

The Discrete Fourier Transform and Cyclical Overflow

by Leigh J. Halliwell

ABSTRACT

More casualty actuaries would employ the discrete Fourier transform (DFT) if they understood it better. In addition to the many fine papers on the DFT, this paper might be regarded as just one more introduction. However, the topic uniquely explained herein is how the DFT treats the probability of amounts that overflow its upper bound, a topic that others either have not noticed or have deemed of little importance. The cyclical overflow originates in the modular arithmetic whereby the DFT evaluates characteristic functions. To understand this is to attain a deeper understanding of the DFT, which may lead to its wider use.

KEYWORDS

*Collective-risk model, discrete Fourier transform,
characteristic function, roots of unity*

1. Introduction

A common tool of casualty actuaries is the collective-risk model $S = X_1 + \dots + X_N$, according to which aggregate loss S is composed of a random number N of independent, identically distributed claims X . Although there are several techniques for deriving probability distributions for S , the discrete Fourier transform (DFT) is arguably the most elegant and powerful when severity X is both discrete and finite. However, it suffers from two drawbacks. First, its use of complex numbers may daunt some actuaries; certainly it does not easily program into a spreadsheet.¹ And, second, the finite support of S raises the issue of overflow, especially when the support of claim count N is unlimited. Since one can set an arbitrarily large common support for X and S , this issue is not a practical problem;² however, how the true distribution of S overflows the DFT-derived distribution is an interesting topic. Moreover, understanding the overflow issue may enable and encourage others to employ the DFT. It is to this end that we will start in Section 2 with the necessary complex algebra. From there, in Section 3 we will define abstractly the DFT as an invertible transformation (a finite matrix of complex numbers). Bringing in probability, we will in Section 4 derive the DFT of $S = X_1 + \dots + X_N$ in terms of N and X . Finally, in Section 5 we will show what happens to overflow in the DFT, relating it back to the complex algebra of Section 2.

2. The n^{th} roots of unity

Euler's formula $e^{i\theta} = \cos \theta + i \sin \theta$ forms the basis for the n^{th} roots of unity.³ The magnitude of $z = e^{i\theta}$ is $|z| = \cos^2 \theta + \sin^2 \theta = 1$. Hence, $e^{i\theta}$ is a point on the

¹The Analysis ToolPack of Excel allows one to work with complex numbers, as well as to perform a Fourier analysis through the menu "Tools/Data Analysis." But a matrix language with built-in complex arithmetic is far preferable.

²It becomes a practical problem if it involves limitations to computing speed, memory, and accuracy, which limitations we will ignore here. The fast Fourier transform (FFT) is a remarkable algorithm for reducing, but not eliminating, them.

³See in References the Wikipedia articles on "Euler's formula" and "roots of unity." No complex analysis will be used in this paper, but we presume the reader to be proficient in complex algebra.

complex unit circle, and the function $z(\theta) = e^{i\theta}$ can be imagined as a point moving counterclockwise around this circle as θ increases. Plugging $\theta = 2\pi$ into Euler's formula, we have $e^{i \cdot 2\pi} = \cos 2\pi + i \sin 2\pi = 1$. Since the circumference of a circle measures 2π radians, the exponential function is periodic along the imaginary axis.

Now consider the equation $z^n = 1$, where n is a positive integer. For any integer k ,

$$\left(e^{i \frac{2\pi k}{n}} \right)^n = e^{i \frac{2\pi k n}{n}} = e^{i \cdot 2\pi k} = (e^{i \cdot 2\pi})^k = (1)^k = 1.$$

So numbers of the form $\omega_k = e^{i \frac{2\pi k}{n}}$ are n^{th} roots of unity. Furthermore, since $\omega_n = e^{i \frac{2\pi n}{n}} = e^{i \cdot 2\pi} = 1$, within this formally infinite set only n elements are distinct, viz., $\omega_k = e^{i \frac{2\pi k}{n}}$ for $k \in \{0, 1, \dots, n-1\}$. Multiplication of roots of unity involves modular arithmetic,⁴ since

$$\begin{aligned} \omega_k \omega_l &= e^{i \frac{2\pi k}{n}} e^{i \frac{2\pi l}{n}} = e^{i \frac{2\pi(k+l)}{n}} = \omega_{k+l} = \omega_{\text{mod}(k+l, n)} \\ &\Rightarrow k+l \equiv \text{mod}(k+l, n). \end{aligned}$$

Because an n^{th} degree polynomial has at most n distinct roots,⁵ there can be no other n^{th} roots of unity.

