

# Local and Global Quantum Gates

Lin WENG

Graduate School of Mathematics, Kyushu University

## Abstract

New theories on local  $p$ -adic and global adelic quantum gates are developed. In particular, the corresponding universality properties are established using only finitely many local/global quantum gates.

## 1 Quantum Computing

Motivated by the theory of quantum mechanics ([1]), for quantum computings, the state space of 1-qubits is defined as a 2-dimensional  $\mathbb{C}$ -vector space with standard Hermitian inner product

$$\mathcal{H} := \mathbb{C}|0\rangle + \mathbb{C}|1\rangle \quad (1)$$

where  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  and  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ , and similarly, the state space of  $n$ -qubits is defined as the  $N(= 2^n)$ -dimensional  $\mathbb{C}$ -vector space with standard Hermitian inner product

$$\mathcal{H}^n := \mathcal{H}^{\otimes n} = \bigoplus_{k_1, k_2, \dots, k_n \in \{0,1\}} \mathbb{C}|k_n \dots k_2 k_1\rangle = \mathbb{C}|00 \dots 0\rangle + \dots + \mathbb{C}|11 \dots 1\rangle, \quad (2)$$

where  $\{|k_n \dots k_2 k_1\rangle := |k_n\rangle \otimes \dots \otimes |k_2\rangle \otimes |k_1\rangle \ (k_i \in \{0,1\})\}$  forms an orthonormal basis of  $\mathcal{H}^n$ . We call an element  $\mathbf{x} = \sum x_{k_n \dots k_2 k_1} |k_n \dots k_2 k_1\rangle \in \mathcal{H}^n$  *normalized* if  $\sum |x_{k_n \dots k_2 k_1}|^2 = 1$ , in which case,  $|x_{k_n \dots k_2 k_1}|^2$  is called the probability for the pure qubit state  $|k_n \dots k_2 k_1\rangle$  to appear in  $\mathbf{x}$ , which can be observed via measurements.

Partially because normalized states should be preserved by quantum operations, which deeply rooted in the time dependence of the wave solutions for Schrödinger equation by the theory of quantum mechanics, unitary matrices of size  $N$  are used to build up quantum gates for quantum computers when dealing with  $n$  qubits. These quantum gates satisfy the so-called finite (approximate) universality properties. Consequently, each quantum circuit can be (approximately) built up from a family of finite quantum gates, consisting of Hadamard gate, Pauli gates, Toffoli gates and their associates. For examples, we have following quantum gates for one qubits.

(1) Global phase gate

$$M(\alpha) := e^{i\alpha} I_2 \quad \text{with} \quad I_2 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \& \quad \alpha \in \mathbb{R}$$

(2) Relative phase shift

$$P(\alpha) := \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix} \quad \text{with } \alpha \in \mathbb{R}.$$

In particular, we set phase  $\pi/4$ -gate to be  $S = P(\pi/2) = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$  and  $\pi/8$ -gate to be  $T = P(\pi/4) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ .

(3) Pauli gates

$$\sigma_X = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_Y = Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad \sigma_Z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

(4) Rotations with respect to  $\hat{x}, \hat{y}, \hat{z}$  axes of the Bloch sphere

$$\begin{aligned} R_x(\theta) &= \cos \frac{\theta}{2} I_2 - i \sin \frac{\theta}{2} X = \begin{pmatrix} \cos \frac{\theta}{2} & -i \sin \frac{\theta}{2} \\ -i \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \\ R_y(\theta) &= \cos \frac{\theta}{2} I_2 - i \sin \frac{\theta}{2} Y = \begin{pmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \\ R_z(\theta) &= \cos \frac{\theta}{2} I_2 - \sin \frac{\theta}{2} Z = \begin{pmatrix} \exp(\frac{\theta}{2}i) & 0 \\ 0 & \exp(\frac{\theta}{2}i) \end{pmatrix} \end{aligned} \quad (3)$$

