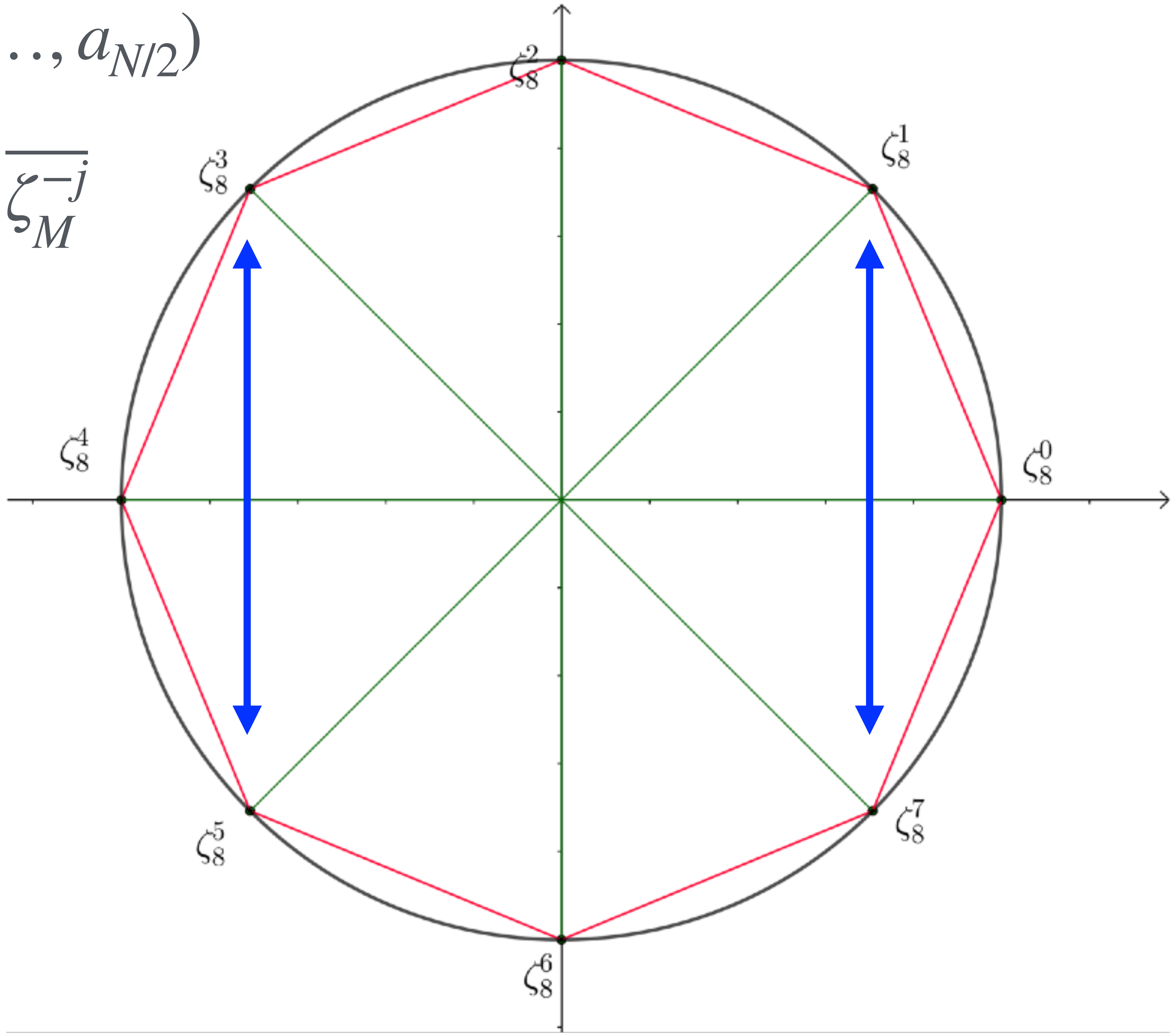
Encodage en vecteurs complexes

Paradigme Single Instruction Multiple Data (SIMD)

$\mathcal{R} = \mathbb{Z}_q[X]/(X^N + 1)$

- On note $\pi : \mathbb{C}^N \to \mathbb{C}^{N/2}$ telle que $\pi(a_1, \ldots a_N) = (a_1, \ldots, a_{N/2})$
- Puisque nos coefficients sont entiers $\forall j \in \mathbb{Z}_M^\times : \zeta_M^j = \overline{\zeta_M^{-j}}$
- Par ex pour $a(x) \in \mathbb{Z}_q[X]/\Phi_8(X)$
- On a 4 coefficients $\Phi_8(X) = X^4 + 1$
- Et $\sigma(a) = (a(\zeta_8^1), a(\zeta_8^3), a(\zeta_8^5), a(\zeta_8^7)) = (z_1, z_2, \overline{z_2}, \overline{z_1})$
- $\pi(\sigma(a)) = (z_1, z_2)$



Encodage en vecteurs complexes

Paradigme Single Instruction Multiple Data (SIMD)

$\mathscr{R} = \mathbb{Z}_q[X]/(X^N + 1)$

- Un polynôme $a(x) \in \mathscr{R}$ peut être décodé dans $\mathbb{C}^{N/2}$ via $\tau : \mathscr{R} \xrightarrow{\sigma} \mathbb{C}^N \xrightarrow{\pi} \mathbb{C}^{N/2}$
- Un vecteur $z \in \mathbb{C}^{N/2}$ peut être encodé dans $\mathscr{R}$ via $\tau^{-1} : \mathbb{C}^{N/2} \xrightarrow{\pi^{-1}} \mathbb{C}^N \xrightarrow{\sigma^{-1}} \mathscr{R}$
- τ est une transformation linéaire, avec une matrice de transformation
- τ^{-1} est calculable en inversant la matrice de τ