The operation of multiplication on G , the set of the n^{th} roots of unity, constitutes an algebraic group (Clark 1984, pp. 17f). In addition to closure (if a ,

⁴More accurately, such multiplication is the basis of modular arithmetic. It has enriched the concept in classical number theory of congruence modulo n , i.e., $p \equiv q \pmod n$, and made complex analysis, culminating in the Riemann zeta function, essential to modern number theory.

⁵See Wikipedia, "Fundamental theorem of algebra," for a history of the attempts to prove this. The article disputes the opinion of most mathematical historians that Gauss in his 1799 doctoral dissertation produced the first rigorous proof. Appendix D of Havil [2003], "Complex Function Theory," a readable introduction to complex analysis, contains an elegant proof of one version of the theorem, viz., that every finite polynomial with complex coefficients has a complex root (pp. 241f). Induction completes the proof: If r is a root, factoring $z - r$ out of the polynomial leaves a polynomial for solution whose degree is one less.

$b \in G$, then $a \cdot b \in G$), multiplication on G has the three defining properties:

1. $\forall a, b, c \in G (a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. $\exists e \in G : \forall a \in G a \cdot e = e \cdot a = a$
3. $\forall a \in G \exists b \in G : a \cdot b = b \cdot a = e$

The properties are (1) associativity, (2) identity existence, and (3) inverse existence. That multiplication is associative hardly needs to be mentioned. The identity element is $\omega_0 = 1$. Abstractly, the identity element must be unique, for if e_1 and e_2 satisfy the identity property, then $e_1 = e_1 \cdot e_2 = e_2$. Similarly, the inverse of an element must be unique, for, if both $a \cdot b_1 = b_1 \cdot a = e$ and $a \cdot b_2 = b_2 \cdot a = e$, then

$$b_1 = b_1 \cdot e = b_1 \cdot (a \cdot b_2) = (b_1 \cdot a) \cdot b_2 = e \cdot b_2 = b_2.$$

For group G , the inverse of ω_k is $\omega_k^{-1} = \omega_{n-k} = \omega_{\text{mod}(n-k, n)}$; the third part of the equation applies to the identity element: $\omega_0^{-1} = \omega_0$. But, again from Euler's formula:

$$\begin{aligned} \omega_k^{-1} &= e^{-i\frac{2\pi k}{n}} = \cos\left(-\frac{2\pi k}{n}\right) + i \sin\left(-\frac{2\pi k}{n}\right) \\ &= \cos\left(\frac{2\pi k}{n}\right) - i \sin\left(\frac{2\pi k}{n}\right) = \bar{\omega}_k. \end{aligned}$$

This means that the inverse of a root of unity is its complex conjugate.

Of all the n^{th} roots of unity, $\omega_1 = e^{i\frac{2\pi}{n}}$ is the principal, from which the others can be derived by exponentiation $\omega_k = \omega_1^k$. We will often drop the subscript from the principal root and designate all the roots as $\omega_k = \omega_1^k = \omega^k$. The value of n will be understood; however, were it forgotten, it could always be reclaimed as the smallest positive integer for which $\omega^n = 1$.

