# Fast Fourier Transform, convolutions, Applications.

$$A(x) = a_0 + a_1 x + \cdots + a_d x^d$$
$$B(x) = b_0 + b_1 x + \cdots + b_d x^d$$

Goal: Compute the product $C(x)$

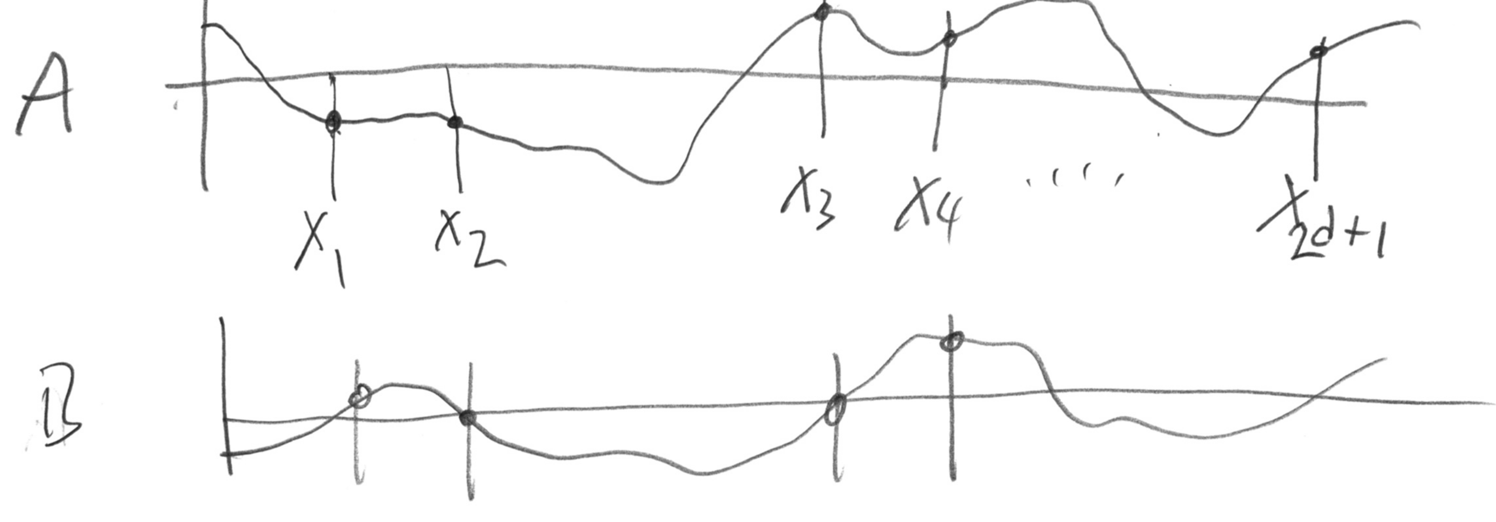
$$C(x) = c_0 + c_1 x + \cdots + c_{2d} x^{2d}$$

$$c_k = \sum_{\substack{0 \le i, j \le k \\ i+j=k}} a_i b_j \Leftarrow O(d^2)$$

convolution of $[a_0 \cdots a_d] *$
$[b_0 \cdots b_d]$

# Alternative Rep of Polynomials

Point-Value rep.




$C = A \cdot B$ $\qquad C(x_i) = A(x_i) \cdot B(x_i)$ $\qquad O(d)$ time

Convolution

$O(d^2)$ naive

$O(d^{1.58})$ Karatsuba's

Today $O(d \log d)$ using FFT

shoenhaga Strassen

integer mult.

