Jonathan Parlett

February 5, 2023

What well cover

- Cyclotomic polynomials and their degrees

What well cover

- Cyclotomic polynomials and their degrees
- A simplified encoding scheme from polynomials with complex coefficients to vectors with complex coefficients

What well cover

- Cyclotomic polynomials and their degrees
- A simplified encoding scheme from polynomials with complex coefficients to vectors with complex coefficients
- The actual encoding scheme from polynomials with integer coefficients to vectors of complex coefficients.

- The n-th Cyclotomic polynomial is defined as $\Phi_n(x) = \Pi_{1 \le k \le n \mid \gcd(k,n)=1}(x - e^{2i\pi\frac{k}{n}})$

- The n-th Cyclotomic polynomial is defined as $\Phi_n(x) = \Pi_{1 \leq k \leq n \mid \gcd(k,n)=1}(x - e^{2i\pi\frac{k}{n}})$
- From the constraint that $gcd(k, n) = 1$ you may be able to infer that the degree of the n-th cyclotomic polynomial is equal to $\rho(n)$ where ρ is Eulers totient function.

- The n-th Cyclotomic polynomial is defined as $\Phi_n(x) = \Pi_{1 \le k \le n \mid \gcd(k,n)=1}(x - e^{2i\pi\frac{k}{n}})$
- From the constraint that $gcd(k, n) = 1$ you may be able to infer that the degree of the n-th cyclotomic polynomial is equal to $\rho(n)$ where ρ is Eulers totient function.
- This property will be important to consider when you we select a cyclotomic to use for our encoding

- The n-th Cyclotomic polynomial is defined as $\Phi_n(x) = \Pi_{1 \leq k \leq n \mid \gcd(k,n)=1}(x - e^{2i\pi\frac{k}{n}})$
- From the constraint that $gcd(k, n) = 1$ you may be able to infer that the degree of the n-th cyclotomic polynomial is equal to $\rho(n)$ where ρ is Eulers totient function.
- This property will be important to consider when you we select a cyclotomic to use for our encoding
- Another important property of cyclotomics is that there roots are complex conjugates of each other. To see this lets look at the 8-th cyclotomic $X^4 + 1$

- The n-th Cyclotomic polynomial is defined as
  $\Phi_n(x) = \Pi_{1 \leq k \leq n \mid \gcd(k,n)=1}(x - e^{2i\pi\frac{k}{n}})$
- From the constraint that $gcd(k, n) = 1$ you may be able to infer that the degree of the n-th cyclotomic polynomial is equal to $\rho(n)$ where ρ is Eulers totient function.
- This property will be important to consider when you we select a cyclotomic to use for our encoding
- Another important property of cyclotomics is that there roots are complex conjugates of each other. To see this lets look at the 8-th cyclotomic $X^4 + 1$
- $\Phi_8(x) = (x - e^{2i\pi\frac{1}{8}})(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - e^{2i\pi\frac{7}{8}})$

Cyclotomic polynomial roots are complex conjugates: Example

- $x^4 + 1 = \Phi_8(x) = (x - e^{2i\pi\frac{1}{8}})(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - e^{2i\pi\frac{7}{8}})$

Cyclotomic polynomial roots are complex conjugates: Example

- $x^4 + 1 = \Phi_8(x) = (x - e^{2i\pi\frac{1}{8}})(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - e^{2i\pi\frac{7}{8}})$
- $= (x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))$

Cyclotomic polynomial roots are complex conjugates: Example

- $x^4 + 1 = \Phi_8(x) = (x - e^{2i\pi\frac{1}{8}})(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - e^{2i\pi\frac{7}{8}})$
- $= (x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))$
- $= (x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - (-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - (-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}))(x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))$

Cyclotomic polynomial roots are complex conjugates: Example

- $x^4 + 1 = \Phi_8(x) = (x - e^{2i\pi\frac{1}{8}})(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - e^{2i\pi\frac{7}{8}})$
- $= (x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))$
- $= (x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - (-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - (-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}))(x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))$
- $= (x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})(x + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})(x + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})(x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})$

