


PAPER

# Elementary quantum recursion schemes that capture quantum polylogarithmic-time computability of quantum functions<sup>a</sup>

Tomoyuki Yamakami 

Faculty of Engineering, University of Fukui, Fukui, Japan  
Email: [TomoyukiYamakami@gmail.com](mailto:TomoyukiYamakami@gmail.com)

(Received 20 March 2023; revised 19 July 2024; accepted 21 July 2024)

## Abstract

Quantum computing has been studied over the past four decades based on two computational models of quantum circuits and quantum Turing machines. To capture quantum polynomial-time computability, a new recursion-theoretic approach was taken lately by Yamakami [J. Symb. Logic 80, pp. 1546–1587, 2020] by way of recursion schematic definition, which constitutes six initial quantum functions and three construction schemes of composition, branching, and multi-qubit quantum recursion. By taking a similar approach, we look into quantum polylogarithmic-time computability and further explore the expressing power of elementary schemes designed for such quantum computation. In particular, we introduce an elementary form of the quantum recursion, called the fast quantum recursion, and formulate *EQS* (elementary quantum schemes) of “elementary” quantum functions. This class *EQS* captures exactly quantum polylogarithmic-time computability, which forms the complexity class *BQPOLYLOGTIME*. We also demonstrate the separation of *BQPOLYLOGTIME* from *NLOGTIME* and *PPOLYLOGTIME*. As a natural extension of *EQS*, we further consider an algorithmic procedural scheme that implements the well-known divide-and-conquer strategy. This divide-and-conquer scheme helps compute the parity function, but the scheme cannot be realized within our system *EQS*.

**Keywords:** Recursion schematic definition; quantum Turing machine; fast quantum recursion; quantum polylogarithmic-time computability; divide-and-conquer strategy

## 1. Background, motivations, and challenges

We provide a quick overview of this work from its background to challenging open questions to tackle.

### 1.1 Recursion schematic definitions that capture quantum computability

Over the four decades, the study of quantum computing has made significant progress in both theory and practice. Quantum computing is one of the most anticipated nature-inspired computing paradigms today because it relies on the principle of quantum mechanics, which is assumed to govern nature. The core of quantum computing is an exquisite handling of *superpositions*, which

<sup>a</sup>A preliminary report (Yamakami, 2022b) has appeared under a slightly different title in the Proceedings of the 28th International Conference on Logic, Language, Information, and Computation (WoLLIC 2022), Iași, Romania, September 20–23, 2022, Lecture Notes in Computer Science, vol. 13468, pp. 88–104, Springer, 2022.

are linear combinations of basic quantum states expressing classical strings, and *entanglement*, which binds multiple quantum bits (or qubits, for short) with no direct contact, of quantum states. Early models of quantum computation were proposed by Benioff (1980), Deutsch (1985, 1989), and Yao (1993) as quantum analogs of Turing machines and Boolean circuits. Those models have been used in a theoretical study of quantum computing within the area of computational complexity theory since their introduction. The quantum Turing machine (QTM) model is a natural quantum extension of the classical Turing machine (TM) model, which has successfully served for decades as a basis to theoretical aspects of computer science. The basic formulation of the QTM model<sup>1</sup> used today attributes to Bernstein and Vazirani (1997). QTMs provide a blueprint of algorithmic procedures by describing how to transform each superposition of configurations of the machines. There have been other computational models proposed to capture different aspects of quantum computing, including a (black-box) query model.

A *recursion schematic approach* has been a recent incentive for the full characterization of the notion of quantum polynomial-time computability (Yamakami, 2020), which can be seen as a quantum extension of deterministic polynomial-time computability. The primary purpose of taking such an exceptional approach toward quantum computability stems from a successful development of recursion theory (or recursive function theory) for classical computability. Earlier, Peano, Herbrand, Gödel, and Kleene (1936, 1943) all made significant contributions to paving a straight road to a coherent study of computability and decidability from a purely logical aspect (see, e.g., (Soare, 1996) for further references therein). In this theory, recursive functions are formulated in the following simple “schematic” way. (i) We begin with a few initial functions. (ii) We sequentially build more complicated functions by applying a small set of construction schemes to the already-built functions. The description of how to construct a recursive function actually serves as a blueprint of the function, which resembles like a “computer program” of the modern times in such a way that each construction scheme is a command line of a computer program. Hence, a schematic definition itself may be viewed as a high-level programming language by which we can render a computer program that describes the movement of any recursive function. As the benefit of the use of such a schematic definition, when we express a target function as a series of schemes, the “size” of this series can serve as a “descriptive complexity measure” of the function. This has led to a fully enriched study of the descriptive complexity of functions. This schematic approach sharply contrasts the ones based on Turing machines as well as Boolean circuit families to formulate the recursive functions. A similar approach taken by Yamakami (2020) aims at capturing the polynomial-time computability of *quantum functions*,<sup>2</sup> each of which maps a finite-dimensional Hilbert space to itself, in place of the aforementioned recursive functions. Unlike quantum transitions of QTMs, the recursion schemes can provide a clear view of how quantum transforms act on target quantum states in the Hilbert space.

Two important classes of quantum functions, denoted  $\square_1^{\text{QP}}$  and  $\widehat{\square}_1^{\text{QP}}$ , were formulated by Yamakami (2020) from six initial quantum functions and three basic construction schemes. The major difference between  $\square_1^{\text{QP}}$  and  $\widehat{\square}_1^{\text{QP}}$  is the permitted use of *quantum measurement operations*, which make quantum states collapse to classical states with incurred probabilities. Unfortunately, this is a non-reversible operation. Shown by Yamakami (2020) are a precise characterization of quantum polynomial-time computability and a quantum analog of the normal form theorem. A key in his recursion schematic definition is an introduction of the *multi-qubit quantum recursion scheme*, which looks quite different in its formulation from the corresponding classical recursion scheme. We will give its formal definition in Section 3.1 as *Scheme T*. This quantum recursion scheme turns out to be so powerful that it has helped us capture the notion of quantum polynomial-time computability.

There are a few but important advantages of using recursion schematic definitions to introduce the notion of quantum computation over other quantum computational models, such as QTMs and quantum circuits. The most significant advantage is in fact that there is no use of the

*well-formedness requirement* of QTMs and the *uniformity requirement* of quantum circuit families. These natural but cumbersome requirements are necessary to guarantee the unitary nature of QTMs and the algorithmic construction of quantum circuit families. Recursion schematic definitions, on the contrary, avoid such extra requirements and make it much simpler to design a quantum algorithm in the form of a quantum function for solving a target combinatorial problem. This is because each basic scheme naturally embodies “well-formedness” and “uniformity” in its formulation. More accurately, the scheme produces only “well-formed” and “uniform” quantum functions by way of applying the scheme directly to the existing quantum functions. In fact, the schematic definition of Yamakami (2020) constitutes only six initial quantum functions together with three basic construction schemes and this fact helps us render a short procedural sequence of how to construct each target quantum function. A descriptive aspect of the recursion schematic definition of Yamakami (2020) has become a helpful guide to develop even a suitable form of quantum programming language (Hainry et al., 2023). It is worth mentioning that such a recursion schematic definition has been made possible because of an extensional use of the bra and ket notations. See Section 2.3 for detailed explanations.

A schematic approach of Yamakami (2020) to quantum computing has exhibited a great possibility of treating quantum computable functions in such a way that is quite different from the traditional ways with QTMs and quantum circuit families. Recursion schemes further lead us to the descriptive complexity of quantum functions. Concerning such recursion schematic definitions, numerous questions still remain unanswered. It is important and also imperative to expand the scope of our research to various resource-bounded quantum computing. In this work, we particularly wish to turn our attention to a “limited” form of quantum computing, which can be naturally implemented by small runtime-restricted QTMs as well as families of small depth-bounded quantum circuits, and we further wish to examine how the schematic approach of Yamakami (2020) copes with such restricted quantum computing.

Of practical importance, resource-bounded computability has been studied in the classical setting based on various computational models, including families of Boolean circuits and time-bounded (classical) Turing machines (or TMs, for short). Among all reasonable resource bounds, we are particularly keen to *(poly)logarithmic time*. The logarithmic-time (abbreviated as logtime) computability may be one of the most restricted but meaningful, practical resource-bounded computabilities and it was discussed earlier by Buss (1987) and Barrington et al. (1990) in terms of TMs equipped with index tapes to access particular locations of input symbols. Hereafter, we denote by DLOGTIME (resp., NLOGTIME) the class of decision problems solvable by logtime deterministic (resp., nondeterministic) TMs. The logtime computability has played a central role in characterizing a uniform notion of constant-depth Boolean circuit families. As shown by Barrington et al. (1990), logtime computability is also closely related to the first-order logic with the special predicate *BIT*. As slightly more general resource-bounded computability, *polylogarithmic-time* (abbreviated as *polylogtime*) computability has been widely studied in the literature. Numerous polylogtime algorithms were developed to solve, for example, the matrix chain ordering problem (Bradford et al., 1994) and deterministic graph construction (Holm et al., 2001). There were also studies on data structures that support polylog operations (Munro, 1984) and probabilistic checking of polylog bits of proofs (Babai et al., 1991). We denote by PPOLYLOGTIME the complexity class of decision problems solvable by polylogtime probabilistic TMs with unbounded-error probability.

In the setting of quantum computing, nevertheless, we are able to take a similar approach using resource-bounded QTMs. A quantum analog of DLOGTIME, called BQLOGTIME, was lately discussed in connection to an oracle separation between BQP and the polynomial hierarchy in (Raz and Tal, 2022). In this work, however, we are interested in polylogtime-bounded quantum computations, and thus we wish to look into the characteristics of quantum polylogtime computability. Later in Section 5.1, we formally describe the fundamental model of *polylogtime QTMs* as a quantum analog of classical polylogtime TMs. These polylogtime QTMs naturally

induce the corresponding bounded-error complexity class BQPOLYLOGTIME. In Section 5.2, BQPOLYLOGTIME is shown to differ in computational power from NLOGTIME as well as PPOLYLOGTIME.

### 1.2 Our challenges in this work

We intend to extend the scope of the existing research on resource-bounded quantum computability by way of an introduction of a small set of recursion schemes defining runtime-restricted quantum computability. In particular, we look into quantum polylogtime computability and seek out an appropriate recursion schematic definition to exactly capture such computability.

Since  $\square_1^{\text{QP}}$  and  $\overline{\square}_1^{\text{QP}}$  precisely capture quantum polynomial-time computability, it is natural to raise a question of how we can capture quantum polylogtime computability in a similar fashion.

As noted earlier, the multi-qubit quantum recursion scheme of Yamakami (2020) is capable of precisely capturing quantum polynomial-time computability. A basic idea of this quantum recursion scheme is, starting with  $n$  qubits, to modify at each round of recursion the first  $k$  qubits and continue to the next round with the rest of the qubits after discarding the first  $k$  qubits. This recursive process slowly consumes the entire  $n$  qubits and finally grinds to halt after linearly-many recursive rounds. To describe limited quantum computability, in contrast, how can we weaken the quantum recursion scheme? Our attempt in this work is to speed up this recursive process significantly by discarding a bundle of  $\lceil n/2 \rceil$  (or  $\lfloor n/2 \rfloor$ ) qubits from the entire  $n$  qubits at each round. Such a way of halving the number of qubits at each recursive round makes the recursive process terminate significantly faster; in fact, ending in at most  $\lceil \log n \rceil$  recursive rounds. For this very reason, we intend to call this weakened recursive process the (*code-controlled*) *fast quantum recursion scheme*.

Although the fast quantum recursion scheme is significantly weaker in power than the quantum recursion scheme of Yamakami (2020), the scheme still generates numerous interesting and useful quantum functions, as listed in Lemmas 4–8 and 15–22. More importantly, it is possible to implement the binary search strategy, which has been a widely used key programming technique. We call the set of all quantum functions generated from six initial quantum functions and three construction schemes together with the fast quantum recursion scheme by EQS (elementary quantum schemes) in Section 3. This class EQS turns out to precisely characterize quantum polylogtime computability (Theorems 33–34).

To cope with polylogtime computability, we need an appropriate encoding of various types of “objects” (such as numbers, graphs, matrices, and tape symbols) into qubits of an equal length and also another efficient way of decoding the original “objects” from those encoded qubits. For this purpose, we introduce in Section 3.2 a code-skipping scheme, which recognizes encoded segments to skip them one by one. This scheme in fact plays a key role in performing the fast recursion scheme.

Throughout this work, we try to promote much better understandings of resource-bounded quantum computing in theory and in practice.

**New Materials after the Preliminary Conference Report.** The current work corrects and significantly alters the preliminary conference report (Yamakami, 2022b), particularly in the following points. Five schemes, which constitute EQS, in the preliminary report have been modified and reorganized, and thus they look slightly different in their formulations. In particular, Scheme V is introduced to establish a precise characterization of quantum functions computable by polylogtime QTMs.

Beyond the scope of the preliminary report (Yamakami, 2022b), this work further looks into another restricted quantum algorithmic procedure, known as the *divide-and-conquer strategy* in Section 6. A key idea behind this strategy is to inductively split an given instance into small pieces

and then inductively assemble them piece by piece after an appropriate modification. This new scheme helps us capture the parity function, which requires more than polylogtime quantum computation. This fact implies that this new procedure is not “realized” in the framework of EQS.

## 2. Preparation: notions and notation

We will briefly explain basic notions and notation used throughout this work.

### 2.1 Numbers, strings, and languages

The notations  $\mathbb{Z}$ ,  $\mathbb{Q}$ , and  $\mathbb{R}$  respectively denote the sets of all integers, of all rational numbers, and of all real numbers. In particular, we set  $\bar{\mathbb{Q}} = \mathbb{Q} \cap [0, 1]$ . The *natural numbers* are nonnegative integers and the notation  $\mathbb{N}$  expresses the set of those numbers. We further write  $\mathbb{N}^+$  to denote the set  $\mathbb{N} - \{0\}$ . For two integers  $m, n$  with  $m \leq n$ ,  $[m, n]_{\mathbb{Z}}$  indicates the *integer interval*  $\{m, m + 1, m + 2, \dots, n\}$ . In particular, we abbreviate  $[1, n]_{\mathbb{Z}}$  as  $[n]$  when  $n \geq 1$ . In addition,  $\mathbb{C}$  denotes the set of all complex numbers. We use the notations  $\lceil \cdot \rceil$  and  $\lfloor \cdot \rfloor$  for the ceiling function and the floor function, respectively. In this work, all *polynomials* have nonnegative integer coefficients and all *logarithms* are taken to the base 2. We further define  $\text{ilog}(n)$  and  $\text{iloglog}(n)$  to be  $\lceil \log n \rceil$  and  $\lceil \log \log n \rceil$  for any  $n \in \mathbb{N}$ , respectively. To circumvent any cumbersome description to avoid the special case of  $n = 0$ , we intentionally set  $\text{ilog}(0) = \text{iloglog}(0) = 0$ . The notation  $\iota$  denotes  $\sqrt{-1}$  and  $e$  does the base of natural logarithms. Given a complex number  $\alpha$ ,  $\alpha^*$  denotes the *complex conjugate* of  $\alpha$ . As for a nonempty set of quantum amplitudes, which is a subset of  $\mathbb{C}$ , we use the notation  $K$ .

A nonempty finite set of “symbols” (or “letters”) is called an *alphabet* and a sequence of such symbols from a fixed alphabet  $\Sigma$  is called a *string* over  $\Sigma$ . The total number of occurrences of symbols in a given string  $x$  is the *length* of  $x$  and is denoted  $|x|$ . The *empty string*  $\lambda$  is a unique string of length 0. A collection of those strings over  $\Sigma$  is a *language* over  $\Sigma$ . Throughout this work, we deal only with *binary strings*, which are sequences of 0s and 1s. Given a number  $n \in \mathbb{N}$ ,  $\Sigma^n$  (resp.,  $\Sigma^{\leq n}$ ) denotes the set of all strings of length exactly  $n$  (resp., at most  $n$ ). Let  $\Sigma^* = \bigcup_{n \in \mathbb{N}} \Sigma^n$  and  $\Sigma^+ = \Sigma^* - \{\lambda\}$ . Given a string  $x$  and a bit  $b \in \{0, 1\}$ , the notation  $\#_b(x)$  denotes the total number of occurrences of the symbol  $b$  in  $x$ . Due to the nature of quantum computation, we also discuss “promise” decision problems. A pair  $(A, R)$  of subsets of  $\Sigma^*$  is said to be a *promise (decision) problem* over  $\Sigma$  if  $A \cup R \subseteq \Sigma^*$  and  $A \cap R = \emptyset$ . Intuitively,  $A$  and  $R$  are, respectively, composed of accepted strings and rejected strings. When  $A \cup R = \Sigma^*$ ,  $(A, R)$  becomes  $(A, \Sigma^* - A)$ , and this can be identified with the language  $A$ .

Given a number  $n \in \mathbb{N}$ , we need to partition it into two halves. To describe the “left half” and the “right half” of  $n$ , we introduce two special functions:  $LH(n) = \lceil n/2 \rceil$  and  $RH(n) = \lfloor n/2 \rfloor$ .

For a function  $f$  and a number  $k \in \mathbb{N}^+$ , we write  $f^k$  for the  $k$  consecutive applications of  $f$  to an input. For example,  $f^2(x) = f \circ f(x) = f(f(x))$  and  $f^3(x) = f \circ f \circ f(x) = f(f(f(x)))$ . The functions  $LH$  and  $RH$  satisfy the following property.

**Lemma 1.** *Let  $k, n \in \mathbb{N}^+$  be any two numbers. (1) If  $n$  is in  $[2^{k-1} + 1, 2^k]_{\mathbb{Z}}$  (i.e.,  $\lceil \log n \rceil = k$ ), then  $LH^k(n) = 1$  holds. Moreover, if  $k \geq 2$ , then  $LH^{k-1}(n) = 2$ . (2) If  $n$  is in  $[2^k, 2^{k+1} - 1]_{\mathbb{Z}}$  (i.e.,  $\lfloor \log n \rfloor = k$ ), then  $RH^k(n) = 1$  holds. Moreover, if  $k \geq 2$ , then  $RH^{k-1}(n) \in \{2, 3\}$ .*

*Proof.* (1) Consider a series:  $n, LH(n), LH^2(n), \dots, LH^k(n)$ . It follows that, for any number  $n > 2$ ,  $n \in [2^{k-1} + 1, 2^k]_{\mathbb{Z}}$  iff  $LH(n) \in [2^{k-2} + 1, 2^{k-1}]_{\mathbb{Z}}$ . Thus, we obtain  $LH^{k-1}(n) \in \{2\}$  and  $LH^k(n) \in \{1\}$ . When  $n \geq 3$ , the last two numbers of the above series must be 2 and 1.

(2) In a similar fashion to (1), let us consider a series:  $n, RH(n), RH^2(n), \dots, RH^k(n)$ . It then follows that  $n \in [2^k, 2^{k+1} - 1]_{\mathbb{Z}}$  iff  $RH(n) \in [2^{k-1}, 2^k - 1]_{\mathbb{Z}}$ . We then obtain  $RH^{k-1}(n) \in \{2, 3\}$  and  $RH^k(n) \in \{1\}$ . □

We assume the standard *lexicographical order* on  $\{0, 1\}^*$ :  $\lambda, 0, 1, 00, 01, 10, 11, 000, \dots$  and, based on this ordering, we assign natural numbers to binary strings as  $bin(0) = \lambda, bin(1) = 0, bin(2) = 1, bin(3) = 00, bin(4) = 01, bin(5) = 10, bin(6) = 11, bin(7) = 000$ , etc. In contrast, for a fixed number  $k \in \mathbb{N}^+$ ,  $bin_k(n)$  denotes lexicographically the  $n$ th string in  $\{0, 1\}^k$  as long as  $n \in [2^k]$ . For instance, we obtain  $bin_3(1) = 000, bin_3(2) = 001, bin_3(3) = 010, bin_3(4) = 011$ , etc. Remember that  $bin_k(0)$  is not defined whereas  $bin(0)$  means  $\lambda$ .

**2.2 Quantum States and Hilbert spaces**

We assume the reader’s familiarity with basic quantum information and computation (see, e.g., textbooks (Kitaev et al., 2002; Nielsen and Chuang, 2016)). A basic concept in quantum computing is a Hilbert space and unitary transformations over it. The *ket notation*  $|\phi\rangle$  expresses a (column) vector in a Hilbert space and its transposed conjugate is expressed as a (row) vector of the dual space and is denoted by the *bra notation*  $\langle\phi|$ . The notation  $\langle\psi|\phi\rangle$  denotes the *inner product* of two vectors  $|\psi\rangle$  and  $|\phi\rangle$ . We use the generic notation  $I$  to denote the identity matrix of an arbitrary dimension. A square complex matrix  $U$  is called *unitary* if  $U$  satisfies  $UU^\dagger = U^\dagger U = I$ , where  $U^\dagger$  is the transposed conjugate of  $U$ .

The generic notation  $\mathbf{0}$  is used to denote the *null vector* of an arbitrary dimension. A *quantum bit* (or a *qubit*, for short) is a linear combination of two basis vectors  $|0\rangle$  and  $|1\rangle$ . The notation  $\mathcal{H}_2$  indicates the Hilbert space spanned by  $|0\rangle$  and  $|1\rangle$ . More generally,  $\mathcal{H}_{2^n}$  refers to the Hilbert space spanned by the computational basis  $B_n = \{|s\rangle \mid s \in \{0, 1\}^n\}$ . For convenience, we write  $\mathcal{H}_\infty$  for the collection of all quantum states in  $\mathcal{H}_{2^n}$  for any  $n \in \mathbb{N}^+$ . Remember that  $\mathcal{H}_\infty$  does not form a Hilbert space. Given a non-zero quantum state  $|\phi\rangle \in \mathcal{H}_\infty$ , its *length*  $\ell(|\phi\rangle)$  denotes a unique number  $n \in \mathbb{N}$  for which  $|\phi\rangle \in \mathcal{H}_{2^n}$ . We stress that the length of  $|\phi\rangle$  is defined only for a quantum state residing in  $\mathcal{H}_\infty$ . As a special case, we set  $\ell(\mathbf{0}) = 0$  for the null vector  $\mathbf{0}$  (although  $\mathbf{0}$  belongs to  $\mathcal{H}_k$  for any  $k \in \mathbb{N}^+$ ). For convenience, we also set  $\ell(\alpha) = 0$  for any scalar  $\alpha \in \mathbb{C}$ . For a quantum state  $|\phi\rangle$ , if we make a measurement in the computational basis, then each binary string  $x$  of length  $\ell(|\phi\rangle)$  is observed with probability  $|\langle x|\phi\rangle|^2$ . Thus,  $|\phi\rangle$  can be expressed as  $|0\rangle\langle 0|\phi\rangle + |1\rangle\langle 1|\phi\rangle$  and also as  $\sum_{x \in \{0,1\}^n} |x\rangle \otimes \langle x|\phi\rangle$ , where  $|\phi\rangle \otimes |\psi\rangle$  is the *tensor product* of  $|\phi\rangle$  and  $|\psi\rangle$ . The *norm* of  $|\phi\rangle$  is defined as  $\sqrt{\langle\phi|\phi\rangle}$  and is denoted  $\| |\phi\rangle \|$ .

A *qustring of length n* is a unit-norm quantum state in  $\mathcal{H}_{2^n}$ . As a special case, the null vector is treated as the *qustring of length 0* (although its norm is 0). Let  $\Phi_n$  denote the set of all qustrings of length  $n$ . Clearly,  $\Phi_n \subseteq \mathcal{H}_{2^n}$  holds for all  $n \in \mathbb{N}^+$ . We then set  $\Phi_\infty$  to be the collection of all qustrings of length  $n$  for any  $n \in \mathbb{N}$ .

Abusing the aforementioned notations of  $LH(n)$  and  $RH(n)$ , we set  $LH(|\phi\rangle) = \lceil \ell(|\phi\rangle)/2 \rceil$  and  $RH(|\phi\rangle) = \lfloor \ell(|\phi\rangle)/2 \rfloor$  for any quantum state  $|\phi\rangle \in \mathcal{H}_\infty$ . It then follows that  $\ell(|\phi\rangle) = LH(|\phi\rangle) + RH(|\phi\rangle)$ .

We are interested only in functions mapping  $\mathcal{H}_\infty$  to  $\mathcal{H}_\infty$ , and these functions are generally referred to as *quantum functions on  $\mathcal{H}_\infty$*  to differentiate from “functions” working with natural numbers or strings. Such a quantum function  $f$  is said to be *dimension-preserving* (resp., *norm-preserving*) if  $\ell(|\phi\rangle) = \ell(f(|\phi\rangle))$  (resp.,  $\| |\phi\rangle \| = \| f(|\phi\rangle) \|$ ) holds for any quantum state  $|\phi\rangle \in \mathcal{H}_\infty$ .

**2.3 Conventions on the bra and the ket notations**

To calculate the outcomes of quantum functions on  $\mathcal{H}_\infty$ , we must take advantage of making a purely symbolic treatment of the bra and the ket notations together with the tensor product



notation  $\otimes$ . We generally follow (Yamakami, 2020) for the conventions on the specific usage of these notations. These notational conventions in fact help us simplify the description of various qubit operations in later sections. Since we greatly deviate from the standard usage of those notations, hereafter, we explain how to use them throughout this work.

