaginary (and odd). Multiplying by i turns the imaginary partial result into real. And so on.

There remains one issue, which is what to call these subspaces. In analogy with the "even" and "odd" subspaces, the following names are proposed "recto even," ($\lambda = +1$), "verso even," ($\lambda = -1$), "recto odd" ($\lambda = -i$), and "verso odd," ($\lambda = +i$). Suggestions for more intuitive names would be appreciated!

Finally, with regret, but no real suprise, we note then that the obvious implementation of the required projection operators involves Fourier transforms! So apparently the "super cheap" Fourier transform based on the four-way decomposition of a function is not a viable approach.

IV. Discrete Version

A particular instance of the general analysis above may help illuminate these ideas. Consider discrete sequences of period n. In this case, R is an $n \times n$ symmetric matrix with $R_{i,j} = \delta_{i+j-(n-1)}$ — that is, with 1's along the "anti-diagonal," and 0's elsewhere. It is easy to see that $R^2 = I$. We have already shown that the eigenvalues of R are $+1$ and -1, but what about the eigenvectors? For a symmetric $n \times n$ matrix we expect to be able to find n independent eigenvectors. But here we only have 2 distinct eigenvalues, so the eigenvectors are not uniquely defined. But we can easily find *some* basis for each of the two subspaces.

For the even subspace we can, for example, use the basis $\{e_i\}$, with $e_0 = [1, 0, 0 \ldots 0, 0]$, $e_1 = [0, 1, 0 \ldots 0, 1]$, $e_2 = [0, 0, 1 \ldots 1, 0]$, etc. For the odd subspace we can use the basis $\{o_i\}$, with $o_1 = [0, 1, 0 \ldots 0, -1]$, $o_2 = [0, 0, 1 \ldots -1, 0]$, etc. (note that there are slight differences between the case when n is even and when n is odd, and that the two subspaces do *not* have the same dimensions). There are, of course, an infinite number of alternate bases for the two subspaces.

Moving on to the (unitary) discrete Fourier transform (DFT) now, we see that F is an $n \times n$ symmetric matrix, with $F_{k,l} = (1/\sqrt{n})e^{-2\pi i\ kl/n}$ for $k = 0$ to $n - 1$ and $l = 0$ to $n-1$. We have already shown that there are four eigenvalues, but what about the eigenvectors?

Here again, it may seem odd that the DFT should have eigenvectors, but note that the matrix F is orthonormal ($(F^T)^* F = I$) and so represents a kind of "rotation" of an n dimensional space — with the inverse transform ($F^{-1} = F^*$) performing a counter-rotation. This view of the DFT perhaps makes the notion of eigenvectors appear less surprising.

While F has a full complement of n eigenvectors because it is unitary, the eigenvectors are not uniquely determined, since there are only four distinct eigenvalues (the number of eigenvectors corresponding to each eigenvalue depends on the congruence class of n mod 4 [1]). Several sets of basis vectors have been investigated based on different criteria for what make "nice" bases. Some have been motivated by the notion of a "fractional" DFT [3], [4]. The idea is that if the DFT represents a rotation, then one should be able to consider a smaller rotation that, say, goes only half way, but that, when repeated, yields the full rotation.

V. Detailed example of discrete case

To explore the notion of the projection operators that yield the four components, consider, as a specific example, the case $n = 4$, where

$$F = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \qquad (14)$$

a symmetric matrix with characteristic equation

$$\lambda^4 - (1 + i)\lambda^3 - (1 - i)\lambda^2 + (1 + i)\lambda - i = 0 \qquad (15)$$

or $(\lambda - 1)^2(\lambda + 1)(\lambda - i) = 0$. (Note that, in this particular case, the root $\lambda = -i$ is "missing" and that the root $\lambda = +1$ is repeated). We construct

$$P_{+1} = \frac{1}{4}\begin{pmatrix} 3 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 3 & -1 \\ 1 & 1 & -1 & 1 \end{pmatrix} \qquad (16)$$

Here P_{+1} directly provides two eigenvectors for the "recto even" subspace, namely $[3, 1, 1, 1]^T$ and $[1, 1, -1, 1]^T$ (Note that P_{+1} only has rank two because the third column equals the difference of the first and twice the second, and the fourth column is the same as the second). Next,

$$P_{-1} = \frac{1}{4}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix} \qquad (17)$$

Here P_{-1} yields the eigenvector $[1, -1, -1, -1]^T$ for the "verso even" subspace. Further

$$P_{+i} = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix} \qquad (18)$$

where P_{+i} yields the eigenvector $[0, 1, 0, -1]^T$ for the "verso odd" subspace. Finally,

$$P_{-i} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{19}$$

For $n = 4$, F does not have the eigenvalue $-i$, so there is no "recto odd" subspace and indeed the projection matrix P_{-i} is zero. Note that all four of the projection matrices are real, as expected, and also symmetrical. For $n > 4$, all four subspaces exist. As can be seen, in general the four subspaces do not have the same dimensions.