More generally, for 2-qubits/3-qubits, we introduce controlled-NOT/controlled-controlled NOT gate or CNOT/Toffoli gate  $C/C^{(2)}$  by

$$\begin{aligned} C|00\rangle &= |00\rangle, \quad C|01\rangle = |01\rangle, \quad C|10\rangle = |11\rangle, \quad C|11\rangle = |10\rangle. \\ C^{(2)}|t_1, t_2, \psi\rangle &:= \begin{cases} |t_1, t_2, \psi\rangle, & t_1 t_2 = 0 \\ |t_1, t_2, 1 \oplus \psi\rangle, & t_1 t_2 = 1. \end{cases} \end{aligned} \quad (4)$$

**Theorem 1** (Approximate universality, see e.g. [10]). *We have*

- (1) *The CNOT gate together with the above 1-qubit gates is universal.*
- (2) *The CNOT gate  $C$ , Hadamard gate  $H$ , and  $\pi/8$ -gate  $T$  are approximately universal.*
- (3) *The CNOT gate  $C$ , Hadamard gate  $H$ , phase gate  $S$  and Toffoli gate are approximately universal.*

For details on fundamentals of quantum computer, quantum information and quantum programming, please refer to [5, 10, 18]. The reader may also find some background materials in [3].

## 2 Local $p$ -Adic Quantum Computings

Motivated by the above discussion and our own researches on distributions of zeros of non-abelian zeta functions for number fields ([15]), we now initiate an approach to what might be called the theory of local  $p$ -adic quantum computings

(and  $p$ -adic quantum computers). This is based on  $p$ -adic probability theory of Khrennikov ([6]),  $p$ -adic quantum mechanics and  $p$ -adic string theory of, say, Freund, Witten and others.

Fix a prime integer  $p$ , and let  $\mathbb{Q}_p$  be the field of  $p$ -adic rationals with  $\mathbb{Z}_p$  the ring of  $p$ -adic integers. By definition, a  $p$ -adic 1-qubit is an element of the  $p$ -adic quantum state space

$$\mathcal{H}_p := \mathbb{Q}_p|0\rangle + \mathbb{Q}_p|1\rangle,$$

and a  $p$ -adic  $n$ -qubit is an element in the  $p$ -adic quantum state space

$$\mathcal{H}_p^n := \mathcal{H}_p^{\otimes n} := \mathbb{Q}_p|00 \cdots 0\rangle + \cdots + \mathbb{Q}_p|11 \cdots 1\rangle.$$

Moreover, a  $p$ -adic  $n$ -qubit  $\mathbf{x} := \sum x_{k_n \dots k_2 k_1} |k_n \dots k_2 k_1\rangle$  is called normalized if  $x_{k_n \dots k_2 k_1} \in \mathbb{Z}_p$  ( $k_i \in \{0, 1\}$ ).

**Remark 1.** *The definition of normalized states is based on the fact that  $p$ -adic probability is taken values in  $\mathbb{Z}_p$  for which negative values is possible. In fact any negative natural number is considered to be of small  $p$ -adic probability. This also offers a reason why we decide to remove the constrain that 1 is the totality of probabilities since it does not make a good sense in  $p$ -adic setting.*

Ideally,  $p$ -adic quantum gates should preserve normalized states. Hence, it is only natural to consider the elements in the maximal compact subgroup group  $\mathrm{GL}_N(\mathbb{Z}_p)$  of  $\mathrm{GL}_N(\mathbb{Q}_p)$ . That is to say, an element  $g \in \mathrm{GL}_N(\mathbb{Z}_p)$  defines a  $p$ -adic quantum gate. This appears to be perfectly compatible with nowadays mathematics: With respect to the structure of the general linear group  $\mathrm{GL}_N$  over the adelic ring  $\mathbb{A} = \mathbb{A}_F$  associated to a global algebraic number field  $F$ , it is central for us to introduce its canonical maximal open compact subgroup  $K := \prod_{\mathfrak{p}:\text{finite}} K_{\mathfrak{p}} \times \prod_{\sigma|\infty} K_{\sigma}$  where for each finite place  $\mathfrak{p}$  of  $F$ ,  $K_{\mathfrak{p}} = \mathrm{GL}_N(\mathcal{O}_{\mathfrak{p}})$  is the general linear group over the local ring  $\mathcal{O}_{\mathfrak{p}}$  of  $\mathfrak{p}$ -adic integers, and for each infinite place  $\sigma$  of  $F$ , when  $\sigma$  is real, resp. complex, we set  $K_{\sigma} = O_N$ , resp.  $U_N$ , the orthogonal group, resp., the unitary group, of size  $N$ .

