

# OptTrot

## Optimized Trotter Circuit Library

Hyunseong Kim  
GIST, qwqwhsnote@gm.gist.ac.kr

**Memebbers**  
Hyunseong Kim  
Hanseo Kim  
Gaya Yun

**Mentor**  
Sayonee Ray

### Abstract

OptTrot is a library of generating optimized Trotter circuit for a given hamiltonian. Trotterization is a standard way to accomplish time evolution circuit on gate model computer, however, their long depth circuit has significantly contributed to the hurdle of practical application. In the library, we combined commuting partition method and Pauli Frame search method. If the given Pauli term mutually commuted with Pauli Frame axis, then the Clifford gate combination was reduced to combinations of CX gate. Moreover, their specific decomposition is easily derived from Gauss elimination of matrix over module 2 field,  $\mathbb{Z}/2\mathbb{Z}$ . In the library, the overall process are easily achieved by convenience interfaces. Furthermore, researchers could combine the library with various optimization tools from classic to quantum methods for partitioning of Pauli terms.

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Commuting Partition for Optimization</b>	<b>3</b>
2.1	Trotter Error by applying order . . . . .	3
<b>3</b>	<b>Optimizing a circuit over commuting Pauli set</b>	<b>5</b>
3.1	Standard Trotterization . . . . .	5
3.2	Pauli Frame method . . . . .	6
3.3	Symplectic representation of Pauli elements . . . . .	9
3.4	Clifford transformation over commuting cliques . . . . .	9
3.4.1	Over IZ family . . . . .	9
3.4.2	General Commuting set . . . . .	11
3.5	Summary of Clifford operator search process . . . . .	14
<b>4</b>	<b>Expansion to general frames</b>	<b>14</b>
4.1	Qubit-wise Pauli frame . . . . .	14
4.1.1	QPF under Clifford transformation . . . . .	15
4.1.2	Pauli frame construction . . . . .	15
<b>5</b>	<b>Mutually Commuting Partition</b>	<b>16</b>
5.1	Solve clique problem on Quantum computer . . . . .	16

# 1 Introduction

Aim of the report is to introduce about theoretical backgrounds of OptTrot library. Why the library was developed, and how we can optimize the circuit for time evolution with Trotterization method. In OptTrot, many optimization techniques were used to design and implement the library. Each part and structure are significantly important to accomplish the object of the library, but the core part is a circuit synthesis algorithm.

Trotterization is a standard method used to implement a time evolution operator by combining several local hamiltonian evolution operators. By using the method, we can expect the approximated operator closed to the original operator, even the local terms did not commute with each other with quadratic,  $O(t^2)$ , error, and better bounds with higher order approximations[1].

$$\lim_{n \rightarrow \infty} (e^{A/2} e^{B/2})^n = e^{A+B} \quad (1)$$

However, standard Trotterization method increases circuit depth with linear order by number of Pauli terms. That is, a hamiltonian whose number of local terms are  $N$  has, at least,  $N$  time deeper circuit than single Pauli term evolution circuit. If the time evolution was an ultimate goal to achieve in quantum circuit, it could be meaningful, but in the most algorithms and applications, time evolution is just a part of the whole process. Thus, reducing techniques are significant to apply the quantum computer to general applications. In addition, increased circuit depth for reducing Trotter error yields impractical errors on NISQ, which caused by gate fidelity between ideal and implemented gates. By the limitation, there have been studied many alternative methods, to implement a time evolution operator with shorter depth circuit than Trotterization, such as linear combination of unitary(LCU) method[2], Qubitization[3], Taylorization[4], and Fractional query[5]. Such methods make the evolution circuit more practical, however, they loose identity of the given system, especially the cases, when the given hamiltonian is nearly commute or local observable was a dominant feature[6]. Only problem is a high cost of the Trotterization circuit. However, there is an unwarranted problem of Trotterization. A problem is circuit synthesis process of standard method[7] is often misinterpreted as a problem of Trotterization.

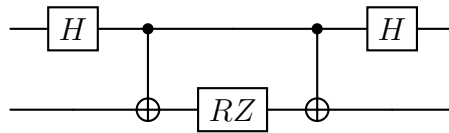


Figure 1: Example of trotter evolution circuit. Where  $H = X \otimes Z$

How can we optimize the circuit synthesis for trotter evolution circuit? There have been various studies of circuit optimization[8, 9] but in here, the report is focusing especially for trotter circuit implementation.

Schmitz et al would be a milestone paper[10] for the implementation. They analyzed what term would be rotated when we apply entanglement gates on quantum circuit using Pauli Frame, and suggested a practical method to find a better depth evolution circuit



of given hamiltonian. However, the paper has some limitations in frame search methods, which is not practical for rapidly generating various hamiltonian circuits. In the library, we combine the tools with commuting partitioning method. Especially, we will focus on an attempt that author Kim's study[11], using commuting pair to reduce the circuit depth.

This report consists of 5 parts,

1. Commuting partition effect on Trotter error.
2. Pauli Frame method and their limitation.
3. Pauli Frame method on mutually commuting partition.
4. Pauli Frame method on general frames.
5. Construction of mutually commuting partition.

## 2 Commuting Partition for Optimization

When hamiltonian is given, first thing to do is decomposing into combination of Pauli elements.

$$H \rightarrow \sum_i \lambda_i P_i \quad (2)$$

The decomposed Pauli terms are used for not only time-evolution but also measurement of the hamiltonian. In circuit optimization, the commuting partition provides more convenience properties for manipulation.

### 2.1 Trotter Error by applying order

It is well known that the exponential mapping error is represented with Baker Campbell Hausdorff formula. Usually, the formula is not written with commutator form, Childs et al proved that the error term as a function of sequential commutator of local terms[6].

$$O(\alpha t^2) \quad (3)$$

The result theorem of Childs et al allow us to calculate the error boundary more precisely including a physical structure of the given hamiltonian. Furthermore, the applying order effect of  $\exp(-itH_L)$ ,  $H = \sum_L H_L$  is well derived from the theorem.

