Contents

Fourier Transforms on Finite Groups

Tianyu Bai, Bruno Segovia, & Qilin Ye

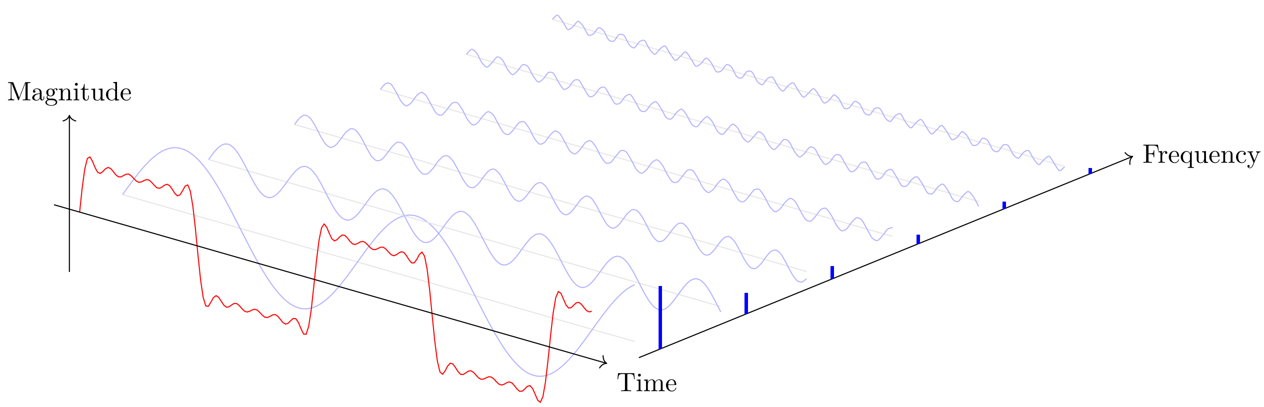
April 13, 2021

0 But What is a Fourier Transform?

A magical theorem in mathematical analysis says the following:

> A *suitably nice* function $f\colon \mathbb{R} \to \mathbb{R}$ can be approximated *nicely* by a combination of basic trigonometric polynomials of form $\sin(nx)$ and $\cos(nx)$ where $n \in \mathbb{Z}$.

Heuristically, think of the sounds that our ears hear every day. We hear a wide range of pitches (frequencies of sound waves) and levels of loudness (amplitudes). Among all these chaotic combinations of sounds, how can we even tell what we are actually hearing? It turns out that our inner ears, in particular the *basilar membrane*, automatically carry out **Fourier transforms**: the original sound wave, a function of time, is expressed as a "combination" of a bunch of simpler, nicer sound waves that resemble the sine curves with different frequencies. Our brains then receives the latter, i.e., the "frequency decomposition" of these sound waves. This explains why we are able to identify musical chords consisting of multiple notes.



Our focus today, however, is on finite Fourier transforms on groups (this is 410 not 425 after all).

For the remainder of this presentation, we assume $(G, +)$ is a finite cyclic group of order n where $+$ denotes the usual addition (so it can be identified with $\mathbb{Z}/n\mathbb{Z}$).

1 Preliminaries and Basic Definitions

1.1 Complex Numbers

We begin by bringing up some basic definitions and properties, some of which hopefully you have seen elsewhere:

(1) For $z = a + bi \in \mathbb{C}$, the **modulus** of z, written $|z|$, is defined to be $\sqrt{a^2 + b^2}$ (the distance to origin).

(2) For $z = a + bi \in \mathbb{C}$, the **conjugate** of z, written $\overline{z}$, is defined to be $a - bi$.

(3) Let S^1 be the **unit circle** in $\mathbb{C}$, that is, $S^1 \coloneqq \{z \in \mathbb{C} : |z| = 1\}$.

(4) **Euler's formula**: $e^{i\theta} = \cos(\theta) + i\sin(\theta)$. More importantly, each $z \in S^1$ can be uniquely represented by $e^{i\theta}$ for some $\theta \in [0, 2\pi)$.

1.2 Convolution (on Finite Groups): A $*$ is Born

Yes, it looks like a fancy multiplication symbol, and yes, it is an "upgraded" version of function multiplication (which we'll show very soon).