Cyclotomic polynomial roots are complex conjugates: Example

- $x^4 + 1 = \Phi_8(x) = (x - e^{2i\pi\frac{1}{8}})(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - e^{2i\pi\frac{7}{8}})$
- $= (x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))$
- $= (x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - (-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - (-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}))(x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))$
- $= (x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})(x + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})(x + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})(x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})$
- Grouping real and imaginary parts we can see that the 1st root is the complex of the 4th and the 2nd root is the complex conjugate of the 3rd

Cyclotomic polynomial roots are complex conjugates: Example

- $x^4 + 1 = \Phi_8(x) = (x - e^{2i\pi\frac{1}{8}})(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - e^{2i\pi\frac{7}{8}})$
- $= (x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))$
- $= (x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - (-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - (-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}))(x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))$
- $= (x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})(x + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})(x + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})(x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})$
- Grouping real and imaginary parts we can see that the 1st root is the complex of the 4th and the 2nd root is the complex conjugate of the 3rd
- $= ([x - \frac{\sqrt{2}}{2}] - i\frac{\sqrt{2}}{2})([x + \frac{\sqrt{2}}{2}] - i\frac{\sqrt{2}}{2})([x + \frac{\sqrt{2}}{2}] + i\frac{\sqrt{2}}{2})([x - \frac{\sqrt{2}}{2}] - i\frac{\sqrt{2}}{2})$

Cyclotomic polynomial roots are complex conjugates: Example

- $x^4 + 1 = \Phi_8(x) = (x - e^{2i\pi\frac{1}{8}})(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - e^{2i\pi\frac{7}{8}})$
- $= (x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - e^{2i\pi\frac{3}{8}})(x - e^{2i\pi\frac{5}{8}})(x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))$
- $= (x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - (-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))(x - (-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}))(x - (\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}))$
- $= (x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})(x + \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})(x + \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})(x - \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})$
- Grouping real and imaginary parts we can see that the 1st root is the complex of the 4th and the 2nd root is the complex conjugate of the 3rd
- $= ([x - \frac{\sqrt{2}}{2}] - i\frac{\sqrt{2}}{2})([x + \frac{\sqrt{2}}{2}] - i\frac{\sqrt{2}}{2})([x + \frac{\sqrt{2}}{2}] + i\frac{\sqrt{2}}{2})([x - \frac{\sqrt{2}}{2}] - i\frac{\sqrt{2}}{2})$
- This fact will become important when we are discussing the mapping of polynomials with integer coefficients to complex vectors

Simplified encoding scheme

- The input messages in the CKKS scheme are vectors of complex numbers $z \in \mathbb{C}^N$ where N is called the degree modulus for reasons that will become obvious

- The input messages in the CKKS scheme are vectors of complex numbers $z \in \mathbb{C}^N$ where N is called the degree modulus for reasons that will become obvious
- All homomorphic operations in the CKKS scheme are performed on polynomials in the ring $\frac{\mathbb{Z}[X]}{X^N+1}$. The homomorphic properties of these operations come as a consequence of the properties of these polynomial rings

- The input messages in the CKKS scheme are vectors of complex numbers $z \in \mathbb{C}^N$ where N is called the degree modulus for reasons that will become obvious
- All homomorphic operations in the CKKS scheme are performed on polynomials in the ring $\frac{\mathbb{Z}[X]}{X^N+1}$. The homomorphic properties of these operations come as a consequence of the properties of these polynomial rings
- So the first big thing to understand in order to fully understand CKKS is this encoding scheme. How do we get from our complex vectors to our plaintext polynomials

