The Geometry of Rings

Chris Peikert
Georgia Institute of Technology

SCPQ
29 November 2012

LWE Over Rings (Over-Simplified) [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1 + X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

LWE Over Rings (Over-Simplified) [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1 + X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

- Problem: for $s \leftarrow R_q$, distinguish $\{(a_i\ ,\ b_i)\}$ from uniform $\{(a_i\ ,\ b_i)\}$.

$$\begin{array}{ccc} a_1 \leftarrow R_q & , & b_1 = a_1 \cdot s + e_1 \in R_q \\ a_2 \leftarrow R_q & , & b_2 = a_2 \cdot s + e_2 \in R_q \\ & \vdots & \end{array}$$

LWE Over Rings (Over-Simplified) [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1+X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

- Problem: for $s \leftarrow R_q$, distinguish $\{(a_i\ ,\ b_i)\}$ from uniform $\{(a_i\ ,\ b_i)\}$.

$$\begin{array}{ccc} a_1 \leftarrow R_q & , & b_1 = a_1 \cdot s + e_1 \in R_q \\ a_2 \leftarrow R_q & , & b_2 = a_2 \cdot s + e_2 \in R_q \\ & \vdots & \end{array}$$

- Errors $e(X) \in R$ are "short." What could this mean?

LWE Over Rings (Over-Simplified) [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1+X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

- Problem: for $s \leftarrow R_q$, distinguish $\{(a_i \, , \, b_i)\}$ from uniform $\{(a_i \, , \, b_i)\}$.

$$\begin{array}{ccc} a_1 \leftarrow R_q & , & b_1 = a_1 \cdot s + e_1 \in R_q \\ a_2 \leftarrow R_q & , & b_2 = a_2 \cdot s + e_2 \in R_q \\ & \vdots & \end{array}$$

- Errors $e(X) \in R$ are "short." What could this mean? Identify

$$e(X) = \sum_{j=0}^{n-1} e_j X^j \quad \overset{(?)}{\longleftrightarrow} \quad (e_0, e_1, \ldots e_{n-1}) \in \mathbb{Z}^n.$$

LWE Over Rings (Over-Simplified) [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1 + X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

- Problem: for $s \leftarrow R_q$, distinguish $\{(a_i \, , \, b_i)\}$ from uniform $\{(a_i \, , \, b_i)\}$.

$$\begin{array}{ccc} a_1 \leftarrow R_q & , & b_1 = a_1 \cdot s + e_1 \in R_q \\ a_2 \leftarrow R_q & , & b_2 = a_2 \cdot s + e_2 \in R_q \\ & \vdots & \end{array}$$

- Errors $e(X) \in R$ are "short." What could this mean? Identify

$$e(X) = \sum_{j=0}^{n-1} e_j X^j \quad \overset{(?)}{\longleftrightarrow} \quad (e_0, e_1, \ldots e_{n-1}) \in \mathbb{Z}^n.$$

- Applications need $(+, \cdot)$-combinations of errors to remain short.

LWE Over Rings (Over-Simplified) [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/(1+X^n)}$ for some $n = 2^k$, $\quad R_q := R/qR$.

- Problem: for $s \leftarrow R_q$, distinguish $\{(a_i\ ,\ b_i)\}$ from uniform $\{(a_i\ ,\ b_i)\}$.

$$
\begin{array}{ccc}
a_1 \leftarrow R_q & , & b_1 = a_1 \cdot s + e_1 \in R_q \\
a_2 \leftarrow R_q & , & b_2 = a_2 \cdot s + e_2 \in R_q \\
 & \vdots &
\end{array}
$$

- Errors $e(X) \in R$ are "short." What could this mean? Identify

$$
e(X) = \sum_{j=0}^{n-1} e_j X^j \quad \stackrel{(?)}{\longleftrightarrow} \quad (e_0, e_1, \ldots e_{n-1}) \in \mathbb{Z}^n.
$$

- Applications need $(+, \cdot)$-combinations of errors to remain short. Yes!

$$
\|e + f\| \leq \|e\| + \|f\| \qquad \|e \cdot f\| \leq \sqrt{n} \cdot \|e\| \cdot \|f\|.
$$

"Expansion factor" $\sqrt{n}$ is worst-case. ("On average," $\approx \sqrt{\log n}$.)

Example Application: Homomorphic Encryption [BV'11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k}), R_q = R/qR$. Symmetric key $s \leftarrow R_q$.

Example Application: Homomorphic Encryption [BV'11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k}), R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathsf{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ s.t. $e = m \bmod 2$. Let

$$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

  and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \bmod q$.)

Example Application: Homomorphic Encryption [BV'11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k}), R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathsf{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ s.t. $e = m \bmod 2$. Let

$$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

  and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \bmod q$.)

  Security: (c_1, c_0) is an RLWE sample (essentially).

Example Application: Homomorphic Encryption [BV'11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k}), R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathsf{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ s.t. $e = m \bmod 2$. Let

  $$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

  and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \bmod q$.)

  Security: (c_1, c_0) is an RLWE sample (essentially).
- $\mathsf{Dec}_s(c(S))$: get short $d \in R$ s.t. $d = c(s) \bmod q$. Output $d \bmod 2$.

  Correctness: $d = e$, as long as e has $\mathbb{Z}$-coeffs $\in (-q/2, q/2)$.

Example Application: Homomorphic Encryption [BV'11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k}), R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathsf{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ s.t. $e = m \bmod 2$. Let

$$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

  and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \bmod q$.)

  Security: (c_1, c_0) is an RLWE sample (essentially).

- $\mathsf{Dec}_s(c(S))$: get short $d \in R$ s.t. $d = c(s) \bmod q$. Output $d \bmod 2$.

  Correctness: $d = e$, as long as e has $\mathbb{Z}$-coeffs $\in (-q/2, q/2)$.

- $\mathsf{EvalAdd}(c, c') = (c + c')(S)$, $\mathsf{EvalMul}(c, c') = (c \cdot c')(S)$.

Example Application: Homomorphic Encryption [BV'11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k}), R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\text{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ s.t. $e = m \bmod 2$. Let

  $$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

  and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \bmod q$.)

  Security: (c_1, c_0) is an RLWE sample (essentially).
- $\text{Dec}_s(c(S))$: get short $d \in R$ s.t. $d = c(s) \bmod q$. Output $d \bmod 2$.

  Correctness: $d = e$, as long as e has $\mathbb{Z}$-coeffs $\in (-q/2, q/2)$.
- $\text{EvalAdd}(c, c') = (c + c')(S)$, $\text{EvalMul}(c, c') = (c \cdot c')(S)$.

  Decryption works if $e + e'$, $e \cdot e'$ "short enough."

Example Application: Homomorphic Encryption [BV'11a]

- $R = \mathbb{Z}[X]/(1+X^{2^k})$, $R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathsf{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ s.t. $e = m \bmod 2$. Let

  $$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

  and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \bmod q$.)

  Security: (c_1, c_0) is an RLWE sample (essentially).
- $\mathsf{Dec}_s(c(S))$: get short $d \in R$ s.t. $d = c(s) \bmod q$. Output $d \bmod 2$.

