

3.1 Definition of \square_1^{QP} -Functions

Our schematic definition induces a special function class, called \square_1^{QP} (where \square is pronounced “square”), capturing polynomial-time computable quantum functions mapping \mathcal{H}_∞ to \mathcal{H}_∞ , which is composed of a small set of initial quantum functions and four special construction rules: composition, swapping, branching, and multi-qubit quantum recursion. Definition 3.1 formally presents our schematic definition.

Hereafter, we say that a quantum function f from \mathcal{H}_∞ to \mathcal{H}_∞ is *dimension-preserving* if, for every quantum state $|\phi\rangle \in \mathcal{H}_\infty$ and any number $n \in \mathbb{N}^+$, $|\phi\rangle \in \mathcal{H}_{2^n}$ implies $f(|\phi\rangle) \in \mathcal{H}_{2^n}$ (i.e., $\ell(|\phi\rangle) = \ell(f(|\phi\rangle))$).

Definition 3.1 Let \square_1^{QP} denote the collection of all quantum functions that are obtained from the initial quantum functions in Scheme I by a finite number (including zero) of applications of construction rules II–IV to quantum functions that have been already constructed, where Schemata I–IV[¶] are given as follows. Let $|\phi\rangle$ be any quantum state in \mathcal{H}_∞ .

- I. The initial quantum functions. Let $\theta \in [0, 2\pi) \cap \tilde{\mathbb{C}}$ 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 θ)
 - 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 rule. 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 rule. 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) $Branch[g, h](|\phi\rangle) = |0\rangle \otimes g(|\phi\rangle) + |1\rangle \otimes h(|\phi\rangle)$ otherwise.
- IV. The multi-qubit quantum recursion rule. From g, h , dimension-preserving p , and $k, t \in \mathbb{N}^+$, we define $kQRec_t[g, h, p|\mathcal{F}_k]$ as:
 - (i) $kQRec_t[g, h, p|\mathcal{F}_k](|\phi\rangle) = g(|\phi\rangle)$ if $\ell(|\phi\rangle) \leq t$,
 - (ii) $kQRec_t[g, h, p|\mathcal{F}_k](|\phi\rangle) = h(\sum_{s:|s|=k} |s\rangle \otimes f_s(|\psi_{p,\phi}\rangle))$ otherwise,
 where $|\psi_{p,\phi}\rangle = p(|\phi\rangle)$ and $\mathcal{F}_k = \{f_s\}_{s \in \{0,1\}^k} \subseteq \{kQRec_t[g, h, p|\mathcal{F}_k], I\}$. To emphasize “ k ,” we call this rule by the *k -qubit quantum recursion*. In the case of $k = 1$, we write $QRec_t[g, h, p|f_0, f_1]$ in place of $1QRec_t[g, h, p|\{f_0, f_1\}]$ for brevity.

In Scheme I, $PHASE_\theta$ and ROT_θ correspond respectively to the matrices $Z_{2,\theta}$ and R_θ given in Section 2.3. Latter, we will argue that an angle θ in $PHASE_\theta$ and ROT_θ could be fixed to $\pi/4$. The quantum function $MEAS$ is associated with a *partial projective measurement*, in the computational basis $\{0, 1\}$, applied to the first qubit of $|\phi\rangle$, when $\ell(|\phi\rangle) \geq 1$, and it obviously follows that $\ell(MEAS[i](|\phi\rangle)) \leq \ell(|\phi\rangle)$.

Before proceeding further, to help the reader understand the behaviors of the initial quantum functions listed in Scheme I, we briefly illustrate how these functions transform basic qustrings of length 3. For bits $a, b, c, d \in \{0, 1\}$ with $d \neq a$, it follows that $I(|abc\rangle) = |abc\rangle$, $PHASE_\theta(|abc\rangle) = e^{i\theta a}|abc\rangle$, $ROT_\theta(|abc\rangle) = \cos \theta|abc\rangle + (-1)^a \sin \theta|\bar{a}bc\rangle$, $NOT(|abc\rangle) = |\bar{a}bc\rangle$, $SWAP(|abc\rangle) = |bac\rangle$, $MEAS[a](|abc\rangle) = |abc\rangle$, and $MEAS[d](|abc\rangle) = \mathbf{0}$, where $\bar{a} = 1 - a$.

Scheme IV is a core of the definition of \square_1^{QP} . The standard recursion rule used to define a primitive recursive function f from two functions g and h has the form: $f(0, x) = g(x)$ and $f(n+1, x) = h(n, x, f(n, x))$ for any $n \in \mathbb{N}$. This rule requires an internal counter (in the first argument place of f) that controls the number of iterated applications of h . In Scheme IV, however, we do not use such a counter. Instead, we use a divide-and-conquer strategy to slice a given quantum state qubit by qubit. At each inductive step, we deal with k -qubit shorter quantum states until the quantum state has become length t or less. We wish to provide two concrete examples of how Scheme IV works in the cases of $k = 1, 2$. Notice that, in the case of $k = 1$, Scheme IV becomes the *1-qubit* (or *single-qubit*) *quantum recursion rule* described as:

- (i') $QRec_t[g, h, p|f_0, f_1](|\phi\rangle) = g(|\phi\rangle)$ if $\ell(|\phi\rangle) \leq t$,
 - (ii') $QRec_t[g, h, p|f_0, f_1](|\phi\rangle) = h(|0\rangle \otimes f_0(|\psi_{p,\phi}\rangle) + |1\rangle \otimes f_1(|\psi_{p,\phi}\rangle))$ otherwise,
- where each of f_0 and f_1 must be either I or $QRec_t[g, h, p|f_0, f_1]$.

[¶]The current formalism of Schemata I–IV corrects discrepancies caused by the early formalism given in the extended abstract [39].

Example 1. We first consider the case of $k = 1$. In this example, we set $t = 1$, $g = NOT$, $h = SWAP$, and $p = NOT$, and we briefly write F for $QRec_1[NOT, SWAP, NOT|f_0, f_1]$ with $f_0 = I$ and $f_1 = F$. It is worth mentioning that $\mathbf{0}$ is a special object and we obtain $g(\mathbf{0}) = \mathbf{0}$ for any quantum function g by Lemma 3.4(1). Let $|\phi\rangle$ denote any quantum state in \mathcal{H}_∞ given as an input to F .

