Solution by Radicals and the DFT

Introduction: Babylonian scribes solved quadratic equations that we write as

$$ax^2 + bx + c = 0$$

in 1700 B.C.[1] More than 3000 years later[2] Tartaglia, Cardano, and other mathematicians discovered how to solve the cubic equations that we write as

$$ax^3 + bx^2 + cx + d = 0.$$

The cubic is much harder to solve than the quadratic. We learn to solve the quadratic by completing the square, but it is not clear how to complete the cube — at least, it is not clear *straightaway* how. The purpose of this note is to provide that generalization in its natural setting.

In his *Réflexions*[3], Lagrange analyzes the solution to the cubic using what amounts to the Discrete Fourier Transform (DFT). This was long before matrices were invented, and Lagrange's analysis is essentially scalar, not vector, in nature. He says that solving the cubic "requires particular artifices that do not present themselves naturally", but no such "artifices" are required if we are willing to use the DFT.

The DFT: Solving quadratic, cubic, and quartic equations requires very little of the theory about the Discrete Fourier Transform (DFT). I've described the motivation for, and some of the properties of, the DFT in the appendix. This section is a brief description of the three DFTs we'll use.

The 2-, 3-, and 4-dimensional DFTs are, respectively, the (operators represented by the) matrices

$$\mathsf{F}_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$\mathsf{F}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix} \qquad \text{where} \qquad \omega = e^{-\frac{2\pi i}{3}} = \cos\left(\frac{2\pi}{3}\right) - i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i,$$

and

$$\mathsf{F}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}.$$

We want to be able to recognize the 2-dimensional DFT when we see it, so that we'll know how to generalize. It is simply "sum and difference":

$$\mathsf{F}_2\mathsf{r} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \begin{bmatrix} r_1 + r_2 \\ r_1 - r_2 \end{bmatrix}.$$

The numbers that make up the matrix F_n are all **roots of unity**. The two numbers making up F_2 are square roots of unity:

$$1^2 = (-1)^2 = 1,$$

[1] Harold M. Edwards, *Galois Theory*, Springer-Verlag, 1984, pp. 3–4. Edwards cites Otto Neugebauer, *The Exact Sciences in Antiquity*, Princeton University Press, Princeton, 1952.

[2] See B. L. van der Waerden, *A History of Algebra*, Springer-Verlag, Berlin, 1985, pp. 54ff. for a fascinating story.

[3] Lagrange, J. L., *Réflexions sur la Résolution Algebraique des Équations*, Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin, 1770–1771. Also appears in *Oeuvres de Lagrange*, vol. 3, pp. 205–420. Freely downloadable copies available at https://gallica.bnf.fr/ark:/12148/bpt6k229222d/f206.

the three numbers making up F_3 are cube roots of unity:

$$1^3 = (\omega)^3 = \left(\omega^2\right)^3 = 1,$$

and the four numbers making up F_4 are fourth roots of unity:

$$1^4 = i^4 = (1)^4 = (-i)^4 = 1.$$

The roots of unity lie equally spaced around the unit circle in the complex plane. They are useful when finding roots of complex numbers — the "radicals" in the title. Suppose, for example, that $a^4 = b$. Then $a = \sqrt[4]{b}$ — a is a fourth root of b — and the remaining fourth roots are ia, $(-1)a$, and $(-i)a$. This property is Lagrange's primary motivation in using (what amounts to) the DFT. More information about roots of unity is in the appendix.

F_2 is practically its own inverse:

$$\mathsf{F}_2\mathsf{F}_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 2\,\mathsf{I}.$$

In particular, the columns of F_2 are mutually orthogonal.

The higher dimensional DFTs also have mutually orthogonal columns. This is easiest to see in F_4. Complex vectors u and v are orthogonal when $\overline{\mathsf{u}}^T\mathsf{v} = 0$, where the "bar" represents complex conjugation. Consequently, the columns of F_4 are mutually orthogonal because

$$\overline{\mathsf{F}_4^T}\mathsf{F}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} = 4\,\mathsf{I}.$$

F_3 is less familiar, perhaps, but it is easy to check that $\overline{\omega} = \omega^2$ and that

$$\overline{\mathsf{F}_3^T}\mathsf{F}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix} = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix} = 3\,\mathsf{I}.$$

The proof that $\overline{\mathsf{F}_n^T}\mathsf{F}_n = n\,\mathsf{I}$ is in the appendix. The only result we need is

$$\mathsf{F}_n^{-1} = \frac{1}{n}\overline{\mathsf{F}_n^T} \qquad \text{for } n = 2, 3, 4,$$

which follows from the three computations above.

The Quadratic:

We begin our analysis with the quadratic[4]

$$f_2(x) = x^2 + bx + c. \tag{Q_1}$$

We are looking for the roots of f_2, so there is no loss of generality in assuming that f_2 is **monic** — the leading coefficient, which we denoted by a in the introduction, is 1. This restriction simplifies the factorizations below.

Early in our algebra classes, we learn to find the roots of f_2 by completing the square:

$$f_2(x) = x^2 + bx + c = \left(x + \frac{b}{2}\right)^2 - \frac{b^2}{4} + c. \tag{Q_2}$$

[4] Lagrange says the quadratic is so simple that he will skip it and begin by analyzing the cubic. We start with the quadratic because it motivates the analysis of higher-degree equations.