It is important to distinguish between the number 0 and the null vector  $\mathbf{0}$ . To deal with the null vector, we conveniently take the following specific conventions concerning the operator “ $\otimes$ ”. For any  $|\phi\rangle \in \mathcal{H}_\infty$ , (i)  $0 \otimes |\phi\rangle = |\phi\rangle \otimes 0 = \mathbf{0}$  (scalar case), (ii)  $|\phi\rangle \otimes \mathbf{0} = \mathbf{0} \otimes |\phi\rangle = \mathbf{0}$ , and (iii) if  $|\psi\rangle$  is the null vector, then  $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle = \mathbf{0}$ . In the case of (i), we here extend the standard usage of  $\otimes$  to even cover “scalar multiplication” to simplify later calculations. Given two binary strings  $u, s \in \{0, 1\}^+$ , if  $|s| = |u|$ , then  $\langle u|s\rangle = 1$  if  $u = s$ , and  $\langle u|s\rangle = 0$  otherwise. On the contrary, when  $|u| < |s|$ ,  $\langle u|s\rangle$  expresses the quantum state  $|z\rangle$  if  $s = uz$  for a certain string  $z$ , and  $\mathbf{0}$  otherwise. By sharp contrast, if  $|u| > |s|$ , then  $\langle u|s\rangle$  always denotes  $\mathbf{0}$ . More generally, if  $|\phi\rangle = \sum_{u \in \{0,1\}^n} \sum_{s \in \{0,1\}^m} \alpha_{u,s} |u\rangle \otimes |s\rangle$  and  $u_0 \in \{0, 1\}^n$ , then  $\langle u_0|\phi\rangle$  expresses the quantum state  $\sum_{s \in \{0,1\}^m} \alpha_{u_0,s} |s\rangle$ . For instance, if  $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ , then  $\langle 0|\phi\rangle$  equals  $\frac{1}{\sqrt{2}}|0\rangle$  and  $\langle 1|\phi\rangle$  does  $\frac{1}{\sqrt{2}}|1\rangle$ . These notations  $\langle 0|\phi\rangle$  and  $\langle 1|\phi\rangle$  together make it possible to express any qustring  $|\phi\rangle$  as  $|0\rangle \otimes \langle 0|\phi\rangle + |1\rangle \otimes \langle 1|\phi\rangle$ . In a more general case with  $|\xi\rangle = \sum_{u \in \{0,1\}^n} \beta_u |u\rangle$ ,  $\langle \xi|\phi\rangle$  means  $\sum_{u \in \{0,1\}^n} \beta_u^* \langle u|\phi\rangle$ , which equals  $\sum_{u \in \{0,1\}^n} \sum_{s \in \{0,1\}^m} \alpha_{u,s} \beta_u^* |s\rangle$ . Moreover,  $|\phi\rangle$  can be expressed as  $\sum_{u \in \{0,1\}^n} \beta_u |u\rangle \otimes \langle u|\phi\rangle$ . We often abbreviate  $|\phi\rangle \otimes |\psi\rangle$  as  $|\phi\rangle|\psi\rangle$ . In particular, for strings  $s$  and  $u$ ,  $|s\rangle \otimes |u\rangle$  is further abbreviated as  $|s, u\rangle$  or even  $|su\rangle$ . When  $\langle s|\phi\rangle$  is just a scalar, say,  $\alpha \in \mathbb{C}$ , the notation  $|s\rangle \otimes \langle s|\phi\rangle$  (or equivalently,  $|s\rangle\langle s|\phi\rangle$ ) is equal to  $\alpha|s\rangle$ .

We also expand the norm notation  $\|\cdot\|$  for vectors to scalars in the following way. For any quantum states  $|\phi\rangle$  and  $|\psi\rangle$  with  $\ell(|\phi\rangle) = \ell(|\psi\rangle) > 0$ , the notation  $\|\langle\phi|\psi\rangle\|$  is used to express the absolute value  $|\langle\phi|\psi\rangle|$ . In general, for any scalar  $\alpha \in \mathbb{C}$ ,  $\|\alpha\|$  denotes  $|\alpha|$ . This notational convention is quite useful in handling the value obtained after making a measurement without worrying about whether the resulting object is a quantum state or a scalar.

Later, we will need to encode (or translate) a series of symbols into an appropriate qustring. In such an encoding, the empty string  $\lambda$  is treated quite differently. Notably, we tend to automatically translate  $|\lambda\rangle$  into the null vector  $\mathbf{0}$  unless otherwise stated.

### 3. A recursion schematic definition of EQS

We will present a recursion schematic definition to formulate a class of special quantum functions on  $\mathcal{H}_\infty$  (i.e., from  $\mathcal{H}_\infty$  to  $\mathcal{H}_\infty$ ), later called EQS. To improve the readability, we first provide a skeleton system of EQS and later we expand it to the full-fledged system.

#### 3.1 Skeleton EQS

As a starter, we discuss a “skeleton” of our recursion schematic definition for “elementary” quantum functions, which are collectively called EQS (elementary quantum schemes) in Definition 20, involving six initial quantum functions and two construction schemes. All initial quantum functions were already presented when defining  $\square_1^{\text{QP}}$  and  $\widehat{\square}_1^{\text{QP}}$  in (Yamakami, 2020).

Throughout the rest of this work, we fix a nonempty amplitude set  $K$ , and we often omit the clear reference to  $K$  as long as the choice of  $K$  is not important in our discussion.

**Definition 2.** *The skeleton class EQS<sub>0</sub> is composed of all quantum functions constructed by selecting the initial quantum functions of Scheme I and then inductively applying Schemes II–III a finite number of times. In what follows,  $|\phi\rangle$  denotes an arbitrary quantum state in  $\mathcal{H}_\infty$ . When the item 6) of Scheme I is not used, we denote the resulting class by EQS<sub>0</sub>.*

I. The initial quantum functions. Let  $\theta \in [0, 2\pi) \cap K$  and  $a \in \{0, 1\}$ .

- 1)  $I(|\phi\rangle) = |\phi\rangle$ . (identity)
- 2)  $PHASE_\theta(|\phi\rangle) = |0\rangle\langle 0|\phi\rangle + e^{i\theta}|1\rangle\langle 1|\phi\rangle$ . (phase shift)
- 3)  $ROT_\theta(|\phi\rangle) = \cos \theta|\phi\rangle + \sin \theta(|1\rangle\langle 0|\phi\rangle - |0\rangle\langle 1|\phi\rangle)$ . (rotation around  $xy$ -axis at angle  $\theta$ )
- 4)  $NOT(|\phi\rangle) = |0\rangle\langle 1|\phi\rangle + |1\rangle\langle 0|\phi\rangle$ . (negation)
- 5)  $SWAP(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ \sum_{a,b \in \{0,1\}} |ab\rangle\langle ba|\phi\rangle & \text{otherwise.} \end{cases}$  (swapping of 2 qubits)
- 6)  $MEAS[a](|\phi\rangle) = |a\rangle\langle a|\phi\rangle$ . (partial projective measurement)

II. The composition scheme. From  $g$  and  $h$ , we define  $Compo[g, h]$  as follows:  $Compo[g, h](|\phi\rangle) = g \circ h(|\phi\rangle)$  ( $= g(h(|\phi\rangle))$ ).

III. The branching scheme.<sup>3</sup> From  $g$  and  $h$ , we define  $Branch[g, h]$  as:

- (i)  $Branch[g, h](|\phi\rangle) = |\phi\rangle$  if  $\ell(|\phi\rangle) \leq 1$ ,
- (ii)  $Branch[g, h](|\phi\rangle) = |0\rangle \otimes g(|0\rangle|\phi\rangle) + |1\rangle \otimes h(|1\rangle|\phi\rangle)$  otherwise.

We remark that all quantum functions in Items 1)–4) and 6) in Scheme I directly manipulate only the first qubit of  $|\phi\rangle$  and that  $SWAP$  manipulates the first two qubits of  $|\phi\rangle$ . All other qubits of  $|\phi\rangle$  are intact. Notice that the length function  $\ell(|\phi\rangle)$  is not included as part of  $EQS_0$ . Since  $|\phi\rangle$  is always taken from  $\mathcal{H}_\infty$ , the value  $\ell(|\phi\rangle)$  is uniquely determined from  $|\phi\rangle$ . It is also important to remark that, for any  $|\phi\rangle$  and  $a \in \{0, 1\}$ ,  $\ell(MEAS[a](|\phi\rangle)) = \ell(|\phi\rangle)$ .

In Schemes II and III, the constructions of  $Compo[g, h]$  and  $Branch[g, h]$  need two quantum functions,  $g$  and  $h$ , which are assumed to have been already constructed in their own construction processes. To refer to these supporting quantum functions used in the scheme, we call them the ground (quantum) functions of  $Compo[g, h]$  and  $Branch[g, h]$ . In the case of a special need to emphasize  $K$ , we write  $EQS_{K,0}$  and  $\bar{E}QS_{K,0}$  with a clear reference to  $K$ .

We quickly provide simple examples of how to compute the quantum functions induced by appropriate applications of Schemes I–III.

**Example 3.** It follows that  $PHASE_\pi(|1\rangle) = -|1\rangle$  and  $PHASE_{\pi/2}(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ ,  $ROT_{\pi/4}(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  and  $ROT_{\pi/4}(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ ,  $NOT(|a\rangle) = |1 - a\rangle$ , and  $SWAP(|abc\rangle) = |bac\rangle$  for three bits  $a, b, c \in \{0, 1\}$ . We also obtain  $MEAS[0](ROT_{\pi/4}(|00\rangle)) = MEAS[0](\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle) = \frac{1}{\sqrt{2}}|00\rangle$ . As for Scheme III, it is important to note that  $Branch[g, g]$  is not the same as  $g$  itself. For example,  $Branch[NOT, NOT](|b\rangle|\phi\rangle)$  equals  $|b\rangle \otimes NOT(|\phi\rangle)$  by Scheme III(ii) whereas  $NOT(|b\rangle|\phi\rangle)$  is just  $|1 - b\rangle|\phi\rangle$ , where  $b$  denotes any bit. The EPR pair  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  is obtainable from  $|0\rangle|0\rangle$  as follows. By first applying  $ROT_{\pi/4}$  to  $|0\rangle|0\rangle$ , we obtain  $|\phi\rangle = ROT_{\pi/4}(|0\rangle|0\rangle)$ . We then apply  $Branch[I, NOT]$  and obtain  $Branch[I, NOT](|\phi\rangle) = Branch[I, NOT](\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) = |0\rangle \otimes I(\frac{1}{\sqrt{2}}|0\rangle) + |1\rangle \otimes NOT(\frac{1}{\sqrt{2}}|0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ .

For later reference, let us review from Yamakami (2020) the multi-qubit quantum recursion scheme, which is a centerpiece of schematically characterizing quantum polynomial-time computability. In this work, this special scheme is referred to as Scheme T.

(T) The multi-qubit quantum recursion scheme (Yamakami, 2020). Let  $g, h, p$  be quantum functions and let  $k, t \in \mathbb{N}^+$  be numbers. Assume that  $p$  is dimension-preserving. For  $\mathcal{F}_k = \{f_u\}_{u \in \{0,1\}^k}$ , we define  $F \equiv kQRec_t[g, h, p|\mathcal{F}_k]$  as follows:

- (i)  $F(|\phi\rangle) = g(|\phi\rangle)$  if  $\ell(|\phi\rangle) \leq t$ ,
  - (ii)  $F(|\phi\rangle) = h(\sum_{u:|u|=k} |u\rangle \otimes f_u(\langle u|\psi_{p,\phi}\rangle))$  otherwise,
- where  $|\psi_{p,\phi}\rangle = p(|\phi\rangle)$  and  $f_u \in \{F, I\}$  for any  $u \in \{0, 1\}^k$ .



This quantum recursion scheme together with Schemes I–III given above and another quantum function called REMOVE (removal) defines the function class  $\square_1^{\text{QP}}$ , which constitutes all polynomial-time computable quantum functions (Yamakami, 2020). Although we do not consider REMOVE here, its restricted form, called CodeREMOVE[·], will be introduced in Section 3.2.

Let us present a short list of typical quantum functions “definable” within EQS<sub>0</sub>; that is, those quantum functions are actually constructed from Items 1)–5) of Scheme I and by finitely many applications of Schemes II–III. As the first simple application of Scheme I–III, we demonstrate how to construct the special quantum function called Skip<sub>k</sub>[·].

**Lemma 4.** *Let  $g$  denote any quantum function in EQS<sub>0</sub> and let  $k \in \mathbb{N}^+$ . The quantum function Skip<sub>k</sub>[ $g$ ] is defined by Skip<sub>k</sub>[ $g$ ]( $|\phi\rangle$ ) =  $|\phi\rangle$  if  $\ell(|\phi\rangle) \leq k$ , and  $\sum_{u:|u|=k} |u\rangle \otimes g(\langle u|\phi\rangle)$  otherwise. This Skip<sub>k</sub>[ $g$ ] is definable within EQS<sub>0</sub>.*

*Proof.* We construct the desired quantum function Skip<sub>k</sub>[ $g$ ] inductively for any  $k \in \mathbb{N}^+$ . When  $k = 1$ , we set Skip<sub>1</sub>[ $g$ ]  $\equiv$  Branch[ $g, g$ ]. Clearly, when  $\ell(|\phi\rangle) > 1$ , we obtain Skip<sub>1</sub>[ $g$ ]( $|\phi\rangle$ ) = Branch[ $g, g$ ]( $|\phi\rangle$ ) =  $\sum_{a \in \{0,1\}} |a\rangle \otimes g(\langle a|\phi\rangle)$ . For any index  $k \geq 2$ , we define Skip<sub>k+1</sub>[ $g$ ] as Branch[Skip<sub>k</sub>[ $g$ ], Skip<sub>k</sub>[ $g$ ]]. It then follows that, if  $\ell(|\phi\rangle) > k + 1$ , then Skip<sub>k+1</sub>[ $g$ ]( $|\phi\rangle$ ) =  $\sum_{a \in \{0,1\}} |a\rangle \otimes \text{Skip}_k[g](\langle a|\phi\rangle) = \sum_{a \in \{0,1\}} \sum_{s:|s|=k} |a\rangle|s\rangle \otimes g(\langle s|\psi_{\text{Skip}_k[g], \langle a|\phi\rangle}\rangle) = \sum_{s':|s'|=k+1} |s'\rangle \otimes g(\langle s'|\phi\rangle)$ , as requested.  $\square$

**Lemma 5.** *Fix  $\theta \in [0, 2\pi) \cap K$  and  $i, j, k \in \mathbb{N}^+$  and  $i < j$ . Let  $|\phi\rangle$  be any quantum state in  $\mathcal{H}_\infty$ , let  $a, b$ , and  $c$  be any bits. The following quantum functions are definable by Schemes I–III and thus in EQS<sub>0</sub>.*

1. CNOT( $|\phi\rangle$ ) =  $|\phi\rangle$  if  $\ell(|\phi\rangle) \leq 1$  and CNOT( $|\phi\rangle$ ) =  $|0\rangle\langle 0|\phi\rangle + |1\rangle \otimes \text{NOT}(\langle 1|\phi\rangle)$  otherwise. (controlled NOT)
2. GPS <sub>$\theta$</sub> ( $|\phi\rangle$ ) =  $e^{i\theta}|\phi\rangle$ . (global phase shift)
3. WH( $|\phi\rangle$ ) =  $\frac{1}{\sqrt{2}}|0\rangle \otimes (\langle 0|\phi\rangle + \langle 1|\phi\rangle) + \frac{1}{\sqrt{2}}|1\rangle \otimes (\langle 0|\phi\rangle - \langle 1|\phi\rangle)$ . (Walsh-Hadamard transform)
4. Z<sub>1, $\theta$</sub> ( $|\phi\rangle$ ) =  $e^{i\theta}|0\rangle\langle 0|\phi\rangle + |1\rangle\langle 1|\phi\rangle$ .
5. zROT <sub>$\theta$</sub> ( $|\phi\rangle$ ) =  $e^{i\theta}|0\rangle\langle 0|\phi\rangle + e^{-i\theta}|1\rangle\langle 1|\phi\rangle$ . (rotation around the z-axis)
6. C <sub>$\theta$</sub> ( $|\phi\rangle$ ) =  $|\phi\rangle$  if  $\ell(|\phi\rangle) \leq 1$  and C <sub>$\theta$</sub> ( $|\phi\rangle$ ) =  $|0\rangle\langle 0|\phi\rangle + |1\rangle \otimes \text{ROT}_\theta(\langle 1|\phi\rangle)$  otherwise. (controlled ROT <sub>$\theta$</sub> )
7. CPHASE <sub>$\theta$</sub> ( $|\phi\rangle$ ) =  $|\phi\rangle$  if  $\ell(|\phi\rangle) \leq 1$ , and CPHASE <sub>$\theta$</sub> ( $|\phi\rangle$ ) =  $\frac{1}{\sqrt{2}} \sum_{b \in \{0,1\}} (|0\rangle\langle b|\phi\rangle + e^{i\theta b}|1\rangle\langle b|\phi\rangle)$  otherwise. (controlled PHASE)
8. CSWAP( $|a\rangle|\phi\rangle$ ) =  $|0\rangle \otimes \langle 0|a\rangle|\phi\rangle + |1\rangle \otimes \text{SWAP}(\langle 1|a\rangle|\phi\rangle)$  (controlled SWAP)
9. LengthQ <sub>$k$</sub> ( $|b\rangle|\phi\rangle$ ) =  $|b\rangle|\phi\rangle$  if  $\ell(|\phi\rangle) < k$  and LengthQ <sub>$k$</sub> ( $|b\rangle|\phi\rangle$ ) =  $|1 - b\rangle|\phi\rangle$  otherwise. (length query)
10. SWAP <sub>$i,j$</sub> ( $|\phi\rangle$ ) =  $\sum_{a_1 \dots a_j \in \{0,1\}} |a_1 \dots a_{i-1} a_j a_{i+1} \dots a_{j-1} a_i a_{j+1} \dots a_n\rangle \otimes (a_1 \dots a_{i-1} a_i a_{i+1} \dots a_{j-1} a_j a_{j+1} \dots a_n|\phi\rangle$  if  $\ell(|\phi\rangle) \geq j$  and SWAP <sub>$i,j$</sub> ( $|\phi\rangle$ ) =  $|\phi\rangle$  otherwise, where  $n = \ell(|\phi\rangle)$ .

*Proof.* (1)–(5) These quantum functions are constructed in (Yamakami, 2020, Lemma 3.3). (6) We set C <sub>$\theta$</sub>   $\equiv$  Branch[ $I, \text{ROT}_\theta$ ]. (7) This was shown in (Yamakami, 2020, Lemma 3.6). (8) We set CSWAP to be Branch[ $I, \text{SWAP}$ ]. This gives the equation CSWAP( $|a\rangle|\phi\rangle$ ) =  $|0\rangle \otimes I(\langle 0|a\rangle|\phi\rangle) + |1\rangle \otimes \text{SWAP}(\langle 1|a\rangle|\phi\rangle)$ .

(9) For simplicity, we write  $g \circ f$  in place of  $Compo[g, f]$ . Let  $h \equiv Branch[NOT, NOT] \circ SWAP$ . We construct  $LengthQ_k$  inductively for any  $k \geq 1$  as follows. Firstly, when  $k = 1$ ,  $LengthQ_1$  is set to be  $SWAP \circ Skip_1[SWAP] \circ Skip_1[h] \circ SWAP$ . It then follows that  $LengthQ_1(|b\rangle) = |b\rangle$  and  $LengthQ_1(|b\rangle|\phi\rangle) = |1 - b\rangle|\phi\rangle$ . Letting  $k \geq 2$ , assume that  $LengthQ_{k-1}$  has been already defined. We then define  $LengthQ_k$  as  $SWAP \circ Skip_1[Branch[LengthQ_{k-1}, LengthQ_{k-1}]] \circ SWAP$ .

(10) Notice that  $SWAP_{1,2}$  coincides with  $SWAP$  of Scheme I. For any fixed constant  $k \geq 1$ , we first define  $SWAP_{k,k+1}$  to be  $Skip_{k-1}[SWAP]$ . For any indices  $i, j \geq 1$  with  $i < j$ , we further define  $MOVE_{i,j}$  to be  $SWAP_{i,i+1} \circ SWAP_{i+1,i+2} \circ \dots \circ SWAP_{j-1,j}$ . Note that  $MOVE_{1,j-1}^{-1}$  equals  $SWAP_{j-2,j-1} \circ SWAP_{j-3,j-2} \circ \dots \circ SWAP_{1,2}$ . With the use of  $MOVE_{1,j}$ , we define  $SWAP_{1,j}$  as  $MOVE_{1,j} \circ MOVE_{1,j-1}^{-1}$ . The target quantum function  $SWAP_{i,j}$  is finally set to be  $Skip_{i-1}[SWAP_{1,j-i}]$ . □

**Lemma 6.** Fix  $i, j, k \in \mathbb{N}^+$  with  $k \geq 2$  and  $i < j$ , and let  $|\phi\rangle$  denote any quantum state in  $\mathcal{H}_\infty$ . The following quantum functions are definable using Schemes I–III and thus in  $EQS_0$ .

1.  $SecSWAP_{i,j}^{(k)}(|x_1\rangle|x_2\rangle \dots |x_{i-1}\rangle|x_i\rangle|x_{i+1}\rangle \dots |x_{j-1}\rangle|x_j\rangle|\phi\rangle) = |x_1\rangle|x_2\rangle \dots |x_{i-1}\rangle|x_j\rangle|x_{i+1}\rangle \dots |x_{j-1}\rangle|x_i\rangle|\phi\rangle$  for any  $k$ -bit strings  $x_1, x_2, \dots, x_i, \dots, x_j \in \{0, 1\}^k$ . (section SWAP)
2.  $SecMOVE_{i,j}^{(k)}(|x_1\rangle|x_2\rangle \dots |x_{i-1}\rangle|x_i\rangle|x_{i+1}\rangle \dots |x_j\rangle|\phi\rangle) = |x_1\rangle|x_2\rangle \dots |x_{i-1}\rangle|x_{i+1}\rangle \dots |x_j\rangle|x_i\rangle|\phi\rangle$  for any  $k$ -bit strings  $x_1, x_2, \dots, x_i, \dots, x_j \in \{0, 1\}^k$ . (section MOVE)

*Proof.* (1) Since  $x_1, x_2, \dots, x_i, \dots, x_j$  are  $k$ -bit strings, we obtain  $|x_1x_2 \dots x_{i-1}| = (i - 1)k$  and  $|x_1x_2 \dots x_{j-1}| = (j - 1)k$ . For convenience, we write  $i_k$  for  $(i - 1)k$  and  $j_k$  for  $(j - 1)k$ . We then define the desired quantum function  $SecSWAP_{i,j}^{(k)}$  to be  $SWAP_{i_k+1,j_k+1} \circ SWAP_{i_k+2,j_k+2} \circ \dots \circ SWAP_{i_k+k,j_k+k}$ .

(2) The quantum function  $SecMOVE_{i,j}^{(k)}$  is set to be  $SecSWAP_{j-1,j}^{(k)} \circ \dots \circ SecSWAP_{i+1,i+2}^{(k)} \circ SecSWAP_{i,i+1}^{(k)}$ . □

Hereafter, let us construct more quantum functions in  $EQS_0$ .

**Lemma 7.** Consider  $COPY_1$  that satisfies  $COPY_1(|a\rangle|\phi\rangle) = \sum_{s \in \{0,1\}} |a \oplus s\rangle|s\rangle\langle s|\phi\rangle$  for any quantum state  $|\phi\rangle \in \mathcal{H}_\infty$  and any bit  $a$ , where  $\oplus$  denotes the bitwise XOR. More generally, for each fixed constant  $k \geq 2$ , let  $COPY_k(|x\rangle|\phi\rangle) = \sum_{z \in \{0,1\}^k} |x \oplus z\rangle|z\rangle\langle z|\phi\rangle$  for any quantum state  $|\phi\rangle \in \mathcal{H}_\infty$  and any  $k$ -bit string  $x$ . These quantum functions are all definable using Schemes I–III.

*Proof.* We inductively define  $COPY_k$  for any index  $k \geq 1$ . In the case of  $k = 1$ , we set  $COPY_1$  to be  $SWAP \circ CNOT \circ SWAP$ . It then follows that  $COPY_1(|a\rangle|\phi\rangle) = SWAP \circ CNOT \circ SWAP(|a\rangle|\phi\rangle) = SWAP \circ CNOT(\sum_{s \in \{0,1\}} |s\rangle|a\rangle \otimes \langle s|\phi\rangle) = \sum_{s \in \{0,1\}} SWAP(|s\rangle|a \oplus s\rangle) \otimes \langle s|\phi\rangle = \sum_{s \in \{0,1\}} |a \oplus s\rangle\langle s|\phi\rangle$ .

Let  $k \geq 2$ . Assume by induction hypothesis that  $COPY_{k-1}$  has been already defined. The quantum function  $COPY_k(|x\rangle|\phi\rangle)$  is obtained by taking the following process. To  $|x\rangle|\phi\rangle$ , we first apply  $SWAP_{[2,k]} \equiv SWAP_{2,3} \circ SWAP_{3,4} \circ \dots \circ SWAP_{k-1,k}$ . Next, we apply  $COPY_1$  and then  $Skip_2[COPY_{k-1}]$ . Finally, we apply  $SWAP_{[2,k]}^{-1}$ . It is not difficult to check that the obtained quantum function matches  $COPY_k$ . □

Let us construct the basic quantum functions  $g_{AND}$  and  $g_{OR}$ , which “mimic” the behaviors of the two-bit operations  $AND$  and  $OR$ , using only Schemes I–III.

**Lemma 8.** *There exist two quantum functions  $g_{AND}$  and  $g_{OR}$  that satisfy the following. Let  $x, y \in \{0, 1\}$  and  $b \in \{0, 1\}$ . (1)  $AND(x, y) = b$  iff  $\| \langle b | \psi_{0xy}^{(AND)} \rangle \| = 1$ , where  $|\psi_{0xy}^{(AND)}\rangle = g_{AND}(|0\rangle|x\rangle|y\rangle)$ . (2)  $OR(x, y) = b$  iff  $\| \langle b | \psi_{0xy}^{(OR)} \rangle \| = 1$ , where  $|\psi_{0xy}^{(OR)}\rangle = g_{OR}(|0\rangle|x\rangle|y\rangle)$ . These quantum functions are defined by Schemes I–III.*

*Proof.* Recall the quantum functions  $SWAP_{i,j}$  and  $COPY_1$ , respectively, from Lemmas 5 and 7. We first define  $g_{OR}$  to be  $SWAP_{1,3} \circ CSWAP \circ COPY_1$ . From this definition, for any  $x, y \in \{0, 1\}$ , it follows that  $g_{OR}(|0\rangle|x\rangle|y\rangle) = \langle 0|x\rangle|y\rangle|x\rangle|0\rangle + \langle 1|x\rangle|x\rangle|y\rangle|1\rangle$ . Thus, we obtain  $g_{OR}(|0\rangle|0\rangle|y\rangle) = |y\rangle|0\rangle|0\rangle$  and  $g_{OR}(|0\rangle|1\rangle|y\rangle) = |1\rangle|y\rangle|1\rangle$ .