It is probably more intuitive to think of convolutions in probability theory. Suppose we are rolling two unfair (just to make the idea clearer) six-sided dices. Let X be the outcome of the first dice and let Y that of the second. What would be the distribution of the sum $Z = X + Y$?

For example, what events would lead to $Z = 7$, given X, Y can output any integer in $[1, 6]$? The answer is clear: 7 can be written as $1 + 6, 2 + 5$, ..., all the way till $6 + 1$. Therefore the probability of $Z = 7$ is given by

$$P(Z = 7) = \sum_{i=1}^{6} P(X = i)P(Y = 7 - i),$$

and more generally,

$$P(Z = z) = \sum_{i=1}^{6} P(X = i)P(Y = z - i)$$

as long as both functions on the RHS make sense (e.g., to get $Z = 8$, both rolls must be at least 2 as $1 + 6 < 8$).

Definition: Convolution (on finite group)

Let f, g be functions $G \to \mathbb{C}$. We define the **convolution** of f, g written $f * g$ and read "f splat g", by

$$(f * g)(a) = \frac{1}{|G|} \sum_{b \in G} f(a - b)g(b) \text{ for any } a \in G.$$

Definition: Indicator Function

For any $a \in G$, we define the **indicator function** $\delta_a : G \to \{0, 1\}$ by $\delta_a(x) = 1$ if $x = a$ and $\delta_a \equiv 0$ otherwise. *Relate this to the Dirac delta function if you have any Fourier background.*

Convolution is extremely useful in a variety of fields. From the definitions above, we will be able to derive a list of "nice" properties of convolutions (on finite groups):

(1) $|G|\delta_0$ is the identity for convolution (note that $|G|$ is just a constant):

$$(f * |G|\delta_0)(a) = \frac{1}{|G|}\sum_{b\in G} f(a-b)(|G|\delta_0)(b) = \frac{1}{|G|}\cdot f(a)|G| = f(a) \qquad \text{for all } a \in G$$

because $(|G|\delta_0)(b)$ only evaluates to nonzero (to 1) when $b = a$.

(2) $*$ is commutative, i.e., $f * g = g * f$ (a nice property to have in 410, right?):

$$\begin{aligned}(f * g)(a) &= \frac{1}{|G|}\sum_{b\in G} f(a-b)g(b) = \frac{1}{|G|}\sum_{a-b\in G} f(a-(a-b))g(a-b) \\ &= \frac{1}{|G|}\sum_{b\in G} f(a-(a-b))g(a-b) && \sum_{a-b\in G} = \sum_{b\in G}\text{: they sum over the same elements} \\ &= \frac{1}{|G|}\sum_{b\in G} f(b)g(a-b) = (g * f)(a).\end{aligned}$$

(3) $*$ is (left) distributive, i.e., $f * (g+h) = f * g + f * h$:

$$\begin{aligned}[f * (g+h)](a) &= \frac{1}{|G|}\sum_{b\in G} f(a-b)[g(b)+h(b)] \\ &= \frac{1}{|G|}\sum_{b\in G} f(a-b)g(b) + \frac{1}{|G|}\sum_{b\in G} f(a-b)h(b) \\ &= (f * g)(a) + (f * h)(a).\end{aligned}$$

(4) $*$ is associative, i.e., $f * (g * h) = (f * g) * h$ (this is really just done by brutal computation along with some slick ways to rewrite the summations; similar to (2)):

$$\begin{aligned}[(f * g) * h](a) &= \frac{1}{|G|}\sum_b (f * g)(a-b)h(b) \\ &= \frac{1}{|G|}\sum_b \left[\frac{1}{|G|}\sum_c f(a-b-c)g(c)\right]h(b) \\ &= \frac{1}{|G|^2}\sum_b\sum_c f(a-b-c)g(c)h(b) \\ &= \frac{1}{|G|^2}\sum_{b'}\sum_{c'} f(a-b)g(b-c)h(c) && \text{setting } b' := b+c \text{ and } c' := b \\ &= \frac{1}{|G|^2}\sum_{b}\sum_{c} f(a-b)g(b-c)h(c) && \sum_{b'} = \sum_b \text{ and } \sum_{c'} = \sum_c \\ &= \frac{1}{|G|}\sum_b f(a-b)\left[\frac{1}{|G|}\sum_c g(b-c)h(c)\right] \\ &= \frac{1}{|G|}\sum_b f(a-b)(g * h)(b) \\ &= [f * (g * h)](a).\end{aligned}$$