As an exercise, the reader may wish to work out the details for the case $n = 3$, where the three eigenvalues are $+i$, -1, and $+1$, with no repeated roots.

VI. Eigenvectors of the DFT with particularly interesting properties

While there are an inifinite number of eigenvectors of each of the four subspaces, some are of particular interest. Consider, for example, eigenvectors that have components that are restricted to take on the values $+1$ and -1 (except for a 0 for the 0-th component). Exhaustive search for small n yields some candidates. For example, the even sequence

0	+1	−1	−1	+1

for $n = 5$ has the (real) transform

0	+1	−1	−1	+1

while the (odd) sequence

0	+1	+1	−1	+1	−1	−1

for $n = 7$ has the (purely imaginary) transform

0	$-i$	$-i$	$+i$	$-i$	$+i$	$+i$

It is perhaps surprising that a sequence composed merely of $+1$'s and -1's could be an eigenvector. It turns out that this is not just a curiosity, but has important practical implications. The power spectrum of such a sequence is flat (except for the zero frequency, or DC, term, which we shall silently ignore from now on), since the power spectrum is the magnitude squared of the transform, and here, the transform is the sequence itself multiplied by a (possibly complex) eigenvalue of unit magnitude.

Sequences with flat power spectrum are of particular interest in coding and communications. One reason is that if a signal is convolved with such a waveform (on the sending end), then deconvolution (on the receiving end) amplifies noise equally at all frequencies, because the deconvolution filter (inverse of the coding filter) also has a flat spectrum. If a coding filter is used that does *not* have a flat spectrum, then the decoding filter must have a higher response at frequencies were the coding filter has low response. This means that noise at some frequencies will be amplified more than at others, leading to an overall loss in signal-to-noise performance (for fixed signal power).

The decoding sequence here has the same spectrum as the original coding sequence, except that the phases are all reversed (so that the product of the transforms of the coding and decoding sequences has the same value at all frequencies).

It is well known that impulses and chirps have flat power spectra. These waveforms are widely used in radar, for example. Here we find another class of waveforms that have flat power spectra. Such waveforms are used, for example, in cell phone communication and coded aperture imaging.

VII. Ideal Bi-level Auto-correlation

An equivalent way of understanding the above is to consider the auto-correlation of such a sequence with itself. Correlation with a sequence corresponds to convolution with that sequence reversed. Reversing a sequence flips the sign of the phases in the Fourier transform. Convolution of two sequences corresponds to multiplication of their transforms (scaled by $\sqrt{n}$ in the case of the unitary DFT). So we find that the transform of the auto-correlation here is the same for all frequencies (except for the zero frequency term). Inverse transforming, we obtain a large value for zero shift and a constant (small) value for all other shifts. Thus these special sequences have the so-called bi-level auto-correlation feature. As a result, the sequence itself can be used effectively in decoding.

For such a sequence $\{l_k\}$ of period n we have

$$\sum_{k=0}^{n-1} l_k l_{k+m} = n\,\delta_m - 1 \tag{20}$$

where indices are treated $\bmod n$ (see Appendix B for a proof). It is illuminating to correlate the sample sequences shown above for $n = 5$ and $n = 7$ with themselves to check this property. It is remarkable that sequences with this property exist.

A small modification is needed for some practical applications of these sequences. A coded aperture used in imaging with radiation that cannot be refracted or reflected, for example, can only have a hole in a mask, or no hole, at each point on a regular grid of points [5], [6]. So incoming radiation intensity can in effect be multiplied by $+1$ (open hole) or 0 (no hole) — but not by -1. We can arrive at a usable hole pattern by picking only the $+1$'s (or the -1's for that matter) in the sequence to drill a hole. Equivalently, we can add 1 to the sequence and divide the result by 2, to get a binary pattern $\{l'_k\}$, where $l'_k = (l_k + 1)/2$, which *can* be represented by holes (1's) and blocked areas (0's) in a mask (except for the zeroth term of the sequence, which we won't get into here).

The addition of a constant to all elements of the sequence adds an impulse at zero frequency to the transform and so does modify the result a bit. Such binary sequences still have the ideal bi-level auto-correlation property (now something like $(n\,\delta_m - 1 + n)/4$). That is, there is one (large) correlation value for zero shift, and another (smaller) value for *all* other shifts — although now the "smaller" value is about half the size of the larger one, rather than very much smaller. In deconvolution this non-zero value leads to a constant background "pedestal" which can be subtracted

out after deconvolution. The constant background is not without disadvantage, however, since, in practice, measurements are corrupted by noise, and so the "constant" background won't be quite constant, and the signal-to-noise ratio will be adversely affected by this compromise forced on us by our inability to drill "negative holes."

VIII. Generating eigenvectors with special properties

Aside from brute force search, is there some systematic way of finding eigenvectors with these special properties?