Note that  $\mathrm{GL}_N(\mathbb{Z})$  is finitely generated and moreover is dense in  $\{\pm 1\} \times \mathrm{SL}_N(\mathbb{Z}_p)$  (with respect to the topology induced from the  $p$ -adic topology), it is in principal not very difficult but rather fundamental to establish the  $p$ -adic approximate universality theorem for  $p$ -adic quantum gates. Before explain the details, let us make some preparations.

For an element  $a \in \mathbb{Q}_p$ , set

$$E(a) := \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \quad U(a) := \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad L(a) := \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \quad (5)$$

In addition, as usual, when  $p \neq 2$ , we introduce the  $p$ -adic exponential  $\exp_p(pa) := \sum_{n \geq 0} \frac{p^n a^n}{n!}$  as the isomorphism of the additive group  $p\mathbb{Z}_p$  onto the multiplicative group  $1 + p\mathbb{Z}_p$  such that  $|\exp_p(pa) - \exp_p(pb)| = |p||a - b|$ , whose reciprocal isomorphism is given by the  $p$ -adic logarithmic function  $\log_p(1 + pa) = \sum_{n \geq 1} (-1)^{n-1} \frac{p^n a^n}{n}$ .<sup>1</sup> Fix also a primitive  $(p - 1)$ -th root  $\zeta_p$  of unity in  $\mathbb{Z}_p$ .

<sup>1</sup>when  $p = 2$ , we instead consider the isomorphism  $\exp_2(2^2 a) = \sum_{n \geq 0} \frac{2^{2n} a^n}{n!}$ , an isomorphism of the additive group  $2^2\mathbb{Z}_2$  onto the multiplicative group  $1 + 2^2\mathbb{Z}_2$  such that  $|\exp_2(2^2 a) - \exp_2(2^2 b)| = |2^2||a - b|$  whosereciprocal isomorphism is given by the 2-adic logarithmic function  $\log_2(1 + 2^2 a) = \sum_{n \geq 0} (-1)^{n-1} \frac{2^{2n} a^n}{n}$ .

**Theorem 2** (*p*-Adic Approximate Universality). *The following set of p-adic quantum gates is approximately universal:*

(1) if  $p \neq 2$ ,

$$\{M_\zeta := E(\zeta_p), E(\exp_p(p)), U(1), L(1)\}$$

or

$$\{M_\zeta := E(\zeta_p), P_{1+p} := E(1+p), P_+ := U(1), P_- := L(1)\}$$

(2) if  $p = 2$ ,

$$\{M_{-1} := E(-1), P_{2^2} := E(\exp_2(2^2)), P_+ := U(1), P_- := L(1)\}$$

or

$$\{M_{-1} := E(-1), P_{1+2^2} := E(1+2^2), P_+ := U(1), P_- := L(1)\}$$

*Proof.* Since the proof for  $p = 2$  is similar, we here only give a proof for  $p \neq 2$  and briefly sketch how modifications can be made to apply the same argument to the case  $p = 2$ . Let us first consider the case  $N = 2$ . Obviously,  $GL_s(\mathbb{Z}_p)$  admits a natural semi-product decomposition

$$GL_2(\mathbb{Z}_p) = E(\mathbb{Z}_p^*) \rtimes SL_2(\mathbb{Z}_p). \quad (6)$$

Hence it suffices to find the topological generators of the  $p$ -adic unit group  $\mathbb{Z}_p^*$  and  $SL_2(\mathbb{Z}_p)$ . First we deal with  $\mathbb{Z}_p^*$  by considering the canonical quotient map  $\mathbb{Z}_p \mapsto \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$ . Obviously,  $\mathbb{F}_p^* = \langle \zeta_p \rangle$  as a cyclic group of order  $p - 1$ , and an element  $x \in \mathbb{Z}_p$  belongs to  $\mathbb{Z}_p^*$  if and only if

$$z = \zeta_p^{n(z)}(1+pb(z)) = \zeta_p^{n(z)} \exp(\exp_p(p\alpha(z))) \quad \exists \alpha(z) := \frac{\log_p(1+pb(z))}{p} \in \mathbb{Z}_p. \quad (7)$$