Finally, as to the sum of the n^{th} roots of unity:

$$(\omega - 1) \sum_{k=0}^{n-1} \omega^k = \sum_{k=1}^n \omega^k - \sum_{k=0}^{n-1} \omega^k = \omega^n - \omega^0 = 1 - 1 = 0.$$

Either $\omega = 1$ or $\sum_{k=0}^{n-1} \omega^k = 0$. But the principal root is unity if and only if $n = 1$. Hence

$$\sum_{k=0}^{n-1} \omega^k = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}.$$

Intuitively, the formula for $n > 1$ is obvious from the equal dispersion of the roots about the circle; the origin is the center of their mass.⁶

3. The discrete Fourier transform

The DFT is simply an $n \times n$ matrix Ω involving the n^{th} roots of unity ω^k . The jk^{th} element of Ω is $\omega^{j \cdot k}$. As in the previous section, ω is the principal n^{th} root of unity, and the indexing starts at zero. Define the two $n \times 1$ vectors:

$$\mathbf{n} = \begin{bmatrix} 0 \\ \vdots \\ n-1 \end{bmatrix} \text{ and } \mathbf{p} = \begin{bmatrix} p_0 \\ \vdots \\ p_{n-1} \end{bmatrix}$$

The DFT of \mathbf{p} is $\Omega \mathbf{p}$. Understanding the exponentiation as elementwise, we can express this as $\Omega = \omega^{\mathbf{nn}'}$, which matrix is symmetric. But it is unnecessary to perform the exponentiation on ω . Due to the cyclical-ity of the multiplication, the elements of \mathbf{nn}' can be reduced modulo n to the set $\{0, 1, \dots, n-1\}$, at which point they are just as much n^{th} -root subscripts as they are exponents. In sum, $\Omega = \omega^{\mathbf{nn}'} = \omega^{\text{mod}(\mathbf{nn}', n)}$.

To reclaim vector \mathbf{p} , one needs the inverse DFT, or Ω^{-1} , whose existence we will now show. Define the conjugate of matrix Ω , or $\bar{\Omega}$, as the matrix of the conjugated elements of Ω . According to Section 2, the conjugate of a root of unity is the inverse of the root. So the jk^{th} element of $\bar{\Omega}$ is ω^{-jk} . Since Ω is

⁶Alternatively, according to the theory of equations, the sum of the roots of $z^n + a_1 z^{n-1} + \dots + a_n = 0$ equals $-a_1$. Since the ω^k are the roots of the equation $z^n - 1 = 0$, they sum either to one (if $n = 1$) or to zero (if $n > 1$).

symmetric, so too is $\overline{\Omega}$. Now the jk^{th} element of $\overline{\Omega}\Omega$ is the dot product of the j^{th} row of $\overline{\Omega}$ and the k^{th} column of Ω . Hence:

$$[\overline{\Omega}\Omega]_{jk} = \sum_{l=0}^{n-1} \overline{\omega}_j \omega_{lk} = \sum_{l=0}^{n-1} \omega_j^{-1} \omega_{lk} = \sum_{l=0}^{n-1} \omega^{-jl} \omega^{lk} = \sum_{l=0}^{n-1} (\omega^{k-j})^l.$$

The formula for the geometric series gives us

$$[\overline{\Omega}\Omega]_{jk} = \sum_{l=0}^{n-1} (\omega^{k-j})^l = \begin{cases} n & \text{if } \omega^{k-j} = 1 \\ \frac{(\omega^{k-j})^n - 1}{(\omega^{k-j}) - 1} & \text{if } \omega^{k-j} \neq 1 \end{cases} = \begin{cases} n & \text{if } \omega^{k-j} = 1 \\ 0 & \text{if } \omega^{k-j} \neq 1 \end{cases}.$$

But $\omega^{k-j} = 1$ if and only if $\text{mod}(k-j, n) = 0$. Since $j, k \in \{0, 1, \dots, n-1\}$, $\text{mod}(k-j, n) = 0$ if and only if $j = k$. So, finally,

$$[\overline{\Omega}\Omega]_{jk} = \begin{cases} n & \text{if } j = k \\ 0 & \text{if } j \neq k \end{cases} \Rightarrow \overline{\Omega}\Omega = n\mathbf{I}_n.$$

And since both Ω and $\overline{\Omega}$ are symmetric, $\Omega\overline{\Omega} = \Omega'\overline{\Omega}' = (\overline{\Omega}\Omega)' = (n\mathbf{I}_n)' = n\mathbf{I}_n$. Therefore, Ω is invertible: $\Omega^{-1} = \overline{\Omega}/n$.⁷

