blank symbol. For our later convenience, we use "b" to denote the blank symbol, instead of #. In a similar vein, suppose that the outcome of a $\Box_1^{\mathrm{QP}}$-function f is composed of an important, meaningful portion and the other "garbage" portion, which is a remnant of the computation process. Since we use only qubits ($|0\rangle$ and $|1\rangle$) to express inputs and outputs, how can we distinguish between the meaningful portion and the garbage portion? In order to simulate QTMs by $\Box_1^{\mathrm{QP}}$-functions, we therefore need to "encode" all tape symbols into qubits.

This paper introduces the following simple coding scheme. We set $\hat{0} = 00$, $\hat{1} = 01$, and $\hat{b} = 10$. We also set $\hat{2} = 11$ and $\hat{3} = 10$ for a later use. The input alphabet $\Sigma = \{0, 1\}$ is thus translated into $\{\hat{0}, \hat{1}\}$ and the tape alphabet $\Gamma = \Sigma \cup \{b\}$ is encoded into $\{\hat{0}, \hat{1}, \hat{b}\}$. Given each binary string $s = s_1 s_2 \cdots s_n$ with $s_i \in \{0, 1\}$ for every index $i \in [n]$, a *code* $\tilde{s}$ of s indicates the string $\hat{s}_1 \hat{s}_2 \cdots \hat{s}_n \hat{2}$, where the last item $\hat{2}$ serves as an endmarker, which marks the end of the code. It then follows that $|\tilde{s}| = 2|s| + 2$. As quick examples, we obtain $\widetilde{0110} = \hat{0}\hat{1}\hat{1}\hat{0}\hat{2} = 0001010011$ and $\widetilde{01} \cdot \widetilde{11} = \hat{0}\hat{1}\hat{2}\hat{1}\hat{1}\hat{2} = 000111010111$. Later, we will show in lemma 5.1 that the encoding of strings and the decoding of encoded strings can be carried out by suitable $\widehat{\Box_1^{\mathrm{QP}}}$-functions.

Another difficulty comes from the inability of $\widehat{\Box_1^{\mathrm{QP}}}$-functions to expand their qubits. Notice that a QTM is designed to freely use additional storage space by moving its tape head simply to new, blank tape cells beyond its *input area*, in which an input is initially written. To simulate such a QTM, we need to simulate its entire activities made in the freely expanding tape space as well. On the contrary, every $\widehat{\Box_1^{\mathrm{QP}}}$-function is dimension-preserving by Lemma 3.4(4), and thus the number of input qubits must match that of output qubits. If we want to simulate extra storage space of the QTM, then we need to feed the same amount of extra qubits to the target $\widehat{\Box_1^{\mathrm{QP}}}$-function for use at the very beginning.

We resolve this second issue by extending each input of quantum functions by adding extra 0s whose length is associated with the running time of the QTM. For any polynomial p and any quantum function g on $\mathcal{H}_\infty$, we define $|\phi^p(x)\rangle = |0^{|x|}1\rangle|0^{p(|x|)}10^{11p(|x|)+6}1\rangle|x\rangle$ and $|\phi_g^p(x)\rangle = g(|\phi^p(x)\rangle)$ for every string $x \in \{0, 1\}^*$. Similarly, for any function f on $\{0, 1\}^*$, we set $|\phi^{p,f}(x)\rangle = |\widetilde{0^{|f(x)|}}\rangle|0^{|f(x)|+1}1\rangle|\phi^p(x)\rangle$ and $|\phi_g^{p,f}(x)\rangle = g(|\phi^{p,f}(x)\rangle)$.

Any FBQP-function takes classical input strings and produces classical strings that are outcomes of a polynomial-time quantum Turing machine with high probability. In contrast, our $\Box_1^{\mathrm{QP}}$-functions f are to transform each quantum state in $\mathcal{H}_\infty$ to another one in $\mathcal{H}_\infty$. To obtain classical output strings, we need to observe the outcomes of f.

The main theorem (Theorem 4.1) roughly asserts the following: for any FBQP-function f, there always exists a $\widehat{\Box_1^{\mathrm{QP}}}$-function g such that, when we observe the first $|f(x)|$ qubits of the outcome $g(|\phi^p(x)\rangle)$ ($= |\phi_g^p(x)\rangle$) of g on input $|\phi^p(x)\rangle$, we correctly obtain $f(x)$ with high probability. Notice that $g(|\phi^p(x)\rangle)$ also contains extra qubits, called "garbage" qubits, which are left unobserved in the process of calculating $f(x)$. Those garbage qubits are actually the remnant of the computation process of f. It is, however, possible to remove those qubits by partly reversing the whole computation, if we know the output size $|f(x)|$ ahead of the computation (by expanding $|\phi^p(x)\rangle$ to $|\phi^{p,f}(x)\rangle$ and $|\phi_g^p(x)\rangle$ to $|\phi_g^{p,f}(x)\rangle$).

Theorem 4.1 (Main Theorem) *Let f be a polynomially-bounded function on $\{0, 1\}^*$. The following three statements are logically equivalent.*

1. *The function f is in* FBQP.
2. *For any constant $\varepsilon \in [0, 1/2)$, there exist a quantum function g in $\widehat{\Box_1^{\mathrm{QP}}}$ and a polynomial p such that $|f(x)| \leq p(|x|)$ and $\|\langle f(x)|\phi_g^p(x)\rangle\|^2 \geq 1 - \varepsilon$ for all $x \in \{0, 1\}^*$.*
3. *For any constant $\varepsilon \in [0, 1/2)$, there exist a quantum function g in $\widehat{\Box_1^{\mathrm{QP}}}$ and a polynomial p such that $|f(x)| \leq p(|x|)$ and $|\langle \Psi_{f(x)}|\phi_g^{p,f}(x)\rangle|^2 \geq 1 - \varepsilon$ for all $x \in \{0, 1\}^*$, where $|\Psi_{f(x)}\rangle = |f(x)\rangle|(0^{|f(x)|+1}1)^2\rangle|\phi^p(x)\rangle$.*

In Statements 2–3 of Theorem 4.1, $\langle f(x)|\phi_g^p(x)\rangle$ is a non-null vector whereas $\langle \Psi_{f(x)}|\phi_g^{p,f}(x)\rangle$ is just a scalar because $\ell(|f(x)\rangle|\phi^p(x)\rangle) = \ell(|\phi_g^{p,f}(x)\rangle)$.

Hereafter, we wish to prove the main theorem, Theorem 4.1. For a strategic reason, we split the theorem into two technical lemmas, Lemmas 4.2 and 4.3. To present the lemmas, we need to introduce additional terminology for QTMs. It is easier in practice to design multi-tape well-formed QTMs rather than single-tape ones. However, since multi-tape QTMs can be simulated by single-tape QTMs by translating multiple tapes to multiple tracks of a single tape, toward the proof of Theorem 4.1, it suffices to focus our attention only on single-tape QTMs.