We next define  $g_{AND}$  to be  $SWAP_{1,3} \circ SWAP_{2,3} \circ CSWAP \circ COPY_1$ . It then follows that  $g_{AND}(|0\rangle|x\rangle|y\rangle) = \langle 0|x\rangle|x\rangle|y\rangle|0\rangle + \langle 1|x\rangle|y\rangle|x\rangle|1\rangle$ . From this equality, we obtain  $g_{AND}(|0\rangle|0\rangle|y\rangle) = |0\rangle|y\rangle|0\rangle$  and  $g_{AND}(|0\rangle|1\rangle|y\rangle) = |y\rangle|1\rangle|1\rangle$ . □

For later use, we define another quantum function, which splits the entire input qubits into two halves and then swaps them. We do not intend to include this quantum function to our system, but it will be used to support the description of a new scheme given in Section 3.2. We remark that, to construct this quantum function, we need Schemes I–III together with the quantum recursion Scheme T. By recalling the left-half function  $LH$  and the right-half function  $RH$  from Section 2.1, let us introduce  $HalfSWAP$  as

$$*) \text{ HalfSWAP}(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ \sum_{s:|s|=LH(|\phi\rangle)} \langle s|\phi\rangle \otimes |s\rangle & \text{otherwise.} \end{cases}$$

The inverse of  $HalfSWAP$ , denoted  $HalfSWAP^{-1}$ , matches the quantum function obtained from  $HalfSWAP$  by replacing  $LH(|\phi\rangle)$  in its definition with  $RH(|\phi\rangle)$ . In the special case where  $\ell(|\phi\rangle)$  is even,  $HalfSWAP \circ HalfSWAP(|\phi\rangle)$  equals  $|\phi\rangle$  since  $LH(|\phi\rangle) = RH(|\phi\rangle)$ .

**Example 9.** Consider a quantum state  $|\phi\rangle = \sum_{u:|u|=3} \alpha_u|u\rangle$ , which is  $\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \dots + \alpha_{111}|111\rangle$ . Notice that  $LH(|\phi\rangle) = \lceil \ell(|\phi\rangle)/2 \rceil = 2$  and  $RH(|\phi\rangle) = \lfloor \ell(|\phi\rangle)/2 \rfloor = 1$ . Since  $\langle s|\phi\rangle = \sum_{u:|u|=3} \alpha_u \langle s|u\rangle$ , it then follows that  $HalfSWAP(|\phi\rangle) = \sum_{s:|s|=2} \sum_{u:|u|=3} \alpha_u \langle s|u\rangle \otimes |s\rangle$ , which equals  $\alpha_{000}|000\rangle + \alpha_{001}|100\rangle + \alpha_{010}|001\rangle + \alpha_{011}|101\rangle + \dots + \alpha_{111}|111\rangle$ .

### 3.2 Binary encoding of various types of objects

All quantum functions discussed in Section 3.1 take only “single” quantum states in  $\mathcal{H}_\infty$  as their inputs. For practical applications of these quantum functions, we need to further deal with a problem that consists of various types of “objects,” such as numbers, graphs, matrices, and tape symbols. Since each QTM uses multiple tapes with their associated tape heads, these tapes hold possibly different qubits and their tape heads move separately. This is an advantage of the QTM model over quantum functions. For our purpose, nevertheless, it is imperative to set up an appropriate *binary encoding* to transform multiple objects into a single quantum state with an appropriate use of designated “separators”. In the polynomial-time setting (Yamakami, 2020), the scheme of quantum recursion (Scheme T) is powerful enough to handle several inputs altogether as a single encoded quantum state in a way similar to a multiple-tape QTM being simulated by a single-tape QTM with only polynomial overhead. However, since we aim at capturing quantum polylogtime computability instead, we cannot take the same approach to cope with multiple

inputs. We thus need to ponder how to circumvent this difficulty to expand the scope of our quantum functions. As a feasible solution to this problem, we introduce “extra” schemes that help us handle intended binary encodings.

In what follows, we attempt to design an encoding (or a translation) of various types of objects into binary strings of the same fixed length so that a series of these encoded objects forms a larger-dimensional quantum state. Each “segment” of such a quantum state representing one encoded object is referred to as a *section*, and this fixed-length encoding makes it possible to work with each section separately.

Let us describe our encoding scheme for eight symbols in  $\{0, 1, 2, \neg, B, H, S, T\}$ , where  $\neg, B, H, S,$  and  $T,$  respectively, stand for an “ending,” a “blank,” a “head,” a “separator,” and a “time”. With the use of three bits, we take the following abbreviations:  $\hat{0} = 000, \hat{1} = 001, \hat{B} = 010, \hat{\neg} = 011, \hat{2} = 111, \hat{H} = 100, \hat{S} = 110,$  and  $\hat{T} = 101.$  Given a binary string  $s = s_1s_2 \cdots s_k,$  the notation  $\tilde{s}^{(-)}$  denotes  $\hat{s}_1\hat{s}_2 \cdots \hat{s}_k,$  and  $\tilde{s}$  denotes  $\tilde{s}^{(-)}\hat{\neg}.$  For convenience, we also define  $\tilde{\lambda}$  to be  $\hat{\neg}.$  This makes us encode, for example, the number 8 into  $\widetilde{bin}(8) = 001 = 00\hat{1}\hat{\neg},$  while  $\widetilde{bin}_3(2)$  also equals  $001.$  Given an arbitrary quantum state  $|\phi\rangle$  in  $\mathcal{H}_\infty,$  we finally define its encoding  $|\tilde{\phi}\rangle$  as  $\sum_{s:|s|=\ell(|\phi\rangle)} |\tilde{s}\rangle \langle s|\phi\rangle.$  Notice that  $\ell(|\tilde{\phi}\rangle) = 3\ell(|\phi\rangle) + 3.$

To mark the end of a series of encoded objects, we use a designated separator, say,  $r_0$  in  $\{0, 1\}^+.$  We fix such  $r_0$  in the following discussion. We make each series of encoded objects have length proportional to the section size  $|r_0|,$  and thus any encoding  $x$  satisfies  $|x| = k|r_0|$  for an appropriate, fixed number  $k \in \mathbb{N}^+.$  This helps us partition  $x$  section-wise as  $x_1x_2 \cdots x_k$  with  $|x_i| = |r_0|$  for all indices  $i \in [k].$  We also demand that no  $x_i$  should match  $r_0.$  Here, we say that  $x$  *section-wise contains no  $r_0$*  if  $x_i \neq r_0$  holds for all indices  $i \in [k].$  Let  $NON_{r_0} = \{x \in \{0, 1\}^+ \mid |x| \equiv 0 \pmod{|r_0|}, x \text{ section-wise contains no } r_0\}.$  Similarly, we set  $NON_{r_0}(|\phi\rangle) = \{x \in NON_{r_0} \mid \langle xr_0|\phi\rangle \neq 0\}.$  For convenience, when  $r_0 = \hat{2},$  we tend to omit  $r_0$  from  $NON_{r_0}$  and  $NON_{r_0}(|\phi\rangle).$

**Example 10.** Fix  $r_0 \in \{0, 1\}^+.$  Choose three strings  $x_1, x_2, x_3 \in \{0, 1\}^{|r_0|}$  satisfying  $x_i \neq r_0$  for all  $i \in [3],$  and consider three quantum states  $|\psi\rangle = |x_1x_2x_3\rangle|r_0\rangle|\phi\rangle, |\psi'\rangle = |x_1x_2r_0x_3\rangle|\phi\rangle,$  and  $|\psi''\rangle = |x_1r_0x_2x_3\rangle|\phi\rangle$  for any  $|\phi\rangle \in \mathcal{H}_\infty.$  We then obtain  $NON_{r_0}(|\psi\rangle) = \{x_1x_2x_3\}, NON_{r_0}(|\psi'\rangle) = \{x_1x_2\},$  and  $NON_{r_0}(|\psi''\rangle) = \{x_1\}.$  By contrast, when  $|\psi\rangle$  has the form  $(\alpha|x_1\rangle|r_0\rangle + \beta|x_2\rangle|r_0\rangle)|\phi\rangle,$   $NON_{r_0}(|\psi\rangle)$  equals  $\{x_1, x_2\}.$

As another example, if  $x = 0111$  and  $r_0 = \hat{2},$  then  $\tilde{x}$  equals  $\tilde{x}^{(-)}\hat{\neg} = \hat{0}\hat{1}\hat{1}\hat{\neg}.$  Notice that  $|\tilde{x}| \equiv 0 \pmod{|r_0|}.$  Thus, we obtain  $NON_{r_0}(|\tilde{x}\rangle|r_0\rangle|\phi\rangle) = \{\tilde{x}\}.$

We then need a quantum function that splits an input into sections and apply “section-wise” two predetermined quantum operations. We actually introduce two slightly different *code skipping schemes* described below. We do not unconditionally include them to EQS, but we use them in a certain restricted situation, which will be discussed later. Such a restriction is in fact necessary because these schemes are too powerful to use for quantum polylogtime computability.

\*) The *code skipping schemes.* From  $g, h$  and  $r_0 \in \{0, 1\}^+,$  we define  $CodeSKIP_+[r_0, g, h]$  and  $CodeSKIP_-[r_0, g, h]$  as follows:

$$(i) \text{ CodeSKIP}_+[r_0, g, h](|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } NON_{r_0}(|\phi\rangle) = \emptyset, \\ \sum_{x \in NON_{r_0}(|\phi\rangle)} (g(|xr_0\rangle) \otimes h(\langle xr_0|\phi\rangle)) & \text{otherwise.} \end{cases}$$

$$(ii) \text{ CodeSKIP}_-[r_0, g, h](|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } NON_{r_0}(|\phi\rangle) = \emptyset, \\ \sum_{x \in NON_{r_0}(|\phi\rangle)} (g(|x\rangle) \otimes h(\langle x|\phi\rangle)) & \text{otherwise.} \end{cases}$$

The difference between  $CodeSKIP_+[r_0, g, h]$  and  $CodeSKIP_-[r_0, g, h]$  looks subtle but becomes clear in the following example. When  $|\phi\rangle = |x\rangle|r_0\rangle|y\rangle$  with  $|x| = |r_0|$  and  $x \neq r_0$ , it follows that  $CodeSKIP_+[r_0, g, h](|\phi\rangle) = g(|xr_0\rangle) \otimes h(|y\rangle)$  but  $CodeSKIP_-[r_0, g, h](|\phi\rangle) = g(|x\rangle) \otimes h(|r_0y\rangle)$ . These schemes are not interchangeable in most applications.

A quantum function  $g$  is said to be *query-independent* if, in the process of constructing  $g$ , for any input of the form  $|xr_0\rangle|\phi\rangle$ , any quantum function that appears in this construction process does not directly access  $|\phi\rangle$  and thus it does not depend on  $|\phi\rangle$ . This instantly implies that  $g(|xr_0\rangle|\phi\rangle) = g(|xr_0\rangle) \otimes |\phi\rangle$  for any  $x$  and  $|\phi\rangle$ . Using this terminology, when  $h = I$  in the code skipping schemes,  $CodeSKIP_+[r_0, g, I]$  and  $CodeSKIP_-[r_0, g, I]$  are query-independent.

Here, we present a few more examples of  $CodeSKIP_+$ .

**Example 11.** Let  $g = ROT_{\pi/4}$  and  $h = NOT$ . Let  $r_0 = 0^5$  and let  $|\phi\rangle = |x_1x_2\rangle|r_0\rangle|x_3x_4\rangle|r_0\rangle|\psi\rangle$  with binary strings  $x_i = bin_5(i)$  for any  $i \in [4]$  and a qustring  $|\psi\rangle$ . Since  $NON_{r_0}(|\phi\rangle) = \{x_1x_2\}$ , we obtain  $CodeSKIP_+[r_0, g, h](|\phi\rangle) = ROT_{\pi/4}(|x_1x_2r_0\rangle) \otimes NOT(|x_3x_4r_0\rangle|\psi\rangle)$ .

Let  $|\phi'\rangle = \alpha|y_1r_0\rangle|\psi_1\rangle + \beta|y_2r_0\rangle|\psi_2\rangle$  with  $|y_1| = |y_2| = |r_0|$  and  $y_1, y_2 \notin \{r_0\}$ . In this case,  $NON_{r_0}$  is the set  $\{y_1, y_2\}$ . It then follows that  $CodeSKIP_+[r_0, g, h](|\phi'\rangle) = \alpha g(|y_1r_0\rangle) \otimes h(|\psi_1\rangle) + \beta g(|y_2r_0\rangle) \otimes h(|\psi_2\rangle)$ .

We wish to recall the two useful quantum functions *REMOVE* (removal) and *REP* (replacement) introduced by Yamakami (2020). We introduce the “code-controlled” versions of them. Let  $r_0 \in \{0, 1\}^+$  be a separator.

$$(i) \text{ CodeREMOVE}[r_0](|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } NON_{r_0}(|\phi\rangle) = \emptyset, \\ \sum_{x \in NON_{r_0}(|\phi\rangle)} \sum_{a \in \{0,1\}} (\langle a|x\rangle \otimes |ar_0\rangle \otimes \langle xr_0|\phi\rangle) & \text{otherwise.} \end{cases}$$

$$(ii) \text{ CodeREP}[r_0](|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } NON_{r_0}(|\phi\rangle) = \emptyset, \\ \sum_{x \in NON_{r_0}(|\phi\rangle)} \sum_{u:|u|=|x|-1} (\langle u|x\rangle \otimes |ur_0\rangle \otimes \langle xr_0|\phi\rangle) & \text{otherwise.} \end{cases}$$

Notice that the quantum functions  $CodeREMOVE[r_0]$  and  $CodeREP[r_0]$  are query-independent.

We wish to include a simple example of  $CodeREMOVE$  and  $CodeREP$ .

**Example 12.** Let  $|\phi\rangle = \alpha|x_1r_0\rangle|\psi_1\rangle + \beta|x_2r_0\rangle|\psi_2\rangle + \gamma|r_0\rangle|\psi_3\rangle$  with  $\ell(|x_1r_0\rangle|\psi_1\rangle) = \ell(|x_2r_0\rangle|\psi_2\rangle) = \ell(|r_0\rangle|\psi_3\rangle)$ ,  $NON_{r_0}(|\psi\rangle) = \{x_1, x_2\}$ ,  $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$ , and  $\alpha\beta\gamma \neq 0$ . If  $x_1 = 0y_1$  and  $x_2 = 1y_2$  for two strings  $y_1$  and  $y_2$ , then  $CodeREMOVE[r_0](|\psi\rangle)$  equals  $\alpha|y_10r_0\rangle|\psi_1\rangle + \beta|y_21r_0\rangle|\psi_2\rangle + \gamma|r_0\rangle|\psi_3\rangle$ . If  $x_1 = z_10$  and  $x_2 = z_21$ , then we obtain  $CodeREP[r_0](|\phi\rangle) = \alpha|0z_1r_0\rangle|\psi_1\rangle + \beta|1z_2r_0\rangle|\psi_2\rangle + \gamma|r_0\rangle|\psi_3\rangle$ .

### 3.3 Code-controlled fast quantum recursion scheme

Let us introduce a new scheme, called Scheme IV, which is a variant of the multi-qubit quantum recursion scheme (Scheme T) geared up with the code skipping schemes in Section 3.2. Recall that, in Scheme T, we inductively discard  $k$  qubits from an input quantum state  $|\phi\rangle$  until we consume all qubits except for the last (at most)  $t$  qubits. Unlike Scheme T, since our access to input qubits is quite limited, we need to split the whole input into two separate parts, which play quite different roles as we will see.

Before formally introducing the complexity class  $EQS$ , for each quantum function  $f$  in  $EQS_0$ , we define its “code-controlled” version  $f^*$  by setting  $f^*(|xr_0\rangle|\phi\rangle) = |xr_0\rangle|\phi\rangle$  if  $|x| \leq 2$ ,  $\ell(|\phi\rangle) \leq 1$ , or  $|x| > |r_0| \lceil \log(\ell(|\phi\rangle)) \rceil$ , and  $f^*(|xr_0\rangle|\phi\rangle) = f(|xr_0\rangle) \otimes |\phi\rangle$  otherwise, for any  $x \in \{0, 1\}^*$  and any  $|\phi\rangle \in \mathcal{H}_\infty$ . In the rest of this work, it is convenient to identify  $f$  with  $f^*$ . It is important to note that  $f^*$  does not access  $|\phi\rangle$  in  $|xr_0\rangle|\phi\rangle$  by its definition.

In the fast quantum recursion, on the contrary, we discard a half of the second part of input quantum state  $|xr_0\rangle \otimes |\phi\rangle$ . By halving the input at each step, this recursive process quickly terminates.

**Definition 13.** We introduce the following scheme.

IV. The code-controlled fast quantum recursion scheme. Assume that we are given quantum functions  $d, g, h$ , a number  $t \in \mathbb{N}^+$ , and a string  $r_0 \in \{0, 1\}^+$  (where  $d$  is not defined using  $MEAS[\cdot]$  but  $d$  and  $h$  may be defined using  $CodeSKIP_+[\cdot]$  and  $CodeSKIP_-[\cdot]$ ). We then define  $F \equiv CFQRec_t[r_0, d, g, h | \mathcal{P}_{|r_0|}, \mathcal{F}_{|r_0|}]$  for  $\mathcal{P}_{|r_0|} = \{p_u\}_{u \in \{0,1\}^{|r_0|}}$  with  $p_u \in \{I, HalfSWAP\}$  and  $\mathcal{F}_{|r_0|} = \{f_u\}_{u \in \{0,1\}^{|r_0|}}$  with  $f_u \in \{I, F\}$  as follows. For any  $x \in \{0, 1\}^*$  and any  $|\phi\rangle \in \mathcal{H}_\infty$ , let

$$(i) \quad F(|xr_0\rangle|\phi\rangle) = g(|xr_0\rangle|\phi\rangle) \quad \text{if } x = \lambda, \ell(|\phi\rangle) \leq t, \text{ or } |x| > |r_0|k,$$

$$(ii) \quad F(|xr_0\rangle|\phi\rangle) = \sum_{u:|u|=|r_0|} \sum_{v:|v|=\ell(\langle u|xr_0\rangle)} (h(|u\rangle|v\rangle) \otimes p_u^{-1}(\langle v|\zeta_{u,p_u,\phi}^{(x'r_0)}\rangle)) \quad \text{otherwise,}$$

where  $k = \text{ilog}(\ell(|\phi\rangle))$ ,  $x \in NON_{r_0}$ ,  $|\zeta_{u,p_u,\phi}^{(x'r_0)}\rangle = \sum_{s:|s|=m_u(|\phi\rangle)} (f_u(\langle u|x'r_0\rangle \otimes |s\rangle) \otimes \langle s|\psi_{p_u,\phi}\rangle)$ ,  $d(|xr_0\rangle) = |x'r_0\rangle$  with  $x' \in NON_{r_0}$ ,  $|\psi_{p_u,\phi}\rangle = p_u(|\phi\rangle)$ . Moreover,  $m_u(\cdot)$  is determined to be LH if  $p_u = I$  and RH if  $p_u = HalfSWAP$ . Notice that  $u \neq r_0$  follows from  $x' \in NON_{r_0}$ . In the other case where an input, say,  $|y\rangle$  to  $F$  satisfies  $NON_{r_0}(|y\rangle) = \emptyset$ , we automatically set  $F(|y\rangle) = |y\rangle$ .

For readability, the prefix term “code-controlled” is often dropped and  $|\zeta_{u,p_u,\phi}^{(x'r_0)}\rangle$  is expressed briefly as  $|\zeta_{u,p_u,\phi}\rangle$  as long as  $x'r_0$  is clear from the context.

The quantum functions  $d, g, h$  in the above definition are called *ground (quantum) functions* of  $F$ . If  $g$  is query-independent, Scheme IV is said to be *query-independent*.

Although the description of Items (i)–(ii) in Scheme IV concerns only with a classical string  $xr_0$ , whenever any quantum state  $|\psi\rangle = \sum_x \alpha_x |xr_0\rangle \otimes |\phi_x\rangle$  is plugged in to  $F$ , we obtain the result  $\sum_x \alpha_x F(|xr_0\rangle|\phi_x\rangle)$ .

Since  $p_u \in \{I, HalfSWAP\}$  and  $|x'| = |x|$ , it follows that  $\ell(|\psi_{u,p_u,\phi}\rangle) = \ell(|\phi\rangle)$ ,  $\ell(|\zeta_{u,p_u,\phi}^{(x'r_0)}\rangle) = \ell(\langle u|x'r_0\rangle) + \ell(|\phi\rangle)$ , and  $\ell(\langle v|\zeta_{u,p_u,\phi}^{(x'r_0)}\rangle) = \ell(|\phi\rangle)$ . In Item (ii), since the size  $|s|$  is exactly LH( $|\phi\rangle$ ) (or RH( $|\phi\rangle$ )),  $f_u$  takes inputs of length  $(\ell(|x'r_0\rangle) - |r_0|) + \lceil \ell(|\phi\rangle)/2 \rceil$  (or  $(\ell(|x'r_0\rangle) - |r_0|) + \lfloor \ell(|\phi\rangle)/2 \rfloor$ ). Hence, within  $\lceil \log \ell(|\phi\rangle) \rceil$  recursive steps, the whole process terminates.

As a special case of Scheme IV, when  $r_0 = 1$ , Item (ii) has the following simple form:

$$(ii') \quad F(|0^n 1\rangle|\phi\rangle) = \sum_{v:|v|=n} (h(|0\rangle \otimes |v\rangle) \otimes p_0^{-1}(\langle v|\zeta_{0,p_0,\phi}^{(0^n 1)}\rangle)),$$

where  $|\zeta_{0,p_0,\phi}^{(0^n 1)}\rangle = \sum_{s:|s|=m(|\phi\rangle)} (f_0(|0^{n-1} 1\rangle \otimes |s\rangle) \otimes \langle s|\psi_{p_0,\phi}\rangle)$ .

At this moment, it is worth remarking the usage of the length function  $\ell(\cdot)$ . In Scheme IV, the input quantum state  $|xr_0\rangle|\phi\rangle$  is reduced to  $\langle u|x'r_0\rangle|s\rangle$  (with  $|s| = m_u(|\phi\rangle)$  and  $|u| = |r_0|$ ) so that we can inductively apply  $F$  (when  $f_u = F$ ) to it. The length  $\ell(|\phi\rangle)$  then becomes  $\ell(|s\rangle)$ , and thus the conditional execution of Item (i) depends on the value  $\ell(|s\rangle)$ .

To understand Scheme IV better, we provide in Example 14 a simple example of how to calculate the quantum function  $F \equiv CFQRec_t[r_0, d, g, h | \mathcal{P}_{|r_0|}, \mathcal{F}_{|r_0|}]$  step by step.

**Example 14.** In this example, we wish to show how to calculate the quantum function  $F \equiv CFQRec_t[r_0, d, g, h | \mathcal{P}_{|r_0|}, \mathcal{F}_{|r_0|}]$  defined with the parameters  $t = 1$ ,  $r_0 = 1$ ,  $d = I$ , and  $g \equiv I$ . Furthermore,  $h$  is defined as  $h(|01\rangle) = |11\rangle$  and  $h(|010^m 1\rangle) = |10^{m+1} 1\rangle$  for any  $m \in \mathbb{N}$ . We also set  $p_0 = HalfSWAP$ ,  $p_1 = I$ ,  $f_0 = F$ , and  $f_1 = I$ . Let  $x \in \{0\}^*$  and  $|\phi\rangle \in \mathcal{H}_\infty$ . In what follows, we will calculate  $F(|x1\rangle|\phi\rangle)$  in a “bottom-up” fashion.



(1) We start with the base case. If  $x = \lambda$ , then  $F(|1\rangle|\phi\rangle) = g(|1\rangle|\phi\rangle) = |1\rangle|\phi\rangle$ . If  $x = 0^m 1$  with  $m \geq 1$  and  $\ell(|\phi\rangle) \leq 1$ , then  $F(|0^m 1\rangle|\phi\rangle) = g(|0^m 1\rangle|\phi\rangle) = |0^m 1\rangle|\phi\rangle$ .

(2) Hereafter, we assume that  $x \neq \lambda$  and  $\ell(|\phi\rangle) \geq 2$ . For simplicity, let  $|\phi\rangle$  denote  $|u\rangle$  for a certain string  $u \in \{0, 1\}^*$ . When  $u = u_1 u_2 \cdots u_n$  and  $1 \leq i < j \leq n$ , we use the succinct notation  $u_{[i,j]}$  to express the string  $u_i u_{i+1} \cdots u_j$ .

(a) We first calculate  $F(|01\rangle|u\rangle)$  for  $u = u_1 u_2 u_3 u_4$ . Since  $|u\rangle = |u_{[1,2]}\rangle|u_{[3,4]}\rangle$ , we obtain  $p_0(|u\rangle) = |u_{[3,4]}\rangle|u_{[1,2]}\rangle$ . We also obtain  $|\zeta_{0,p_0,u}\rangle = F(|1\rangle|u_{[3,4]}\rangle) \otimes |u_{[1,2]}\rangle = |1\rangle \otimes |u_{[3,4]}\rangle|u_{[1,2]}\rangle$  by (1), and thus  $F(|01\rangle|u\rangle)$  equals  $h(|0\rangle \otimes |1\rangle) \otimes p_0^{-1}(|u_{[3,4]}\rangle|u_{[1,2]}\rangle)$ , which is  $|11\rangle|u_{[1,2]}\rangle|u_{[3,4]}\rangle = |11\rangle|u\rangle$ .

(b) Next, we calculate  $F(|001\rangle|u'\rangle)$  for  $u' = u_1 u_2 \cdots u_8$ . Note that  $|\zeta_{0,p_0,u'}\rangle = F(|01\rangle|u'_{[5,8]}\rangle) \otimes |u'_{[1,4]}\rangle = |11\rangle \otimes |u'_{[5,8]}\rangle|u'_{[1,4]}\rangle$  by (a). From this, we obtain  $F(|001\rangle|u'\rangle) = h(|0\rangle \otimes |11\rangle) \otimes p_0^{-1}(|u'_{[5,8]}\rangle|u'_{[1,4]}\rangle) = |101\rangle|u'\rangle$ .

### 3.4 Power of Scheme IV

In what follows, we intend to show the usefulness of Scheme IV by applying it to construct a quantum function, which calculates the logarithmic value of (part of) input size. Formally, for any  $|\phi\rangle \in \mathcal{H}_\infty$  and  $m \in \mathbb{N}^+$ , we define  $SIZE_1$  as  $SIZE_1(|0^m 1\rangle|\phi\rangle) = |0^k 1\rangle|0^{m-k-1} 1\rangle|\phi\rangle$  if  $\ell(|\phi\rangle) \leq 2^{m-1}$ , where  $k = \text{ilog}(\ell(|\phi\rangle))$ , and  $SIZE_1(|0^m 1\rangle|\phi\rangle) = |0^m 1\rangle|\phi\rangle$  otherwise. More generally, for any  $r_0 \notin \{0\}^*$  with  $|r_0| \geq 1$ , we define  $SIZE_{r_0}$  as  $SIZE_{r_0}(|0^{|r_0|} r_0\rangle|\phi\rangle) = |0^{k|r_0|} r_0\rangle|0^{(m-k-1)|r_0|} r_0\rangle|\phi\rangle$ . The choice of  $0^{m|r_0|}$  here is only for simplicity.