One way is to exploit quadratic residues from number theory. A number n is a quadratic residue $\bmod p$ if there exists a number i such that $i^2 \equiv n \mod p$. When no such number exists, then n is a quadratic non-residue $\bmod p$. We can find all the quadratic residues $\bmod p$ simply by taking all numbers from 0 to $(p-1)$ (actually 0 to $(p-1)/2$ suffice), squaring them, and taking the result $\bmod p$. By convention, 0 is not considered a quadratic residue (while 1 is obviously always a quadratic residue, for all p). It is easy to see that the quadratic residues from a group, and that the non-residues form the coset of that group.

If one finds the quadratic residues for $p = 5$ and $p = 7$, and puts a $+1$ in the sequence for every quadratic residue and -1 for every quadratic non-residue, one obtains the sample eigenvector sequences presented above. This construction can be written using the Legendre symbol:

$$\left(\frac{n}{p}\right)_2 = \begin{cases} 0 & \text{when } n \text{ is } 0 \bmod p \\ +1 & \text{when } n \text{ is a quadratic residue} \\ -1 & \text{when } n \text{ is a quadratic non-residue} \end{cases} \quad (21)$$

Then the special sequences of length p that we are interested in are just $\{l_n\}$, where l_n is the Legendre symbol.

At this point we have almost enough to try and formally prove that such sequences are eigenvectors of the DFT when p is a prime, and that they have the ideal bi-level auto-correlation property. One way to determine the value of the Legendre symbol that is useful in proving such results is Euler's criterion

$$\left(\frac{n}{p}\right)_2 \equiv n^{\frac{p-1}{2}} \bmod p \quad (22)$$

The value of the expression on the right will always be 0, $+1$, or -1 if we pick the residue of smallest magnitude (rather than using a residue in the range 0 and $p-1$). In this regard, note that $(p-1) \equiv -1 \mod p$.

Using these ideas, one can show that the eigenvalue is $+1$ when $p \equiv 1 \mod 4$ while the eigenvalue is $-i$ when $p \equiv 3 \mod 4$. Actually, it turns out that this is not quite as easy as it might appear at first sight. Fortunately Gauss (!) provided formulae for what are now called Gauss sums [7] in his work on "quadratic reciprocity" that are hepful in this endeavour. See Appendix A for proof of the eigenvector property of the Legendre symbol sequences. See Appendix B for proof of the bi-level auto-correlation property of the Legendre symbol sequences.

IX. Extensions to two dimensions

For imaging, coded aperture masks typically need to be two-dimensional [5], [6] The above ideas can be extended to two-dimensional patterns using Gaussian integers and Eisenstein integers. Gaussian integers are of the form $(a + bi)$, where a and b are "rational" integers (our usual numbers) and $i^2 = -1$. Gaussian integers correspond in a natural way to points on a square lattice in the plane. We can, of course, easily generalize the usual arithmetic operations on rational integers to those on Gaussian integers, including multiplication

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i \quad (23)$$

using $i^2 = -1$. The squared norm is the product with the conjugate, and so the squared norm of $(a + bi)$ is $a^2 + b^2$. "Units" are Gaussian integers of norm one ($+1$, -1, $-i$, and $+i$ — i.e. powers of i).

Gaussian primes are Gaussian integers that cannot be decomposed into products of Gaussian integers — other than products involving units. Gaussian integers have many of the properties of ordinary integers, such as being uniquely decomposable into products of Gaussian primes (where "unique" means ignoring multiplication by units). As a result, we can use Euler's criterion to generalize the Legendre symbol, customarily defined only in terms of "rational" integers, to work with Gaussian integers. We can then generate doubly periodic patterns of $+1$'s, -1's (and occasional 0's) on a square grid in the plane.

Hexagonal lattices have certain advantages over square lattices. We can develop patterns for hexagonal lattices using a similar approach, just starting with Eisenstein integers instead of Gaussian integers. Eisenstein integers are of the form $(a + b\omega)$, where $\omega^3 = -1$, with $\omega \neq -1$. From $\omega^3 + 1 = 0$ we obtain $(\omega + 1)(\omega^2 - \omega + 1) = 0$, and, because $\omega \neq -1$, we find $\omega^2 = \omega - 1$.

Eisenstein integers correspond in a natural way to points on a hexagonal lattice in the plane. Again, arithmetic operations on rational integers can be generalized to Eisenstein integers. Multiplication can be written

$$(a + b\omega)(c + d\omega) = (ac - bd) + (ad + bd + bc)\omega \quad (24)$$

using $\omega^2 = -1 - \omega$. Conjugation needs to be defined using $(a + b\omega)^* = (a + b) - b\omega$ and so the squared norm of $(a + b\omega)$ is $a^2 + ab + b^2$. Again, units have norm one and here are ω, $-\omega^*$, -1, $-\omega$, $+\omega^*$, and $+1$ (i.e. powers of ω).

