Cyclotomic Cosets: Hidden Subgroups and Quantum Algorithms for prime-power moduli

Séminaire Crypto 06/11/2026

Mathias BOUCHER · Pierre-Alain FOUQUE · Yixin SHEN

Université de Rennes

Inria

UMR IRISA

Introduction

Quantum preliminaries



Quantum preliminaries





Source: -r/ScienceMemes (Reddit).

Quantum preliminaries

What is a quantum state?

- A quantum state over a set A is of the form

$$|\psi\rangle = \sum_{x \in A} \alpha_x |x\rangle,$$

  where $\alpha_x \in \mathbb{C}$ is such that $\sum_{x \in A} |\alpha_x|^2 = 1$.
- The probability to measure $x \in A$ is $|\alpha_x|^2$.
- The family $(|x\rangle)_{x \in A}$ is a basis of $\mathbb{C}^{|A|}$. Hence, a quantum state over A is a element of $\mathbb{C}^{|A|}$ up to a normalization factor.

(for simplicity we will sometimes omit the normalization factor in this presentation)

Quantum preliminaries

What can we do?

- **Entangle** quantum states.

Let $|\psi_A\rangle = \sum_{x \in A} \alpha_x |x\rangle$ and $|\psi_B\rangle = \sum_{y \in B} \beta_y |y\rangle$ be two quantum states. It is possible two consider the quantum state

$$|\psi_A\rangle \otimes |\psi_B\rangle = \sum_{(x,y) \in A \times B} \alpha_x \beta_y |x\rangle |y\rangle$$

which is a vector of $\mathbb{C}^{|A \times B|}$ up to a normalization factor.

Quantum preliminaries

What can we do?

- Apply a **unitary transformation** (a quantum gate)

This is a linear map $U : \mathbb{C}^{|A|} \to \mathbb{C}^{|A|}$ such that for every quantum state $|\psi\rangle$,

$$\||\psi\rangle\|_2^2 = \|U|\psi\rangle\|_2^2.$$

Quantum preliminaries

What can we do?

- Apply a **unitary transformation** (a quantum gate)

This is a linear map $U : \mathbb{C}^{|A|} \to \mathbb{C}^{|A|}$ such that for every quantum state $|\psi\rangle$,

$$\||\psi\rangle\|_2^2 = \|U|\psi\rangle\|_2^2.$$

An important example: **the control gate**. Suppose $(B, +)$ is a group. Let $f : A \to B$ be a function, one can define the linear map $U_f : \mathbb{C}^{|A\times B|} \to \mathbb{C}^{|A\times B|}$ as,

$$U_f|x\rangle|y\rangle = |x\rangle|y + f(x)\rangle.$$

We "compute a function f in a new register" means that

$$\sum_{x\in A} \alpha_x|x\rangle \overset{\otimes|0\rangle}{\longrightarrow} \sum_{x\in A} \alpha_x|x\rangle|0\rangle \overset{U_f}{\longrightarrow} \sum_{x\in A} \alpha_x|x\rangle|f(x)\rangle.$$

Quantum preliminaries

What can we do?

- **Measure** a register.

If we have only **one** register

$$|\psi\rangle = \sum_{x \in A} \alpha_x |x\rangle,$$

the probability to measure $x_0 \in A$ is $\left|\alpha_{x_0}\right|^2$.

Quantum preliminaries

What can we do?

- **Measure** a register.

If we have only **one** register

$$|\psi\rangle = \sum_{x \in A} \alpha_x |x\rangle,$$

the probability to measure $x_0 \in A$ is $\left|\alpha_{x_0}\right|^2$.

If we have **many** registers

$$|\psi\rangle = \sum_{x \in A, y \in B} \alpha_{x,y} |x\rangle |y\rangle,$$

can always put $|\psi\rangle$ to the form:

$$\sum_{y \in B} \alpha'_y \left|\psi_y\right\rangle |y\rangle,$$

with $\left|\psi_y\right\rangle$ a normalized quantum state over $x \in A$, depending only on y.

We measure $y_0 \in B$ with probability $\left|\alpha'_{y_0}\right|^2$, it remains the state $\left|\psi_{y_0}\right\rangle$.

Example of quantum primitive

Hidden Subgroup Problem. Let G be a group, and H a secret subgroup of G. Given a certain function $f : G \to S$ which is H-periodic (i.e. $f(xh) = f(x)$) $\Rightarrow$ find H.

Example of quantum primitive

Hidden Subgroup Problem. Let G be a group, and H a secret subgroup of G. Given a certain function $f : G \to S$ which is H-periodic (i.e. $f(xh) = f(x)$) $\Rightarrow$ find H.

1. Generate a superposition over G

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle.$$

2. Compute f in a new register (i.e. **entangle** $|0\rangle$ and compute the **unitary** U_f),

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle.$$

3. **Measure** it, output b $(= f(x))$

$$f^{-1}\{b\} = xH$$

the remaining state becomes

$$|\psi_x\rangle = \frac{1}{\sqrt{|f^{-1}\{b\}|}} \sum_{y \in f^{-1}\{b\}} |y\rangle$$

$$= \frac{1}{\sqrt{|H|}} \sum_{h \in H} |xh\rangle.$$

Example of quantum primitive

Hidden Subgroup Problem. Let G be a group, and H a secret subgroup of G. Given a certain function $f : G \to S$ which is H-periodic (i.e. $f(xh) = f(x)$) $\Rightarrow$ find H.

1. Generate a superposition over G

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle.$$

2. Compute f in a new register (i.e. **entangle** $|0\rangle$ and compute the **unitary** U_f),

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle.$$

3. **Measure** it, output b $(= f(x))$

$$f^{-1}\{b\} = xH$$

the remaining state becomes

$$|\psi_x\rangle = \frac{1}{\sqrt{|f^{-1}\{b\}|}} \sum_{y \in f^{-1}\{b\}} |y\rangle$$

$$= \frac{1}{\sqrt{|H|}} \sum_{h \in H} |xh\rangle.$$

Given quantum samples of the form $|\psi_x\rangle$, the goal is to find H.

💡 It is a **Coset Problem**.

Learning With Error

Dimension n, modulus q both $\gg 1$.

Learning With Error (LWE)

Fix a secret $\boldsymbol{s} \in \mathbb{Z}_q^n$. Given samples of the form

$$(a_i, \langle a_i, \boldsymbol{s} \rangle + e \bmod q)$$

$a_i \in \mathcal{U}(\mathbb{Z}_q^n)$ and e a Gaussian error. The $\mathrm{LWE}_{n,q,\alpha}$ problem asks to find $\boldsymbol{s} \in \mathbb{Z}_q^n$.

Why is it so important ?

- Cornerstone of many post-quantum scheme (Kyber, Dilithium...)
- Many reductions with other lattice problems.

↳ Study the security of LWE by watching on quantum primitives.

The Dihedral Coset Problem and its friends

The Dihedral Group

The **dihedral group** of order $2N$ is

$$D_N = \mathbb{F}_2 \rtimes \mathbb{Z}_N$$

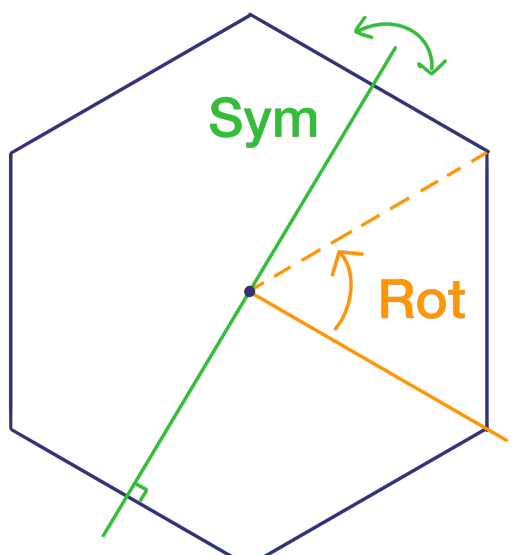
Let (b_1, x_1) and (b_2, x_2) in $\mathbb{F}_2 \times \mathbb{Z}_N$, the **group law** of D_N is,

$$(b_1, x_1) \odot (b_2, x_2) = \big(b_1 + b_2, x_1 + (-1)^{b_1} x_2\big)$$

Proposition

For any $s \in \mathbb{Z}_N$, $(1, s)$ has order 2.

$$(1, s) \odot (1, s) = (0, s - s) = 0$$



$$(\mathrm{Rot} \circ \mathrm{Sym}) \circ (\mathrm{Rot} \circ \mathrm{Sym}) = \mathrm{id}$$

Dihedral Coset Problem

The Dihedral Coset Problem (DCP) is a "Dihedral" Hidden Subgroup Problem (HSP).