**Theorem 1.** *Let  $H = \sum_i^N H_i$  be an operator consisting of  $N$  sum of local hamiltonian, and  $t \geq 0$ . Let  $S(t) = \prod_{k=1}^M \prod_{l=1}^N \exp(ta_{kl} H_{\pi_k(l)})$  be a  $p$ -th order Suzuki Trotter formula, then it's error term is asymptotically bounded by*

$$O(\alpha_{com} t^{p+1} \exp(4tM \sum_{l=1}^N ||H_l||)) \quad (4)$$

where,  $\alpha_{com} = \sum_{l_1, l_2, \dots, l_{p+1}}^N ||[H_{l_{p+1}}, \dots [H_{l_2}, H_{l_1}]]||$



For example, let a given hamiltonian was  $H = c_i P_i + c_j P_j$ .

$$\exp(-it(c_i)P_i) \exp(-it(c_j)P_j) = \exp(-it(c_i P_i + c_j P_j)) + O(\alpha_{com} t^2) \quad (5)$$

$$\text{then, the leading coefficient becomes } \alpha_{com} = \begin{cases} c_i + c_j & \text{if } [P_i, P_j] = 0 \\ c_i - c_j & \text{if } [P_i, P_j] \neq 0 \end{cases}.$$

It is affected by coefficients, their size, and sign, and commutation property. In the above example, we cannot observe the commutation and anti-commutation effect, since, if they were commuting to each other, the  $O(\alpha_{com} t^2) = 0$ . Let us expand the system to more general case. Suppose that the given hamiltonian has two representations,

$$H = H_1 + H_2 + H_3 \quad (6)$$

$$H = c_1 P_1 + c_2 P_2 + c_3 P_3 + c_4 P_4 + c_5 P_5 \quad (7)$$

$$H_1 = c_1 P_1 + c_3 P_3 \quad (8)$$

$$H_2 = c_2 P_2 \quad (9)$$

$$H_3 = c_4 P_4 + c_5 P_5 \quad (10)$$

where,  $[H_i, H_j] \neq 0$ , and  $[P_k, P_l] \neq 0$  if  $P_k \in H_i, P_l \in H_j, i \neq j$ .

$$\Pi_{l=1}^5 \exp(-it(c_l P_l)) = \exp(-itH) + O(\alpha_{com1} t^2) \quad (11)$$

$$\Pi_{k=1}^3 \exp(-it(H_k)) = \exp(-itH) + O(\alpha_{com2} t^2) \quad (12)$$

Following the  $q = 1$  order expansion, then in the first order, the bound error coefficients are reduced to

$$\alpha_{com1} = 2(|c_1 c_2 [P_1, P_2]| + |c_1 c_4 [P_1, P_4]| + |c_1 c_5 [P_1, P_5]|) \quad (13)$$

$$+ |c_2 c_3 [P_2, P_3]| + |c_2 c_4 [P_2, P_4]| + |c_2 c_5 [P_2, P_5]| \quad (14)$$

$$+ |c_3 c_4 [P_3, P_4]| + |c_3 c_5 [P_3, P_5]| \quad (15)$$

$$\alpha_{com2} = 2(|[H_1, H_2]| + |[H_1, H_3]| + |[H_2, H_3]|) \quad (16)$$

$$0.5\alpha_{com1} = |c_1 c_2| + |c_3 c_2| + |c_1 c_4| + |c_2 c_4| + |c_1 c_5| + |c_2 c_5| + |c_2 c_4| + |c_2 c_5| \quad (17)$$

$$0.5\alpha_{com2} = |c_1 c_2 + c_3 c_2| + |c_1 c_4 + c_2 c_4 + c_1 c_5 + c_2 c_5| + |c_2 c_4 + c_2 c_5| \quad (18)$$

Therefore, by the distribution of  $\{c_i\}$  and commutation relationship of the local terms, the constructed error rate vary. However, Eq(12) is just a re-ordering of Eq(11), since

$$\exp(-it(H_1)) = \exp(-it(c_1 P_1)) \exp(-it(c_3 P_3)) \quad (19)$$

$$\exp(-it(H_2)) = \exp(-it(c_2 P_2)) \quad (20)$$

$$\exp(-it(H_3)) = \exp(-it(c_4 P_4)) \exp(-it(c_5 P_5)) \quad (21)$$

$$(22)$$

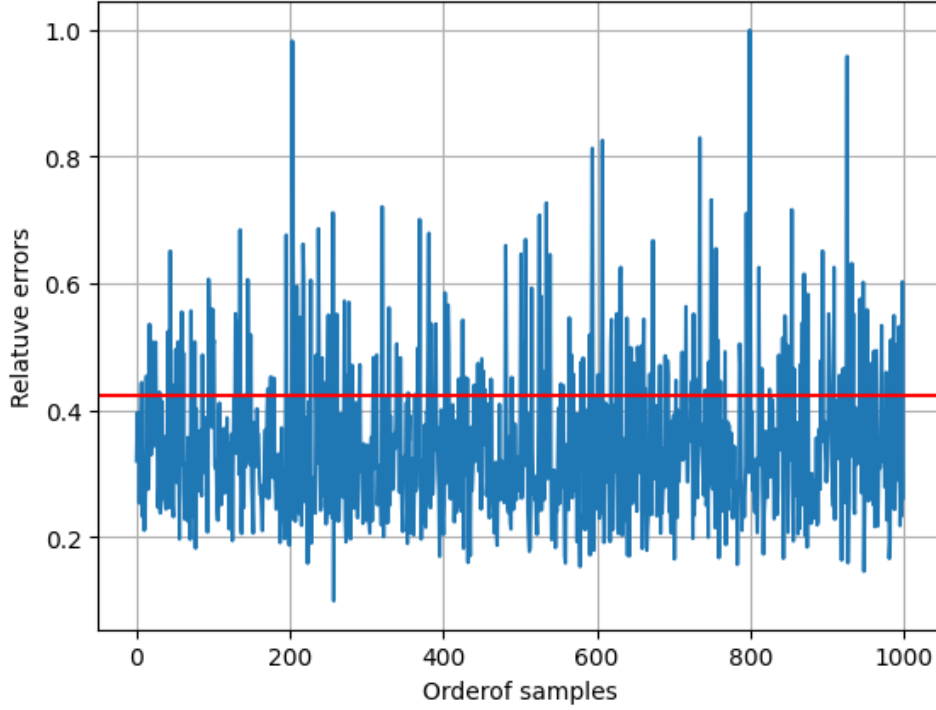


Figure 2: Relative error rate of random Hamiltonian,  $H$ . The red horizontal line is a largest local Hamiltonian decomposition and the each sample are random order of  $\exp(-itP_l)$ .