We can use Euler's criterion to generalize the Legendre symbol to Eisenstein integers using the above arithmetic operations. Consequently we can generate doubly periodic patterns of $+1$'s, -1's (and occasional 0's) on a hexagonal grid in the plane.

X. Fourier transforms of two dimensional patterns

When we compute the Fourier transforms of the two-dimensional patterns described above, we find that they once again resemble the patterns themselves! First, being discrete and periodic, the transform will be periodic and discrete (albeit generally *not* lined up with the spatial grid

itself). Then, the magnitude of the transform is constant (except for the zeros). Further, the pattern of phases matches the original pattern, except, they are reflected about a line through the origin (or equivalently, mirror image reversed and rotated). So they may be considered "eigenvectors" of the two-dimensional Fourier transform, with the "eigenvalue" now being a complex scale factor *and* a reflection in the plane.

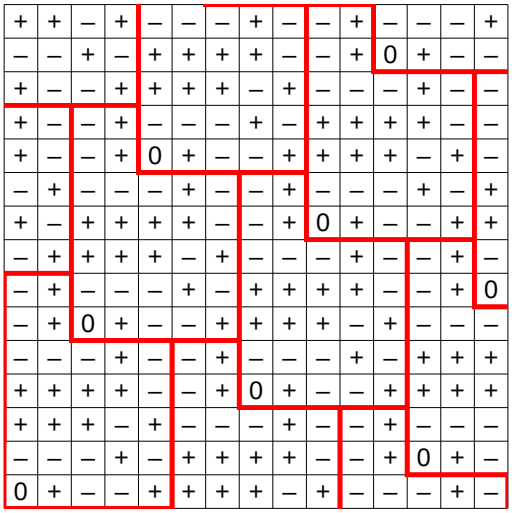

Fig. 1. Doubly periodic pattern with a basic repeating pattern containing $p = 29$ ($p = 5^2 + 2^2$) points.

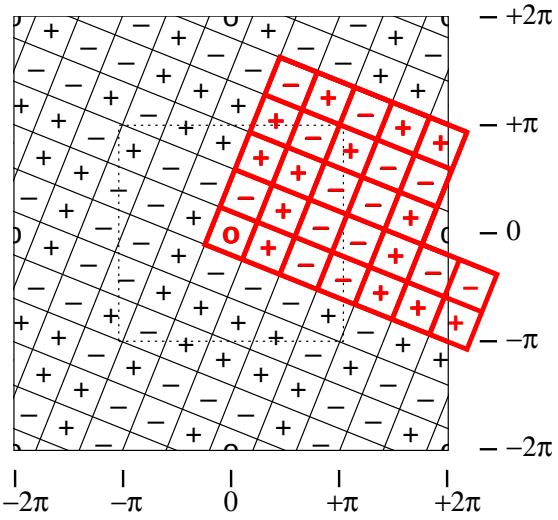

Fig. 2. Fourier transform of the doubly periodic pattern, with basic repeating pattern outlined. The L-shaped region is a reflection of the basic repeating pattern in Fig. 1.

XI. Extension to lower fill factors

Half the numbers from 1 to $p-1$ are quadratic residues and half are not, so a coded aperture mask made using the method described above will be about half holes and half blocked areas. The fraction of open holes is called the fill factor, f say, and is about 50% for this method of

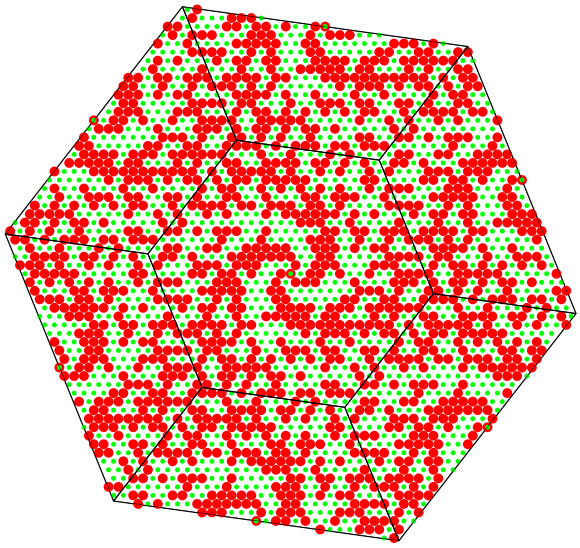

Fig. 3. Doubly periodic pattern with a basic repeating pattern containing $p = 643$ ($p = 18^2 + 18 \times 11 + 11^2$) points (red dot $+1$, green dot -1). The fill factor is 322/643 or about 50.07%.