A single-tape QTM is said to be in *normal form* if $\delta(q_f, \sigma) = |q_0\rangle|\sigma\rangle|R\rangle$ holds for any tape symbol

$\sigma \in \Gamma$. If a QTM halts in a superposition of final configurations in which a tape head returns to the start cell, then we call such a machine *stationary*. Refer to [5] for their basic properties. For convenience, we further call a QTM *conservative* if it is well-formed, stationary, and in normal form. Moreover, a well-formed QTM is said to be *plain* if its transition function satisfies the following specific requirement: for every pair $(p, \sigma) \in Q \times \Gamma$, $\delta(p, \sigma)$ has the form either $\delta(p, \sigma) = e^{i\theta}|q, \tau, d\rangle$ or $\delta(p, \sigma) = \cos\theta|q, \tau, d\rangle + \sin\theta|q', \tau,', d'\rangle$ for certain $\theta \in [0, 2\pi)$ and two distinct tuples (q, τ, d) and (q', τ', d'). Bernstein and Vazirani [5] claimed that any single-tape, polynomial-time, conservative QTM M can be simulated by an appropriate single-tape, polynomial-time, conservative, plain QTM M'. Additionally, when M is of $\tilde{\mathbb{C}}$-amplitudes, so is M'.

Let us recall that any output string of a QTM begins at the start cell and stretches to the right until the first blank symbol although there may be tape symbols left unerased in other parts of the tape. For our later convenience, a QTM M is said to have *clean outputs* if, when M halts, no non-blank symbol appears in the left-side region of the output string, i.e., the region consisting of all cells indexed by negative integers. Take a polynomial p that bounds the running time of M on every input. Since M halts in at most $p(|x|)$ steps on every instance $x \in \{0,1\}^*$, it suffices for us to pay attention only to its *essential tape region* that covers all tape cells indexed by numbers between $-p(|x|)$ and $+p(|x|)$. In practice, we redefine a configuration γ of M on input x of length n as a triplet $(q, h, \sigma_1 \cdots \sigma_{2p(n)+1})$, where $p \in Q$, $h \in \mathbb{Z}$ with $-p(n) \leq h \leq p(n)$, and $\sigma_1, \cdots, \sigma_{2p(n)+1} \in \{0, 1, b\}$ such that, for every index $i \in [2p(n)+1]$, σ_i is a tape symbol written at the cell indexed by $i - p(n) - 1$. Note that the start cell comes in the middle of $\sigma_1 \cdots \sigma_{2p(n)+1}$. For notational convenience, we further modify the notion of configuration by splitting the essential tape region into two parts (z_1, z_2), in which $z_1 = \sigma_1\sigma_2 \cdots \sigma_{p(n)}$ refers to the left-side region of the start cell, not including the start cell, and $z_2 = \sigma_{p(n)+1}\sigma_{p(n)+2} \cdots \sigma_{2p(n)+1}$ refers to the rest of the essential tape region. This provides us with a modified configuration of the form $(q, h, z_1 z_2)$. For a practical reason, we further alter it into (z_2, z_1, h, q), which we call by a *skew configuration*. Associated with this alteration of configurations, we also modify the original time-evolution operator, U_δ, of M so that it works on skew configurations. Be aware that this new operator cannot be realized by the standard QTM model. To distinguish it from the original time-evaluation operator U_δ of M, we call it the *skew time-evolution operator* and write it as $\widehat{U}_\delta$.

Lemma 4.2 *Let f be any quantum function in $\Box_1^{\mathrm{QP}}$. There exist a polynomial p and a single-tape, conservative, plain QTM M producing clean outputs with $\tilde{\mathbb{C}}$-amplitudes such that, for any quantum state $|\phi\rangle$ in $\mathcal{H}_{2^n}$, M starts with a non-null quantum state $|\phi\rangle$ given on its input/work tape and, when it halts after $p(n)$ steps, the superposition $|\eta_{M,\phi}\rangle$ of skew final configurations of M on $|\phi\rangle$ is of the form $f(|\phi\rangle) \otimes |0, q_f\rangle$, where $f(|\phi\rangle)$ appears as the content of the tape from the start cell to the right until the first blank symbol and q_f is a unique final inner state of M.*

Proof. We first show that all the initial functions in Scheme I can be exactly computed in polynomial time on appropriate single-tape, $\tilde{\mathbb{C}}$-amplitude, conservative, plain QTMs having clean outputs over input/output alphabet $\{0,1\}$. For clarity, our goal here is to demonstrate that, for every quantum function f in Scheme I, there exists a QTM with the lemma's properties such that a superposition $|\eta_{M,\phi}\rangle$ of M's skew final configurations is of the form $f(|\phi\rangle) \otimes |0, q_f\rangle$, where $f(|\phi\rangle)$ is the content of M's tape from the start cell to the right until the first blank symbol.

Since I (identity) is easy to simulate, let us consider $PHASE_\theta$. In this case, we take a QTM that applies a transition of the form $\delta(q_0, \sigma) = e^{i\theta\sigma}|q_f, \sigma, N\rangle$ for any bit $\sigma \in \{0,1\}$. Clearly, if we start with a skew initial configuration $|\phi\rangle|0\rangle|q_0\rangle$, then we halt with $PHASE_\theta(|\phi\rangle) \otimes |0\rangle|q_f\rangle$; in short, this QTM "exactly computes" $PHASE_\theta$. For ROT_θ, we use the transition defined by $\delta(q_0, \sigma) = \cos\theta|q_f, \sigma, N\rangle + (-1)^\sigma \sin\theta|q_f, \bar{\sigma}, N\rangle$ to exactly compute ROT_θ. To simulate NOT, we then define a QTM to have a transition of $\delta(q_0, \sigma) = |q_f, \overline{\sigma}, N\rangle$. In the case of $SWAP$, it suffices to prepare inner states p_{σ_1} and r_{σ_2} as well as the following transitions: $\delta(q_0, \sigma_1) = |p_{\sigma_1}, \#, R\rangle$, $\delta(p_{\sigma_1}, \sigma_2) = |r_{\sigma_2}, \sigma_1, L\rangle$, $\delta(r_{\sigma_2}, \#) = |q_f, \sigma_2, N\rangle$ for bits $\sigma_1, \sigma_2 \in \{0,1\}$. Concerning $MEAS[a](|\phi\rangle)$, we start with checking the first qubit of $|\phi\rangle$. If it is not a, then we make a QTM *reject* the input; otherwise, we do nothing. More formally, we define $\delta(q_0, \overline{a}) = |q_{rej}, \overline{a}, N\rangle$ and $\delta(q_0, a) = |q_f, a, N\rangle$. It is not difficult to see that $|\eta_{M,\phi}\rangle$ has the form $f(|\phi\rangle) \otimes |0, q_0\rangle$.

Next, we intend to simulate each of the construction rules on an appropriate QTM. By induction hypothesis, there exist three polynomial-time, single-tape, $\tilde{\mathbb{C}}$-amplitude, conservative, plain QTMs M_g, M_h, and M_p that satisfy the lemma for g, h, and p, respectively. By installing an *internal clock* in an appropriate way with a certain polynomial r, we can make M_g, M_h, and M_p halt in exactly $r(n)$ time on any input of length $n \in \mathbb{N}$. In what follows, let $|\phi\rangle$ denote any input in $\mathcal{H}_\infty$.