Therefore, if we set  $\alpha_n(z) := \sum_{k=0}^{n-1} \lambda_k(z)p^k$  be the  $(n - 1)$ -th truncated sum of the  $p$ -adic expansion of  $\alpha(z)$ , then

$$1 + pb(z) = \exp(p\alpha(z)) = \lim_{n \rightarrow \infty} \exp_p(p\alpha_n(z)) = \lim_{n \rightarrow \infty} \exp_p(p)^{\alpha_n(z)}.$$

Hence

$$z = \zeta_p^{n(z)} \cdot \lim_{n \rightarrow \infty} \exp_p(p)^{\alpha_n(z)}.$$

In other words,  $\mathbb{Z}_p^*$  is topologically generated by  $\{\zeta_p, \exp_p(p)\}$ .

In addition, using the  $p$ -adic logarithmic function  $\log_p(1+pa)$ , any element  $x = 1 + pc$  of  $1 + p\mathbb{Z}_p$  can be written uniquely as

$$(1+p)^{\alpha(x)} = \sum_{k \geq 0} \binom{\alpha(x)}{k} p^k = \exp_p(\alpha(x) \log_p(1+p)) \quad \left( \exists \alpha(x) := \frac{\log_p(1+pc)}{\log_p(1+p)} \right).$$

Thus for a sequence  $\{\alpha_n(x)\}_n \subset \mathbb{Z}_{\geq 0}$  satisfying  $\alpha(x) = \lim_{n \rightarrow \infty} \alpha_n(x)$ , we have

$$x = \lim_{n \rightarrow \infty} (1+p)^{\alpha_n(x)}.$$

This implies that  $\{\zeta_p, 1+p\}$  topologically generates  $\mathbb{Z}_p^*$  as well.

When  $p = 2$ , we have  $\mathbb{Z}_2^* = \{-1, 1\} \times (1+2^2\mathbb{Z}_2)$ . Hence the above arguments works well as claimed.

From the discussions above, to complete the proof of this theorem for  $N = 2$ , it suffices to show that  $\mathrm{SL}_2(\mathbb{Z}_p)$  is topologically generated by  $P_+$  and  $P_-$  together with  $E(\mathbb{Z}_p^*)$ .

For this, let  $s = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_p)$ . Following [9], we note that, if  $c$  is a  $p$ -adic unit, with  $ad - bc = 1$ , or the same  $b = (ad - 1)c^{-1}$ ,

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} 1 & -(1-a)c^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & -(1-d)c^{-1} \\ 0 & 1 \end{pmatrix} \\ \begin{pmatrix} a & c \\ b & d \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ -(1-a)c^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -(1-d)c^{-1} & 1 \end{pmatrix}. \end{aligned} \quad (8)$$

Each of the factors on the right hand sides of both relations can be topologically generated by  $P_+$  and  $P_-$ . Hence we may assume that  $c$  is not a  $p$ -adic unit. This implies that  $a$  is a  $p$ -adic unit since  $ad = 1 + bc$ . Hence we may instead consider the matrix

$$\begin{pmatrix} c & d \\ -a & -b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and apply the above argument. This then complete the proof for the case  $N = 2$  since

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = P_+ P_-^{-1} P_+.$$

To deal with general  $N$ , it suffices to use the Schmit normal form for matrices  $A = (a_{ij}) \in M_N(\mathbb{Z}_p)$ . In fact, it is a standard fact that there exist two elements  $L, R \in \mathrm{GL}_N(\mathbb{Z}_p)$  such that  $LAR = \mathrm{diag}(d_1, d_2, \dots, d_N)$ , where  $d_1, d_2, \dots, d_N$ , the so-called elementary divisors of  $A$ , satisfy the condition that  $d_1 | d_2 | \dots | d_N$  and  $d_i = \Delta_i / \Delta_{i-1}$  ( $1 \leq i \leq N$ ), where  $\Delta_0 = 1$  and  $\Delta_i$  ( $1 \leq i \leq N$ ) denotes the gcd of all  $i \times i$ -minors of  $M$ . Furthermore,  $L$  and  $R$  are products of the elementary matrices of the following three types:

$$\begin{aligned} T_{ij}(b) &:= I_N + bE_{ij} \quad (1 \leq i \neq j \leq N, b \in \mathbb{Z}_p), \\ P_{ij} &:= I_N - E_{ii} - E_{jj} + E_{ij} + E_{ji} \quad (1 \leq i \neq j \leq N), \\ D_i(u) &:= I_N - (1-u)E_{ii} \quad (1 \leq i \leq N, u \in \mathbb{Z}_p^*). \end{aligned} \quad (9)$$

Here  $I_N$  denotes the identity matrix of size  $N$  and  $E_{ij} \in M_N(\mathbb{Z}_p)$  denotes the matrix whose  $(k, l)$ -entry is 1 if  $(k, l) = (i, j)$ , 0 otherwise.  $\square$

### 3 Global Adelic Quantum Computings

Quantum computers and  $p$ -adic quantum computers should be viewed as local versions of more global quantum computers. For this reason, we sometimes call current quantum computers analytic quantum computers, while saving the terminology of quantum computer for both analytic quantum and  $p$ -adic quantum computers.

Recall that in mathematics, naturally associated to global fields  $F$  are local fields first, both archimedean  $F_\sigma$  and non-archimedean  $(F_v, \mathcal{O}_v, k_v)$ , and then the global adelic ring  $\mathbb{A}_F$ , defined as the restricted product of  $F_v$  and  $F_\sigma$  with respect to  $\prod_v \mathcal{O}_v$ . In parallel, for the theory of quantum computers, there should be one for what might be called global or adelic quantum computers.

Our first task is to understand what should be the state space  $\mathcal{H}_{\mathbb{A}}$ . It is only natural to take it to be  $\mathbb{A}^N$  or more generally  $\bigoplus_{i \in I} \mathbb{A}$  where  $I$  is a countable index set. For simplicity, in the sequel, we only work over finite 'dimensional' state space, namely, assuming that  $\#I = N < +\infty$ . A state vector  $x = (x_v; x_\sigma) \in \mathcal{H}_{\mathbb{A}}$  is called normalized if for all finite places  $v$ , resp. infinite places  $\sigma$  of  $F$ ,  $x_v$ , resp.  $x_\sigma$  are locally normalized. Consequently, adelic quantum gates should be associated to the elements of a maximal compact subgroup  $K = \prod_v K_v \times \prod_\sigma K_\sigma$  of  $\mathrm{GL}_N(\mathbb{A})$  with  $K_v = \mathrm{GL}_N(\mathcal{O}_v)$  and  $K_\sigma$  are either orthogonal group  $O_N$  or unitary group  $U_N$  depending whether  $\sigma$  is real or complex.

To be more precise, 2-dimensional adelic state space consisting of adelic one qubit is defined to be  $\mathcal{H}_{\mathbb{A},2} := \mathbb{A}|0\rangle + \mathbb{A}|1\rangle$ , and more generally,  $N = (2^n)$ -dimensional adelic state space consisting of adelic  $n$  qubit is defined to be

$$\mathcal{H}_{\mathbb{A}}^n := \bigoplus_{\substack{(k_n \dots k_2 k_1) \\ k_1, k_2, \dots, k_n \in \{0,1\}}} \mathbb{A} |k_n \dots k_2 k_1\rangle.$$

An adelic  $n$ -qubit

$$a = \sum_{\substack{(k_n \dots k_2 k_1) \\ k_1, k_2, \dots, k_n \in \{0,1\}}} a_{k_n \dots k_2 k_1} |k_n \dots k_2 k_1\rangle \in \mathcal{H}_{\mathbb{A},N}$$

is called normalized if for each  $(k_n \dots k_2 k_1) \in \{(0 \dots 00), \dots, (1 \dots 11)\}$ ,  $a_{k_n \dots k_2 k_1} = (a_{k_n \dots k_2 k_1, v}; a_{k_n \dots k_2 k_1, \sigma}) \in \mathbb{A}$ , and for each finite place  $v$ ,  $a_{k_n \dots k_2 k_1, v} \in \mathcal{O}_v$  while for each infinite place  $\sigma$ ,

$$\sum_{\substack{(k_n \dots k_2 k_1) \\ k_1, k_2, \dots, k_n \in \{0,1\}}} |a_{k_n \dots k_2 k_1, \sigma}|^2 = 1.$$