This is not at all, local Hamiltonian consists of mutually commuting Pauli terms provides us a lot of freedom to optimize the circuit. Whatever we switch and reorder the Pauli terms in the applying trotter circuit, if the larger structure,  $\exp(-itH_j) = \Pi_k \exp(-itc_{jk}P_{jk})$ , was preserved then, the trotter error would be bounded while we reduce the number of gates in the implementation. Thus, we don't have to choose one between trotter error and large gate error to optimize the evolution circuit.

**Note:** The partitioning the hamiltonian into large local terms does not yield the optimized order in every situation. The term  $\alpha$  only indicates upper bound of the error. So, the minimum trotter error could be worse than the arbitrary applying case. In here, the main focus is reducing errors associated with gate operations by using minimum number of gates. See, Fig 2.

### 3 Optimizing a circuit over commuting Pauli set

#### 3.1 Standard Trotterization

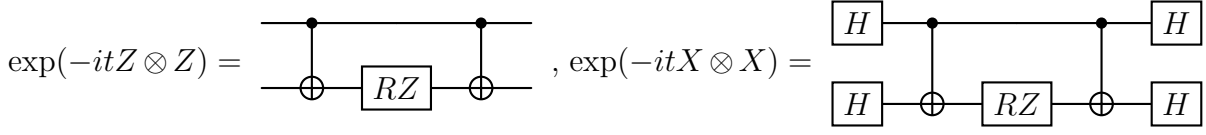
A standard method to implement time evolution of hamitonian  $H$  requires next steps.

1. If  $H$  was given as a hermit matrix, decompose the hamiltonian as Pauli elements.  

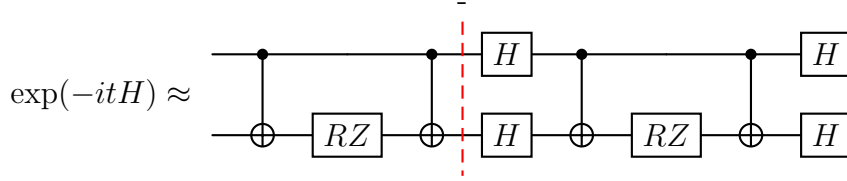
$$H \rightarrow \sum_i \lambda_i P_i.$$
2. Construct an evolution circuit on quantum circuit for each Pauli element.
3. Concatenate circuits to approximate the  $\exp(-itH/n) \approx \Pi_i \exp(-it\lambda P_i/n)$ .

4. Repeat the result circuit of 3rd to reach  $\exp(-itH) = \Pi_k^n \exp(-itH/n)$ .

For example, let the given hamiltonian as  $H = ZZ + XX$ . It is a 2 qubit system, and evolution circuits for each term are [7]



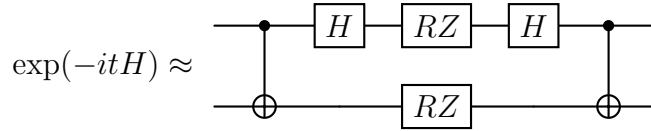
We can approximate the  $\exp(-itH)$  as next circuit,



If the required precision was higher than the above circuit, then using Eq (1) we can raise the precision of the implementation. The method requires total circuit depth as  $M$  times of single Pauli term circuit, when the given hamiltonian consists of  $M$  number of Pauli terms.

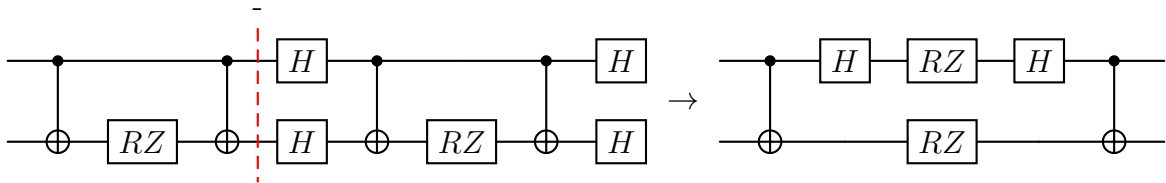
### 3.2 Pauli Frame method

A question arises as *when we apply some rotation gate on the empty wire of single Pauli evolution circuit, what hamiltonian would be accomplished?* More precisely, the next circuit is a modified  $\exp(-itZ \otimes Z)$  operator.



$$H = ZZ + P_{unknown}$$

What is a  $P_{unknown}$ ? The answer is  $XX$ . We can reduce the sequential Trotterized circuit by the properties of Pauli terms.



Recall that the physical meaning of commutation,  $[P_i, P_j]$ . Any two Pauli elements  $P_i, P_j$ , if they satisfy  $[P_i, P_j] = 0$ . It means we can manipulate  $P_i$  observable without affecting to  $P_j$  observable. In circuit aspect, the meaning is more direct. We can prepare a circuit state which rotation gates act as an evolution operator of each Pauli element, simultaneously. Therefore, commuting set of Pauli elements provides good properties to optimize Trotterized circuit. One method to accomplish the method is using *Pauli Frame* representation of the circuit[10]. Pauli Frame is a collection of Pauli terms indicating axes on each quantum circuit wires when we apply Rotation Z gate on the circuit.

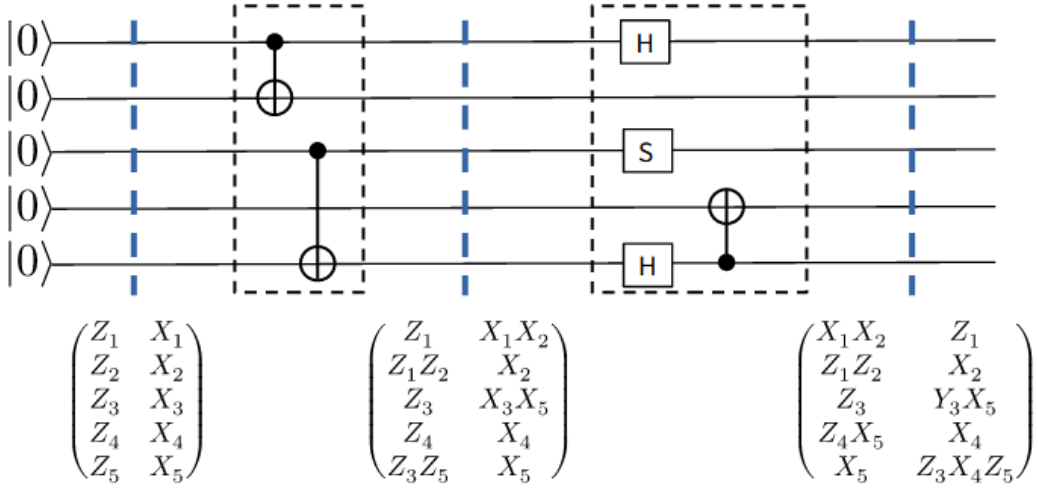


Figure 3: Example of Pauli Frame analysis of a quantum circuit. The dashed blue lines are corresponded to the below Pauli Frame. If we apply RZ gate on 5th qubit after we applied two CX gates, then the rotation gate is corresponding to  $\exp(-itZ_3Z_5)$ .

