Algorithms and datastructures II

Lecture 8: Fast Fourier Transform 2/2

Jan Hubička

Department of Applied Mathematics
Charles University
Prague

Nov 23 2020

Polynomials

Definition (Polynomial)

Polynomial is an expression of form

$$P(x) = \sum_{i=0}^{n-1} p_i \cdot x^i.$$

Where x is a variable and p_i are some constants called coefficients.

We will represent polynomial by a vector of coefficients $(p_0, \ldots, p_{n-1})$.
Number of coefficients is called the size of the polynomial and denoted $|P|$.
Normal form of a polynomial is created by removing trailing zero coefficients.
Multiplication of polynomials is defined as:

$$P(x) \cdot Q(x) = \left(\sum_{i=0}^{n-1} p_i \cdot x^i \right) \cdot \left(\sum_{i=0}^{m-1} q_i \cdot x^i \right) = \sum_{i,j} p_i q_j x^{i+j}.$$

Result of the multiplication is a polynomial $R(x)$ with

$$r_k = p_0 q_k + p_1 q_{k-1} + \cdots + p_k q_0.$$

Observation

Polynomial $R(x) = P(x) \cdot Q(x)$ can be computed in $\Theta(n^2)$ where $n = |P| = |Q|$.

Polynomials: identity and vector of values

Polynomials P and Q are identical, denoted by $P \equiv Q$, iff they have same coefficients.
Polynomials P and Q are equivalent, denoted by $P = Q$, iff $\forall_x : P(x) = Q(x)$.

Lemma

Let $x_0, \ldots, x_d$ by any sequence of distinct numbers. Let P and Q be polynomials of degree at most d. If $P(x_i) = Q(x_i)$ for every $i = 0, 1, \ldots d$ then P and Q are equivalent.

Recall:

Lemma

Non-zero polynomial R of degree $t \geq 0$ has at most t roots.

division of polynomials: $R(x) \equiv (x - \alpha) \cdot R'(x) + \beta$ for constant β. If α is root then $\beta = 0$.
Now consider $R(x) \equiv P(x) - Q(x)$. Degree of R is at most d and all of $x_0, \ldots, x_d$ are roots.

We established bijection between polynomials and vectors of values.

Multiplication

Multiply (P, Q)

WLOG assume that $|P| = |Q| = n$ and upper $n/2$ coefficients are 0.

1. Choose distinct numbers $x_0, x_1, \ldots, x_{n-1}$.
2. Compute $(P(x_0), \ldots, P(x_{n-1}))$ and $(Q(x_0), \ldots, Q(x_{n-1}))$.
3. Multiply component to determine $(R(x_0), \ldots, R(x_{n-1}))$
4. Find corresponding coefficients of vector R of length n.

Fast Fourier Transform

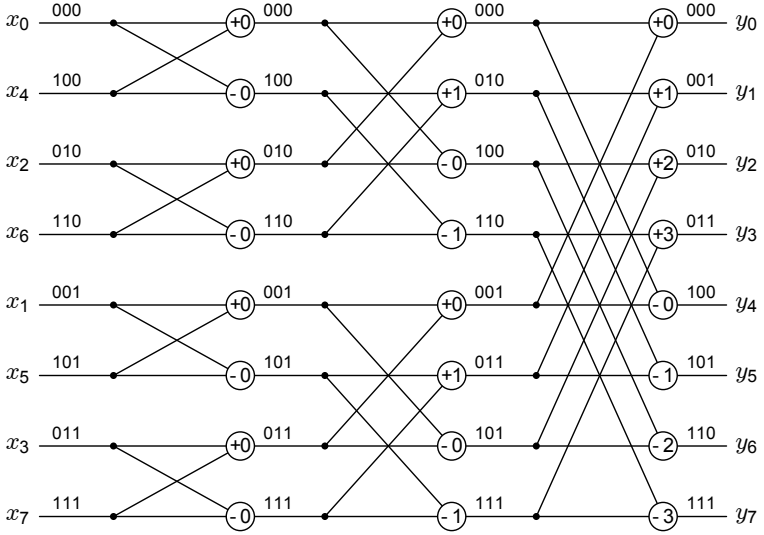
FFT(n, ω, $(p_0, \ldots, p_{n-1})$)

Assume $n = 2^k$, ω is n-th primitive root of 1.