From the completed square, we solve for the roots

$$\begin{aligned} r_1 &= -\frac{b}{2} + \frac{\sqrt{b^2-4c}}{2}, \text{ and} \\ r_2 &= -\frac{b}{2} - \frac{\sqrt{b^2-4c}}{2}. \end{aligned} \tag{Q_3}$$

We also learn early in our algebra classes that, knowing the roots r_1 and r_2, we can factor and then expand f_2 as

$$\begin{aligned} f_2(x) &= (x-r_1)(x-r_2) \\ &= x^2 - (r_1+r_2)\,x + r_1 r_2. \end{aligned} \tag{Q_4}$$

We conclude, by comparing the coefficients in Equations (Q_1) and (Q_4), that

$$\begin{aligned} b &= -(r_1+r_2) \\ c &= r_1 r_2. \end{aligned} \tag{Q_5}$$

(This is where assuming f_2 is monic helps — otherwise, the left sides are $\frac{b}{a}$ and $\frac{c}{a}$, respectively.) Equations (Q_5) express the coefficients b and c of f_2 as **symmetric** functions of the roots r_1 and r_2. By symmetric, we mean that exchanging r_1 and r_2 does not change the sum $r_1 + r_2$ or the product $r_1 r_2$. In general, a function $g(r_1, r_2, \ldots, r_n)$ is **symmetric** in the r_i if

$$g(r_{p_1}, r_{p_2}, \ldots r_{p_n}) = g(r_1, r_2, \ldots, r_n)$$

whenever $(p_1, p_2, \ldots, p_n)$ is a permutation (a re-ordering) of $(1, 2, \ldots, n)$. Symmetry and the DFT are the only tools we need to solve the cubic and quartic.

Now for the analysis: Equations (Q_5) imply that the discriminant (the part under the radical) in Equations (Q_3) is

$$b^2 - 4c = (r_1+r_2)^2 - 4r_1 r_2 = (r_1 - r_2)^2. \tag{Q_6}$$

Reading Equation (Q_6) from right to left illustrates an important point about our technique. The difference $r_1 - r_2$ is *not* symmetric in r_1 and r_2, but its square, $(r_1 - r_2)^2$, *is* symmetric. This symmetry *guarantees* that we can write the square $(r_1 - r_2)^2$ in terms of the coefficients b and c. In this case we already know $(r_1 - r_2)^2 = b^2 - 4c$. In general, the **Fundamental Theorem of Symmetric Polynomials** guarantees that we can express *any* symmetric polynomial of the roots r_1 and r_2 in terms of b and c. A representative computation goes like this: $r_1^3 r_2 + r_1 r_2^3$ is symmetric, and we compute

$$\begin{aligned} r_1^3 r_2 + r_1 r_2^3 &= \left(r_1^2 + r_2^2\right)(r_1 r_2) \\ &= \left((r_1+r_2)^2 - 2r_1 r_2\right)(r_1 r_2) \\ &= \left((-b)^2 - 2c\right)c = b^2 c - 2c^2. \end{aligned}$$

The Fundamental Theorem amounts to a division algorithm for symmetric polynomials. It is one of those theorems whose proof is harder to write than to understand. We'll work enough explicit examples to illustrate the division algorithm. Cox, Little, and O'Shea[5] describe some general division algorithms in detail, and prove the Fundamental Theorem as a special case.

Equation (Q_6) for the discriminant means Equations (Q_3) are

$$\begin{aligned} r_1 &= \frac{r_1+r_2}{2} + \frac{\sqrt{(r_1-r_2)^2}}{2}, \text{ and} \\ r_2 &= \frac{r_1+r_2}{2} - \frac{\sqrt{(r_1-r_2)^2}}{2}. \end{aligned} \tag{Q_7}$$

[5] Cox, D.; Little, J.; O'Shea, D, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, second edition, 1997, pp. 312 ff. Only a small fraction of the first 312 pages is needed to understand the algorithm, so start on p. 312 and refer back to previous results as needed.

It is tempting to say that Equations (Q_7) are simply the tautology

$$\begin{aligned} r_1 &= \frac{r_1+r_2}{2} + \frac{r_1-r_2}{2}, \text{ and} \\ r_2 &= \frac{r_1+r_2}{2} - \frac{r_1-r_2}{2}, \end{aligned} \tag{Q_8}$$

but there is a hitch. Suppose r_1 and r_2 are real and $r_2 > r_1$. Then our bias for positive square roots would likely lead us to compute $\frac{\sqrt{(r_1-r_2)^2}}{2} = \frac{r_2-r_1}{2}$, not $\frac{r_1-r_2}{2}$, and the subscripts on the left side of Equations (Q_7) would be reversed. But we don't care what order the roots come out of the formula in — the labels are just a convenience. Come to think of it, it's the choice of square root that determines the subscripts on the roots on the left side of (Q_7). This hitch is fundamental in Galois theory.

Finally, we write Equations (Q_8) using matrices to reveal the structure we seek:

$$\begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \begin{bmatrix} \frac{r_1+r_2}{2} + \frac{r_1-r_2}{2} \\ \frac{r_1+r_2}{2} - \frac{r_1-r_2}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{bmatrix} \begin{bmatrix} r_1+r_2 \\ r_1-r_2 \end{bmatrix} = \underbrace{\begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{bmatrix}}_{\mathsf{F}_2^{-1}} \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}}_{\mathsf{F}_2} \begin{bmatrix} r_1 \\ r_2 \end{bmatrix}. \tag{Q_9}$$

Matrix F_2 is the 2-dimensional **Discrete Fourier Transform** (DFT).

The Cubic: We next attempt to find the roots r_1, r_2, and r_3 of the cubic

$$f_3(x) = x^3 + bx^2 + cx + d. \tag{C_1}$$

Let us (attempt to) "complete the cube", just as we completed the square in Equation (Q_2):

$$f_3(x) = \left(x + \frac{b}{3}\right)^3 + \underbrace{\left(c - 3\left(\frac{b}{3}\right)^2\right)}_{\hat{c}} \left(x + \frac{b}{3}\right) + \underbrace{d - c\frac{b}{3} + 2\left(\frac{b}{3}\right)^3}_{\hat{d}}. \tag{C_2}$$

(It's worth your time to check that I computed correctly — we'll see these numbers again, later.) Equation (C_2) permits us to solve for the roots of f_3 provided $\hat{c} = 0$. That's not nearly frequently enough.

What's our next step? As in Equation (Q_4), if we knew the roots r_1, r_2, and r_3, we could factor and then expand f_3 as

$$\begin{aligned} f_3(x) &= (x-r_1)(x-r_2)(x-r_3) \\ &= x^3 - (r_1+r_2+r_3)\,x^2 + (r_1r_2 + r_1r_3 + r_2r_3)\,x + r_1r_2r_3. \end{aligned} \tag{C_3}$$

We conclude, by comparing the coefficients in Equations (C_1) and (C_3), that

$$\begin{aligned} b &= -(r_1+r_2+r_3) \\ c &= r_1r_2 + r_1r_3 + r_2r_3 \\ d &= -r_1r_2r_3. \end{aligned} \tag{C_4}$$

Three equations and three unknowns looks good, but trying to solve Equation (C_4) for the r_j is disheartening. Don't let me discourage you from trying, but do let me know if you make progress!