**Definition 1.** *Pauli frame*

For  $N$  qubit system, Pauli Frame is a collection of  $2N$  number of generalized Pauli elements,  $B = (\{s_i\}_{i=1}^N, \{\tilde{s}_i\}_{i=1}^N), \forall i, s_i, \tilde{s}_i \in \mathcal{P}$ , satisfying the next conditions.

1.  $[s_i, s_j] = 0 \forall i, j \in [N]$
2.  $[s_i, \tilde{s}_i] \neq 0 \forall i \in [N]$
3.  $[s_i, \tilde{s}_j] = 0 \forall i \neq j$

$$B = \begin{bmatrix} s_1 & , & \tilde{s}_1 \\ s_2 & , & \tilde{s}_2 \\ \vdots & , & \vdots \\ s_N & , & \tilde{s}_N \end{bmatrix}$$

$\{s_i\}$  is called by stabilizer, and  $\{\tilde{s}_i\}$  is called by destabilizer.

The Clifford gates act as a transformation of one frame to another frame. That is the frame structure is closed under Clifford gates. The closeness and detailed properties were proved in the original paper[10]. Description for all detail is not wise but, the operation of basic Clifford gates  $[CX, H, S]$  is worth to note here.

$$CX_{ij} = \begin{cases} s_j = s_i + s_j \\ \tilde{s}_i = \tilde{s}_i + \tilde{s}_j \end{cases}, H_i = \begin{cases} s_i = \tilde{s}_i \\ \tilde{s}_i = s_i \end{cases}, S_i = \begin{cases} \tilde{s}_i = s_i + \tilde{s}_i \\ S_i^\dagger = \begin{cases} \tilde{s}_i = \tilde{s}_i + s_i \end{cases} \end{cases} \quad (23)$$

Using the method, we can chase what Pauli elements were applied, and what elements we can rotate on the circuit. Fig 3 is an example of chasing Pauli terms on the circuit.

Furthermore, if we analyze two evolution circuits of  $H = ZZ + XX$  hamiltonian, with Pauli frame method, then the gates are classified as Fig 4, 5. Comparing the two figures, we can observe a *frame path*,

1.  $B_0 \rightarrow B_1 \rightarrow B_2 \rightarrow B_0$
2.  $B_0 \rightarrow B_3 \rightarrow B_0$

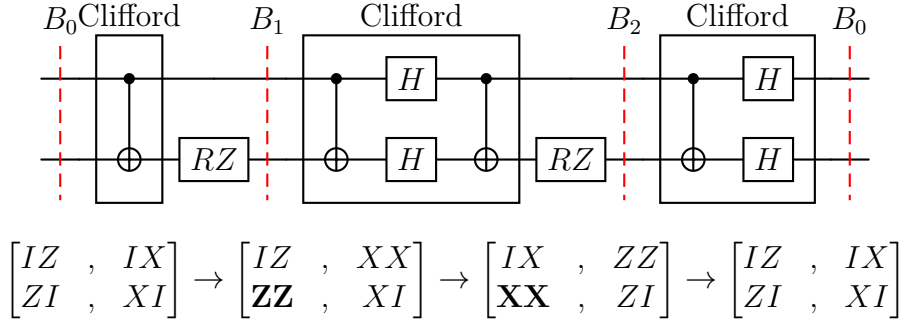


Figure 4: Pauli frame analysis of standard Trotterized circuit of  $H = ZZ + XX$ .

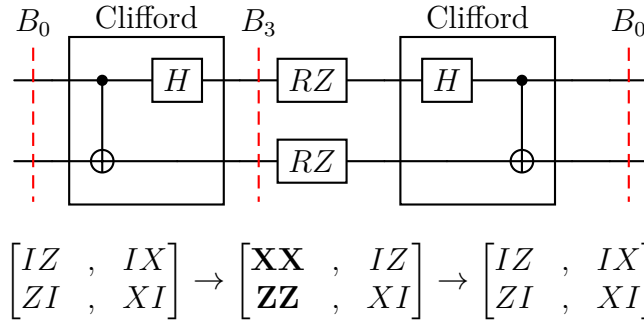


Figure 5: Pauli frame analysis of optimized Trotterized circuit of  $H = ZZ + XX$ .

The optimization direction is clear now.

**Proposiiton 1.** For given  $H$  consists of  $M$  number of Pauli terms, find a sequence of Pauli frames  $\{B_i\}_{i=1}^N$  minimizing number of Clifford operation to take the path defined by the sequence.

The original paper formulated the problem with *relative support* as measure[10]. With the measure, we can find a minimum entanglement gates to change to frame to rotate a new Pauli element. However, the problem was identified as Traversal purchaser problem(TPP)[10]. It is a well-known NP-hard problem so the authors did not directly solve the TPP problem. Meanwhile, they adopted a dynamic programming method to find a proper frame path. Their method did not use a set of specific frames and distances between the set. There are two major reasons. To calculate a distance between two frames,  $B_i, B_j$ , we have to know all Frame information before we calculate. However, what frames would be sufficient set to represent an optimized Trotter path for the hamiltonian? We cannot know the solution of such problem when arbitrary hamiltonian was





given. The only thing we have is a set of Pauli elements given by the hamiltonian. Moreover, when two frames were given,  $B_i, B_j$ , what do Clifford gates yield a transformation from  $B_i$  to  $B_j$ ?

$$B_i \rightarrow_{\text{Clifford}} B_j$$

There was no solid process to make the transformation with optimized number of basic gates. The questions are still remained from Schmitz et al paper. Even though the restrictions, their dynamic programming method was practically enough, to generate optimized low-order Suzuki Trotterized circuit for the given hamiltonian[10].