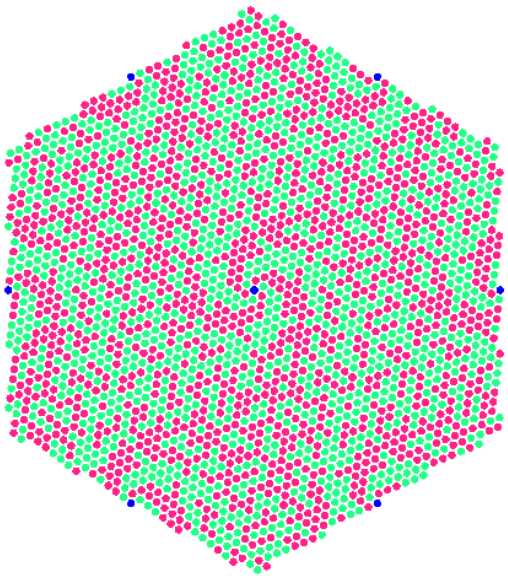

Fig. 4. Fourier transform of the doubly periodic pattern, with color indicating phase. The phase pattern is a reflection of the mask pattern in the spatial domain, shown in Fig. 3.

generating coded patterns. This means that the background pedestal described above is rather large and its deliterious effect on the signal-to-noise ratio significant.

One can do better with lower fill factor, for, while the signal is proportional to the fill factor, f, the background pedestal is proportional to the fill factor squared, f.[2] That is, even as the signal is reduced with lower fill factors, the signal-to-noise ratio (or more precisely contrast-to-noise ratio) may be improved with lower fill factors. But do patterns with lower fill factor exist that have the ideal bi-level auto-correlation properties?

The answer is in the affirmative. For example, for certain values of p, bi-quadratic residues — where we replace

squaring with raising to the fourth power in the above — have only about 25% fill factor and have the desired auto-correlation property. It is possible to show that, in this case, the bi-quadratic residues form a group, and that this group has *three* cosets.

These extensions can be analysed using a generalization of the Legendre symbol to also include the power to which the number is to be raised (here the fourth). We can try and generalize Euler's criterion using the definition

$$\left(\frac{n}{p}\right)_4 \equiv n^{\frac{p-1}{4}} \bmod p \tag{25}$$

In this case, the result can take on *four* values (rather than just $+1$ and -1). The sets defined by the four different values correspond to the bi-quadratic residue group and its three cosets. As an example, here is the result for $p = 5$:

0	$+1$	$+2$	-2	-1

Now $(+2)^2 \equiv -1 \bmod 5$ and $(-2)^2 \equiv -1 \bmod 5$, so we can think of $+2$ and -2 as square roots of -1. Replacing them with $+i$ and $-i$, we obtain the sequence

0	$+1$	$+i$	$-i$	-1

In this fashion we obtain periodic sequences consisting of $+1$'s, -1's, $-i$'s, and $+i$'s (instead of just $+1$'s and -1's).

Sequences defined by the above generalization of the Euler criterion, suprisingly, still have the bi-level auto-correlation property — as long as we take correlation of two complex sequences to mean addition of products of terms from one sequence with the *complex conjugate* of corresponding terms from the other sequence. For a sequence of period p, the auto-correlation for zero shift is $(p-1)$, while it is -1 for all other shifts, as before.

These sequences also have a kind of eigenvector property w.r.t the DFT. Namely, the DFT of the sequence equals the complex conjugate of the sequence multiplied by a complex factor of magnitude one (i.e. no longer just $+1$ or $-i$).

For practical applications we typically need a real binary sequence. These can be obtained by considering all positions where the residue computed in this fashion have the same value, e.g. $+1$. Unfortunately, while quadratic residue patterns with the bi-level auto-correlation property are ubiquitous, bi-quadratic patterns with this property are rarer: the prime p has to be of the form $16k(k+1)+5$ or $16k(k+1)+13$ for some integer k.

Octic residue patterns have only about 12.5% fill factor, which is even better from a signal-to-noise point of view. The octic residues form a group, and there are seven cosets of that group. If we try to generalize Euler's criterion as

$$\left(\frac{n}{p}\right)_8 \equiv n^{\frac{p-1}{8}} \bmod p \tag{26}$$

we obtain a result that can take on eight values. These correspond to the octic residue group and its seven cosets. As an example, here is the first half of the result for $p = 17$:

0	$+1$	$+4$	-8	-1	$+8$	$+2$	-2	-4

(the second half is the same sequence in reverse order, since this sequence is even).

Now $(+4)^2 \equiv -1 \bmod 17$ and $(-4)^2 \equiv -1 \bmod 17$, so we can think of $+4$ and -4 as the two square roots of -1. Further, $(+2)^4 \equiv -1 \bmod 17$ and $(-2)^4 \equiv -1 \bmod 17$, $(+8)^4 \equiv -1 \bmod 17$ and $(-8)^4 \equiv -1 \bmod 17$, so we can think of $+2$, -2, $+8$ and -8 as the four fourth roots of -1. If we let $w = (1+i)/\sqrt{2}$, then $w^2 = +i$, $(w^*)^2 = -i$. This leads to an even sequence, the first half of which is:

0	$+1$	$+i$	$-w^*$	-1	$+w^*$	$+w$	$-w$	$-i$

The result can be called a "phase sequence", a periodic sequence of complex values of unit magnitude.