1. If $n = 1$: return (p_0).
2. $(e_0, \ldots, e_{n/2-1}) \leftarrow$FFT $(n/2, \omega^2, (p_0, p_2, \ldots, p_{n-2}))$
3. $(o_0, \ldots, o_{n/2-1}) \leftarrow$FFT $(n/2, \omega^2, (p_1, p_3, \ldots, p_{n-1}))$
4. For $j = 0, \ldots, n/2 - 1$:
5. $\quad y_j \leftarrow e_j + \omega^j \cdot o_j$ (ω^j can be computed incrementally)
6. $\quad y_{j+n/2} \leftarrow e_j - \omega^j \cdot o_j$
7. Return $(y_0, \ldots, y_{n-1})$.

Time complexity $T(n) = 2T(n/2) + \Theta(n) = \Theta(n \log n)$.

FFT as boolean circuit



Fast Fourier Transform without recursion

FFT(n, ω, $(p_0, \ldots, p_{n-1})$)

Assume $n = 2^k$, ω is n-th primitive root of 1.

1. Precompute $\omega^0, \omega^1, \ldots, \omega^{n-1}$
2. For $k = 0, \ldots, n-1$ put $y_k \leftarrow x_{r(k)}$
   here r is function representing the bit mirroring
3. $b \leftarrow 1$
4. While $b < n$:
5. For $j = 0, \ldots, n-1$ with step 2b:
6. For $k = 0, \ldots, b-1$:
7. $\alpha \leftarrow \omega^{(nk/2b) \mod n}$
8. $(y_{j+k}, y_{j+k+b}) \leftarrow (y_{j+k} + \alpha y_{j+k+b}, y_{j+k} - \alpha y_{j+k+b})$
9. $b \leftarrow 2b$
10. Return $(y_0, \ldots, y_{n-1})$

Antisymetry

Lemma

For every vector $\vec{x} \in \mathbb{R}^n$ it holds that $\vec{y} = \mathcal{F}(\vec{x})$ is antisymetric. That is $y_j = \overline{y_{n-j}}$.

Proof.

Antisymetry

Lemma

For every vector $\vec{x} \in \mathbb{R}^n$ it holds that $\vec{y} = \mathcal{F}(\vec{x})$ is antisymetric. That is $y_j = \overline{y_{n-j}}$.

Proof.

$$y_{n-j} = \sum_k x_k \omega^{(n-j)k} = \sum_k x_k \omega^{nk-jk} = \sum_k x_k \omega^{-jk} = \sum_k x_k \overline{\omega}^{jk}.$$

Antisymetry

Lemma

For every vector $\vec{x} \in \mathbb{R}^n$ it holds that $\vec{y} = \mathcal{F}(\vec{x})$ is antisymetric. That is $y_j = \overline{y_{n-j}}$.

Proof.

$$y_{n-j} = \sum_k x_k \omega^{(n-j)k} = \sum_k x_k \omega^{nk-jk} = \sum_k x_k \omega^{-jk} = \sum_k x_k \overline{\omega}^{jk}.$$

$$\overline{y_{n-j}} = \sum_k \overline{x_k} \omega^{jk}$$

Antisymetry

Lemma

For every vector $\vec{x} \in \mathbb{R}^n$ it holds that $\vec{y} = \mathcal{F}(\vec{x})$ is antisymetric. That is $y_j = \overline{y_{n-j}}$.

Proof.

$$y_{n-j} = \sum_k x_k \omega^{(n-j)k} = \sum_k x_k \omega^{nk-jk} = \sum_k x_k \omega^{-jk} = \sum_k x_k \overline{\omega}^{jk}.$$

$$\overline{y_{n-j}} = \sum_k \overline{x_k} \omega^{jk}$$

For real values equality follows.

Antisymetry

Lemma

For every vector $\vec{x} \in \mathbb{R}^n$ it holds that $\vec{y} = \mathcal{F}(\vec{x})$ is antisymetric. That is $y_j = \overline{y_{n-j}}$.

Proof.

$$y_{n-j} = \sum_k x_k \omega^{(n-j)k} = \sum_k x_k \omega^{nk-jk} = \sum_k x_k \omega^{-jk} = \sum_k x_k \overline{\omega}^{jk}.$$

$$\overline{y_{n-j}} = \sum_k \overline{x_k} \omega^{jk}$$

For real values equality follows. □

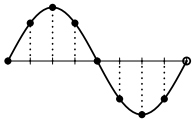
In particular $y_0 = \overline{y_0}$ and $y_{n/2} = \overline{y_{n/2}}$ and thus both are real values.