  Correctness: $d = e$, as long as e has $\mathbb{Z}$-coeffs $\in (-q/2, q/2)$.
- $\mathsf{EvalAdd}(c, c') = (c + c')(S)$, $\mathsf{EvalMul}(c, c') = (c \cdot c')(S)$.

  Decryption works if $e + e'$, $e \cdot e'$ "short enough."

  Many mults $\Rightarrow$ large power of expansion factor $\Rightarrow$ tiny error rate $\alpha \Rightarrow$ big parameters!

Other Rings: Cyclotomics

- Used in faster bootstrapping [GHS'12a], homomorphic AES [GHS'12b].

Other Rings: Cyclotomics

- Used in faster bootstrapping [GHS'12a], homomorphic AES [GHS'12b].

  $\boxed{R = \mathbb{Z}[X]/\Phi_m(X)}$ for mth cyclotomic polynomial $\Phi_m(X)$.

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}$$

Other Rings: Cyclotomics

- Used in faster bootstrapping [GHS'12a], homomorphic AES [GHS'12b].

  $\boxed{R = \mathbb{Z}[X]/\Phi_m(X)}$ for mth cyclotomic polynomial $\Phi_m(X)$.

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}$$

- Roots ω^i run over all $n = \varphi(m)$ primitive mth roots of unity.

  "Power" $\mathbb{Z}$-basis of R is $\{1, X, X^2, \ldots, X^{n-1}\}$.

Other Rings: Cyclotomics

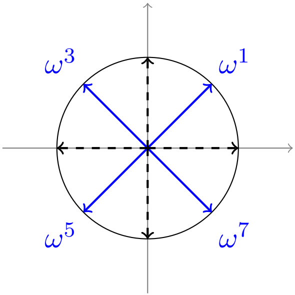
- Used in faster bootstrapping [GHS'12a], homomorphic AES [GHS'12b].

  $\boxed{R = \mathbb{Z}[X]/\Phi_m(X)}$ for mth cyclotomic polynomial $\Phi_m(X)$.

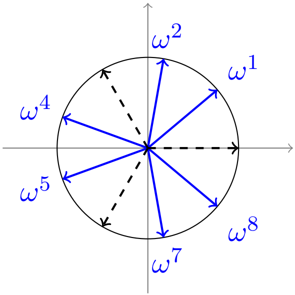
$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}$$

- Roots ω^i run over all $n = \varphi(m)$ primitive mth roots of unity.

  "Power" $\mathbb{Z}$-basis of R is $\{1, X, X^2, \ldots, X^{n-1}\}$.



$\Phi_8(X) = 1 + X^4$



$\Phi_9(X) = 1 + X^3 + X^6$

Other Rings: Cyclotomics

- Used in faster bootstrapping [GHS'12a], homomorphic AES [GHS'12b].

  $\boxed{R = \mathbb{Z}[X]/\Phi_m(X)}$ for mth cyclotomic polynomial $\Phi_m(X)$.

  $$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}$$

- Roots ω^i run over all $n = \varphi(m)$ primitive mth roots of unity.
  "Power" $\mathbb{Z}$-basis of R is $\{1, X, X^2, \ldots, X^{n-1}\}$.

Non-prime power m?

✗ $\Phi_{21}(X) = 1 - X + X^3 - X^4 + X^6 - X^8 + X^9 - X^{11} + X^{12}$

Other Rings: Cyclotomics

- Used in faster bootstrapping [GHS'12a], homomorphic AES [GHS'12b].

  $\boxed{R = \mathbb{Z}[X]/\Phi_m(X)}$ for mth cyclotomic polynomial $\Phi_m(X)$.

  $$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}$$

- Roots ω^i run over all $n = \varphi(m)$ primitive mth roots of unity.

  "Power" $\mathbb{Z}$-basis of R is $\{1, X, X^2, \ldots, X^{n-1}\}$.

Non-prime power m?

✗ $\Phi_{21}(X) = 1 - X + X^3 - X^4 + X^6 - X^8 + X^9 - X^{11} + X^{12}$

✗✗ $\Phi_{105}(X) =$ [degree 48; 33 monomials with $\{-2, -1, 1\}$-coefficients]

Other Rings: Cyclotomics

- Used in faster bootstrapping [GHS'12a], homomorphic AES [GHS'12b].

  $\boxed{R = \mathbb{Z}[X]/\Phi_m(X)}$ for mth cyclotomic polynomial $\Phi_m(X)$.

  $$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}$$

- Roots ω^i run over all $n = \varphi(m)$ primitive mth roots of unity.
  "Power" $\mathbb{Z}$-basis of R is $\{1, X, X^2, \ldots, X^{n-1}\}$.

Non-prime power m?

✗ $\Phi_{21}(X) = 1 - X + X^3 - X^4 + X^6 - X^8 + X^9 - X^{11} + X^{12}$

✗✗ $\Phi_{105}(X) =$ [degree 48; 33 monomials with $\{-2, -1, 1\}$-coefficients]

Annoyances

✗ Irregular $\Phi_m(X) \Rightarrow$ slower, more complex operations

Other Rings: Cyclotomics

- Used in faster bootstrapping [GHS'12a], homomorphic AES [GHS'12b].

  $\boxed{R = \mathbb{Z}[X]/\Phi_m(X)}$ for mth cyclotomic polynomial $\Phi_m(X)$.

  $$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}$$

- Roots ω^i run over all $n = \varphi(m)$ primitive mth roots of unity.
  "Power" $\mathbb{Z}$-basis of R is $\{1, X, X^2, \ldots, X^{n-1}\}$.

Non-prime power m?

✗ $\Phi_{21}(X) = 1 - X + X^3 - X^4 + X^6 - X^8 + X^9 - X^{11} + X^{12}$

✗✗ $\Phi_{105}(X) =$ [degree 48; 33 monomials with $\{-2, -1, 1\}$-coefficients]

Annoyances

✗ Irregular $\Phi_m(X) \Rightarrow$ slower, more complex operations

✗ Large expansion factor $\gg \sqrt{n}$ – even super-poly(n)!

Other Rings: Cyclotomics

- Used in faster bootstrapping [GHS'12a], homomorphic AES [GHS'12b].

  $\boxed{R = \mathbb{Z}[X]/\Phi_m(X)}$ for mth cyclotomic polynomial $\Phi_m(X)$.

$$\Phi_m(X) = \prod_{i \in \mathbb{Z}_m^*} (X - \omega^i) \in \mathbb{Z}[X], \quad \omega = \exp(2\pi\sqrt{-1}/m) \in \mathbb{C}$$

- Roots ω^i run over all $n = \varphi(m)$ primitive mth roots of unity.
  "Power" $\mathbb{Z}$-basis of R is $\{1, X, X^2, \ldots, X^{n-1}\}$.

Non-prime power m?

✗ $\Phi_{21}(X) = 1 - X + X^3 - X^4 + X^6 - X^8 + X^9 - X^{11} + X^{12}$

✗✗ $\Phi_{105}(X) =$ [degree 48; 33 monomials with $\{-2, -1, 1\}$-coefficients]

Annoyances

✗ Irregular $\Phi_m(X) \Rightarrow$ slower, more complex operations

✗ Large expansion factor $\gg \sqrt{n}$ – even super-poly(n)!