Furthermore, among all elements  $g = (g_v; g_\sigma) \in \mathrm{GL}_N(\mathbb{A})$ , adelic quantum gates should be build up merely from the elements of its maximal compact subgroup

$$K_N := \prod_{v:\text{finite}} \mathrm{GL}_N(\mathcal{O}_v) \times \prod_{\sigma:F \hookrightarrow \mathbb{R}} O_N \times \prod_{\tau:F \hookrightarrow \mathbb{C}} U_N.$$

The first difficulty faced by adopting this approach to adelic quantum gates is that, for each such a adelic quantum gate, there are infinitely many operations which should be proceeded. To understand this, we may recall the so-called strong approximation theorem for algebraic groups.

Let  $G$  be an algebraic group over a global field  $F$ . Within the adelic ring  $\mathbb{A}$  of  $F$ , for a non-empty finite set  $S$  of places of  $F$ , define  $\mathbb{A}^S$  to be the ring of  $S$ -adeles and  $\mathbb{A}_S$  to be the product of  $K_v$ 's for all  $v \in S$ . Obviously, via the diagonal embeddings,  $G(F)$  can be viewed as a subgroups of both  $G(\mathbb{A}^S)$  and  $G(\mathbb{A}_S)$ . Then the weak approximation is a property that  $G(F)$  is dense in  $G(\mathbb{A}_S)$ , while the strong approximation is a property that  $G(F)$  is dense in

$G(\mathbb{A}^S)$ . This latter property is equivalent to that  $G(F)G(\mathbb{A}_S)$  is dense in  $G(\mathbb{A})$ . If so then the approximate universality can be answered using elements of  $G(F)$ , since  $G(\mathbb{A}_S)$  always satisfies approximate universality for the reason that  $S$  is finite.

For general algebraic groups, the strong approximation is not satisfied. However, when  $G$  is a semi-simple and simply-connected, the strong approximation holds, established by Kneser ([7]) and Platonov ([11, 12]), resp. Margulis ([9]) and Prasad ([13]), when  $F$  is a number field, resp. a function field over a finite field.

Related to this, one may wonder how the classical reduction theory enters into the picture. In case  $\mathrm{SL}_2$ , we may consider the quotient  $\mathrm{SL}_2(F)\backslash\mathrm{SL}_2(\mathbb{A})/K_2$ . This is studied intensively in ([14]) using stability, as an integrated part of rank two non-abelian zeta function of  $F$ . In terms of integral model to be discussed below, this means that the global quantum gates are build up from  $\mathrm{SL}(\mathcal{O}_F \oplus \mathfrak{a})$ , which enjoys the universality property since  $\mathrm{SL}(\mathcal{O}_F \oplus \mathfrak{a})$  is finitely generated (See e.g. [2]), and admits a natural action on  $\mathcal{H}^{r_1} \times \mathbb{H}^{r_2}$  where  $\mathcal{H}$ , resp.  $\mathbb{H}$ , denotes the hyperbolic upper half plane resp. the 3-dimensional hyperbolic upper half space. In this way, then geometry is naturally involved.<sup>2</sup>

To avoid this, we may use the adelic topology involved to do the approximation. The ideal situation then should be for each adelic quantum gate, there should be only finitely many places which are not trivial. For our own use, we call such adelic quantum gates one of finite type. Put this in an equivalent way, in terms of adelic quantum state vectors, for the difference between the input and the output adelic quantum state vectors, there is a finite set  $S$  of places, including possibly parts of infinite places, such that for  $v \notin S$ , the  $v$ -component of the adelic quantum gates is trivial, i.e. degenerates to the identity operators. This then would mean that the difference between the input and output state vectors should be the same for almost all but finitely many components. In other words, there should be a global integral structure involved for adelic quantum calculations. To understand this, we supply the following discussion on global quantum computings.