(1) Assume that $|\phi\rangle$ has length 1 and is of the form $\alpha|0\rangle + \beta|1\rangle$ in general. By Lemma 3.4(2), it suffices for us to consider the computational basis $B_1 = \{|0\rangle, |1\rangle\}$. Since $\ell(|\phi\rangle) \leq t$, the outcomes of f for those basis qubits $|0\rangle$ and $|1\rangle$ are calculated as follows.

$$(i) F(|0\rangle) = g(|0\rangle) = NOT(|0\rangle) = |1\rangle.$$

$$(ii) F(|1\rangle) = g(|1\rangle) = NOT(|1\rangle) = |0\rangle.$$

Obviously, $F(\mathbf{0}) = \mathbf{0}$ holds. Since $|\phi\rangle$ is a superposition of the form $\alpha|0\rangle + \beta|1\rangle$, the above calculations instantly imply

$$F(|\phi\rangle) = F(\alpha|0\rangle + \beta|1\rangle) = NOT(\alpha|0\rangle + \beta|1\rangle) = \alpha NOT(|0\rangle) + \beta NOT(|1\rangle) = \alpha|1\rangle + \beta|0\rangle.$$

(2) Next, let us assume that $|\phi\rangle$ is of length 2. In the case where $|\phi\rangle$ is the basis quantum state $|00\rangle$ in $B_2 = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, we obtain $|\psi_{p,\phi}\rangle = |\psi_{NOT,00}\rangle = NOT(|00\rangle) = |10\rangle$. Similarly, if $|\phi\rangle$ is $|01\rangle$, $|10\rangle$, and $|11\rangle$, then the quantum state $|\psi_{p,\phi}\rangle$ is $|11\rangle$, $|00\rangle$, and $|01\rangle$, respectively. Concerning the partial projective measurement, it follows that, for any bit $a \in \{0, 1\}$, $\langle 1|1a\rangle = |a\rangle$, $\langle 0|0a\rangle = |a\rangle$, $\langle 1|0a\rangle = \mathbf{0}$, and $\langle 0|1a\rangle = \mathbf{0}$. Note also that $I(\mathbf{0}) = \mathbf{0}$. Using these equalities together with $F(|0\rangle) = |1\rangle$ and $F(|1\rangle) = |0\rangle$ obtained in (1), we can calculate the outcome $F(|\phi\rangle)$ as follows.

$$(i) F(|00\rangle) = h(|0\rangle \otimes f_0(\langle 0|\psi_{NOT,00}\rangle) + |1\rangle \otimes f_1(\langle 1|\psi_{NOT,00}\rangle) = h(|0\rangle \otimes I(\langle 0|10\rangle) + |1\rangle \otimes F(\langle 1|10\rangle)) = h(|0\rangle \otimes I(\mathbf{0}) + |1\rangle \otimes F(|0\rangle)) = h(|1\rangle \otimes F(|0\rangle)) = SWAP(|1\rangle \otimes |1\rangle) = SWAP(|11\rangle) = |11\rangle.$$

$$(ii) F(|10\rangle) = h(|0\rangle \otimes f_0(\langle 0|\psi_{NOT,10}\rangle) + |1\rangle \otimes f_1(\langle 1|\psi_{NOT,10}\rangle) = h(|0\rangle \otimes I(\langle 0|00\rangle) + |1\rangle \otimes F(\langle 1|00\rangle)) = h(|0\rangle \otimes I(|0\rangle) + |1\rangle \otimes F(\mathbf{0})) = h(|0\rangle \otimes I(|0\rangle)) = SWAP(|0\rangle \otimes |0\rangle) = SWAP(|00\rangle) = |00\rangle.$$

$$(iii) F(|01\rangle) = h(|0\rangle \otimes f_0(\langle 0|\psi_{NOT,01}\rangle) + |1\rangle \otimes f_1(\langle 1|\psi_{NOT,01}\rangle) = h(|0\rangle \otimes I(\langle 0|11\rangle) + |1\rangle \otimes F(\langle 1|11\rangle)) = h(|0\rangle \otimes I(\mathbf{0}) + |1\rangle \otimes F(|1\rangle)) = h(|1\rangle \otimes F(|1\rangle)) = SWAP(|1\rangle \otimes |0\rangle) = SWAP(|10\rangle) = |01\rangle.$$

$$(iv) F(|11\rangle) = h(|0\rangle \otimes f_0(\langle 0|\psi_{NOT,11}\rangle) + |1\rangle \otimes f_1(\langle 1|\psi_{NOT,11}\rangle) = h(|0\rangle \otimes I(\langle 0|01\rangle) + |1\rangle \otimes F(\langle 1|01\rangle)) = h(|0\rangle \otimes I(|1\rangle) + |1\rangle \otimes F(\mathbf{0})) = h(|0\rangle \otimes I(|1\rangle)) = SWAP(|0\rangle \otimes |1\rangle) = SAWP(|01\rangle) = |10\rangle.$$

By Lemma 3.4(2), when $|\phi\rangle$ is of the form $\alpha|00\rangle + \beta|10\rangle$ for example, we obtain

$$F(|\phi\rangle) = F(\alpha|00\rangle + \beta|10\rangle) = \alpha F(|00\rangle) + \beta F(|10\rangle) = \alpha|11\rangle + \beta|00\rangle.$$

(3) Let us consider the case where the length of $|\phi\rangle$ is 3. For the computational basis $B_3 = \{|000\rangle, |001\rangle, |010\rangle, \dots, |111\rangle\}$, we calculate the outcomes $F(|\phi\rangle)$ only for inputs $|\phi\rangle$ in $\{|001\rangle, |101\rangle\}$. Notice that $|\psi_{NOT,001}\rangle = |101\rangle$ and $|\psi_{NOT,101}\rangle = |001\rangle$. Recall from (1)–(2) that $F(|01\rangle) = |01\rangle$ and $F(\mathbf{0}) = \mathbf{0}$.

$$(i) F(|001\rangle) = h(|0\rangle \otimes f_0(\langle 0|\psi_{NOT,001}\rangle) + |1\rangle \otimes f_1(\langle 1|\psi_{NOT,001}\rangle) = h(|0\rangle \otimes I(\langle 0|101\rangle) + |1\rangle \otimes F(\langle 1|101\rangle)) = h(|0\rangle \otimes I(\mathbf{0}) + |1\rangle \otimes F(|01\rangle)) = h(|1\rangle \otimes F(|01\rangle)) = SWAP(|1\rangle \otimes |01\rangle) = SAWP(|101\rangle) = |011\rangle.$$

$$(ii) F(|101\rangle) = h(|0\rangle \otimes f_0(\langle 0|\psi_{NOT,101}\rangle) + |1\rangle \otimes f_1(\langle 1|\psi_{NOT,101}\rangle) = h(|0\rangle \otimes I(\langle 0|001\rangle) + |1\rangle \otimes F(\langle 1|001\rangle)) = h(|0\rangle \otimes I(|01\rangle) + |1\rangle \otimes F(\mathbf{0})) = h(|0\rangle \otimes I(|01\rangle)) = SWAP(|0\rangle \otimes |01\rangle) = SAWP(|001\rangle) = |001\rangle.$$

If $|\phi\rangle$ is of the form $\alpha|001\rangle + \beta|101\rangle$ for example, Lemma 3.4(2) implies that $F(|\phi\rangle) = F(\alpha|001\rangle + \beta|101\rangle) = \alpha F(|001\rangle) + \beta F(|101\rangle) = \alpha|011\rangle + \beta|001\rangle$.

