

# Average Matrix of the DFT ensemble

Benevolent Tomato

**Definition** *Average Matrix*

Let  $N$  be a positive integer. We define the average matrix of the DFT ensemble of order  $N$  to be a  $(N - 1)$  square matrix defined as the following.

$$A_{ij} = \begin{cases} 1 & N|ij \\ 0 & N \nmid ij \end{cases}$$

For example, the average matrix of order 6 is

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

**Definition** *Spaced Bases*

Consider the vector space  $\mathbb{R}^{(N-1)}$ . Define the  $m$ th spaced base  $\nu_m$  as follows.

$$(\nu_m)_i := \begin{cases} 1 & (m|i) \\ 0 & (m \nmid i) \end{cases}$$

For example, in a  $(9 - 1)$  dimensional vector space, the 3rd space base will be

$$\nu_3 = \{0, 0, 1, 0, 0, 1, 0, 0\}$$

Moreover, if  $m|N$ , we call the vector a divisor vector. Otherwise, the vector is called a nondivisor vector. For convinience  $\nu_1$  is identified as a nondivisor vector.

**Proposition** *The image of divisor vectors under transformation*

Let  $A$  be the average matrix of the *DFT* ensemble of order  $N$ , that is a  $(N - 1)$ -by- $(N - 1)$  matrix. Let  $m|N$ . Then, the following formula precisely describes the entries of the image of the  $m$ th spaced vector under the transformation induced by  $A$ .

$$(A\nu_m)_i = \frac{N}{\text{lcm}(N/\text{gcd}(i, N), m)} - 1$$

*Proof.* By direct computation, we write the  $i$ th entry of  $A\nu_m$ .

$$A\nu_m = \sum_{j=1}^{N-1} A_{ij}(\nu_m)_j$$

The terms in the sum is nonvanishing if and only if

$$N|ij \quad \text{and} \quad m|j$$

which is equivalent to the condition

$$\frac{N}{\gcd(N, i)}|j \quad \text{and} \quad m|j$$

. We wish to count the number of  $j$ 's in the range  $[1, N-1]$  that satisfy the condition. We conclude

$$(A\nu_m)_i = \frac{N}{\text{lcm}(N/\gcd(i, N), m)} - 1$$

□

**Remark** *Image of nondivisor vectors*

By a similar argument, when  $m \nmid N$ ,

$$(A\nu_m)_i = \left\lfloor \frac{N-1}{\text{lcm}(N/\gcd(i, N), m)} \right\rfloor$$

**Corollary** *Divisor vectors map to divisor vectors*

Let  $m|N$ . Then  $A\nu_m$  can be expressed as a linear combination of divisor vectors, i.e

$$A\nu_m = \sum_{d|N} \tilde{a}_{md} \nu_d$$

*Proof.* Suppose we start from  $A\nu_m$  and subtract divisor vectors to make it zero. We demonstrate this with  $A\nu_2$  for  $N=8$ . We start with the vector

$$\{0, 1, 0, 3, 0, 1, 0\}$$

Subtract  $\nu_2$  to obtain

$$\{0, 0, 0, 1, 0, 0, 0\}$$

and subtract  $\nu_4$  to obtain the zero vector. We conclude

$$A\nu_2 = \nu_2 + \nu_4$$

Now we prove the theorem in a genereral sense. Suppose we have subtracted  $k$  vectors in a sense described above, and call the remainder vector  $r_k$ . We induct on  $k$ . If  $k=0$ , we take  $p$ , the smallest prime divisor of  $N$ . Look at all the entries  $j$  such that  $p|j$ . We know

$$(A\nu_m)_j = \frac{N}{\text{lcm}(N/\gcd(j, N), m)} - 1 \geq \frac{N}{\text{lcm}(N/\gcd(p, N), m)} - 1$$

and thus subtracting  $(A\nu_m)_p \nu_p$  will preserve all the matrix entries positive.