### 3.1 Integral Structures

Even this first level consideration above would certainly lead to a nice and rich theory of adelic quantum computers, it may prove to be too complicated for us human beings to achieve in even a distance future. Accordingly, as a more realistic goal, we may instead work over a global integral version of this adelic theory. That is to say, we only work over finite rank  $\mathcal{O}_F$ -lattices  $\Lambda = (P, \rho)$ , or the same, the metrized locally free sheaves of finite rank over arithmetic curves  $\overline{X} = \overline{\mathrm{Spec}}\mathcal{O}_F$ . Here  $P$  denotes a projective  $\mathcal{O}_F$ -module of finite rank  $N = 2^n$  over the ring of integers  $\mathcal{O}_F$  of  $F$ , and  $\rho$  denotes a compatible metric on the

---

<sup>2</sup>For example, we may viewed both upper half plane  $\mathcal{H} = \mathbb{R}|0\rangle + \mathbb{R}_{\geq 0}|1\rangle$  and 3-dimensional hyperbolic upper half-space  $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}_{\geq 0}j$  as topological subspaces in  $\mathcal{H} = \mathbb{C}|0\rangle + \mathbb{C}|1\rangle$ . Despite the fact they are not vector subspaces, the action on these subspaces by global quantum gates still make perfect sense.

Minkowski space

$$\begin{aligned}
P &\simeq \mathcal{O}_F^{N-1} \oplus \mathfrak{a} \hookrightarrow \bigoplus_{k_1, k_2, \dots, k_n \in \{0,1\}} \binom{k_n \dots k_2 k_1}{k_1, k_2, \dots, k_n} F |k_n \dots k_2 k_1\rangle \\
&\hookrightarrow \bigoplus_{k_1, k_2, \dots, k_n \in \{0,1\}} \binom{k_n \dots k_2 k_1}{k_1, k_2, \dots, k_n} F_\infty |k_n \dots k_2 k_1\rangle \\
&= \bigoplus_{k_1, k_2, \dots, k_n \in \{0,1\}} \binom{k_n \dots k_2 k_1}{k_1, k_2, \dots, k_n} (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}) |k_n \dots k_2 k_1\rangle \\
&=: \mathcal{H}_{\text{glo}}^n.
\end{aligned} \tag{10}$$

Here  $\mathfrak{a}$  denotes a fractional ideal of  $F$ , and  $r_1$ , resp.  $r_2$  denotes the number of real, resp. complex places of  $F^3$ . A element  $x \in \mathcal{H}_{\text{glo}}$  is called a state vector and a state vector  $x$  is called normalized if  $x$  is in an Minkowski image of  $P$ . In this way, we are lead to build up global quantum gates through elements of  $\text{GL}_N(\mathcal{O}_F)$ . Since  $\text{GL}_N(\mathcal{O}_F)$  is known to be of finitely generated, global (quantum) gates satisfy universality property.

To simplify our presentation, let us assume that  $F = \mathbb{Q}$ , the field of rationals. Then the fact that global quantum gates enjoy the universality property can be justified as follows. For  $N = 2$ ,  $\text{GL}_2(\mathbb{Z})$  is well known to be generated by

$$\left\{ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

More generally, thanks to Hua and Reiner ([4]), we know that  $\text{GL}_N(\mathbb{Z})$  is generated by two elements. To be more precise, for any positive integer  $m$ , the general linear group  $\text{GL}_m(\mathbb{Z})$  of size  $m$  is generated by  $X$  and  $P$  when  $m$  is even and by  $-X$  and  $P$  when  $m$  is odd. Here

$$X = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, P = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

In terms of lattices,  $X$  corresponds to the state swap, and  $P$  corresponds to the state shift. Since these gates can be realized classically, we may use classical computer to help us to understand this type of global quantum computings. In particular, these global gates are adelic quantum gates of finite type.