$O(n \log n \log \log n)$

Plan

Pick $N \geq 2d+1$ ($N$ power of 2)

1. Pick $N$ points $x_0 \cdots x_{N-1}$ in a special way
2. Evaluate $A(\,)$ at them
3. Evaluate $B(\,)$ at them
4. compute $C(x_0) \cdots C(x_{N-1})$ $O(N)$
5. "Interpolate" $C$ back to the coefficient rep

# Picking the points ($x$ values)

$$A(x) = a_0 + a_1 x + \cdots + a_7 x^7$$

$$x_0 = 1, \quad x_1 = -1$$

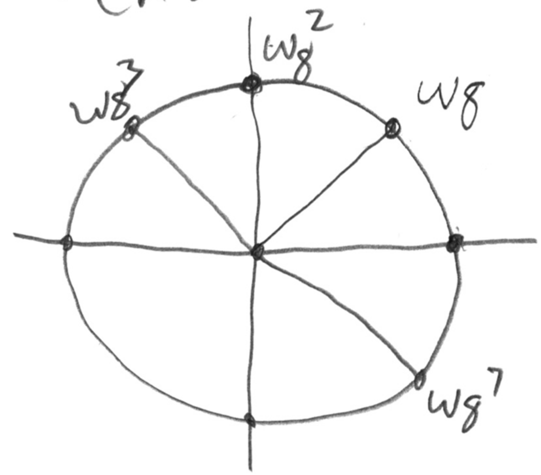
$$\left.\begin{aligned} A(1) &= a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 \\ A(-1) &= a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + a_6 - a_7 \end{aligned}\right] \; 14$$

$$\left.\begin{aligned} w &= a_0 + a_2 + a_4 + a_6 \\ z &= a_1 + a_3 + a_5 + a_7 \end{aligned}\right] \; 6$$

$$\left.\begin{aligned} A(1) &= w + z \\ A(-1) &= w - z \end{aligned}\right] \; 2$$

8

# complex numbers



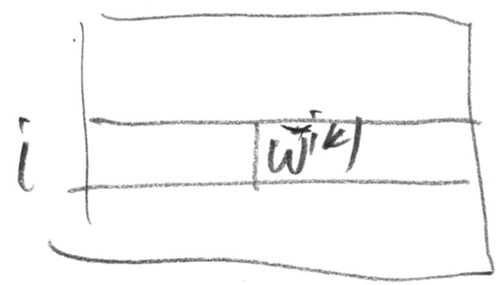

$\omega_8^8 = 1$

$\omega_N$ = the <u>primitive</u> Nth root of unity

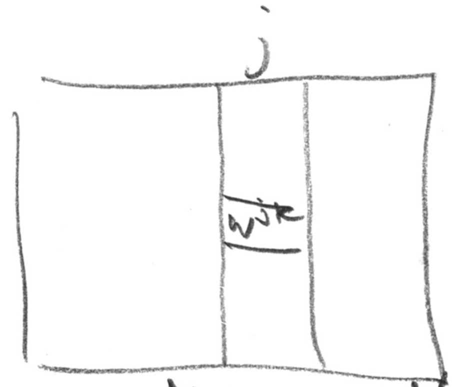
$$\omega_N = e^{2\pi i/N} = i\sin\left(\frac{2\pi}{N}\right) + \cos\left(\frac{2\pi}{N}\right)$$

$$\omega_N^N = 1$$

$$\omega_N^i \neq 1 \text{ for } 0 < i < N$$




$\mathrm{DFT}(\omega^{-1}, N)$




$\mathrm{DFT}(\omega, N)$

$$\begin{pmatrix} \omega^{0\cdot 0} & \omega^{0\cdot 1} & \cdots & \omega^{0\cdot(N-1)} \\ \omega^{1\cdot 0} & \omega^{1\cdot 1} & \cdots & \omega^{1\cdot(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{(N-1)\cdot 0} & \omega^{(N-1)\cdot 1} & \cdots & \omega^{(N-1)\cdot(N-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{pmatrix} = \begin{pmatrix} A(\omega^0) \\ A(\omega^1) \\ \vdots \\ A(\omega^{N-1}) \end{pmatrix}$$