To make progress on the cubic, we try to generalize the computations with the DFT in Equation (Q_9). Certainly

$$\begin{bmatrix} r_1 \\ r_2 \\ r_3 \end{bmatrix} = \mathsf{F}_3^{-1}\mathsf{F}_3 \begin{bmatrix} r_1 \\ r_2 \\ r_3 \end{bmatrix} = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ r_3 \end{bmatrix}. \tag{C_5}$$

We therefore attempt to identify (meaning, solve for)

$$\mathsf{F}_3 \begin{bmatrix} r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} r_1 + r_2 + r_3 \\ r_1 + \omega r_2 + \omega^2 r_3 \\ r_1 + \omega^2 r_2 + \omega r_3 \end{bmatrix}. \tag{C_6}$$

The top row looks promising. It is symmetric in the r_j, and the top line of Equation (C_4) says $r_1+r_2+r_3 = -b$. We therefore need only identify the bottom two rows.

Consider the second row,

$$t_1 = r_1 + \omega r_2 + \omega^2 r_3.$$

It is not symmetric in the r_j, so we can't solve for it straightaway using Equation (C_4). Instead, we build a polynomial $F(t)$ which *is* symmetric in the r_j, and which has t_1 as a root. This clever idea is called **symmetrization**. As long as we're naming things, t_1 (and the other t_i that will appear below) are **Lagrange resolvents** or Lagrange-Vandermonde resolvents, and $F(t)$ is the **resolvent polynomial**. Note that Lagrange resolvents are (individual) components of the DFTs of the roots.

There are $3! = 6$ permutations of $(1, 2, 3)$, and they determine 6 Lagrange resolvents:

$$\begin{aligned} t_1 &= r_1 + \omega r_2 + \omega^2 r_3 \\ t_2 &= r_1 + \omega r_3 + \omega^2 r_2 \\ t_3 &= r_2 + \omega r_1 + \omega^2 r_3 \\ t_4 &= r_2 + \omega r_3 + \omega^2 r_1 \\ t_5 &= r_3 + \omega r_1 + \omega^2 r_2 \\ t_6 &= r_3 + \omega r_2 + \omega^2 r_1. \end{aligned} \tag{C_7}$$

The resolvent polynomial is

$$F(t) = (t - t_1)(t - t_2)(t - t_3)(t - t_4)(t - t_5)(t - t_6). \tag{C_8}$$

Any permutation of the r_j permutes the t_k, so every coefficient of $F(t)$ is symmetric in the r_j. By the Fundamental Theorem for Symmetric Polynomials, we'll be able to compute the coefficients of $F(t)$ in terms of the coefficients b, c, and d in Equation (C_1).

Let us pause to make some observations before we expand Equation (C_8). First, it just so happens that t_2 is the third row of Equation (C_6). When we solve $F(t) = 0$ for t_1, we'll likely find t_2 at the same time. Since there is quite a lot of work involved, it's nice to know beforehand that we'll find both resolvents with one computation.

Second, some of the t_i are not significantly different from the others. For example, since $\omega^3 = 1$, t_5 is really just ωt_1. Visually, multiplying t_1 by ω shifts the r_j to the right and wraps r_3 back around to first position. This is the shift property of the DFT, and is explored in the appendix.

The shift property means

$$\begin{aligned} t_1 &= r_1 + \omega r_2 + \omega^2 r_3 \\ t_2 &= r_1 + \omega r_3 + \omega^2 r_2 \\ t_3 &= r_2 + \omega r_1 + \omega^2 r_3 = \omega t_2 \\ t_4 &= r_2 + \omega r_3 + \omega^2 r_1 = \omega^2 t_1 \\ t_5 &= r_3 + \omega r_1 + \omega^2 r_2 = \omega t_1 \\ t_6 &= r_3 + \omega r_2 + \omega^2 r_1 = \omega^2 t_2. \end{aligned} \tag{C_9}$$

The resolvent polynomial is therefore

$$\begin{aligned} F(t) &= (t - t_1)(t - \omega t_1)\left(t - \omega^2 t_1\right)(t - t_2)(t - \omega t_2)\left(t - \omega^2 t_2\right) \\ &= \left(t^3 - t_1^3\right)\left(t^3 - t_2^3\right). \end{aligned} \tag{C_{10}}$$

You can compute this factorization by straightforward expansion, but there is a cleverer way. Since ω and ω^2 are cube roots of unity, and since t_1 is a cube root of t_1^3, the other two roots are ωt_1 and $\omega^2 t_1$. Since we know all three roots of $t^3 - t_1^3$, we know its factorization is

$$t^3 - t_1^3 = (t - t_1)\left(t - \omega t_1\right)\left(t - \omega^2 t_1\right).$$

Pretty clever.

The resolvent polynomial in Equation (C_{10}) expands as

$$F(t) = \left(t^3\right)^2 - \left(t_1^3 + t_2^3\right) t^3 + \left(t_1 t_2\right)^3. \tag{C_{11}}$$

We have completed the cube. The only powers of t in Equation (C_{11}) are multiples of 3 — cubes. The result isn't as nice as completing the square was, because $F(t)$ is a *quadratic* in t^3, not linear. Nevertheless, this is the generalization of completing the square.