For brevity, we intend to use the notation  $EQS_0 + IV$  to express the set of quantum functions constructed by applying Schemes I–IV.

**Lemma 15.** *Let  $r_0 \notin \{0\}^*$  with  $|r_0| \geq 1$ . The above quantum function  $SIZE_{r_0}$  can be definable within  $EQS_0 + IV$ .*

*Proof.* We prove the lemma only for the simple case of  $r_0 = 1$ . Given  $m \in \mathbb{N}^+$  and  $|\phi\rangle \in \mathcal{H}_\infty$ , let  $|\xi\rangle = |0^m 1\rangle|\phi\rangle$ . Recall the quantum function  $LengthQ_1$  from Lemma 5(9) and, for simplicity, write  $g$  for  $LengthQ_1$ . It then follows that  $g(|1\rangle) = |1\rangle$  and  $g(|0^m 1\rangle) = |10^{m-1} 1\rangle$  if  $m \geq 1$ . We denote by  $F$  the quantum function  $CFQRec_1[1, I, g, I|\{p_0, p_1\}, \{f_0, f_1\}]$  with the parameters  $f_0 = F, f_1 = I$ , and  $p_0 = p_1 = I$ .

If either  $m = 0$  or  $\ell(|\phi\rangle) \leq 1$ , then  $F(|1\rangle|\phi\rangle)$  equals  $g(|1\rangle) \otimes |\phi\rangle = |1\rangle|\phi\rangle$ . Hereafter, we assume that  $m \geq 1$  and  $\ell(|\phi\rangle) \geq 2$ . By induction hypothesis, we obtain  $F(|0^{m-1} 1\rangle \otimes |s\rangle) = |0^{k-1} 1\rangle|0^{m-k-1} 1\rangle|\phi\rangle$  if  $\ell(|s\rangle) \leq 2^{m-2}$  and  $k - 1 = \text{ilog}(\ell(|s\rangle))$ . Starting with  $|\xi\rangle = |0^m 1\rangle|\phi\rangle$ ,  $F(|\xi\rangle)$  equals  $|0\rangle \otimes \sum_{s:|s|=LH(|\phi\rangle)} F(|0^{m-1} 1\rangle \otimes |s\rangle) \otimes |s\rangle|\phi\rangle = |0\rangle \otimes |0^{k-1} 1\rangle|0^{m-k-1} 1\rangle|\phi\rangle = |0^k 1\rangle|0^{m-k-1} 1\rangle|\phi\rangle$ .

The general case of  $r_0 \neq 1$  is similarly handled. The desired quantum function  $SIZE_1$  is therefore set to be  $F$ . □

Given an input of the form  $|xr_0\rangle|\phi\rangle$ , it is possible to apply any quantum function  $g$  in  $EQS_0$  to the first segment  $|xr_0\rangle$  with keeping the second segment  $|\phi\rangle$  intact. This can be done by the use of Scheme IV in the following way.

**Lemma 16.** *For any string  $r_0 \in \{0, 1\}^+$  and any quantum function  $g \in \widehat{EQS}_0$  satisfying  $g(|r_0\rangle \otimes |\phi\rangle) = g(|r_0\rangle) \otimes |\phi\rangle$ , there exists another quantum function  $F$  definable within  $EQS_0 + IV$  such that  $F(|xr_0\rangle|\phi\rangle) = g(|xr_0\rangle) \otimes |\phi\rangle$  for any  $x \in \text{NON}_{r_0}$  and any  $|\phi\rangle \in \mathcal{H}_\infty$ .*

*Proof.* Let us recall the quantum function  $Skip_k[g]$  from Lemma 4. For a given  $g \in \widehat{EQS}_0$ , we set  $h \equiv g \circ Skip_{|r_0|}[g^{-1}]$ . Notice that  $h$  belongs to  $\widehat{EQS}_0$  because  $g^{-1}$  exists within  $\widehat{EQS}_0$

(as shown in Lemma 23). The desired quantum function  $F$  is defined by Scheme IV as  $F \equiv CFQRec_1[r_0, I, g, h | \mathcal{P}_{|r_0|}, \mathcal{F}_{|r_0|}]$ , where  $\mathcal{P}_{|r_0|} = \{p_u\}_{u \in \{0,1\}^{|r_0|}}$  with  $p_u = I$  for all  $u$ 's and  $\mathcal{F}_{|r_0|} = \{f_u\}_{u \in \{0,1\}^{|r_0|}}$  with  $f_u = F$  for all  $u$ 's. As a special case, we then obtain  $F(|r_0\rangle|\phi\rangle) = g(|r_0\rangle|\phi\rangle) = g(|r_0\rangle) \otimes |\phi\rangle$ .

Assume by induction hypothesis that  $F(|xr_0\rangle|\phi\rangle) = g(|xr_0\rangle) \otimes |\phi\rangle$ . Let us consider  $F(|axr_0\rangle|\phi\rangle)$  for an arbitrary string  $a \in \{0, 1\}^{|r_0|} \cap NON_{r_0}$ . It then follows that  $|\zeta_{a,I,\phi}^{(xr_0)}\rangle = \sum_{s:|s|=LH(|\phi\rangle)} (F(|xr_0\rangle) \otimes |s\rangle) \otimes \langle s|\phi\rangle = \sum_{s:|s|=LH(|\phi\rangle)} (g(|xr_0\rangle) \otimes |s\rangle) \langle s|\phi\rangle = g(|xr_0\rangle) \otimes |\phi\rangle$ . We therefore conclude that  $F(|axr_0\rangle|\phi\rangle) = \sum_{v:|v|=|xr_0|} (h(|a\rangle|v\rangle) \otimes |v\rangle) \langle \zeta_{a,I,\phi}^{(xr_0)} | \rangle = \sum_{v:|v|=|xr_0|} (h(|a\rangle|v\rangle) \otimes |v\rangle) \langle \psi_{g,xr_0} | \rangle \otimes |\phi\rangle = h(|a\rangle|\psi_{g,xr_0}\rangle) \otimes |\phi\rangle = h(|a\rangle) \otimes g(|xr_0\rangle) \otimes |\phi\rangle$  since  $|v\rangle = |xr_0\rangle$ , where  $|\psi_{g,xr_0}\rangle = g(|xr_0\rangle)$ . Because  $h(|a\rangle) \otimes g(|xr_0\rangle)$  equals  $g(|a\rangle) \otimes g^{-1}(g(|xr_0\rangle)) = g(|axr_0\rangle)$ , it follows that  $F(|0xr_0\rangle|\phi\rangle) = g(|axr_0\rangle) \otimes |\phi\rangle$ , as requested.  $\square$

As shown in Proposition 18, Scheme IV turns out to be so powerful that it generates quantum functions, which can modify the first segment,  $|xr_0\rangle$ ,  $\text{ilog}(\ell(|\phi\rangle))$  times for any given input of the form  $|xr_0\rangle|\phi\rangle$ .

Let  $h$  be any quantum function defined by Schemes I–III. Consider a quantum function  $\hat{h}$  defined inductively as

$$(*) \quad \hat{h}(|r_0\rangle) = |r_0\rangle \text{ and } \hat{h}(|xr_0\rangle) = \sum_{u:|u|=|r_0|} h(|u\rangle) \otimes \hat{h}(|uxr_0\rangle)$$

for any  $x \in NON_{r_0}$  with  $x \neq \lambda$ . This recursive construction scheme  $(*)$  looks similar to Scheme T but it is not supported in our system  $EQS_0 + IV$ . Nevertheless, as shown in Proposition 18, whenever the length of an input qustring  $|xr_0\rangle$  is “short” enough compared to another supplemental input qustring  $|\phi\rangle$ , it may be possible to “realize” this scheme within  $EQS_0 + IV$ .

**Example 17.** As a concrete example of the above function  $\hat{h}$ , we consider  $CodeSKIP_+[r_0, g, I]$  (as well as  $CodeSKIP_-[r_0, g, I]$ ) for a norm-preserving quantum function  $g$ . To see this, we set  $h$  to be  $g \circ Skip_{|r_0|}[g^{-1}]$  and define  $\hat{h}$  from  $h$  by applying the above scheme  $(*)$ . Here, we wish to claim that this quantum function  $\hat{h}$  coincides with  $CodeSKIP_+[r_0, g, I]$ . Initially, we obtain  $CodeSKIP_+[r_0, g, I](|r_0\rangle) = |r_0\rangle = \hat{h}(|r_0\rangle)$  by  $(*)$ . For any two strings  $a, x \in NON_{r_0} \cap \{0, 1\}^+$  with  $|a| = |r_0|$ , it follows from  $(*)$  that  $\hat{h}(|axr_0\rangle) = \sum_{u:|u|=|r_0|} h(|u\rangle) \otimes \hat{h}(|uaxr_0\rangle) = h(|a\rangle) \otimes CodeSKIP_+[r_0, g, I](|xr_0\rangle) = h(|a\rangle) \otimes g(|xr_0\rangle) = g \circ Skip_{|r_0|}[g^{-1}](|a\rangle) \otimes g(|xr_0\rangle) = g(|axr_0\rangle)$ .

The quantum function  $\hat{h}$  given by the recursive scheme  $(*)$  may not be constructed by the only use of Schemes I–IV since the  $k$ -qubit quantum recursion scheme is required. For relatively “short” inputs, however, it is possible to compute the value of  $\hat{h}$  within the existing system  $EQS_0 + IV$ .

**Proposition 18.** For a quantum function  $h$  in  $EQS_0$ , let  $\hat{h}$  satisfy the conditions of the aforementioned recursive scheme  $(*)$ . There exists a quantum function  $F$  definable within  $EQS_0 + IV$  such that, for any  $(x, |\phi\rangle)$  with  $x \in NON_{r_0}$  and  $|\phi\rangle \in \mathcal{H}_\infty$ , if  $|x| \leq |r_0| \log \ell(|\phi\rangle)$ , then  $F(|xr_0\rangle|\phi\rangle) = \hat{h}(|xr_0\rangle) \otimes |\phi\rangle$  holds. However, there is no guarantee that  $F(|xr_0\rangle|\phi\rangle)$  matches  $\hat{h}(|xr_0\rangle) \otimes |\phi\rangle$  when  $|x| > |r_0| \log \ell(|\phi\rangle)$ .

*Proof.* Assume that  $|x| \leq |r_0| \log \ell(|\phi\rangle)$ . Consider the quantum function  $F \equiv CFQRec_{|r_0|-1}[r_0, I, g, h | \mathcal{P}_{|r_0|}, \mathcal{F}_{|r_0|}]$ , where  $\mathcal{P}_{|r_0|} = \{p_u\}_{u \in \{0,1\}^{|r_0|}}$  and  $\mathcal{F}_{|r_0|} = \{f_u\}_{u \in \{0,1\}^{|r_0|}}$  with  $p_u \equiv I$  and  $f_u \equiv F$  for all  $u \in \{0, 1\}^{|r_0|}$ . We verify the proposition by induction on the

number of applications of  $F$ . In the base case, we obtain  $F(|r_0\rangle|\phi\rangle) = |r_0\rangle|\phi\rangle = \hat{h}(|r_0\rangle) \otimes |\phi\rangle$  since  $\hat{h}(|r_0\rangle) = |r_0\rangle$  by (\*). Next, we consider any string  $ax$  with  $a \in \{0, 1\}^{|r_0|} \cap \text{NON}_{r_0}$  and  $x \in \text{NON}_{r_0}$ . We obtain  $F(|xr_0\rangle|\phi\rangle) = \hat{h}(|xr_0\rangle) \otimes |\phi\rangle$  by induction hypothesis. It then follows that  $F(|axr_0\rangle|\phi\rangle) = \sum_{v:|v|=|xr_0|} (h(|a\rangle \otimes |v\rangle) \otimes \langle v|\zeta_{a,I,\phi}^{(xr_0)}\rangle)$ , where  $|\zeta_{a,I,\phi}^{(xr_0)}\rangle = \sum_{s:|s|=LH(|\phi\rangle)} (F(|xr_0\rangle \otimes |s\rangle) \otimes \langle s|\phi\rangle)$ . Since  $F(|xr_0\rangle|\phi\rangle) = \hat{h}(|xr_0\rangle) \otimes |\phi\rangle$ ,  $|\zeta_{a,I,\phi}^{(xr_0)}\rangle$  equals  $\sum_{s:|s|=LH(|\phi\rangle)} (\hat{h}(|xr_0\rangle) \otimes |s\rangle \otimes \langle s|\phi\rangle) = \hat{h}(|xr_0\rangle) \otimes |\phi\rangle$ . We briefly write  $|\psi_{\hat{h},xr_0}\rangle$  for  $\hat{h}(|xr_0\rangle)$ . We then obtain  $F(|axr_0\rangle|\phi\rangle) = \sum_{v:|v|=|xr_0|} (h(|a\rangle \otimes |v\rangle) \otimes \langle v|\psi_{\hat{h},xr_0}\rangle) \otimes |\phi\rangle$ . This implies that  $F(|axr_0\rangle|\phi\rangle) = h(|a\rangle \otimes \hat{h}(|xr_0\rangle)) \otimes |\phi\rangle = \hat{h}(|axr_0\rangle) \otimes |\phi\rangle$  by the definition of  $\hat{h}$ .  $\square$

Since  $\text{CodeSKIP}_+[\cdot]$  can be realized by the recursive construction scheme (\*), Proposition 18 allows us to use  $\text{CodeSKIP}_+[\cdot]$  freely as if it is a quantum function in  $\text{EQS}_0 + IV$ .

**Corollary 1.** *There exists a quantum function  $F$  definable within  $\text{EQS}_0 + IV$  such that  $F(|xr_0\rangle|\phi\rangle) = \text{CodeSKIP}_+[r_0, g, I](|xr_0\rangle|\phi\rangle)$  if  $|x| \leq |r_0| \log \ell(|\phi\rangle)$ .*

### 3.5 Elementary quantum schemes

Formally, let us introduce  $\widehat{\text{EQS}}$  and  $\text{EQS}$ . We have already explained Schemes I–IV. Now, we wish to add the final piece of construction schemes, called Scheme V, which intuitively supports successive  $\text{ilog}(\ell(|\phi\rangle))$  applications of  $\text{Compo}[g, g]$  for a given quantum function  $g$  taking  $|xr_0\rangle|\phi\rangle$  as an input.

**Definition 19.** *We introduce the following scheme.*

V. *The logarithmically many composition scheme. From  $g$ , we define  $L\text{Compo}[g]$  as follows:*

- (i)  $L\text{Compo}[g](|xr_0\rangle|\phi\rangle) = |xr_0\rangle \otimes |\phi\rangle$  *if  $x = \lambda$ ,  $\ell(|\phi\rangle) \leq 1$ , or  $|x| > |r_0|k$ ,*
- (ii)  $L\text{Compo}[g](|xr_0\rangle|\phi\rangle) = g^k(|xr_0\rangle|\phi\rangle)$  *otherwise,*

where  $x \in \text{NON}_{r_0}$  and  $k = \text{ilog}(\ell(|\phi\rangle))$ .

When  $g$  is query-independent, we say that Scheme V is *query-independent*. We remark that query-independent Scheme V is actually redundant because Proposition 18 helps us realize  $L\text{Compo}[g]$  by an application of Scheme IV.

**Definition 20.** *The class  $\text{EQS}$  is the smallest set of (code-controlled) quantum functions that contains the quantum functions of Scheme I and is closed under Schemes II–V. Similarly,  $\widehat{\text{EQS}}$  is defined with no use of Item 6) of Scheme I.*

Note that any quantum function  $F$  in  $\text{EQS}$  is constructed by sequential applications of Schemes I–V. Such a finite series is referred to as a *construction history* of  $F$ . The length of this construction history serves as a *descriptive complexity measure* of  $F$ . Refer to (Yamakami, 2020) for more discussions.

## 4. Quantum functions definable within EQS

In Section 3.5, we have introduced the system  $\widehat{\text{EQS}}$  as well as  $\text{EQS}$ . In this section, we will study the basic properties of all quantum functions in  $\widehat{\text{EQS}}$  and  $\text{EQS}$  by introducing several useful quantum functions and extra schemes, which are also definable within  $\text{EQS}$ . One of the most important properties we can show is an implementation of a simple “binary search strategy” in  $\text{EQS}$ .

**4.1 Basic properties of  $\widehat{EQS}$**

The only difference between  $\widehat{EQS}$  and  $EQS$  is the free use of Item 6) (quantum measurement) of Scheme I. Since  $\widehat{EQS}$  does not involve quantum measurement, we naturally expect that  $\widehat{EQS}$  enjoys the unitary nature of quantum computation described in the following three lemmas, Lemmas 21–23.

**Lemma 21.** *Any quantum function in  $\widehat{EQS}$  is dimension-preserving and norm-preserving.*

*Proof.* Let us check Schemes I–V separately to verify the lemma. Note that Items 1)–5) of Scheme I are clearly dimension-preserving and norm-preserving. The lemma was already shown for Schemes II–III by Yamakami (2020). Therefore, it suffices to check Schemes IV and V. Let  $F \equiv CFQRec_t[r_0, g, h | \mathcal{P}_{|r_0|}, \mathcal{F}_{|r_0|}]$  be any quantum function defined by Scheme IV. It is easy to verify that *HalfSWAP* is dimension-preserving and norm-preserving. Thus, so are all quantum functions in  $\mathcal{P}_{|r_0|}$ . By induction hypothesis, we assume that  $g$  and  $h$  are dimension-preserving and norm-preserving. In what follows, we argue by way of induction on the input length of  $F$  that  $F$  is dimension-preserving and norm-preserving. If either  $x = \lambda$  or  $\ell(|\phi\rangle) \leq t$ , then we obtain  $\ell(F(|xr_0\rangle|\phi)) = \ell(g(|xr_0\rangle|\phi)) = \ell(|xr_0\rangle|\phi)$  and  $\|F(|xr_0\rangle|\phi)\| = \|g(|xr_0\rangle|\phi)\| = \||xr_0\rangle|\phi\rangle\|$ .

Let us consider the case where  $x \neq \lambda$  and  $\ell(|\phi\rangle) > t$ . We then obtain  $\ell(h(|u\rangle|v)) \otimes p_u^{-1}(\langle v|\zeta_{u,p_u,\phi}\rangle) = \ell(|u\rangle) + \ell(|v\rangle\langle v|\zeta_{u,p_u,\phi}) = \ell(|xr_0\rangle) - |r_0| + \ell(|\zeta_{u,p_u,\phi}\rangle)$ . By induction hypothesis, we obtain  $\ell(F(\langle u|xr_0\rangle|s)) = \ell(\langle u|xr_0\rangle|s)$ . This implies that  $\ell(|\zeta_{u,p_u,\phi}\rangle) = \ell(\sum_s F(\langle u|xr_0\rangle|s) \otimes \langle s|\psi_{p_u,\phi}\rangle) = \ell(\langle u|xr_0\rangle|\phi)$ . It then follows that  $\ell(F(|xr_0\rangle|\phi)) = \ell(\sum_u \sum_v h(|u\rangle|v) \otimes p_u^{-1}(\langle v|\zeta_{u,p_u,\phi}\rangle)) = \ell(|xr_0\rangle|\phi)$ . The property of norm-preserving is similarly proven.

For Scheme V, it is obvious that, if  $g$  is dimension-preserving and norm-preserving, then so is  $g^k$  for any number  $k \in \mathbb{N}^+$ . Thus,  $LCompo[g]$  satisfies the lemma.  $\square$

We further discuss two useful construction schemes, which are definable within  $\widehat{EQS}$ .

**Lemma 22.** *Let  $k \in \mathbb{N}^+$  and let  $\mathcal{G}_k = \{g_u\}_{u \in \{0,1\}^k}$  be a series of  $\widehat{EQS}$ -functions. The following quantum functions all belong to  $\widehat{EQS}$ . The lemma also holds even if  $\widehat{EQS}$  is replaced by  $EQS$ . Let  $|\phi\rangle$  be any quantum state in  $\mathcal{H}_\infty$  and let  $x \in \{0, 1\}^k$ .*

1.  $Compo[\mathcal{G}_k](|\phi\rangle) = g_{s_1} \circ g_{s_2} \circ \dots \circ g_{s_{2^k}}(|\phi\rangle)$ . (multiple composition)
2.  $Branch_k[\mathcal{G}_k](|\phi\rangle) = |\phi\rangle$  if  $\ell(|\phi\rangle) < k$  and  $Branch_k[\mathcal{G}_k](|\phi\rangle) = \sum_{s:|s|=k} |s\rangle \otimes g_s(|\phi\rangle)$  otherwise.

*Proof.* (1)–(2) The above schemes were shown in (Yamakami, 2020, Lemma 3.6) to be valid for  $\square_1^{QP}$  and  $\square_1^{QP}$ , and their argument also work for  $EQS$  and  $\widehat{EQS}$ .  $\square$

As a quick example of  $Branch_k[\mathcal{G}_k]$ , let us recall the quantum function  $Skip_k[g]$  from Lemma 4. It is obvious that  $Skip_k[g]$  is simply defined to be  $Branch_k[\{g_u\}_{u \in \{0,1\}^k}]$  with  $g_u = g$  for all  $u \in \{0, 1\}^k$ .

For any given quantum function, when there exists another quantum function  $g$  satisfying  $f \circ g(|\phi\rangle) = g \circ f(|\phi\rangle) = |\phi\rangle$  for any  $|\phi\rangle \in \mathcal{H}_\infty$ , we express this  $g$  as  $f^{-1}$  (or sometimes  $f^\dagger$ ) and call it the *inverse (function) of  $f$* .

**Lemma 23.** *For any quantum function  $g$  in  $\widehat{EQS}$ , its inverse function  $g^{-1}$  exists in  $\widehat{EQS}$ . Moreover, if  $g$  is in  $\widehat{EQS}_0$ , then  $g^{-1}$  is also in  $\widehat{EQS}_0$ .*

*Proof.* For Scheme I, it is obvious that  $PHASE_{\theta}^{-1} = PHASE_{-\theta}$ ,  $ROT_{\theta}^{-1} = ROT_{-\theta}$ ,  $NOT^{-1} = NOT$ , and  $SWAP^{-1} = SWAP$ . For Scheme II,  $Compo[g, h]^{-1}$  equals  $Compo[h^{-1}, g^{-1}]$ . For Scheme III, it suffices to set  $Branch[g, h]^{-1}$  to be  $Branch[g^{-1}, h^{-1}]$ . For Scheme IV, let  $F \equiv CFQRec_t[r_0, d, g, h | \mathcal{P}_{|r_0|}, \mathcal{F}_{|r_0|}]$ . If  $x = \lambda$ ,  $\ell(|\phi\rangle) \leq t$ , or  $|x| > |r_0|k$  with  $k = \text{ilog}(\ell(|\phi\rangle))$ , then we set  $F^{-1} \equiv g^{-1}$ . In this case, we obtain  $F^{-1} \circ F(|x_{r_0}\rangle|\phi\rangle) = F^{-1}(g(|x_{r_0}\rangle|\phi\rangle)) = g^{-1} \circ g(|x_{r_0}\rangle|\phi\rangle) = |x_{r_0}\rangle|\phi\rangle$ . Assuming otherwise, we define  $F^{-1}$  to be the consecutive applications of two quantum functions:  $h^{-1}$  and  $G \equiv CFQRec_t[r_0, d^{-1}, g^{-1}, I | \mathcal{P}_{|r_0|}, \mathcal{F}_{|r_0|}^{-1}]$ , where  $\mathcal{F}_{|r_0|}^{-1} = \{f_u^{-1}\}_{u \in \{0,1\}^{|r_0|}}$ . It is important to note that we do not use  $\mathcal{P}_{|r_0|}^{-1} = \{p_u^{-1}\}_{u \in \{0,1\}^{|r_0|}}$  in place of  $\mathcal{P}_{|r_0|}$  in the definition of  $G$ . Let us show that  $F^{-1} \circ F(|x_{r_0}\rangle|\phi\rangle) = |x_{r_0}\rangle|\phi\rangle$ . Assume that  $F(|x_{r_0}\rangle|\phi\rangle)$  has the form  $\sum_{u:|u|=|r_0|} \sum_{v:|v|=\ell(\langle u|x_{r_0}\rangle)} (h(|u\rangle|v\rangle) \otimes p_u^{-1}(\langle v|\zeta_{u,p_u,\phi}^{(x'_{r_0})}\rangle))$ . We first apply  $h^{-1}$  to the first  $|x_{r_0}|$  qubits and then obtain  $\sum_{u:|u|=|r_0|} \sum_{v:|v|=\ell(\langle u|x_{r_0}\rangle)} (|u\rangle|v\rangle \otimes p_u^{-1}(\langle v|\zeta_{u,p_u,\phi}^{(x'_{r_0})}\rangle))$ . To this quantum state, we further apply  $G$ . By an application of  $p_u$  to  $p_u^{-1}(\langle v|\zeta_{u,p_u,\phi}^{(x'_{r_0})}\rangle)$ , we obtain  $\sum_{u:|u|=|r_0|} \sum_{v:|v|=\ell(\langle u|x_{r_0}\rangle)} |u\rangle|\zeta_{u,p_u,\phi}^{(x'_{r_0})}\rangle$ . Notice that  $|\zeta_{u,p_u,\phi}^{(x'_{r_0})}\rangle$  equals  $\sum_{s:|s|=m_u(\phi)} (f_u(\langle u|x'_{r_0}\rangle \otimes |s\rangle) \otimes \langle s|\psi_{p_u,\phi}\rangle)$ . An application of  $f_u^{-1}$  to  $f_u(\langle u|x'_{r_0}\rangle \otimes |s\rangle)$  leads to  $\sum_{u:|u|=|r_0|} \langle u|x'_{r_0}\rangle \otimes |\psi_{p_u,\phi}\rangle$ . Since  $|x'_{r_0}\rangle = d(|x_{r_0}\rangle)$ , by applying  $d^{-1}$  and  $p_u^{-1}$  (which come from the definition of  $G$ ), we finally obtain  $|x_{r_0}\rangle \otimes |\phi\rangle$ . For Scheme V, it suffices to set  $LCompo[g]^{-1}$  to be  $LCompo[g^{-1}]$ .