Recall that $G = \mathbb{F}_2 \rtimes \mathbb{Z}_N$, $H = \{(0,0),(1,s)\}$. Moreover HSP asks to find H, given quantum samples of the form:

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |xh\rangle \rightsquigarrow \frac{1}{\sqrt{2}}(|0,x\rangle + |1,x+s\rangle).$$

Dihedral Coset Problem (DCP)

Find a secret $s \in \mathbb{Z}_N$ given ℓ quantum samples

$$|\varphi_i\rangle = \frac{1}{\sqrt{2}}(|0,x_i\rangle + |1,x_i+s\rangle),$$

with x_i sampled uniformly over $\mathbb{Z}_N$.

Dihedral Coset Problem

- Used in a lot of context:
  - Dihedral Hidden Subgroup Problem,
  - Hidden Shift Problem,
  - Two Points problem,
  - ...
- [Regev02] LWE $\leq$ DCP for some specific parameters.
- Kuperberg algorithm [Kuperberg05] solves DCP in **subexponential time** given a **subexponential** number of **samples**.

Generalized Hidden Shift Problem

💡 Consider a larger size support M.

Generalized Hidden Shift Problem (2005)

Find the secret $s \in \mathbb{Z}_N$, given ℓ quantum samples of the form

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle |x_i + js\rangle.$$

- **[Childs05]** Algorithmic results: In the case $M = N^{\varepsilon}$, with $\varepsilon > 0$ constant, there exists an algorithm that runs in time $\mathrm{Poly}(\log(N))$, using $\mathcal{O}\left(\frac{1}{\varepsilon}\right)$ samples.

Generalized Hidden Shift Problem

💡 Consider a larger size support M.

Generalized Hidden Shift Problem (2005)

Find the secret $s \in \mathbb{Z}_N$, given ℓ quantum samples of the form

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle |x_i + js\rangle.$$

- **[Childs05]** Algorithmic results: In the case $M = N^\varepsilon$, with $\varepsilon > 0$ constant, there exists an algorithm that runs in time $\mathrm{Poly}(\log(N))$, using $\mathcal{O}\left(\frac{1}{\varepsilon}\right)$ samples.

shift problem for yet smaller M may be a promising path toward improved quantum algorithms for lattice problems. Indeed, for the case $M = 2$, Kuperberg's subexponential-time algorithm outperforms the algorithm given in this paper, so it seems likely that an improved algorithm could be found for values of M intermediate between 2 and N^ϵ.

Another problem suggested by this work is the following generalization

Extrapolated Dihedral Coset Problem

💡 High dimension n, distribution $\chi : \mathbb{Z} \to \mathbb{C}$.

Extrapolated Dihedral Coset Problem (EDCP) (2018)

Find the secret $s \in \mathbb{Z}_q^n$ given ℓ samples of the form

$$\sum_{j \in \mathrm{supp}(\chi)} \chi(j)|j\rangle|x_i + js\rangle$$

- Usually χ is the gaussian distribution, or the uniform distribution over $\{0, ..., M-1\}$.
- **(2018)** In certain parameter regimes, LWE is **equivalent** to EDCP.
- **(2025)** Bai, Jangir, Kirshanova, Ngo, and Youmans developed an algorithm that solves EDCP in **quasi-polynomial** time when q is a power of 2.

Notable algorithms for EDCP

Algorithm	Modulus q	Support size M	Number of samples	Complexity
[Regev04][1]		2	$2^{\log^2(n)}$	$\exp(n)$
[Kuperberg05][2]		2	$2^{\sqrt{n}}$	$2^{\sqrt{n}}$
[Childs05][3]		$M = q^{\varepsilon}$	$\frac{1}{\varepsilon}$	$\mathrm{Poly}(n)$
[BJKNY25][4]	$q = 2^t$	2	$2^{\log^2(n)}$	$2^{\log^2(n)}$

🤓☝️ In fact, there are algorithms for the case where $M > 2$, but they all reduce the problem to samples with $M = 2$.

↳ **Why is the case $q = 2^t$ so special? Can this algorithm be generalized to small prime-power moduli?**

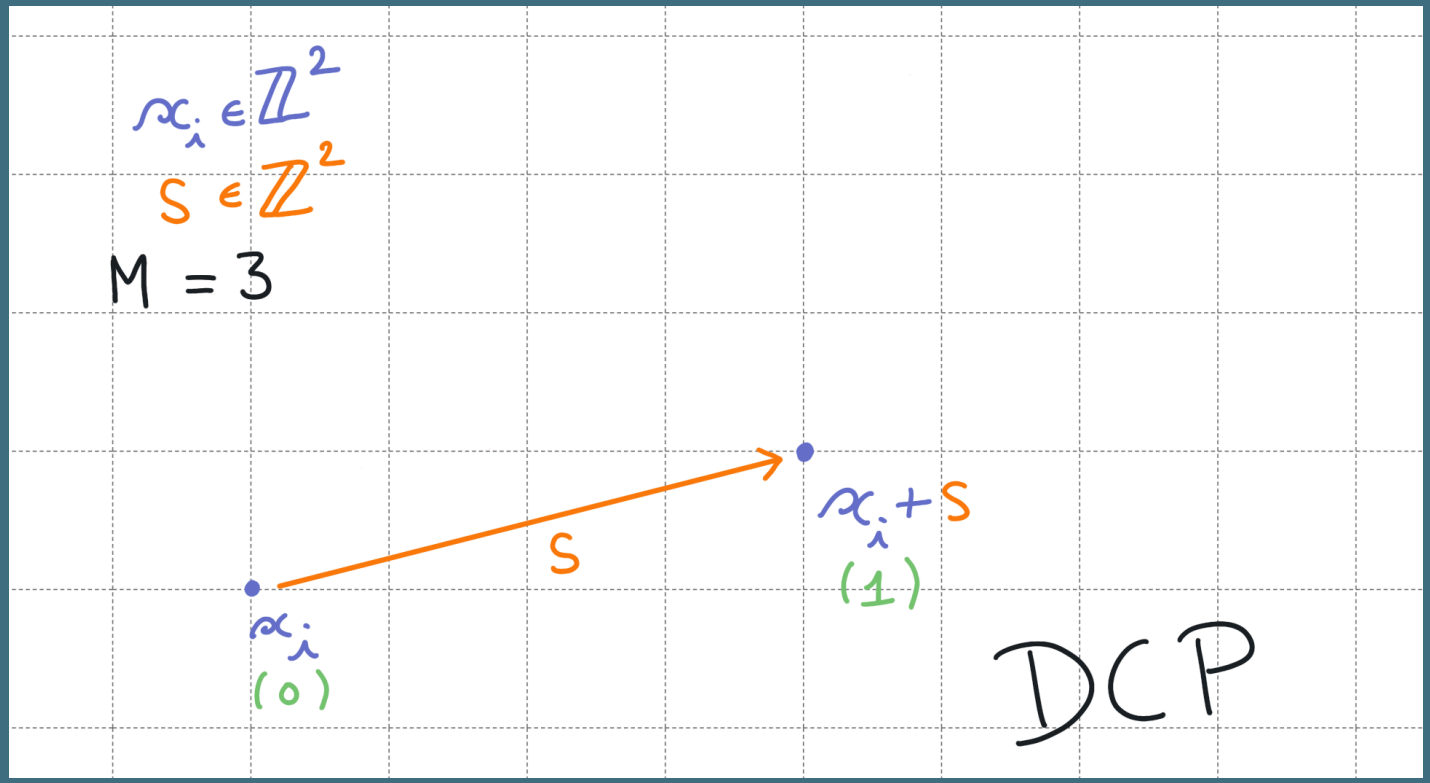
[1] 2004, Regev, Quantum Computation and Lattice Problems.

[2] 2005, Kuperberg, A subexponential-time quantum algorithm for the dihedral hidden subgroup problem.