We identify $F(t)$ by computing its coefficients $-(t_1 + t_2)$ and $t_1^3 t_2^3$ in terms of the coefficients b, c, and d from Equation (C_1). The Fundamental Theorem guarantees our success. We begin with the simpler of the computations, collecting terms in powers of ω:

$$\begin{aligned} t_1 t_2 &= \left(r_1 + \omega r_2 + \omega^2 r_3\right)\left(r_1 + \omega r_3 + \omega^2 r_2\right) \\ &= \left(r_1^2 + r_2^2 + r_3^2\right) + \left(r_1 r_3 + r_2 r_1 + r_3 r_2\right)\omega + \left(r_1 r_2 + r_2 r_3 + r_3 r_1\right)\omega^2 \\ &= \left(r_1^2 + r_2^2 + r_3^2\right) + \left(r_1 r_2 + r_1 r_3 + r_2 r_3\right)\left(\omega + \omega^2\right). \end{aligned}$$

The last term looks promising: Equation (C_4) says $r_1 r_2 + r_1 r_3 + r_2 r_3 = c$ and direct computation says $\omega + \omega^2 = -1$. The next-to-last term is not too bad, either:

$$\begin{aligned} r_1^2 + r_2^2 + r_3^2 &= \left(r_1 + r_2 + r_3\right)^2 - 2\left(r_1 r_2 + r_1 r_3 + r_2 r_3\right) \quad \text{which, by Equation } (C_4), \text{ is} \\ &= (-b)^2 - 2c. \end{aligned}$$

The total is

$$\begin{aligned} t_1 t_2 &= b^2 - 3c \\ &= -3\left(c - 3\left(\frac{b}{3}\right)^2\right) = -3\hat{c}, \end{aligned} \tag{C_{12}}$$

where $\hat{c}$ was defined in Equation (C_2).

The more demanding of the expansions is $t_1^3 + t_2^3$. We begin with t_1^3. There are $3^3 = 27$ terms in the expansion, which we collect again in powers of ω:

$$\begin{aligned} t_1^3 &= \left(r_1 + \omega r_2 + \omega^2 r_3\right)\left(r_1 + \omega r_2 + \omega^2 r_3\right)\left(r_1 + \omega r_2 + \omega^2 r_3\right) \\ &= \left(r_1^3 + r_2^3 + r_3^3 + 6 r_1 r_2 r_3\right) + 3\left(r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1\right)\omega + 3\left(r_1 r_2^2 + r_2 r_3^2 + r_3 r_1^2\right)\omega^2. \end{aligned}$$

The first term on the last line is symmetric in the r_j, and it is worthwhile to write it in terms of b, c, and d. If we were to set $\omega = \omega^2 = 1$ in the expansion of t_1^3, we would have (without further computation)

$$\left(r_1 + r_2 + r_3\right)^3 = \left(r_1^3 + r_2^3 + r_3^3 + 6 r_1 r_2 r_3\right) + 3\left(r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1\right) + 3\left(r_1 r_2^2 + r_2 r_3^2 + r_3 r_1^2\right).$$

Consequently,

$$\begin{aligned} t_1^3 &= \left(r_1 + r_2 + r_3\right)^3 + 3\left(r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1\right)(\omega - 1) + 3\left(r_1 r_2^2 + r_2 r_3^2 + r_3 r_1^2\right)\left(\omega^2 - 1\right) \\ &= -b^3 + 3\left(r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1\right)(\omega - 1) + 3\left(r_1 r_2^2 + r_2 r_3^2 + r_3 r_1^2\right)\left(\omega^2 - 1\right). \end{aligned}$$

We can also compute t_2^3 without further effort by switching the roles of ω and ω^2. The sum is

$$\begin{aligned} t_1^3 + t_2^3 &= -2b^3 + 3\left(r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1 + r_1 r_2^2 + r_2 r_3^2 + r_3 r_1^2\right)\left(\omega + \omega^2 - 2\right) \\ &= -2b^3 - 9\left(r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1 + r_1 r_2^2 + r_2 r_3^2 + r_3 r_1^2\right). \end{aligned}$$

The last term is symmetric in the r_j, and it is easy to see that it must involve the product of b and c. The division algorithm for the Fundamental Theorem gives us

$$\begin{aligned} r_1^2 r_2 + r_2^2 r_3 + r_3^2 r_1 + r_1 r_2^2 + r_2 r_3^2 + r_3 r_1^2 &= (r_1 + r_2 + r_3)(r_1 r_2 + r_1 r_3 + r_2 r_3) - 3 r_1 r_2 r_3 \\ &= -bc + 3d. \end{aligned}$$

Consequently,

$$\begin{aligned} t_1^3 + t_2^3 &= -2b^3 - 9(-bc + 3d) \\ &= -27\left(d - c\frac{b}{3} + 2\left(\frac{b}{3}\right)^3\right) = -27\hat{d}, \end{aligned}$$

where $\hat{d}$ is defined in Equation (C_2).

The rest of the computation is straightforward. The resolvent equation is

$$F(t) = (t^3)^2 + 27\hat{d}t^3 - 27\hat{c}^3 = 0.$$

This is a quadratic in t^3, with roots satisfying

$$t_k^3 = -27\frac{\hat{d}}{2} \pm 27\frac{\sqrt{\hat{d}^2 + 4\left(\frac{\hat{c}}{3}\right)^3}}{2}.$$

Choose for t_1 any cube root of either expression, say

$$t_1 = -3\sqrt[3]{\frac{\hat{d}}{2} + \frac{\sqrt{\hat{d}^2 + 4\left(\frac{\hat{c}}{3}\right)^3}}{2}}.$$

Equation (C_{12}) means

$$t_2 = \frac{-3\hat{c}}{t_1}.$$

This value is usually written by "rationalizing the denominator" as

$$t_2 = -3\sqrt[3]{\frac{\hat{d}}{2} - \frac{\sqrt{\hat{d}^2 + 4\left(\frac{\hat{c}}{3}\right)^3}}{2}},$$

where we take care that the cube root is chosen so that Equation (C_{12}) holds.