[composition] Consider the case of $f = Compo[g, h]$. We compute f as follows. We first run M_h on $|\phi\rangle$ and obtain a superposition of skew final configurations, say, $h(|\phi\rangle) \otimes |0, q'_f\rangle$ for a unique final inner state q'_f of M_h. Since M_h is stationary and in normal form, we can further run M_g on the resulted quantum state

$h(|\phi\rangle)$, treating q'_f as its new initial inner state and generating $|\eta_{M,\phi}\rangle = g(h(|\phi\rangle)) \otimes |0, q_f\rangle$ for a unique final inner state q_f of M_g.

[branching] Assume that $f = Branch[g, h]$. We check the first qubit of $|\phi\rangle$. If it is 0, then we run M_g on $\langle 0|\phi\rangle$; otherwise, we run M_h on $\langle 1|\phi\rangle$. This produces $|0\rangle \otimes g(\langle 0|\phi\rangle) \otimes |0, q_{h,f}\rangle + |1\rangle \otimes h(\langle 1|\phi\rangle) \otimes |0, q_{g,f}\rangle$, where $q_{g,f}$ and $q_{h,f}$ are respectively unique final inner states of M_g and M_h. Notice that we do not need to check whether $\ell(|\phi\rangle) \geq 2$. Formally, we add the following transitions to those of M_g and M_h: $\delta(q_0, 0) = |q_0, \#_g, R\rangle$ and $\delta(q_0, 1) = |q_0, \#_h, R\rangle$, where $\#_g$ and $\#_h$ are designated symbols marking the left of the new "start cells" for M_g and M_h, respectively. At terminating, the tape head moves back to the start cell. We then replace $\#_g$ and $\#_h$ respectively with 0 and 1 by entering a new final inner state q_f; namely, $\delta(q_{g,f}, \#_g) = |q_f, 0, N\rangle$ and $\delta(q_{h,f}, \#_h) = |q_f, 1, N\rangle$. This transition is unitarily possible.

[multi-qubit quantum recursion] Finally, let us demonstrate a simulation of the multi-qubit quantum recursion introduced by $f = kQRec_t[g, h, p|\mathcal{F}_k]$ with $\mathcal{F}_k = \{f_s\}_{s\in\{0,1\}^k}$. For readability, let us consider only the simplest case where $k = 1$, $f_0 = f$, and $f_1 = I$. The other cases can be similarly treated. Consider the "multi-tape" QTM M_f that roughly behaves as described below. Let T be a sufficiently large positive constant.

(1) In this initial phase, starting with input $|\phi\rangle$, we prepare a counter in a new work tape and an internal clock in another work tape. We use the clock to adjust the terminating timing of all computation paths. Count the number $\ell(|\phi\rangle)$ of qubits simply by incrementing the counter as moving the input tape head from the start cell to the right. Initially, we set the current quantum state, say, $|\xi\rangle$ expressed on the tape to be $|\phi\rangle$ and set the current counter k to be $\ell(|\xi\rangle)$ $(= n)$. Go to the splitting phase.

(2) In this splitting phase, we inductively perform the following procedure using the clock. (*) Assume that the input tape currently contains a quantum state $|\xi\rangle$ and the counter has $k = \ell(|\xi\rangle)$. If $k \leq t$, then idle until the clock hits T and then go to the processing phase. Otherwise, run M_p on $|\xi\rangle$ to generate $|\psi_{p,\xi}\rangle$ and observe the first qubit of $|\psi_{p,\xi}\rangle$ in the computational basis, obtaining $\langle b|\psi_{p,\xi}\rangle$ for each $b \in \{0, 1\}$. If b is 1, then run M_h on $|1\rangle\langle 1|\psi_{p,\xi}\rangle$, obtain $h(|1\rangle\langle 1|\psi_{p,\xi}\rangle)$, which is viewed as $f(|1\rangle\langle 1|\xi\rangle)$, idle until the clock hits T, and then start the processing phase. On the contrary, when b is 0, move this bit 0 to a separate tape to remember and then update both $|\xi\rangle$ and k to be $\langle 0|\psi_{p,\xi}\rangle$ and $k - 1$, respectively. Continue (*).

(3) In this processing phase, we start with a quantum state $|\xi\rangle$, which is produced in the splitting phase. Let $k = \ell(|\xi\rangle)$. We inductively perform the following procedure. (**) If $k \leq t$, then we run M_g on the input $|\xi\rangle$ and produce $g(|\xi\rangle)$, which is viewed as $f(|\xi\rangle)$. Update $|\xi\rangle$ to be the resulted quantum state. Otherwise, we move back the last stored bit 0 from the separate tape, run M_h on $|0\rangle|\xi\rangle$, obtain $h(|0\rangle|\xi\rangle)$, and then update $|\xi\rangle$ to be the obtained quantum state and k to be $k + 1$ since $\ell(|0\rangle|\xi\rangle) = k + 1$. If all b's are consumed (equivalently, $k = n$), then idle until the clock hits $2T$, output $|\xi\rangle$, and halt. Otherwise, continue (**).

The running time of the above QTM is bounded from above by a certain polynomial in the length $\ell(|\phi\rangle)$ because each of the procedures (*) and (**) is repeated for at most $\ell(|\phi\rangle)$ times. Although M_f stores bits on the separate tape, those bits are all moved back and used up by the end of the computation. This fact shows that a superposition of M_f's skew final configurations is of the form $f(|\phi\rangle) \otimes |0, q_f\rangle$ for a unique final inner state q_f. Finally, we convert this multi-tape QTM into a computationally equivalent single-tape QTM of the desired properties in the lemma.

This completes the proof of Lemma 4.2. □

For notational sake, we write $M[r]$ for an output string written in a skew final configuration r, which covers only an essential tape region of M. We write $FSC_{M,n}$ to denote the set of all possible skew final configurations of M produced for any input of length n.

The key to the proof of Theorem 4.1 is the following lemma, which ensures the existence of a $\widehat{\Box_1^{\mathrm{QP}}}$-function g whose outcome $g(|\phi^p(|\psi\rangle)\rangle)$ $(= |\phi_g^p(|\psi\rangle)\rangle)$ "almost" characterize the encoded skew final configuration $\sum_{x:|x|=n}\sum_{r\in FSC_{M,n}}\langle x|\psi\rangle|\widetilde{M[r]}\rangle|\xi_{x,r}\rangle$ of M, where $\widetilde{M[r]}$ is the encoding of $M[r]$. Here, the encoding $\widetilde{M[r]}$ is needed for the construction of g in the proof of the lemma. However, as shown also in the proof, executing an extra decoding procedure for $\widetilde{M[r]}$ allows us to replace $\widetilde{M[r]}$ by $M[r]$.