Example 2. We see another example for the case of $k = 2$. By setting $t = 3$, $g = NOT$, $h = SWAP$, and $p = NOT$ for instance, we write F for $2QRec_3[NOT, SWAP, NOT|f_{00}, f_{01}, f_{10}, f_{11}]$ with $f_{00} = I$, $f_{01} = NOT$, $f_{10} = F$, and $f_{11} = F$. Let $|\phi\rangle$ denote any quantum state in \mathcal{H}_∞ .

(1) When the length of $|\phi\rangle$ is at most 3, we instantly obtain $F(|\phi\rangle) = g(|\phi\rangle) = NOT(|\phi\rangle)$. For example, $F(|0\rangle) = |1\rangle$, $F(|10\rangle) = |00\rangle$, and $F(|101\rangle) = |001\rangle$.

(2) Assuming that the length of $|\phi\rangle$ is 4, let us consider the basis quantum states in $B_4 = \{|0000\rangle, |0001\rangle, |0010\rangle, \dots, |1111\rangle\}$. Here, we are focused only on two cases: $|\phi\rangle \in \{|0101\rangle, |1011\rangle\}$. We remark that $|\psi_{NOT,0010}\rangle = NOT(|0010\rangle) = |1010\rangle$ and $|\psi_{NOT,1011}\rangle = NOT(|1011\rangle) = |0011\rangle$.

$$(i) F(|0010\rangle) = h(|00\rangle \otimes f_{00}(\langle 00|\psi_{NOT,0010}\rangle) + |01\rangle \otimes f_{01}(\langle 01|\psi_{NOT,0010}\rangle) + |10\rangle \otimes f_{10}(\langle 10|\psi_{NOT,0010}\rangle) + |11\rangle \otimes f_{11}(\langle 11|\psi_{NOT,0010}\rangle)) = h(|00\rangle \otimes I(\langle 00|1010\rangle) + |01\rangle \otimes NOT(\langle 01|1010\rangle) + |10\rangle \otimes F(\langle 10|1010\rangle) + |11\rangle \otimes F(\langle 11|1010\rangle)) = h(|00\rangle \otimes I(\mathbf{0}) + |01\rangle \otimes NOT(\mathbf{0}) + |10\rangle \otimes F(|10\rangle) + |11\rangle \otimes F(\mathbf{0})) = h(|10\rangle \otimes F(|10\rangle)) = SWAP(|10\rangle \otimes |00\rangle) = SWAP(|1000\rangle) = |0100\rangle.$$

$$(ii) F(|1011\rangle) = h(|00\rangle \otimes f_{00}(\langle 00|\psi_{NOT,1011}\rangle) + |01\rangle \otimes f_{01}(\langle 01|\psi_{NOT,1011}\rangle) + |10\rangle \otimes f_{10}(\langle 10|\psi_{NOT,1011}\rangle) + |11\rangle \otimes f_{11}(\langle 11|\psi_{NOT,1011}\rangle)) = h(|00\rangle \otimes I(\langle 00|0101\rangle) + |01\rangle \otimes NOT(\langle 01|0101\rangle) + |10\rangle \otimes F(\langle 10|0101\rangle) + |11\rangle \otimes F(\langle 11|0101\rangle)) = h(|00\rangle \otimes I(\mathbf{0}) + |01\rangle \otimes NOT(|01\rangle) + |10\rangle \otimes F(\mathbf{0}) + |11\rangle \otimes F(\mathbf{0})) = h(|01\rangle \otimes NOT(|01\rangle)) = SWAP(|01\rangle \otimes |11\rangle) = SWAP(|0111\rangle) = |1011\rangle.$$

3.2 A Subclass of \square_1^{QP} and Basic Properties

Among the six initial quantum functions in Scheme I, *MEAS* makes a quite different behavior. It can change the norm as well as the dimensionality of quantum states, and that fact makes it irreversible in nature. For this reason, it is often beneficial in practice to limit our attention to a subclass of \square_1^{QP} , called $\widehat{\square_1^{\text{QP}}}$, which entirely prohibits the use of *MEAS*.

Definition 3.2 The notation $\widehat{\square_1^{\text{QP}}}$ denotes the subclass of \square_1^{QP} defined by Schemata I-IV except for *MEAS* listed in Scheme I.

With no use of *MEAS* in Scheme I, every quantum function f in $\widehat{\square_1^{\text{QP}}}$ preserves the dimensionality of inputs; in other words, f satisfies $\ell(f(|\phi\rangle)) = \ell(|\phi\rangle)$ for any input $|\phi\rangle \in \mathcal{H}_\infty$.

Next, let us demonstrate how to construct typical unitary gates using our schematic definition.

Lemma 3.3 The following functions are in $\widehat{\square_1^{\text{QP}}}$. Let $|\phi\rangle$ be any element in \mathcal{H}_∞ .

1. $CNOT(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ |0\rangle\langle 0|\phi\rangle + |1\rangle \otimes NOT(\langle 1|\phi\rangle) & \text{otherwise.} \end{cases} \quad (\text{controlled-NOT})$
2. $Z_{1,\theta}(|\phi\rangle) = e^{i\theta}|0\rangle\langle 0|\phi\rangle + |1\rangle\langle 1|\phi\rangle.$
3. $zROT_\theta(|\phi\rangle) = e^{i\theta}|0\rangle\langle 0|\phi\rangle + e^{-i\theta}|1\rangle\langle 1|\phi\rangle. \quad (\text{rotation around the } z\text{-axis})$
4. $GPS_\theta(|\phi\rangle) = e^{i\theta}|\phi\rangle. \quad (\text{global phase shift})$
5. $WH(|\phi\rangle) = \frac{1}{\sqrt{2}}|0\rangle \otimes (\langle 0|\phi\rangle + \langle 1|\phi\rangle) + \frac{1}{\sqrt{2}}|1\rangle \otimes (\langle 0|\phi\rangle - \langle 1|\phi\rangle). \quad (\text{Walsh-Hadamard transform})$
6. $CPHASE_\theta(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ \frac{1}{\sqrt{2}} \sum_{b \in \{0,1\}} (|0\rangle\langle b|\phi\rangle + e^{i\theta b}|1\rangle\langle b|\phi\rangle) & \text{otherwise.} \end{cases} \quad (\text{controlled-PHASE})$