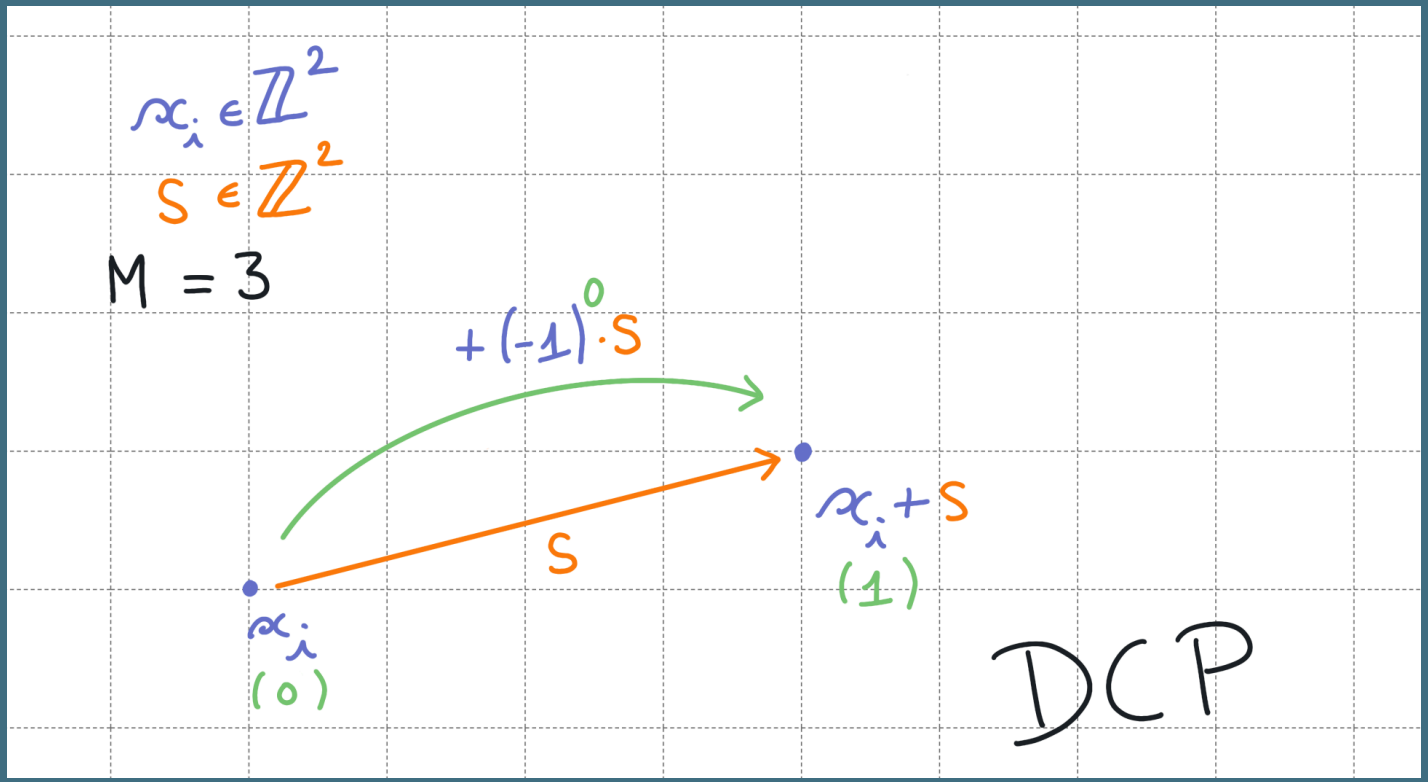
[3] 2005, Childs, van Dam, Quantum algorithm for a generalized hidden shift problem.

[4] 2025, Baï, Jangir, Kirshanova, Ngo, Youmans, A Quasi-polynomial Time Algorithm for the Extrapolated Dihedral Coset Problem over Power-of-Two Moduli.

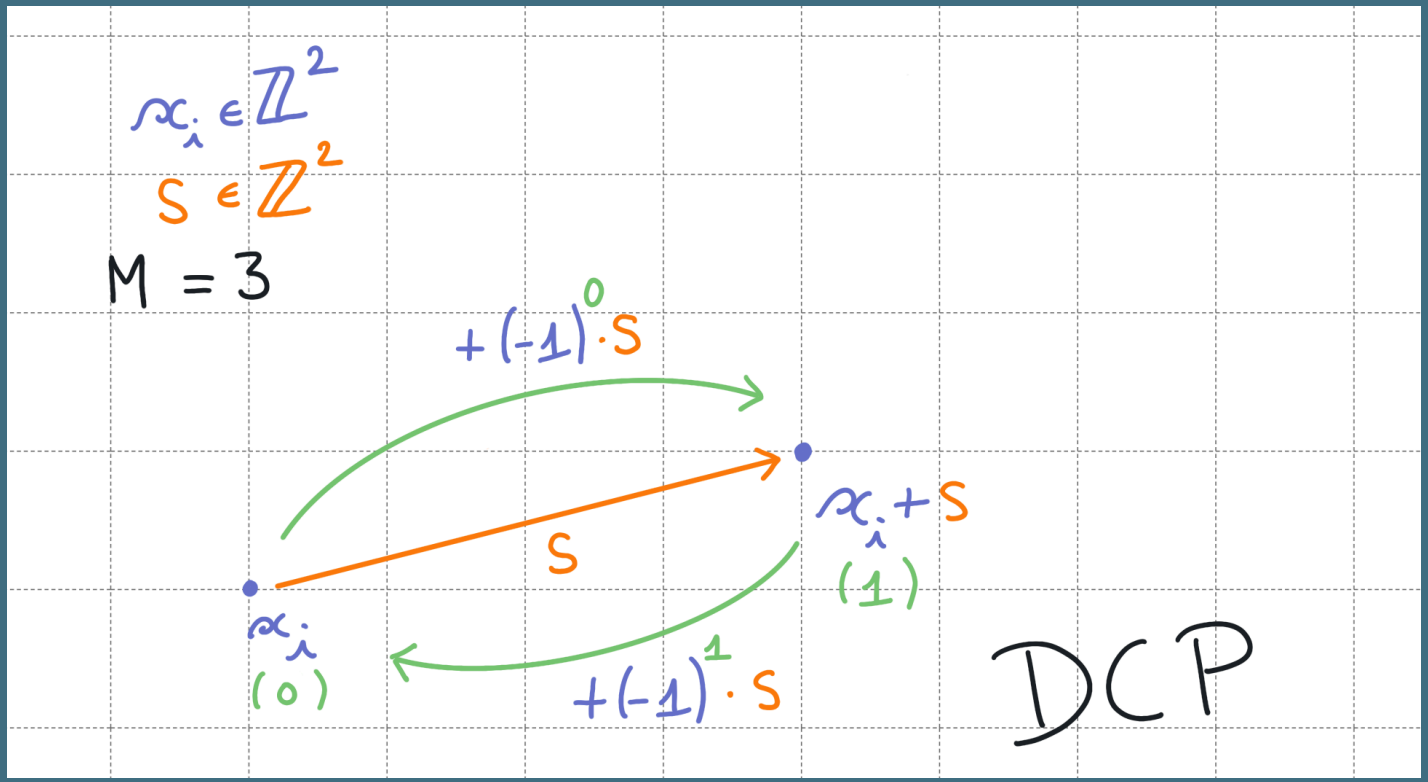
$$|\varphi_i\rangle = \frac{1}{\sqrt{2}}(|0, x_i\rangle + |1, x_i + s\rangle)$$