In the report, the author followed Schmitz et al perspective in the problem, however, the direction of solution would be different. We can construct a required Clifford transformation consists of  $\{CX, H, S\}$  gates.

### 3.3 Symplectic representation of Pauli elements

It is natural that the Pauli group is a kind of Clifford group of  $Cl_{2,0}$ , where two elements could generate all elements.

### 3.4 Clifford transformation over commuting cliques

#### 3.4.1 Over IZ family

$I, Z$  family would be a good example to see the process of gate construction over mutually commuting Pauli set. Consider that the local term of the hamiltonian are composite of  $I, Z$  tensor product. Then, for a given frame  $B$  and suppose that we have to make next frame to have  $P = IIZZ$ . Since, we don't have to consider terms containing  $X, Y$ , we can simply write the term as single stabilizer of the Frame, and the required entanglement gate is  $CX$  gate only.

$$B = \begin{bmatrix} ZZZI \\ ZZIZ \\ ZIZZ \\ IZZZ \end{bmatrix} \rightarrow B' = \begin{bmatrix} \dots \\ IIZZ \\ \dots \\ \dots \end{bmatrix} \quad (24)$$

The answer is shortly applying a  $CX$  gate on line 1 and 2.

Now, let the representation as binary vector

$$B = \begin{bmatrix} ZZZI \\ ZZIZ \\ ZIZZ \\ IZZZ \end{bmatrix} = \begin{bmatrix} 1110 \\ 1101 \\ 1011 \\ 0111 \end{bmatrix} = \begin{bmatrix} \vec{w}_1 \\ \vec{w}_2 \\ \vec{w}_3 \\ \vec{w}_4 \end{bmatrix} \quad (25)$$

With the binary represent, the  $CX$  combination of  $i, j$ -th wires is identical to generate XOR of two  $w_i$ s,  $w_i \oplus w_j$ . XOR is commutative so that, the problem becomes the next statement.

Find the minimum size subset  $\{w_k\} \subset B$  whose XOR products is  $P$  where,

$$P = \oplus_k \vec{w}_k$$



More simply, it is equivalent with finding a binary vector  $\vec{x} \in \{0, 1\}^N$  of

$$P = \bigoplus_{i=1}^N x_i \& \vec{w}_i \quad (26)$$

The solution could be derived with simple linear algebra on specific field,  $\mathbb{Z}/2\mathbb{Z}$ . Logical *XOR*, and *AND* operators form commuting field,  $(\mathbb{Z}/2\mathbb{Z}, \wedge, \&)$ . See the proof in Appendix A. The Gauss elimination process yields a solution of the above problem.

Suppose that we have circuit of the state where the Pauli Frame representation was,

$$B_i = \begin{pmatrix} w_1 & , \cdot \\ w_2 & , \cdot \\ w_3 & , \cdot \\ w_4 & , \cdot \end{pmatrix}, \begin{matrix} w_1 & = & Z_2 Z_3 Z_4 & = & ZZZI & = & 1110_{sym} \\ w_2 & = & Z_1 Z_3 Z_4 & = & ZZIZ & = & 1101_{sym} \\ w_3 & = & Z_1 Z_2 Z_4 & = & ZIZZ & = & 1011_{sym} \\ w_4 & = & Z_1 Z_2 Z_3 & = & IZZZ & = & 0111_{sym} \end{matrix} \quad (27)$$

and we want to apply  $\exp(-itZ_1Z_2)$  gate on circuit, what CX gate combination yields the quantum circuit state for the unitary operator, by simply applying RZ gate on a wire? Luckily, XOR is commute as like the CX gate becomes a conjugation of itself. Let,  $v = [1, 1, 0, 0]^T$ , it is a symplectic representation of  $Z_1Z_2$ , and  $x = [x_1, x_2, x_3, x_4]^T, x_i \in \{0, 1\}$ .

$$Mx = v \quad (28)$$

$$M = \left[ \begin{array}{c|c|c|c} w_1 & w_2 & w_3 & w_4 \end{array} \right] \quad (29)$$

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad (30)$$

With Gauss elimination method, Reduced row echelon form would be obtained.

$$[M \mid v] \rightarrow \left[ \begin{array}{cccc|c} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array} \right] \quad (31)$$

$$1. \ w_1 \oplus w_2 = 0$$

$$2. \ w_2 \oplus w_3 = 1$$

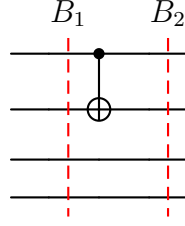
$$3. \ w_3 = 0$$

$$4. \ w_4 = 0$$

Thus, we get  $x = [1, 1, 0, 0]$ , and

$$[0, 1, 1, 1] \oplus [1, 0, 1, 1] = [1, 1, 0, 0] \quad (32)$$

It means that CX over 1st and 2nd yields  $Z_1Z_2 = IIZZ$  Pauli element on the frame. The process reached the same point we had predicted at first. You can observe same process in linear reversible circuit generation[12].



$$B_i = \begin{pmatrix} ZZZI & \cdot \\ ZZIZ & \cdot \\ ZIZZ & \cdot \\ IZZZ & \cdot \end{pmatrix} \xrightarrow{CX(1,2)} B_{i+1} = \begin{pmatrix} ZZZI & \cdot \\ \mathbf{IIZZ} & \cdot \\ ZIZZ & \cdot \\ IZZZ & \cdot \end{pmatrix} \quad (33)$$

The above process holds same for  $X$  and  $Y$  families each. Gauss elimination process is enough to determine the exact entanglement mapping. However, we cannot adopt the process to the general local terms. Since, there is no guarantee that the CX gate is enough to construct Clifford gate that connects two given frames. There are 5 number of entanglements gate to make a Pauli terms from one frame to the other frame[10].

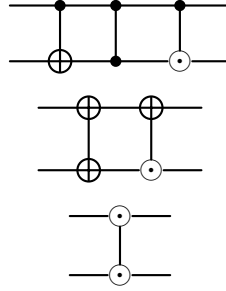


Figure 6: Type of entanglement gate from the left top, Controlled-X, Controlled-Z, Controlled-Y, XControlled-X, XControlled-Y, YControlled-Y.