Lemma 4.3 (Key Lemma) *Let M be a single-tape, polynomial-time, $\tilde{\mathbb{C}}$-amplitude, conservative, plain QTM having clean outputs over input/output alphabet $\Sigma = \{0, 1\}$ and tape alphabet $\Gamma = \{0, 1, b\}$. Assume that, when M halts on input $|\psi\rangle$ of length n, a superposition of coded skew final configurations is of the*

form $\sum_{x:|x|=n}\sum_{r\in FSC_{M,n}}\langle x|\psi\rangle|\widetilde{M[r]}\rangle|\xi_{x,r}\rangle$*, where* $|\xi_{x,r}\rangle$ *denotes an appropriate quantum state describing the rest of the coded skew final configurations other than* $\widetilde{M[r]}$*. There exist a quantum function* g *in* $\widehat{\Box_1^{\mathrm{QP}}}$ *and a polynomial* p *such that, for any number* $n\in\mathbb{N}^+$ *and every quantum state* $|\psi\rangle\in\mathcal{H}_{2^n}$*,* $|\phi_g^p(|\psi\rangle)\rangle$ *has the form* $\sum_{x:|x|=n}\sum_{r\in FSC_{M,n}}\langle x|\psi\rangle|\widehat{M[r]}\rangle|\widehat{\xi}_{x,r}\rangle$ *for certain quantum states* $\{|\widehat{\xi}_{x,r}\rangle\}_{x,r}$ *satisfying that, for any* $x,x'\in\{0,1\}^n$ *and* $r,r'\in FSC_{M,n}$*, (i)* $\|\langle\xi_{x,r}|\xi_{x',r'}\rangle\|=\|\langle\widehat{\xi}_{x,r}|\widehat{\xi}_{x',r'}\rangle\|$ *and (ii)* $\langle\widehat{\xi}_{x,r}|\widehat{\xi}_{x,r'}\rangle=0$ *if* $r\neq r'$*. Furthermore, it is possible to modify* g *to* g'*, which satisfies* $|\phi_{g'}^p(|\phi\rangle)\rangle=\sum_{x:|x|=n}\sum_{r\in FSC_{M,n}}\langle x|\psi\rangle|M[r]\rangle|\widehat{\xi}'_{x,r}\rangle$ *for appropriate quantum states* $\{|\widehat{\xi}'_{x',r'}\rangle\}_{x',r'}$ *satisfying Conditions (i)–(ii).*

The proof of Lemma 4.3 is lengthy and it is postponed until Section 5. Meanwhile, we return to Theorem 4.1 and present its proof using Lemmas 4.2 and 4.3.

Proof of Theorem 4.1. Let $\varepsilon\in[0,1/2)$ be any constant and let f be any polynomially-bounded function mapping $\{0,1\}^*$ to $\{0,1\}^*$.

$(1\Rightarrow 2)$ Assume that f is in FBQP. Take a multi-tape, polynomial-time, $\tilde{\mathbb{C}}$-amplitude, well-formed QTM N that computes f with bounded-error probability. Let us choose a polynomial p that bounds the running time of N on every input. It is possible to "simulate" N with high success probability by a ceratin single-tape, $\tilde{\mathbb{C}}$-amplitude, conservative, plain QTM, say, M having clean outputs in such a way that the machine takes input x and terminates with generating $f(x)bw$ in the right-side region of the start cell of the input/work tape with bounded-error probability, where b is a unique blank tape symbol. Since any bounded-error QTM freely amplifies its success probability, we assume without loss of generality that the error probability of M is at most ε. Notice that the coded skew final configuration begins with an output string. Thus, the superposition of coded skew final configurations of M on input x of length n must be of the form $\sum_{r\in FSC_{M,n}}|\widetilde{M[r]}\rangle|\xi_{x,r}\rangle$ for appropriately chosen quantum states $\{|\xi_{x,r}\rangle\}_{r\in FSC_{M,n}}$. Since M computes f with error probability at most ε, we conclude that $\sum_{r\in FSC_{M,n}}\|\langle\widetilde{f(x)}|\widetilde{M[r]}\rangle|\xi_{x,r}\rangle\|^2\geq 1-\varepsilon$ for all x. Lemma 4.3 further provides us with a special quantum function $g\in\widehat{\Box_1^{\mathrm{QP}}}$ such that, for any number $n\in\mathbb{N}$ and any string $x\in\{0,1\}^n$, $|\phi_g^p(x)\rangle$ has the form $\sum_{r\in FSC_{M,n}}|M[r]\rangle|\widehat{\xi}_{x,r}\rangle$ for certain quantum states $\{|\widehat{\xi}_{x,r}\rangle\}_{r\in FSC_{M,n}}$ satisfying that, for all $r,r'\in FSC_{M,n}$, $\|\langle\xi_{x,r}|\xi_{x,r'}\rangle\|=\|\langle\widehat{\xi}_{x,r}|\widehat{\xi}_{x,r'}\rangle\|$ and $\langle\widehat{\xi}_{x,r}|\widehat{\xi}_{x,r'}\rangle=0$ if $r\neq r'$. We thus conclude that $\|\langle f(x)|\phi_g^p(x)\rangle\|^2=\sum_{r\in FSC_{M,n}}\|\langle f(x)|M[r]\rangle|\widehat{\xi}_{x,r}\rangle\|^2=\sum_{r\in FSC_{M,n}}|\langle\widetilde{f(x)}|\widetilde{M[r]}\rangle|^2\||\widehat{\xi}_{x,r}\rangle\|^2$ since and $\langle f(x)|M[r]\rangle=\langle\widetilde{f(x)}|\widetilde{M[r]}\rangle$ and $\langle\widehat{\xi}_{x,r}|\widehat{\xi}_{x,r'}\rangle=0$ if $r\neq r'$. Moreover, from $\||\xi_{x,r}\rangle\|=\||\widehat{\xi}_{x,r}\rangle\|$, it follows that the term $|\langle\widetilde{f(x)}|\widetilde{M[r]}\rangle|^2\||\widehat{\xi}_{x,r}\rangle\|^2$ equals $\|\langle\widetilde{f(x)}|\widetilde{M[r]}\rangle|\xi_{x,r}\rangle\|^2$. Therefore, $\|\langle f(x)|\phi_g^p(x)\rangle\|^2$ is at least $1-\varepsilon$.