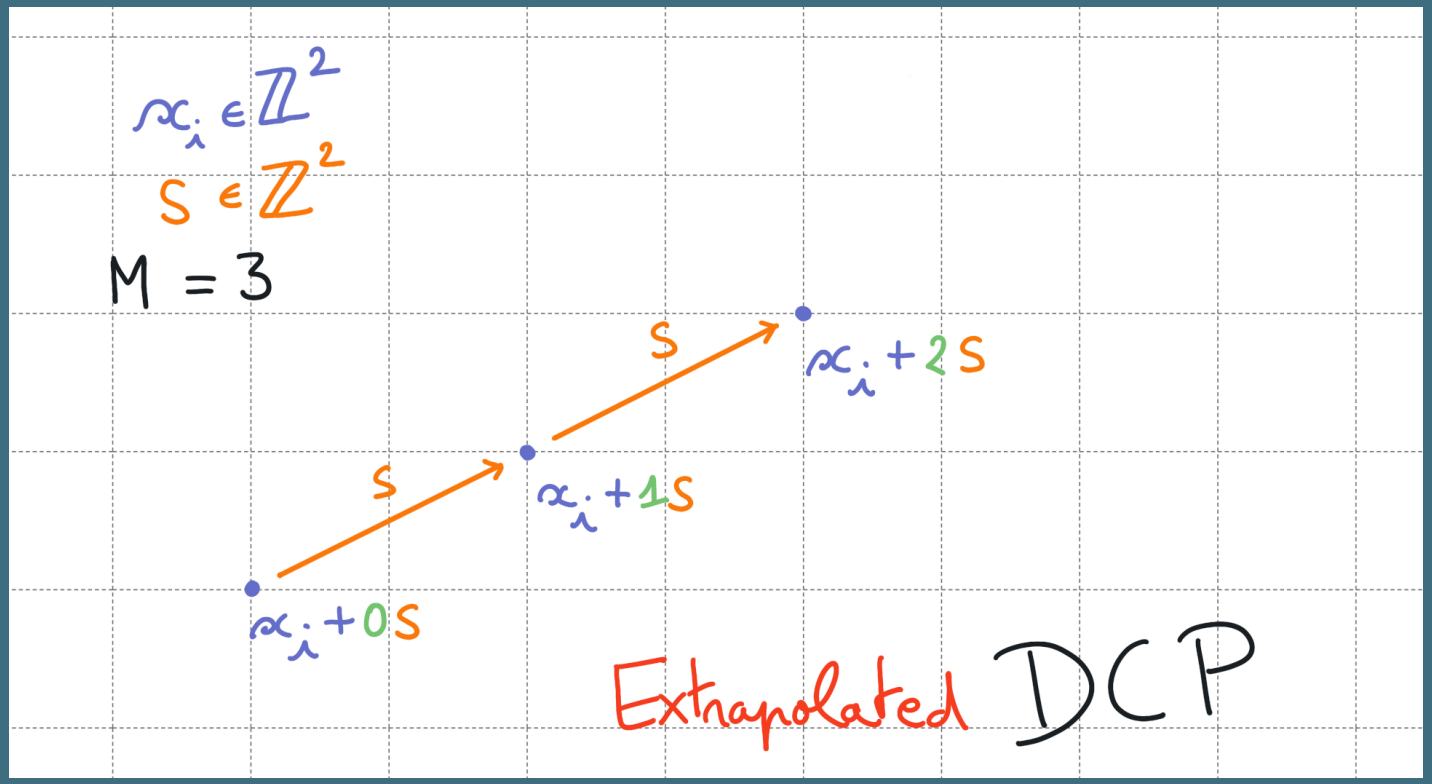
$$|\varphi_i\rangle = \frac{1}{\sqrt{2}}(|0, x_i\rangle + |1, x_i + s\rangle)$$



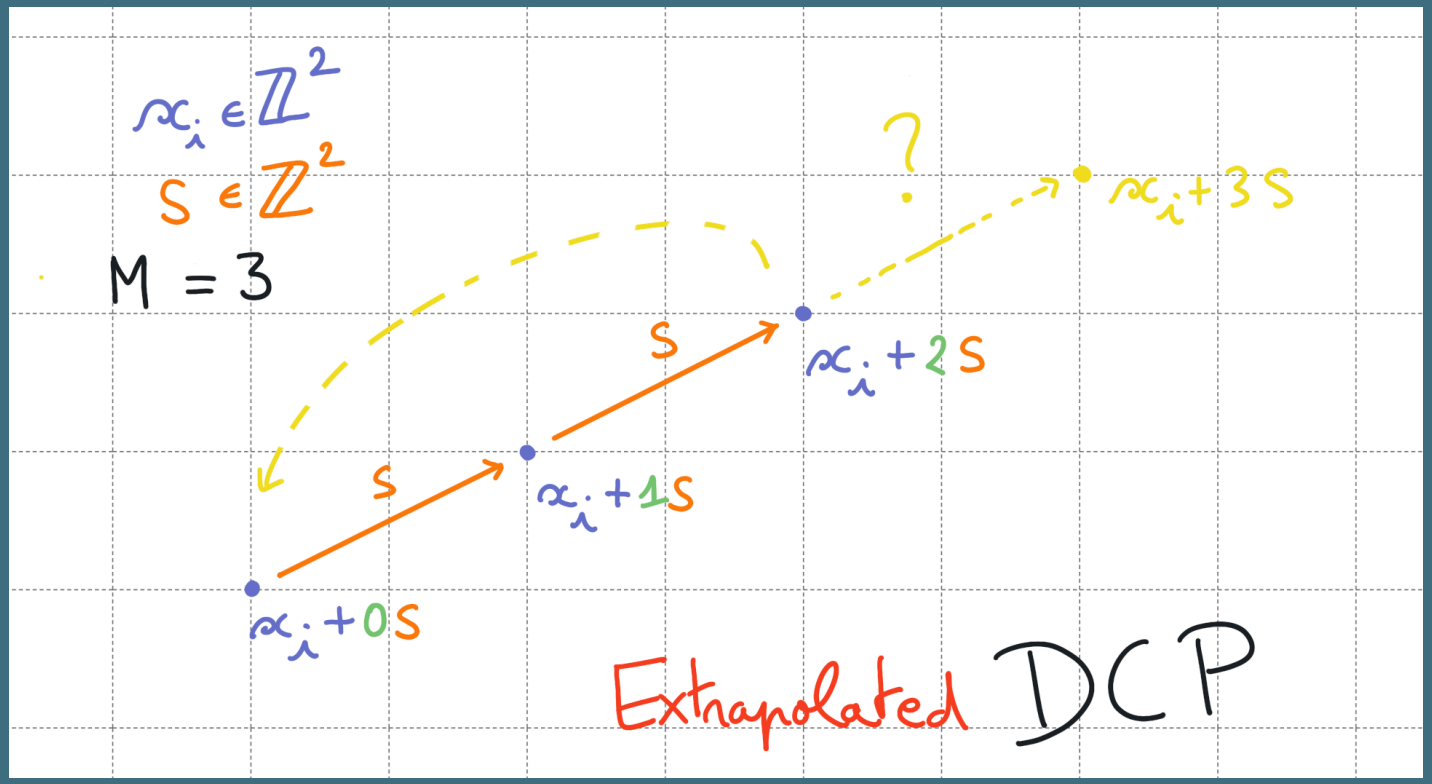
$$|\varphi_i\rangle = \frac{1}{\sqrt{2}}(|0, x_i\rangle + |1, x_i + s\rangle)$$



$$\frac{1}{\sqrt{M}} \sum_{j=1}^{M-1} |j\rangle |x_i + js\rangle$$



$$\frac{1}{\sqrt{M}} \sum_{j=1}^{M-1} |j\rangle |x_i + js\rangle$$



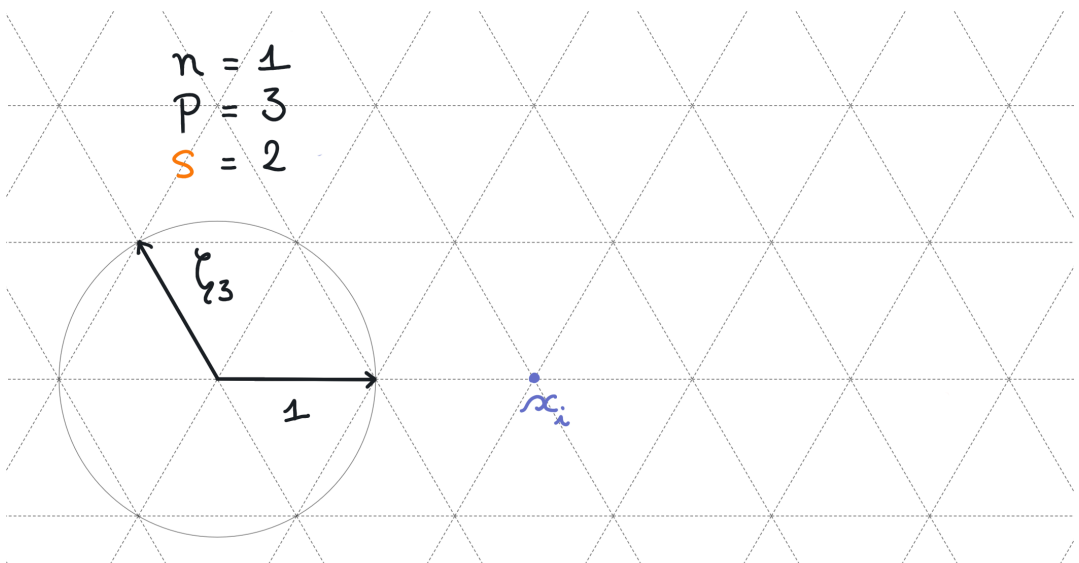
Introducing the Cyclotomic Coset Problem