Finally, the roots themselves are given by the inverse DFT in Equation (C_5):

$$\begin{aligned} \begin{bmatrix} r_1 \\ r_2 \\ r_3 \end{bmatrix} &= \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{bmatrix}\begin{bmatrix} -b \\ t_1 \\ t_2 \end{bmatrix} \\ &= \begin{bmatrix} -\frac{b}{3} - \sqrt[3]{\frac{\hat{d}}{2} + \frac{\sqrt{\hat{d}^2+4\left(\frac{\hat{c}}{3}\right)^3}}{2}} - \sqrt[3]{\frac{\hat{d}}{2} - \frac{\sqrt{\hat{d}^2+4\left(\frac{\hat{c}}{3}\right)^3}}{2}} \\ -\frac{b}{3} - \omega^2\sqrt[3]{\frac{\hat{d}}{2} + \frac{\sqrt{\hat{d}^2+4\left(\frac{\hat{c}}{3}\right)^3}}{2}} - \omega\sqrt[3]{\frac{\hat{d}}{2} - \frac{\sqrt{\hat{d}^2+4\left(\frac{\hat{c}}{3}\right)^3}}{2}} \\ -\frac{b}{3} - \omega\sqrt[3]{\frac{\hat{d}}{2} + \frac{\sqrt{\hat{d}^2+4\left(\frac{\hat{c}}{3}\right)^3}}{2}} - \omega^2\sqrt[3]{\frac{\hat{d}}{2} - \frac{\sqrt{\hat{d}^2+4\left(\frac{\hat{c}}{3}\right)^3}}{2}} \end{bmatrix}. \end{aligned}$$

These are **Cardan's formulas**. They are obviously correct when $\hat{c} = 0$. If you like, try them out on

$$f(x) = (x-1)(x-2)(x-3) = x^3 - 6x^2 + 11x - 6$$

to find a disappointing fact: even though the roots are real, Cardan's formulas force complex computations.

The Quartic: The quartic

$$f_4(x) = x^4 + bx^3 + cx^2 + dx + e \tag{B_1}$$

is also called a **biquadratic** (hence the equation number "B_1"). We'll find the quartic "equation" using the DFT. Actually, we'll describe the algorithm without writing it out in full.

If the roots are r_1, r_2, r_3, and r_4, then factoring and expanding f_4 gives

$$\begin{aligned} f_4(x) &= (x - r_1)(x - r_2)(x - r_3)(x - r_4) \\ &= x^4 - (r_1 + r_2 + r_3 + r_4)x^3 + (r_1r_2 + r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 + r_3r_4)x^2 \\ &\quad - (r_1r_2r_3 + r_1r_2r_4 + r_1r_3r_4 + r_2r_3r_4)x + r_1r_2r_3r_4. \end{aligned} \tag{B_2}$$

We deduce, by comparing Equation (B_2) with the coefficients in Equation (B_1) that

$$\begin{aligned} b &= -(r_1 + r_2 + r_3 + r_4), \\ c &= r_1r_2 + r_1r_3 + r_1r_4 + r_2r_3 + r_2r_4 + r_3r_4, \\ d &= -(r_1r_2r_3 + r_1r_2r_4 + r_1r_3r_4 + r_2r_3r_4), \\ e &= r_1r_2r_3r_4. \end{aligned} \tag{B_3}$$

These, of course, are the building blocks to be used in the Fundamental Theorem.

The DFT of the roots is

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{bmatrix} = \begin{bmatrix} r_1 + r_2 + r_3 + r_4 \\ r_1 - r_2i - r_3 + r_4i \\ r_1 - r_2 + r_3 - r_4 \\ r_1 + r_2i - r_3 - r_4i \end{bmatrix}. \tag{B_4}$$

The top row, as always, is symmetric in the roots, and is $-b$. The second and fourth rows are similar — they both qualify as Lagrange resolvents — but the third row is different. There are $4! = 24$ permutations of the roots r_j, but

$$r_1 - r_2 + r_3 - r_4 = (r_1 + r_3) - (r_2 + r_4)$$

takes on only the $\binom{4}{2} = 6$ values

$$\begin{aligned} t_1 &= (r_1 + r_2) - (r_3 + r_4) \\ t_2 &= (r_1 + r_3) - (r_2 + r_4) \\ t_3 &= (r_1 + r_4) - (r_2 + r_3) \\ t_4 &= (r_2 + r_3) - (r_1 + r_4) = -t_3 \\ t_5 &= (r_2 + r_4) - (r_1 + r_3) = -t_2 \\ t_6 &= (r_3 + r_4) - (r_1 + r_2) = -t_1, \end{aligned}$$

and half of those are negatives of the other half. Any of the 24 permutations of the r_j simply permute the t_k. Consequently, the simplest symmetrized polynomial of which t_1 is a root is

$$\begin{aligned} F(t) &= (t - t_1)(t + t_1)(t - t_2)(t + t_2)(t - t_3)(t + t_3) \\ &= \left(t^2 - t_1^2\right)\left(t^2 - t_2^2\right)\left(t^2 - t_3^2\right) \end{aligned}$$

The three t_k^2 are therefore the roots of a cubic with coefficients we can compute using the Fundamental Theorem. Since we have a cubic formula, we can find the three t_k^2, and since we can take square roots, we can find all six of the t_i. This suffices to solve the quartic since

$$\begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \end{bmatrix} = \frac{1}{4} \begin{bmatrix} (r_1 + r_2 + r_3 + r_4) + t_1 + t_2 + t_3 \\ (r_1 + r_2 + r_3 + r_4) + t_1 - t_2 - t_3 \\ (r_1 + r_2 + r_3 + r_4) - t_1 + t_2 - t_3 \\ (r_1 + r_2 + r_3 + r_4) - t_1 - t_2 + t_3 \end{bmatrix}.$$

Remark: This "trick" avoids taking the 4-dimensional DFT. In a sense, the trick amounts to using the 4-dimensional *fast* Fourier Transform (FFT). One can also solve the quartic using the Lagrange resolvents. See Edwards[6].

Appendix: Fourier Transforms: Fourier Transforms represent functions using trigonometric functions — sines and cosines. The most intuitive of the transforms is Fourier Series, which writes a function $x(t)$ on the interval $0 \leq t \leq T$ as

$$\begin{aligned} x(t) = a_0 + a_1 \cos\left(\frac{2\pi t}{T}\right) + a_2 \cos\left(2\frac{2\pi t}{T}\right) + a_3 \cos\left(3\frac{2\pi t}{T}\right) + \cdots \\ + b_1 \sin\left(\frac{2\pi t}{T}\right) + b_2 \sin\left(2\frac{2\pi t}{T}\right) + b_3 \sin\left(3\frac{2\pi t}{T}\right) + \cdots . \end{aligned} \tag{1}$$

The Fourier transform maps the function $x(t)$ to the coefficients a_i and b_i.