Proof. It suffices to build each of the quantum functions given in the lemma from the initial quantum functions and by applying the construction rules. These target functions are constructed as follows. (1) $CNOT = \text{Branch}[I, NOT]$. Note that, when $\ell(|\phi\rangle) \leq 1$, Scheme III(i) implies $CNOT(|\phi\rangle) = |\phi\rangle$, matching Item 1 for *CNOT*. (2) $Z_{1,\theta} = NOT \circ PHASE_\theta \circ NOT$. (3) $zROT_\theta = Z_{1,\theta} \circ PHASE_{-\theta}$. (4) $GPS_\theta = Z_{1,\theta} \circ PHASE_\theta$. (5) $WH = ROT_{\frac{\pi}{4}} \circ NOT$. (6) $CPHASE_\theta = \text{Branch}[WH, f]$, where $f = \text{Branch}[I, GPS_\theta] \circ WH \circ NOT$. \square

Since any \square_1^{QP} -function f is constructed by applying Schemata I–IV, an application of one of the schemata is viewed as a basic step of the construction process of generating f . This fact helps us define the *descriptive complexity* of f to be the minimal number of times we use those schemata in order to construct f . For instance, all the initial functions have descriptive complexity 1 because they use Scheme I only once. As demonstrated in the proof of Lemma 3.3, the quantum functions *CNOT*, $Z_{1,\theta}$, and *WH* have descriptive complexity at most 3 and $zROT_\theta$ and GPS_θ have descriptive complexity at most 4, whereas $CPHASE_\theta$ is of descriptive complexity at most 15. This complexity measure is essential in proving, e.g., Lemma 3.4 since the lemma will be proven by induction on the descriptive complexity of a target quantum function. In Section 6.2, we will give a short discussion on this complexity measure for a future study.

Fundamental properties of $\widehat{\square_1^{\text{QP}}}$ -functions are given in the following lemma. A quantum function from \mathcal{H}_∞ to \mathcal{H}_∞ is called *norm-preserving* if $\|f(|\phi\rangle)\| = \||\phi\rangle\|$ holds for all quantum states $|\phi\rangle$ in \mathcal{H}_∞ .

Lemma 3.4 Let f be any quantum function in $\widehat{\square_1^{\text{QP}}}$ and let $|\phi\rangle, |\psi\rangle \in \mathcal{H}_\infty$ and $\alpha \in \mathbb{C}$.

1. $f(\mathbf{0}) = \mathbf{0}$, where $\mathbf{0}$ is the null vector.
2. $f(|\phi\rangle + |\psi\rangle) = f(|\phi\rangle) + f(|\psi\rangle).$
3. $f(\alpha|\phi\rangle) = \alpha \cdot f(|\phi\rangle).$
4. f is dimension-preserving and norm-preserving.

Proof. Let f be any $\widehat{\square_1^{\text{QP}}}$ -function, let $|\phi\rangle, |\psi\rangle \in \mathcal{H}_\infty$, and let $\alpha \in \mathbb{C}$ and $\theta \in [0, 2\pi)$ be constants. As mentioned earlier, we will prove the lemma by induction of the *descriptive complexity* of f . If f is one of the initial quantum functions in Scheme I, then it is easy to check that it satisfies Conditions 1–4 of the lemma. In particular, when $|\phi\rangle$ is the null vector $\mathbf{0}$, all of $e^{i\theta}|\phi\rangle$, $\cos\theta|\phi\rangle$, $\sin\theta|\phi\rangle$, $\langle 0|\phi\rangle$, $\langle 1|\phi\rangle$, and $\langle ba|\phi\rangle$ used in Scheme I are $\mathbf{0}$; thus, $|b\rangle \otimes \langle 1|\phi\rangle$ and $|b\rangle \otimes \langle 0|\phi\rangle$ are also $\mathbf{0}$ for each bit $b \in \{0, 1\}$. Therefore, Condition 1 follows.

Among Schemata II–IV, let us consider Scheme IV since the other schemata are easily shown to meet Conditions 1–4. Let g , h , and p be quantum functions in $\widehat{\square}_1^{\text{QP}}$ and assume that p is dimension-preserving. By induction hypothesis, we assume that g , h , and p satisfy Conditions 1–4. For readability, we write f for $kQRec_t[g, h, p|\mathcal{F}_k]$. In what follows, we are focused only on Conditions 2 and 4 since the other conditions are easy to check. Our argument will employ induction on the length of input $|\phi\rangle$ given to f .

(i) Our goal is to show that f satisfies Condition 2. Firstly, consider the case of $\ell(|\phi\rangle) \leq t$. It then follows that $f(|\phi\rangle + |\xi\rangle) = g(|\phi\rangle + |\xi\rangle) = g(|\phi\rangle) + g(|\xi\rangle)$ since g is assumed to meet Condition 2. Next, we consider the case where $\ell(|\phi\rangle) > t$. From the definition of f , we obtain $f(|\phi\rangle + |\xi\rangle) = h(\sum_{s:|s|=k} |s\rangle \otimes f_s(\langle s|\psi_{p,\phi,\xi}\rangle))$, where $|\psi_{p,\phi,\xi}\rangle = p(|\phi\rangle + |\xi\rangle)$. Since $p(|\phi\rangle + |\xi\rangle) = p(|\phi\rangle) + p(|\xi\rangle)$ by induction hypothesis, we conclude that $\langle s|\psi_{p,\phi,\xi}\rangle = \langle s|\psi_{p,\phi}\rangle + \langle s|\psi_{p,\xi}\rangle$ for each string $s \in \{0,1\}^k$. It then follows by induction hypothesis that $f_s(\langle s|\psi_{p,\phi,\xi}\rangle) = f_s(\langle s|\psi_{p,\phi}\rangle) + f_s(\langle s|\psi_{p,\xi}\rangle)$, leading to the equation $|s\rangle \otimes f_s(\langle s|\psi_{p,\phi,\xi}\rangle) = |s\rangle \otimes f_s(\langle s|\psi_{p,\phi}\rangle) + |s\rangle \otimes f_s(\langle s|\psi_{p,\xi}\rangle)$. Using Condition 2 for h , we obtain $h(\sum_{s:|s|=k} |s\rangle \otimes f_s(\langle s|\psi_{p,\phi,\xi}\rangle)) = \sum_{s:|s|=k} h(|s\rangle \otimes f_s(\langle s|\psi_{p,\phi}\rangle)) + \sum_{s:|s|=k} h(|s\rangle \otimes f_s(\langle s|\psi_{p,\xi}\rangle))$. We then conclude that $f(|\phi\rangle + |\xi\rangle) = f(|\phi\rangle) + f(|\xi\rangle)$.