Cyclotomic ring

Let q be a power of a prime p. Let ζ_p be a primitive p-th root of the unity. The **cyclotomic ring** corresponds to:

$$R = \mathbb{Z}\left[\zeta_p\right] \rightsquigarrow a_0 + a_1\zeta_p + \ldots + a_{p-2}\zeta_p^{p-2},$$

$$R_q = \mathbb{Z}_q\left[\zeta_p\right] \rightsquigarrow \overline{a}_0 + \overline{a}_1\zeta_p + \ldots + \overline{a}_{p-2}\zeta_p^{p-2}.$$



Cyclotomic group

Consider the **cyclotomic group**,

$$G = \mathbb{F}_p \rtimes_u R_q$$

Let $(j_1, s_1), (j_2, s_2) \in \mathbb{F}_p \times R_q$, the group law via G is,

$$(j_1, s_1) \odot (j_2, s_2) = \left(j_1 + j_2, s_1 + \zeta_p{}^{j_1} s_2\right).$$

Cyclic subgroups of order p

Let H cyclic generated by $(1, \boldsymbol{s}) \in G$:

- $(1, \boldsymbol{s})^{\odot 2} = (1, \boldsymbol{s}) \odot (1, \boldsymbol{s}) = \left(2, \left(1 + \zeta_p\right)\boldsymbol{s}\right)$,
- $(1, \boldsymbol{s})^{\odot j} = \left(j, \sum_{i=0}^{j-1} \zeta_p^i \cdot \boldsymbol{s}\right)$,
- $(1, \boldsymbol{s})^{\odot p} = \left(p, \sum_{i=0}^{p-1} \zeta_p^i \cdot \boldsymbol{s}\right) = (0, 0)$.

$$\hookrightarrow H = \left\{\left(j, \sum_{i=0}^{j} \zeta_p^i \cdot \boldsymbol{s}\right)\right\}$$

Cyclotomic Coset Problem

Let p be a prime, $q = p^t$ and ζ_p be a p-th root of the unity.

Coset Problem. Find the subgroup H of a group G given $|\varphi_x\rangle = \frac{1}{\sqrt{H}} \sum_{h \in H} |xh\rangle$.

Take $G = \mathbb{F}_p \rtimes_u R_q$ and $H = \langle (1, s) \rangle$.

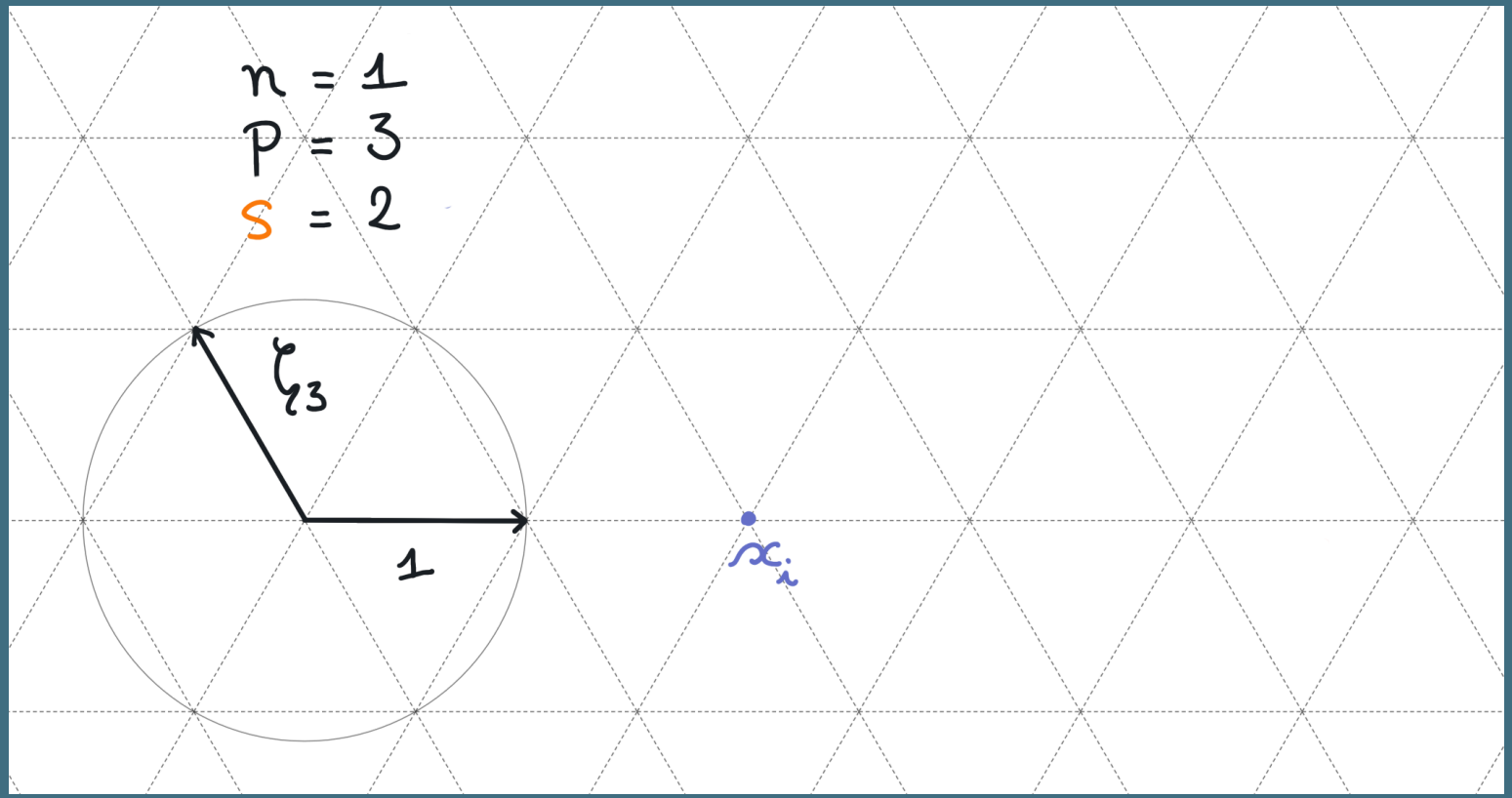
Cyclotomic Coset Problem (CCP)