Lemma

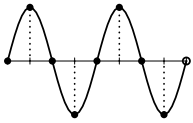
Antisymetric vectors in $\mathbb{C}^n$ forms a vector field of dimension n over real numbers.

Spectral analysis

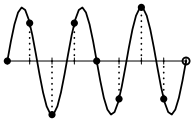
Fix n and $\omega = 2^{2\pi i/n}$. Denote by $\vec{e}^k, \vec{s}^k, \vec{c}^k$ vectors created by sampling functions $e^{2k\pi ix}, \sin 2k\pi x, \cos 2k\pi x$ at $[0, 1)$.



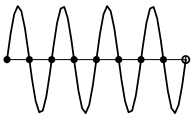
s^1



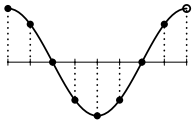
s^2



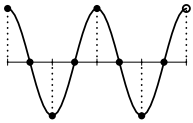
s^3



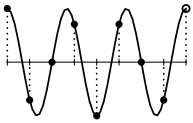
s^4



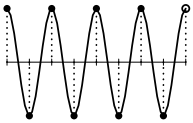
c^1



c^2



c^3



c^4

Lemma

For every $0 < k < n/2$ it holds:

$$\begin{aligned} \mathcal{F}(\vec{e}^k) &= (0, \ldots, 0, n, 0, \ldots, 0) \\ \mathcal{F}(\vec{s}^k) &= (0, \ldots, 0, n/2i, 0, \ldots, 0, -n/2i, 0 \ldots, 0) \\ \mathcal{F}(\vec{c}^k) &= (0, \ldots, 0, n/2, 0, \ldots, 0, n/2, 0 \ldots, 0) \end{aligned}$$

First vector is non-zero in position $n - k$ and other two in positions k and $n - k$.

Lemma

For every $0 < k < n/2$ it holds:

$$\begin{aligned}\mathcal{F}(\vec{e}^k) &= (0,\ldots,0,n,0,\ldots,0)\\ \mathcal{F}(\vec{s}^k) &= (0,\ldots,0,n/2i,0,\ldots,0,-n/2i,0\ldots,0)\\ \mathcal{F}(\vec{c}^k) &= (0,\ldots,0,n/2,0,\ldots,0,n/2,0\ldots,0)\end{aligned}$$

First vector is non-zero in position $n-k$ and other two in positions k and $n-k$.

1. For $\vec{e}^k$ the formula holds for $k = 0$ and $k = n/2$.
2. $\vec{s}^0$ and $\vec{s}^{n/2}$ are zero vectors.
3. $\vec{c}^0 = (n, 0, \ldots, 0)$ and $\vec{c}^{n/2} = (0, \ldots, 0, n, 0, \ldots, 0)$.

Lemma

For every $0 < k < n/2$ it holds:

$$\begin{aligned}\mathcal{F}(\vec{e}^k) &= (0,\ldots,0,n,0,\ldots,0)\\ \mathcal{F}(\vec{s}^k) &= (0,\ldots,0,n/2i,0,\ldots,0,-n/2i,0\ldots,0)\\ \mathcal{F}(\vec{c}^k) &= (0,\ldots,0,n/2,0,\ldots,0,n/2,0\ldots,0)\end{aligned}$$

First vector is non-zero in position $n-k$ and other two in positions k and $n-k$.

1. For $\vec{e}^k$ the formula holds for $k = 0$ and $k = n/2$.
2. $\vec{s}^0$ and $\vec{s}^{n/2}$ are zero vectors.
3. $\vec{c}^0 = (n,0,\ldots,0)$ and $\vec{c}^{n/2} = (0,\ldots,0,n,0,\ldots,0)$.

Proof.

$$e_j^k = e^{2k\pi ij/n} = e^{jk2\pi i/n} = \omega^{jk}$$

t-th element of Fourier transform is

$$\sum_j = \omega^{jk}\omega^{jt} = \sum_j \omega^{j(k+t)}$$

We can again apply the observation about geometric sequence as while computing the inverse. □