(ii) We want to show that f satisfies Condition 4. By induction hypothesis, it follows that, for any $s \in \{0,1\}^k$, $\|f_s(\langle s|\psi_{p,\phi}\rangle)\| = \|\langle s|\psi_{p,\phi}\rangle\|$ and $\|h(|\phi\rangle)\| = \|\phi\|$. These equalities imply that $\|f(|\phi\rangle)\|^2 = \|h(\sum_{s:|s|=k} |s\rangle \otimes f_s(\langle s|\psi_{p,\phi}\rangle))\|^2 = \|\sum_{s:|s|=k} |s\rangle \otimes f_s(\langle s|\psi_{p,\phi}\rangle)\|^2 = \sum_{s:|s|=k} \|f_s(\langle s|\psi_{p,\phi}\rangle)\|^2$, which equals $\sum_{s:|s|=k} \|\langle s|\psi_{p,\phi}\rangle\|^2$. The last term coincides with $\|\psi_{p,\phi}\|^2$, which equals $\|p(|\phi\rangle)\|^2$. This implies Condition 4 because $\|p(|\phi\rangle)\| = \|\phi\|$. \square

Lemma 3.4(4) indicates that all functions in $\widehat{\square}_1^{\text{QP}}$ also serve as functions mapping Φ_∞ to Φ_∞ in place of \mathcal{H}_∞ to \mathcal{H}_∞ .

Given a quantum function g that is dimension-preserving and norm-preserving, the *inverse* of g is a unique quantum function f satisfying the condition that, for every $|\phi\rangle \in \mathcal{H}_\infty$, $f \circ g(|\phi\rangle) = g \circ f(|\phi\rangle) = |\phi\rangle$. This special quantum function f is expressed as g^{-1} .

The next proposition guarantees that $\widehat{\square}_1^{\text{QP}}$ is closed under “inverse” since $\widehat{\square}_1^{\text{QP}}$ lacks *MEAS*.

Proposition 3.5 *For any quantum function $g \in \widehat{\square}_1^{\text{QP}}$, g^{-1} exists and belongs to $\widehat{\square}_1^{\text{QP}}$.*

Proof. We prove this proposition by induction on the aforementioned *descriptive complexity* of g . If g is one of the initial quantum functions, then we define its inverse g^{-1} as: $I^{-1} = I$, $PHASE_\theta^{-1} = PHASE_{-\theta}$, $ROT_\theta^{-1} = ROT_{-\theta}$, $NOT^{-1} = NOT$, and $SWAP^{-1} = SWAP$. If g is obtained from another quantum function or functions by one of the construction rules, then its inverse is defined as: $Compo[g, h]^{-1} = Compo[h^{-1}, g^{-1}]$, $Branch[g, h]^{-1} = Branch[g^{-1}, h^{-1}]$, and $kQRec_t[g, h, p|\{f_s\}_{s \in \{0,1\}^k}]^{-1} = kQRec_t[g^{-1}, p^{-1}, h^{-1}|\{f_s^{-1}\}_{s \in \{0,1\}^k}]$. \square

Our choice of Schemata I–IV is motivated by a particular universal set of quantum gates. Notice that a different choice of initial quantum functions and construction rules may lead to a different set of \square_1^{QP} -functions. Scheme I uses an “arbitrary” angle of θ in $[0, 2\pi) \cap \mathbb{C}$ to introduce $PHASE_\theta$ and ROT_θ ; however, we can restrict θ to a unique value of $\frac{\pi}{4}$ since $PHASE_\theta$ and ROT_θ for an arbitrary value $\theta \in [0, 2\pi)$ can be approximated to any desired accuracy using WH and $Z_{2, \frac{\pi}{4}}$. This last part comes from the fact that any single-qubit unitary operator can be approximated to any accuracy from the quantum gates WH and $Z_{2, \frac{\pi}{4}}$ [6] (see also [25]). For a further discussion on the choice of the schemata, see Section 6.1.

3.3 Construction of More Complicated Quantum Functions

Before presenting the main theorem (Theorem 4.1), we wish to prepare useful quantum functions and new construction rules derived directly from Schemata I–IV. These quantum functions and construction rules will be used for the proof of our key lemma (Lemma 4.3), which supports the main theorem.

For each $k \in \mathbb{N}^+$, let us assume the standard lexicographic ordering $<$ on $\{0,1\}^k$ and all elements in $\{0,1\}^k$ are enumerated lexicographically as $s_1 < s_2 < \dots < s_{2^k}$. For example, when $k = 2$, we obtain $00 < 01 < 10 < 11$. Given each string $s \in \{0,1\}^n$, s^R denotes the *reversal* of s ; that is, $s^R = s_n s_{n-1} \dots s_2 s_1$ if $s = s_1 s_2 \dots s_{n-1} s_n$. We expand this notion to quantum states in the following manner. Given a quantum state $|\phi\rangle \in \mathcal{H}_{2^n}$, the *reversal* of $|\phi\rangle$, denoted by $|\phi^R\rangle$, is of the form $\sum_{s:|s|=n} \langle s|\phi\rangle \otimes |s^R\rangle$, where $\langle s|\phi\rangle$ is merely a scalar. For instance, if $|\phi\rangle = \alpha|01\rangle + \beta|10\rangle$, then $|\phi^R\rangle = \alpha|10\rangle + \beta|01\rangle$.

Lemma 3.6 *Let $k \in \mathbb{N}$ with $k \geq 2$, let $g, h \in \widehat{\square}_1^{\text{QP}}$, and let $\mathcal{G}_k = \{g_s \mid s \in \{0,1\}^k\}$ be a set of $\widehat{\square}_1^{\text{QP}}$ -functions. The following quantum functions all belong to $\widehat{\square}_1^{\text{QP}}$. The lemma also holds even if $\widehat{\square}_1^{\text{QP}}$ is replaced by \square_1^{QP} .*

Let $|\phi\rangle$ be any quantum state in \mathcal{H}_∞ .