- The input messages in the CKKS scheme are vectors of complex numbers $z \in \mathbb{C}^N$ where N is called the degree modulus for reasons that will become obvious
- All homomorphic operations in the CKKS scheme are performed on polynomials in the ring $\frac{\mathbb{Z}[X]}{X^N+1}$. The homomorphic properties of these operations come as a consequence of the properties of these polynomial rings
- So the first big thing to understand in order to fully understand CKKS is this encoding scheme. How do we get from our complex vectors to our plaintext polynomials
- The ultimate is goal to be able to fully understand the map that defines CKKS encoding algorithm

$$\sigma^{-1} : \mathbb{C}^N \to \frac{\mathbb{Z}[X]}{X^N + 1}$$

- To start we will first understand the simpler map from complex vectors to polynomials with complex coefficients

$$\sigma^{-1} : \mathbb{C}^N \to \frac{\mathbb{C}[X]}{X^N + 1}$$

- To start we will first understand the simpler map from complex vectors to polynomials with complex coefficients

$$\sigma^{-1} : \mathbb{C}^N \to \frac{\mathbb{C}[X]}{X^N + 1}$$

- The forward map may be easier to consider

$$\sigma : \frac{\mathbb{C}[X]}{X^N + 1} \to \mathbb{C}^N$$

- First lets notice a few things about the modulus N. The ring $\frac{\mathbb{Z}[X]}{X^N+1}$ is in some way defined by a cyclotomic polynomial of degree N.

- First lets notice a few things about the modulus N. The ring $\frac{\mathbb{Z}[X]}{X^N+1}$ is in some way defined by a cyclotomic polynomial of degree N.
- In CKKS they usually consider N to be a power of 2, $N = 2^k$. So we need cyclotomic polynomial of degree $N = 2^k$.

- First lets notice a few things about the modulus N. The ring $\frac{\mathbb{Z}[X]}{X^N+1}$ is in some way defined by a cyclotomic polynomial of degree N.
- In CKKS they usually consider N to be a power of 2, $N = 2^k$. So we need cyclotomic polynomial of degree $N = 2^k$.
- Since as we noted earlier the degree of the n-th cyclotomic is equal to $\rho(n)$ it is easy to find a cyclotomic of the appropriate degree as $\rho(2^{k+1}) = 2^k$, since the only numbers that have a common factor with 2^k will be only the even numbers less than 2^k

- Once we have our cyclotomic of degree N to map a polynomial of degree N to a vector in C^N we simply evaluate that polynomial at the N roots our our cyclotomic

- Once we have our cyclotomic of degree N to map a polynomial of degree N to a vector in C^N we simply evaluate that polynomial at the N roots our our cyclotomic
- For a single root of unity ω, and a polynomial $P(x)$ we have

$$P(\omega) = a_N\omega^N + a_{N-1}\omega^{N-1} + \cdots + a_0\omega^0 = b_i$$

- Once we have our cyclotomic of degree N to map a polynomial of degree N to a vector in C^N we simply evaluate that polynomial at the N roots our our cyclotomic
- For a single root of unity ω, and a polynomial $P(x)$ we have

$$P(\omega) = a_N \omega^N + a_{N-1}\omega^{N-1} + \cdots + a_0 \omega^0 = b_i$$

- Our output vector $b \in C^N$ will be the vector of b_is for all roots of our cyclotomic which is ultimately the result of this matrix vector product for $\Phi_8(x) = X^4 + 1$

- Once we have our cyclotomic of degree N to map a polynomial of degree N to a vector in C^N we simply evaluate that polynomial at the N roots our our cyclotomic
- For a single root of unity ω, and a polynomial $P(x)$ we have

$$P(\omega) = a_N\omega^N + a_{N-1}\omega^{N-1} + \cdots + a_0\omega^0 = b_i$$

- Our output vector $b \in C^N$ will be the vector of b_is for all roots of our cyclotomic which is ultimately the result of this matrix vector product for $\Phi_8(x) = X^4 + 1$
- $$\begin{pmatrix} 1 & (e^i\pi/4)^1 & (e^i\pi/4)^2 & (e^i\pi/4)^3 & (e^i\pi/4)^4 \\ 1 & (e^i\pi 3/4)^1 & (e^i\pi 3/4)^2 & (e^i\pi 3/4)^3 & (e^i\pi 3/4)^4 \\ 1 & (e^i\pi 5/4)^1 & (e^i\pi 5/4)^2 & (e^i\pi 5/4)^3 & (e^i\pi 5/4)^4 \\ 1 & (e^i\pi 7/4)^1 & (e^i\pi 7/4)^2 & (e^i\pi 7/4)^3 & (e^i\pi 7/4)^4 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix}$$