What may appear to be a somewhat *ad hoc* process can be formalized by noting that the eight values themselves from a group that can be generated from a primitive root. In this example, 2 is a primitve root (while 1 and 4 are not), and $2^0 \equiv +1$, $2^1 \equiv +2$, $2^3 \equiv +8$, $2^4 \equiv -1$, $2^5 \equiv -2$, $2^6 \equiv -4$ and $2^7 \equiv -8$ (all taken mod 17 of course). If we assign w to the primitve root, then powers of that root can be assigned to all elements of the periodic sequence.

Sequences defined by the above generalization of the Euler criterion still have the bi-level auto-correlation property (as long as we define correlation of two complex sequences as above). Their DFT also is equal to the complex conjugate of the sequence itself multiplied by a complex constant of magnitude one.

Again, we can derive useful binary sequences from the periodic phase sequences using the technique described for bi-quadratic residues. Sadly, octic residue patterns obtained this way with the bi-level auto-correlation property are rare. The first few values of p for which octic residue patterns exist are $p = 73$, $p = 26,041$, $p = 104,411,704,393$, $p = 660,279,756,217$, $p = 160,459,573,394,847,767,113$. Now $p = 73$ is too small to be useful for imaging (one would have only 73 independent pixels in the resulting image), and noone plans to drill a coded aperture mask with a few hundred billion holes or more!

The above generalization of Euler's criterion can be used to define periodic phase sequences for arbitrary $m > 1$ for any odd prime p such that $p \equiv 1 \bmod m$. Such sequences can be one-dimensional or two-dimensional, using another generalization of the Euler criterion. Methods for mapping these periodic phase sequences to binary sequences, however, only work for particular values of the prime p, which depend on the value of m chosen.

XII. Conclusions

An arbitrary function can be decomposed into four functions, each being an eigenvector of the Fourier transform, the four differing in eigenvalue. This generalizes the decomposition into even and odd parts. Unfortunately, this does not appear to provide a cheap way for computing the Fourier transform.

The operators projecting a function into the four subspaces can be conveniently illustrated in the discrete case, where the DFT is a symmetric $n \times n$ matrix and periodic sequences can be treated as n-vectors. The four projection operators are degenerate symmetric real matrices.

The eigenvectors are not unique because there are only 4 distinct eigenvalues. Some eigenvectors with particularly interesting properties are used in coding, communications and coded aperture imaging. Number theory is an aid to generating sequences with these special properties. Extensions to two-dimensional patterns are possible using Gaussian integers and Eisenstein integers.

References

[1] J. H. McClellan and T. W. Parks, "Eigenvalues and eigenvectors of the discrete fourier transformation," *IEEE Transactions on Audio and Electroacoustics*, vol. 20, no. 1, pp. 66–74, 1972.

[2] F. A. Grünbaum, "The eigenvectors of the discrete fourier transform," *Journal of Mathematical Analysis Applications*, vol. 88, no. 2, pp. 355–363, 1982.

[3] D. H. Bailey and P. N. Swarztrauber, "The fractional fourier transform and applications," *SIAM Review*, vol. 33, pp. 389–404, 1991.

[4] L. B. Almeida, "The fractional fourier transform and time-frequency representations," *IEEE Transactions on Signal Processing*, vol. 42, no. 11, pp. 3084–3091, 1994.

[5] E. E. Fenimore and T. M. Cannon, "Coded aperture imaging with uniformly redundant arrays," *Applied Optics*, vol. 17, no. 3, pp. 337–347, February 1978.

[6] B. K. P. Horn, R. C. Lanza, J. T. Bell, and G. E. Kohse, "Dynamic reconstruction," *IEEE Transactions on Nuclear Engineering*, vol. 57, no. 1, pp. 193–205, February 2010.

[7] C. F. Gauss, *Untersuchungen über höhere Arithmetik*, 2nd ed., H. Maser, Ed. New York: Chelsea, 1965.

[8] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 2nd ed., A. Jeffrey and D. Zwillinger, Eds. New York: Academic Press, 1980.

Appendix A
The DFT of the Legendre symbol sequence

The unitary DFT $\{L_k\}$ of the Legendre symbol sequence $\{l_n\}$ is given by

$$L_k = \frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) e^{-i2\pi kn/p} \tag{27}$$

This can be rewritten as follows, given the definition of l_n, and noting in particular that $l_0 = 0$:

$$L_k = \frac{1}{\sqrt{p}} \sum_{n\in R} e^{-i2\pi kn/p} - \frac{1}{\sqrt{p}} \sum_{n\in N} e^{-i2\pi kn/p} \tag{28}$$

where R is the set of quadratic residues mod p, and N is the set of nonresidues (where we exclude 0 as is customary). If $k = 0$, the above sum is simply the difference between the number of quadratic residues and nonresidues lying between 1 and $(p-1)$. The difference is zero since there are as many quadratic residues as quadratic nonresidues. So $L_0 = 0$, which is not surprising given that the sum of the terms in the sequence $\{l_n\}$ is 0 (the zero frequency component is proportional to the sum of the elements of the sequence).