$(2\Rightarrow 3)$ Let ε be any constant in $[0,1/2)$ and set $\varepsilon'=1-\sqrt{1-\varepsilon}$. Let us choose a polynomial p and a function $g\in\widehat{\Box_1^{\mathrm{QP}}}$ for which $|f(x)|\leq p(|x|)$ and $\|\langle f(x)|\phi_g^p(x)\rangle\|^2\geq 1-\varepsilon'$ for all strings $x\in\{0,1\}^*$. Starting with an input $|\phi^{p,f}(x)\rangle$ $(=|\widetilde{0^{|f(x)|}}\rangle|0^{|f(x)|+1}1\rangle|\phi^p(x)\rangle)$, we first apply g to the last part $|\phi^p(x)\rangle$ of $|\phi^{p,f}(x)\rangle$ and obtain $|\widetilde{0^{|f(x)|}}\rangle|0^{|f(x)|+1}1\rangle|\phi_g^p(x)\rangle$. Next, we apply Lemma 5.1 to encode the first $|f(x)|$ qubits of $|\phi_g^p(x)\rangle$ with the help of $|0^{|f(x)|+1}1\rangle$ and then obtain $|\eta_{f,x}\rangle=\sum_{s:|s|=|f(x)|}|\widetilde{0^{|f(x)|}}\rangle|\tilde{s}\rangle\otimes\langle s|\phi_g^p(x)\rangle$. Using the quantum function $COPY_2$ given in Lemma 5.2, we then copy each qustring $|\tilde{s}\rangle$ of $|\eta_{f,x}\rangle$ onto $|\widetilde{0^{|f(x)|}}\rangle$ and generate a quantum state of the form $\sum_{s:|s|=|f(x)|}(|\tilde{s}\rangle|\tilde{s}\rangle\otimes\langle s|\phi_g^p(x)\rangle)$. We then decode the first and the second occurrences of $|\tilde{s}\rangle$ to $|0^{|f(x)|+1}1\rangle|s\rangle$. For later convenience, we transform the first occurrence of $|0^{|f(x)|+1}1\rangle|s\rangle$ to $|s\rangle|0^{|f(x)|+1}1\rangle$. In what follows, we abbreviate $|s\rangle\langle s|\phi_g^p(x)\rangle$ as $|\zeta_g^p[s]\rangle$. Finally, we locally apply g^{-1} to the last part $|\zeta_g^p[s]\rangle$, producing $|\xi_x\rangle=\sum_{s:|s|=|f(x)|}(|s\rangle|(0^{|f(x)|+1}1)^2\rangle\otimes g^{-1}(|\zeta_g^p[s]\rangle))$.

Let $|\Psi_{f(x)}\rangle=|f(x)\rangle|(0^{|f(x)|+1}1)^2\rangle|\phi^p(x)\rangle$. Since $|\phi_g^p(x)\rangle=\sum_{s:|s|=|f(x)|}|\zeta_g^p[s]\rangle$ and $g^{-1}(|\phi_g^p(x)\rangle)=|\phi^p(x)\rangle$, we derive $|\phi^p(x)\rangle=\sum_{s:|s|=|f(x)|}g^{-1}(|\zeta_g^p[s]\rangle)$. Therefore, $|\Psi_{f(x)}\rangle$ coincides with $\sum_{s:|s|=|f(x)|}(|f(x)\rangle|(0^{|f(x)|+1}1)^2\rangle\otimes g^{-1}(|\zeta_g^p[s]\rangle))$. Let us consider the inner product $\langle\Psi_{f(x)}|\xi_x\rangle$. By a simple calculation, $\langle\Psi_{f(x)}|\xi_x\rangle$ equals $\sum_{s:|s|=|f(x)|}\langle f(x)|s\rangle\otimes\tau_x(s)$, where $\tau_x(s)$ is the inner product between $|\phi^p(x)\rangle$ and $g^{-1}(|\zeta_g^p[s]\rangle)$. Since g^{-1} belongs to $\widehat{\Box_1^{\mathrm{QP}}}$ and is dimension-preserving and norm-preserving by Proposition 3.5 and Lemma 3.4, $\tau_x(s)$ equals $\langle\zeta_g^p[s]|\zeta_g^p[s]\rangle$. Since s is forced to take the value $f(x)$ in $\langle\Psi_{f(x)}|\xi_x\rangle$, it follows that $\langle\Psi_{f(x)}|\xi_x\rangle=\langle\zeta_g^p[f(x)]|\zeta_g^p[f(x)]\rangle$, which equals $\|\langle f(x)|\phi_g^p(x)\rangle\|^2$. Therefore, we conclude that $|\langle\Psi_{f(x)}|\xi_x\rangle|^2=\|\langle f(x)|\phi_g^p(x)\rangle\|^4\geq(1-\varepsilon')^2=1-\varepsilon$, as requested.

$(3\Rightarrow 1)$ Since f is polynomially bounded, take a polynomial p such that $|f(x)|\leq p(|x|)$ holds for all strings

x. Since we do not know the length of $f(x)$, we want to expand f by setting $f_1(x) = f(x)01^{p(|x|)+2-|f(x)|}$ so that $|f_1(x)| = p(|x|) + 2$ for all strings x. Fix $\varepsilon \in [0, 1/2)$. Let us assume that there exist a function $g_1 \in \widehat{\Box_1^{\mathrm{QP}}}$ and a polynomial p_1 that satisfy $|f_1(x)| \leq p_1(|x|)$ and $|\langle \Psi_{f_1(x)} | \phi_g^{p_1,f_1}(x)\rangle|^2 \geq 1-\varepsilon$ for all instances $x \in \{0,1\}^*$.

Using Lemma 4.2 for the quantum function g_1, we can take a single-tape, polynomial-time, conservative, plain QTM M with $\tilde{\mathbb{C}}$-amplitudes for which M on input $|\phi\rangle$ produces a clean output of $g_1(|\phi\rangle)$ on its tape. We consider the following machine. On input $x \in \Sigma^*$, we first compute the value $p(|x|)$ deterministically and generate $|\phi^{p,f_1}\rangle = |0^{p(|x|)+2}1\rangle|0^{p(|x|)}10^{9p(|x|)}1\rangle \otimes |x\rangle$. We then run M on $|\phi^{p,f_1}(x)\rangle$ to produce $|\phi_{g_1}^{p,f_1}(x)\rangle$. Since $|\langle \Psi_{f_1(x)} | \phi_{g_1}^{p,f_1}(x)\rangle|^2 \geq 1-\varepsilon$, $|\phi_{g_1}^{p,f_1}(x)\rangle$ contains $f_1(x)$ with probability at least $1-\varepsilon$. From $f_1(x)$, we extract $f(x)$ and output it. This concludes that f is in $FBQP$. □

4.2 Quantum Normal Form Theorem

Our key lemmas, Lemmas 4.2 and 4.3, further lead to a quantum version of Kleene's *normal form theorem* [19, 20], which asserts the existence of a primitive recursive predicate $T(e,x,y)$ and a primitive recursive function $U(y)$ such that, for any recursive function $f(x)$, an appropriate index (called a Gödel number) $e \in \mathbb{N}$ satisfies $f(x) = U(\mu y.T(e,x,y))$ for all inputs $x \in \mathbb{N}$, where μ is the *minimization operator*. This statement is, in essence, equivalent to the existence of universal Turing machine [32]. Here, we wish to prove a slightly weaker form of the *quantum normal form theorem* using Lemmas 4.2–4.3.

Theorem 4.4 (Quantum Normal Form Theorem) *There exists a quantum function f in $\Box_1^{\mathrm{QP}}$ such that, for any quantum function g in $\Box_1^{\mathrm{QP}}$ and any constant $\varepsilon \in (0, 1/2)$, there exist a binary string e and a polynomial p satisfying $\| |\psi_{g,x}\rangle\langle\psi_{g,x}| - tr_n(|\eta_{f,x}\rangle\langle\eta_{f,x}|)\|_{\mathrm{tr}} \leq \varepsilon$ for any input $|x\rangle$ with $x \in \{0,1\}^n$, where $|\psi_{g,x}\rangle = g(|x\rangle)$ and $|\eta_{f,x}\rangle = f(|\tilde{e}\rangle|0^{p(|x|)}1\rangle|x\rangle)$. Such a function f is called* universal.

