1

Introduction

1.1 Motivation

In 1935, Erwin Schrödinger, an Austrian physicist, proposed a thought experiment to illustrate the interpretation of uncertainty in quantum mechanics. This thought experiment later acquired the fond connotation of the "Schrödinger's Cat" experiment [1, 2]. In this treatise, we will refer to another thought experiment, namely the "Black Box Experiment." Let us assume that we have a black box with a coin spinning in it. It does not have to be a fair coin. Inside the box, we then start spinning the coin. We do not have any prior knowledge about the coin, namely whether the coin is fair or biased and we do not know whether it landed on the face or the tail side when it finally stopped spinning. At this moment, we may say that the coin inside the box is within a *superposition* of two states and has a certain probability for each of the two states. Let us continue the experiment by using several boxes. We may proceed by using two, three, or even an arbitrary number of $N \in \mathbb{N}$ boxes for this experiment. Similarly, we spin all the N coins simultaneously and close the boxes. This situation may be viewed as having 2^N states, suggesting that we can increase the computational power exponentially in line with 2^N if we can exploit the above-mentioned superposition. Let us now continue the experiment with the following step. Up to this moment, all of the boxes are completely sealed and we have secured the 2^N states of the coins simultaneously. Now, we decide to open all of the boxes at once and observe all the coins. After observing the state of each coin in each box, we are now in the position to observe a single specific state from the full set of 2^N possible states. This illustrates that after lifting the lid of the boxes the quantum states suddenly collapse into a single deterministic classical state due to the action of "observation," which is also often termed in parlance as a "measurement." This property is exploited by quantum computers, which will create a powerful computational tool that is potentially capable of breaking conventional cryptography.

Consequently, while an N-bit classical register can store only a single N-bit value, an N-qubit quantum register can store all the 2^N states concurrently. This allows the parallel evaluation of certain functions with regular global structure at a complexity cost that is equivalent to a single classical evaluation [3, 4], as illustrated in Figure 1.1. Therefore, as exemplified by Shor's factorization algorithm [5] and Grover's search algorithm [6], quantum-based computation is capable of solving certain complex problems at a substantially lower complexity than classical computing.

In 1965, Gordon E. Moore released the general rule of thumb projecting the number of transistors on a single integrated circuit chip used in the semiconductor industry. This notable rule of thumb was later termed "Moore's Law," which dictates that the number of the transistors on an integrated circuit chip will be doubled every 18 months or two years [9]. This law has maintained its validity over the past few decades, as illustrated in Figure 1.2, but it has been hypothesized that the trend is expected to slow down [10]. As the transistor's size is reduced, we encounter new physical phenomena as we enter the nanoscale world, which can only be described using the postulates of quantum mechanics [11]. We encounter both pros and cons as we embark on this journey into the unknown. First, the ability to create the above-mentioned simultaneous states at any instant lends itself to high-power parallel computing by exploiting the quantum-domain superposition. Second, the collapse of quantum superposition into a classical state upon observation potentially allows us to conceive unbreachable communication schemes and detect eavesdropping, which is the main advantage of quantum communication.

From Classical to Quantum Coding, First Edition. Zunaira Babar et al.

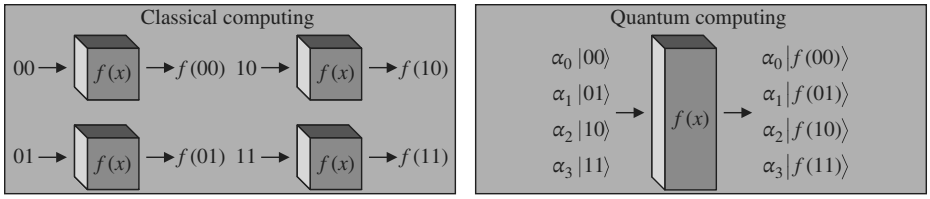


Figure 1.1 Quantum Parallelism: Given a function $f(x)$, which has a regular global structure such that $f(x) : \{0,1\}^2 \rightarrow \{0,1\}^2$, a classical system requires four evaluations to compute $f(x)$ for all possible $x \in \{00, 01, 10, 11\}$. By contrast, a two-qubit quantum register can be in a superposition of all the four possible states concurrently. This may be written as $|\psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle$, where the operation $|\ \rangle$ distinguishes the quantum states. Therefore, quantum computing requires only a single classical evaluation/observation to yield the outcome, which is also in a superposition of all the four possibilities, i.e. $\alpha_0 |f(00)\rangle + \alpha_1 |f(01)\rangle + \alpha_2 |f(10)\rangle + \alpha_3 |f(11)\rangle$. However, it is not possible to read all the four states, because the quantum register collapses to one of the four superimposed states upon measurement. Nevertheless, we may manipulate the resultant superposition of the four possible states before observing the quantum register for the sake of determining a desired property of the function. *Source*: Adapted from [5–8].