The above argument also proves the second part of the lemma. □

**4.2 Section-wise handling of binary encoding**

We have discussed in Section 3.2 the binary encodings of various objects usable as part of inputs. We further explore the characteristics of quantum functions that can handle these binary encodings.

Given  $k$  encoded strings  $\tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_k$ , we merge them into a single string of the form  $\tilde{x}_1\tilde{x}_2 \cdots \tilde{x}_k\hat{2}$ , where  $\hat{2}$  serves as an endmarker. Let  $k \geq 2$  and let  $\mathcal{G} = \{g_i\}_{i \in [k]}$  denote a series of  $k$  quantum functions. We then consider a simultaneous application of all quantum functions in  $\mathcal{G}$ ,  $MultiApp_k[\mathcal{G}]$ , given as

$$\begin{aligned} &MultiApp_k[\hat{2}, \mathcal{G}] (|\tilde{x}_1\tilde{x}_2 \cdots \tilde{x}_k\hat{2}\rangle|\phi\rangle) \\ &= g_1(|\tilde{x}_1\rangle) \otimes g_2(|\tilde{x}_2\rangle) \otimes \cdots \otimes g_k(|\tilde{x}_k\hat{2}\rangle) \otimes |\phi\rangle. \end{aligned}$$

**Lemma 24.** *For any  $k \geq 2$  and any series  $\mathcal{G} = \{g_i\}_{i \in [k]}$  of  $k$  quantum functions, the quantum function  $MultiApp_k[\hat{2}, \mathcal{G}]$  is definable from  $\mathcal{G}$  and the code skipping scheme.*

*Proof.* Let  $\mathcal{G} = \{g_i\}_{i \in [k]}$  denote any series of  $k$  quantum functions, not necessarily in EQS. For brevity, we set  $\bar{r}_0 = \hat{1}$  and  $r_0 = \hat{2}$ . The quantum function  $MultiApp_k[\hat{2}, \mathcal{G}]$  is constructed from  $\mathcal{G}$  by applying  $CodeSKIP_+[\cdot]$  in the following inductive way. Initially, we set  $G_{[k,k]} \equiv CodeSKIP_+[r_0, g_k, I]$ . Let  $X_k = \tilde{x}_k (= \hat{x}_k\hat{1})$ . Since  $NON_{r_0}(|X_k\rangle|r_0\rangle|\phi\rangle) = \{X_k\}$ , we obtain  $G_{[k,k]}(|X_k\rangle|r_0\rangle|\phi\rangle) = g_k(|X_k\rangle|r_0\rangle) \otimes |\phi\rangle$ . Let  $i$  be any index in  $[k-1]$  and set  $X_{i+1} = \tilde{x}_{i+1}\tilde{x}_{i+2} \cdots \tilde{x}_k$ . We assume by induction hypothesis that  $G_{[i+1,k]}(|X_{i+1}\rangle|r_0\rangle|\phi\rangle) = g_{i+1}(|\tilde{x}_{i+1}\rangle) \otimes g_{i+2}(|\tilde{x}_{i+2}\rangle) \otimes \cdots \otimes g_k(|\tilde{x}_k\rangle|r_0\rangle) \otimes |\phi\rangle$ . We then define  $G_{[i,k]} \equiv CodeSKIP_+[\bar{r}_0, g_i, G_{[i+1,k]}]$ . Since  $NON_{\bar{r}_0}(|X_i\rangle|r_0\rangle|\phi\rangle) = \{\hat{x}_i\}$ , it follows that  $G_{[i,k]}(|X_i\rangle|r_0\rangle|\phi\rangle) = g_i(|\hat{x}_i\bar{r}_0\rangle) \otimes G_{[i+1,k]}(|X_{i+1}\rangle|r_0\rangle|\phi\rangle) = g_i(|\tilde{x}_i\rangle) \otimes g_{i+1}(|\tilde{x}_{i+1}\rangle) \otimes \cdots \otimes g_k(|\tilde{x}_k\rangle|r_0\rangle) \otimes |\phi\rangle$ .

The desired quantum function  $MultiApp_k[r_0, \mathcal{G}]$  therefore equals  $G_{[1,k]}$ , which is  $g_1(|\tilde{x}_1\rangle) \otimes g_2(|\tilde{x}_2\rangle) \otimes \cdots \otimes g_k(|\tilde{x}_k\hat{2}\rangle) \otimes |\phi\rangle$ . □

By Lemma 24, we can construct  $MultiApp_k[\hat{2}, \mathcal{G}]$  from  $\mathcal{G} = \{g_i\}_{i \in [k]}$  and  $CodeSKIP_+[r_0, g, h]$ . Since  $CodeSKIP_+[r_0, g, h]$  stays outside of EQS,  $MultiApp_k[\hat{2}, \mathcal{G}]$  in general does not belong to EQS. However, as the next lemma ensures, we can use  $MultiApp_k[\hat{2}, \mathcal{G}]$  as if it is an EQS function under certain circumstances.

To describe our result, let us recall the 3-bit encoding of  $\hat{S}$ , which indicates “separator”.

**Lemma 25.** *Let  $k \in \mathbb{N}^+$  and let  $\mathcal{G} = \{g_i\}_{i \in [k]}$  be any series of  $k$  quantum functions in EQS. There exists a quantum function  $F$  in EQS such that  $F(|\hat{S}\tilde{x}_1\tilde{x}_2 \cdots \tilde{x}_k\hat{2}\rangle|\phi\rangle) = MultiApp_k[\hat{2}, \mathcal{G}](|\hat{S}\tilde{x}_1\tilde{x}_2 \cdots \tilde{x}_k\hat{2}\rangle|\phi\rangle)$  as long as  $|\hat{S}\tilde{x}_1\tilde{x}_2 \cdots \tilde{x}_k\hat{2}\rangle \leq |\hat{2}\rangle \log \ell(|\phi\rangle)$ . However, the equality may not hold if  $|\hat{S}\tilde{x}_1\tilde{x}_2 \cdots \tilde{x}_k\hat{2}\rangle > |\hat{2}\rangle \log \ell(|\phi\rangle)$ .*

*Proof.* Let  $k \in \mathbb{N}^+$  and let  $\mathcal{G} = \{g_i\}_{i \in [k]}$  be given as in the premise of the lemma. Since  $|\hat{2}\rangle = 3$ , we set  $h$  to be  $Branch_3[\{h_u\}_{u \in \{0,1\}^3}]$  with  $h_{\hat{S}} \equiv MultiApp_k[\hat{2}, \mathcal{G}]$  and  $h_u \equiv I$  for any  $u \neq \hat{S}$ . The desired quantum function  $F$  is defined to be  $CFQRec_1[\hat{2}, I, I, h|\mathcal{P}_3, \mathcal{F}_3]$ , where  $\mathcal{P}_3 = \{p_u\}_{u \in \{0,1\}^3}$  with  $p_u = I$  for all  $u \in \{0, 1\}^3$  and  $\mathcal{F}_3 = \{f_u\}_{u \in \{0,1\}^3}$  with  $f_u = F$  for all  $u \in \{0, 1\}^3$ . Because of  $|\hat{S}\tilde{x}_1\tilde{x}_2 \cdots \tilde{x}_k\hat{2}\rangle \leq |\hat{2}\rangle \log \ell(|\phi\rangle)$ , in the following recursive process of computing  $F$ , it suffices to start with  $F(|\hat{2}\rangle|\phi'\rangle)$  with  $\ell(|\phi'\rangle) \geq 1$ .

For each index  $i \in [k]$ , we abbreviate  $\tilde{x}_i\tilde{x}_{i+1} \cdots \tilde{x}_k$  as  $X_i$ . In what follows, we fix  $i \in [k]$  arbitrarily and assume that  $F(|X_i\hat{2}\rangle|\phi\rangle) = |X_i\hat{2}\rangle|\phi\rangle$ . Note that  $|\zeta_{u,I,\phi}\rangle = \sum_{s:|s|=LH(|\phi\rangle)} (F(|u|X_{i-1}\hat{2}\rangle|s\rangle) \otimes \langle s|\phi\rangle)$ . If  $u = \tilde{x}_{i-1}$ , then  $|\zeta_{u,I,\phi}\rangle = \sum_{s:|s|=LH(|\phi\rangle)} (F(|X_i\hat{2}\rangle|s\rangle) \otimes \langle s|\phi\rangle) = \sum_{s:|s|=LH(|\phi\rangle)} (|X_i\hat{2}\rangle|s\rangle \otimes \langle s|\phi\rangle) = |X_i\hat{2}\rangle|\phi\rangle$ . From this, it follows that  $F(|X_i\hat{2}\rangle|\phi\rangle) = h(|\tilde{x}_{i-1}\rangle|X_i\hat{2}\rangle) \otimes \langle X_i\hat{2}|\zeta_{\tilde{x}_{i-1},I,\phi}\rangle = |X_{i-1}\hat{2}\rangle|\phi\rangle$ . Finally, we consider the case of  $|\hat{S}\rangle|X_1\hat{2}\rangle|\phi\rangle$ . We then obtain  $F(|\hat{S}\rangle|X_1\hat{2}\rangle|\phi\rangle) = h(|\hat{S}\rangle|X_1\hat{2}\rangle) \otimes \langle X_1\hat{2}|\zeta_{\hat{S},I,\phi}\rangle$ . Since  $|\zeta_{\hat{S},I,\phi}\rangle = |X_1\hat{2}\rangle \otimes |\phi\rangle$ , it follows that  $F(|\hat{S}\rangle|X_1\hat{2}\rangle|\phi\rangle) = h(|\hat{S}\rangle|X_1\hat{2}\rangle) \otimes \langle X_1\hat{2}|X_1\hat{2}\rangle|\phi\rangle = h(|\hat{S}\rangle|X_1\hat{2}\rangle) \otimes |\phi\rangle = Branch_3[\{h_u\}_{u \in \{0,1\}^3}] (|\hat{S}\rangle|X_1\hat{2}\rangle) \otimes |\phi\rangle = MultiApp_k[\hat{2}, \mathcal{G}] (|\hat{S}\rangle|X_1\hat{2}\rangle) \otimes |\phi\rangle$ . □

In a certain limited case, Lemma 25 makes possible a repeated application of any quantum function within  $EQS_0 + IV$  (as well as EQS). Let us recall the notation  $\hat{T}$ , which indicates “time”.

**Proposition 26.** *Let  $r_0 \in \{0, 1\}^+$  and let  $g$  be any quantum function definable within  $EQS_0 + IV$  (resp., EQS). There exists a quantum function  $F$  definable within  $EQS_0 + IV$  (resp., EQS) such that, for any  $|\phi\rangle \in \mathcal{H}_\infty$  and  $x \in \{0, 1\}^*$ , if  $\ell(|\phi\rangle) \leq 1$ , then  $F(|\hat{T}^{m(|\phi\rangle)}\hat{S}\rangle|x\hat{2}\rangle|\phi\rangle) = |\hat{T}^{m(|\phi\rangle)}\hat{S}\rangle|x\hat{2}\rangle|\phi\rangle$ , and otherwise,  $F(|\hat{T}^{m(|\phi\rangle)}\hat{S}\rangle|x\hat{2}\rangle|\phi\rangle) = |\hat{T}^{m(|\phi\rangle)}\hat{S}\rangle \otimes g^{m(|\phi\rangle)}(|x\hat{2}\rangle) \otimes |\phi\rangle$ , where  $m(|\phi\rangle) = \text{ilog}(\ell(|\phi\rangle))$ .*

*Proof.* Let  $F$  denote the desired quantum function. Remember that  $|\hat{2}\rangle = |\hat{T}\rangle = |\hat{S}\rangle = 3$ . We set  $\mathcal{P}_3 = \{p_u\}_{u \in \{0,1\}^3}$  with  $p_u = I$  for all  $u \in \{0, 1\}^3$  and set  $\mathcal{G} = \{g_u\}_{u \in \{0,1\}^3}$  with  $g_{\hat{T}} = CodeSKIP_+[\hat{S}, I, g]$ , and  $g_u = I$  for all other indices  $u \in \{0, 1\}^3 - \{\hat{T}\}$ . We then define  $h$  to be  $Branch_3[\mathcal{G}]$ . Finally,  $F$  is defined as  $F \equiv CFQRec_1[\hat{2}, I, I, h|\mathcal{P}_3, \mathcal{F}_3]$ , where  $\mathcal{F}_3 = \{f_u\}_{u \in \{0,1\}^3}$  with  $f_u = F$  for all  $u \in \{0, 1\}^3$ .

For any index  $i \in [0, m(|\phi\rangle)]_{\mathbb{Z}}$ , we set  $z_i = \hat{T}^{m(|\phi\rangle)-i}$ . If  $\ell(|\phi\rangle) \leq 1$ , then we obtain  $F(|z_i\hat{S}\rangle|x\hat{2}\rangle|\phi\rangle) = |z_i\hat{S}\rangle|x\hat{2}\rangle|\phi\rangle$  for any  $i \in [0, m(|\phi\rangle)]_{\mathbb{Z}}$ . Next, we assume that  $\ell(|\phi\rangle) \geq 2$ . Let  $i \in [0, m(|\phi\rangle)]_{\mathbb{Z}}$  and set  $y = z_i\hat{S}x$ . By induction hypothesis,  $F(|z_{i+1}\hat{S}\rangle|x\hat{2}\rangle|\phi\rangle) = |z_{i+1}\hat{S}\rangle \otimes g^{m(|\phi\rangle)-i-1}(|x\hat{2}\rangle) \otimes |\phi\rangle$  holds. Let us consider the value  $F(|z_i\hat{S}\rangle|x\hat{2}\rangle|\phi\rangle)$ . Note that  $h(|z_i\hat{S}\rangle \otimes g^{m(|\phi\rangle)-i}(|x\hat{2}\rangle)) = CodeSKIP_+[\hat{S}, I, g] (|z_i\hat{S}\rangle \otimes g^{m(|\phi\rangle)-i}(|x\hat{2}\rangle)) = |z_i\hat{S}\rangle \otimes g^{m(|\phi\rangle)-i-1}(|x\hat{2}\rangle)$ . It thus



follows that  $F(|z_i\hat{S}\rangle|x\hat{2})|\phi\rangle = \sum_{u:|u|=|\hat{2}|} \sum_{v:|v|=\ell(\langle u|y\hat{2}\rangle)} (h(|u\rangle \otimes |v\rangle) \otimes \langle v|\zeta_{u,I,\phi}\rangle)$ , where  $|\zeta_{u,I,\phi}\rangle$  is calculated as follows. If  $u \neq \hat{T}$ , then  $|\zeta_{u,I,\phi}\rangle = \mathbf{0}$  holds. Otherwise,  $|\zeta_{u,I,\phi}\rangle$  is equal to  $\sum_{s:|s|=LH(|\phi\rangle)} (F(\langle u|z_i\hat{S}\rangle|x\hat{2}) \otimes |s\rangle) \otimes \langle s|\phi\rangle = \sum_{s:|s|=LH(|\phi\rangle)} (F(|z_{i+1}\hat{S}\rangle|x\hat{2}) \otimes |s\rangle) \otimes \langle s|\phi\rangle = \sum_{s:|s|=LH(|\phi\rangle)} h(|z_{i+1}\hat{S}\rangle \otimes g^{m(|\phi\rangle)-i-1}(|x\hat{2}\rangle) \otimes |s\rangle \langle s|\phi\rangle) = |z_{i+1}\hat{S}\rangle \otimes g^{m(|\phi\rangle)-i-1}(|x\hat{2}\rangle) \otimes |\phi\rangle$ . Thus, we obtain  $F(|z_i\hat{S}\rangle|x\hat{2})|\phi\rangle = |z_i\hat{S}\rangle \otimes g^{m(|\phi\rangle)-i}(|x\hat{2}\rangle) \otimes |\phi\rangle$ . In particular, when  $i = 0$ , we conclude that  $F(|\hat{T}^{m(|\phi\rangle)}\hat{S}\rangle|x\hat{2})|\phi\rangle = |\hat{T}^{m(|\phi\rangle)}\hat{S}\rangle \otimes g^{m(|\phi\rangle)}(|x\hat{2}\rangle) \otimes |\phi\rangle$ .  $\square$

**4.3 Implementing the binary search strategy**

The strength of Scheme IV is further exemplified by an implementation of a simple *binary search* algorithm. Given any string  $x \in \{0, 1\}^k$  with  $k \geq 1$ , assume that  $x$  equals  $bin_k(m)$  for a certain number  $m \in [2^k]$ . For any  $s$  with  $|s| = 2^k$  and  $b \in \{0, 1\}$ , the quantum function *BinSearch* satisfies the following equality:  $BinSearch(|\tilde{x}\rangle|\hat{b}\rangle|\hat{2}\rangle|s\rangle) = |\tilde{x}\rangle|\widehat{b \oplus s_{(m)}}\rangle|\hat{2}\rangle|s\rangle$ , where  $s_{(m)}$  is the  $m$ th bit of  $s$ . This quantum function finds the  $m$ th bit of  $s$  and extracts its bit  $s_{(m)}$  from  $s$  by way of modifying  $|\hat{b}\rangle$  to  $|\widehat{b \oplus s_{(m)}}\rangle$ .

**Theorem 27.** *The above quantum function BinSearch is definable within EQS<sub>0</sub> + IV.*

*Proof.* We remark that the length of  $s$  given to  $BinSearch(|\tilde{x}\rangle|\hat{b}\rangle|\hat{2}\rangle|s\rangle)$  is a power of 2. In this proof, we intend to use the quantum functions  $SecSWAP_{i,j}^{(3)}$  and  $COPY_1$  introduced in Lemmas 6(1) and 7, respectively. Given any strings  $x = x_1x_2 \cdots x_k$ ,  $s = s_1s_2 \cdots s_{2^k}$ , and  $b \in \{0, 1\}$  associated with the number  $m \in [2^k]$  satisfying  $x = bin_k(m)$ , we define the quantum function  $g$  by setting  $g(|\hat{1}\rangle|\hat{b}\rangle|\hat{2}\rangle|s_m\rangle) = |\hat{1}\rangle|\widehat{b \oplus s_m}\rangle|\hat{2}\rangle|s_m\rangle$ . Notice that  $\hat{b} = 00b$  and  $\widehat{b \oplus s_m} = 00b'$  with  $b' = b \oplus s_m$ . It is possible to realize  $g$  by simply setting  $g \equiv SWAP_{7,10} \circ Skip_5[COPY_1] \circ SWAP_{7,10}$  since  $COPY_1(|b\rangle|s_m\rangle|w\rangle) = |b \oplus s_m\rangle|s_m\rangle|w\rangle$  for any  $w$ . Let  $p_0 \equiv I$ ,  $p_1 \equiv HalfSWAP$ , and  $p_u = I$  for all indices  $u \in \{0, 1\}^3 - \{\hat{0}, \hat{1}\}$ . We then define  $F$  to be  $CFQRec_1[\hat{2}, I, g, I|\mathcal{P}_3, \mathcal{F}_3]$ , where  $\mathcal{P}_3 = \{p_u\}_{u \in \{0,1\}^3}$  and  $\mathcal{F}_3 = \{f_u\}_{u \in \{0,1\}^3}$  with  $f_u = F$  for all  $u \in \{0, 1\}^3$ . Now, our goal is to verify that  $F$  indeed matches *BinSearch*.

For any string  $s \in \{0, 1\}^+$  whose length is a power of 2 and for any number  $m \in [|s|]$ , we explain how to find the  $m$ th bit  $s_m$  of  $s$ . We first split  $s$  into the left part and the right part of  $s$  whose lengths are  $LH(|s|)$  and  $RH(|s|)$ , respectively. We assign 0 to the left part and 1 to the right part and we call the left part by  $s_0$  and the right part by  $s_1$ . Starting  $s_0$  (resp.,  $s_1$ ), we further split it into its left part, called  $s_{00}$  (resp.,  $s_{10}$ ), and its right part, called  $s_{01}$  (resp.,  $s_{11}$ ). Inductively, we repeat this process until the target strings become single symbols. In the end, a string  $x \in \{0, 1\}^{\log(|s|)}$  is assigned to the single symbol obtained by the series of the above-described processes. We denote this unique symbol by  $s_x$ . If  $x = bin_{\log(|s|)}(m)$ , then  $s_x$  coincides with the desired bit  $s_m$ . We then treat  $x$  as the binary representation of an index of the symbol  $s_x$  in  $s$ .

Let  $X_{k+1} = \hat{1}$  and let  $X_i = \widehat{x_i x_{i+1} \cdots x_k}$  for any index  $i \in [k]$ . We split  $s$  into two parts as  $s = s^{(l)}s^{(r)}$  with  $|s^{(l)}| = LH(|s|)$  and  $|s^{(r)}| = RH(|s|)$ . We set  $m_1 = m$  and, for each index  $i \in [2, k]_{\mathbb{Z}}$ , we take the number  $m_i$  satisfying  $bin_{k-i+1}(m_i) = x_i x_{i+1} \cdots x_k$ . Note that  $s_{m_i} = s_{m_{i+1}}^{(r)}$  if  $x_i = 1$ , and  $s_{m_i} = s_{m_{i+1}}^{(l)}$  otherwise. When  $\ell(|s|) = 1$ , we conclude that  $F(|X_{k+1}\rangle|\hat{b}\rangle|\hat{2}\rangle|s\rangle) = g(|X_{k+1}\rangle|\hat{b}\rangle|\hat{2}\rangle|s\rangle) = g(|\hat{1}\rangle|\hat{b}\rangle|\hat{2}\rangle|s\rangle) = |\hat{1}\rangle|\widehat{b \oplus s}\rangle|\hat{2}\rangle|s\rangle = BinSearch(|X_{k+1}\rangle|\hat{b}\rangle|\hat{2}\rangle|s\rangle)$ . Next, we assume that  $\ell(|s|) = i \geq 2$ . It follows by induction hypothesis that  $F(|X_{i+1}\rangle|\hat{b}\rangle|\hat{2}\rangle|s^{(r)}\rangle) = |X_{i+1}\rangle|\hat{u}\rangle|\hat{2}\rangle|s^{(r)}\rangle$  with  $u = b \oplus s_{m_{i+1}}^{(r)}$  if  $x_i = 1$ , and  $F(|X_{i+1}\rangle|\hat{b}\rangle|\hat{2}\rangle|s^{(l)}\rangle) = |X_{i+1}\rangle|\hat{v}\rangle|\hat{2}\rangle|s^{(l)}\rangle$  with  $v = b \oplus s_{m_{i+1}}^{(l)}$  otherwise. In the case of  $u = 1$ , since  $|\psi_{p_{\hat{u},s}}\rangle = HalfSWAP(|s\rangle)$ , it follows that  $|\zeta_{\hat{u},p_{\hat{u},s}}\rangle =$

$\sum_{t:|t|=RH(|s|)} (F(|X_{i+1}| \hat{b}\hat{2})|t\rangle) \otimes \langle t|s^{(r)}s^{(l)}\rangle = |X_{i+1}| \hat{u}\rangle \hat{2}|s^{(l)}\rangle$ . Therefore, when  $x_i = 1$ , we obtain  $F(|X_i| \hat{b}\hat{2})|s\rangle = |x_i| |X_{i+1}| \hat{u}\rangle \hat{2}|s\rangle = \text{BinSearch}(|X_i| \hat{b}\hat{2})|s\rangle$ . When  $x_i = 0$ , in contrast, we obtain  $F(|X_i| \hat{b}\hat{2})|s\rangle = |x_i| |X_{i+1}| \hat{v}\rangle \hat{2}|s\rangle = \text{BinSearch}(|X_i| \hat{b}\hat{2})|s\rangle$ .

As a result, we conclude that  $F = \text{BinSearch}$ , as requested. □

Hereafter, we demonstrate how to use the quantum function *BinSearch*. For this purpose, we first show the following statement.

**Corollary 2.** *Given  $|\phi\rangle \in \mathcal{H}_\infty$  and  $x = \text{bin}_k(m)$  for  $k \in \mathbb{N}^+$  and  $m \in [2^k]$ , if  $|\phi\rangle$  is of the form  $\sum_{s:|s|=2^k} \alpha_s |s\rangle$ , then we set  $\text{Bit}(|0^5|b|\hat{x})|\phi\rangle) = \sum_{s:|s|=2^k} \alpha_s |0^5|b \oplus s_{(m)}|\hat{x}|s\rangle$ , where  $s_{(m)}$  is the  $m$ th bit of  $s$ . This quantum function *Bit* is definable within  $\text{EQS}_0 + IV$ .*

*Proof.* Recall the quantum function  $\text{Skip}_k[g]$  from Lemma 4. We first change the quantum state  $|0^5|b|\hat{x})|\phi\rangle$  into  $|\hat{b}\rangle \hat{2}|\hat{x})|\phi\rangle$  by applying  $h \equiv \text{SWAP}_{1,4} \circ \text{SWAP}_{2,5} \circ \text{SWAP}_{3,6} \circ \text{Skip}_2[\text{NOT}] \circ \text{Skip}_1[\text{NOT}] \circ \text{NOT}$ .

Consider the quantum function  $f$  defined by  $f(|\phi\rangle) = \sum_{z:|z|=6} \langle z|\phi\rangle \otimes |z\rangle$  for all  $|\phi\rangle \in \mathcal{H}_\infty$ . This  $f$  satisfies the following recursive property:  $f(|x\rangle|\hat{1}\rangle) = \text{SecSWAP}_{1,3}^{(3)} \circ \text{SecSWAP}_{2,4}^{(3)}(|u_1u_2\rangle \otimes f(|u_1u_2|x\hat{1}\rangle))$ , where  $x = u_1u_2x'$  with  $|u_1| = |u_2| = 3$ .