4. The discrete Fourier transform as a characteristic function

The relevance of the previous two sections will become clear in connection with the characteristic function, which is a moment generating function (mgf) with an imaginary argument. The characteristic function of any real-valued random variable X , or ϕ_X , is $\phi_X(t) = E[e^{itX}]$. Because $|E[e^{itX}]| = \left| \int_{x=-\infty}^{\infty} e^{itx} dF_x(x) \right| \leq$

⁷One could define the DFT as $\Omega = \omega^{nm}/\sqrt{n}$, in which case Ω^{-1} would simply be $\overline{\Omega}$. But we have kept the standard definition, on account of which one must be careful to include the $1/n$ factor.

$\int_{x=-\infty}^{\infty} |e^{itx}| dF_x(x) = \int_{x=-\infty}^{\infty} 1 \cdot dF_x(x) = 1$, the characteristic function, unlike the mgf, always converges. However, since here we are concerned with discrete and finite random variables, whose mgfs do converge, this is of no advantage. Its advantage here lies in the simplicity and accuracy of its inversion.

First, we give a probability interpretation to vector \mathbf{p} of Section 3. The k^{th} element of \mathbf{p}_X will be the probability for random variable X to equal k : $Pr ob[X = k] = p_k$. So now the elements of \mathbf{p}_X must be non-negative real numbers whose sum is unity. Second, we define $t_k = \frac{2\pi k}{n}$ for $k \in \{0, 1, \dots, n-1\}$. These n values of t are the radian measures on the unit circle of the n^{th} roots of unity, so $\omega_k = e^{\frac{i2\pi k}{n}} = e^{it_k}$. Accordingly,

$$\phi_X(t_j) = E[e^{it_j X}] = \sum_{k=0}^{n-1} e^{it_j k} p_k = \sum_{k=0}^{n-1} (\omega_j)^k p_k = \sum_{k=0}^{n-1} \omega^{jk} p_k.$$

The last expression is the j^{th} element of the matrix product $\Omega\mathbf{p}_X$. In fact, defining \mathbf{t} as the $n \times 1$ vector whose j^{th} element is t_j , and applying ϕ_X elementwise, we have $\phi_X(\mathbf{t}) = \Omega\mathbf{p}_X$. Therefore, the DFT is a discrete form of the characteristic function, from which one can reclaim the probabilities as $\mathbf{p}_X = \Omega^{-1} \phi_X(\mathbf{t}) = \frac{\overline{\Omega}}{n} \phi_X(\mathbf{t})$.

Even so, it seems that we are just playing games, jumping from probabilities to the characteristic function and back again. Must not one know the probabilities before knowing the characteristic function? The answer is “Not necessarily.” The collective-risk model is a case in point, for if $S = X_1 + \dots + X_N$:

$$\phi_S(t) = E[e^{itS}] = E[e^{it(X_1 + \dots + X_N)}] = E\left[\prod_{k=1}^N e^{itX_k}\right].$$

Separate N from the X variables by conditional expectation:

$$E\left[\prod_{k=1}^N e^{itX_k}\right] = E_N\left[E\left[\prod_{k=1}^N e^{itX_k} \middle| N\right]\right] = E_N\left[\prod_{k=1}^N E\left[e^{itX_k} \middle| N\right]\right].$$

Finally, simplify due to the identical distribution of the X variables:

$$\begin{aligned} E \left[\prod_{k=1}^N E[e^{ix_k}] \middle| N \right] &= E \left[\prod_{k=1}^N \varphi_X(t) \middle| N \right] \\ &= E [\varphi_X(t)^N | N] = E [\varphi_X(t)^N]. \end{aligned}$$

Therefore, $\varphi_S(t) = E [\varphi_X(t)^N]$, in agreement with Heckman and Meyers (1983, p. 34), Klugman, Panjer, and Willmot (1998, p. 316), and Wang (1998, p. 864). The point is made: one can obtain the characteristic function of S without knowledge of its probabilities, and by DFT inversion (i.e., $\mathbf{p}_S = \frac{\bar{\Omega}}{n} \varphi_S$) work back to the probabilities.