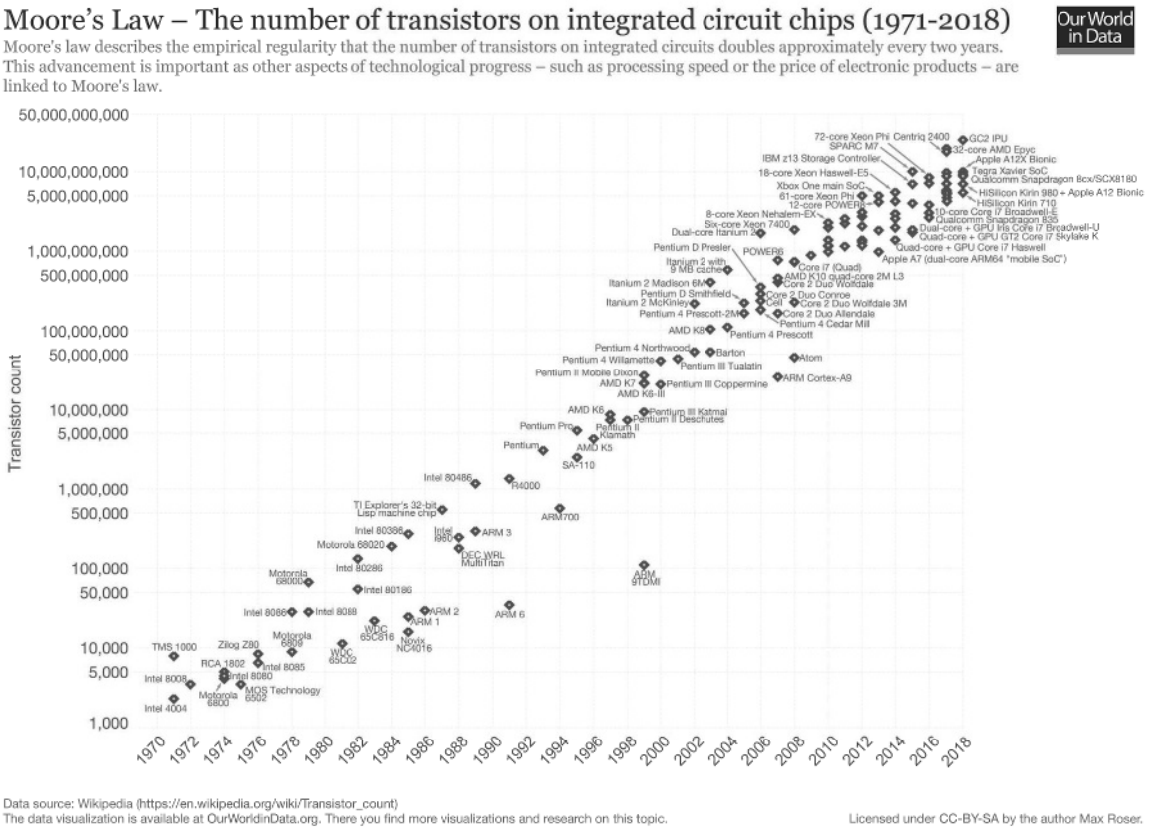


Figure 1.2 The number of transistors on an integrated circuit has doubled every two years since 1971. *Source*: [12]/Our World in Data/CC BY 4.0.

The field of theoretical quantum computing was established five decades after the Schrödinger Cat experiment by the renowned physicist Richard Feynman, who suggested how to simulate quantum phenomena using quantum computers [13]. Since then, diverse quantum-domain algorithms have been invented and indeed have shown that the laws of quantum mechanics can help us to speed up computations in some applications [4–7, 14–26]. In parallel to the quantum computing developments, attractive quantum-based solutions capable of providing absolute security have also been conceived [27–36].