Proposition 18 makes it possible to realize the quantum function  $F$  that satisfies  $F(|\hat{b}\rangle \hat{2}|\hat{x})|\phi\rangle) = f(|\hat{b}\rangle \hat{2}|\hat{x})|\phi\rangle$ . The last term actually equals  $|\hat{x}\rangle |\hat{b}\rangle \hat{2}|\phi\rangle$ . We apply *BinSearch* to  $|\hat{x}\rangle |\hat{b}\rangle \hat{2}|s\rangle$  and obtain  $|\hat{x}\rangle |b \oplus s_{(m)}\rangle \hat{2}|s\rangle$ . We further apply  $f^{-1}$  to obtain  $f^{-1}(|\hat{x}\rangle |b \oplus s_{(m)}\rangle \hat{2}|s\rangle) = |b \oplus s_{(m)}\rangle \hat{2}|\hat{x}|s\rangle$ . Finally, we apply  $h^{-1}$  to  $|b \oplus s_{(m)}\rangle \hat{2}|\hat{x}|s\rangle$  and obtain  $|0^5|b \oplus s_{(m)}|\hat{x}|s\rangle$ . Therefore, *Bit* can be defined by a finite series of applications of Scheme I–IV. □

As the second application of *BinSearch*, we wish to “count” the number of 0s and 1s in an input string in a quantum-mechanical fashion. It is impossible to do so deterministically in polylogarithmic time. Fix a constant  $\varepsilon \in [0, 3/4)$  and consider the *promise decision problem MAJPDPE* in which we determine whether the total number of 0s in  $x$  is at least  $\sqrt{1 - \varepsilon}|x|$  or the total number of 1s is at least  $\sqrt{1 - \varepsilon}|x|$ . Formally, *MAJPDPE* is expressed as  $(A_\varepsilon, B_\varepsilon)$ , where  $A_\varepsilon = \{x \in \{0, 1\}^* \mid \#_1(x) \geq \sqrt{1 - \varepsilon}|x|\}$  and  $B_\varepsilon = \{x \in \{0, 1\}^* \mid \#_0(x) \geq \sqrt{1 - \varepsilon}|x|\}$ . We intend to prove the existence of a quantum function in  $\text{EQS}_0 + IV$  that “solves” this promise problem *MAJPDPE* in the following sense.

**Proposition 28.** *Let  $\varepsilon$  be any constant in  $[0, 3/4)$ . There exists a quantum function  $F$  in  $\text{EQS}_0 + IV$  such that, for any  $x \in \{0, 1\}^*$ , (1) if  $x \in A_\varepsilon$ , then  $\|\langle 1|\psi_{F,x}\rangle\|^2 \geq 1 - \varepsilon$  and (2) if  $x \in B_\varepsilon$ , then  $\|\langle 0|\psi_{F,x}\rangle\|^2 \geq 1 - \varepsilon$ , where  $|\psi_{F,x}\rangle = F(|0^{3k}| \hat{1}\rangle|x\rangle)$  with  $k = \text{ilog}(|x|)$ .*

To prove this proposition, we first demonstrate how to produce a superposition of all “indices” of a given input. This can be done by recursively applying *WH* to  $|0^{3k}| \hat{1}\rangle$  as shown below.

**Lemma 29.** *There exists a quantum function  $G$  in  $\text{EQS}_0 + IV$  satisfying  $G(|0^{3k}| \hat{1}\rangle \otimes |\phi\rangle) = \frac{1}{\sqrt{2^k}} \sum_{x:|x|=k} |\hat{x}\rangle|\phi\rangle$  for any  $n \in \mathbb{N}^+$  and any  $|\phi\rangle \in \mathcal{H}_\infty$ , provided that  $k = \text{ilog}(\ell(|\phi\rangle))$ .*

*Proof.* Consider the quantum function  $\hat{h}(|0^{3k}| \hat{1}\rangle) = \frac{1}{\sqrt{2^k}} \sum_{x:|x|=k} |\hat{x}\rangle$ . This function  $\hat{h}$  satisfies the following recursive property:  $\hat{h}(|\hat{1}\rangle) = |\hat{1}\rangle$  and  $\hat{h}(|0^3|w\hat{1}\rangle) = h(|0^3\rangle \otimes \hat{h}(|w\hat{1}\rangle))$  for any string  $w$ , where  $h \equiv \text{Branch}_2\{g_u\}_{u \in \{0,1\}^2}$  with  $g_{00} = WH$  and  $g_u = I$  for all indices  $u \in$

$\{0, 1\}^2 - \{00\}$ . Let us prove this property. Assume that  $\hat{h}(|0^{3k}\rangle|\hat{1}\rangle) = \frac{1}{\sqrt{2^k}} \sum_{x:|x|=k} |\tilde{x}\rangle$ . For the value  $\hat{h}(|0^{3k+3}\rangle|\hat{1}\rangle)$ , we calculate  $h(|0^3\rangle \otimes \hat{h}(|0^{3k}\rangle|\hat{1}\rangle))$  as  $|00\rangle \otimes g(|0\rangle \otimes \hat{h}(|0^{3k}\rangle|\hat{1}\rangle)) = |00\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \hat{h}(|0^{3k}\rangle|\hat{1}\rangle) = \frac{1}{\sqrt{2}}(|\hat{0}\rangle + |\hat{1}\rangle) \otimes \frac{1}{\sqrt{2^k}} \sum_{x:|x|=3k} |\tilde{x}\rangle = \frac{1}{\sqrt{2^{k+1}}} \sum_{y:|y|=k+1} |\tilde{y}\rangle$ . The last term clearly equals  $\hat{h}(|0^{3k+3}\rangle|\hat{1}\rangle)$ .

By Proposition 18, there exists a quantum function  $G$  in  $EQS_0 + IV$  for which  $G(|0^{3k}\rangle|\hat{1}\rangle \otimes |\phi\rangle) = \hat{h}(|0^{3k}\rangle|\hat{1}\rangle) \otimes |\phi\rangle$ , where  $k = \text{ilog}(\ell(|\phi\rangle))$ . This completes the lemma’s proof.  $\square$

With the help of Lemma 29, the proof of Proposition 28 easily follows.

*Proof of Proposition 28.* Consider  $MAJDPDP_\varepsilon = (A_\varepsilon, B_\varepsilon)$  defined above. We wish to construct a quantum function, say,  $F$  in  $EQS_0 + IV$  that “solves”  $MAJDPDP_\varepsilon$  in the proposition’s sense. Recall the quantum function  $G$  of Lemma 29. Since  $G$  is norm-preserving and thus in  $\widehat{EQS}$ , Lemma 23 ensures that  $G^{-1}$  exists.

Let  $x$  denote any string. We then set  $b_x = 1$  if  $x \in A_\varepsilon$  and  $b_x = 0$  if  $x \in B_\varepsilon$ . We start the desired computation with the quantum state  $|\phi_x\rangle = |0^6\rangle|0^{3k}\rangle|\hat{1}\rangle|x\rangle$ , where  $k = \text{ilog}(|x|)$ , and apply  $Skip_6[G]$  to generate  $\frac{1}{\sqrt{2^k}} \sum_{u:|u|=k} |\tilde{u}\rangle|x\rangle|0^6\rangle$ . We then move  $|0^6\rangle$  to the front and obtain  $\frac{1}{\sqrt{2^k}} \sum_{u:|u|=k} |0^6\rangle|\tilde{u}\rangle|x\rangle$ . We further apply  $Bit$  to the resulting quantum state and generate  $\frac{1}{\sqrt{2^k}} \sum_{u:|u|=k} |0^5\rangle|x_{(m(u))}\rangle|\tilde{u}\rangle|x\rangle$ , where  $m(u)$  denotes a unique number satisfying that  $u = \text{bin}_k(m(u))$  and  $x_{(m(u))}$  is the  $m(u)$ -th bit of  $x$ . We change it to  $|\gamma_x\rangle = \frac{1}{\sqrt{2^k}} \sum_{u:|u|=k} |\tilde{u}\rangle|x\rangle|0^5\rangle|x_{(m(u))}\rangle$  and then apply  $G^{-1}$ . We denote the resulting quantum state by  $|\beta_x\rangle$ . Letting  $|\xi\rangle = |0^{3k}\rangle|\hat{1}\rangle$ , we wish to calculate  $\langle\xi|\beta_x\rangle$ . Note that  $|\beta_x\rangle = G^{-1}(|\gamma_x\rangle)$  is equivalent to  $G(|\beta_x\rangle) = |\gamma_x\rangle$ . It thus follows that  $\langle\xi|\beta_x\rangle$  equals  $\langle\psi_{G,\xi}|\gamma_x\rangle$ , which is further calculated to  $(\frac{1}{\sqrt{2^k}} \sum_{v:|v|=k} |\tilde{v}\rangle) \cdot (\frac{1}{\sqrt{2^k}} \sum_{u:|u|=k} |\tilde{u}\rangle|x\rangle|0^5\rangle|x_{(m(u))}\rangle) = \frac{1}{2^k} |x\rangle|0^5\rangle|x_{(m(u))}\rangle$ , where  $|\psi_{G,\xi}\rangle = G(|\xi\rangle)$ .

After removing the last qubit to the front, we obtain a unique quantum state, say,  $|\eta_x\rangle$ . Finally, we measure the first qubit of  $|\eta_x\rangle$  in the computational basis. If  $x \in A_\varepsilon \cup B_\varepsilon$ , then  $b_x$  satisfies that  $\| (b_x|\eta_x)\|^2 \geq (\frac{1}{2^k} \sum_u \langle b_x|x_{(m(u))}\rangle)^2 = (\frac{\#_{b_x}(x)}{2^k})^2 \geq (\sqrt{1-\varepsilon})^2 = 1 - \varepsilon$  because of the promise given by  $(A_\varepsilon, B_\varepsilon)$ .  $\square$

### 5. Relationships to quantum computability

Throughout Section 3, we have studied basic properties of quantum functions in  $EQS$ . In this section, we will look into relationships of these quantum functions to other platforms of limited computability, in particular, a model of polylogarithmic-time (or polylogtime) Turing machine.

#### 5.1 Runtime-restricted quantum Turing machines

We wish to describe a computational model of *quantum Turing machine* (or QTM, for short) that runs particularly in polylogarithmic time. For this purpose, we need to modify a standard model of QTM defined in (Bernstein and Vazirani, 1997; Ozawa and Nishimura, 2000; Yamakami, 1999) structurally and behaviorally. This new model also expands the classical model of (poly)logtime Turing machine (TM) discussed in (Barrington et al., 1990). Notice that quantum polylogtime computability was already discussed by, for example, Raz and Tal (2022) based on uniform quantum circuit families. For more information, refer to (Raz and Tal, 2022) and references therein.

A (*random-access*) QTM<sup>4</sup> (or just a QTM in this work) is equipped with a random-access read-only input tape, multiple rewritable work tapes of  $O(\log^k n)$  cells, and a rewritable index

tape of exactly  $\text{ilog}(n) + 1$  cells, where  $k$  is a constant in  $\mathbb{N}^+$  and  $n$  refers to the length of an input. The index tape indicates the cell location (or address) of the input tape, specifying which qubit of a given input we wish to access. This QTM  $M$  is formally expressed as  $(Q, \Sigma, \{\triangleright, \triangleleft\}, \delta, q_0, Q_{acc}, Q_{rej})$ , where  $Q$  is a finite set of inner states,  $\Sigma = \{0, 1\}$  is an alphabet,  $\triangleright$  and  $\triangleleft$  are endmarkers,  $\delta$  is a quantum transition function,  $q_0 (\in Q)$  is the initial (inner) state, and  $Q_{acc}$  (resp.,  $Q_{rej}$ ) ( $\subseteq Q$ ) is a set of accepting (resp., rejecting) states. We use an additional convention that the input tape, the index tape, and all the work tapes have two endmarkers to mark the usable areas of these tapes. This in fact helps the machine understand the “size” of a given input. The QTM  $M$  begins with an input qustring  $|\phi\rangle$  given on the input tape marked by the endmarkers. Let  $|\phi\rangle = \sum_{x \in \Sigma^n} \alpha_x |x\rangle$  with  $n \in \mathbb{N}^+$  and  $\alpha_x \in \mathbb{C}$  for all  $x$ 's.

Recall from Section 2.1 the binary encoding of natural numbers. Let  $k_n = \text{ilog}(n)$ . To access the tape cell indexed by  $m$ ,  $M$  first produces the binary string  $\text{bin}_{k_n}(m)$  on the index tape with an auxiliary bit  $b$  and then enters a designated query state, say,  $q_{query}$  in  $Q$ . If the index tape contains  $|\text{bin}_{k_n}(m)\rangle|b\rangle$ , then this quantum state becomes  $|\text{bin}_{k_n}(m)\rangle|b \oplus x_{(m)}\rangle$  as the immediate consequence of the query, where  $x_{(m)}$  is the  $m$ th input symbol of an input  $x \in \Sigma^+$ . With the proper use of work tapes, we assume that, while writing  $|\text{bin}_{k_n}(m)\rangle|b\rangle$  until entering a query state, the tape head never moves to the left and, whenever it writes a non-blank symbol, it must move to the right. We remark that the number of queries and their timings may vary on all computation paths of  $M$  on  $|\phi\rangle$ .

Concerning a random access to an input, a classical polylogtime TM takes the following convention (Barrington et al., 1990; Vollmer, 1999). When the machine enters a query state with index-tape content  $\text{bin}_{k_n}(m)$ , an input-tape head instantly jumps to the target bit  $x_{(m)}$  of an input  $x$  and reads it. After this query process, the index tape remains unerased and the corresponding tape head does not automatically return to the start cell. Therefore, for the next query, the machine can save time to rewrite the same query word, but it must overwrite a different query word over the previous query word on the index tape.

The quantum transition function  $\delta$  takes a quantum transition of the form  $\delta(q, \sigma, \tau_1, \tau_2, \dots, \tau_c) = \sum_r \alpha_r |p, \xi, \eta_1, \eta_2, \dots, \eta_c, d, d'_1, d'_2, \dots, d'_c\rangle$ , where  $r = (p, \xi, \eta_1, \eta_2, \dots, \eta_c, d, d'_1, d'_2, \dots, d'_c)$ , which indicates that, if  $M$  is in inner state  $q$  reading  $\sigma$  on the index tape and  $(\tau_1, \tau_2, \dots, \tau_c)$  on the  $c$  work tapes, then, in a single step, with transition amplitude  $\alpha_r$ ,  $M$  changes  $q$  to  $p$ , writes  $\xi$  over  $\sigma$  by moving the input-tape head in direction  $d \in \{-1, +1\}$ , and writes  $\eta_i$  over  $\tau_i$  by moving the  $i$ th work-tape head in direction  $d'_i \in \{-1, +1\}$ . For practicality, we can limit the scope of transition amplitudes of QTMs. In this work, we allow only the following two forms of quantum transitions:

$$\delta(q, \sigma, \tau_1, \tau_2, \dots, \tau_c) = \cos \theta |p_1, \xi_1, \eta_{11}, \eta_{12}, \dots, \eta_{1c}, d_1, d'_{11}, d'_{12}, \dots, d'_{1c}\rangle + \sin \theta |p_2, \xi_2, \eta_{21}, \eta_{22}, \dots, \eta_{2c}, d_2, d'_{21}, d'_{22}, \dots, d'_{2c}\rangle \quad \text{and} \quad \delta(q, \sigma, \tau_1, \tau_2, \dots, \tau_c) = e^{i\theta} |p, \xi, \eta_1, \eta_2, \dots, \eta_c, d, d'_1, d'_2, \dots, d'_c\rangle,$$

based on the universality of a set of quantum gates of Barenco et al. (1995).

A QTM is required to satisfy the so-called “well-formedness condition” (see, e.g., Yamakami, 1999, 2003) to guarantee that the behaviors of the QTM obeys the laws of quantum physics. A surface configuration of  $M$  on an input  $x$  of length  $n$  is an element  $(q, u, r, w_1, s_1, w_2, s_2, \dots, w_c, s_c)$  of the surface-configuration set  $Q \times \{\triangleright u \triangleleft\} \times \{u \in \{0, 1, B\}^{k_n+1}\} \times [0, k_n + 2]_{\mathbb{Z}} \times (\{\triangleright w \triangleleft\} \times \{w \in \{0, 1, B\}^{k_n}\} \times [0, k_n + 1]_{\mathbb{Z}})^c$ , which depicts the circumstance where  $M$  is in inner state  $q$ , scanning the  $r$ th bit of the index tape content  $u$ , and the  $s_i$ th bit of the  $i$ th work tape content  $w_i$ . We call the space spanned by this set of surface configurations the surface configuration space of  $M$  on  $x$ . The time-evolution operator of  $M$  on the input  $x$  is a map from superpositions of surface configurations of  $M$  on  $x$  to other superpositions of surface configurations resulting from a single application of  $\delta$  of  $M$ . A QTM  $M$  is said to be well-formed if its time-evolution operator of  $M$  preserves the  $\ell_2$ -norm in the surface configuration space of  $M$  on all inputs.

At every step, we first apply  $\delta$  to a superposition of surface configurations and then perform a measurement in the halting inner states (i.e., either accepting states or rejecting states). If  $M$  is not in a halting state, we move to the next step with the quantum state obtained by tracing out all halting surface configurations. Generally, QTMs can “recognize” not only sets of classical strings but also sets of qustrings.

For convenience, we modify  $M$  slightly so that  $M$  produces 1 (resp., 0) in the first cell of the first work tape when  $M$  enters a designated final state (in place of accepting/rejecting states). We say that  $M$  produces  $b$  with probability  $\gamma$  if, after  $M$  halts, we observe  $b$  as an outcome of  $M$  with probability  $\gamma$ .

We call  $M$  *polylogarithmic time* (or *polylogtime*) if we force  $M$  to stop its application of  $\delta$  after  $O(\log^k n)$  steps for a certain fixed constant  $k \in \mathbb{N}^+$ , not depending on the choice of inputs. We do not require all computation paths to terminate within the specified time.

Let us consider a language  $L$  over  $\{0, 1\}$  that satisfies the following condition: there are a constant  $\varepsilon \in [0, 1/2)$  and a polylogtime QTM  $M$  whose amplitude set is  $K$  such that (i) for any input  $x \in L$ ,  $M$  accepts  $x$  with probability at least  $1 - \varepsilon$  and (ii) for any  $x \notin L$ ,  $M$  rejects  $x$  with probability at least  $1 - \varepsilon$ . These conditions are referred to as *bounded-error probability*. The notation  $\text{BQPOLYLOGTIME}_K$  denotes the collection of all such languages  $L$ .

**5.2 Computational complexity of polylogtime QTMs**

We begin with a discussion on the computational complexity of polylogtime QTMs. Remember that input tapes of these machines are read-only and accessed by way of writing cell locations onto index tapes.

In the classical setting, the notation  $\text{DLOGTIME}$  was used by Barrington *et al.* (1990) to express the family of all languages recognized by logtime deterministic TMs (or succinctly, DTMs). Similarly, we denote the nondeterministic variant of  $\text{DLOGTIME}$  by  $\text{NLOGTIME}$ . With the use of classical probabilistic TMs (or PTMs) in place of DTMs, we say that a PTM  $M$  recognizes a language  $L$  with *unbounded-error probability* if, for any  $x \in L$ ,  $M$  accepts it with probability more than  $1/2$  and, for any  $x \notin L$ ,  $M$  rejects with probability at least  $1/2$ . We further define  $\text{PPOLYLOGTIME}$  using unbounded-error polylogtime PTMs.

**Theorem 30.**  $\text{BQPOLYLOGTIME}_{\mathbb{Q}} \subsetneq \text{PPOLYLOGTIME}$  and  $\text{NLOGTIME} \not\subseteq \text{BQPOLYLOGTIME}_{\mathbb{C}}$ .

For the proof of Theorem 30, nevertheless, we first verify the following impossibility result of the parity function and the OR function by polylogtime QTMs, where the parity function, *Parity*, is defined by  $\text{Parity}(x) = \bigoplus_{i=1}^n x_i$  and the OR function, *OR*, is defined by  $\text{OR}(x) = \max\{x_i \mid i \in [n]\}$  for any number  $n \in \mathbb{N}^+$  and any  $n$ -bit string  $x = x_1 x_2 \dots x_n$ .

**Lemma 31.** *The parity function and the OR function cannot be computed by any polylogtime QTM with bounded-error probability.*

*Proof.* This proof comes from a result on the quantum query complexity gap between quantum and deterministic query complexities of the parity function. Assume that a polylogtime QTM, say,  $M$  computes the parity function with bounded-error probability.

We encode  $M$ 's surface configuration *conf* into a “single” quantum state  $|\phi\rangle$ . As done in Lemma 29, it is possible to produce in polylog time a superposition of all locations of the input-tape cells by repeatedly applying  $WH$  to  $|0^{\log(n)}\rangle$ . This helps us access all input bits quantumly at once with the equal probability. Since the input tape is read-only, this type of input access can be



realized as a (black-box) quantum query model<sup>5</sup> used in the study of quantum query complexity. Refer to, for example, (Ambainis, 2002; Beals et al., 2001; Nishimura and Yamakami, 2004).

In such a (black-box) quantum query model, we run the following quantum algorithm on a binary input  $x$  of length  $n$ . We prepare a series of unitary transformations  $U_0, U_1, \dots, U_{t-1}, U_t$  and a special oracle transformation<sup>6</sup>  $Q_x$  that changes  $|bin_{k_n}(m)\rangle|b\rangle|\phi\rangle$  to  $|bin_{k_n}(m)\rangle|b \oplus x_{(m)}\rangle|\phi\rangle$ , where  $k_n = \text{ilog}(n)$  and  $x_{(m)}$  is the  $m$ th bit of  $x$ . We start with the initial quantum state  $|\psi_0\rangle = |0^m\rangle$ . We then compute  $U_t Q_x U_{t-1} Q_x \dots U_1 Q_x U_0 |\psi_0\rangle$ . Finally, we measure the resulting quantum state in the computational basis. The number  $t$  indicates the total number of queries made by this algorithm on each computation path.

**Claim 32.** *Each polylogtime QTM can be simulated by a (black-box) quantum query model with  $O(\log^k n)$  queries for an appropriate constant  $k \in \mathbb{N}^+$ .*

*Proof.* Recall that a QTM has an read-only input tape, which holds an input string. Whenever a QTM makes a query on the  $i$ th position by entering a unique query state  $q_{query}$ , the machine instantly receives the information on the  $i$ th bit of a given input string written on the input tape. We view this input tape as an oracle of a (black-box) quantum query model and we further view this entire query process of the QTM as a procedure of forming a superposition of query words indicating input-bit positions and receiving their answers from the oracle.

We first construct a unitary transformation to simulate a single non-query transition of  $M$ . Recall that, when  $M$  enters  $q_{query}$ , it changes  $|bin_{k_n}(m)\rangle|b\rangle|\phi\rangle$  to  $|bin_{k_n}(m)\rangle|b \oplus x_{(m)}\rangle|\phi\rangle$  in a single step. To translate  $M$ 's query process, we generate  $|bin_{k_n}(1)\rangle|0\rangle$  in an extra register. If  $M$  is in the inner state  $q_{query}$ , then we swap between this register and the register containing the content of  $M$ 's index tape. Otherwise, we do nothing. We then apply  $Q_x$  to change  $|bin_{k_n}(m)\rangle|b\rangle|\phi\rangle$  to  $|bin_{k_n}(m)\rangle|b \oplus x_{(m)}\rangle|\phi\rangle$ . Notice that this process does not alter the inner state of  $M$ . After applying  $Q_x$ , we swap back the two registers exactly when  $M$ 's inner state is  $q_{query}$  and then we follow the transition of  $M$ 's inner state.

Note that the given QTM makes only  $O(\log^k n)$  queries because it runs in  $O(\log^k n)$  time. Therefore, we can transform this QTM to a query model of  $O(\log^k n)$  queries. □

By Claim 32, the parity function requires only  $O(\log n)$  queries in the (black box) quantum query model. However, it is shown by Beals et al. (2001) that, for the parity function of  $n$  Boolean variables,  $n/2$  queries are necessary in the bounded-error quantum query model (while  $n$  queries are necessary in the deterministic query model). This is obviously a contradiction. The case of the OR function can be similarly handled. □

Let us return to Theorem 30. Using Lemma 31, we can prove the theorem as described below. The core of its proof is founded on a simulation result of one-tape linear-time QTMs in (Tadaki et al., 2010, Section 8).

Shown in (Tadaki et al., 2010, Lemma 8) is how to simulate a one-tape well-formed stationary QTM running in linear time on an appropriate one-tape probabilistic Turing machine (or a PTM) in linear time. In a similar vein, we can simulate polylogtime QTMs on polylogtime PTMs.

*Proof of Theorem 30.* Let us take an arbitrary language  $L$  in  $\text{BQPOLYLOGTIME}_{\bar{Q}}$  and consider a polylogtime QTM  $M$  that recognizes  $L$  with bounded-error probability. We intend to show that  $L$  falls in  $\text{PPOLYLOGTIME}$ . We first modify  $M$  in the following way. We prepare two extra work tapes. One of them is used as an *internal clock* by moving a tape head always to the right. To avoid any unwanted interference after a computation halts prematurely, we use the other extra tape as a “garbage tape”, to which  $M$  dumps all information produced at the time of entering halting states, so that  $M$  continues its operation without actually halting. Lemma 8 of Tadaki et al. (2010) shows



the existence of a constant  $d \in \mathbb{N}^+$  and an NTM  $N$  such that  $d^{\text{Time}_M(x)} \cdot p_M(x) = \#N(x) - \#\bar{N}(x)$  for every  $x$ , where  $\#N(x)$  (resp.,  $\#\bar{N}(x)$ ) denotes the total number of accepting (resp., rejecting) computation paths of  $N$  on input  $x$ . This equality holds for polylogtime machines. The desired polylogtime PTM is obtained from  $N$  by assigning an equal probability to all nondeterministic transitions.

The OR function can be computed by the polylogtime NTM that nondeterministically writes a number, say  $i$  on an index tape, makes a query for the  $i$ th bit  $x_{(i)}$  of an input  $x$ , and accepts exactly when  $x_{(i)}$  is 1. Thus, the OR function belongs to NLOGTIME. The separation between  $\text{BQPOLYLOGTIME}_{\bar{0}}$  and NLOGTIME comes from Lemma 31. Since  $\text{PPOLYLOGTIME}$  includes NLOGTIME, we obtain the desired separation between  $\text{BQPOLYLOGTIME}_{\bar{0}}$  and  $\text{PPOLYLOGTIME}$ .  $\square$

**5.3 Comparison between EQS and BQPOLYLOGTIME**

In what follows, we discuss a close relationship between quantum functions definable within EQS and quantum functions computable by polylogtime QTM’s despite numerous differences between EQS and polylogtime QTM’s. One such difference is that input tapes of QTM’s are read-only and thus inputs are not changeable, whereas quantum functions in EQS can freely modify their inputs. In the following two theorems (Theorems 33 and 34); however, we can establish the “computational” equivalence between polylogtime QTM’s and quantum functions in EQS.

To make the later simulation process simpler, we first modify a polylogtime QTM so that it uses the binary alphabet on an index tape as well as all work tapes by way of encoding each non-binary tape symbol into a binary one using an appropriately chosen encoding scheme. This modification makes it possible to assume that the QTM should hold superpositions  $|\phi\rangle$  of binary strings on its input tape and its work tapes. For convenience, a QTM that satisfies these conditions is called *normalized*.