1.3 Dual Groups

Consider the two groups $(G, +)$ and $(S^1, \cdot)$ [notice that the latter is indeed a group by Euler's formula]. Between groups we have various morphisms, and this leads to the following definition:

Definition: Dual Group

Let G be defined as above. We define $\hat{G}$, the **dual group** of G, to be the group of homomorphisms $\chi: G \to S^1$. The group operation is simply defined to be function multiplication, i.e., for any $\chi_1, \chi_2 \in \hat{G}$ and $g \in G$, we have $(\chi_1\chi_2)(g) = \chi_1(g) \cdot \chi_2(g)$. (*These χs are called* ***characters***.)

Remark. It might help to simply not try to understand what an abstract homomorphism $\chi : G \to S^1$ looks like. We are more interested in the group itself, i.e., the collection of these homomorphisms and the interactions among them. Not a big deal if this definition seems too abstract on first glance; hopefully it will come along nicely later.

2 Fourier Transform of $f: G \to \mathbb{C}$

2.1 Fourier Transform of $f: G \to \mathbb{C}$

But why do we need to abruptly introduce the notion of a dual group?

Recall from the very beginning that, when our ears hear something, they decompose the sound waves, a function $f: \mathbb{R} \to \mathbb{C}$ of time, i.e., $f(t)$, into a function $\hat{f}: \hat{\mathbb{R}} \to \mathbb{C}$ of frequencies, i.e., $\hat{f}(\xi)$. By doing so, our brain understands what the decomposition of the sound looks like. The underlying magic here is that the **Pontryagin dual** $\hat{\mathbb{R}}$ of $\mathbb{R}$ is in fact $\mathbb{R}$ itself, and this explains why f and $\hat{f}$ are ultimately both functions $\mathbb{R} \to \mathbb{C}$.

The upshot of the above paragraph is that under Fourier transform, a function $f: \mathbb{R} \to \mathbb{C}$ becomes a function $\hat{f}: \hat{\mathbb{R}} \to \mathbb{C}$. Connecting this to our finite cyclic group G, the Fourier transform of a function $f: G \to \mathbb{C}$ is, unsurprisingly, a function $\hat{f}: \hat{G} \to \mathbb{C}$ (yeah it's still abstract...). To put formally:

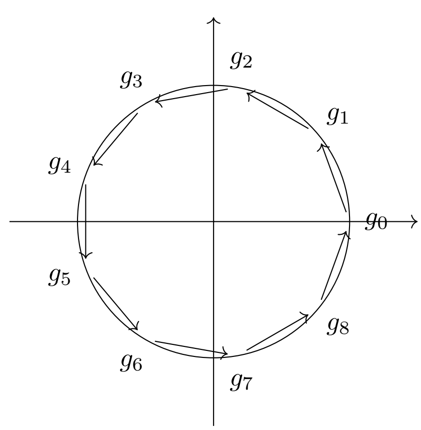
Definition: Fourier Transform

We define the **Fourier transform** $\hat{f}: \hat{G} \to \mathbb{C}$ of a function $f: G \to \mathbb{C}$ by

$$\hat{f}(\chi) = \frac{1}{|G|} \sum_{y \in G} f(y)\overline{\chi(y)}.$$

(To wrap your head around it: χ is an element of $\hat{G}$, i.e., a homomorphism $\chi : G \to S^1$, $\chi(y)$ a complex number, and $\overline{\chi(y)}$ the complex conjugate of $\chi(y)$.)

In our case, since $(G, +)$ can be identified with $\mathbb{Z}/n\mathbb{Z}$, we see $\hat{G}$ is in fact the set of all homomorphisms from G to the multiplicative groups of roots of unity in $\mathbb{C}$.