✗ Provable hardness also degrades with expansion factor: pay twice!

Talk Agenda

1. Cyclotomic rings and their canonical geometry
   - ✔ No expansion factor anywhere
   - ✔ Provable, tight hardness – same for all cyclotomics
   - ✔ Fast, modular ring operations

Talk Agenda

1. Cyclotomic rings and their canonical geometry
   - ✔ No expansion factor anywhere
   - ✔ Provable, tight hardness – same for all cyclotomics
   - ✔ Fast, modular ring operations

2. The dual ideal $R^\vee$ and ring-LWE

Talk Agenda

1. Cyclotomic rings and their canonical geometry
   - ✔ No expansion factor anywhere
   - ✔ Provable, tight hardness – same for all cyclotomics
   - ✔ Fast, modular ring operations
2. The dual ideal $R^\vee$ and ring-LWE
3. The decoding basis of $R^\vee$ and its properties

Talk Agenda

1. Cyclotomic rings and their canonical geometry
   - ✔ No expansion factor anywhere
   - ✔ Provable, tight hardness – same for all cyclotomics
   - ✔ Fast, modular ring operations
2. The dual ideal $R^\vee$ and ring-LWE
3. The decoding basis of $R^\vee$ and its properties
4. Benefits in applications: tight parameters, algorithmic efficiency

Talk Agenda

1. Cyclotomic rings and their canonical geometry
   - ✔ No expansion factor anywhere
   - ✔ Provable, tight hardness – same for all cyclotomics
   - ✔ Fast, modular ring operations
2. The dual ideal $R^\vee$ and ring-LWE
3. The decoding basis of $R^\vee$ and its properties
4. Benefits in applications: tight parameters, algorithmic efficiency

Based on:

LPR'10 V. Lyubashevsky, C. Peikert, O. Regev.
"On Ideal Lattices and Learning with Errors Over Rings."

LPR'12 V. Lyubashevsky, C. Peikert, O. Regev.
"A Toolkit for Ring-LWE Cryptography."

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more dense.

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more dense.

Reducing to the Prime-Power Case

- Let m have prime-power factorization $m = m_1 \cdots m_\ell$.

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more dense.

Reducing to the Prime-Power Case

- Let m have prime-power factorization $m = m_1 \cdots m_\ell$. Then

$$R = \mathbb{Z}[X]/\Phi_m(X) \;\cong\; \mathbb{Z}[X_1, \ldots, X_\ell]/(\Phi_{m_1}(X_1), \ldots, \Phi_{m_\ell}(X_\ell))$$

via $X_i \mapsto X^{m/m_i}$. (Indeed, X^{m/m_i} has order m_i.)

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more dense.

Reducing to the Prime-Power Case

- Let m have prime-power factorization $m = m_1 \cdots m_\ell$. Then

$$R = \mathbb{Z}[X]/\Phi_m(X) \;\cong\; \mathbb{Z}[X_1, \ldots, X_\ell]/(\Phi_{m_1}(X_1), \ldots, \Phi_{m_\ell}(X_\ell))$$
$$= \bigotimes_i \mathbb{Z}[X_i]/\Phi_{m_i}(X_i),$$

via $X_i \mapsto X^{m/m_i}$. (Indeed, X^{m/m_i} has order m_i.)

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more dense.

Reducing to the Prime-Power Case

- Let m have prime-power factorization $m = m_1 \cdots m_\ell$. Then

$$R = \mathbb{Z}[X]/\Phi_m(X) \;\cong\; \mathbb{Z}[X_1, \ldots, X_\ell]/(\Phi_{m_1}(X_1), \ldots, \Phi_{m_\ell}(X_\ell))$$
$$= \bigotimes_i \mathbb{Z}[X_i]/\Phi_{m_i}(X_i),$$

  via $X_i \mapsto X^{m/m_i}$. (Indeed, X^{m/m_i} has order m_i.)

- R has tensor $\mathbb{Z}$-basis $\{X_1^{j_1} \cdots X_\ell^{j_\ell}\}$, where each $0 \le j_i < \varphi(m_i)$.

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more dense.

Reducing to the Prime-Power Case

- Let m have prime-power factorization $m = m_1 \cdots m_\ell$. Then

$$R = \mathbb{Z}[X]/\Phi_m(X) \;\cong\; \mathbb{Z}[X_1, \ldots, X_\ell]/(\Phi_{m_1}(X_1), \ldots, \Phi_{m_\ell}(X_\ell))$$
$$= \bigotimes_i \mathbb{Z}[X_i]/\Phi_{m_i}(X_i),$$

  via $X_i \mapsto X^{m/m_i}$. (Indeed, X^{m/m_i} has order m_i.)

- R has tensor $\mathbb{Z}$-basis $\{X_1^{j_1} \cdots X_\ell^{j_\ell}\}$, where each $0 \le j_i < \varphi(m_i)$.
  Notice!: tensor basis $\neq$ power basis $\{X^j\}$, $0 \le j < \varphi(m)$.

Cyclotomic Rings

Key Facts

1. For prime p: $\Phi_p(X) = 1 + X + X^2 + \cdots + X^{p-1}$
2. For $m = p^e$: $\Phi_m(X) = \Phi_p(X^{m/p}) = 1 + X^{m/p} + \cdots + X^{m-m/p}$

✗ Otherwise, $\Phi_m(X)$ is less "regular" and more dense.

Reducing to the Prime-Power Case

- Let m have prime-power factorization $m = m_1 \cdots m_\ell$. Then

$$R = \mathbb{Z}[X]/\Phi_m(X) \;\cong\; \mathbb{Z}[X_1, \ldots, X_\ell]/(\Phi_{m_1}(X_1), \ldots, \Phi_{m_\ell}(X_\ell))$$

$$= \bigotimes_i \mathbb{Z}[X_i]/\Phi_{m_i}(X_i),$$

  via $X_i \mapsto X^{m/m_i}$. (Indeed, X^{m/m_i} has order m_i.)

- Bottom line: can reduce operations in R to independent operations in prime-power cyclotomic rings $\mathbb{Z}[X_i]/\Phi_{m_i}(X_i)$.

Canonical Geometry of R

- $R = \mathbb{Z}[X]/\Phi_m(X)$ has $n = \varphi(m)$ ring embeddings (homomorphisms) into $\mathbb{C}$, each given by evaluation at a root of Φ_m:

$$X \mapsto \omega^i \text{ for each } i \in \mathbb{Z}_m^*.$$

Canonical Geometry of R

- $R = \mathbb{Z}[X]/\Phi_m(X)$ has $n = \varphi(m)$ ring embeddings (homomorphisms) into $\mathbb{C}$, each given by evaluation at a root of Φ_m:

$$X \mapsto \omega^i \text{ for each } i \in \mathbb{Z}_m^*.$$

- The *canonical embedding* σ of R into $\mathbb{C}^n$ is $\sigma(a) = \big(\, a(\omega^i) \,\big)_{i \in \mathbb{Z}_m^*}$.