1. $\text{Compo}[\mathcal{G}_k](|\phi\rangle) = g_{s_1} \circ g_{s_2} \circ \dots \circ g_{s_{2^k}}(|\phi\rangle)$. (multiple composition)
2. $\text{Switch}_k[g, h](|\phi\rangle) = g(|\phi\rangle)$ if $\ell(|\phi\rangle) < k$ and $\text{Switch}_k[g, h](|\phi\rangle) = h(|\phi\rangle)$ otherwise. (switching)
3. $\text{LENGTH}_k[g](|\phi\rangle) = |\phi\rangle$ if $\ell(|\phi\rangle) < k$ and $\text{LENGTH}_k[g](|\phi\rangle) = g(|\phi\rangle)$ otherwise.
4. $\text{REMOVE}_k(|\phi\rangle) = |\phi\rangle$ if $\ell(|\phi\rangle) < k$ and $\text{REMOVE}_k(|\phi\rangle) = \sum_{s:|s|=k} \langle s|\phi\rangle \otimes |s\rangle$ otherwise.
5. $\text{REP}_k(|\phi\rangle) = |\phi\rangle$ if $\ell(|\phi\rangle) < k$ and $\text{REP}_k(|\phi\rangle) = \sum_{s:|s|=n-k} \langle s|\phi\rangle \otimes |s\rangle$ otherwise.
6. $\text{SWAP}_k(|\phi\rangle) = |\phi\rangle$ if $\ell(|\phi\rangle) < 2k$ and $\text{SWAP}_k(|\phi\rangle) = \sum_{s:|s|=k} \sum_{t:|t|=k} |st\rangle \langle ts|\phi\rangle$ otherwise.
7. $\text{REVERSE}(|\phi\rangle) = |\phi^R\rangle$.
8. $\text{Branch}_k[\mathcal{G}_k](|\phi\rangle) = |\phi\rangle$ if $\ell(|\phi\rangle) < k$ and $\text{Branch}_k[\mathcal{G}_k](|\phi\rangle) = \sum_{s:|s|=k} |s\rangle \otimes g_s(\langle s|\phi\rangle)$ otherwise.
9. $\text{RevBranch}_k[\mathcal{G}_k](|\phi\rangle) = |\phi\rangle$ if $\ell(|\phi\rangle) < k$ and $\text{RevBranch}_k[\mathcal{G}_k](|\phi\rangle) = \sum_{s:|s|=k} g_s \left(\sum_{u:|u|=n-k} \langle us|\phi\rangle \otimes |u\rangle \right) \otimes |s\rangle$ otherwise, where $n = \ell(|\phi\rangle)$.

The difference between REMOVE_k and REP_k is subtle but REMOVE_k moves the first k qubits of an input to the end, whereas REP_k moves the last k qubits to the front. For basic qustrings of length 4, for instance, it holds that $\text{REP}_1(|a_1a_2a_3a_4\rangle) = |a_4a_1a_2a_3\rangle$ and $\text{REMOVE}_1(|a_1a_2a_3a_4\rangle) = |a_2a_3a_4a_1\rangle$. Similarly, $\text{Branch}_k[\mathcal{G}_k]$ applies each g_s in \mathcal{G}_k to the quantum state obtained from $|\phi\rangle$ by eliminating the first k qubits whereas $\text{RevBranch}_k[\mathcal{G}_k]$ applies g_s to the quantum state obtained by eliminating the last k qubits, whenever $k \leq \ell(|\phi\rangle)$. For example, if $\mathcal{G}_k = \{h\}_{s \in \{0,1\}^k}$ for a single quantum function h , then, for every string $s \in \{0,1\}^k$, we obtain $\text{Branch}_k[\mathcal{G}_k](|s\rangle|\phi\rangle) = |s\rangle \otimes h(|\phi\rangle)$ and $\text{RevBranch}_k[\mathcal{G}_k](|\phi\rangle|s\rangle) = h(|\phi\rangle) \otimes |s\rangle$.

Proof of Lemma 3.6. Let $k \in \mathbb{N}^+$, $g \in \widehat{\square_1^{\text{QP}}}$, and $\mathcal{G}_k = \{g_s \mid s \in \{0,1\}^k\} \subseteq \widehat{\square_1^{\text{QP}}}$. For each index $i \in [k]$, let s_i denote lexicographically the i th element of $\{0,1\}^k$.

1) We first set $f_{2^k} = g_{s_{2^k}}$ and inductively define $f_{i-1} = \text{Compo}[g_{s_{i-1}}, f_i]$ for every index $i \in [2, 2^k]_{\mathbb{Z}}$ to obtain $f_1 = \text{Compo}[\mathcal{G}_k]$. The resulted quantum function f_1 clearly belongs to $\widehat{\square_1^{\text{QP}}}$ because k is a fixed constant independent of inputs to f_1 .

2) This is a special case of the single-qubit quantum recursion rule (or the 1-qubit quantum recursion rule) in which $t = k - 1$, $p = I$, and $f_0 = f_1 = I$. Therefore, $\text{Switch}_k[g, h]$ belongs to $\widehat{\square_1^{\text{QP}}}$.

3) Since $\text{LENGTH}_k[g] = \text{Switch}_k[I, g]$, LENGTH_k is in $\widehat{\square_1^{\text{QP}}}$.

4) We begin with the case of $k = 1$. The desired quantum function REMOVE_1 is defined as

$$\text{REMOVE}_1(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ \sum_{a \in \{0,1\}} |a\rangle \otimes \text{REMOVE}_1(\langle a|\psi_{\text{SWAP}, \phi}\rangle) & \text{otherwise,} \end{cases}$$

More formally, we set $\text{REMOVE}_1 = Q\text{Rec}_1[I, I, \text{SWAP}|\text{REMOVE}_1, \text{REMOVE}_1]$. In the case of $k = 2$, we define $\text{REMOVE}_2 = \text{REMOVE}_1 \circ \text{REMOVE}_1$. For each index $k \geq 3$, REMOVE_k is obtained as follows. Let h'_k be the k compositions of REMOVE_1 and define REMOVE_k to be $\text{LENGTH}_k[h'_k]$. We remark that LENGTH_k is necessary in our definition because h'_k is not guaranteed to equal REMOVE_k when $\ell(|\phi\rangle) \leq k - 1$.

5) First, we define REP_1 as $\text{REP}_1 = Q\text{Rec}_1[I, \text{SWAP}, I|\text{REP}_1, \text{REP}_1]$, that is,

$$\text{REP}_1(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ \sum_{a \in \{0,1\}} \text{SWAP}(|a\rangle \otimes \text{REP}_1(\langle a|\phi\rangle)) & \text{otherwise.} \end{cases}$$

Clearly, REP_1 belongs to $\widehat{\square_1^{\text{QP}}}$. For a general index $k > 1$, we define REP_k in the following way. We first set h'_k to be the k compositions of REP_1 . Finally, we set $\text{REP}_k = \text{LENGTH}_k[h'_k]$.