The extra term $|0^{p(|x|)}1\rangle$ in $|\eta_{f,x}\rangle$ is needed for providing g with enough work space as in the case of Theorem 4.1. To prove the theorem, we utilize the fact that there is a *universal QTM*, which can simulate all single-tape well-formed QTMs with polynomial slowdown with any desired accuracy. Such a universal machine was constructed by Bernstein and Vazirani [5, Theorem 7.1] and by Nishimura and Ozawa [26, Theorem 4.1]. We say that M_1 on input x_1 *simulates* M_2 on input x_2 *with accuracy* at most ε if the total variation distance between two probability distributions $\{\|\langle y|U_{M_1}^{p_1(|x_1|)}|c_{0,1}^{(x_1)}\rangle\|^2\}_{y\in\{0,1\}^{\leq n}}$ and $\{\|\langle y|U_{M_2}^{p_2(|x_2|)}|c_{0,2}^{(x_2)}\rangle\|^2\}_{y\in\{0,1\}^{\leq n}}$ is at most ε, where $n = \max\{p_1(|x_1|), p_2(|x_2|)\}$ and, for each index $i \in \{1,2\}$, U_{M_i} is the time-evolution operator of M_i, $p_i(\cdot)$ expresses the running time of M_i, $c_{0,i}^{(x_i)}$ is the skew initial configuration of M_i on input x_i, and y ranges over all possible output strings of M_i.

Proposition 4.5 [5, 17, 25, 26] *There exists a single-tape, well-formed, stationary QTM U such that, for every constant $\varepsilon \in (0,1)$, a number $t \in \mathbb{N}$, a single-tape well-formed QTM M with $\tilde{\mathbb{C}}$-amplitudes, U on input $\langle M, x, t, \varepsilon\rangle$ simulates M on input x for t steps with accuracy at most ε with slowdown of a polynomial in t and $\log(1/\varepsilon)$, where $\langle M, x, t, \varepsilon\rangle$ refers to a fixed, efficient encoding of a quadruplet (M, x, t, ε). Such a QTM is called* universal.

The improved factor $\log(1/\varepsilon)$ in Proposition 4.5 is attributed to Kitaev [17] and Solovay (cited in [25, Appendix 3]).

For the proof of Theorem 4.4, we need to simulate a universal QTM U provided by Proposition 4.5 on a certain conservative QTM even with lower accuracy. Concerning the form of inputs given to f, we need to split a quadruplet (M, x, t, ε) in the proposition into three parts (M, ε), t, and x and then modify U so that U can take any input of the form $|\tilde{e}\rangle|0^t1\rangle|x\rangle$, where $e = \langle M, \varepsilon\rangle$, and mimic M on x within time t with accuracy at most ε. Furthermore, we need to force U to produce *clean outputs* by relocating all non-blank symbols appearing in the left-side region of any output string to elsewhere in time polynomial in t.

Theorem 4.4 now follows directly by combining Lemmas 4.2–4.3 and Proposition 4.5.

Proof of Theorem 4.4. As explained above, let U denote a modified universal QTM that takes inputs of the form $|\tilde{e}\rangle|0^t1\rangle|x\rangle$ for any numbers $e, t \in \mathbb{N}^+$ and any string $x \in \{0,1\}^*$ and produces clean outputs. Given any quantum function $g \in \Box_1^{\mathrm{QP}}$, Lemma 4.2 guarantees the existence of a polynomial r and a single-tape, $\tilde{\mathbb{C}}$-amplitude, conservative, plain QTM M having clean outputs for which, on any input string $x \in \{0,1\}^n$, M produces within $r(n)$ steps a superposition $g(|0^{p(n)}1\rangle|x\rangle) \otimes |0, q_f\rangle$ of skew final configurations composed

of M's essential tape region and M's internal status. To be more precise, we denote by $\widehat{U}_M$ the skew time-evolution operator of M and by $c^{(x)}_{0,M}$ the skew initial configuration of M on any input $|x\rangle$. We further set $|\zeta_{M,x}\rangle$ to be $\widehat{U}_M^{r(n)}|c^{(x)}_{0,M}\rangle$ and $g(|0^{p(n)}1\rangle|x\rangle)$ to be $|\psi_{g,x}\rangle$. Note that $|\zeta_{M,x}\rangle$ equals $|\psi_{g,x}\rangle \otimes |0,q_f\rangle$. Since $|\psi_{g,x}\rangle\langle\psi_{g,x}| = tr_n(|\psi_{g,x}\rangle\langle\psi_{g,x}| \otimes |0,q_f\rangle\langle 0,q_f|)$, $|\psi_{g,x}\rangle\langle\psi_{g,x}|$ can be expressed as $tr_n(|\zeta_{M,x}\rangle\langle\zeta_{M,x}|)$.

In contrast, we denote by $\widehat{U}_\delta$ the skew time-evolution operator of U and by $c^{(x_e)}_{0,U}$ the skew initial configuration of U on the input $|x_e\rangle$ for $e = \langle M,\varepsilon\rangle$ and $x_e = \tilde{e}0^{r(|x|)}1x$. Let $m = |x_e|$ and set $|\zeta_{U,x_e}\rangle$ to be $\widehat{U}_\delta^{p(m)}|c^{(x_e)}_{0,U}\rangle$, which is written as $\sum_{r\in FSC_{U,m}} |U[r]\rangle|\xi_{x_e,r}\rangle$ for an appropriate set $\{|\xi_{x_e,r}\rangle\}_r$ of orthogonal quantum states. Proposition 4.5 then ensures that, by an appropriate choice of a polynomial s, the total variation distance between $\{\|\langle y|\widehat{U}_M^t|c^{(x)}_{0,M}\rangle\|^2\}_{y\in\{0,1\}^n}$ and $\{\|\langle y|\widehat{U}_\delta^{s(t)}|c^{(x_e)}_{0,U}\rangle\|^2\}_{y\in\{0,1\}^n}$ is at most ε for any number $t \geq 0$.