Now, let  $k \geq 1$ . Let  $p$  to be the index of the first positive value occurring in  $r_i$ . If  $p \nmid N$ , then the  $p$ th entry of  $A\nu_m$  will be zero, so we can assume  $p|N$ . By subtracting  $(r_k)_k\nu_p$ , we only affect the entries of  $r_k$  that are a multiple of  $k$ . It suffices to show that for all  $p|j$ ,  $(A\nu_m)_j \geq (A\nu_m)_p$

$$(A\nu_m)_j = \frac{N}{\text{lcm}(N/\gcd(j, N), m)} - 1 \geq \frac{N}{\text{lcm}(N/\gcd(p, N), m)} - 1$$

and the theorem holds.  $\square$

**Remark** *Nondivisor vectors map to divisor vectors*

Replace the formula for divisor vectors to nondivisor vectors, and repeat the same inductive argument used for the divisor vectors.

**Theorem** *Eigenvalues of  $A$*

The nonzero eigenvalues of  $A$  are exactly the eigenvalues of the simplified matrix

$$\tilde{A} := [\tilde{a}_{d_i d_j}]$$

where  $d_i$  is the  $i$ th proper divisor of  $A$  greater than 1. Therefore, if  $N$  has  $\sigma(N)$  divisors including  $N$ , it can have at maximum  $\sigma(N) - 2$  eigenvalues, for  $\tilde{A}$  is a square matrix of order  $\sigma(N) - 2$ .

*Proof.* We first notice that the set of all spacing vectors

$$\{\nu_1, \nu_2, \dots, \nu_{N-1}\}$$

form a basis of  $\mathbb{R}^{N-1}$ . By the proposition, we notice that the image of this base under the transformation  $A$  maps to the space induced by

$$\{\nu_{d_1}, \nu_{d_2}, \dots, \nu_{d_{\sigma(N)-1}}\}$$

. Hence, all nonzero eigenvectors must be in the subspace

$$\text{span}(\nu_{d_1}, \nu_{d_2}, \dots, \nu_{d_{\sigma(N)-1}})$$

and the coefficients  $\tilde{a}$  are described in the proposition.  $\square$

**Remark** *The simplified matrix for prime powers*

If  $N = 2^k$ , the simplified matrix can be simply written as

$$\begin{bmatrix} 1 & 2 & \dots & 2^{k-2} & 2^{k-1} \\ 1 & 2 & \dots & 2^{k-2} & 0 \\ & & \vdots & & \\ 1 & 0 & \dots & 0 & 0 \end{bmatrix}$$

**Theorem** *Lower bounds of the largest eigenvalue of the DFT matrix*

. Let  $\lambda_{max}$  be the maximum eigenvalue of a  $(N-1)$ -by- $(N-1)$  average matrix. The lower bound is

$$\lambda_{max} \geq \frac{N}{2\sigma(N)-2} \sqrt{\sum_{d|N} \frac{1}{d^2}}$$

*Proof.* Since the average matrix is real symmetric, its eigenvalues must be real. We also know that there are only  $\sigma(N)$  nonzero eigenvalues of this matrix. Thus,

$$\sum_{i \leq \sigma(N)} \lambda_i^2 \leq \sigma(N) \lambda_{max}^2$$

By the eigenvalue trace lemma,

$$\sum_{i \leq \sigma(N)} \lambda_i^2 = \text{tr}(A^2) = \sum_{1 \leq i, j \leq N} a_{ij}^2 = \sum_{d|N} \left( \frac{N}{d} - 1 \right) \left( \frac{N}{d} - \varphi \left( \frac{N}{d} \right) \right) \geq \sum_{d|N} \left( \frac{N}{d} - \varphi \left( \frac{N}{d} \right) \right)^2$$

Trivially,

$$\sum_{d|N} \left( \frac{N}{d} - \varphi \left( \frac{N}{d} \right) \right)^2 \geq \frac{1}{4} \sum_{d|N} \left( \frac{N}{d} \right)^2$$

Combining the two observations, we conclude

$$\lambda_{max} \geq \frac{N}{2\sigma(N)-2} \sqrt{\sum_{d|N} \frac{1}{d^2}}$$

□

**Corollary** When  $N$  is a power of 2

By plugging in  $N = 2^k$ , we obtain

$$\lambda_{max} = o \left( \frac{2^k}{k} \right)$$