A SUBEXPONENTIAL QUANTUM ALGORITHM FOR THE SEMIDIRECT DISCRETE LOGARITHM PROBLEM

Friday 14th June, 2024

Christopher Battarbee, Delaram Kahrobaei,
Ludovic Perret and Siamak F. Shahandashti

Historical Disclaimer

Comparison with Recent Work

Not this work[1,2]	This work
Reduction to quantum-easy problems	Reduction to quantum-hard-ish problem
Works for some finite groups but not for semigroups	Works for any finite semigroup

[1] Imran and Ivanyos 2023.
[2] Mendelsohn, Dable-Heath, and Ling 2023.

Timeline

SCIENCES SORBONNE UNIVERSITÉ

2014-2021: design/analysis of different versions of an SDLP-based cryptosystem[3]

↓

Summer 2022: this work, first dedicated analysis of SDLP

↓

Spring 2023: applications of techniques in this paper to DSS[4]

↓

Christmas 2023: faster SDLP methods in some finite groups[5]

---

[3] Habeeb, Kahrobaei, Koupparis, and Shpilrain 2014.

[4] B., Kahrobaei, Perret, and Shahandashti 2023.

[5] Imran and Ivanyos 2023; Mendelsohn, Dable-Heath, and Ling 2023.

SDLP

Definitions

Semidirect Product

Let G be a finite semigroup and $End(G)$ its semigroup of endomorphisms. We define $G \rtimes End(G)$ to be the semigroup of pairs in $G \times End(G)$ equipped with the following multiplication:

$$(g, \phi)(h, \psi) := (g\phi(h), \phi \circ \psi)$$

Definitions

SCIENCES SORBONNE UNIVERSITÉ

Semidirect Product

Let G be a finite semigroup and $End(G)$ its semigroup of endomorphisms. We define $G \rtimes End(G)$ to be the semigroup of pairs in $G \times End(G)$ equipped with the following multiplication:

$$(g, \phi)(h, \psi) := (g\phi(h), \phi \circ \psi)$$

Notice

$$(g, \phi)^2 = (g\phi(g), \phi^2)$$
$$(g, \phi)^3 = (g, \phi)(g\phi(g), \phi^2) = (g\phi(g)\phi^2(g), \phi^3)$$
$$(g, \phi)^4 = (g, \phi)(g\phi(g)\phi^2(g), \phi^3) = (g\phi(g)\phi^2(g)\phi^3(g), \phi^4)$$

Definitions

SCIENCES SORBONNE UNIVERSITÉ

Semidirect Exponentiation

Fix $(g, \phi) \in G \rtimes End(G)$. Define $s_{g,\phi} : \mathbb{N} \to G$ to be the group element such that

$$(g, \phi)^x = (s_{g,\phi}(x), \phi^x)$$

We have seen that

$$s_{g,\phi}(x) = g\phi(g)...\phi^{x-1}(g)$$

SDLP

Fix $G \rtimes End(G)$ and a pair (g, ϕ). Suppose we are given $s_{g,\phi}(x)$ for some $x \in \mathbb{N}$. The **S**emidirect **D**iscrete **L**ogarithm **P**roblem is to recover x.

Examples

SCIENCES SORBONNE UNIVERSITÉ

Let $G = M_3(\mathbb{Z}_3)$, $A = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix}$, $\phi_B(M) = BMB^{-1}$.

Then

Examples

SCIENCES SORBONNE UNIVERSITÉ

Let $G = M_3(\mathbb{Z}_3)$, $A = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix}$, $\phi_B(M) = BMB^{-1}$.

Then

$$s_{A,\phi_B}(2) = A\phi_B(A) = ABAB^{-1} = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Examples

Let $G = M_3(\mathbb{Z}_3)$, $A = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix}$, $\phi_B(M) = BMB^{-1}$.