Despite the above-mentioned advances, the physical implementation of quantum computers is still far from perfection. Substantial efforts have been invested in building a scalable and reliable quantum computer relying on

different solutions. For instance, by using spin electron-based techniques [37, 38], photonic chips [39–41], superconducting qubits [42–44], and recently also by using silicon [45, 46] as well as microwave trapped-ion techniques have been conceived [47, 48]. In order to arrive at the best architecture for quantum computers, the physical implementations of quantum computation must satisfy the so-called "DiVincenzo's Criteria" [49] described below:

a. **A scalable physical system with well-characterized qubits**
   The elementary unit of information in classical computers is represented by *binary digits* or *bits*. Each bit can hold only a logical value of "0" or "1" at any instant, but not both. By contrast, the elementary unit of information in quantum computers is represented by a *quantum bit* or *qubit*. In quantum mechanics, the states of "0" and "1" are commonly represented using the Dirac notation, i.e. $|0\rangle$ for state "0" and $|1\rangle$ for state "1" [50]. Each qubit can hold a value of $|0\rangle$, $|1\rangle$, or the superposition of both states. The physical realization of a qubit should reliably distinguish the state $|0\rangle$ and $|1\rangle$ as well as the superposition of both states. For instance, we can have a two-level quantum system using the up/down spin states of a particle, or the ground and excited states of an atom, or the vertical and horizontal polarization of a single photon.
b. **The ability to initialize the state of the qubits to a simple fiducial state**
   One of the essential requirements in classical computing is to know the initial state of a register before starting the computations. Similar requirements are also applicable in the quantum domain. For instance, to initialize the process of quantum search and quantum factoring algorithms, the quantum registers must supply a certain number of fresh auxiliary qubits in the state $|0\rangle$. Similarly, operations such as quantum teleportation, quantum superdense coding, and quantum key distribution (QKD) also require the quantum registers to provide a continuous supply of fresh qubits in a certain superposition state.
c. **Sufficiently long decoherence times, much longer than the gates' operation time**
   In quantum computers, the qubits will be involved in a series of quantum-domain operations to carry out certain quantum computation or quantum communication tasks. Ideally, a quantum computing algorithm and similarly a quantum communication scheme should be designed by ensuring that the computational process or transmission finishes before the qubits are corrupted by the decoherence phenomenon caused by their undesired coupling with the surrounding environment. However, a long decoherence time does not necessarily mean that the qubits are more reliable. We primarily care about the number of operations that can be completed before the qubits decohere. Hence, we should take into account the gate operation time. The maximal number of reliable operations in quantum computers is defined by the ratio of the qubits' decoherence time to the per-gate operation duration. A quantum solution with a higher maximal number of reliable operations may be more preferable, because as we scale up the quantum computers, the number of gate operations will increase.
d. **A universal set of quantum gates**
   The power of quantum computers in speeding up some computations hinges on the availability of a universal set of quantum gates. More specifically, a universal set of quantum gates primarily entails the family of gates that can be simulated by classical probabilistic computers in polynomial time – namely, the so-called Clifford group defined in [51]. Additionally, there are non-Clifford gates, which impose higher simulation complexity. Hence, in order to develop fully functioning quantum computers achieving a beneficial quantum speed-up, a set of quantum gates outside the Clifford group also have to be realized.
e. **A qubit-specific measurement capability**
   Eventually, the results from a series of quantum operations carrying out certain computational tasks have to be read out. For this reason, quantum computers require so-called measurement operators, which have to be reliable and capable of operating in various measurement bases.

As for quantum communications, there are two additional criteria, as described below:

a. **The ability to convert stationary qubits to "flying" qubits and vice versa**
   Numerous applications of quantum computers require the transmission of qubits to different locations. Hence, the capability of converting the stationary qubits to flying qubits is essential.
b. **The capability of reliably transmit flying qubits between specific locations**
   To guarantee that the state of the qubits remains intact after their displacement to a different location, their protection against quantum decoherence is required, since we cannot completely isolate the interaction of the qubits with the surrounding environment, even when high-grade electromagnetic shielding and near-absolute-zero temperatures are used.

Quantum computers face the same problem as their classical counterparts, namely decoherence. The aforementioned criteria for developing scalable and reliable quantum computers may not be accomplishable if the deleterious effects of quantum decoherence cannot be mitigated. Therefore, it is a challenge to ensure the reliability of quantum computers in the face of ubiquitous quantum decoherence. Quantum error correction codes (QECCs) constitute one of the most popular techniques for tackling the deleterious effects of quantum decoherence. The employment of QECCs may enable quantum computers to achieve high-reliability, reproducible operations, in line with the DiVincenzo's Criteria [52]. Therefore, it might be surmised that one of the key ingredients in realizing reliable quantum computers is the employment of QECCs.