Find the secret $s \in \mathbb{Z}_q^n$ given samples of the form,

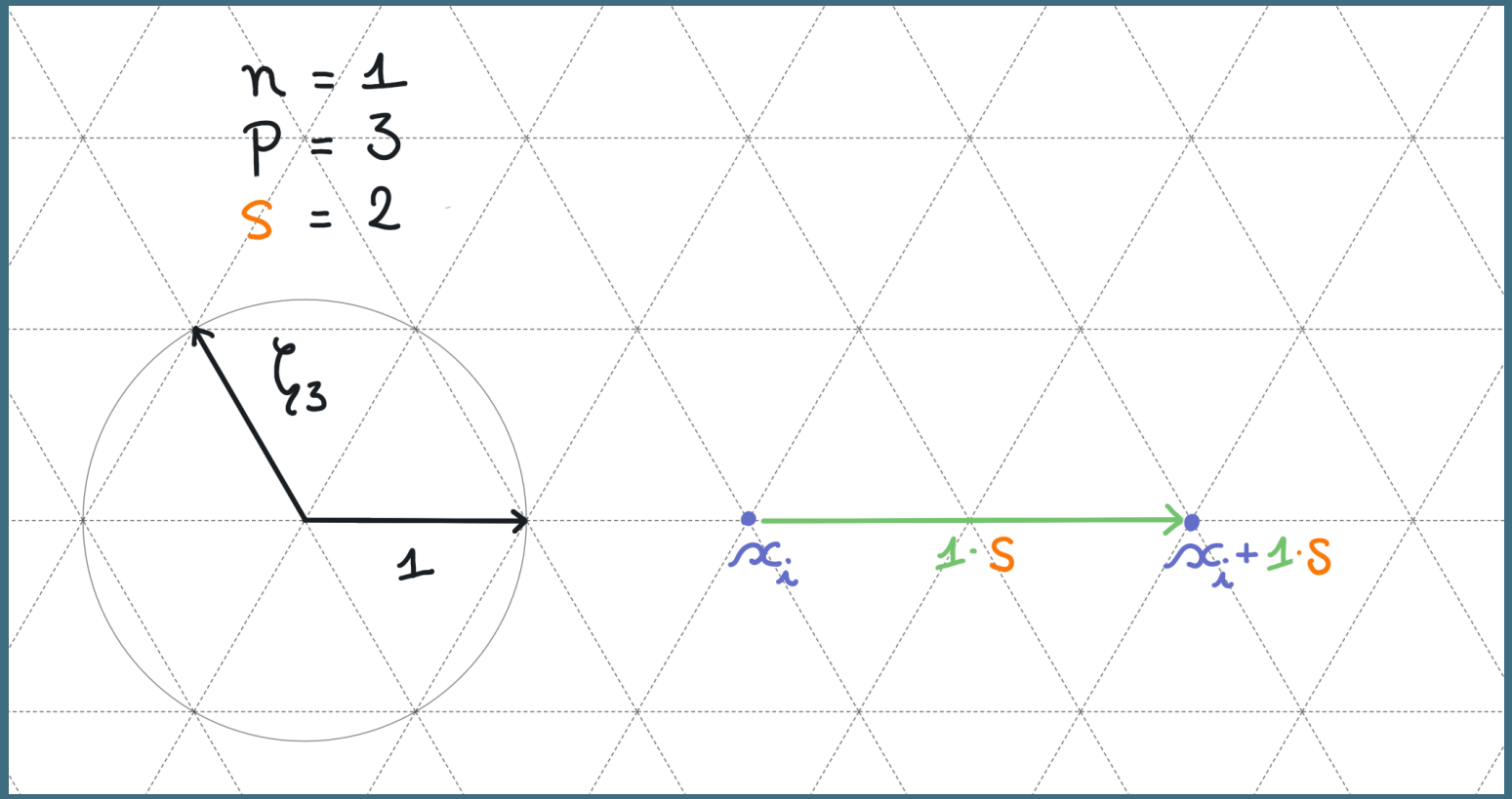
$$\frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} |j\rangle \left| x_i + \lambda_j s \right\rangle$$

with $x_i \in \mathcal{U}\left(R_q^n\right)$ and $\lambda_j = 1 + \zeta_p + \ldots + \zeta_p^{j-1}$.

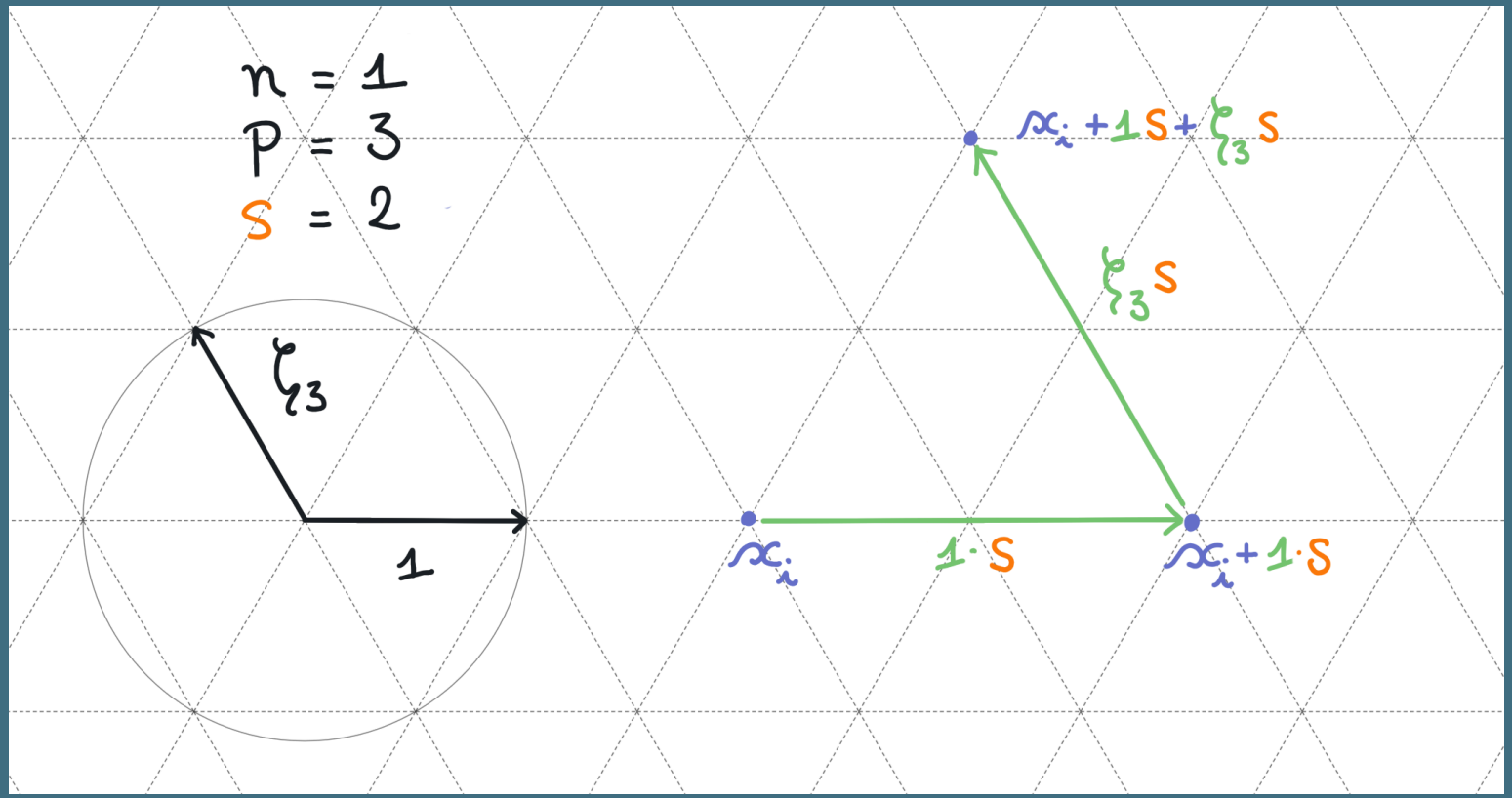
$$\frac{1}{\sqrt{M}} \sum_{j=1}^{M-1} |j\rangle \left| x_i + \sum_{i=0}^{j-1} \zeta_p^i \cdot s \right\rangle$$