If N is a constant, or $\text{Prob}[N = k] = 1$, then $S = X_1 + \dots + X_k$ and $\varphi_S(t) = \varphi_X(t)^k$. Therefore, $\mathbf{p}_S = \frac{\bar{\Omega}}{n} \varphi_S = \frac{\bar{\Omega}}{n} (\Omega \mathbf{p}_X)^k$. This is the formula for the k^{th} convolution of X , which holds for any non-negative integer k .⁸ We will check it for $k = 0$. In this case $(\Omega \mathbf{p}_X)^k = \mathbf{1}_n$, an $n \times 1$ vector of ones, and $\mathbf{p}_S = \frac{\bar{\Omega}}{n} \mathbf{1}_n$, which contains the row averages of $\bar{\Omega}$. Its j^{th} element is

$$\begin{aligned} [\mathbf{p}_S]_j &= \frac{1}{n} \sum_{t=0}^{n-1} \bar{\omega}_{jt} = \frac{1}{n} \sum_{t=0}^{n-1} \omega^{-jt} = \frac{1}{n} \sum_{t=0}^{n-1} (\omega^{-j})^t \\ &= \frac{1}{n} \begin{cases} n & \text{if } j = 0 \\ \frac{(\omega^{-j})^n - 1}{\omega^{-j} - 1} & \text{if } j > 0 \end{cases} \\ &= \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{if } j > 0 \end{cases} \end{aligned}$$

So $\text{Prob}[S = 0] = 1$, as it must.

⁸Even fractional convolutions make sense. The half convolution of X is a distribution of a random variable whose second convolution is the distribution of X . If X can be formed from a second convolution, the DFT will yield the correct result. For example, if $\mathbf{p}_X = [0.25 \ 0.50 \ 0.25]'$, then $\mathbf{p}_S = \frac{\bar{\Omega}}{3} (\Omega \mathbf{p}_X)^{0.5} = [0.5 \ 0.5 \ 0]$. If X cannot be so formed and n is large enough (\mathbf{p}_X right-padded with zeros), non-zero probabilities will appear beyond $\max(X)$, even though all the probabilities will sum to unity. Moreover, when the convolution is impossible, negative probabilities may arise.

Again, if $\text{Prob}[X = 1] = 1$, $S = 1_1 + \dots + 1_N = N$. In this case $\varphi_X(t) = E[e^{itX}] = e^{it}$ and

$$\varphi_S(t) = E[\varphi_X(t)^N] = E[(e^{it})^N] = E[e^{itN}] = \varphi_N(t).$$

This means that S is distributed as N ; in the realm of the DFT, $\mathbf{p}_S = \mathbf{p}_N$.

In general, $E[z^N]$ is called the probability generating function (Klugman, Panjer, and Willmot (1998, p. 201) and denoted as $P_N(z)$. Therefore, $\varphi_S(t) = E[\varphi_X(t)^N] = P_N(\varphi_X(t))$. Klugman's Appendix B contains the probability generating functions of many claim-count distributions, and our purpose here does not require us to duplicate his and others' work. So we turn at last to the overflow problem.

5. The discrete Fourier transform and overflow

Example 4.11 of Klugman, Panjer, and Willmot (1998, pp. 319f) demonstrates the use of the DFT to obtain the distribution of $S = X_1 + \dots + X_N$, where N is Poisson-distributed with a mean of 3, and $\mathbf{p}_X = [0 \ 0.5 \ 0.4 \ 0.1 \ 0 \ \dots]'$. The demonstration is performed twice, once over the support $[0 \ 1 \ \dots \ 7]'$ and once over the support $[0 \ 1 \ \dots \ 4095]'$. For the first support, $n = 8$; for the second, $n = 4096$. The purpose of the twofold demonstration is to show the importance of choosing a value for n large enough for the overflow to be negligible. Having replicated his calculations, we present the results in Table 1.