Heuristically, suppose $G = \langle g \rangle$ and $\chi(g)$ corresponds to the vertex labeled g_1 in the diagram (by Euler's formula, this point is $e^{2\pi i/n}$). Traversing through the list $(g, g^2, \ldots, g^{n-1}, g^n)$ under multiplication by g is equivalent to traversing through the list of vertices of the polygon since $e^{2k\pi i/n}$ is precisely the vertex g_k. (Similar to how g^n is the identity of the group G of order n, we define $g_n \coloneqq g_0 = 1$, the identity element of the multiplicative group of roots of unity in $\mathbb{C}$.) To put this into mathematical language:

Definition

Suppose $a, b \in G = \mathbb{Z}/n\mathbb{Z}$. We define $\chi_a \in \hat{G}$ by $\chi_a(b) = e^{2\pi i ab/n}$. Note that since $e^{2\pi i} = e^{2\pi i n/n} = 1$, the exponent already takes care of the "modulo n" part.

2.2 The Space $L^2(\mathbb{Z}/n\mathbb{Z})$

Now we consider the space of functions $L^2(\mathbb{Z}/n\mathbb{Z}) \coloneqq \{f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}\}$. Notice that our previously discussed χ_as are all in this space. In fact, this is an **inner product space** (a vector space equipped with an inner product) where the inner product is given by

$$\langle f, g \rangle \coloneqq \sum_{x \in \mathbb{Z}/n\mathbb{Z}} f(x)\overline{g(x)}.$$

In addition, $L^2(\mathbb{Z}/n\mathbb{Z})$ is <u>n-dimensional</u> and — you might have guessed — a basis is naturally given by χ_as where $a \in G$. Even better, they don't just form a basis — they are an <u>orthogonal basis</u>.

Theorem: $\{\chi_a\}$ is Orthogonal

For $a, b \in \mathbb{Z}/n\mathbb{Z}$, define $\chi_a(b) = e^{2\pi i ab/n}$ (as above). Then $\{\chi_a : a \in \mathbb{Z}/n\mathbb{Z}\}$ forms an orthogonal set, i.e.,

$$\langle \chi_a, \chi_b \rangle = \begin{cases} n & a \equiv b \pmod{n} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The inner product gives $\langle \chi_a, \chi_b \rangle = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_a(x)\overline{\chi_b(x)} = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} e^{2\pi i ax/n} e^{-2\pi i bx/n} = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_{a-b}(x)$. If $n \mid a - b$ then we are immediately done since there are n elements in $\mathbb{Z}/n\mathbb{Z}$ and each $\chi_{a-b}(x)$ is $e^{2\pi i(a-b)/n} = 1$.

On the other hand, if $n \mid a - b$, for convenience write $c = a - b$ and $S = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_x(x)$ the RHS. Notice that

$$\{\chi_c(0), \chi_c(1), \ldots, \chi_c(n-1)\} = \{\chi_c(1), \chi_c(2), \ldots, \chi_c(n)\},$$

i.e., the set is invariant under right shift $x \mapsto x + 1$. Therefore,

$$\chi_c(1)S = \chi_c(1) \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_c(x) = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_c(1)\chi_c(x) = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \chi_c(x+1) = S,$$

which can happen only if $\chi_c(1) = 1$ or $S = 0$. Note that $\chi_c(1) = \chi_{a-b}(1) = e^{2\pi i(a-b)/n}$. Since $n \mid a - b$ by assumption, this expression cannot be 1, and therefore $S = 0$, as desired. $\square$

2.3 Properties of the Fourier Transform

One of the best things about Fourier transform is that it reduces the complicated convolution to a much simpler form.