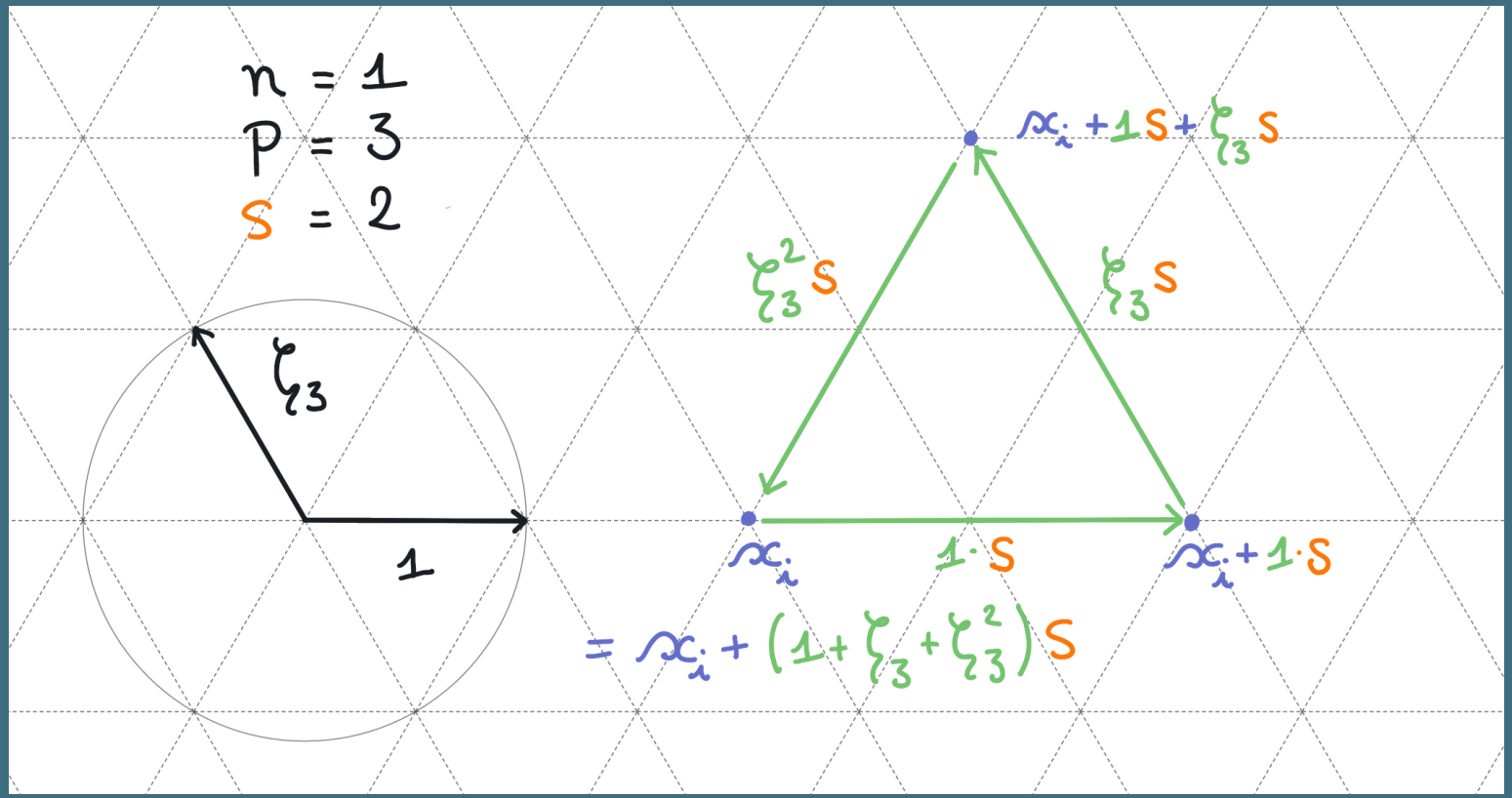
$$\frac{1}{\sqrt{M}} \sum_{j=1}^{M-1} |j\rangle \left| x_i + \sum_{i=0}^{j-1} \zeta_p^i \cdot s \right\rangle$$



$$\frac{1}{\sqrt{M}} \sum_{j=1}^{M-1} |j\rangle \left| x_i + \sum_{i=0}^{j-1} \zeta_p^i \cdot s \right\rangle$$



$$\frac{1}{\sqrt{M}} \sum_{j=1}^{M-1} |j\rangle \left| x_i + \sum_{i=0}^{j-1} \zeta_p^i \cdot s \right\rangle$$



Cyclotomic Coset Problem

	EDCP with $M \geq 3$	DCP with $q \neq 2^t$	DCP with $q = 2^t$	CCP with $q = p^t$
Coset Structure	× No	✓ Yes	✓ Yes	✓ Yes
Group nilpotent	× No	× No	✓ Yes	✓ Yes

Group nilpotent. It is a crucial group property asking a group to admit a particular decreasing chain of subgroups. (Its central series converges to the trivial group.)

Cyclotomic Coset Problem

	EDCP with $M \geq 3$	DCP with $q \neq 2^t$	DCP with $q = 2^t$	CCP with $q = p^t$
Coset Structure	× No	✓ Yes	✓ Yes	✓ Yes
Group nilpotent	× No	× No	✓ Yes	✓ Yes

Group nilpotent. It is a crucial group property asking a group to admit a particular decreasing chain of subgroups. (Its central series converges to the trivial group.)

Why do the group nilpotent property matters?

2024, Imran, Ivanyos, *Zero sum subsequences and hidden subgroups*.

"The consequence is a polynomial time exact quantum algorithm for the hidden subgroup problem in nilpotent groups having constant nilpotency class and whose order only have prime factors also bounded by a constant."

An algorithm for small prime-power moduli

Framework of most Kuperberg-style solvers DCP

Everything is in $\mathbb{Z}_q^n$ with $q = p^t$ and p prime.

1. Convert your DCP-states into a **phase-state** with current modulo q :

$$(\text{DCP state}) \quad \sum_j |j\rangle|x + js\rangle \rightsquigarrow \sum_j \exp\left(\frac{2i\pi}{q}\langle jy, s\rangle\right)|j\rangle \quad (\text{phase-state}),$$

   with $y \in \mathbb{Z}_q^n$ known.
   To do that you need the **Quantum Fourier Transform** unitary (i.e. a Discrete Fourier Transform over the kets).

Framework of most Kuperberg-style solvers DCP

Everything is in $\mathbb{Z}_q^n$ with $q = p^t$ and p prime.

1. Convert your DCP-states into a **phase-state** with current modulo q :

$$(\text{DCP state}) \quad \sum_j |j\rangle|x + js\rangle \rightsquigarrow \sum_j \exp\left(\frac{2i\pi}{q}\langle jy, s\rangle\right)|j\rangle \quad (\text{phase-state}),$$

   with $y \in \mathbb{Z}_q^n$ known.
   To do that you need the **Quantum Fourier Transform** unitary (i.e. a Discrete Fourier Transform over the kets).

2. **Modulo reduction step.** By considering this decreasing ring chain,

$$\mathbb{Z}_q = \mathbb{Z}_{p^t} \to \mathbb{Z}_{p^{t-1}} \to \ldots \to \mathbb{Z}_{p^2} \to \mathbb{Z}_p = \mathbb{F}_p,$$

   and using a bunch of phase-states involving a modulo p^i, try to construct one with modulo p^{i-1}.

   ☝ Keep your fingers crossed that no errors carry over from one iteration to the next ☝

3. When you get enough phase-states with **current modulo** p, it is easy to recover the secret.

Framework of most Kuperberg-style solvers DCP

Everything is in $\mathbb{Z}_q^n$ with $q = p^t$ and p prime.

1. Convert your DCP-states into a **phase-state** with current modulo q :

$$(\text{DCP state}) \quad \sum_j |j\rangle|x + js\rangle \rightsquigarrow \sum_j \exp\left(\frac{2i\pi}{q}\langle jy, s\rangle\right)|j\rangle \quad (\text{phase-state}),$$

   with $y \in \mathbb{Z}_q^n$ known.
   To do that you need the **Quantum Fourier Transform** unitary (i.e. a Discrete Fourier Transform over the kets).

2. **Modulo reduction step.** By considering this decreasing ring chain,

$$\mathbb{Z}_q = \mathbb{Z}_{p^t} \to \mathbb{Z}_{p^{t-1}} \to \ldots \to \mathbb{Z}_{p^2} \to \mathbb{Z}_p = \mathbb{F}_p,$$

   and using a bunch of phase-states involving a modulo p^i, try to construct one with modulo p^{i-1}.

   🤞 Keep your fingers crossed that no errors carry over from one iteration to the next 🤞

3. When you get enough phase-states with **current modulo** p, it is easy to recover the secret.

↳ **What does all this mean for CCP?**

Adaptation to a cyclotomic context

Group Theory $\rightarrow$ Number Theory

Fix $q = p^t$ with p a prime in $\mathbb{Z}$. Let ζ_p be the p-th primitive root of the unity, Φ_p be the p-th cyclotomic polynomial.

$$R_q = R/qR \rightsquigarrow \text{Quotient ring}$$

Important subtlety,

In R and R_q, p **is no longer prime!**

$$\Phi_p(X) = 1 + X + ... + X^{p-1} = \prod_{i=1}^{p-1}(X - \zeta_p^i)$$

$$p = \Phi_p(1) = \prod_{i=1}^{p-1}(1 - \zeta_p^i)$$

Adaptation to a cyclotomic context

Consequences

Fix $q = p^t$ with p a prime in $\mathbb{Z}$

- The ring integer $\pi = 1 - \zeta_p$ is prime and is such that $p \approx \pi^{p-1}$ (up to multiplication by a unit)
- Hence, $q \approx \pi^L$ with $L = t(p-1)$.
- $R_q = R/qR \approxeq R/\pi^L R$.