$$\|$$

$$\mathrm{DFT}(\omega_N, N)$$

$F_N(A) = [A(\omega^0), A(\omega^1) \cdots A(\omega^{N-1})]$

$$
\begin{aligned}
F_N(A)_j &= A(\omega^j) \\
&= \sum_{i=0}^{N-1} a_i \omega^{ij} \\
&= \sum_{\substack{i\,=\,0 \\ i \text{ even}}}^{N-1} a_i \omega^{ij} + \sum_{\substack{i\,=\,1 \\ i \text{ odd}}}^{N-1} a_i \omega^{ij} \\
&= \sum_{i=0}^{\frac{N}{2}-1} a_{2i} \omega^{2ij} + \sum_{i=0}^{\frac{N}{2}-1} a_{2i+1} \omega^{(2i+1)j} \\
&= \sum_{i=0}^{\frac{N}{2}-1} a_{2i} (\omega^2)^{ij} + \omega^j \sum_{i=0}^{\frac{N}{2}-1} a_{2i+1} (\omega^2)^{ij} \\
&= \sum_{i=0}^{\frac{N}{2}-1} a_{2i} (\omega_{N/2})^{i(j \bmod N/2)} + \omega_N^j \sum_{i=0}^{\frac{N}{2}-1} a_{2i+1} (\omega_{N/2})^{i(j \bmod N/2)}
\end{aligned}
$$

$$F_N(A)_j = F_{N/2}(A_{\text{even}})_{j \bmod N/2} + \omega_N^j F_{N/2}(A_{\text{odd}})_{j \bmod N/2}$$

---

**FFT**$([a_0, \ldots, a_{N-1}], \omega, N)$

- **if** $N = 1$ **then return** $[a_0]$
- $F_{\text{even}} \leftarrow$ **FFT**$([a_0, a_2, \ldots, a_{N-2}], \omega^2, N/2)$
- $F_{\text{odd}} \leftarrow$ **FFT**$([a_1, a_3, \ldots, a_{N-1}], \omega^2, N/2)$
- $F \leftarrow$ a new vector of length $N$
- $x \leftarrow 1$
- **for** $j = 0$ to $N - 1$ **do**
  - $F[j] \leftarrow F_{\text{even}}[j \mod (N/2)] + x * F_{\text{odd}}[j \bmod (N/2)]$
  - $x \leftarrow x * w$
- **return** $F$

---

$$T(N) = 2T(N/2) + O(N)$$

Let's see what happens if we multiply $\mathbf{DFT}(\omega_N^{-1}, N)$ by $\mathbf{DFT}(\omega_N, N)$.

$$\text{The } (i,j) \text{ entry of } \mathbf{DFT}(\omega^{-1}, N)\ \mathbf{DFT}(\omega, N) = \sum_{k=0}^{N-1} \omega^{-ik}\omega^{kj}$$

So let's try to evaluate the summation on the right in the two cases of $i = j$ and $i \neq j$.

If $i = j$ then we get:

$$\sum_{k=0}^{N-1} \omega^{-ik}\omega^{kj} \;=\; \sum_{k=0}^{N-1} \omega^{0} \;=\; N$$

If $i \neq j$ then we get:

$$\sum_{k=0}^{N-1} \omega^{-ik}\omega^{kj} \;=\; \sum_{k=0}^{N-1} \omega^{(j-i)\cdot k} \;=\; \boxed{\sum_{k=0}^{N-1} (\omega^{j-i})^{k}}$$

$$1 + r + r^2 + \cdots + r^{N-1} = \frac{1 - r^N}{1 - r}$$

So

$$\sum_{k=0}^{N-1} (\omega^{j-i})^k = \frac{1 - (\omega^{j-i})^N}{1 - \omega^{j-i}} = \frac{1 - 1}{1 - \omega^{j-i}} = 0$$

So, summarizing what we just learned:

$$\text{The } (i, j) \text{ entry of } \mathbf{DFT}(\omega^{-1}, N)\ \mathbf{DFT}(\omega, N) = \begin{cases} N & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

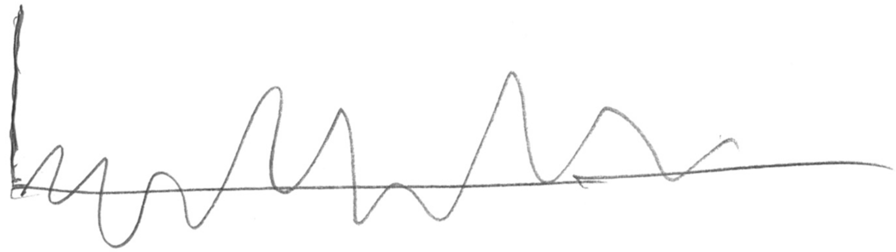
This is just the identity matrix times $N$. So what we've just proven is that:

$$\mathbf{DFT}(\omega, N)^{-1} = \frac{1}{N}\mathbf{DFT}(\omega^{-1}, N)$$

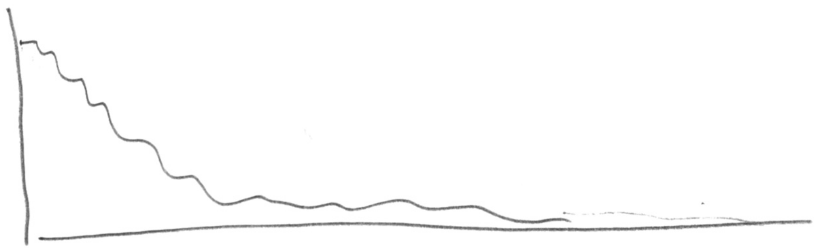
```
       A =   1  2  3  4  5  6  7  8  0  0  0  0  0  0  0  0
       B =   1  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0
conv A B =   1  2  3  4  5  6  7  8  0  0  0  0  0  0  0  0

       A =   1  2  3  4  5  6  7  8  0  0  0  0  0  0  0  0
       B =   0  0  0  0  0  0  0  1  0  0  0  0  0  0  0  0
conv A B =   0  0  0  0  0  0  0  1  2  3  4  5  6  7  8  0

       A =   1  2  3  4  5  6  7  8  0  0  0  0  0  0  0  0
       B =   0  0  0  0  0  0  0  0  0  0  0  0  0  1  0  0
conv A B =   4  5  6  7  8  0  0  0  0  0  0  0  0  1  2  3

       A =   1  2  3  4  5  6  7  8  0  0  0  0  0  0  0  0
       B =   0  0  0  0  0  1  0  0  0  0  1  0  0  0  0  0
conv A B =   7  8  0  0  0  1  2  3  4  5  7  9 11  4  5  6

       A =   1  2  3  4  5  6  7  8  9 10 11 12  0  0  0  0
       B =   0  0  0  0  0  1  0  0  0  0  1  0  0  0  0  0
conv A B =  19  8  9 10 11 13  2  3  4  5  7  9 11 13 15 17
```

# Digital Signal Processing

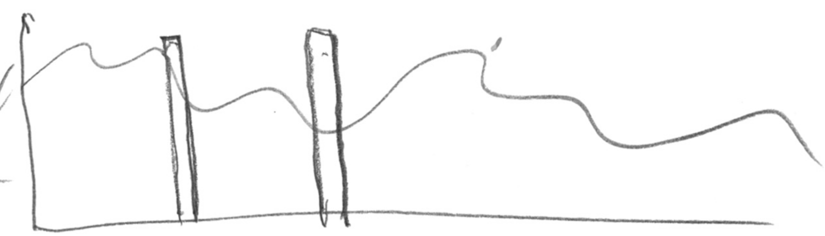
signal



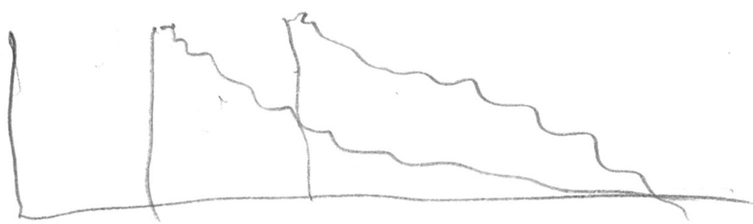
Impulse response



signal



conv.



# Evenly Spaced Ones

S is a binary String

$$\begin{array}{rl} & \scriptstyle 0\ 1\ 2\ 3\ 4 \\ S = & 11011100010 \end{array}$$

Brute force : $O(n^2)$

FFT method

$$p(x) = x^0 + x^1 + x^3 + x^4 + x^7$$

$$p^2(x) = x^0 + 2x^1 + x^2 + 2x^3 + 4x^4 + \cdots + 3x^8 + \cdots$$

the coefficient of $x^t$ is the number of pairs $(a, c)$ with ones and $a + c = t$

position $b = 4$ $\quad x^{2b}$ term