Then

$$s_{A,\phi_B}(2) = A\phi_B(A) = ABAB^{-1} = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$s_{A,\phi_B}(3) = A\phi_B(A)\phi_B^2(A) = A(BAB^{-1})(B^2AB^{-2}) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Examples

Let $G = M_3(\mathbb{Z}_3)$, $A = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix}$, $\phi_B(M) = BMB^{-1}$.

Then

$$s_{A,\phi_B}(2) = A\phi_B(A) = ABAB^{-1} = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$s_{A,\phi_B}(3) = A\phi_B(A)\phi_B^2(A) = A(BAB^{-1})(B^2AB^{-2}) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$s_{A,\phi_B}(4) = A(BAB^{-1})(B^2AB^{-2})(B^3AB^{-3}) = \begin{pmatrix} 2 & 0 & 2 \\ 2 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

Examples

SCIENCES SORBONNE UNIVERSITÉ

Let $G = M_3(\mathbb{Z}_3)$, $A = \begin{pmatrix} 0 & 2 & 1 \\ 0 & 2 & 1 \\ 1 & 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \\ 0 & 0 & 2 \end{pmatrix}$, $\phi_B(M) = BMB^{-1}$.

Then

$$s_{A,\phi_B}(2) = A\phi_B(A) = ABAB^{-1} = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$s_{A,\phi_B}(3) = A\phi_B(A)\phi_B^2(A) = A(BAB^{-1})(B^2AB^{-2}) = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$s_{A,\phi_B}(4) = A(BAB^{-1})(B^2AB^{-2})(B^3AB^{-3}) = \begin{pmatrix} 2 & 0 & 2 \\ 2 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\ldots$$

$$s_{A,\phi_B}(10) = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} = s_{A,\phi_B}(2)$$

A Group Action

The $*$ Operator

SCIENCES SORBONNE UNIVERSITÉ

$$
\begin{aligned}
(s_{g,\phi}(x+y), \phi^{x+y}) = (g,\phi)^{x+y} &= (g,\phi)^x (g,\phi)^y \\
&= (s_{g,\phi}(x), \phi^x)(s_{g,\phi}(y), \phi^y) \\
&= (s_{g,\phi}(x)\phi^x(s_{g,\phi}(y)), \phi^{x+y})
\end{aligned}
$$

so $s_{g,\phi}(x + y) = s_{g,\phi}(x)\phi^x(s_{g,\phi}(y))$. We can add in the argument of $s_{g,\phi}$.

The $*$ Operator

SCIENCES SORBONNE UNIVERSITÉ

$$\begin{aligned}(s_{g,\phi}(x+y), \phi^{x+y}) = (g,\phi)^{x+y} &= (g,\phi)^x (g,\phi)^y \\ &= (s_{g,\phi}(x), \phi^x)(s_{g,\phi}(y), \phi^y) \\ &= (s_{g,\phi}(x)\phi^x(s_{g,\phi}(y)), \phi^{x+y})\end{aligned}$$

so $s_{g,\phi}(x+y) = s_{g,\phi}(x)\phi^x(s_{g,\phi}(y))$. We can add in the argument of $s_{g,\phi}$.

$*$

Let $\mathcal{X}_{g,\phi} = \{s_{g,\phi}(i) : i \in \mathbb{N}\}$, and define $* : \mathbb{N} \times \mathcal{X}_{g,\phi} \to \mathcal{X}_{g,\phi}$ by

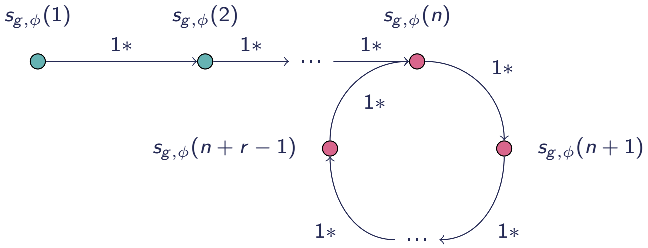
$$x * s_{g,\phi}(y) = s_{g,\phi}(x)\phi^x(s_{g,\phi}(y))$$

We have $x * s_{g,\phi}(y) = s_{g,\phi}(x+y)$.