**Theorem 33.** *Any normalized polylogtime QTM  $M$  with  $c$  work tapes can be simulated by an appropriate quantum function  $F$  in EQS in the sense that, for any  $b \in \{0, 1\}$ ,  $\alpha \in [0, 1]$ , and  $|\phi\rangle \in \Phi_\infty$ ,  $M$  takes  $|\phi\rangle$  as an input and finally produces  $b$  with probability  $\alpha$  exactly when  $\| \langle b | \psi_{F, \xi_\phi} \rangle \|^2 = \alpha$  holds, where  $|\xi_\phi\rangle = |\hat{S}\rangle |\hat{B}^k\rangle^{\otimes(c+1)} |\hat{2}\rangle \otimes |\phi\rangle$  with  $k = \text{ilog}(\ell(|\phi\rangle))$  and  $|\psi_{F, \xi_\phi}\rangle = F(|\xi_\phi\rangle)$ .*

*Proof.* Let  $M$  denote any polylogtime QTM equipped with a read-only input tape, a rewritable index tape, and multiple rewritable work tapes. We further assume that  $M$  is normalized. For readability, we hereafter deal with the special case where  $M$  has a single work tape. A general case of  $c$  work tapes can be handled in a similar but naturally extended way. Assume that  $M$ ’s input tape holds a superposition  $|\phi\rangle$  of binary inputs with  $\ell(|\phi\rangle) \geq 4$  and that  $M$  runs in time at most  $\text{ilog}(\ell(|\phi\rangle))^e$  for a fixed constant  $e \geq 1$ . For convenience, let  $k = \text{ilog}(\ell(|\phi\rangle))$ . We denote by  $Q$  the set of all inner states of  $M$ . Since  $Q$  is finite, without loss of generality,  $Q$  assumed to have the form  $\{\text{bin}_{3t'}(i) \mid i \in [2^{3t'}]\}$  for an appropriate constant  $t' \in \mathbb{N}^+$ . We set the initial inner state  $q_0$  to be  $\text{bin}_{3t'}(1)$ . For each inner state  $q \in Q$ , since  $q$  is expressed as a binary string, we can encode it into the string  $\tilde{q}^{(-)}$  defined in Section 3.2.

We treat the content of each tape (except for the input tape) as a code block of the desired quantum function  $F$ . We maintain the contents of the index tape and of the work tape as a part of two appropriate qustrings. We intend to simulate each move of  $M$  on  $|\phi\rangle$  by applying an adequately defined quantum function.

Since  $M$ ’s computation is a series of surface configurations of  $M$ , we thus need to “express” such a surface configuration using a single quantum state. Initially,  $M$ ’s index tape holds  $B^k \triangleleft$  and  $M$ ’s single work tape holds  $B^{kt} \triangleleft$  for a fixed constant  $t \in \mathbb{N}^+$ . Let  $w$  and  $z$ , respectively, denote

the contents of the index tape and of the work tape without the right endmarker  $\triangleleft$  and let  $q$  be any inner state of  $M$ . Associated with  $(q, w, z)$ , we describe  $M$ 's current surface configuration as  $q\#w_1Hw_2\#z_1Hz_2$  with  $w = w_1w_2$  and  $z = z_1z_2$  by including a designated symbol  $H$  and  $M$ 's inner state  $q$ , where  $H$  is used to indicate the locations of the index-tape head and of the work-tape head, which are scanning the leftmost symbols of  $w_2$  and  $z_2$ , respectively. Assume that these two tape heads are, respectively, scanning tape symbols  $\eta$  and  $\sigma$  on the index tape and the work tape, that is,  $w_2 = \eta x_2$  and  $z_2 = \sigma y_2$ . For technical reason, we slightly modify the above description of a surface configuration and express it as  $w_1HBx_2\#z_1HBy_2\#q\eta\sigma$  by inserting the extra symbol  $B$ . To refer to this special form, we call it a *modified (surface) configuration*. In particular, the suffix  $q\eta\sigma$  is called a *transition status*.

By Lemma 25, it suffices for us to focus on each block of encoded tape content. The modified configuration  $w_1HBx_2\#z_1HBy_2\#q\eta\sigma$  is encoded into the quantum state  $|\widetilde{w}_1^{(-)}\widehat{HB}\widetilde{x}\rangle|\widetilde{z}_1^{(-)}\widehat{HB}\widetilde{y}\rangle|\widetilde{q}^{(-)}\widehat{\eta}\widehat{\sigma}\rangle|\widehat{\triangleleft}\rangle$ . We conveniently refer to it as the *encoded (surface) configuration*. Note that  $|\widetilde{q}^{(-)}\widehat{\eta}\widehat{\sigma}\rangle = 6t' + 6 = 6(t' + 1)$ . In fact, the modified initial configuration is of the form  $HB^k\#HB^{kt}\#q_0BB$  and its encoding is of the form  $|\widehat{HB}^k\rangle|\widehat{HB}^{kt}\rangle|\widetilde{q}_0^{(-)}\widehat{B}\widehat{B}\rangle|\widehat{\triangleleft}\rangle$ .

A run of  $M$ , which covers from the initial surface configuration to certain halting surface configurations, can be simulated using the fast quantum recursion. To explain this simulation, for convenience, we split each move of  $M$  into three separate “phases”: (1) a tape content change, (2) an input access by a query, and (4) an output production. We consider these three different phases of  $M$  separately. In Phase (3), in particular, we will use Scheme V to repeat Phases (1) and (2)  $\text{ilog}(\ell(|\phi|))$  times. In the end, we will combine Phases (1)–(4) into a single quantum function.

(1) The first case to consider is that  $M$  modifies multiple tapes (except for the input tape) by a single move. We begin with paying our attention to the modification of the index-tape symbol and describe how to simulate this tape-symbol modification. In a single step, as our convention, a tape head firstly changes a tape symbol and secondly moves to an adjacent cell. In other words,  $M$  locally changes  $w_1Hw_2\#z_1Hz_2\#q\eta\sigma$  to its successor  $w'_1Hw'_2\#z'_1Hz'_2\#q'\eta'\sigma'$  by applying  $\delta$ . This process can be expressed by a single quantum function defined as follows.

Let us consider  $M$ 's single transition of the form  $\delta(q, \eta_2, \sigma_2) = \sum_r \alpha_r |p, \xi_2, \tau_2, d, d'\rangle$ , where  $r$  refers to  $(q, \eta_2, \sigma_2, p, \xi_2, \tau_2, d, d')$ . This transition means that the index-tape head changes  $\eta_2$  to  $\xi_2$  and moves in direction  $d$  and that the work-tape head changes  $\sigma_2$  to  $\tau_2$  and moves in direction  $d'$ . To simulate this transition, it suffices to focus on four consecutive cells whose second cell is being scanned by the tape head. For simplicity, we call such a series an *H-block*. Let  $\eta_1HB\eta_3$  and  $\sigma_1HB\sigma_3$  denote two *H-blocks*, and let  $q\eta_2\sigma_2$  denote the current transition status of  $\delta$ .

(a) We make an application of Scheme IV in the following fashion. Let  $v = (q, \eta_2, \sigma_2, p, \xi_2, \tau_2, d, d')$ . We first change  $|\widetilde{q}^{(-)}\widehat{\eta}_2\widehat{\sigma}_2\rangle$  to  $|\widetilde{p}^{(-)}\widehat{B}\widehat{B}\rangle$  by remembering  $(\xi_2, \tau_2, d, d')$  in the form of different quantum functions  $g_u$ , which are controlled by  $\text{Branch}[\{g_u\}_u]$ . We then search for an *H-block* of the form  $|\widehat{\eta}_1\widehat{H}\widehat{B}\widehat{\eta}_3\rangle$  and change it to  $|\widehat{H}\widehat{\eta}_1\widehat{\xi}_2\widehat{\eta}_3\rangle$  if  $d = -1$  and to  $|\widehat{\eta}_1\widehat{\xi}_2\widehat{H}\widehat{\eta}_3\rangle$  if  $d = +1$ . Similarly, we change  $|\widehat{\sigma}_1\widehat{H}\widehat{B}\widehat{\sigma}_3\rangle$  according to the value of  $d'$ . These changes can be made by an appropriate quantum function, say,  $F_{v,d}$ . This quantum function  $F_{v,d}$  is realized as follows.

In the case of  $\tau_2 \in \{0, 1\}$ , we introduce  $f_{B,\tau_2}$  that satisfies  $f_{B,\tau_2}(|\widehat{B}\rangle|\widehat{H}\rangle) = |\widehat{\tau}_2\rangle|\widehat{H}\rangle$ . This quantum function  $f_{B,\tau_2}$  is constructed as  $f_{B,\tau_2} \equiv \text{Branch}_3[\{g'_u\}_{u \in \{0,1\}^3}] \circ \text{SecSWAP}_{1,2}^{(3)} \circ \text{Branch}_3[\{g_u\}_{u \in \{0,1\}^3}]$ , where  $g_{010}(|100\rangle) = |00\tau_2\rangle$ ,  $g_u = I$  for all other  $u$ 's,  $g'_{000} = g'_{001}$ ,  $g'_{000}(|010\rangle) = |100\rangle$ ,  $g'_{000}(|100\rangle) = |010\rangle$ ,  $g'_{000}(|x\rangle) = |x\rangle$  for all other  $x$ 's, and  $g'_u = I$  for all other  $u$ 's. The remaining cases are similarly handled. Now, let us define  $\widehat{G}$  to be  $\text{SecSWAP}_{1,3}^{(3)}$ , which transforms  $|\alpha\rangle|\widehat{H}\rangle|\beta\rangle$  to  $|\beta\rangle|\widehat{H}\rangle|\alpha\rangle$  for any  $\alpha, \beta \in \{0, 1\}^3$ . Finally, when  $d = -1$ , we define  $F_{v,d}$  to be  $\text{SecSWAP}_{2,3}^{(3)} \circ \text{SecSWAP}_{1,2}^{(3)} \circ f_{B,\tau_2} \circ \widehat{G}$ , which satisfies  $F_{v,d}(|\widehat{\sigma}_1\rangle|\widehat{H}\rangle|\widehat{B}\rangle|\widehat{\sigma}_3\rangle) = |\widehat{H}\rangle|\widehat{\sigma}_1\rangle|\widehat{\tau}_2\rangle|\widehat{\sigma}_3\rangle$ . In a similar way, when  $d = +1$ , we define

$F_{v,d} \equiv \text{SecSWAP}_{1,2}^{(3)} \circ \text{SecSWAP}_{2,3}^{(3)} \circ f_{B,\tau_2} \circ \hat{G}$ , which transforms  $|\hat{\sigma}_1\rangle|\hat{H}\rangle|\hat{B}\rangle|\hat{\sigma}_3\rangle$  to  $|\hat{\sigma}_1\rangle|\hat{\tau}_2\rangle|\hat{H}\rangle|\hat{\sigma}_3\rangle$ . A similar treatment works for the simulation of the work-tape head.

Notice that  $M$  uses only two forms of quantum transitions. These transitions can be correctly simulated by Items 1)–3) of Scheme I. Let  $r_0 = \hat{\cdot}$ . Proposition 18 makes it possible, under a certain condition, to make a quantum function definable in a recursive fashion. We first define a quantum function  $K$  by setting  $K(|r_0\rangle) = |r_0\rangle$  and  $K(|xr_0\rangle) = \sum_{u:|u|=9} h(|u\rangle \otimes K(|u|xr_0\rangle))$ , where  $h(|u\rangle|wr_0\rangle) = \sum_{v,d} \alpha_{v,d} F_{v,d}(|u\rangle|wr_0\rangle)$  if  $u = \hat{\sigma}_1 \hat{H} \hat{\sigma}_2$ , and  $h(|u\rangle|wr_0\rangle) = |u\rangle|wr_0\rangle$  otherwise. The proposition then guarantees the existence of a quantum function that mimics  $K$  in the presence of the large-size qustring  $|\phi\rangle$ . In the proof of the proposition, such a quantum function is constructed with the use of Scheme IV. It is important to note that, its ground (quantum) functions are all query-independent. Thus, Scheme IV used here is also query-independent.

(b) Secondly, we apply *CodeREP*<sup>6</sup> to move the last six qubits  $|\hat{B}\hat{B}\rangle$  obtained by (a) to the front.

(c) We then make the second application of Scheme IV. We change  $|\hat{H}\hat{\eta}_1\hat{\xi}_2\hat{\eta}_3\rangle$  (resp.,  $|\hat{\eta}_1\hat{\xi}_2\hat{H}\hat{\eta}_3\rangle$ ) to  $|\hat{H}\hat{B}\hat{\xi}_2\hat{\eta}_3\rangle$  (resp.,  $|\hat{\eta}_1\hat{\xi}_2\hat{H}\hat{B}\rangle$ ) by remembering  $\eta_1$  (resp.,  $\eta_3$ ). This change is handled in essence similarly to (a). Moreover, a similar construction deals with the case of  $|\hat{H}\hat{\sigma}_1\hat{\tau}_2\hat{\sigma}_3\rangle$  (resp.,  $|\hat{\sigma}_1\hat{\tau}_2\hat{H}\hat{\sigma}_3\rangle$ ).

Toward the end, we change the first six qubits  $|\hat{B}\hat{B}\rangle$  to  $|\hat{\xi}\hat{\tau}\rangle$  for symbols  $\xi \in \{\xi_2, \eta_3\}$  and  $\tau \in \{\tau_2, \sigma_3\}$ .

(d) Finally, we apply *CodeREMOVE*<sup>6</sup> to move  $|\hat{\xi}\hat{\tau}\rangle$  back to the end.

(2) Next, we simulate  $M$ 's query access to its input qubits. Assume that the current encoded surface configuration contains  $|\widetilde{q_{query}^{(-)}}\hat{\eta}_2\hat{\sigma}_2\rangle$ . Assume that  $|\phi\rangle = \sum_{s:|s|=2^k} \alpha_s |s\rangle$  is written on the input tape and that the index tape contains  $|\text{bin}_k(m)\rangle|a\rangle$ , where  $a$  is an auxiliary bit. When entering the query state  $q_{query}$ ,  $M$  changes  $q_{query}$  to another inner state, say,  $p$  and  $|\text{bin}_k(m)\rangle|a\rangle$  to  $|\text{bin}_k(m)\rangle|a \oplus s_{(m)}\rangle$ , where  $s_{(m)}$  is the  $m$ th bit of  $s$ . We need to build a quantum function that simulates this entire query process. As the first step, we change  $|\widetilde{q_{query}^{(-)}}\rangle$  to  $|\widetilde{p}^{(-)}\rangle$ . Since  $|\text{bin}_k(m)\rangle|a\rangle$  is encoded into  $|\text{bin}_k(m)\rangle|\widetilde{a}\rangle$ , we can transform it to  $|\widetilde{a}\rangle|\text{bin}_k(m)\rangle$  and then to  $|0^5\rangle|a\rangle|\text{bin}_k(m)\rangle$ . Finally, we apply *Bit* (defined in Corollary 2) to  $|0^5\rangle|a\rangle|\text{bin}_k(m)\rangle$  and obtain  $\sum_s \alpha_s |0^5\rangle|a \otimes s_{(m)}\rangle|\text{bin}_k(m)\rangle|s\rangle$ . Since *Bit* is query-dependent, Scheme IV used here is also query-dependent.

(3) We then combine the above two types of moves into one and express it by a single application of an appropriate quantum function. Note that  $M$  accesses only the first  $O(\log \ell(|\phi\rangle))$  cells of the work tape. We compose (1)–(2) by applying *Compo* $[\cdot, \cdot]$ . We call by  $F'$  the obtained quantum function. We repeatedly apply it  $\text{ilog}(\ell(|\phi\rangle))^e$  times to complete the simulation of the entire computation of  $M$  until  $M$  enters a halting (either accepting or rejecting) inner state. This repetition procedure is realized by the  $e$  applications of *LCompo* $[\cdot]$  to  $F'$ .

(4) When  $M$  finally enters a halting inner state,  $M$  produces an output bit, say,  $b$  on the first cell of the first work tape. By (1)–(2) described above, the encoded configuration has the form  $|\hat{b}\widetilde{w}_1^{(-)}\hat{H}\widetilde{w}_2\rangle|\widetilde{z}_1^{(-)}\hat{H}\widetilde{z}_2\rangle|\widetilde{q_{halt}}\hat{\eta}\hat{\sigma}\rangle|\hat{\cdot}\rangle$ . We then change  $\hat{b}$  ( $= 00b$ ) to  $b00$  by applying  $\text{SWAP}_{1,3}$  to prepare the “correct” output qubit. We combine this quantum function with  $F'$  to obtain the desired quantum function  $F$ .

This completes the entire simulation of  $M$ . □

The converse of Theorem 33 is stated as Theorem 34, which is given below. Recall that, at the start of a QTM  $M$ , its index tape and all work tapes hold the blank symbol  $B$  (except for the right endmarker) in their tape cells. From this fact, we assume that inputs of quantum functions must be of the form  $|\gamma_\phi\rangle = |B^k\rangle|r_0\rangle \otimes |\phi\rangle$  with the designated separator  $r_0 = \hat{\cdot}$  and  $k = \text{ilog}(\ell(|\phi\rangle))$  for any qustring  $|\phi\rangle \in \Phi_\infty$ .

**Theorem 34.** For any quantum function  $F$  defined by Schemes I–V,  $F$  is computed by a certain polylogtime QTM  $M$  in the following sense: for any  $b \in \{0, 1\}$ , for any  $\alpha \in [0, 1]$ , and  $|\phi\rangle \in \Phi_\infty$ , if  $\ell(|\phi\rangle)$  is sufficiently large, then  $M$  on input  $|\phi\rangle$  produces  $b$  with probability  $\alpha$  iff  $\| \langle b | \psi_{F, \gamma_\phi} \rangle \| = \alpha$  holds, where  $|\psi_{F, \gamma_\phi}\rangle = F(|\gamma_\phi\rangle)$ .

In the description of the above theorem, we need to use the norm  $\| \cdot \|$  instead of  $| \cdot |$  because the superposition of  $M$ 's final configurations may contain not only the value  $F(|\gamma_\phi\rangle)$  but also additional “garbage” information, which might possibly be a quantum state of large dimension, and we may need to ignore it when making a measurement.

We wish to prove Theorem 34 by induction on the construction process of  $F$ . To make this induction work, we slightly modify the theorem into the following key lemma.

**Lemma 35.** For any quantum function  $F$  defined by Schemes I–V,  $F$  is computed by a certain polylogtime QTM  $M$  in the following sense: for any  $b \in \{0, 1\}$ , any  $|\phi\rangle \in \Phi_\infty$ , and any  $x$  in  $NON_{r_0}(|\phi\rangle) \cap \{0, 1\}^{|r_0|^k}$ , if  $\ell(|\phi\rangle)$  is sufficiently large, then  $\| \langle \psi_{F, \bar{\gamma}_{\phi, x}} | \xi_{M, \bar{\gamma}_{\phi, x}} \rangle \| = 1$  holds, where  $|\bar{\gamma}_{\phi, x}\rangle = |xr_0\rangle|\phi\rangle$ ,  $k = \text{ilog}(\ell(|\phi\rangle))$ ,  $|\psi_{F, \bar{\gamma}_{\phi, x}}\rangle = F(|\bar{\gamma}_{\phi, x}\rangle)$ , and  $|\xi_{M, \bar{\gamma}_{\phi, x}}\rangle$  is the superposition of final configurations of  $M$  that starts with  $|\phi\rangle$  on the input tape and  $|xr_0\rangle$  on the first work tape.

Theorem 34 follows immediately from Lemma 35 by setting  $xr_0$  in the lemma to be  $\tilde{B}^k$ . The remaining task is to verify the lemma.

*Proof of Lemma 35.* Let  $F$  denote any quantum function in EQS. For any qustring  $|\phi\rangle \in \Phi_\infty$  and any string  $x \in NON_{r_0}(|\phi\rangle) \cap \{0, 1\}^{|r_0|^k}$  with  $k = \text{ilog}(\ell(|\phi\rangle))$ , let  $|\bar{\gamma}_{\phi, x}\rangle = |xr_0\rangle|\phi\rangle$  denote a qustring given as an input to  $F$ . Assuming that  $\ell(|\phi\rangle)$  is sufficiently large, we first focus on  $F$  and simulate the outcome of  $F$  by an appropriate QTM that takes an input of the form  $|\bar{\gamma}_{\phi, x}\rangle$ . The desired polylogtime QTM  $M$  reads  $|\phi\rangle$  on its input tape and  $|xr_0\rangle$  on its first work tape.

As seen later in (3) of this proof, Scheme IV may allow  $F$  to access at most a constant number of locations of the input  $|\phi\rangle$ , whereas  $M$  does not. To circumvent this difficulty in simulating  $F$  on the QTM, whenever  $F$  modifies any qubit of  $|\phi\rangle$ ,  $M$  remembers this qubit modification using its work tape as a reference to the future access to it since  $M$  cannot alter any qubit of  $|\phi\rangle$ .

We intend to prove the lemma by induction on the descriptive complexity of  $F$ . We assume that the work-tape head is scanning the cell that contains the first qubit on the first work tape before each series of applications of the schemes of EQS.

(1) We first assert that all quantum functions  $F$  defined by Items 1)–6) of Scheme I are computable by appropriate polylogtime QTMs, say,  $M$  because the target qubits of these items lie in  $xr_0$ , which are written on the work tape, not on the input tape. To verify this assertion, let us consider PHASE $_\theta$  of Item 2). Starting with  $|\phi\rangle$  as well as  $|xr_0\rangle$ , if the first bit of  $xr_0$  is 1, then we use the QTM's quantum transition function  $\delta$  to make a phase shift of  $e^{i\theta}$ . Otherwise, we do nothing. A similar treatment works for Items 3)–4). For SWAP of Item 5), we simply swap between the content of the cell currently scanned by  $M$ 's work-tape head and the content of its right adjacent cell. For Item 6), it suffices to “observe” the first qubit on the first work tape in the computational basis  $|a\rangle$ .

(2) We next show by way of induction on the construction process of the target quantum function  $F$  by Scheme II. Let us consider the quantum function  $F$  of the form *Compo*[ $g, h$ ] for two ground (quantum) functions  $g$  and  $h$ . By induction hypothesis, there are two polylogtime QTMs  $M_g$  and  $M_h$  that respectively compute  $g$  and  $h$  in the lemma's sense. The desired QTM  $M$  first checks whether  $\ell(|\phi\rangle) \leq 1$ . This part is called the *first phase*, and it can be done by searching for the location of the right endmarker on the index tape. We then run  $M_h$  on  $|\phi\rangle$  as well as  $|xr_0\rangle$ . After  $M_h$  halts, we wish to run  $M_g$  in the *second phase*.

Now, there are two issues to deal with. Unlike the classical case of “composing” two TMs, we need to distinguish work tapes of  $M_g$  and those of  $M_h$  since we may not be able to erase the contents of  $M_g$ ’s work tapes freely at the start of the simulation of  $M_h$  in the second phase. Since we want to use  $M_h$ ’s index tape as the index tape of  $M$ , we need to rename  $M_g$ ’s index tape to one of the work tapes of  $M$ . Since the original input of  $M_g$  is the qustring  $h(|\phi\rangle)$ , we also need to mimic  $M_g$ ’s access to  $h(|\phi\rangle)$  using only  $|\phi\rangle$ . For this purpose, we need to remember the “history” of how we have modified qubits of  $|\phi\rangle$  so far and, whenever  $M_g$  accesses its input, we first consult this history log to check whether or not the accessed qubit has already been modified.

(3) To simulate Scheme III, let  $F \equiv \text{Branch}[g, h]$  for two ground functions  $g$  and  $h$ . By induction hypothesis, we take two polylogtime QTMs  $M_g$  and  $M_h$ , respectively, for  $g$  and  $h$  working with  $|\phi\rangle$  written on their input tapes and  $|zr_0\rangle$  written on their first work tapes. Let us design the desired QTM  $M$  to simulate  $F$  on  $|\phi\rangle$  and  $|xr_0\rangle$  as follows. We first check if  $\ell(|\phi\rangle) \leq 1$ . If so, we do nothing. Hereafter, we assume otherwise. Since  $\text{Branch}[g, h](|xr_0\rangle|\phi\rangle) = |0\rangle \otimes g(|0\rangle|xr_0\rangle \otimes |\phi\rangle) + |1\rangle \otimes h(|1\rangle|xr_0\rangle \otimes |\phi\rangle)$ , we scan the first qubit of  $|xr_0\rangle$  by a tape head and determine which machine (either  $M_g$  or  $M_h$ ) to run with the rest of the input. Since  $M_g$  and  $M_h$  correctly simulate  $g$  and  $h$ , respectively, this new machine  $M$  correctly simulates  $F$ .

(4) Concerning Scheme IV, let  $F \equiv \text{CFQRec}_t[r_0, d, g, h]_{\mathcal{P}_{|r_0|}, \mathcal{P}_{|r_0|}}$  and assume that  $M$ ’s input tape holds  $|\phi\rangle$  and its first work tape holds  $|xr_0\rangle$ . We first calculate the length  $\ell(|\phi\rangle)$  by checking the size of the available area of the index tape in logarithmic time. If either  $\ell(|\phi\rangle) < t$  or  $x = \lambda$ , then we run  $M_g$  on  $|\phi\rangle$  as well as  $|xr_0\rangle$  until it eventually halts. Now, we assume that  $\ell(|\phi\rangle) \geq t$  and  $x \neq \lambda$ .

If  $h$  is defined using none of  $\text{CodeSKIP}_+$  and  $\text{CodeSKIP}_-$ , then the induction hypothesis guarantees the existence of a polylogtime QTM  $M_h$  for  $h$ . In the case where  $h$  is constructed using  $\text{CodeSKIP}_\tau$  for a certain sign  $\tau \in \{+, -\}$ , we first build a QTM that simulates  $\text{CodeSKIP}_\tau[r_0, g', h']$  for certain ground functions  $g'$  and  $h'$  without requiring “polylogarithmic” runtime. It is important to note that such a QTM reads target qubits written on the work tape, not on the input tape. The QTM  $M$  searches for the first appearance of  $r_0$  and then runs the corresponding QTMs  $M_{g'}$  and  $M_{h'}$  in parallel. Since the input length is  $\ell(|\phi\rangle)$ , the QTM halts within  $O(\log \ell(|\phi\rangle))$  steps.

Similarly, we can handle  $\text{CodeREMOVE}$  and  $\text{CodeREP}$ .