The sines and cosines in Equation (1) are periodic with common period T. The representation of $x(t)$ in Equation (1) is therefore useful if x represents some periodic phenomenon: tides, pendulums, or masses on springs. Much of the language is related to music, where

$$\begin{aligned} a_1 \cos\left(\frac{2\pi t}{T}\right) + b_1 \sin\left(\frac{2\pi t}{T}\right) &\text{ represents the } \textbf{fundamental} \text{ or } \textbf{first harmonic}, \\ a_2 \cos\left(2\frac{2\pi t}{T}\right) + b_2 \sin\left(2\frac{2\pi t}{T}\right) &\text{ represents the } \textbf{first overtone} \text{ or } \textbf{second harmonic}, \\ a_3 \cos\left(3\frac{2\pi t}{T}\right) + b_3 \sin\left(3\frac{2\pi t}{T}\right) &\text{ represents the } \textbf{second overtone} \text{ or } \textbf{third harmonic}, \end{aligned}$$

and so on. The first overtone is an octave above the fundamental because doubling the frequency increases the pitch by an octave. The second overtone is a fifth above the octave because tripling the frequency increases the pitch by a fifth above the octave. The third overtone is two octaves above the fundamental, and so on. The Fourier series therefore decomposes a signal $x(t)$ into its harmonics. The study of Fourier Transforms is called **Harmonic Analysis**.

Remark: The coefficient a_0 in Equation (1) is universally written as $\frac{a_0}{2}$ in textbooks in order to simplify the formulas, as we'll see below.

Remark: The coefficients a_i and b_i are easy to find in theory. The trigonometric functions all have average value zero, so if Equation (1) holds, then

$$\text{the average of } x(\cdot) = a_0.$$

To find the other coefficients, multiply both sides of Equation (1) by one of the trig functions, say $\cos\left(\frac{2\pi t}{T}\right)$:

$$\begin{aligned} \cos\left(\frac{2\pi t}{T}\right) x(t) = a_0 \cos\left(\frac{2\pi t}{T}\right) + a_1 \cos^2\left(\frac{2\pi t}{T}\right) + a_2 \cos\left(\frac{2\pi t}{T}\right) \cos\left(2\frac{2\pi t}{T}\right) + + \cdots \\ + b_1 \cos\left(\frac{2\pi t}{T}\right) \sin\left(\frac{2\pi t}{T}\right) + b_2 \cos\left(\frac{2\pi t}{T}\right) \sin\left(2\frac{2\pi t}{T}\right) + + \cdots . \end{aligned}$$

The average of the first term on the right is zero — that's why we multiplied by the cosine. The trig identity

$$\cos^2(w) = \frac{1 + \cos(2w)}{2}$$

[6] Harold M. Edwards, *Galois Theory*, Springer-Verlag, 1984, pp. 21, Exercise 4. Note that Edwards uses "complex conjugate" to mean "exchange i and $-i$ in t_j, but don't conjugate the roots r_k".

means the average of the second term on the right is $\frac{a_1}{2}$. All the remaining terms on the right have average value zero by the trig identities

$$\begin{aligned}\cos(kw)\cos(jw) &= \frac{\cos((k-j)w)+\cos((k+j)w)}{2}\\ \sin(kw)\sin(jw) &= \frac{\cos((k-j)w)-\cos((k+j)w)}{2}\\ \sin(kw)\cos(jw) &= \frac{\sin((k+j)w)+\sin((k-j)w)}{2}.\end{aligned} \tag{2}$$

Consequently,

$$\text{the average of } \cos\left(\tfrac{2\pi t}{T}\right) x(t) = \frac{a_1}{2},$$

and similarly for the other coefficients. In short, if Equation (1) is to hold, then

$$\begin{aligned}\frac{a_k}{2} &= \frac{1}{T}\int_0^T \cos\left(k\frac{2\pi t}{T}\right) x(t)\,dt, \text{ and}\\ \frac{b_k}{2} &= \frac{1}{T}\int_0^T \sin\left(k\frac{2\pi t}{T}\right) x(t)\,dt\end{aligned}$$

for all integers $k > 0$. The formula holds for a_0 as well, if we replace a_0 in Equation (1) by $\frac{a_0}{2}$ (as suggested above).

The Real DFT: The Discrete Fourier Transform does for vectors what the Fourier series does for functions:

$$\begin{bmatrix}x_0\\x_1\\x_2\\x_3\\\vdots\\x_{\hat{n}}\end{bmatrix} = a_0\begin{bmatrix}1\\1\\1\\1\\\vdots\\1\end{bmatrix} + a_1\begin{bmatrix}c_0\\c_1\\c_2\\c_3\\\vdots\\c_{\hat{n}}\end{bmatrix} + b_1\begin{bmatrix}s_0\\s_1\\s_2\\s_3\\\vdots\\s_{\hat{n}}\end{bmatrix} + a_2\begin{bmatrix}c_0\\c_2\\c_4\\c_6\\\vdots\\c_{2\hat{n}}\end{bmatrix} + b_2\begin{bmatrix}s_0\\s_2\\s_4\\s_6\\\vdots\\s_{2\hat{n}}\end{bmatrix} + a_3\begin{bmatrix}c_0\\c_3\\c_6\\c_9\\\vdots\\c_{3\hat{n}}\end{bmatrix} + b_3\begin{bmatrix}s_0\\s_3\\s_6\\s_9\\\vdots\\s_{3\hat{n}}\end{bmatrix} + \cdots, \tag{3}$$

where, to save space, we abbreviate $\hat{n} = n-1$ and

$$\begin{aligned}c_j &= \cos\left(j\frac{2\pi}{n}\right)\\ s_j &= \sin\left(j\frac{2\pi}{n}\right).\end{aligned}$$

Each column spells out in full the (discretized) trig function from the Fourier series; you can read the values off, top-to-bottom.

The sum in Equation (3) terminates, of course, because there can not be more than n linearly independent vectors in n-dimensional space. If n is odd, the last vector has elements $s_{i\frac{n-1}{2}}$; if n is even, the last vector has elements $c_{i\frac{n}{2}}$. The highest frequency present is the **Nyquist** frequency.