Shape of $\mathcal{X}_{g,\phi}$

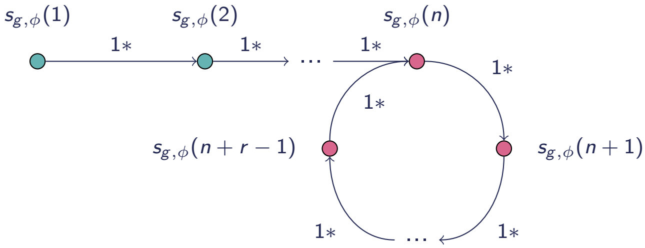
SCIENCES SORBONNE UNIVERSITÉ

Set $\mathcal{X}_{g,\phi} = \{s_{g,\phi}(i) : i \in \mathbb{N}\}$.



Shape of $\mathcal{X}_{g,\phi}$

Set $\mathcal{X}_{g,\phi} = \{s_{g,\phi}(i) : i \in \mathbb{N}\}$.



Terminology

We call n the **index**, r the **period**, $\{g, ..., s_{g,\phi}(n-1)\}$ the **tail**, and $\{s_{g,\phi}(n), ..., s_{g,\phi}(n+r-1)\}$ the **cycle**.

Definitions

SCIENCES SORBONNE UNIVERSITÉ

Finite Group Action

Let G be a finite group, X be a finite set and $*$ be a function $* : G \times X \to X$. The tuple $(G, X, *)$ is a **group action** if

$$1_G * x = x \text{ for each } x \in X$$

$$(gh) * x = g * (h * x) \text{ for each } g, h \in G,\ x \in X$$

Vectorisation[6]/Group Action DLog

Let $(G, X, *)$ be a group action. Given $x, y \in X$, the **vectorisation problem** is to find a g (if one exists) such that $g * x = y$.

[6] Couveignes 2006.

Contributions

SCIENCES SORBONNE UNIVERSITÉ

Theorem [B., Kahrobaei, Perret, Shahandashti]

Let G be a finite semigroup and consider the semigroup $G \rtimes End(G)$. Fix a pair $(g, \phi) \in G \rtimes End(G)$, and let $\mathcal{C}_{g,\phi}$ denote the corresponding cycle. The tuple $(\mathbb{Z}_r, \mathcal{C}_{g,\phi}, \circledast)$ is a free, transitive group action, where r, the period associated to (g, ϕ), is $|\mathcal{C}_{g,\phi}|$.

Contributions

Theorem [B., Kahrobaei, Perret, Shahandashti]

Let G be a finite semigroup and consider the semigroup $G \rtimes End(G)$. Fix a pair $(g, \phi) \in G \rtimes End(G)$, and let $\mathcal{C}_{g,\phi}$ denote the corresponding cycle. The tuple $(\mathbb{Z}_r, \mathcal{C}_{g,\phi}, \circledast)$ is a free, transitive group action, where r, the period associated to (g, ϕ), is $|\mathcal{C}_{g,\phi}|$.

Theorem [B., Kahrobaei, Perret, Shahandashti]

There is a fast quantum reduction from SDLP w.r.t (g, ϕ) to a vectorisation problem, and therefore quantum algorithms for SDLP of quantum complexity $2^{\mathcal{O}(\sqrt{\log r})}$, where r is the period associated to (g, ϕ).