Canonical Geometry of R

- $R = \mathbb{Z}[X]/\Phi_m(X)$ has $n = \varphi(m)$ ring embeddings (homomorphisms) into $\mathbb{C}$, each given by evaluation at a root of Φ_m:

$$X \mapsto \omega^i \text{ for each } i \in \mathbb{Z}_m^*.$$

- The *canonical embedding* σ of R into $\mathbb{C}^n$ is $\sigma(a) = \big(a(\omega^i) \big)_{i \in \mathbb{Z}_m^*}$.
- Define all geometric quantities using σ (*not* coefficient vectors!!).
  E.g., $\|a\|_2 := \|\sigma(a)\|_2$.

Canonical Geometry of R

- $R = \mathbb{Z}[X]/\Phi_m(X)$ has $n = \varphi(m)$ ring embeddings (homomorphisms) into $\mathbb{C}$, each given by evaluation at a root of Φ_m:

$$X \mapsto \omega^i \text{ for each } i \in \mathbb{Z}_m^*.$$

- The *canonical embedding* σ of R into $\mathbb{C}^n$ is $\sigma(a) = \big(a(\omega^i) \big)_{i \in \mathbb{Z}_m^*}$.
- Define all geometric quantities using σ (*not* coefficient vectors!!).

  E.g., $\|a\|_2 := \|\sigma(a)\|_2$.

Nice Properties

✔ Under σ, *both* $+$ and $\cdot$ are coordinate-wise: $\sigma(a \cdot b) = \sigma(a) \odot \sigma(b)$.

Canonical Geometry of R

- $R = \mathbb{Z}[X]/\Phi_m(X)$ has $n = \varphi(m)$ ring embeddings (homomorphisms) into $\mathbb{C}$, each given by evaluation at a root of Φ_m:

$$X \mapsto \omega^i \text{ for each } i \in \mathbb{Z}_m^*.$$

- The *canonical embedding* σ of R into $\mathbb{C}^n$ is $\sigma(a) = \big(a(\omega^i) \big)_{i \in \mathbb{Z}_m^*}$.
- Define all geometric quantities using σ (*not* coefficient vectors!!). E.g., $\|a\|_2 := \|\sigma(a)\|_2$.

Nice Properties

✔ Under σ, *both* $+$ and $\cdot$ are coordinate-wise: $\sigma(a \cdot b) = \sigma(a) \odot \sigma(b)$.

This yields the "expansion" bound

$$\|a \cdot b\|_2 \le \|a\|_\infty \cdot \|b\|_2, \quad \text{where } \|a\|_\infty = \max_i \big| a(\omega^i) \big|.$$

Canonical Geometry of R

- $R = \mathbb{Z}[X]/\Phi_m(X)$ has $n = \varphi(m)$ ring embeddings (homomorphisms) into $\mathbb{C}$, each given by evaluation at a root of Φ_m:

$$X \mapsto \omega^i \text{ for each } i \in \mathbb{Z}_m^*.$$

- The *canonical embedding* σ of R into $\mathbb{C}^n$ is $\sigma(a) = \big(a(\omega^i) \big)_{i \in \mathbb{Z}_m^*}$.
- Define all geometric quantities using σ (*not* coefficient vectors!!). E.g., $\|a\|_2 := \|\sigma(a)\|_2$.

Nice Properties

✔ Under σ, *both* $+$ and $\cdot$ are coordinate-wise: $\sigma(a \cdot b) = \sigma(a) \odot \sigma(b)$. This yields the "expansion" bound

$$\|a \cdot b\|_2 \leq \|a\|_\infty \cdot \|b\|_2 , \quad \text{where } \|a\|_\infty = \max_i \big|a(\omega^i)\big|.$$

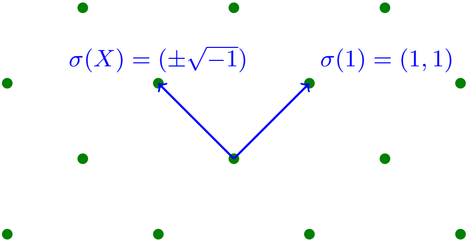
✔ Expansion is element-specific. No more ring "expansion factor."

Example 1

- 4th cyclotomic $R = \mathbb{Z}[X]/(1 + X^2)$: embeddings $X \mapsto \pm\sqrt{-1}$

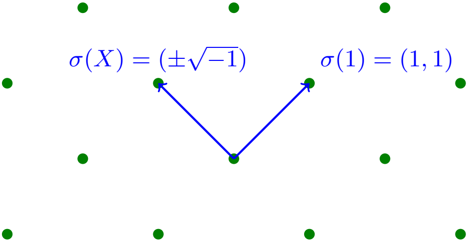
Example 1

- 4th cyclotomic $R = \mathbb{Z}[X]/(1+X^2)$: embeddings $X \mapsto \pm\sqrt{-1}$



Example 1

- 4th cyclotomic $R = \mathbb{Z}[X]/(1+X^2)$: embeddings $X \mapsto \pm\sqrt{-1}$

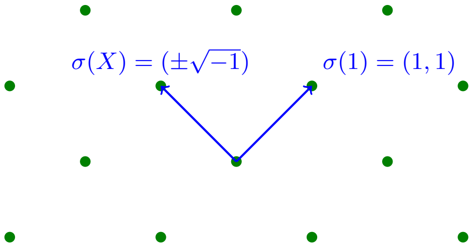


In Any 2^k-th Cyclotomic...

✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.

Example 1

- 4th cyclotomic $R = \mathbb{Z}[X]/(1+X^2)$: embeddings $X \mapsto \pm\sqrt{-1}$



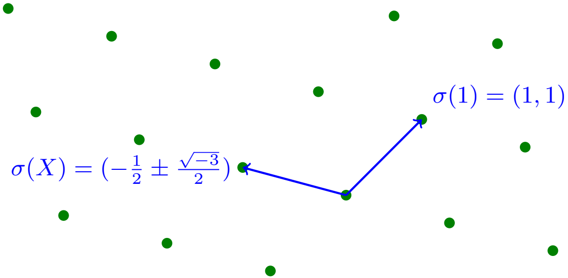
In Any 2^k-th Cyclotomic...

✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.

✔ Power basis $\{1, X, \ldots, X^{n-1}\}$ is orthogonal under embedding σ.
So coefficient/canonical embeddings equivalent (up to $\sqrt{n}$ scaling).

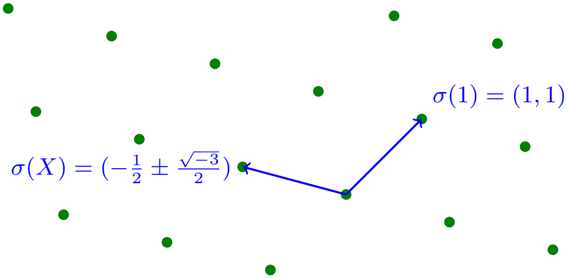
Example 2

- 3rd cyclotomic $R = \mathbb{Z}[X]/(1+X+X^2)$: embed $X \mapsto -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$



Example 2

- 3rd cyclotomic $R = \mathbb{Z}[X]/(1+X+X^2)$: embed $X \mapsto -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$

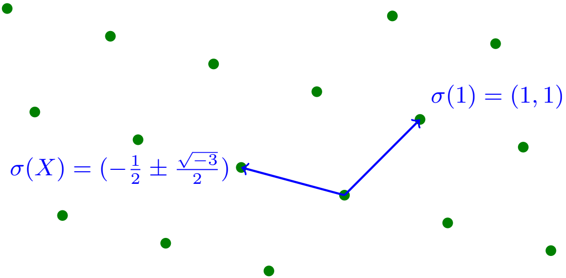


In Any Cyclotomic. . .

✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.

Example 2

- 3rd cyclotomic $R = \mathbb{Z}[X]/(1 + X + X^2)$: embed $X \mapsto -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$

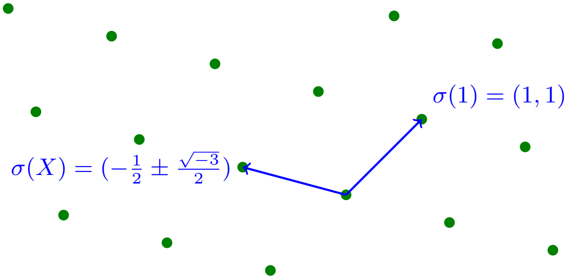


In Any Cyclotomic...

- ✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.
- Power basis $\{1, X, \ldots, X^{n-1}\}$ is not orthogonal (unless $m = 2^k$).

Example 2

- 3rd cyclotomic $R = \mathbb{Z}[X]/(1 + X + X^2)$: embed $X \mapsto -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$

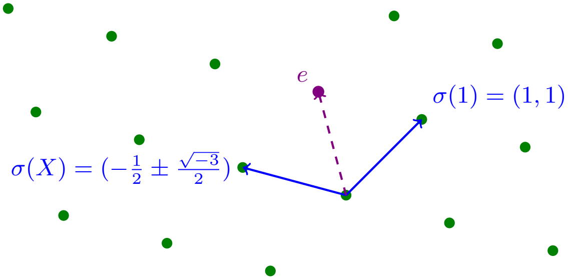


In Any Cyclotomic...

- ✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.
- Power basis $\{1, X, \ldots, X^{n-1}\}$ is not orthogonal (unless $m = 2^k$).
- So in power basis, short elements can have long coeff vectors.

Example 2

- 3rd cyclotomic $R = \mathbb{Z}[X]/(1 + X + X^2)$: embed $X \mapsto -\frac{1}{2} \pm \frac{\sqrt{-3}}{2}$



In Any Cyclotomic...

- ✔ For any j, $\|X^j\|_2 = \sqrt{n}$ and $\|X^j\|_\infty = 1$.
- Power basis $\{1, X, \ldots, X^{n-1}\}$ is not orthogonal (unless $m = 2^k$).
- So in power basis, short elements can have long coeff vectors.

  E.g., $\|e\| = \|1\| = \|X\| = \sqrt{n}$ <u>but</u> $e = 1 + X$.

Duality and the Dual Ideal $R^\vee$

- Define trace function $\mathrm{Tr}\colon R \to \mathbb{Z}$ as $\mathrm{Tr}(a) = \sum_{i \in \mathbb{Z}_m^*} a(\omega^i)$.

Duality and the Dual Ideal $R^\vee$

- Define trace function $\mathrm{Tr}\colon R \to \mathbb{Z}$ as $\mathrm{Tr}(a) = \sum_{i \in \mathbb{Z}_m^*} a(\omega^i)$.
  $\mathrm{Tr}(a \cdot b)$ is (essentially) the "inner product" of embedded a, b:

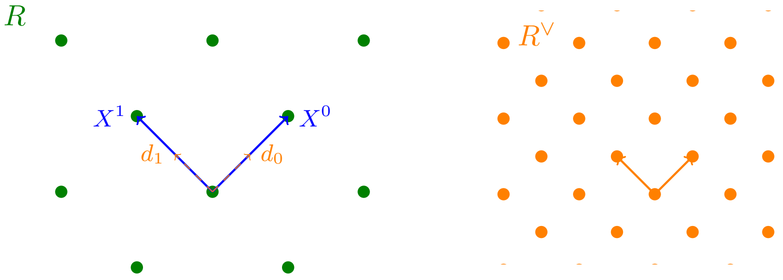
$$\mathrm{Tr}(a \cdot b) = \sum_i a(\omega^i) \cdot b(\omega^i) = \langle \sigma(a) \, , \, \overline{\sigma(b)} \rangle .$$

Duality and the Dual Ideal $R^\vee$

- Define trace function $\mathrm{Tr}\colon R \to \mathbb{Z}$ as $\mathrm{Tr}(a) = \sum_{i \in \mathbb{Z}_m^*} a(\omega^i)$.
  $\mathrm{Tr}(a \cdot b)$ is (essentially) the "inner product" of embedded a, b:

$$\mathrm{Tr}(a \cdot b) = \sum_i a(\omega^i) \cdot b(\omega^i) = \langle \sigma(a) \, , \, \overline{\sigma(b)} \rangle.$$

- Define R's "dual" $R^\vee := \{d : \mathrm{Tr}(a \cdot d) \in \mathbb{Z}, \ \forall \ a \in R\}$.

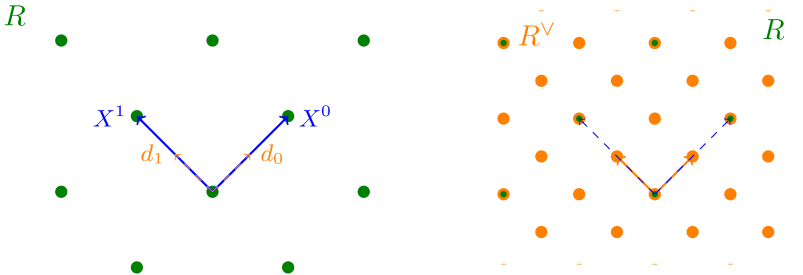


Duality and the Dual Ideal $R^\vee$

- Define trace function $\mathrm{Tr}\colon R \to \mathbb{Z}$ as $\mathrm{Tr}(a) = \sum_{i \in \mathbb{Z}_m^*} a(\omega^i)$.
  $\mathrm{Tr}(a \cdot b)$ is (essentially) the "inner product" of embedded a, b:

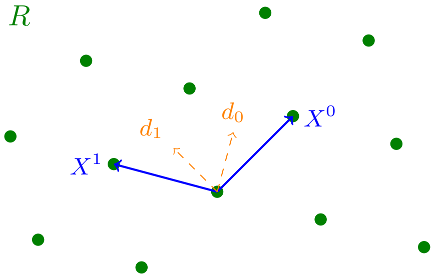
$$\mathrm{Tr}(a \cdot b) = \sum_i a(\omega^i) \cdot b(\omega^i) = \langle \sigma(a) \,,\, \overline{\sigma(b)} \rangle.$$

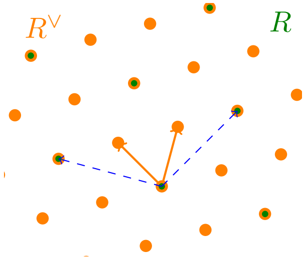
- Define R's "dual" $R^\vee := \{d : \mathrm{Tr}(a \cdot d) \in \mathbb{Z},\ \forall\, a \in R\}$.
  Has "decoding" $\mathbb{Z}$-basis $\{d_{j'}\}$, where $\mathrm{Tr}(X^j \cdot d_{j'}) = \delta_{j,j'}$.