Since  $x \neq \lambda$ ,  $F(|xr_0\rangle|\phi\rangle)$  is calculated as  $\sum_{u:|u|=|r_0|} \sum_{v:|v|=\ell(|xr_0\rangle)} (h(|u\rangle|v\rangle) \otimes p_u^{-1}(\langle v|\zeta_{u,p_u,\phi}^{(x'r_0)}\rangle))$ , where  $|\zeta_{u,p_u,\phi}^{(x'r_0)}\rangle = \sum_{s:|s|=H(|\phi\rangle)} (f_u(\langle u|x'r_0\rangle|s\rangle) \otimes \langle s|\psi_{p_u,\phi}\rangle)$  and  $d(|xr_0\rangle) = |x'r_0\rangle$ . Starting with  $|\phi\rangle$  as well as  $|xr_0\rangle$ , we first move a work-tape head, passing through at most  $\text{ilog}(\ell(|\phi\rangle))$  blocks of size  $|r_0|$ . Recursively, we move back the tape head to the start cell (i.e., cell 0) and run  $M_h$ . For this purpose, we write 0 and 1 on an index tape whenever we choose  $p_u = I$  and  $p_u = \text{HalfSWAP}$ , respectively, because we need to trace the location of the start of each recursively halved input until we reach  $x = \lambda$  or  $|x| > |r_0|k$ . The entire algorithm thus requires  $O(\log \ell(|\phi\rangle))$  steps.

By the definition of Scheme IV, the quantum function  $F$  can make a direct access to  $|\phi\rangle$  when  $g$  is finally called to compute the value of  $F$ . Notice that  $g$  accesses at most  $t$  locations of  $|\phi\rangle$ . Therefore, during the simulation of  $F$ ,  $M$  makes the same number of queries to its input  $|\phi\rangle$ .

(5) Finally, let us consider Scheme V. Assume that  $F$  is defined to be  $L\text{Compo}[g]$  for a ground function  $g$ . By induction hypothesis, we take a polylogtime QTM  $M_g$  that simulates  $g$ . Assume further that, for a fixed constant  $t \in \mathbb{N}^+$ ,  $M_g$  runs in  $O(\log^t \ell(|\phi\rangle))$  time for any input  $|\phi\rangle$ . Let  $k = \text{ilog}(\ell(|\phi\rangle))$ . To simulate  $F$ ,  $M$  repeats a run of  $M_g$   $k$  times since  $F(|xr_0\rangle|\phi\rangle) = g^k(|xr_0\rangle|\phi\rangle)$ . The total runtime of  $M$  is at most  $k \cdot O(\log^t \ell(|\phi\rangle))$ , which equals  $O(\log^{t+1} \ell(|\phi\rangle))$ .  $\square$

We have shown in Section 5.2 that the parity function, *Parity*, cannot be computed by polylog-time QTMs. It is possible to generalize *Parity* and treat it as a quantum function defined on  $\mathcal{H}_\infty$ . Lemma 31 together with Lemma 35 then leads to the following conclusion.



**Proposition 36.** *The parity function is not definable within EQS.*

**6. The divide-and-conquer scheme and EQS**

We have formulated the system EQS in Section 3 by the use of recursion schematic definition and discussed in Section 5.1 the EQS-characterization of quantum polylogtime computing. In what follows, we intend to strengthen the system EQS by appending an extra scheme. As such a scheme, we particularly consider the *divide-and-conquer strategy*, which is one of the most useful algorithmic strategies in solving many practical problems. We further show that the divide-and-conquer strategy cannot be “realized” within EQS. This implies that the addition of this strategy as a new scheme truly strengthens the expressing power of EQS.

**6.1 Multi-qubit divide-and-conquer scheme**

A basic idea of the *divide-and-conquer strategy* is to continue splitting an input of a given combinatorial problem into two (or more) smaller parts until each part is small enough to handle separately and efficiently and then to combine all the small parts in order to solve the entire problem on the given input.

To define the scheme that expresses this divide-and-conquer strategy, we first introduce a useful scheme called the *half division scheme*. Given two quantum functions  $g$  and  $h$  and any input quantum state  $|\phi\rangle$  in  $\mathcal{H}_\infty$ , we simultaneously apply  $g$  to the left half of  $|\phi\rangle$  and  $h$  to the right half of  $|\phi\rangle$  and then obtain the new quantum function denoted by  $HalfD[g, h]$ .

\*) The *half division scheme*. From  $g$  and  $h$ , we define  $HalfD[g, h]$  as follows:

- (i)  $HalfD[g, h](|\phi\rangle) = |\phi\rangle$  if  $\ell(|\phi\rangle) \leq 1$ ,
- (ii)  $HalfD[g, h](|\phi\rangle) = \sum_{s:|s|=LH(|\phi\rangle)} (g(|s\rangle) \otimes h(|s|\phi\rangle))$  otherwise.

Here is a quick example of how this scheme works.

**Example 37.** *Let us consider  $F_1 \equiv HalfD[g, h]$  with  $g = NOT$  and  $h = WH$ . Given an input  $|0^n\rangle|0^n\rangle$ , we obtain  $F_1(|0^n\rangle|0^n\rangle) = g(|0^n\rangle) \otimes h(|0^n\rangle) = \frac{1}{\sqrt{2}}|10^{n-1}\rangle \otimes (|0^n\rangle + |10^{n-1}\rangle)$ . Similarly, consider  $F_2 \equiv HalfD[I, h]$ . We then obtain  $F_2(|0^n\rangle|0^n\rangle) = \frac{1}{\sqrt{2}}|0^n\rangle \otimes (|0^n\rangle + |10^{n-1}\rangle)$ . For the quantum function  $F' \equiv HalfD[F_1, F_2]$ , if  $|0^{2n}\rangle|0^{2n}\rangle$  is an input to  $F'$ , then we obtain  $F'(|0^{2n}\rangle|0^{2n}\rangle) = \frac{1}{2}(|10^{2n-1}\rangle + |10^{n-1}10^{n-1}\rangle) \otimes (|0^{2n}\rangle + |0^n10^{n-1}\rangle)$ .*

We intend to formulate the *multi-qubit divide-and-conquer scheme* (Scheme DC) using  $HalfD[g, h]$ . Recall the quantum function  $SWAP_{i,j}$  given in Lemma 5(10). We expand it by allowing its parameter  $j$  to take a non-constant value. In particular, we intend to take  $LH(\ell(|\phi\rangle)) + 1$  for  $j$  and then define  $midSWAP_1(|\phi\rangle)$  to be  $SWAP_{2,LH(\ell(|\phi\rangle))+1}(|\phi\rangle)$  for any  $|\phi\rangle \in \mathcal{H}_\infty$ . More generally, for a constant  $k \in \mathbb{N}^+$ , we set  $midSWAP_k(|\phi\rangle)$  to be  $SWAP_{2k,m+k} \circ SWAP_{2k-1,m+k-1} \circ \dots \circ SWAP_{k+2,m+2} \circ SWAP_{k+1,m+1}$ , where  $m = LH(\ell(|\phi\rangle))$ . With the use of  $midSWAP_k$ , for any given quantum function  $h$ , we introduce another scheme  $MidApp_k[h]$  by setting  $MidApp_k[h] \equiv midSWAP_k^{-1} \circ h \circ midSWAP_k$ .

Let us quickly examine the behavior of  $MidApp_k[\cdot]$  with a concrete example.

**Example 38.** *For a later argument, we consider the case of quantum function  $h_0 \equiv SWAP^{-1} \circ CNOT \circ SWAP$ , which obviously belongs to  $EQS_0$ . Let  $|\phi\rangle$  denote  $|x_1x_2 \dots x_n\rangle$  for  $n \in \mathbb{N}^+$  and  $x_1, x_2, \dots, x_n \in \{0, 1\}$ . The quantum function  $MidApp_1[h_0]$  satisfies that  $MidApp_1[h_0](|\phi\rangle) = |x_1\rangle$  if  $n = 1$ , and  $MidApp_1[h_0](|\phi\rangle) = |x_1 \oplus x_{LH(n)+1}\rangle |x_2x_3 \dots x_n\rangle$  if  $n \geq 2$ . If we are allowed to use*



extra qubits, then  $MidApp_1[h_0]$  can be realized by an appropriate quantum function, say,  $K$  in EQS obtained with Bit given in Corollary 2 in the following sense:  $K(|0^{3k+8}\rangle_{|x_1x_2 \cdots x_n}) = |0^{3k+8}\rangle \otimes MidApp_1[h_0](|x_1x_2 \cdots x_n)$  if  $k \in \mathbb{N}^+$  satisfies  $n = 2^k$ .

Now, we formally introduce Scheme DC, which “expresses” the divide-and-conquer strategy.

**Definition 39.** We express as DC the following scheme.

(DC) The multi-qubit divide-and-conquer scheme. From  $g, h$ , and  $p$ , and  $k \in \mathbb{N}^+$ , (where  $p$  is not defined using  $MEAS[\cdot]$  and  $g, h$ , and  $p$  are not defined using Scheme DC), we define  $F \equiv DivConq_k[g, h, p|f_1, f_2]$  as:

- (i)  $F(|\phi\rangle) = g(|\phi\rangle)$  if  $\ell(|\phi\rangle) \leq k$ ,
  - (ii)  $F(|\phi\rangle) = MidApp_k[h](HalfD[f_1, f_2](p(|\phi\rangle)))$  otherwise,
- where  $f_1, f_2 \in \{F, I\}$ .

The notation  $EQS + DC$  denotes the smallest set including the quantum functions of Scheme I and being closed under Schemes II–V and DC.

Hereafter, we discuss the usefulness of Scheme DC. Recall the parity function *Parity* from Section 5.2. We have shown in Corollary 36 that EQS is not powerful enough to include *Parity*. In sharp contrast, we argue that *Parity* is in fact definable by applying Schemes I–V and DC.

**Proposition 40.** There exists a quantum function  $f$  in  $EQS + DC$  that simulates *Parity* in the following sense: for any  $x \in \{0, 1\}^*$  and any  $b \in \{0, 1\}$ ,  $Parity(x) = b$  iff  $\|\langle b | \psi_{f,x} \rangle\|^2 = 1$ , where  $|\psi_{f,x}\rangle = f(|x\rangle)$ .

*Proof.* Let us recall the quantum function  $h_0$  described in Example 38 and define  $F$  to be  $DivConq_1[g, h, p|f_1, f_2]$  with  $g = p = I$  and  $f_1 = f_2 = F$ . For any  $n$ -bit string  $x = x_1x_2 \cdots x_n$ , we want to show by induction on  $n \in \mathbb{N}^+$  that (\*) there exist  $y_2, y_3, \dots, y_n \in \{0, 1\}$  for which  $F(|x\rangle) = |\bigoplus_{i=1}^n x_i |y_2 \rangle \cdots |y_n \rangle$ .

If  $n = 1$ , then we instantly obtain  $F(|\phi\rangle) = |\phi\rangle$ . Assume that  $n = 2$ . Since  $HalfD[f_1, f_2](|x_1x_2\rangle) = f_1(|x_1\rangle) \otimes f_2(|x_2\rangle)$ , it follows that  $F(|x_1x_2\rangle) = MidApp_1[h_0](F(|x_1\rangle) \otimes F(|x_2\rangle)) = MidApp_1[h_0](|x_1x_2\rangle) = |x_1 \oplus x_2\rangle |x_2\rangle$ . Let  $n \geq 3$  and assume by induction hypothesis that (\*) is true for all indices  $k \in [n - 1]$ ; namely,  $F(|x_1x_2 \cdots x_k\rangle) = |\bigoplus_{i=1}^k x_i |y_2 \rangle \cdots |y_k \rangle$  for certain suitable bits  $y_2, y_3, \dots, y_k \in \{0, 1\}$ . Let us concentrate on the case of  $x \in \{0, 1\}^n$  with  $x = x_1x_2 \cdots x_n$ . For simplicity, we write  $m$  in place of  $LH(n)$ . Let  $x' = x_1x_2 \cdots x_m$  and  $x'' = x_{m+1} \cdots x_n$  so that  $x = x'x''$ . It thus follows that  $HalfD[f_1, f_2](|x\rangle) = f_1(|x'\rangle) \otimes f_2(|x''\rangle)$ . Since  $F(|x'\rangle) = |\bigoplus_{i=1}^m x_i |y_2 \cdots y_m \rangle$  and  $F(|x''\rangle) = |\bigoplus_{i=m+1}^n x_i |y_{m+2} \cdots y_n \rangle$  by induction hypothesis, we conclude that  $MidApp_1[h_0](F(|x'\rangle) \otimes F(|x''\rangle)) = MidApp_1[h_0](|\bigoplus_{i=1}^m x_i |y_2 \cdots y_m \rangle \otimes |\bigoplus_{i=m+1}^n x_i |y_{m+2} \cdots y_n \rangle) = |\bigoplus_{i=1}^n x_i |y_2 \cdots y_n \rangle$ . This implies that (\*) holds for all  $n \in \mathbb{N}^+$ .  $\square$

### 6.2 Approximately admitting

By Proposition 40, we may anticipate that the multi-qubit divide-and-conquer scheme (Scheme DC) cannot be “realized” or even “approximated” within the system EQS. We formalize this latter notion under the new terminology of “approximately admitting”.

Let us consider an arbitrary scheme (such as composition and fast quantum recursion) whose construction requires a series of quantum functions. Recall the notion of ground (quantum) functions from Section 3.1. Let  $\mathcal{S}$  denote a class of quantum functions and assume that  $\mathcal{R}$  is a scheme requiring a series of  $k$  ground functions taken from  $\mathcal{S}$ . We say that  $\mathcal{S}$  approximately admits  $\mathcal{R}$  if,

for any series  $\mathcal{G} = (g_1, g_2, \dots, g_k)$  with  $g_1, g_2, \dots, g_k \in \mathcal{S}$ , there exists a quantum function  $f \in \mathcal{S}$  and a constant  $\varepsilon \in [0, 1/2)$  such that, for any  $|\phi\rangle \in \mathcal{H}_\infty$ ,  $\|\langle \psi_{f,\phi} | \xi_{\mathcal{R},\mathcal{G},\phi} \rangle\|^2 \geq 1 - \varepsilon$  holds, where  $|\psi_{f,\phi}\rangle = f(|\phi\rangle)$  and  $|\xi_{\mathcal{R},\mathcal{G},\phi}\rangle = \mathcal{R}(g_1, g_2, \dots, g_k)(|\phi\rangle)$ . With this new terminology, we can claim that all schemes listed in Lemma 22, for example, are indeed approximately admitted by EQS.

**Theorem 41.** *EQS does not approximately admit the multi-qubit divide-and-conquer scheme.*

*Proof.* Assume that EQS approximately admits Scheme DC. Since the parity function is realized in EQS + DC (Proposition 40), there exists a polylogtime QTM that computes *Parity* due to the characterization theorem (Theorem 33) of EQS in terms of polylogtime QTMs. This clearly contradicts the fact that no polylogtime QTM can compute the parity function (Lemma 31).  $\square$

### 7. Further discussion and future directions

The schematic approach toward quantum computability was initiated by Yamakami (2020) and made a great success to precisely capture quantum polynomial-time computability using the exquisite scheme of *multi-qubit quantum recursion*. The use of such recursion schemes to characterize quantum computability further leads us to a study on the expressibility of the schemes for quantum computations rather than the more popular algorithmic complexity of quantum computations. In this work, we have made an additional step toward an introduction of a more elementary form of the recursion schematic definition than the one in (Yamakami, 2020). In particular, we have investigated the scheme of (*code-controlled*) *fast quantum recursion* in Section 3.2 as a basis to the class EQS of “elementary” quantum functions, and we have demonstrated the usefulness of various quantum functions based on this new scheme in connection to “parallel” computability in Section 5. An additional scheme, *multi-qubit divide-and-conquer*, has been examined and shown not to be approximately admitted within the framework of EQS in Section 6.

To promote the future research on the schematic definability of quantum computations, we wish to list seven natural open questions that have been left unanswered throughout this work. We expect that fruitful research toward the answers to these questions would make significant progress in the near future on the descriptive aspects of quantum computing.

1. It is quite important to discuss what recursion schemes must be chosen as a basis of EQS. In our formulation, Scheme IV in particular looks rather complicated compared to other schemes. Therefore, we still need to find more “natural” and “simpler” schemes needed to define EQS precisely.
2. Scheme V looks quite different from the other schemes. For instance, the recursive application of  $f_u$  to compute  $F$  in Scheme IV is controlled by “internal” conditions, whereas the repeated application of  $g$  to compute  $F$  in Scheme V is controlled by an “external” condition. It is thus desirable to remove Scheme V from the definition of EQS by simply modifying the definitions of Schemes I–IV. How can we modify them to achieve this goal?
3. We have shown in Theorem 41 that EQS + DC has more expressing power than EQS alone. However, we do not know the exact computational complexity of EQS + DC. It is of great importance to determine its exact complexity.
4. Concerning recursion-schematic characterizations of quantum computing, we have focussed our attention only on “runtime-restricted” quantum computations. Any discussion on “space-restricted” quantum computing has eluded from our attention so far. How can we characterize such computations in terms of recursion schemes?
5. We have discussed the relative complexity of BQPOLYLOGTIME in Section 5.2 in comparison to NLOGTIME and PPOLYLOGTIME. On the contrary, we still do not know whether

$BQPOLYLOGTIME_{\mathbb{Q}}$  differs from  $BPPOLYLOGTIME$ , which is the bounded-error analog of  $PPOLYLOGTIME$ . Are they truly different?

6. It is well known that the choice of (quantum) amplitudes of QTMs affects their computational complexity. In the polynomial-time setting, for example, the bounded-error quantum polynomial-time class  $BQP_{\mathbb{C}}$  differs from  $BQP_{\tilde{\mathbb{C}}}$ , where  $\tilde{\mathbb{C}}$  is the set of polynomial-time approximable complex numbers. On the contrary, the nondeterministic variant  $NQP_{\mathbb{C}}$  collapses to  $NQP_{\tilde{\mathbb{C}}}$  (Yamakami and Yao, 1999). In the polylogtime setting, is it true that  $BQPOLYLOGTIME_{\mathbb{C}} \neq BQPOLYLOGTIME_{\tilde{\mathbb{C}}}$ ?
7. It is desirable to develop a general theory of descriptonal complexity based on recursion schematic definitions of quantum functions for a better understanding of quantum computability and beyond. For a further extension of quantum computability by quantum quantifiers, for example, see (Yamakami, 2002)

## Notes

1 Bernstein and Vazirani discussed only single-tape QTMs. The multiple-tape model of QTMs was distinctly discussed by Yamakami (1999, 2003). The foundation of QTMs was also studied in (Nishimura and Ozawa, 2002; Ozawa and Nishimura, 2000).

2 This notion should be distinguished from the same terminology used by Yamakami (2003), where “quantum functions” mean mappings from binary strings to acceptance probabilities of QTMs.

3 We remark that  $Branch[g, h]$  can be expressed as an appropriate unitary matrix (if  $g$  and  $h$  are expressed as unitary matrices) and thus it is a legitimate quantum operation to consider.

4 This model is also different from the “log-space QTMs” of Yamakami (2022a), which are equipped with “garbage” tapes onto which any unwanted information is discarded to continue their quantum computation.

5 This model is sometimes called a quantum network. See, e.g., (Beals et al., 2001).

6 In (Ambainis, 2002), for example,  $Q_x$  is defined to change  $|bin_k(m)\rangle|\phi\rangle$  to  $(-1)^{x(m)}|bin_k(m)\rangle|\phi\rangle$ . This model is in essence equivalent to our current definition by a simple computation shown as follows. Let  $|\xi\rangle = |bin_k(m)\rangle$ . Starting with  $|\xi\rangle|b\rangle$ , swap between  $|\xi\rangle$  and  $|b\rangle$ , apply  $WH$ , apply  $CQ_x$  (Controlled- $Q_x$ ), apply  $WH$ , and swap back the registers, where  $CQ_x(|0\rangle|\phi\rangle) = |0\rangle|\phi\rangle$  and  $CQ_x(|1\rangle|\phi\rangle) = (-1)^{x(m)}|1\rangle|\phi\rangle$ . We then obtain  $|\xi\rangle|b \oplus x(m)\rangle$ .

## References

- Ambainis, A. (2002). Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences* **64** (4) 750–767.
- Babai, L., Fortnow, L., Levin, L. A. and Szegedy, M. (1991). Checking computations in polylogarithmic time. In: *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing (STOC'91)*, 21–31.
- Barenco, A., Bennett, C. H., Cleve, R., DiVincenzo, D., Margolus, N., Shor, P., Sleator, T., Smolin, J. and Weinfurter, H. (1995). Elementary gates for quantum computation. *Physical Review A*. **52** (5) 3457–3467.
- Barrington, D. A. M., Immerman, N. and Straubing, H. (1990). On uniformity within  $NC^1$ . *Journal of Computer and System Sciences*. **41** 274–306.
- Beals, R., Buhrman, H., Cleve, R., Mosca, M. and de Wolf, R. (2001). Quantum lower bounds by polynomials. *Journal of the ACM*. **48** (4) 778–797.
- Benioff, P. (1980). The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*. **22** (5) 563–591.
- Bernstein, E. and Vazirani, U. (1997). Quantum complexity theory. *SIAM Journal on Computing*. **26** (5) 1411–1473.
- Bradford, P. G., Rawlins, G. J. E. and Shannon, G. E. (1994). Efficient matrix chain ordering in polylog time. In: *Proceedings of the 8th International Symposium on Parallel Processing, IEEE Computer Society*, 234–241.
- Buss, S. (1987). The Boolean formula value problem is in  $ALOGTIME$ . In: *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC'87)*, 123–131.
- Deutsch, D. (1985). Quantum theory, the church-turing principle, and the universal quantum computer. *Proceedings Royal Society London, Series A*. **400** 97–117.
- Deutsch, D. (1989). Quantum computational networks. *Proceedings Royal Society London, Series A*. **425** 73–90.
- Hainry, E., Péchoux, R. and Silva, M. (2023). A programming language characterizing quantum polynomial time. In: *Proceedings of the 26th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS 2023), Lecture Notes in Computer Science*, vol. 13992. Springer, 156–175.

- Holm, J., de Lichtenberg, K. and Thorup, M. (2001). Poly-logarithmic deterministic fully-dynamic algorithms for connectivity, minimum spanning tree, 2-edge, and biconnectivity. *Journal of the ACM*. **48** (4) 723–760.
- Kitaev, A. Y., Shen, A. H. and Vyalii, M. N. (2002). *Classical and Quantum Computation (Graduate Studies in Mathematics)*, Americal Mathematical Society.
- Kleene, S. C. (1936). General recursive functions of natural numbers. *Mathematische Annalen*. **112** (1) 727–742.
- Kleene, S. C. (1943). Recursive predicates and quantifiers. *Transactions of the American Mathematical Society*. **53** (1) 41–73.
- Munro, J. I. (1984). An implicit data structure for the dictionary problem that runs in polylogtime. In: *Proceedings of the 25th Annual Symposium on Foundations of Computer Science (FOCS'84)*, 369–374.
- Nielsen, M. A. and Chuang, I. L. (2016). *Quantum Computation and Quantum Information*, 10th Anniverswary edn., Cambridge University Press.
- Nishimura, H. and Ozawa, M. (2002). Computational complexity of uniform quantum circuit families and quantum turing machines. *Theoretical Computer Science*. **276** (1-2) 147–181.
- Nishimura, H. and Yamakami, T. (2004). An Algorithmic argument for nonadaptive query complexity lower bounds on advised quantum computation (extended abstract). In: *Proceedings of the 29th International Symposium on Mathematical Foundations of Computer Science (MFCS 2004), Lecture Notes in Computer Science*, vol. 3153. Springer, 827–838. A complete version is available at arXiv:quant-ph/0312003.
- Ozawa, M. and Nishimura, H. (2000). Local transition functions of quantum turing machines. *RAIRO - Theoretical Informatics and Applications*. **276** (5) 379–402.
- Raz, R. and Tal, A. (2022). Oracle separation of BQP and PH. *Journal of the ACM*. **69** (4) article 30.
- Soare, R. I. (1996). Computability and recursion. *Bulletin of Symbolic Logic*. **2** (3) 284–321.
- Tadaki, K., Yamakami, T. and Lin, J. C. H. (2010). Theory of one-tape linear-time Turing machines. *Theoretical Computer Science*. **411** (1) 22–43. An early extended abstract appeared in the Proceedings of the 30th SOFSEM Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM 2004), Lecture Notes in Computer Science, vol.2932, pp.335-348, Springer, 2004.
- Vollmer, H. (1999). *Introduction to Curcuit Complexity*, Springer-Verlag.
- Yamakami, T. (1999). A foundation of programming a multi-tape quantum Turing machine. In: *Proceedings of the 24th International Conference on Mathematical Foundations of Computer Science (MFCS'99), Lecture Notes in Computer Science*, Springer, 430–441. Available also at arXiv:quant-ph/9906084.
- Yamakami, T. (2002). Quantum NP and a quantum hierarchy. In: *Proceedings of the 2nd IFIP International Conference on Theoretical Computer Science (TCS 2002), Kluwer Academic Press (under the title of Foundations of Information Technology in the Era of Network and Mobile Computing)*, The International Federation for Information Processing, 323–336.
- Yamakami, T. (2003). Analysis of quantum functions. *International Journal of Foundations of Computer Science*. **14** (05) 815–852.
- Yamakami, T. (2020). A schematic definition of quantum polynomial time computability. *The Journal of Symbolic Logic*. **85** (4) 1546–1587. An early extended abstract appeared under a slightly different title in the Proceeedngs of the 9th Workshop on Non-Classical Models of Automata and Applications (NCMA 2017), Österreichische Computer Gesellschaft 2017, pp. 243-258, 2017.
- Yamakami, T. (2022a). Nonuniform families of polynomial-size quantum finite automata and quantum logarithmic-space computation with polynomial-size advice. *Information and Computation*. **286**, article 104783. A preliminary version appeared in the Proceedings of the 20th International Conference on Descriptive Complexity of Formal Systems (DCFS 2018), Lecture Notes in Computer Science, vol. 10952, pp. 237–249, Springer, 2018.
- Yamakami, T. (2022b). Expressing power of elementary quantum recursion schemes for quantum logarithmic-time computability. In: *Proceedings of the 28th International Conference on Logic, Language, Information, and Computation (WoLLIC 2022), Lecture Notes in Computer Science*, vol. 13468, pp. 88–104, Springer, 2022.
- Yamakami, T. and Yao, A. C. (1999).  $NQP_C = co-C = P$ . *Information Processing Letters*. **71** 63–69.
- Yao, A. C. (1993). Quantum circuit complexity. In: *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science (FOCS'93)*, 80–91.