The Reduction

Background

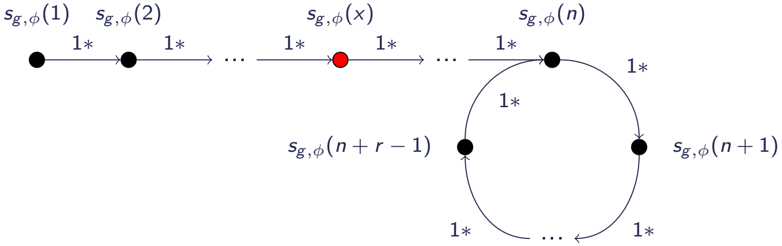
Well-known that the Vectorisation Problem reduces to dihedral hidden subgroup problem.[7]

Dihedral hidden subgroup problem admits (a) quantum algorithm with complexity $2^{\mathcal{O}(\sqrt{\log n})}$ for D_{2n}.[8]

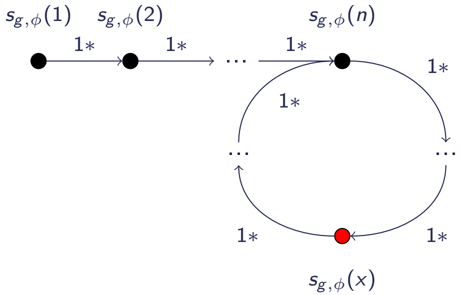
Reduction of Semigroup DLog to a DLog problem has to address a similar structure to us.[9]

[7] Childs, Jao, and Soukharev 2014.
[8] Kuperberg 2005.
[9] Childs and Ivanyos 2014.

Scenario 1: $x < n$



Scenario 2: $x \geq n$



Roadmap Given n, r

Suppose we are given n, r.

Roadmap Given n, r

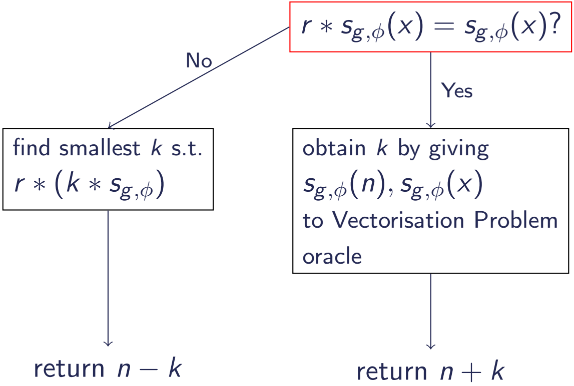
SCIENCES SORBONNE UNIVERSITÉ

Suppose we are given n, r.
Notice that $r * s_{g,\phi}(x) = s_{g,\phi}(x) \iff s_{g,\phi}(x) \in \mathcal{C}_{g,\phi}$

Roadmap Given n, r

SCIENCES SORBONNE UNIVERSITÉ

Suppose we are given n, r.
Notice that $r * s_{g,\phi}(x) = s_{g,\phi}(x) \iff s_{g,\phi}(x) \in \mathcal{C}_{g,\phi}$

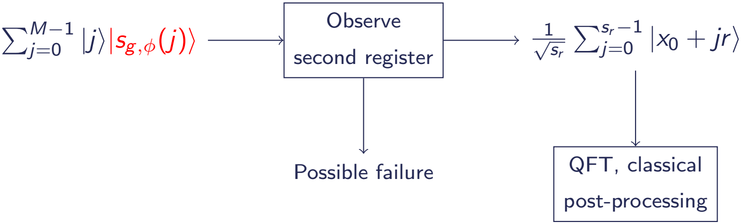


Computing n, r

Given r compute n as the smallest integer such that $r * s_{g,\phi}(n) = s_{g,\phi}(n)$.

Computing n, r

Given r compute n as the smallest integer such that $r * s_{g,\phi}(n) = s_{g,\phi}(n)$.



Conclusions

Takeaways and Open Problems

SCIENCES SORBONNE UNIVERSITÉ

One can solve SDLP for (g, ϕ) in quantum time $2^{\mathcal{O}(\sqrt{\log r})}$ where r is a function of g, ϕ - not much known about its size.

In the generic case this remains state-of-the-art; possible that specific semigroups would yield faster results

Fast classical methods of computing n, r might give us interesting crypto.

Further Reading

Fast SDLP now resolved for *all** finite groups.

https://eprint.iacr.org/2024/905

More on group-based cryptography:

http://aimpl.org/postquantgroup/ .

*up to constructive recognition.