6) We first realize a quantum function $\text{SWAP}_{i,i+j}$, which swaps between the i th and the $(i+j)$ th qubits of any input. This goal is achieved by inductively constructing $\text{SWAP}_{i,i+j}$ in the following way. Initially, we set $\text{SWAP}_{i,i+1} = \text{REP}_{i-1} \circ \text{SWAP} \circ \text{REMOVE}_{i-1}$. For any index $j \in [k-i]$, we define $\text{SWAP}_{i,i+j} = \text{SWAP}_{i+j-1,i+j} \circ \text{SWAP}_{i,i+j-1} \circ \text{SWAP}_{i+j-1,i+j}$. We then set $g = \text{SWAP}_{k,2k} \circ \text{SWAP}_{k-1,2k-1} \circ \dots \circ \text{SWAP}_{2,k+2} \circ \text{SWAP}_{1,k+1}$. At last, it suffices to define SWAP_k to be $\text{LENGTH}_{2k}[g]$.

7) The desired quantum function REVERSE can be defined as $\text{REVERSE} = Q\text{Rec}_1[I, \text{REMOVE}_1, I|\text{REVERSE}, \text{REVERSE}]$, namely,

$$\text{REVERSE}(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ \text{REMOVE}_1(\sum_{a \in \{0,1\}} |a\rangle \otimes \text{REVERSE}(\langle a|\phi\rangle)) & \text{otherwise.} \end{cases}$$

8) Note that, when $k = 2$, $Branch_k[\mathcal{G}_k]$ coincides with $Branch$ and it thus belongs to $\widehat{\square_1^{\text{QP}}}$. Hereafter, we assume that $k \geq 3$. For each string $s \in \{0, 1\}^k$, let $g_s^{(0)} = g_s$. For each index $i \in \mathbb{N}$ with $i < k$ and each string $s \in \{0, 1\}^*$ with $|s| = k - i - 1$, we inductively define $g_s^{(i+1)}$ to be $Branch[g_{s0}^{(i)}, g_{s1}^{(i)}]$, that is,

$$g_s^{(i+1)}(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ |0\rangle \otimes g_{s0}^{(i)}(\langle 0|\phi\rangle) + |1\rangle \otimes g_{s1}^{(i)}(\langle 1|\phi\rangle) & \text{otherwise.} \end{cases}$$

Finally, we set $Branch_k[\mathcal{G}_k] = g_\lambda^{(k)}$, where λ is the empty string.

9) Assuming $k \geq 2$, let $RevBranch_k[\{g_s\}_{s \in \{0,1\}^k}] = REMOVE_k \circ Branch_k[\{g_s\}_{s \in \{0,1\}^k}] \circ REP_k$. \square

The next lemma shows that we can extend any classical bijection on $\{0, 1\}^k$ to its associated $\widehat{\square_1^{\text{QP}}}$ -function, which behaves in exactly the same way as the bijection does on the first k bits of its input.

Lemma 3.7 *Let k be a constant in \mathbb{N}^+ . For any bijection f from $\{0, 1\}^k$ to $\{0, 1\}^k$, there exists a $\widehat{\square_1^{\text{QP}}}$ -function g_f such that, for any quantum state $|\phi\rangle \in \mathcal{H}_\infty$,*

$$g_f(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq k - 1, \\ \sum_{s \in \{0,1\}^k} |f(s)\rangle \langle s|\phi\rangle & \text{otherwise.} \end{cases}$$

Proof. Given a bijection f on $\{0, 1\}^k$, it suffices to show the existence of $\widehat{\square_1^{\text{QP}}}$ -function h satisfying $h(|s\rangle|\phi\rangle) = |f(s)\rangle|\phi\rangle$ for any string $s \in \{0, 1\}^k$ and any quantum state $|\phi\rangle \in \mathcal{H}_\infty$ since g_f is obtained from h simply by setting $g_f = LENGTH_k[h]$. Notice that, if $h \in \widehat{\square_1^{\text{QP}}}$, $h(\mathbf{0}) = \mathbf{0}$ makes $g_f(\mathbf{0})$ equal $\mathbf{0}$.

A bijection on $\{0, 1\}^k$ is, in essence, a *permutation* on $\{s_1, s_2, \dots, s_{2^k}\}$, where each s_i is lexicographically the i th string in $\{0, 1\}^k$, and thus it can be expressed as the multiplication of a finite number of *transpositions*, each of which swaps between two distinct numbers. This can be done by an application of the multiple composition of the corresponding $SWAP_{i,i+j}$, which is defined in the proof of Lemma 3.6(6). Therefore, h belongs to $\widehat{\square_1^{\text{QP}}}$. \square

Given a quantum state $|\phi\rangle$, it is possible to apply simultaneously a quantum function f to the first k qubits of $|\phi\rangle$ and another quantum function g to the rest.

Lemma 3.8 *Given $f, g \in \widehat{\square_1^{\text{QP}}}$ and $k \in \mathbb{N}^+$, the quantum function $f^{\leq k} \otimes g$, which is defined by*

$$(f^{\leq k} \otimes g)(|\phi\rangle) = \begin{cases} f(|\phi\rangle) & \text{if } \ell(|\phi\rangle) \leq k, \\ \sum_{s \in \{0,1\}^k} f(|s\rangle) \otimes g(\langle s|\phi\rangle) & \text{otherwise,} \end{cases}$$

belongs to $\widehat{\square_1^{\text{QP}}}$. We write this g as $Skip[f]$.

Proof. Given a quantum function f , we restrict the application of f to the last k qubits of any input $|\phi\rangle$ by setting $f' = QRec_k[f, I, I|f_0, f_1]$, where f_0 and f_1 are f' . It follows that $f'(|\phi\rangle|s\rangle) = |\phi\rangle \otimes f(|s\rangle)$ for any $|\phi\rangle \in \mathcal{H}_\infty$ and $s \in \{0, 1\}^k$.

Let $h = REP_k \circ f' \circ REMOVE_k$. This quantum function h satisfies that $h(|s\rangle|\phi\rangle) = f(|s\rangle) \otimes |\phi\rangle$ for any $s \in \{0, 1\}^k$. We then define $\mathcal{G}_k = \{g_s\}_{s \in \{0,1\}^k}$ with $g_s = g$ for every string $s \in \{0, 1\}^k$ and set $g' = h \circ Branch_k[\mathcal{G}_k]$. It then follows that the desired quantum function $f^{\leq k} \otimes g$ equals $Switch_{k+1}[f, g']$. \square

Next, we present Lemma 3.9, which is useful for the proof of our key lemma (Lemma 4.3) in Section 5. The lemma allows us to skip, before applying a given quantum function, an arbitrary number of 0s until we read a fixed number of 1s.