Now any number from 1 to $(p-1)$ is either in R or in N, so we can rewrite the sum in the alternate form

$$L_k = \frac{2}{\sqrt{p}} \sum_{n\in R} e^{-i2\pi kn/p} - \frac{1}{\sqrt{p}} \sum_{n\in R\cup N} e^{-i2\pi kn/p} \tag{29}$$

The set $R \cup N$ consists of all the numbers from 1 to $(p-1)$. Now if $k \neq 0$, then

$$\sum_{n=0}^{p-1} e^{-i2\pi kn/p} = 0 \tag{30}$$

Hence the same sum starting with $n = 1$, instead of 0, must equal -1. Consequently, for $k \neq 0$, the difference above can be written

$$L_k = \frac{2}{\sqrt{p}} \sum_{n\in R} e^{-i2\pi kn/p} + \frac{1}{\sqrt{p}} \tag{31}$$

Now the number n is in R iff there exists j such that $n \equiv j^2 \mod p$. This suggests replacing the sum over all $n \in R$ with a sum over j, and replacing n with j^2 in the terms being summed. In particular, the expression $j^2 \mod p$ for $j = 1, 2 \ldots (p-1)$ generates all of the quadratic residues mod p. Larger values of j do not produce new values since $(p+j)^2 \equiv j^2 \mod p$.

Actually, the above expression produces each quadratic residue exactly *twice* since $(p-j)^2 \equiv j^2 \mod p$. Hence the sum over $n \in R$ in the above expression corresponds to a sum over $j = 1$ to $(p-1)/2$ in

$$L_k = \frac{2}{\sqrt{p}} \sum_{j=1}^{(p-1)/2} e^{-i2\pi kj^2/p} + \frac{1}{\sqrt{p}} \tag{32}$$

The sum can be expanded using Euler's formula to yield

$$\sum_{j=1}^{(p-1)/2} \cos\frac{2\pi kj^2}{p} - i \sum_{j=1}^{(p-1)/2} \sin\frac{2\pi kj^2}{p} \tag{33}$$

We first compute L_1 and then show that L_k, for $k \neq 1$, equals either L_1 or $-L_1$.

From Gradshteyn and Ryzhik (1.344 [8]) we have

$$\sum_{k=0}^{n-1} \cos\frac{2\pi k^2}{n} = \frac{\sqrt{n}}{2}\left(1 + \cos\frac{n\pi}{2} + \sin\frac{n\pi}{2}\right) \tag{34}$$

$$\sum_{k=1}^{n-1} \sin\frac{2\pi k^2}{n} = \frac{\sqrt{n}}{2}\left(1 + \cos\frac{n\pi}{2} - \sin\frac{n\pi}{2}\right) \tag{35}$$

When n is odd, the cosine terms on the right equal 0. The sine terms equal $+1$ for $n \equiv 1 \mod 4$ or -1 for $n \equiv 3 \mod 4$. Further,

$$\cos\frac{2\pi(n-k)^2}{n} = \cos\frac{2\pi k^2}{n} \tag{36}$$

$$\sin\frac{2\pi(n-k)^2}{n} = \sin\frac{2\pi k^2}{n} \tag{37}$$

so the terms in the sum from $(n+1)/2$ to $(n-1)$ are equal to the terms from 1 to $(n-1)/2$ (in reverse order). So

$$2\sum_{k=1}^{(n-1)/2} \cos\frac{2\pi k^2}{n} + 1 = \begin{cases} \sqrt{n} & \text{for } n \equiv 1 \mod 4 \\ 0 & for n \equiv 3 \mod 4 \end{cases} \tag{38}$$

(note the change of lower limit in the sum), and

$$2\sum_{k=1}^{(n-1)/2} \sin\frac{2\pi k^2}{n} = \begin{cases} 0 & for n \equiv 1 \mod 4 \\ \sqrt{n} & \text{for } n \equiv 3 \mod 4 \end{cases} \tag{39}$$

Applying these results to the formula for L_k, with $k = 1$,

$$L_1 = \begin{cases} 1 & \text{for } p \equiv 1 \mod 4 \\ -i & \text{for } p \equiv 3 \mod 4 \end{cases} \tag{40}$$

To find L_k for $k > 1$, we distinguish two cases:

(1) When k is a quadratic residue mod p, then:

$$kj^2 \mod p \quad \text{for} j = 1, 2 \ldots (p-1) \tag{41}$$

generates the quadratic residues (twice, in various permuted orders depending on k), since $kj^2 \equiv (j'j)^2 \mod p$ for some j'. So in this case $L_k = L_1$.