We apply Lemma 4.3 and then obtain a $\square_1^{\mathrm{QP}}$-quantum function f such that, for any quantum state $|\phi\rangle$, $f(|\phi\rangle)$ represents the result of $\widehat{U}_\delta^{s(r(n))}$ applied to $|\phi\rangle$. For convenience, we express $f(|x_e\rangle)$ as $|\eta_{f,x_e}\rangle$. Lemma 4.3 again implies that $|\eta_{f,x_e}\rangle = \sum_{r\in FSC_{U,m}} |U[r]\rangle|\widehat{\xi}_{x_e,r}\rangle$ with $\langle\xi_{x_e,r}|\xi_{x_e,r'}\rangle = \langle\widehat{\xi}_{x_e,r}|\widehat{\xi}_{x_e,r'}\rangle$ and $\langle\xi_{x,r}|\xi_{x,r'}\rangle = 0$ if $r \neq r'$ for all $r,r' \in FSC_{U,m}$. We thus obtain $tr_n(|\eta_{f,x_e}\rangle\langle\eta_{f,x_e}|) = \sum_{r,r'\in FSC_{U,m}} |U[r]\rangle\langle U[r']| \cdot tr(|\widehat{\xi}_{x_e,r}\rangle\langle\widehat{\xi}_{x_e,r'}|) = \sum_{r,r'\in FSC_{U,m}} \langle\widehat{\xi}_{x_e,r'}|\widehat{\xi}_{x_e,r}\rangle|U[r]\rangle\langle U[r']|$, which equals $\sum_{r\in FSC_{U,m}} \||\widehat{\xi}_{x_e,r}\rangle\|^2|U[r]\rangle\langle U[r]|$. Similarly, we obtain $tr_n(|\zeta_{U,x_e}\rangle\langle\zeta_{U,x_e}|) = \sum_{r\in FSC_{U,m}} \||\xi_{x_e,r}\rangle\|^2|U[r]\rangle\langle U[r]|$. From those calculations together with $\||\xi_{x_e,r}\rangle\| = \||\widehat{\xi}_{x_e,r}\rangle\|$, the equality $tr_n(|\eta_{f,x_e}\rangle\langle\eta_{f,x_e}|) = tr_n(|\zeta_{U,x_e}\rangle\langle\zeta_{U,x_e}|)$ follows immediately.

We thus conclude that $\||\psi_{g,x}\rangle\langle\psi_{g,x}| - tr_n(|\eta_{f,x}\rangle\langle\eta_{f,x}|)\|_{\mathrm{tr}} = \|tr_n(|\zeta_{M,x}\rangle\langle\zeta_{M,x}|) - tr_n(|\zeta_{U,x_e}\rangle\langle\zeta_{U,x_e}|)\|_{\mathrm{tr}}$. The last term is upper-bounded by $\sum_{y:|y|=n} |\|\langle y|\widehat{U}_\delta^{s(r(n))}|c^{(x)}_{0,U}\rangle\|^2 - \|\langle y|\widehat{U}_M^{r(n)}|c^{(x)}_{0,M}\rangle\|^2|$, which is clearly at most ε. Therefore, f is universal. □

5 Proof of the Key Lemma

To complete the proof of Theorem 4.1, we need to prove the key lemma, Lemma 4.3. This section intends to provide the lemma's desired proof. Our proof is inspired by a result of Yao [40], who demonstrated a quantum-circuit simulation of a QTM.

5.1 Functional Simulation of QTMs

An essence of the proof of Lemma 4.3 is a direct step-by-step simulation of the behavior of a single-tape, $\tilde{\mathbb{C}}$-amplitude, conservative, plain QTM $M = (Q,\Sigma,\Gamma,\delta,q_0,Q_f)$, which has clean outputs. For simplicity, we assume that $\Sigma = \{0,1\}$ and $\Gamma = \{0,1,b\}$, where b here stands for a unique blank tape symbol, instead of # used in early sections. We further assume that $Q_f = \{q_f\}$ and $Q = \{0,1\}^\ell$ for a certain fixed even number $\ell > 0$ with $q_0 = 0^\ell$ and $q_f = 1^\ell$. Let us assume that, starting with *binary* input string x written on the single input/work/output tape, M halts in at most $p(|x|)$ steps, where p is an appropriate polynomial associated only with M. We further assume that all computation paths of M on each input halt simultaneously. For convenience, we also demand that $p(n) > \ell$ for any $n \in \mathbb{N}$. It is important to remember that M eventually halts by entering a unique final inner state q_f and making the tape head stationed at the start cell and that no non-blank symbol appears in the left-side region of any output string.

Let $x = x_1x_2\cdots x_n$ be any input given to M, where x_i is a bit in $\{0,1\}$ for each index $i \in [n]$. Associated with p, an essential tape region of M on x consists of all the tape cells indexed between $-p(n)$ and $+p(n)$. We express the tape content of such an essential tape region as a string of the form $\sigma_1\sigma_2\cdots\sigma_{2p(n)+1}$ having length exactly $2p(|x|)+1$ over the tape alphabet $\Gamma = \{0,1,b\}$. We trace the changes of these symbols as M makes its moves, where σ_i is a tape symbol written at the cell indexed $i - p(n) - 1$ for every index $i \in [2p(n)+1]$.

Since all $\square_1^{\mathrm{QP}}$-functions are defined to handle quantum states in $\mathcal{H}_\infty$, we need to encode each tape symbol and thus a tape content. We thus define a new qustring that properly encodes a configuration $\gamma = (q,h,\sigma_1\sigma_2\cdots\sigma_{2p(n)+1})$ of M to be

$$|q\rangle \otimes |s_1,\hat{\sigma}_1\rangle \otimes |s_2,\hat{\sigma}_2\rangle \otimes |s_3,\hat{\sigma}_3\rangle \otimes \cdots \otimes |s_{2p(n)+1},\hat{\sigma}_{2p(n)+1}\rangle,$$

where each $\hat{\sigma}_i$ is in $\{\hat{0},\hat{1},\hat{b}\}$, each $s_i \in \{\hat{2},\hat{3}\}$ indicates the presence of the tape head (where $\hat{2}$ means "the head rests here" and $\hat{3}$ means "no head is here") at cell $i - p(n) - 1$, and q is an inner state in Q. In the subsequent subsections, we call such a qustring a *code* of the configuration γ of M and denote it by $|\hat{\gamma}\rangle$. This code $|\hat{\gamma}\rangle$ has length $\ell(|\hat{\gamma}\rangle) = 8p(n) + \ell + 4$, which is even and greater than n.

Given any binary input $x = x_1x_2\cdots x_n$ of length n, let us recall from Section 4.1 that $|\phi^p(x)\rangle = |0^{|x|}1\rangle|0^{p(|x|)}1\rangle|0^{11p(|x|)+6}1\rangle|x\rangle$ and $|\phi^{p,f}(x)\rangle = |\widetilde{0^{|f(x)|}}\rangle|0^{|f(x)|+1}1\rangle|\phi^p(x)\rangle$. Except for Step 1) in Section 5.2 as well as all steps in Section 5.4, we always ignore the prefix strings $\widetilde{0^{|f(x)|}}|0^{|f(x)|+1}10^{|x|}10^{p(|x|)}1$ in $|\phi^{p,f}(x)\rangle$ and $0^{|x|}10^{p(|x|)}1$ in $|\phi^p(x)\rangle$, and we pay our attention to the remaining qubits. The desired quantum function g will be constructed step by step through Sections 5.2–5.5.