To expand the result to the general commuting Pauli set. Several properties are needed to guarantee the validation of the algorithm.

### 3.4.2 General Commuting set

To ensure the algorithm is valid for general mutually commuting set, the next thing must be guaranteed. When two Pauli frames  $B_1, B_2$  were given whose stabilizers are mutually commuting to each other, then *all members of second stabilizer could be generated by first stabilizer*.

To prove the property, we need some theorems[13] about commuting subsets of Pauli group on  $N$  qubits system, and general properties of generating sets and definitions[14].

**Theorem 2** (Properties of Pauli group). *For  $N$  qubits system, generalized Pauli group,  $\mathcal{P}/U(1)$ , on the space satisfies the next,*

- A cardinality of maximally commuting subset of  $\mathcal{P}/U(1)$  is  $2^N$ .
- A maximally commuting subset be a subgroup of  $\mathcal{P}/U(1)$ .
- For a subgroup  $S \subset \mathcal{P}/U(1)$ ,  $|S| = 2^l$ , it's generating set  $G$  always exists and  $|G| \geq l$ .



**Definition 2** (Finite generating set). For a group,  $(G, +)$ , a generating set  $X$  of group  $G$  is a finite subset  $X \subset G, |X| = N$  such that  $\forall g \in G, g = \sum_{i=1}^N n_i x_i, x_i \in X, n_i \in \mathbb{N}$ .

**Definition 3** (Independent set). A subset  $X$  of group  $S$  is independent if none of its members can be generated by the others.

**Definition 4** (Exchange property). A group,  $G$ , has an exchange property. If  $y \in G$  is not generated by a subset  $X \subset G$ , but generated by  $X \cup \{z\}, z \in G$  then  $z$  is generated by  $X \cup \{y\}$ .

**Theorem 3.** Let  $G$  be a generating set.

1.  $G$  is a minimal generating set iff  $G$  is a maximally independent set.
2. A maximally independent subset,  $S$ , of group,  $P$ , is a minimal generating set. If generates satisfies exchange property.

Using the cardinality and generating set property, the next corollary is achieved.

Based on the theorems, a finite Abelian group hold the next lemma.

**Lemma 1.** A finite Abelian group whose elements are inverse of themselves each has exchange property.

*Proof.* Suppose it is not, then for a finite Abelian group  $A$ ,  $\exists y, z \in A$ , and finite non-zero sub set  $X \subset A, |X| = N \in \mathbb{N}$ . They satisfy  $y = n_0 z + n_1 x_1 + \dots + n_N x_N, x_i \in X \forall i$ , and  $z \neq n'_0 y + n'_1 x_1 + \dots + n'_N x_N$ . However, adding  $y + n_0 z$  to the RHS and LHS of the first equation yields  $y + n_1 x_1 + \dots + n_N x_N = n_0 z$ . Since, finite Abelian group is a cyclic group,  $\exists M \in \mathbb{N}$  such that  $M(n_0 z) = z, \perp$ . Therefore, a finite Abelian group has an exchange property.  $\square$

**Lemma 2.** For a given generating set  $G$  of mutually commuting subgroup in  $\mathcal{P}/U(1)$ , where  $|G| = N$ . If a Pauli element,  $p$ , is commuting with  $G$ , then  $p \in \langle G \rangle$ .

*Proof.* If  $p \in G$ , it is done. Let  $p \notin G$ . Suppose  $p \notin \langle G \rangle$ , then there is a element  $g \in \langle G \rangle$  such that  $[p, g] \neq 0$ . However,  $g = n_1 g_1 \cdot n_2 g_2 \cdot \dots \cdot n_N g_N$ , and  $[p, g_i] = 0, \forall i \in [N]$ . In addition,  $[p, g_i g_j] = 0$  if  $[p, g_i] = 0$  and  $[p, g_j] = 0$ . Thus,  $[p, n_1 g_1 \cdot n_2 g_2 \cdot \dots \cdot n_N g_N] = 0$ , Therefore,  $p \in \langle G \rangle$ .  $\square$

Now, we can derive the result. For given two frames,  $B_i, B_j$ , Let their stabilizer as  $\text{Stab}(B_i), \text{Stab}(B_j)$ . Let their stabilizers are mutually commuting. Let a generated subgroup of generating set  $G$  as  $\langle G \rangle$ .

**Theorem 4.** The stabilizer of frame  $B$  is a minimum generating set of maximally mutually commuting subgroup of  $N$  qubit Pauli group,  $\mathcal{P}/U(1)$ .

*Proof.* Suppose that  $\text{Stab}(B)$  is a dependent commuting set of Pauli elements.  $\exists a, b, c \in \text{Stab}(B)$  such that  $[a, b] = [b, c] = [a, c] = 0$  but,  $c = a + b$ . From frame representation of  $2N$  element, let the index of  $a, b, c$  as  $i, j, k$ .



Applying  $CX_{ij}$  gate to the frame then,

$$B = \begin{bmatrix} \vdots & \vdots \\ a & \tilde{s}_a \\ b & \tilde{s}_b \\ c & \tilde{s}_c \\ \vdots & \vdots \end{bmatrix} \rightarrow_{CX_{ij}} B' = \begin{bmatrix} \vdots & \vdots \\ a & \tilde{s}_a + \tilde{s}_b \\ c & \tilde{s}_b \\ c & \tilde{s}_c \\ \vdots & \vdots \end{bmatrix}$$

On 2nd frame,  $B'$ ,  $s_j = c$ , where  $[c, \tilde{s}_k] \neq 0$ . However,  $[s_j, \tilde{s}_k] = 0$ ,  $j \neq k$  by the definition of Pauli frame, and all Pauli frames are closed to Clifford transformation  $\perp$ . Therefore,  $\text{Stab}(B)$  is an independent set. For  $N$  qubits Pauli group, the cardinality of maximally independent set is  $N$ , and  $|\text{Stab}(B)| = N$ , so that it is a maximally independent subset of  $\mathcal{P}/U(1)$ . Since,  $\mathcal{P}/U(1)$  has an exchange property by Lemma 1, it is a minimal generating set of mutually commuting subgroup,  $\therefore$  Thm 3.  $\square$

**Corollary 1.** *Let two Pauli frames,  $B_1, B_2$ . If a union of their stabilizers is mutually commuting set, then  $\langle \text{Stab}(B_1) \rangle = \langle \text{Stab}(B_2) \rangle$ .*

*Proof.* By the theorem,  $\text{Stab}(B_1), \text{Stab}(B_2)$  are minimal generating set of maximal mutually commuting subgroup.  $\therefore$  Lemma 2, All Pauli element in  $\text{Stab}(B_j)$  are in  $\langle \text{Stab}B_i \rangle$ . So do,  $\forall p \in \langle \text{Stab}(B_j) \rangle, p \in \langle \text{Stab}(B_i) \rangle$ , and vice verse.  $\square$

This corollary guarantees that Clifford transformation connecting  $B_1$ , and  $B_2$  is a combination of CX gates. If CX gate is enough to construct the Clifford transformation, then the transformation becomes a *linear* transformation. Now, we can apply common linear algebraic methods to calculate the transformation.

