

# Fast Fourier Transformation

Clemens Ballarin

6th February 2026

## Contents

<b>1 Preliminaries</b>	<b>1</b>
<b>2 Complex Roots of Unity</b>	<b>2</b>
2.1 Basic Lemmas . . . . .	3
2.2 Derived Lemmas . . . . .	4
<b>3 Discrete Fourier Transformation</b>	<b>4</b>
<b>4 Discrete, Fast Fourier Transformation</b>	<b>6</b>

```
theory FFT
imports Complex_Main
begin
```

We formalise a functional implementation of the FFT algorithm over the complex numbers, and its inverse. Both are shown equivalent to the usual definitions of these operations through Vandermonde matrices. They are also shown to be inverse to each other, more precisely, that composition of the inverse and the transformation yield the identity up to a scalar.

The presentation closely follows Section 30.2 of Cormen *et al.*, *Introduction to Algorithms*, 2nd edition, MIT Press, 2003.

## 1 Preliminaries

The following two lemmas are useful for experimenting with the transformations, at a vector length of four.

```
lemma Iv14:
```

```
"{0..<4::nat} = {0, 1, 2, 3}"  
⟨proof⟩
```

```
lemma Sum4:  
  "( $\sum$  i=0..<4::nat. x i) = x 0 + x 1 + x 2 + x 3"  
  ⟨proof⟩
```

A number of specialised lemmas for the summation operator, where the index set is the natural numbers

```
lemma sum_add_nat_ivl_singleton:  
  assumes less: "m < (n::nat)"  
  shows "f m + sum f {m<..  ⟨proof⟩
```

```
lemma sum_add_split_nat_ivl_singleton:  
  assumes less: "m < (n::nat)"  
  and g: "!!i. [| m < i; i < n |] ==> g i = f i"  
  shows "f m + sum g {m<..  ⟨proof⟩
```

```
lemma sum_add_split_nat_ivl:  
  assumes le: "m <= (k::nat)" "k <= n"  
  and g: "!!i. [| m <= i; i < k |] ==> g i = f i"  
  and h: "!!i. [| k <= i; i < n |] ==> h i = f i"  
  shows "sum g {m..  ⟨proof⟩
```

```
lemma ivl_splice_Un:  
  "{0..<2*n::nat} = ((* 2 ' {0..\cup ((%i. Suc (2*i)) ' {0..  ⟨proof⟩
```

```
lemma ivl_splice_Int:  
  "((* 2 ' {0..\cap ((%i. Suc (2*i)) ' {0..  ⟨proof⟩
```

```
lemma double_inj_on:  
  "inj_on (%i. 2*i::nat) A"  
  ⟨proof⟩
```

```
lemma Suc_double_inj_on:  
  "inj_on (%i. Suc (2*i)) A"  
  ⟨proof⟩
```

**lemma** sum\_splice:

" $(\sum i::\text{nat} = 0..<2*n. f\ i) = (\sum i = 0..<n. f\ (2*i)) + (\sum i = 0..<n. f\ (2*i+1))$ "  
*<proof>*

## 2 Complex Roots of Unity

The function `cis` from the complex library returns the point on the unity circle corresponding to the argument angle. It is the base for our definition of `root`. The main property, De Moirve's formula is already there in the library.

**definition** root :: "nat => complex" where

"root n == cis (2\*pi/(real (n::nat)))"

**lemma** sin\_periodic\_pi\_diff: "sin (x - pi) = - sin x"

*<proof>*

**lemma** sin\_cos\_between\_zero\_two\_pi:

assumes 0: "0 < x" and pi: "x < 2 \* pi"

shows "sin x ≠ 0 ∨ cos x ≠ 1"

*<proof>*

### 2.1 Basic Lemmas

**lemma** root\_nonzero: "root n ≠ 0"

*<proof>*

**lemma** root\_unity: "root n ^ n = 1"

*<proof>*

**lemma** root\_cancel: "0 < d ==> root (d \* n) ^ (d \* k) = root n ^ k"

*<proof>*

**lemma** root\_summation:

assumes k: "0 < k" "k < n"

shows " $(\sum i=0..<n. (\text{root } n \wedge k) \wedge i) = 0$ "

*<proof>*

**lemma** root\_summation\_inv:

assumes k: "0 < k" "k < n"

shows " $(\sum i=0..<n. ((1 / \text{root } n) \wedge k) \wedge i) = 0$ "

*<proof>*

**lemma** root0 [simp]:

```
"root 0 = 1"
⟨proof⟩
```

```
lemma root1 [simp]:
  "root 1 = 1"
  ⟨proof⟩
```

```
lemma root2 [simp]:
  "root 2 = -1"
  ⟨proof⟩
```

```
lemma root4 [simp]:
  "root 4 = i"
  ⟨proof⟩
```

## 2.2 Derived Lemmas

```
lemma root_cancel1:
  "root (2 * m) ^ (i * (2 * j)) = root m ^ (i * j)"
  ⟨proof⟩
```

```
lemma root_cancel2:
  "0 < n ==> root (2 * n) ^ n = - 1"
```

Note the space between - and 1.

```
⟨proof⟩
```

## 3 Discrete Fourier Transformation

We define operations DFT and IDFT for the discrete Fourier Transform and its inverse. Vectors are simply functions of type `nat => complex`.