Theorem

For every $\vec{x} \in \mathbb{R}^n$ there exists real values $\alpha_0, \ldots, \alpha_{n/2}$ and $\beta_0, \ldots, \beta_{n/2}$ such that

$$x = \sum_{k=0}^{n/2} (\alpha_k c^k + \beta_k s^k)$$

These coefficients can be determined from

$$\vec{y} = \mathcal{F}(\vec{x}) = (a_0 + b_0 i, \ldots, a_{n-1} + b_{n-1} i)$$

by:

$$\begin{aligned}
\alpha_0 &= a_0/n \\
\alpha_j &= 2a_j/n \qquad \text{for } j = 1, \ldots, n/2 - 1 \\
\alpha_{n/2} &= a_{n/2}/n \\
\beta_0 = \beta_{n/2} &= 0 \\
\beta_j &= -2b_j/n \qquad \text{for } j = 1, \ldots, n/2 - 1
\end{aligned}$$

Theorem

For every $\vec{x} \in \mathbb{R}^n$ there exists real values $\alpha_0, \ldots, \alpha_{n/2}$ and $\beta_0, \ldots, \beta_{n/2}$ such that

$$x = \sum_{k=0}^{n/2} (\alpha_k c^k + \beta_k s^k)$$

These coefficients can be determined from

$$\vec{y} = \mathcal{F}(\vec{x}) = (a_0 + b_0 i, \ldots, a_{n-1} + b_{n-1} i)$$

by:

$$\begin{aligned}
\alpha_0 &= a_0/n \\
\alpha_j &= 2a_j/n \qquad \text{for } j = 1, \ldots, n/2 - 1 \\
\alpha_{n/2} &= a_{n/2}/n \\
\beta_0 = \beta_{n/2} &= 0 \\
\beta_j &= -2b_j/n \qquad \text{for } j = 1, \ldots, n/2 - 1
\end{aligned}$$

For every $0 < k < n/2$ it holds:

$$\begin{aligned}
\mathcal{F}(\vec{s}^k) &= (0, \ldots, 0, n/2i, 0, \ldots, 0, -n/2i, 0 \ldots, 0) \\
\mathcal{F}(\vec{c}^k) &= (0, \ldots, 0, n/2, 0, \ldots, 0, n/2, 0 \ldots, 0)
\end{aligned}$$

Vectors are non-zero in positions k and $n - k$.
$\vec{s}^0$ and $\vec{s}^{n/2}$ are zero vectors.
$\vec{c}^0 = (n, 0, \ldots, 0)$ and $\vec{c}^{n/2} = (0, \ldots, 0, n, 0, \ldots, 0)$.

Theorem

For every $\vec{x} \in \mathbb{R}^n$ there exists real values $\alpha_0, \ldots, \alpha_{n/2}$ and $\beta_0, \ldots, \beta_{n/2}$ such that

$$x = \sum_{k=0}^{n/2} (\alpha_k c^k + \beta_k s^k)$$

These coefficients can be determined from

$$\vec{y} = \mathcal{F}(\vec{x}) = (a_0 + b_0 i, \ldots, a_{n-1} + b_{n-1} i)$$

by:

$$\begin{aligned} \alpha_0 &= a_0/n \\ \alpha_j &= 2a_j/n \qquad \text{for } j = 1, \ldots, n/2-1 \\ \alpha_{n/2} &= a_{n/2}/n \\ \beta_0 = \beta_{n/2} &= 0 \\ \beta_j &= -2b_j/n \qquad \text{for } j = 1, \ldots, n/2-1 \end{aligned}$$

For every $0 < k < n/2$ it holds:

$$\begin{aligned} \mathcal{F}(\vec{s}^k) &= (0, \ldots, 0, n/2i, 0, \ldots, 0, -n/2i, 0 \ldots, 0) \\ \mathcal{F}(\vec{c}^k) &= (0, \ldots, 0, n/2, 0, \ldots, 0, n/2, 0 \ldots, 0) \end{aligned}$$

Vectors are non-zero in positions k and $n-k$.
$\vec{s}^0$ and $\vec{s}^{n/2}$ are zero vectors.
$\vec{c}^0 = (n, 0, \ldots, 0)$ and $\vec{c}^{n/2} = (0, \ldots, 0, n, 0, \ldots, 0)$.

Proof.