We can consider the decreasing ring chain: We have the following **decreasing ring chain**:

$$R_q \approxeq R/\pi^L R \to R/\pi^{L-1} R \to \ldots \to R/\pi R \approxeq \mathbb{F}_p$$

↳ more refined than if we had considered only the iterative powers of p.
↳ Directly related to the group-nilpotent property of $\mathbb{F}_p \rtimes R_q$.

Back to the DCP framework

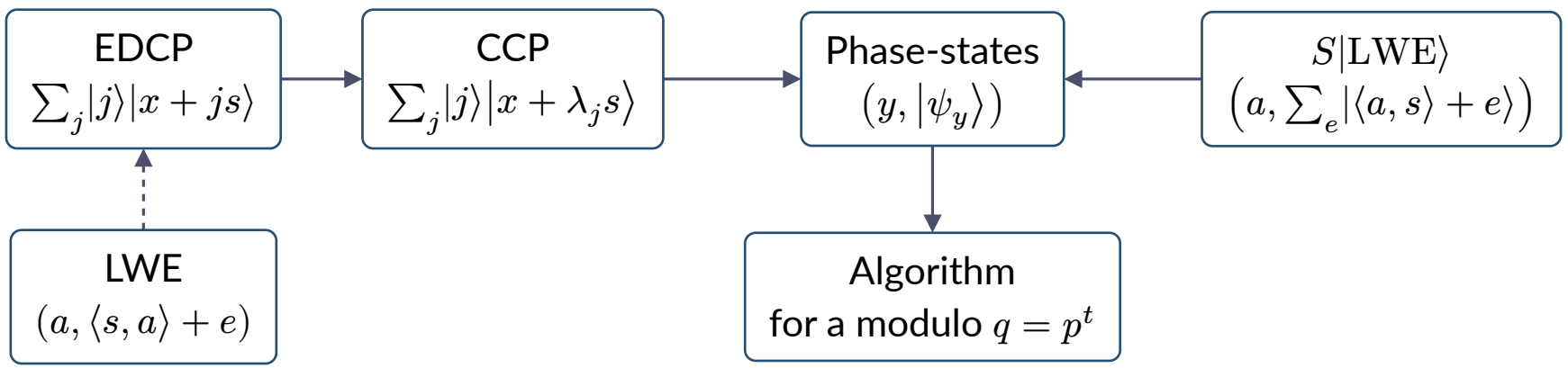
Resume. From DCP/CCP states to phase-states → modulo reduction step → finally recover the secret.

Structure	DCP	CCP
Ring	$\mathbb{Z}_q^n$	R_q^n
DCP/CCP state	$\sum_j \lvert j\rangle \lvert x + js\rangle$	$\sum_j \lvert j\rangle \lvert x + \lambda_j s\rangle$
QFT	$\mathrm{QFT}_{\mathbb{Z}_q^n}(\lvert x\rangle) = \sum_{y\in\mathbb{Z}_q^n} \exp\left(\frac{2i\pi}{q}\langle x, y\rangle\right)\lvert y\rangle$	$\mathrm{QFT}_{R_q^n}(\lvert x\rangle) = \sum_{y\in R_q^n} \chi_x(y)\lvert y\rangle$
Phase-state modulo q	$\sum_j \exp\left(\frac{2i\pi}{q}\langle jy, s\rangle\right)\lvert j\rangle, \quad y \in \mathbb{Z}_q^n$	$\sum_j \chi_s(\lambda_j y)\lvert j\rangle, \quad y \in R_q^n$
Decreasing ring chain	$\mathbb{Z}_{p^t} \to \mathbb{Z}_{p^{t-1}} \to \ldots \to \mathbb{Z}_p = \mathbb{F}_p$	$R/\pi^L R \to R/\pi^{L-1} R \to \ldots \to R/\pi R$

Complexity of the CCP solver algorithm:

- needs **quasi-polynomial** number of samples ;
- runs in **quasi-polynomial** time.

Impact on other problems



- 💡 The reduction from LWE to EDCP exists only for a polynomial number of samples.
- 🤩 We have surprisingly proven that DCP and CCP are equivalent when $q = p^t$.

Conclusion

Conclusion

The problem:

Quasi-polynomial-time algorithms for DCP only works when the modulo is $q = 2^t$.
Why? Any generalization?

We have:

- Understood that the **group structure** of the quantum samples matters.
- Introduced the **Cyclotomic Coset Problem** (CCP) which has a more regular structure.
- Proposed a **quasi-polynomial algorithm** for solving CCP.
- **Proved reductions** with other computational problems.

Conclusion

The problem:

Quasi-polynomial-time algorithms for DCP only works when the modulo is $q = 2^t$.
Why? Any generalization?

We have:

- Understood that the **group structure** of the quantum samples matters.
- Introduced the **Cyclotomic Coset Problem** (CCP) which has a more regular structure.
- Proposed a **quasi-polynomial algorithm** for solving CCP.
- **Proved reductions** with other computational problems.

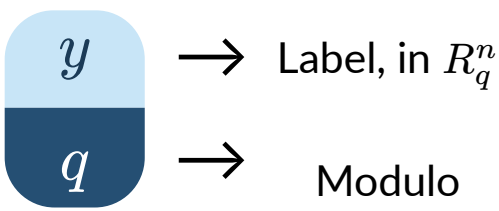
Thanks for your attention! Do you have any questions?

Appendix

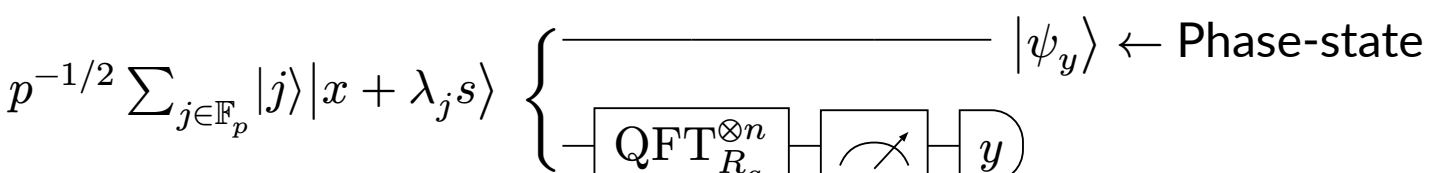
Description of the algorithm

- This is a state of the form:

$$|\psi_y\rangle = p^{-1/2} \sum_{j \in \mathbb{F}_p} \chi_s(\lambda_j y)|y\rangle, \quad y \in R_q^n.$$



- It is easy to construct a **phase-state** starting from a **cyclotomic state**:



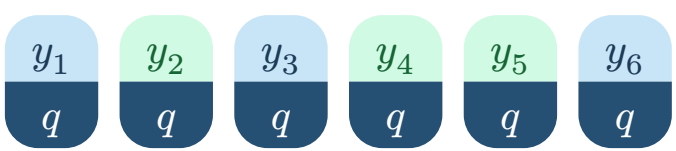
Description of the algorithm

- Fix $q = p^t$ and note $\pi = 1 - \zeta_p$. We have the following **decreasing ring chain**:

$$R_q = R/\pi^L R \to R/\pi^{L-1} R \to ... \to R/\pi R \approxeq \mathbb{F}_p,$$

  the procedure consists to repeatedly pass from a phase-state modulo π^i to π^{i-1}.

- **Modulo reduction step:**
  - Start with a list of phase-states samples modulo $q = \pi^L$. And Among the each labels y, extract a **zero subsequence**.



$$... \Rightarrow y_2 + y_4 + y_5 + ... = 0 \bmod \pi R$$

  - **Combine** each quantum states to obtain a new phase state with label with a modulo π^{L-1}.



$$, \quad y' = \pi^{-1} \sum_i y_i \zeta_p^{a_i}$$