DFT `n a` is the transform of vector `a` of length `n`, IDFT its inverse.

```
definition DFT :: "nat => (nat => complex) => (nat => complex)" where
  "DFT n a == (%i.  $\sum_{j=0..<n.} (\text{root } n)^{(i * j)} * (a \ j))"$ 
```

```
definition IDFT :: "nat => (nat => complex) => (nat => complex)" where
  "IDFT n a == (%i.  $(\sum_{k=0..<n.} (a \ k) / (\text{root } n)^{(i * k}))"$ 
```

```
schematic_goal "map (DFT 4 a) [0, 1, 2, 3] = ?x"
  ⟨proof⟩
```

Lemmas for the correctness proof.

**lemma** DFT\_lower:

```
"DFT (2 * m) a i =
DFT m (%i. a (2 * i)) i +
(root (2 * m)) ^ i * DFT m (%i. a (2 * i + 1)) i"
⟨proof⟩
```

**lemma** DFT\_upper:

```
assumes mbound: "0 < m" and ibound: "m <= i"
shows "DFT (2 * m) a i =
DFT m (%i. a (2 * i)) (i - m) -
root (2 * m) ^ (i - m) * DFT m (%i. a (2 * i + 1)) (i - m)"
⟨proof⟩
```

**lemma** IDFT\_lower:

```
"IDFT (2 * m) a i =
IDFT m (%i. a (2 * i)) i +
(1 / root (2 * m)) ^ i * IDFT m (%i. a (2 * i + 1)) i"
⟨proof⟩
```

**lemma** IDFT\_upper:

```
assumes mbound: "0 < m" and ibound: "m <= i"
shows "IDFT (2 * m) a i =
IDFT m (%i. a (2 * i)) (i - m) -
(1 / root (2 * m)) ^ (i - m) *
IDFT m (%i. a (2 * i + 1)) (i - m)"
⟨proof⟩
```

DFT und IDFT are inverses.

```
declare divide_divide_eq_right [simp del]
divide_divide_eq_left [simp del]
```

**lemma** power\_diff\_inverse:

```
assumes nz: "(a::'a::field) ~= 0"
shows "m <= n ==> (inverse a) ^ (n-m) = (a^m) / (a^n)"
⟨proof⟩
```

**lemma** power\_diff\_rev\_if:

```
assumes nz: "(a::'a::field) ~= 0"
shows "(a^m) / (a^n) = (if n <= m then a ^ (m-n) else (1/a) ^ (n-m))"
⟨proof⟩
```

**lemma** power\_divides\_special:

```
"(a::'a::field) ~= 0 ==>
```

$a^{(i * j)} / a^{(k * i)} = (a^j / a^k)^i$   
 <proof>

**theorem** DFT\_inverse:

**assumes** i\_less: "i < n"

**shows** "IDFT n (DFT n a) i = of\_nat n \* a i"

<proof>

## 4 Discrete, Fast Fourier Transformation

FFT k a is the transform of vector a of length  $2^k$ , IFFT its inverse.

**primrec** FFT :: "nat => (nat => complex) => (nat => complex)" **where**

"FFT 0 a = a"

| "FFT (Suc k) a =

(let (x, y) = (FFT k (%i. a (2\*i)), FFT k (%i. a (2\*i+1)))

in (%i. if i <  $2^k$

then x i + (root ( $2^{(Suc k)}$ ))<sup>i</sup> \* y i

else x (i -  $2^k$ ) - (root ( $2^{(Suc k)}$ ))<sup>(i -  $2^k$ )</sup> \* y (i -  $2^k$ )))"

**primrec** IFFT :: "nat => (nat => complex) => (nat => complex)" **where**

"IFFT 0 a = a"

| "IFFT (Suc k) a =

(let (x, y) = (IFFT k (%i. a (2\*i)), IFFT k (%i. a (2\*i+1)))

in (%i. if i <  $2^k$

then x i + (1 / root ( $2^{(Suc k)}$ ))<sup>i</sup> \* y i

else x (i -  $2^k$ ) -

(1 / root ( $2^{(Suc k)}$ ))<sup>(i -  $2^k$ )</sup> \* y (i -  $2^k$ )))"

Finally, for vectors of length  $2^k$ , DFT and FFT, and IDFT and IFFT are equivalent.

**theorem** DFT\_FFT:

"!!a i. i <  $2^k$  ==> DFT ( $2^k$ ) a i = FFT k a i"

<proof>

**theorem** IDFT\_IFFT:

"!!a i. i <  $2^k$  ==> IDFT ( $2^k$ ) a i = IFFT k a i"

<proof>

**schematic\_goal** "map (FFT (Suc (Suc 0)) a) [0, 1, 2, 3] = ?x"

<proof>

**end**