Duality and the Dual Ideal $R^\vee$

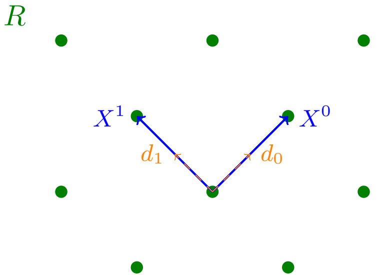
- Define trace function $\mathrm{Tr}\colon R \to \mathbb{Z}$ as $\mathrm{Tr}(a) = \sum_{i \in \mathbb{Z}_m^*} a(\omega^i)$.
  $\mathrm{Tr}(a \cdot b)$ is (essentially) the "inner product" of embedded a, b:
  $$\mathrm{Tr}(a \cdot b) = \sum_i a(\omega^i) \cdot b(\omega^i) = \langle \sigma(a) \, , \, \overline{\sigma(b)} \rangle.$$
- Define R's "dual" $R^\vee := \{d : \mathrm{Tr}(a \cdot d) \in \mathbb{Z}, \ \forall \ a \in R\}$.
  Has "decoding" $\mathbb{Z}$-basis $\{d_{j'}\}$, where $\mathrm{Tr}(X^j \cdot d_{j'}) = \delta_{j,j'}$.

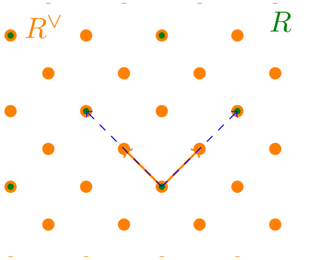




Duality and the Dual Ideal $R^\vee$

- Dual $R^\vee := \{d : \mathrm{Tr}(a \cdot d) \in \mathbb{Z},\ \forall\, a \in R\}$. Basis: $\mathrm{Tr}(X^j \cdot d_{j'}) = \delta_{j,j'}$.



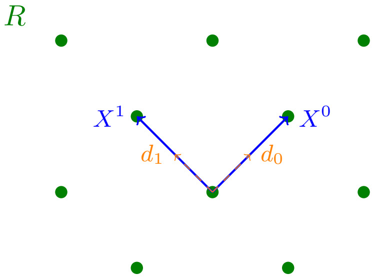


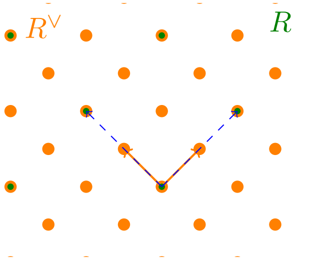
Duality and the Dual Ideal $R^\vee$

- Dual $R^\vee := \{d : \mathrm{Tr}(a \cdot d) \in \mathbb{Z},\ \forall\ a \in R\}$. Basis: $\mathrm{Tr}(X^j \cdot d_{j'}) = \delta_{j,j'}$.

Useful Facts

1. $R^\vee$ is an ideal: $-a$, $a + b$, $a \cdot r \in R^\vee$ for all $a, b \in R^\vee$, $r \in R$.



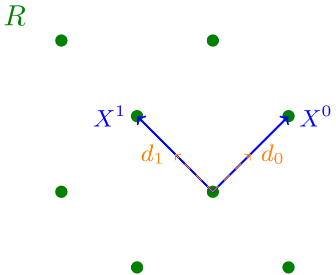


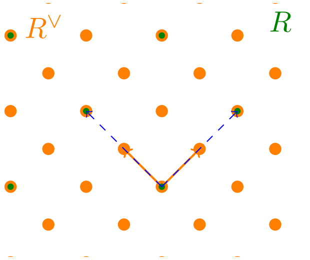
Duality and the Dual Ideal $R^\vee$

- Dual $R^\vee := \{d : \mathrm{Tr}(a \cdot d) \in \mathbb{Z},\ \forall\, a \in R\}$. Basis: $\mathrm{Tr}(X^j \cdot d_{j'}) = \delta_{j,j'}$.

Useful Facts

1. $R^\vee$ is an ideal: $-a,\ a+b,\ a \cdot r \in R^\vee$ for all $a, b \in R^\vee$, $r \in R$.
2. For $m = 2^k$ (dim $n = m/2$): $\{X^j\}$ orthogonal and $\|X^j\| = \sqrt{n}$.
   So $d_j = \frac{1}{n} X^j$ and $R^\vee = \frac{1}{n} R$. I.e., R and $R^\vee$ equivalent up to scale.



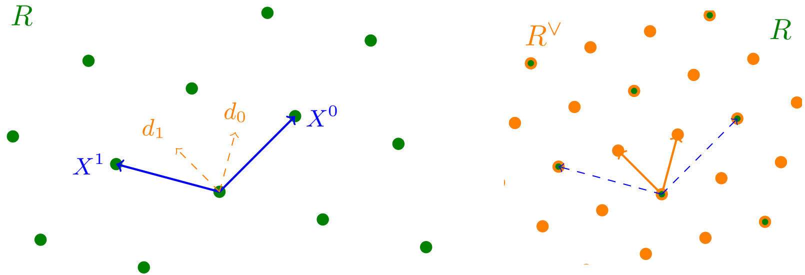


Duality and the Dual Ideal $R^\vee$

- Dual $R^\vee := \{d : \mathrm{Tr}(a \cdot d) \in \mathbb{Z},\ \forall\, a \in R\}$. Basis: $\mathrm{Tr}(X^j \cdot d_{j'}) = \delta_{j,j'}$.

Useful Facts

1. $R^\vee$ is an ideal: $-a$, $a + b$, $a \cdot r \in R^\vee$ for all $a, b \in R^\vee$, $r \in R$.
2. For $m = 2^k$ (dim $n = m/2$): $\{X^j\}$ orthogonal and $\|X^j\| = \sqrt{n}$.
   So $d_j = \frac{1}{n} X^j$ and $R^\vee = \frac{1}{n} R$. I.e., R and $R^\vee$ equivalent up to scale.
3. In general, $mR^\vee \subseteq R \subseteq R^\vee$, with $mR^\vee \approx R$.