Because $\mathcal{F}$ has inverse we need only to check that

$$\begin{aligned} \vec{y} &= \mathcal{F}\left(\sum_{k=0}^{n/2} (\alpha_k \vec{c}^k + \beta_k \vec{s}^k)\right) \\ &= \sum_{k=0}^{n/2} (\alpha_k \mathcal{F}(\vec{c}^k) + \beta_k \mathcal{F}(\vec{s}^k)). \end{aligned}$$

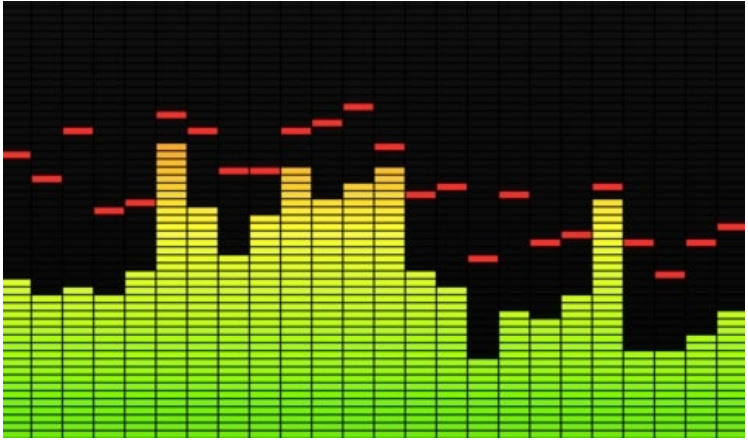
We only need to set up values to match elements $0, \ldots, n/2+1$. Rest follows from anti-symmetry.

$$a_j + b_j i = (2a_j/n)n/2 - (2b_j/n)n/2i = \alpha_j \vec{c}^j + \beta_j \vec{s}^j$$

□

Spectral analysis

Recall that $\alpha \cos x + \beta \sin x = A \sin(x + \varphi)$ for some A and φ. It means that we can, using FFT, decompose every sound to sum of basic sinusoid waves of different amplitudes A and phase shifts φ.



Discrete Cosine transform

Discrete cosine transform

Discrete cosine transform is a spectral analysis of vector $(x_0, \ldots, x_{n/2-1}, x_{n/2}, x_{n/2-1}, \ldots, x_{x_1})$. This is real antisymetric vector and its Fourier transform is also real and antisymmetric $(y_0, \ldots, y_{n/2-1}, y_{n/2}, y_{n/2-1}, \ldots, y_{y_1})$.

We can thus write vector $(x_0, \ldots x_{n/2})$ as a combination of vectors $\vec{c}^0, \ldots, \vec{c}^{n/2}$.

Discrete Cosine transform

Discrete cosine transform

Discrete cosine transform is a spectral analysis of vector $(x_0, \ldots, x_{n/2-1}, x_{n/2}, x_{n/2-1}, \ldots, x_{x_1})$. This is real antisymetric vector and its Fourier transform is also real and antisymmetric $(y_0, \ldots, y_{n/2-1}, y_{n/2}, y_{n/2-1}, \ldots, y_{y_1})$.
We can thus write vector $(x_0, \ldots x_{n/2})$ as a combination of vectors $\vec{c}^0, \ldots, \vec{c}^{n/2}$.

DCT-II:

$$y_k = \sum_{j=0}^{n-1} x_j \cos\left(\frac{\pi(j+1/2)}{n} k\right)$$

Inverse of DCT-II is DCT-III multiplied by $2/n$.

Discrete Cosine transform

Discrete cosine transform

Discrete cosine transform is a spectral analysis of vector $(x_0, \ldots, x_{n/2-1}, x_{n/2}, x_{n/2-1}, \ldots, x_{x_1})$. This is real antisymetric vector and its Fourier transform is also real and antisymmetric $(y_0, \ldots, y_{n/2-1}, y_{n/2}, y_{n/2-1}, \ldots, y_{y_1})$.
We can thus write vector $(x_0, \ldots x_{n/2})$ as a combination of vectors $\vec{c}^0, \ldots, \vec{c}^{n/2}$.

DCT-II:

$$y_k = \sum_{j=0}^{n-1} x_j \cos\left(\frac{\pi(j+1/2)}{n} k\right)$$

Inverse of DCT-II is DCT-III multiplied by $2/n$.
DCT-III:

$$y_k = \frac{1}{2} x_0 + \sum_{j=1}^{n-1} x_j \cos\left(\frac{\pi(k+1/2)}{n} j\right)$$

Discrete Cosine transform

Discrete cosine transform

Discrete cosine transform is a spectral analysis of vector $(x_0, \ldots, x_{n/2-1}, x_{n/2}, x_{n/2-1}, \ldots, x_{x_1})$. This is real antisymetric vector and its Fourier transform is also real and antisymmetric $(y_0, \ldots, y_{n/2-1}, y_{n/2}, y_{n/2-1}, \ldots, y_{y_1})$.
We can thus write vector $(x_0, \ldots x_{n/2})$ as a combination of vectors $\vec{c}^0, \ldots, \vec{c}^{n/2}$.