Equation (3) is more compactly written in matrix form:

$$\underbrace{\begin{bmatrix}x_0\\x_1\\x_2\\x_3\\\vdots\\x_{\hat{n}}\end{bmatrix}}_{\mathsf{x}} = \underbrace{\begin{bmatrix}1 & c_0 & s_0 & c_0 & s_0 & c_0 & s_0 & \cdots\\ 1 & c_1 & s_1 & c_2 & s_2 & c_3 & s_3 & \cdots\\ 1 & c_2 & s_2 & c_4 & s_4 & c_6 & s_6 & \cdots\\ 1 & c_3 & s_3 & c_6 & s_6 & c_9 & s_9 & \cdots\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots\\ 1 & c_{\hat{n}} & s_{\hat{n}} & c_{2\hat{n}} & s_{2\hat{n}} & c_{3\hat{n}} & s_{3\hat{n}} & \cdots\end{bmatrix}}_{\mathsf{C}} \begin{bmatrix}a_0\\a_1\\b_1\\a_2\\b_2\\a_3\\b_3\\\vdots\end{bmatrix} \tag{4}$$

The matrix C is $n \times n$.

The (real) DFT solves Equation (4) for the coefficients a_i and b_i. The philosophy is the same as in the case of Fourier series: the average of any column except the first is zero, so the average of x is a_0. The process for finding the other coefficients a_i and b_i mimics the process for Fourier series: multiply (component-wise) any column by any other column and average. For example, the (component-wise) product of the forth and second columns is

$$\begin{bmatrix} c_0c_0 \\ c_2c_1 \\ c_4c_2 \\ c_6c_3 \\ \vdots \\ c_{2\hat{n}}c_{\hat{n}} \end{bmatrix} \text{ which, by Equation (2), is } \frac{1}{2}\begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{\hat{n}} \end{bmatrix} + \frac{1}{2}\begin{bmatrix} c_0 \\ c_3 \\ c_6 \\ c_9 \\ \vdots \\ c_{3\hat{n}} \end{bmatrix}.$$

Each of the columns in the sum has average value zero.

We have a name for the sum (instead of the average) of the (component-wise) products of the columns: the dot product. In fact, the array of all such sums is simply

$$\mathsf{C}^T\mathsf{C} = \begin{bmatrix} 1 & c_0 & s_0 & c_0 & s_0 & c_0 & s_0 & \cdots \\ 1 & c_1 & s_1 & c_2 & s_2 & c_3 & s_3 & \cdots \\ 1 & c_2 & s_2 & c_4 & s_4 & c_6 & s_6 & \cdots \\ 1 & c_3 & s_3 & c_6 & s_6 & c_9 & s_9 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\ 1 & c_{\hat{n}} & s_{\hat{n}} & c_{2\hat{n}} & s_{2\hat{n}} & c_{3\hat{n}} & s_{3\hat{n}} & \cdots \end{bmatrix}^T \begin{bmatrix} 1 & c_0 & s_0 & c_0 & s_0 & c_0 & s_0 & \cdots \\ 1 & c_1 & s_1 & c_2 & s_2 & c_3 & s_3 & \cdots \\ 1 & c_2 & s_2 & c_4 & s_4 & c_6 & s_6 & \cdots \\ 1 & c_3 & s_3 & c_6 & s_6 & c_9 & s_9 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \\ 1 & c_{\hat{n}} & s_{\hat{n}} & c_{2\hat{n}} & s_{2\hat{n}} & c_{3\hat{n}} & s_{3\hat{n}} & \cdots \end{bmatrix}.$$

By the trig identities in Equation (2), the product is is

$$\mathsf{C}^T\mathsf{C} = \begin{bmatrix} n & 0 & 0 & 0 & \cdots & 0 \\ 0 & \frac{n}{2} & 0 & 0 & \cdots & 0 \\ 0 & 0 & \frac{n}{2} & 0 & \cdots & 0 \\ 0 & 0 & 0 & \frac{n}{2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \frac{n}{2} \end{bmatrix}$$

By this time, we are strongly motivated to make that leading coefficient $\frac{a_0}{2}$ instead of a_0. If we do, then the real DFT is $\mathsf{C}^{-1} = \frac{2}{n}\mathsf{C}^T$. It maps vectors x to their Fourier coefficients $\frac{2}{n}\mathsf{C}^T\mathsf{x}$. The inverse DFT is then C. In some of the literature, multiplication by $\frac{2}{n}\mathsf{C}^T$ is called **analysis** and multiplication by C is called **synthesis**. The scalar $\frac{2}{n}$ often migrates from multiplying C^T to multiplying C. Sometimes it is evenly split between the two as a factor of $\sqrt{\frac{2}{n}}$.

Remark: The fact that $\mathsf{C}^T\mathsf{C}$ is diagonal means that the columns of C are mutually orthogonal — their dot product is zero.

The Complex DFT: The complex DFT is essentially the real DFT with trig functions replaced by complex exponentials using Euler's formula

$$e^{iz} = \cos(z) + i\sin(z). \tag{5}$$

In this equation, $i = \sqrt{-1}$, and the formula is valid for all complex numbers z. The proof is obvious if you believe in (complex) power series. Just write out the (well-known) power series

$$\begin{aligned} e^z &= 1 + \frac{z}{1!} + \frac{z^2}{2!} + \frac{z^3}{3!} + \frac{z^4}{4!} + \cdots \\ \cos(z) &= 1 \qquad - \frac{z^2}{2!} \qquad + \frac{z^4}{4!} + \cdots \\ \sin(z) &= \qquad \frac{z}{1!} \qquad - \frac{z^3}{3!} \qquad + \cdots, \end{aligned}$$

replace z with iz in the exponential, and compare. Alternatively, if you like differential equations instead, solve the initial value problem

$$\begin{aligned} y'' + y &= 0 \\ y(0) &= a \\ y'(0) &= b \end{aligned}$$

in two different ways: first, the "obvious" solution is

$$y(t) = a\cos(t) + b\sin(t).$$

Second, guess a homogeneous solution of the form

$$y(t) = e^{\lambda t}$$

and substitute in:

$$y'' + y = \left(\lambda^2 + 1\right) y,$$

which is zero if $\lambda^2 = -1$. There are two possible solutions, $\lambda = \pm i$, so the general homogeneous solution is

$$y(t) = c_1 e^{it} + c_2 e^{-it}.$$

To match the initial conditions we choose

$$\begin{aligned} y(0) &= c_1 + c_2 = a \\ y'(0) &= c_1 i - c_2 i = b. \end{aligned}$$