The theorem contains several minor results of destabilizer.

**Corollary 2.** *So do on destabilizers of two frames  $B_1$ , and  $B_2$ .*

As a side, not for two frames, but for a frame and a Pauli element, the next lemma hold true.

**Theorem 5.** *In  $N$  qubits system, for a given Pauli term,  $p$ , and Pauli frame,  $B$ , if  $p$  is commute with all terms in stabilizers of  $B$ ,  $\{s_i\}_{i=1}^N$ , then a frame  $B'$  where  $p \in \text{Stab}(B')$  is derived from  $B$  at most  $N - 1$  number of CX gates.*

$$B_0 \rightarrow B' \tag{34}$$

The one thing we need to synthesis circuit, LU decomposition of general Pauli elements. In  $IZ$  element, the elimination process is directly corresponded to the  $z$  binary vectors. However, the general case the element is defined with two binary vectors,  $x, z$ ,  $B = [\{(x_i, z_i)\}_{i=1}^N, \cdot], p = (x, z)$ . The combination vector  $v$  is determined uniquely with two linear system.

$$M_x \vec{v} = \vec{x}, M_z \vec{v} = \vec{z} \tag{35}$$

In that case, we can use a stacked two linear equation

$$\begin{bmatrix} M_x & | & x \\ M_z & | & z \end{bmatrix} \tag{36}$$

where,  $M_x = [x_1|x_2|\cdots|x_N], M_z = [z_1|z_2|\cdots|z_N]$ . Other solution is a constructing a new linear equation by linear combination.

$$Mv = w \leftrightarrow (M_x + M_z)v = (x + z) \tag{37}$$



### 3.5 Summary of Clifford operator search process

Condition: For given two frames,  $B_1, B_2$ ,  $\lambda(\text{Stab}(B_1), \text{Stab}(B_2)) = 0$

1. Calculate the  $\oplus, \text{Stab}(B_1)$  representation of  $p = \vec{b}_p$ ,  $\forall p \in \text{Stab}(B_2)$  by solving a linear equation,  $Ab_p = p$
2. Using  $p$  vectors, construct a matrix representation,  $X$ , of  $\text{Stab}(B_2)$ .
3. An identity matrix  $I$  be a representation of  $\text{Stab}(B_1)$ .
4. Find a transformation matrix,  $A$ ,  $X = A \cdot I$ , using LU or UL decomposition of  $X = LU/UL$ .
5. For  $L, U$ 
  - (a) If there is a zero element on diagonal of  $L$  or  $U$ , the  $\text{Stab}(B_2)$  is not a valid frame.
  - (b) Non-zeros of non-diagonal elements are representing a CNOT gates combination.
  - (c) The summation of non-zeros of non-diagonal elements is a required CNOT gates to make  $B_2$  frame.
  - (d)  $l_{ij}, u_{ij} = 1$  means *CNOT* from  $j$  to  $i$  wire.
6. Convert the two  $L, U$  matrices as CNOT gates, UL or LU decomposition whose circuit length is shorter than the other.

## 4 Expansion to general frames

In previous section, we only described a case that the Clifford transformation was a composite of only *CX* gate. The *CX* map generated from the algorithm did not guarantee the optimal decomposition, however, we can estimate what unitary transformation is required to connect two Pauli frames. In general Clifford transformation, they are combinations of *H, S, CX* gates. Still, entanglement gate is only a *CX* gate but *H*, and *S* gates transform each qubit basis, so that the overall combination is more complicated than *CX* case. To show their properties on Pauli frame graph, a new representation would be useful to analyze their structure.

### 4.1 Qubit-wise Pauli frame

Qubit-wise Pauli frame(QPF)

$$q = \begin{bmatrix} Z - X & I - I & I - I & I - I \\ I - I & Z - X & I - I & I - I \\ I - I & I - I & Z - X & I - I \\ I - I & I - I & I - I & Z - X \end{bmatrix} \Leftrightarrow \begin{bmatrix} Z_1 & X_1 \\ Z_2 & X_2 \\ Z_3 & X_3 \\ Z_4 & X_4 \end{bmatrix} = p \in \text{PF} \quad (38)$$

We can treat QPF as a tuple of qubit-wise stabilizer and destabilizer matrix as



$$q = \left( \begin{bmatrix} Z & I & I & I \\ I & Z & I & I \\ I & I & Z & I \\ I & I & I & Z \end{bmatrix}, \begin{bmatrix} X & I & I & I \\ I & X & I & I \\ I & I & X & I \\ I & I & I & X \end{bmatrix} \right) \quad (39)$$

#### 4.1.1 QPF under Clifford transformation

Table 1: Categories of Qubit frame

Prime	Support
$Z - X$	$I - I$
$Z - Y$	$I - X$
$X - Y$	$I - Y$
-	$I - Z$
-	$X - X$
-	$Y - Y$
-	$Z - Z$

$$\left( \begin{bmatrix} Z & I & I & I \\ I & Z & I & I \\ I & I & Z & I \\ I & I & I & Z \end{bmatrix}, \begin{bmatrix} X & I & I & I \\ I & X & I & I \\ I & I & X & I \\ I & I & I & X \end{bmatrix} \right) \xrightarrow{CX(1,2)} \left( \begin{bmatrix} Z & I & I & I \\ Z & Z & I & I \\ I & I & Z & I \\ I & I & I & Z \end{bmatrix}, \begin{bmatrix} X & X & I & I \\ I & X & I & I \\ I & I & X & I \\ I & I & I & X \end{bmatrix} \right) \quad (40)$$

$$\left( \begin{bmatrix} Z & I & I & I \\ I & Z & I & I \\ I & Y & Z & I \\ I & I & I & Z \end{bmatrix}, \begin{bmatrix} X & I & I & I \\ I & X & I & I \\ I & I & X & I \\ I & I & I & X \end{bmatrix} \right) \xrightarrow{H(3)} \left( \begin{bmatrix} Z & I & I & I \\ I & Z & I & I \\ I & I & X & I \\ I & I & I & Z \end{bmatrix}, \begin{bmatrix} X & I & I & I \\ I & X & I & I \\ I & Y & Z & I \\ I & I & I & X \end{bmatrix} \right) \quad (41)$$

**Theorem 6.** Let  $N_p(q)$  be a number of prime elements of QPF  $q$ .  $N_p(q)$  is conserved in Clifford transformation.