DCT-II:

$$y_k = \sum_{j=0}^{n-1} x_j \cos\left(\frac{\pi(j+1/2)}{n} k\right)$$

Inverse of DCT-II is DCT-III multiplied by $2/n$.
DCT-III:

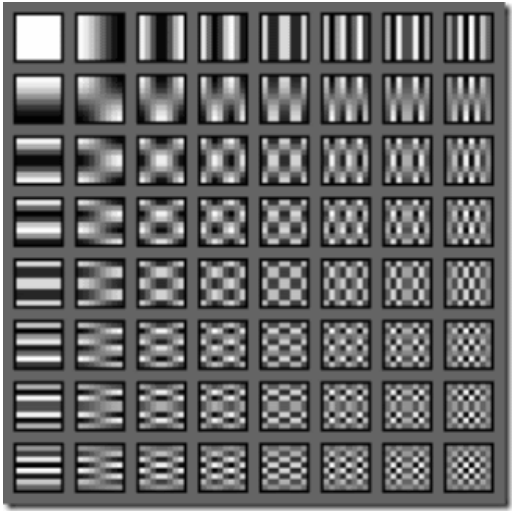
$$y_k = \frac{1}{2} x_0 + \sum_{j=1}^{n-1} x_j \cos\left(\frac{\pi(k+1/2)}{n} j\right)$$

2-dimensional DCT-2:

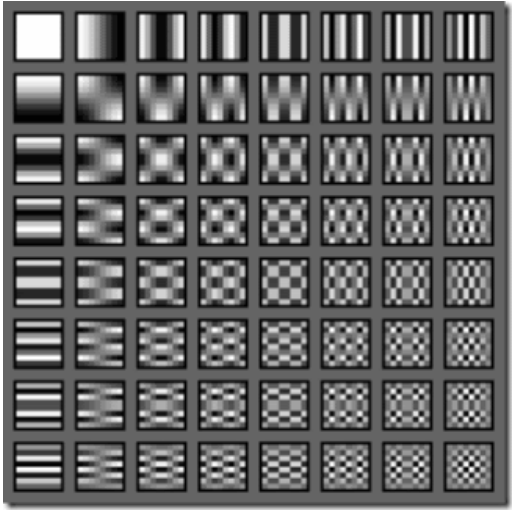
$$y_{k_1,k_2} = \sum_{j_1=0}^{n-1} \sum_{j_2=0}^{n-1} x_{j_1,j_2} \cos\left(\frac{\pi(j_1+1/2)}{n} k_1\right) \cos\left(\frac{\pi(j_2+1/2)}{n} k_2\right)$$

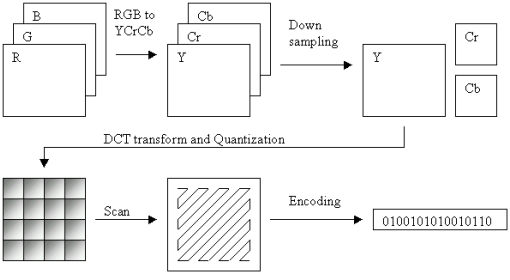
2-dimensional DCT can be computed by applying 1-dimensional DCT on every row and then 1-dimensional DCT to every column.

2-dimensional DCT and JPEG compression



2-dimensional DCT and JPEG compression





JPEG artifacts

Multiplying large numbers

Observation

It is possible to apply FFT in a finite field assuming that there is an n-th primitive root of 1.

Computing *modp* for prime $p = 2^k + 1$ we have $2^{2k} = 1 \mod p$ and $2^0, \dots 2^{k-1}$ mutually different.
Sadly $2k$ is unlikely to be power of 2.

Lemma

Every multiplicative group of $\mathbb{Z}_p$ is cyclic.

It follows that all $p - 1$ element can be written as powers of some g (generator of a group).
It follows that g is primitive $(p - 1)$-st root of 1.
For example we can use:

1. $p = 2^{16} + 1 = 65537, g = 3, \omega = 3^2, n = 2^{15}$
2. $p = 15 \cdot 2^{27} + 1 = 2013265921, g = 31, \omega = 440564289, n = 2^{27}$
3. $p = 3 \cdot 2^{30} + 1 = 3221225473, g = 5, \omega = 125, n = 2^{30}$