5.2 Constructing a Coded Initial Configuration

Given a binary input $x = x_1x_2\cdots x_n$, the initial configuration γ_0 of M on x is of the form $(q_0, 0, b\cdots bxb\cdots b)$, and thus the code $|\hat{\gamma}_0\rangle$ of γ_0 must have the form

$$|q_0\rangle \otimes |\hat{3},\hat{b}\rangle \otimes \cdots \otimes |\hat{3},\hat{b}\rangle \otimes |\hat{2},\hat{x}_1\rangle \otimes |\hat{3},\hat{x}_2\rangle \otimes |\hat{3},\hat{x}_3\rangle \otimes \cdots \otimes |\hat{3},\hat{x}_n\rangle \otimes |\hat{3},\hat{b}\rangle \otimes \cdots \otimes |\hat{3},\hat{b}\rangle,$$

where $\hat{x}_i$ is the code of x_i, q_0 $(= 0^\ell)$ is the initial inner state, and x_1 rests in cell 0. Notice that $\ell(|\hat{\gamma}_0\rangle) = 8p(n) + \ell + 4$. In what follows, we show how to generate this particular code $|\hat{\gamma}_0\rangle$ from the quantum state $|\phi^p(x)\rangle$. For simplicity, we will ignore the term $|\hat{q}_0\rangle$ in the following steps except for Step 8).

1) Starting with the input $|\phi^p(x)\rangle$, we first transform it to $|0^n1\rangle|0^{p(n)}1\rangle|10^{11p(n)+5}1\rangle|x\rangle$ by a quantum function $h_1 = Skip[NOT]$, which satisfies both $h_1(|0^m1\rangle|\psi\rangle) = |0^m1\rangle \otimes NOT(|\psi\rangle)$ and $h_1(|0^{m+1}\rangle) = |0^{m+1}\rangle$ for any number $m \in \mathbb{N}$ and any quantum state $|\psi\rangle \in \mathcal{H}_\infty$. Lemma 3.9 guarantees that h_1 actually exists in $\widehat{\square_1^{\rm QP}}$.

From $|0^{p(n)}1\rangle|10^{11p(n)+5}1\rangle$, we wish to generate $|0^{p(n)}1\rangle|0^{p(n)}1\rangle|0^{10p(n)+5}1\rangle$ by an appropriately constructed $\widehat{\square_1^{\rm QP}}$-function f_1. To define the desired quantum function f_1, we first construct another quantum function g_1 that maps $|0^{p(n)}1\rangle|0^m10^k1\rangle$ to $|0^{p(n)}1\rangle|0^{m+1}10^{k-1}1\rangle$ for any two integers $m \geq 0$ and $k \geq 1$ by setting

$$g_1(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ |0\rangle \otimes g_1(\langle 0|\phi\rangle) + |1\rangle \otimes g_2(\langle 1|\phi\rangle) & \text{otherwise,} \end{cases}$$

where g_2 is introduced as

$$g_2(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ SWAP(|0\rangle \otimes g_2(\langle 0|\phi\rangle) + |1\rangle\langle 1|\phi\rangle) & \text{otherwise.} \end{cases}$$

More formally, we set $g_2 = QRec_1[I, SWAP, I|g_2, I]$ and set $\hat{g}_2 = Branch[I, g_2]$. We then set $g_1 = QRec_1[I, I, \hat{g}_2|g_1, I]$. The quantum function f_1 is finally defined as $f_1 = QRec_1[I, g_1, I|f_1, I]$; namely,

$$f_1(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ g_1(|0\rangle \otimes f_1(\langle 0|\phi\rangle) + |1\rangle\langle 1|\phi\rangle) & \text{otherwise.} \end{cases}$$

In a similar manner, we further transform $|0^{p(n)}1\rangle|0^{10p(n)+5}1\rangle$ to $|0^{p(n)}1\rangle|0^{2p(n)+2}1\rangle|0^{8p(n)+2}1\rangle$. We then change $|0^n1\rangle|0^{2p(n)+2}1\rangle$ to $|0^n1\rangle|0^n1\rangle|0^{2p(n)-n+1}1\rangle$ and $|0^n1\rangle|0^{8p(n)+2}1\rangle$ to $|0^n1\rangle|0^n1\rangle|0^{8p(n)-n+1}1\rangle$. Overall, the input $|\phi^p(x)\rangle$ is turned into $|0^n1\rangle|(0^{p(n)}1)^3\rangle|(0^n1)^2\rangle|0^{2p(n)-n+1}1\rangle|0^{8p(n)-n+1}1\rangle|x\rangle$.

(*) In what follows, by ignoring $|0^n1\rangle|(0^{p(n)}1)^3\rangle|(0^n1)^2\rangle$, we assume that our input is temporarily $|0^{8p(n)-n+1}1\rangle|x\rangle$.

2) For readability, we explain this step using an illustrative example of $|0^61\rangle|x_1x_2x_3\rangle$, which we intend to transform to $|00\rangle|\hat{3}\hat{x}_1\hat{x}_2\hat{x}_3\rangle$. For this purpose, we begin with changing $|0^61x_1x_2x_3\rangle$ to $|x_3x_2x_10^6\rangle$ by applying $REVERSE$.

To obtain $|x_30x_20x_1001\rangle|00\rangle$ from $|x_3x_2x_1\rangle|10^6\rangle$, we further apply $g_3 = SWAP \circ REP_1$, which changes $|x_3x_2x_10^6\rangle$ to $|x_30x_2x_10^5\rangle$. We repeatedly apply g_3 and transform $|x_3x_2x_1\rangle|10^6\rangle$ to $|x_30x_20x_10\rangle|10^3\rangle$. This process can be done by the quantum function $h_3 = 2QRec_2[I, h', g_3|\{h''_s\}_{s\in\{0,1\}^2}]$ defined by the 2-qubit quantum recursion, where $h' = Branch_2[\{h'_s\}_{s\in\{0,1\}^2}]$ with $h'_{a1} = SWAP$ and $h'_{a0} = I$ as well as $h''_{a1} = I$ and $h''_{a0} = h_3$ for each bit $a \in \{0, 1\}$; namely,

$$h_3(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 2, \\ \sum_{a\in\{0,1\}}(SWAP(|a1\rangle\langle a1|\psi_{g_3,\phi}\rangle) + |a0\rangle \otimes h_3(\langle a0|\psi_{g_3,\phi}\rangle)) & \text{otherwise,} \end{cases}$$

where $|\psi_{g_3,\phi}\rangle$ stands for $g_3(|\phi\rangle)$. We further apply $g_4 = REVERSE \circ h_3$ to change $|x_3x_2x_1\rangle|10^6\rangle$ to $|0^31\rangle|\hat{x}_1\hat{x}_2\hat{x}_3\rangle$. In a general case, the above process transforms $|0^n1\rangle|x_1x_2\cdots x_m\rangle$ to $|1\rangle|\hat{x}_1\hat{x}_2\cdots\hat{x}_n\rangle$.

Finally, we apply g_5, which maps $|0^31\rangle|\hat{x}_1\hat{x}_2\hat{x}_3\rangle$ to $|00\rangle|\hat{3}\hat{x}_1\hat{x}_2\hat{x}_3\rangle$, defined by

$$g_5(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ SWAP(|00\rangle \otimes g_5(\langle 00|\phi\rangle) + \sum_{y\in\{0,1\}^2-\{00\}}(|y\rangle\langle y|\phi\rangle)) & \text{otherwise.} \end{cases}$$