*Proof.* CX

H  
S

□

**Corollary 3.** For  $N$  qubits system,  $N_p(q) = N, \forall q \in \mathbb{QP}$

#### 4.1.2 Pauli frame construction

**Theorem 7.** For  $N$  number of mutually commuting Pauli elements, choosing a set of corresponding prime elements determines a unique Pauli frame.



## 5 Mutually Commuting Partition

The remained question is how can we construct mutually commuting partition, from the given hamiltonian and its Pauli polynomial representation. The answer is *we cannot do that efficiently on classical computer*. Suppose that we constructed a graph that indicates commuting relationship of all Pauli terms in the hamiltonian. See Fig

Partitioning the given Pauli elements is equivalent with *Max-clique* problem in computer science and it is a well-known NP-hard problem[15].

There are practical algorithms in many graph libraries. In addition, many quantum computer companies provide convenience interfaces for clique problems. Despite the

### 5.1 Solve clique problem on Quantum computer

Kurita et al, They also investigated an algorithm to find max-clique with limited size clique solver which is smaller than the given problem.

Which method is the most efficient method for the problem? Well, the answer is we don't know yet. Sometimes quantum algorithm would show better with QAOA or annealing system, but by the situation classic method could have some advantages. Choosing an algorithm is a job of researchers or users who want to generate optimized Trotter circuit. In here, providing a convenience interface would be enough.

## A Proof of Modulo field

$(\mathbb{Z}/2\mathbb{Z}, \wedge, \&)$ .

Denote, XOR( $\wedge$ ) as  $\oplus$  and, AND( $\&$ ) as  $\odot$ ,

$$\begin{aligned} 0 \oplus 0 &= 0 & 0 \odot 0 &= 0 \\ 0 \oplus 1 &= 1 & 0 \odot 1 &= 0 \\ 1 \oplus 0 &= 1 & 1 \odot 0 &= 0 \\ 1 \oplus 1 &= 0 & 1 \odot 1 &= 1 \end{aligned} \tag{42}$$

Addition

1. a

## References

- [1] Naomichi Hatano and Masuo Suzuki. Finding Exponential Product Formulas of Higher Orders. In R. Beig, W. Beiglböck, W. Domcke, B.-G. Englert, U. Frisch, P. Hänggi, G. Hasinger, K. Hepp, W. Hillebrandt, D. Imboden, R. L. Jaffe, R. Lipowsky, H. V. Löhneysen, I. Ojima, D. Sornette, S. Theisen, W. Weise, J. Wess, J. Zittartz, Arnab Das, and Bikas K. Chakrabarti, editors, *Quantum Annealing and Other Optimization Methods*, volume 679, pages 37–68. Springer Berlin Heidelberg, Berlin, Heidelberg, November 2005. Series Title: Lecture Notes in Physics.
- [2] Ronald de Wolf. Quantum computing: Lecture notes, 2023.
- [3] Guang Hao Low and Isaac L. Chuang. Hamiltonian simulation by qubitization. *Quantum*, 3:163, July 2019.





- [4] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. Simulating hamiltonian dynamics with a truncated taylor series. *Phys. Rev. Lett.*, 114:090502, Mar 2015.
- [5] Dominic W. Berry, Andrew M. Childs, Richard Cleve, Robin Kothari, and Rolando D. Somma. Exponential improvement in precision for simulating sparse hamiltonians. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, STOC '14. ACM, May 2014.
- [6] Andrew M. Childs, Yuan Su, Minh C. Tran, Nathan Wiebe, and Shuchen Zhu. Theory of Trotter Error with Commutator Scaling. *Physical Review X*, 11(1):011020, February 2021.
- [7] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.
- [8] Johann Ostmeier. Optimised trotter decompositions for classical and quantum computing. *Phys. A: Math. Theor.*, 56(28), 2023.
- [9] Conor Mc Keever and Michael Lubasch. Classically optimized hamiltonian simulation. *Phys. Rev. Res.*, 5:023146, Jun 2023.
- [10] Albert T. Schmitz, Nicolas P. D. Sawaya, Sonika Johri, and A. Y. Matsuura. Graph Optimization Perspective for Low-Depth Trotter-Suzuki Decomposition, May 2023. arXiv:2103.08602 [cond-mat, physics:math-ph, physics:physics, physics:quant-ph].
- [11] Kim Hyunseong. Trotter circuit optimization through adiabatic computer, November 2023.
- [12] Timothée Goubault De Brugière, Marc Baboulin, Benoît Valiron, Simon Martiel, and Cyril Allouche. Gaussian elimination versus greedy methods for the synthesis of linear reversible circuits. *ACM Transactions on Quantum Computing*, 2(3), sep 2021.
- [13] Rahul Sarkar and Ewout Van Den Berg. On sets of maximally commuting and anticommuting Pauli operators. *Research in the Mathematical Sciences*, 8(1):14, March 2021.
- [14] Bernard P. Zeigler. Maximally independent sets, minimal generating sets, and irreducibles. *Mathematical systems theory*, 8(2):176–181, June 1974.
- [15] Richard M. Karp. Reducibility among Combinatorial Problems. In Raymond E. Miller, James W. Thatcher, and Jean D. Bohlinger, editors, *Complexity of Computer Computations: Proceedings of a symposium on the Complexity of Computer Computations, held March 20–22, 1972, at the IBM Thomas J. Watson Research Center, Yorktown Heights, New York, and sponsored by the Office of Naval Research, Mathematics Program, IBM World Trade Corporation, and the IBM Research Mathematical Sciences Department*, pages 85–103. Springer US, Boston, MA, 1972.