(2) When k is *not* a quadratic residue mod p, then:

$$kj^2 \mod p \quad \text{for} j = 1, 2 \ldots (p-1) \tag{42}$$

generates the *non*-residues, since $kj^2 \not\equiv (j'j)^2 \mod p$ for any j'. So in this case the result can be obtained by taking the sum over *all* n and subtracting the sum over values of n that *are* quadratic residues mod p:

$$L_k = \frac{2}{\sqrt{p}} \left(\sum_{n=1}^{p-1} e^{-i2\pi n/p} - \sum_{j=1}^{(p-1)/2} e^{-i2\pi j^2/p} \right) + \frac{1}{\sqrt{p}} \tag{43}$$

The first of the two sums in the parenthesis equals -1 as explained above. So

$$L_k = -\frac{2}{\sqrt{p}} \sum_{j=1}^{(p-1)/2} e^{-i2\pi j^2/p} - \frac{1}{\sqrt{p}} \tag{44}$$

Comparing this to the earlier equation for L_k when $k = 1$, we finally see that $L_k = -L_1$ when k is not a quadratic residue mod p. Overall then

$$L_k = \begin{cases} 0 & \text{if } k \text{ is } 0 \mod p \\ +L_1 & \text{if } k \text{ is a quadratic residue mod } p \\ -L_1 & \text{if } k \text{ is a quadratic nonresidue} \end{cases} \tag{45}$$

We know that $L_1 = 1$ for $p \equiv 1 \mod 4$, and $L_1 = -i$ for $p \equiv 3 \mod 4$. Comparing the equation with $L_1 = 1$ with the equation for the Legendre symbol makes it clear that the transform $\{L_k\}$ is the same sequence as the original Legendre sequence $\{l_k\}$. Similarly for $L_1 = -i$ we see that the transform is simply the Legendre sequence multiplied by $-i$. So finally we obtain

$$\begin{cases} L_k = l_k & \text{if } p \equiv 1 \mod 4 \\ L_k = -il_k & \text{if } p \equiv 3 \mod 4 \end{cases} \tag{46}$$

That is, the DFT of the Legendre symbol sequence is simply a multiple of the sequence itself.

Appendix B
Auto-correlation of Legendre symbol sequence

Consider the Legendre sequence $\{l_n\}$, where

$$l_n = \left(\frac{n}{p} \right) \tag{47}$$

with $l_0 = 0$. By Euler's criterion

$$l_n = n^{\frac{p-1}{2}} \mod p \tag{48}$$

If p is a prime there will exist a primitive root g such that $g^k \mod p$, for $k = 1$ to $p-1$, generates all of the numbers from 1 to $p-1$ exactly once (in some permuted order). The "index" (or "logarithm") of n w.r.t. g is then defined by

$$g^{\text{ind}_g(n)} \equiv n \mod p \tag{49}$$

for $n \not\equiv 0 \mod p$. Consequently

$$l_n = g^{\text{ind}_g(n)\frac{p-1}{2}} \mod p \tag{50}$$

for $n \not\equiv 0 \mod p$, but

$$g^{\frac{p-1}{2}} \equiv -1 \mod p \tag{51}$$

so

$$l_n = (-1)^{\text{ind}_g(n)} \tag{52}$$

That is, for $n \not\equiv 0 \mod p$, l_n equals $+1$ or -1 depending on whether $\text{ind}_g(n)$ is even or odd.

The (periodic) auto-correlation of the sequence $\{l_n\}$ is

$$c_m = \sum_{n=0}^{p-1} l_n l_{n+m} \tag{53}$$

where the indices are taken mod p. For $m = 0$ this is the sum of a zero and $(p-1)$ ones, (since $l_n^2 = +1$ for $n \not\equiv 0 \mod p$) and so $c_0 = (p-1)$. For $m \not\equiv 0$

$$c_m = \sum_{\substack{n=1 \\ n+m \not\equiv 0}}^{p-1} (-1)^{\text{ind}_g(n)} (-1)^{-\text{ind}_g(n+m)} \tag{54}$$

where we omit the two terms involving l_0, since $l_0 = 0$, and made use of the fact that $(-1)^{-m} = (-1)^m$. So finally

$$c_m = \sum_{\substack{n=1 \\ n+m \not\equiv 0}}^{p-1} (-1)^{\text{ind}_g(n) - \text{ind}_g(n+m)} \tag{55}$$

The difference in the exponent assumes all integer values between 1 and $(p-2)$, mod $(p-1)$, exactly once over the indicated range of n (i.e. omitting $n = 0$ and $n + m \equiv 0$). Thus there is one more -1 raised to an odd power than -1 raised to an even power in the sum, and so $c_m = -1$ for $m \not\equiv 0$.

So we see that the auto-correlation comes to $(p\delta_m - 1)$, and so the Legendre symbol sequence has the ideal bi-level auto-correlation property.