Klugman remarks:

... all the entries for $n = 4,096$ are accurate to the five decimal places presented. On the other hand, with $n = 8$, the FFT gives values that are clearly distorted. If any generalization can be made it is that more of the extra probability has been added to the smaller values of S . [p. 319]

In other words, the values for $n = 8$ are distorted by the overflow; but the lower the value of s , the greater

Table 1. Example 4.11 of Klugman, Panjer, and Willmot Loss Models (1998)

<i>s</i>	<i>n</i> = 8	<i>s</i>	<i>n</i> = 4096	<i>s</i>	Cont'd
0	0.11227	0	0.04979	13	0.00666
1	0.11821	1	0.07468	14	0.00381
2	0.14470	2	0.11575	15	0.00212
3	0.15100	3	0.13256	16	0.00115
4	0.14727	4	0.13597	17	0.00060
5	0.13194	5	0.12525	18	0.00031
6	0.10941	6	0.10558	19	0.00015
7	0.08518	7	0.08305	20	0.00008
		8	0.06134	21	0.00004
	1.00000	9	0.04293	22	0.00002
		10	0.02863	23	0.00001
		11	0.01829	24	0.00000
		12	0.01123		⋮
					1.00000

the error. This is true enough; but more generalization can be made.

The probability for *S* to exceed 7, or to overflow the procedure for *n* = 8, is about 17.7 percent. The remarkable point is that the DFT preserves all the probability, regardless of *n*. Why does it not simply cut off accurately at *s* = 7? Instead, it compresses all the probability into the eight values. The explanation will appear from the following example.

Starting with a Bernoulli(0.5)-distributed *X*, we derived its next four convolutions and display them in Table 2. The probabilities of *C*(*n*) are binomial (*n*, 0.5).

Next, we calculated those probabilities according to the DFT with *n* = 4. Accordingly,

Table 2. Exact Probabilities of Convolutions of X

<i>k</i>	<i>X</i>	<i>C</i> (2)	<i>C</i> (3)	<i>C</i> (4)	<i>C</i> (5)
0	0.5	0.250	0.125	0.0625	0.03125
1	0.5	0.500	0.375	0.2500	0.15625
2		0.250	0.375	0.3750	0.31250
3			0.125	0.2500	0.31250
4				0.0625	0.15625
5					0.03125

$$\mathbf{n} = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \end{bmatrix} \quad \mathbf{p}_x = \begin{bmatrix} 0.5 \\ 0.5 \\ 0.0 \\ 0.0 \end{bmatrix}$$

$$\mathbf{\Omega} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \quad \mathbf{\Omega}^{-1} = \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}$$

Hence, $\mathbf{p}_{C(n)} = \mathbf{\Omega}^{-1} (\mathbf{\Omega} \mathbf{p}_x)^n$. Table 3 shows the DFT result.

As expected, *C*(2) and *C*(3) agree. But overflow begins with *C*(4), and the form of the overflow is cyclical. What should have been in the *k* = 4 row added to the *k* = 0 row; what should have been in the *k* = 5 row added to the *k* = 1 row.

The DFT cannot ignore overflow; rather it must recycle it. Instead of calculating probabilities for $S = X_1 + \dots + X_N$, it calculates them for $\text{mod}(S, n)$. Its arithmetic is as modular as that of the *G* group of Section 2:

$$\omega_k \omega_l = \omega_{k+l} = \omega_{\text{mod}(k+l, n)} \Rightarrow k+l \equiv \text{mod}(k+l, n).$$

Alternatively, one may imagine the support to be infinite, over the set of natural numbers {0, 1, 2, ...}. However, there is no least root of unity; one must settle for some finite *n* and its principal root. So to match the roots of unity with the natural numbers, one must cycle endlessly through $\omega^0 \ \omega^1 \ \dots \ \omega^{n-1}$. The roots of unity are like ID variables according to

Table 3. DFT Probabilities with n = 4

<i>k</i>	<i>X</i>	<i>C</i> (2)	<i>C</i> (3)	<i>C</i> (4)	<i>C</i> (5)
0	0.5	0.250	0.125	0.1250	0.18750
1	0.5	0.500	0.375	0.2500	0.18750
2		0.250	0.375	0.3750	0.31250
3			0.125	0.2500	0.31250
4				0.0625	0.15625
5					0.03125

which the probabilities may be summarized, as in the summation:

$$\sum_{k=0}^{\infty} \omega^k p_k = \sum_{k=0}^{\infty} \omega^{\text{mod}(k,n)} p_k = \sum_{k=0}^{n-1} \left(\omega^k \sum_{\text{mod}(l,n)=k} p_l \right) = \sum_{k=0}^{n-1} (\omega^k p_k^*).$$

Summarizing the $n = 4096$ probabilities of Table 1 according to $\text{mod}(s, 8)$ will produce the $n = 8$ probabilities.