Similarly, then the reduction theory for reductive groups naturally enters into the picture. Classically, the theory is developed using Siegel sets. But the classical approach is not neat since nowhere precisely estimations are needed. In contrast, a new very much powerful approach is adopted in ([14] working over number fields, [16, 17] working over function fields) using stability, From this new approach, the involved fundamental domains and their associated cusps are classified and partitioned according to various levels the parabolic subgroups of the groups involved. Even in this sense, we hope that our discussions here on local and global quantum gates certainly opens a narrow door to these wonderful

<sup>3</sup>Indeed, since  $\mathcal{O}_F$  is a Dedekind domain, it is well known that for each fixed projective  $\mathcal{O}_F$ -module  $P$  of rank  $N$ , there exists a fractional ideal  $\mathfrak{a}(P)$  of  $F$  such that as  $\mathcal{O}_F$ -modules,  $P \simeq \mathcal{O}_F^{N-1} \oplus \mathfrak{a}(P)$ . For details, see e.g. [14].



parallel worlds with vast fertile lands and rich structures, and that the studies on what might be called local  $p$ -adic quantum computers and global adelic quantum computers would become more and more attractive.

**Acknowledgement.** We would like to thank Zhan SHI for his discussions, during which a slip in the first version was detected.

## References

- [1] D. Bohm, *Quantum Theory*, Prentice-Hall, Inc. 1951
- [2] J. Elstrodt, F. Grunewald, J.Mennicke, *Groups Acting on Hyperbolic Spaces: Harmonic Analysis and Number Theory*, Springer 1997
- [3] K. Fujii, *Amazing Quantum Computer*, (in Japanese) Iwanami Shoten, 2019
- [4] L.K. Hua, I. Reiner, Automorphisms of the unimodular group. *Trans. Amer. Math. Soc.* 71 (1951), 331-348.
- [5] S. Ishizaka, T. Ogawa, R. Kawauchi, G. Kimura, M. Hayashi, *Introduction to Quantum Information Science*, (in Japanese) Kyoritsu Shuppan, 2012
- [6] A. Khrennikov, Interpretations of probability and their  $p$ -adic extensions, (in Russian) *Teor. Veroyatnost. i Primenen.* 46 (2001), no. 2, 311-325; translation in *Theory Probab. Appl.* 46 (2003), no. 2, 256-273
- [7] M. Kneser, Strong approximation, *Algebraic Groups and Discontinuous Subgroups* (Proc. Sympos. Pure Math., Boulder, Colo., 1965), Providence, R.I.: American Mathematical Society, pp. 187-196
- [8] G. Margulis, Cobounded subgroups in algebraic groups over local fields, *Akademiya Nauk SSSR. Funkcional'nyi Analiz i ego Prilozeniya*, 11 (2): 45-57
- [9] T. Mounkoro, Some subgroups of the general linear group of order two over the ring of  $p$ -adic integers.  *$p$ -Adic Numbers Ultrametric Anal. Appl.* 6 (2014), no. 3, 219-234.
- [10] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition, Cambridge University Press, 2010
- [11] V. Platonov, The problem of strong approximation and the Kneser-Tits hypothesis for algebraic groups, *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya* 33, 1211-1219
- [12] V. Platonov, A. Rapinchuk, *Algebraic groups and number theory*. (Translated from the 1991 Russian original by Rachel Rowen.), *Pure and Applied Mathematics*, 139, Boston, MA: Academic Press
- [13] G. Prasad, Strong approximation for semi-simple groups over function fields, *Annals of Mathematics, Second Series*, 105 (3): 553-572
- [14] L. WENG, *Zeta Functions of Reduction Groups and Their Zeros*, World Scientific, 2018

- [15] L. WENG, Non-Abelian Zeta Function, Fokker-Planck Equation and Projectively Flat Connection, arXiv:1903.03604
- [16] L. WENG, D.Zagier, Higher rank zeta functions for elliptic curves, Proc. Natl. Acad. Sci. USA 117 (2020), no.9, 4546-4558
- [17] L. WENG, D.Zagier, Higher rank zeta functions and  $SL_n$ -zeta functions for curves, Proc. Natl. Acad. Sci. USA 117 (2020), no.12, 6279-6281
- [18] M.S. Ying, *Foundations of Quantum Programming*, Elsevier, 2016

Lin WENG  
Graduate School of Mathematics,  
Kyushu University,  
Fukuoka 819-0395,  
JAPAN  
E-Mail: weng@math.kyushu-u.ac.jp