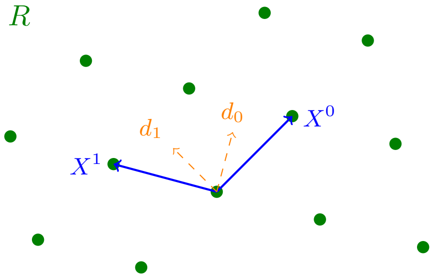


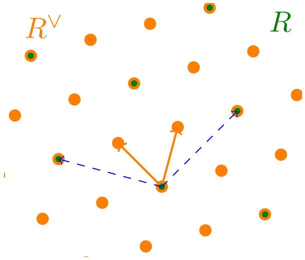
Duality and the Dual Ideal $R^\vee$

- Dual $R^\vee := \{d : \mathrm{Tr}(a \cdot d) \in \mathbb{Z},\ \forall\, a \in R\}$. Basis: $\mathrm{Tr}(X^j \cdot d_{j'}) = \delta_{j,j'}$.

Super-Useful Fact

✔ If $e \in R^\vee$ is short, its $\mathbb{Z}$-coeffs in decoding basis $\{d_j\}$ are small:





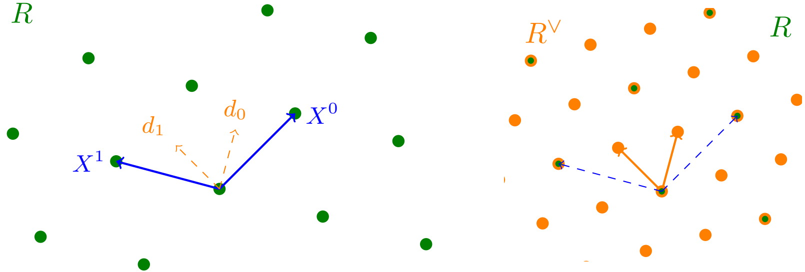
Duality and the Dual Ideal $R^\vee$

- Dual $R^\vee := \{d : \mathrm{Tr}(a \cdot d) \in \mathbb{Z},\ \forall\, a \in R\}$. Basis: $\mathrm{Tr}(X^j \cdot d_{j'}) = \delta_{j,j'}$.

Super-Useful Fact

✔ If $e \in R^\vee$ is short, its $\mathbb{Z}$-coeffs in decoding basis $\{d_j\}$ are small:

$$e = \sum_j e_j d_j \quad (e_j \in \mathbb{Z}) \quad \Longrightarrow \quad e_j = \mathrm{Tr}(X^j \cdot e) \le \|e\| \cdot \sqrt{n}.$$



Duality and the Dual Ideal $R^\vee$

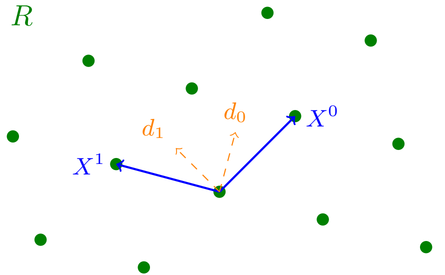
- Dual $R^\vee := \{d : \mathrm{Tr}(a \cdot d) \in \mathbb{Z},\ \forall\, a \in R\}$. Basis: $\mathrm{Tr}(X^j \cdot d_{j'}) = \delta_{j,j'}$.

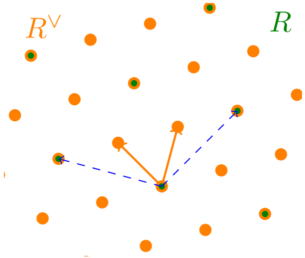
Super-Useful Fact

✔ If $e \in R^\vee$ is short, its $\mathbb{Z}$-coeffs in decoding basis $\{d_j\}$ are small:

$$e = \sum_j e_j d_j \quad (e_j \in \mathbb{Z}) \quad \Longrightarrow \quad e_j = \mathrm{Tr}(X^j \cdot e) \le \|e\| \cdot \sqrt{n}.$$

(Better: Gaussian e w/std. dev. $s \Rightarrow$ Gaussian e_j w/std. dev. $s\sqrt{n}$.)





Ring-LWE: The Complete Definition [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/\Phi_m(X)}$ for any m, $\quad R_q = R/qR,\ R_q^\vee = R^\vee/qR^\vee$.

Ring-LWE: The Complete Definition [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/\Phi_m(X)}$ for any m, $\quad R_q = R/qR,\ R_q^\vee = R^\vee/qR^\vee$.

- Problem: for $s \leftarrow R_q^\vee$, distinguish $\{(a_i\ ,\ b_i)\}$ from uniform $\{(a_i\ ,\ b_i)\}$.

$$\begin{array}{ccc} a_1 \leftarrow R_q & , & b_1 = a_1 \cdot s + e_1 \in R_q^\vee \\ a_2 \leftarrow R_q & , & b_2 = a_2 \cdot s + e_2 \in R_q^\vee \\ & \vdots & \end{array}$$

Ring-LWE: The Complete Definition [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/\Phi_m(X)}$ for any m, $\quad R_q = R/qR,\ R_q^\vee = R^\vee/qR^\vee$.

- Problem: for $s \leftarrow R_q^\vee$, distinguish $\{(a_i\ ,\ b_i)\}$ from uniform $\{(a_i\ ,\ b_i)\}$.

$$\begin{array}{ccc} a_1 \leftarrow R_q & , & b_1 = a_1 \cdot s + e_1 \in R_q^\vee \\ a_2 \leftarrow R_q & , & b_2 = a_2 \cdot s + e_2 \in R_q^\vee \\ & \vdots & \end{array}$$

- Errors $e \in R^\vee$ Gaussian (w/std. dev. αq) in canonical embedding.
  So $|e(\omega^i)| \approx \alpha q$ are independent* – but coeffs $|e_j| \approx \alpha q \sqrt{n}$ are not!

Ring-LWE: The Complete Definition [LPR'10]

Ring $\boxed{R := \mathbb{Z}[X]/\Phi_m(X)}$ for any m, $\quad R_q = R/qR,\ R_q^\vee = R^\vee/qR^\vee$.

- Problem: for $s \leftarrow R_q^\vee$, distinguish $\{(a_i\ ,\ b_i)\}$ from uniform $\{(a_i\ ,\ b_i)\}$.

$$\begin{array}{ccc} a_1 \leftarrow R_q & , & b_1 = a_1 \cdot s + e_1 \in R_q^\vee \\ a_2 \leftarrow R_q & , & b_2 = a_2 \cdot s + e_2 \in R_q^\vee \\ & \vdots & \end{array}$$

- Errors $e \in R^\vee$ Gaussian (w/std. dev. αq) in canonical embedding. So $|e(\omega^i)| \approx \alpha q$ are independent* – but coeffs $|e_j| \approx \alpha q \sqrt{n}$ are not!

Theorem

For any m, ring-LWE with error std. dev. $\alpha q \geq 6^*$ is (quantumly) as hard as $\tilde{O}(n/\alpha)$-SVP on any ideal lattice in R.

BV Homomorphic Encryption, Revisited

- Symmetric key $s \leftarrow R_q$.

BV Homomorphic Encryption, Revisited

- Symmetric key $s \leftarrow R_q$.
- $\mathsf{Enc}_s(m \in R_2^\vee)$: choose Gaussian $e \in R^\vee$ s.t. $e = m \bmod 2R^\vee$. Let

$$c_1 \leftarrow R_q^\vee \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q^\vee$$

and output $c(S) = c_0 + c_1 S \in R_q^\vee[S]$. (Note: $c(s) = e \bmod qR^\vee$.)