Theorem

Let $G = \mathbb{Z}/n\mathbb{Z}$ and let $\chi \in \hat{G}$. Then:

(1) The Fourier transform of the convolution of $f, g: G \to \mathbb{C}$ is equal to the element-wise product of their Fourier transforms:

$$\widehat{f * g}(\chi) = \hat{f}(\chi) \cdot \hat{g}(\chi).$$

(2) Given all the Fourier transforms $\hat{f}(\chi)$, we can recover f via the *Fourier inversion formula*

$$f(x) = \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x).$$

Proof of (1). Hopefully, by now you are fairly comfortable with the notion of convolution (so I won't need to use different colors on different variables).

$$\begin{aligned}
\widehat{f * g}(\chi) &= \frac{1}{|G|} \sum_{z \in G} (f * g)(z)\overline{\chi(z)} \\
&= \frac{1}{|G|} \sum_{z \in G} \left[\frac{1}{|G|} \sum_{y \in G} f(z-y)g(y) \right] \overline{\chi(z)} \\
&= \frac{1}{|G|^2} \sum_{z \in G} \sum_{y \in G} f(z-y)g(y)\overline{\chi(z)} \\
&= \frac{1}{|G|^2} \sum_{y \in G} g(y) \sum_{w \in G} f(w)\overline{\chi(w+y)} && \text{setting } w := z - y \\
&= \left[\frac{1}{|G|} \sum_{y \in G} g(y)\overline{\chi(y)} \right] \left[\frac{1}{|G|} \sum_{w \in G} f(w)\overline{\chi(w)} \right] \\
&= \hat{f}(\chi) \cdot \hat{g}(\chi).
\end{aligned}$$

□

Proof of (2). First recall that $\overline{\chi_a(y)} = e^{-2\pi i a y/n} = e^{2\pi i(-ay)/n} = \chi_a(-y)$ for all $a, y \in \mathbb{Z}/n\mathbb{Z}$. Then,

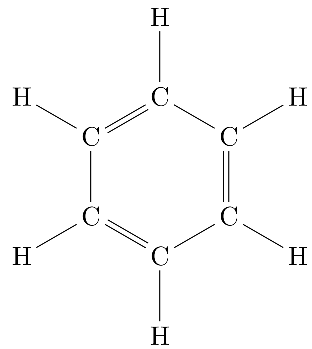
$$\begin{aligned}
\sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x) &= \sum_{\chi \in \hat{G}} \chi(x) \left[\frac{1}{|G|} \sum_{y \in G} f(y)\overline{\chi(y)} \right] \\
&= \sum_{y \in G} f(y) \left[\frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(x)\overline{\chi(y)} \right] \\
&= \sum_{y \in G} f(y) \left[\frac{1}{|G|} \langle \chi_x, \chi_y \rangle \right].
\end{aligned}$$

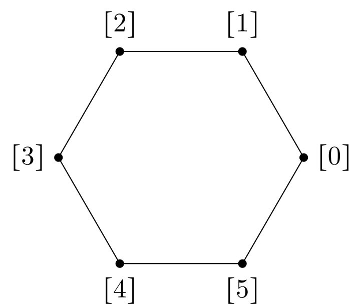
By the orthogonality theorem previously proven, $\langle \chi_x, \chi_y \rangle / |G|$ is 1 if $y = x$ and 0 otherwise, so indeed the RHS evaluates to $f(x)$, and we recover the Fourier inversion formula. □

3 Application: Stability of Benzene

3.1 Benzene & Some *Black Boxes*

In chemistry, Benzene, C_6H_6, is known to be very stable due to its *delocalized* π*-electrons*. The most notable feature of its structure (diagram on the left) is its hexagonal ring, which highly resembles the Cayley graph $X(\mathbb{Z}/6\mathbb{Z}, S)$ (middle) where $S \coloneqq \{\pm 1 \pmod 6\}$.





$$A = \begin{bmatrix} 0 & 1 & & & & 1 \\ 1 & 0 & 1 & & & \\ & 1 & 0 & 1 & & \\ & & 1 & 0 & 1 & \\ & & & 1 & 0 & 1 \\ 1 & & & & 1 & 0 \end{bmatrix}$$

With a few *black boxes* (which you need to take for granted...), we are able to show why is Benzene stable. The **adjacency matrix** of this Cayley graph is the matrix A on the right.