6. Conclusion

Many actuaries have neither the temperament nor the fortitude to penetrate the thicket of Σ operators found in many treatments of the discrete Fourier transform. Hopefully, they will find this treatment gentler, starting as it does with the n^{th} roots of unity. The addition of a dash of group theory, about which much more could be said,⁹ is suggestive of the modular arithmetic underlying the DFT and of the behavior of any overflow. The magic¹⁰ of the DFT is not dispelled by its being opened to examination. But to those who understand the preceding sections of this paper, any impediments to working DFT magic will pertain only to computer hardware and software.¹¹

⁹The properties of an algebraic group ensure that for any element a of group G , $a \cdot G$ and $G \cdot a$ are in one-to-one correspondence with G . Because of this, group theory is all about shifts, cycles, or rotations, especially for finite groups. Moreover, a finite group with a generating element (i.e., an element by repeated operations on which all the elements of G can be generated, such as a primitive root of unity) has a counting mechanism, from which a modular arithmetic can be developed. One who understands this can apply the DFT to abstractions of $\{0, 1, \dots, n-1\}$.

¹⁰A friend of the author and former colleague, James C. Sandor, FCAS, MAAA, who introduced the Fourier transform into his company's pricing models, never tires of saying, "The Fourier transform works like magic."

¹¹After this paper was reviewed and revised, the author was made aware of the paper, "Panjer Recursion versus FFT for Compound Distributions," by Paul Embrechts and Marco Frei (2007). On page 8, the authors wrote, "Compound mass which lies at M and beyond will be 'wrapped around' and erroneously appears in the range $0, \dots, M-1$. For severities with considerable tail mass, the truncation and wrap-around error (the so-called aliasing error) can become quite an issue." Although they did not explicitly claim the wrapping around to be modulo M , it is likely that they so understood it. Also, they called DFT overflow "aliasing" by analogy with a problem in signal processing (cf. Wikipedia, "Aliasing").

References

- Clark, A., *Elements of Abstract Algebra*, New York: Dover, 1984.
- Embrechts, P., and M. Frei, "Panjer Recursion versus FFT for Compound Distributions," *Mathematical Methods of Operations Research* 69 (2009), pp. 497–508; corrected in www.math.ethz.ch/~embrecht/ftp/PanjerVsFFTcorrected.pdf.
- Havil, J., *Gamma: Exploring Euler's Constant*, Princeton: Princeton University Press, 2003.
- Heckman, P.E., and G. G. Meyers, "The Calculation of Aggregate Loss Distributions from Claim Severity and Claim Count Distributions," *Proceedings of the Casualty Actuarial Society* 70 (1983), pp. 22–61, www.casact.org/pubs/proceed/proceed83/83022.pdf.
- Klugman, S.A., H.H. Panjer, and G.E. Willmot, *Loss Models: From Data to Decisions*, New York: Wiley, 1998.
- Wang, S. S., "Aggregation of Correlated Risk Portfolios: Models and Algorithms," *Proceedings of the Casualty Actuarial Society* 85 (1998), pp. 848–939, www.casact.org/pubs/proceed/proceed98/980848.pdf.
- Wikipedia contributors, "Euler's formula," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/wiki/Euler%27s_formula (accessed July 2013).
- Wikipedia contributors, "Fundamental theorem of algebra," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/wiki/Fundamental_theorem_of_algebra (accessed July 2013).
- Wikipedia contributors, "Root of Unity," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/wiki/Root_of_unity (accessed July 2013).