BV Homomorphic Encryption, Revisited

- Symmetric key $s \leftarrow R_q$.
- $\mathsf{Enc}_s(m \in R_2^\vee)$: choose Gaussian $e \in R^\vee$ s.t. $e = m \bmod 2R^\vee$. Let

$$c_1 \leftarrow R_q^\vee \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q^\vee$$

  and output $c(S) = c_0 + c_1 S \in R_q^\vee[S]$. (Note: $c(s) = e \bmod qR^\vee$.)
- $\mathsf{Dec}_s(c(S))$: get short $d \in R^\vee$ s.t. $d = c(s) \bmod qR^\vee$.

  Correctness: $d = e$, if e's decoding basis $\mathbb{Z}$-coeffs $\in (-q/2, q/2)$.

BV Homomorphic Encryption, Revisited

- Symmetric key $s \leftarrow R_q$.
- Enc$_s(m \in R_2^\vee)$: choose Gaussian $e \in R^\vee$ s.t. $e = m \bmod 2R^\vee$. Let

$$c_1 \leftarrow R_q^\vee \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q^\vee$$

  and output $c(S) = c_0 + c_1 S \in R_q^\vee[S]$. (Note: $c(s) = e \bmod qR^\vee$.)
- Dec$_s(c(S))$: get short $d \in R^\vee$ s.t. $d = c(s) \bmod qR^\vee$.

  Correctness: $d = e$, if e's decoding basis $\mathbb{Z}$-coeffs $\in (-q/2, q/2)$.
- EvalMul$(c, c') = (c \cdot c')(S) \in (R^\vee)_q^k[S]$ where $k = \deg(c) + \deg(c')$.

BV Homomorphic Encryption, Revisited

- Symmetric key $s \leftarrow R_q$.
- $\mathsf{Enc}_s(m \in R_2^\vee)$: choose Gaussian $e \in R^\vee$ s.t. $e = m \bmod 2R^\vee$. Let

$$c_1 \leftarrow R_q^\vee \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q^\vee$$

  and output $c(S) = c_0 + c_1 S \in R_q^\vee[S]$. (Note: $c(s) = e \bmod qR^\vee$.)
- $\mathsf{Dec}_s(c(S))$: get short $d \in R^\vee$ s.t. $d = c(s) \bmod qR^\vee$.

  Correctness: $d = e$, if e's decoding basis $\mathbb{Z}$-coeffs $\in (-q/2, q/2)$.
- $\mathsf{EvalMul}(c, c') = (c \cdot c')(S) \in (R^\vee)_q^k[S]$ where $k = \deg(c) + \deg(c')$.
  - ★ Noise $e = e_1 \cdots e_k \in (R^\vee)^k$, so $m^{k-1} e \in R^\vee$.

BV Homomorphic Encryption, Revisited

- Symmetric key $s \leftarrow R_q$.
- $\mathsf{Enc}_s(m \in R_2^\vee)$: choose Gaussian $e \in R^\vee$ s.t. $e = m \bmod 2R^\vee$. Let

$$c_1 \leftarrow R_q^\vee \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q^\vee$$

  and output $c(S) = c_0 + c_1 S \in R_q^\vee[S]$. (Note: $c(s) = e \bmod qR^\vee$.)
- $\mathsf{Dec}_s(c(S))$: get short $d \in R^\vee$ s.t. $d = c(s) \bmod qR^\vee$.

  Correctness: $d = e$, if e's decoding basis $\mathbb{Z}$-coeffs $\in (-q/2, q/2)$.
- $\mathsf{EvalMul}(c, c') = (c \cdot c')(S) \in (R^\vee)_q^k[S]$ where $k = \deg(c) + \deg(c')$.
  - ⋆ Noise $e = e_1 \cdots e_k \in (R^\vee)^k$, so $m^{k-1} e \in R^\vee$.
  - ⋆ Since $\|e_i\|_\infty \approx \alpha q = 6$, $m^{k-1} e$ has Gaussian std. dev. $\approx 6^k m^{k-1}$.

BV Homomorphic Encryption, Revisited

- Symmetric key $s \leftarrow R_q$.
- $\mathsf{Enc}_s(m \in R_2^\vee)$: choose Gaussian $e \in R^\vee$ s.t. $e = m \bmod 2R^\vee$. Let

$$c_1 \leftarrow R_q^\vee \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q^\vee$$

and output $c(S) = c_0 + c_1 S \in R_q^\vee[S]$. (Note: $c(s) = e \bmod qR^\vee$.)

- $\mathsf{Dec}_s(c(S))$: get short $d \in R^\vee$ s.t. $d = c(s) \bmod qR^\vee$.

Correctness: $d = e$, if e's decoding basis $\mathbb{Z}$-coeffs $\in (-q/2, q/2)$.

- $\mathsf{EvalMul}(c, c') = (c \cdot c')(S) \in (R^\vee)_q^k[S]$ where $k = \deg(c) + \deg(c')$.
  - ⋆ Noise $e = e_1 \cdots e_k \in (R^\vee)^k$, so $m^{k-1} e \in R^\vee$.
  - ⋆ Since $\|e_i\|_\infty \approx \alpha q = 6$, $m^{k-1} e$ has Gaussian std. dev. $\approx 6^k m^{k-1}$.
  - ⋆ So need $q \approx 6^k m^{k-1} \sqrt{n} \approx (6m)^k$ to decrypt deg-k ciphertexts.
    Versus $q \approx \gamma^{k-1} n^k$ via expansion factor $\gamma \gg \sqrt{n}$.
    $\Rightarrow \approx \gamma^{k-1}$ factor improvement in error rate.

Conclusions

1. Using canonical geometry yields tight noise expansion, clean analysis in all cyclotomics.

Conclusions

1. Using canonical geometry yields tight noise expansion, clean analysis in all cyclotomics.

2. Using $R^\vee$ with the decoding basis yields smaller coefficients $\Rightarrow$ larger noise rates $\Rightarrow$ smaller params/higher security.

Conclusions

1. Using canonical geometry yields tight noise expansion, clean analysis in all cyclotomics.

2. Using $R^\vee$ with the decoding basis yields smaller coefficients $\Rightarrow$ larger noise rates $\Rightarrow$ smaller params/higher security.

3. Using the tensor basis of

$$R \cong \mathbb{Z}[X_1, \ldots, X_\ell]/(\Phi_{m_1}(X_1), \ldots, \Phi_{m_\ell}(X_\ell))$$

yields fast, modular algorithms for all cyclotomics.

Conclusions

1. Using canonical geometry yields tight noise expansion, clean analysis in all cyclotomics.

2. Using $R^\vee$ with the decoding basis yields smaller coefficients $\Rightarrow$ larger noise rates $\Rightarrow$ smaller params/higher security.

3. Using the tensor basis of

$$R \cong \mathbb{Z}[X_1, \ldots, X_\ell]/(\Phi_{m_1}(X_1), \ldots, \Phi_{m_\ell}(X_\ell))$$

yields fast, modular algorithms for all cyclotomics.

Thanks!