Black box #1: we can view this adjacency matrix as a matrix of the *adjacency operator* acting on complex-valued functions $f(x)$ for x in the Cayley graph $X(\mathbb{Z}/6\mathbb{Z}, S)$. If we generalize the notion of indicator function by defining

$$\delta_S(x) = \begin{cases} 1 & x \in S \\ 0 & \text{otherwise,} \end{cases}$$

then the action of this *adjacency operator* is given by

$$Af(x) = \sum_{s \in S} f(x+s) = f(x-1) + f(x+1) = \sum_{s \in S} \delta_S(x-s) f(s) = n(\delta_S * f)(x).$$

Black box #2 (or not): the **Spectral Theorem** says that $L^2(\mathbb{Z}/n\mathbb{Z})$ has an orthonormal basis of eigenfunctions (generalizations of eigenvectors) of A.

Upshot. In fact, we know what these eigenfunctions are: by linearity of χ_b for any $b \in \mathbb{Z}/6\mathbb{Z}$, we have

$$A\chi_b(x) = \chi_b(x+1) + \chi_b(x-1) = (\chi_b(1) + \chi_b(-1))\chi_b(x).$$

Therefore χ_b's are the eigenfunctions and $(\chi_b(1) + \chi_b(-1))$ the eigenvalues. Recall from Euler's formula

$$\begin{aligned} \chi_b(1) + \chi_b(-1) &= e^{2\pi i b/6} + e^{-2\pi i b/6} \\ &= \cos(2\pi b/6) + i\sin(2\pi b/6) + \cos(-2\pi b/6) + i\sin(-2\pi b/6) \\ &= 2\cos(2\pi b/6). \end{aligned}$$

Letting b vary in $\mathbb{Z}/6\mathbb{Z}$ we obtain the **spectrum** of A, written $\Lambda(A)$, i.e., the set of eigenvalues of A:

$$\begin{aligned} \Lambda(A) &= \{2\cos(2\pi b/6) \mid b \in \mathbb{Z}/6\mathbb{Z}\} = \{2\cos(0), 2\cos(2\pi/6), \ldots, 2\cos(10\pi/6)\} \\ &= \{2, 1, -1, -2, -1, 1\}. \end{aligned}$$

Black box #3: [Hückel, 1932] the stability of a chemical compound is determined by its **rest mass energy**

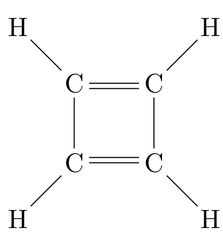
$$E := \left(\sum_{\substack{\text{top } n/2 \\ \lambda \in \Lambda(A)}} \lambda \right) \cdot \frac{2}{n},$$

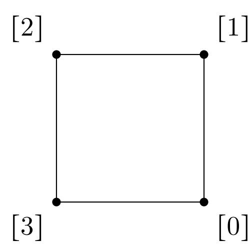
where the summation is taken over the larger half of $\Lambda(A)$. The larger the value E, the more stable the compound.

Upshot. Applying this theorem to the adjacency matrix of Benzene, we see that $E(C_6H_6) = (2+1+1)/3 \approx 1.33$.

3.2 Benzene C_6H_6 is More Stable than Cyclobutadiene C_4H_4

To wrap this presentation up, we present one more highly analogous example and show that cyclobutadiene, C_4H_4, is less stable than benzene is. Below from left to right are (1) the structure diagram of cyclobutadiene, (2) the Cayley graph $X(\mathbb{Z}/4\mathbb{Z}, \{\pm[1]\})$ that (1) resembles, and (3) the corresponding adjacency matrix.





$$B = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

Analogously, we have $Bf(x) = f(x-1) + f(x+1)$ and the eigenfunctions are χ_b, $b \in \mathbb{Z}/4\mathbb{Z}$. Hence the spectrum is

$$\{2\cos(2\pi b/4) \mid b \in \mathbb{Z}/4\mathbb{Z}\} = \{2\cos(0), 2\cos(\pi/2), 2\cos(\pi), 2\cos(3\pi/2)\} = \{2, 0, -2, 0\},$$

and by Hückel,

$$E(C_4H_4) = \frac{2}{4}(2+0) = 1,$$

indeed smaller than $E(C_6H_6)$. Therefore cyclobutadiene is less stable, as claimed.

End of Project