The coefficients are therefore

$$\begin{aligned} c_1 &= \frac{a - ib}{2} \\ c_2 &= \frac{a + ib}{2}, \end{aligned}$$

and the solution is

$$y(t) = a\frac{e^{it} + e^{-it}}{2} - ib\frac{e^{it} - e^{-it}}{2}.$$

By the uniqueness theorem for initial-value problems,

$$\begin{aligned} \cos(t) &= \frac{e^{it} + e^{-it}}{2} \\ \sin(t) &= \frac{e^{it} - e^{-it}}{2i}. \end{aligned}$$

It is easy to check that these are equivalent to Euler's Equation (5).

Exponential identities are simpler than trigonometric identities, so we trade sines and cosines for complex exponentials using Euler's formula. If we abbreviate

$$\omega = e^{\frac{-2\pi i}{n}},$$

then a little experimentation suggests we trade C^T for

$$\mathsf{F} = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(n-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \omega^{3(n-1)} & \cdots & \omega^{(n-1)^2} \end{bmatrix}.$$

F is (the matrix representing) the n-dimensional complex DFT. The first 3 DFTs, which are the only ones needed to solve the cubic and quartic, are

$$\mathsf{F}_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$\mathsf{F}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix},$$

where $\omega = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$ and we have simplified $\omega^4 = \omega$ using $\omega^3 = 1$,

$$\mathsf{F}_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}$$

Properties of the complex DFT are generally simpler to prove than the corresponding properties for the real DFT because the exponential identities are simpler than the corresponding trig identities. The important property, valid for every integer k, is

$$\left(\omega^k\right)^n = \left(e^{\frac{-k2\pi i}{n}}\right)^n = e^{-2k\pi i} = \cos(2k\pi) + i\sin(2k\pi) = 1.$$

In other words, all of the ω^k appearing in F are roots of

$$z^n - 1 = (z-1)\underbrace{\left(z^{n-1} + z^{n-2} + \cdots + z^2 + z + 1\right)}_{\varphi_n(z)}.$$

These roots ω^k are (appropriately) called **roots of unity**. Their geometry is quite regular: the powers ω^k are equally spaced around the unit circle in the complex plane. Euler's formula makes this geometry easy to see. Note that the complex conjugate of any root of unity is also a root of unity:

$$\overline{\omega^k} = \omega^{n-k},$$

again by Euler's formula.

Every root of unity except 1 satisfies

$$\varphi(z) = z^{n-1} + z^{n-2} + \cdots + z^2 + z + 1 = 0.$$

As a consequence, we have the "orthogonality conditions"

$$1 + \omega^k + \omega^{2k} + \cdots + \omega^{(n-1)k} = \begin{cases} 0 & \text{if } k \neq 0 \pmod n, \\ n & \text{if } k = 0 \pmod n. \end{cases}$$

These computations are easy to "see" from the geometry: the average of points equally spaced around the unit circle *must* be the center of the circle — namely, zero.

The complex orthogonality conditions are generally easier to apply than the trig identities. For example, it is not too tedious to check that

$$\overline{\mathsf{F}^T}\mathsf{F} = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega^{n-1} & \omega^{n-2} & \omega^{n-3} & \cdots & \omega \\ 1 & \omega^{n-2} & \omega^{n-4} & \omega^{n-6} & \cdots & \omega^2 \\ 1 & \omega^{n-3} & \omega^{n-6} & \omega^{n-9} & \cdots & \omega^3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{n-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(n-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \omega^{3(n-1)} & \cdots & \omega^{(n-1)^2} \end{bmatrix}$$

$$= \begin{bmatrix} n & 0 & 0 & 0 & \cdots & 0 \\ 0 & n & 0 & 0 & \cdots & 0 \\ 0 & 0 & n & 0 & \cdots & 0 \\ 0 & 0 & 0 & n & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & n \end{bmatrix} = n\mathsf{I}.$$

The columns of F are mutually orthogonal (complex orthogonality requires $\bar{\mathsf{x}}^T\mathsf{y} = 0$ rather than $\mathsf{x}^T\mathsf{y} = 0$). In the language of linear algebra, except for a scaling factor of n, F is **unitary**.

Shifts: Exponentials convert shifts into products:

$$e^{x+h} = e^x e^h.$$

The DFT enjoys a corresponding property. A shift of the data vector means, in this context,

$$\mathsf{x} = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_{\hat{n}} \end{bmatrix} \text{ shifts to } \mathsf{Sx} = \begin{bmatrix} x_{\hat{n}} \\ x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{\hat{n}-1} \end{bmatrix},$$

where we have abbreviated (again) $n - 1 = \hat{n}$. The shift pushes the components of x down, wrapping the bottom component back to the top of the vector. The effect of the DFT on a shift is easy to see in a specific example:

$$\underbrace{\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}}_{\mathsf{F}_3} \underbrace{\begin{bmatrix} x_2 \\ x_0 \\ x_1 \end{bmatrix}}_{\mathsf{Sx}} = \begin{bmatrix} x_2 + x_0 + x_1 \\ x_2 + \omega x_0 + \omega^2 x_1 \\ x_2 + \omega^2 x_0 + \omega x_1 \end{bmatrix}$$

$$= \begin{bmatrix} x_0 + x_1 + x_2 \\ \omega(x_0 + \omega x_1 + \omega^2 x_2) \\ \omega^2(x_0 + \omega^2 x_1 + \omega x_2) \end{bmatrix} \quad \text{since } \omega^3 = 1,$$

$$= \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}}_{\mathsf{D}} \underbrace{\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}}_{\mathsf{F}_3} \underbrace{\begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix}}_{\mathsf{x}}$$

Shifting the vector x first, then taking the DFT is the same as taking the DFT first and multiplying by the diagonal matrix D. This behavior extends to DFTs of all dimension.