- $$\begin{pmatrix} 1 & (e^i\pi/4)^1 & (e^i\pi/4)^2 & (e^i\pi/4)^3 & (e^i\pi/4)^4 \\ 1 & (e^i\pi3/4)^1 & (e^i\pi3/4)^2 & (e^i\pi3/4)^3 & (e^i\pi3/4)^4 \\ 1 & (e^i\pi5/4)^1 & (e^i\pi5/4)^2 & (e^i\pi5/4)^3 & (e^i\pi5/4)^4 \\ 1 & (e^i\pi7/4)^1 & (e^i\pi7/4)^2 & (e^i\pi7/4)^3 & (e^i\pi7/4)^4 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix}$$

- $$\begin{pmatrix} 1 & (e^i\pi/4)^1 & (e^i\pi/4)^2 & (e^i\pi/4)^3 & (e^i\pi/4)^4 \\ 1 & (e^i\pi3/4)^1 & (e^i\pi3/4)^2 & (e^i\pi3/4)^3 & (e^i\pi3/4)^4 \\ 1 & (e^i\pi5/4)^1 & (e^i\pi5/4)^2 & (e^i\pi5/4)^3 & (e^i\pi5/4)^4 \\ 1 & (e^i\pi7/4)^1 & (e^i\pi7/4)^2 & (e^i\pi7/4)^3 & (e^i\pi7/4)^4 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix}$$

- Here we can see we have the coefficient vector **a** that uniquely determines the polynomial and the output vector **b**.

$$\begin{pmatrix} 1 & (e^i\pi/4)^1 & (e^i\pi/4)^2 & (e^i\pi/4)^3 & (e^i\pi/4)^4 \\ 1 & (e^i\pi3/4)^1 & (e^i\pi3/4)^2 & (e^i\pi3/4)^3 & (e^i\pi3/4)^4 \\ 1 & (e^i\pi5/4)^1 & (e^i\pi5/4)^2 & (e^i\pi5/4)^3 & (e^i\pi5/4)^4 \\ 1 & (e^i\pi7/4)^1 & (e^i\pi7/4)^2 & (e^i\pi7/4)^3 & (e^i\pi7/4)^4 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix}$$

- Here we can see we have the coefficient vector **a** that uniquely determines the polynomial and the output vector **b**.
- Its clear from this equation that given one we can compute the other and since this is a square matrix there is one and only one solution

■

$$\begin{pmatrix} 1 & (e^i\pi/4)^1 & (e^i\pi/4)^2 & (e^i\pi/4)^3 & (e^i\pi/4)^4 \\ 1 & (e^i\pi3/4)^1 & (e^i\pi3/4)^2 & (e^i\pi3/4)^3 & (e^i\pi3/4)^4 \\ 1 & (e^i\pi5/4)^1 & (e^i\pi5/4)^2 & (e^i\pi5/4)^3 & (e^i\pi5/4)^4 \\ 1 & (e^i\pi7/4)^1 & (e^i\pi7/4)^2 & (e^i\pi7/4)^3 & (e^i\pi7/4)^4 \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \end{pmatrix}$$

- Here we can see we have the coefficient vector **a** that uniquely determines the polynomial and the output vector **b**.
- Its clear from this equation that given one we can compute the other and since this is a square matrix there is one and only one solution
- so it should be intuitive that this transformation defines an isomorphism between $\mathbb{C}^4$ and $\frac{\mathbb{C}[X]}{X^4+1}$

- At this point we have defined our simplified map and its inverse as essentially the equation we showed in the previous slide

$$\sigma^{-1} : \mathbb{C}^N \to \frac{\mathbb{C}[X]}{X^N + 1}$$

- At this point we have defined our simplified map and its inverse as essentially the equation we showed in the previous slide

$$\sigma^{-1} : \mathbb{C}^N \to \frac{\mathbb{C}[X]}{X^N + 1}$$

- The CKKS map/algorithm $\sigma^{-1} : \mathbb{C}^N \to \frac{\mathbb{Z}[X]}{X^N+1}$ adds further structure in order to place restrictions on this map to ensure that we encode our complex vectors as polynomials with integer coefficients only