Lemma 3.9 *Let f be a quantum function in $\widehat{\square_1^{\text{QP}}}$ and let k be a constant in \mathbb{N}^+ . There exists a quantum function g in $\widehat{\square_1^{\text{QP}}}$ such that $g(|0^m 1^k\rangle \otimes |\phi\rangle) = |0^m 1^k\rangle \otimes f(|\phi\rangle)$ and $g(|0^{m+1}\rangle) = |0^{m+1}\rangle$ for any number $m \in \mathbb{N}$ and any quantum state $|\phi\rangle \in \mathcal{H}_\infty$. The lemma also holds when $\widehat{\square_1^{\text{QP}}}$ is replaced by \square_1^{QP} .*

Proof. Let $k \geq 2$. Given a quantum function $f \in \widehat{\square_1^{\text{QP}}}$, we first expand f to f' so that $f'(|1^{k-1}\rangle|\phi\rangle) = |1^{k-1}\rangle \otimes f(|\phi\rangle)$ for any $|\phi\rangle \in \mathcal{H}_\infty$ and $f'(|0^{m+1}\rangle) = |0^{m+1}\rangle$ for any $m \in \mathbb{N}$. This quantum function f' can be obtained inductively as follows. We set $f_{k-1} = Branch[I, f]$, $f_i = Branch[I, f_{i+1}]$ for each $i \in [k-2]$, and

finally define f' to be f_1 . When $k = 1$, we simply set $f' = f$. The desired quantum function g in the lemma must satisfy

$$g(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ |0\rangle \otimes f'(g(\langle 0|\phi\rangle)) + |1\rangle\langle 1|\phi & \text{otherwise.} \end{cases}$$

This g is formally defined as $g = QRec_1[I, Branch[f', I], I|g, I]$. This completes the proof. \square

Within our framework, it is possible to construct a “restricted” form of the *quantum Fourier transform* (QFT). Given a binary string $s = s_1s_2 \cdots s_k$ of length k with $s_i \in \{0, 1\}$, we denote by $num(s)$ the integer of the form $\sum_{i=1}^k s_i 2^{k-i}$. For instance, $num(011) = 1 \cdot 2^1 + 1 \cdot 2^0 = 5$ and $num(1010) = 1 \cdot 2^3 + 1 \cdot 2^1 = 10$. Moreover, let $\omega_k = e^{2\pi i/2^k}$, where $i = \sqrt{-1}$.

Lemma 3.10 *Let k be any fixed constant in \mathbb{N}^+ . The following k -qubit quantum Fourier transform belongs to $\widehat{\square}_1^{\text{QP}}$. For any element $|\phi\rangle$ in \mathcal{H}_∞ , let*

$$F_k(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) < k, \\ \frac{1}{2^{k/2}} \sum_{t:|t|=k} \sum_{s:|s|=k} \omega_k^{num(s)num(t)} |s\rangle\langle t|\phi & \text{otherwise.} \end{cases}$$

Proof. When $k = 1$, F_1 coincides with WH and therefore F_1 belongs to $\widehat{\square}_1^{\text{QP}}$ by Lemma 3.3. Next, assume that $k \geq 2$. It is known that, for any $x_1, x_2, \dots, x_k \in \{0, 1\}$,

$$F_k(|x_1x_2 \cdots x_k\rangle) = \frac{1}{2^{k/2}} (|0\rangle + \omega_1^{x_k}|1\rangle)(|0\rangle + \omega_1^{x_{k-1}}\omega_2^{x_k}|1\rangle) \cdots (|0\rangle + \prod_{i=1}^k \omega_i^{x_i}|1\rangle). \quad (1)$$

For this fact and its proof, refer to, e.g., [25].

Let us recall the special quantum function $SWAP_{i,i+j}$ from the proof of Lemma 3.6(6), which swaps between the i th and the j th qubits. Using $CPHASE_\theta$, for any index pair i, j with $i < j$, we define $CPHASE_\theta^{(i,j)}$ to be $SWAP_{1,i} \circ SWAP_{2,j} \circ CPHASE_\theta \circ SWAP_{2,j} \circ SWAP_{1,i}$, in which we apply $CPHASE_\theta$ to the i th and the j th qubits. We first want to construct $G_k^{(1)} = F_k \circ REVERSE$, which works similarly to F_k but takes $|\phi^R\rangle$ as an input instead. To achieve this goal, we define $\{G_j^{(i)}\}_{i,j \in \mathbb{N}^+}$ inductively as follows. Initially, we set $G_0^{(i)} = I$ for any $i \in \mathbb{N}^+$. Next, we define $G_1^{(i)}$ as $G_1^{(i)} = H$ if $i = 1$, and $G_1^{(i)} = REP_{i-1} \circ H \circ REMOVE_{i-1}$ otherwise. For any index $k \geq 2$, $G_k^{(i)}$ is defined to be $G_{k-1}^{(i)} \circ CPHASE_{\frac{\pi}{2^{k-1}}}^{(i,i+k-1)} \circ (G_{k-2}^{(i)})^{-1} \circ G_{k-1}^{(i+1)}$. It is not difficult to show that $G_k^{(1)}$ coincides with $F_k \circ REVERSE$ by Eqn. (1).

Since $G_k^{(1)} = F_k \circ REVERSE$, it suffices to define F_k as $G_k^{(1)} \circ REVERSE$. \square

A general form of QFT, in which k is not limited to a particular constant, will be discussed in Section 6.1 in connection to our choice of Schemata I–IV that form the function class $\widehat{\square}_1^{\text{QP}}$.

4 Main Contributions

In Section 3.1, we have introduced the \square_1^{QP} -functions and the $\widehat{\square}_1^{\text{QP}}$ -functions mapping \mathcal{H}_∞ to \mathcal{H}_∞ by applying Schemata I–IV for finitely many times. Our main theorem (Theorem 4.1) asserts that \square_1^{QP} can precisely characterize all functions in FBQP mapping $\{0, 1\}^*$ to $\{0, 1\}^*$, and therefore characterize all languages in BQP over $\{0, 1\}$ by identifying languages with their corresponding characteristic functions. This theorem will be proven by using two key lemmas, Lemmas 4.2–4.3.

4.1 A New Characterization of FBQP

Our goal is to demonstrate the power of \square_1^{QP} -functions (and thus $\widehat{\square}_1^{\text{QP}}$ -functions) by showing in Theorem 4.1 that \square_1^{QP} -functions (as well as $\widehat{\square}_1^{\text{QP}}$ -functions) precisely characterize FBQP-functions on $\{0, 1\}^*$. For this purpose, there are unfortunately two major difficulties to overcome.

The first difficulty arises in dealing with tape symbols of QTMs by qubits alone. Notice that QTMs working over non-binary input alphabets are known to be simulated by QTMs taking the binary input alphabet $\{0, 1\}$. Even if we successfully reduce the size of input alphabets down to 2, in fact, the simulation of such QTMs must require the proper handling of *non-binary tape symbols*, in particular, the distinguished