1.2 Historical Overview

1.2.1 Quantum Stabilizer Codes

The concept of protecting the quantum information from decoherence is similar to that of its classical counterpart by attaching redundancy to the information [53], which is then invoked later for error correction. The quest for finding good QECCs was inspired by Shor, who conceived a 9-qubit code, which is judiciously often referred to as Shor's code [54]. Shor's code encodes a single information qubit, which is also referred to as the "logical qubit," into nine encoded qubits or "physical qubits." Shor's 9-qubit code is capable of protecting the nine physical qubits from any type of single-qubit error. Following the discovery of Shor's code, another QECC scheme—namely, Steane's code—was proposed in [55]. The latter is capable of protecting the physical qubits from any single-qubit error by encoding a single logical qubit into seven physical qubits, instead of nine qubits. The question concerning the minimum number of physical qubits required to protect them from any type of single-qubit error was answered by Laflamme *et al.*, who proposed the 5-qubit quantum code having a quantum coding rate of 1/5 [56]. This 5-qubit code may also be referred to as Laflamme's "perfect code" since the code construction achieves the quantum Hamming bound and the quantum Singleton bound of binary codes. This is the upper bound of the achievable quantum coding rate when aiming to correct a single qubit [57, 58]. To elaborate briefly, each of the five complex-valued qubits may have a bit-flip, a phase-flip as well as a joint bit-flip and phase-flip error. The bit-flip and phase-flip errors are shown in the stylized illustration of Figure 1.3.

Hence, in Laflamme's code, we have $3 \cdot 5 = 15$ legitimate error events plus the error-free scenario. Hence, we have to attach four redundant qubits to the original logical qubit for distinguishing the above-mentioned 16 possible error scenarios. In exchange for this undesirably low code rate we have a powerful error correction capability, since an arbitrary error can be eliminated in a set of five qubits, i.e. when the error rate imposed by decoherence is as high as 20%. Suffice it to say in closing that it is perfectly feasible to create high-rate codes, which would, however, correct a lower error rate, as it will transpire throughout the rest of this monograph.

The field of QECCs entered its golden age following the invention of quantum stabilizer codes (QSCs) [59, 60]. The QSC paradigm allows us to transform classical error correction codes into their quantum counterparts. QSCs must be constructed to circumvent the problem of estimating both the number and the position of quantum-domain errors imposed by quantum decoherence without observing the actual quantum states, since observing the quantum states would collapse the qubits into classical bits. This extremely beneficial error estimation technique

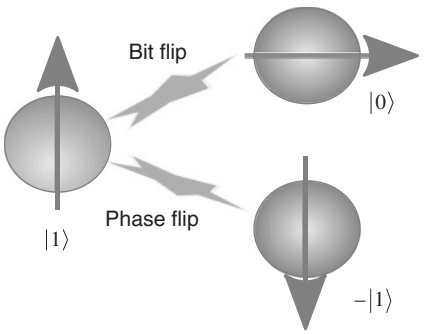


Figure 1.3 Quantum decoherence characterized by bit-flips and phase-flips. The vertical polarization represents the state $|1\rangle$, while the horizontal polarization represents the state $|0\rangle$.

was achieved by introducing the syndrome-measurement-based approach [59, 60]. In classical error correction codes, the syndrome-measurement-based approach has been widely exploited as a popular error detection and correction procedure. Therefore, the formulation of QSCs expanded the search space for good QECCs to a broader horizon. This new paradigm of incorporating the classical-to-quantum isomorphisms led to the transformation of classical codes into their quantum domain dual pairs, such as quantum Bose–Chaudhuri–Hocquenghem (QBCH) codes [61, 62], quantum Reed–Solomon (QRS) codes [63], quantum Reed–Muller (QRM) codes [64], quantum convolutional codes (QCCs) [65, 66], quantum low-density parity-check (QLDPC) codes [67], quantum turbo codes (QTCs) [68], and quantum polar codes (QPCs) [69]. A timeline that portrays the milestones of QSCs at a glance is depicted in Figure 1.4. Although the QSC formulation creates an important class of QECCs, we note that there are also other classes of QECCs beside QSCs, such as the class of decoherence-free subspace (DFS) codes [70–72]. DFS codes can be viewed as a family of passive QECCs, while QSCs constitute a specific example of the active ones. To elaborate a little further, DFS codes constitute a highly degenerate class of QECCs, which rely on the fact that

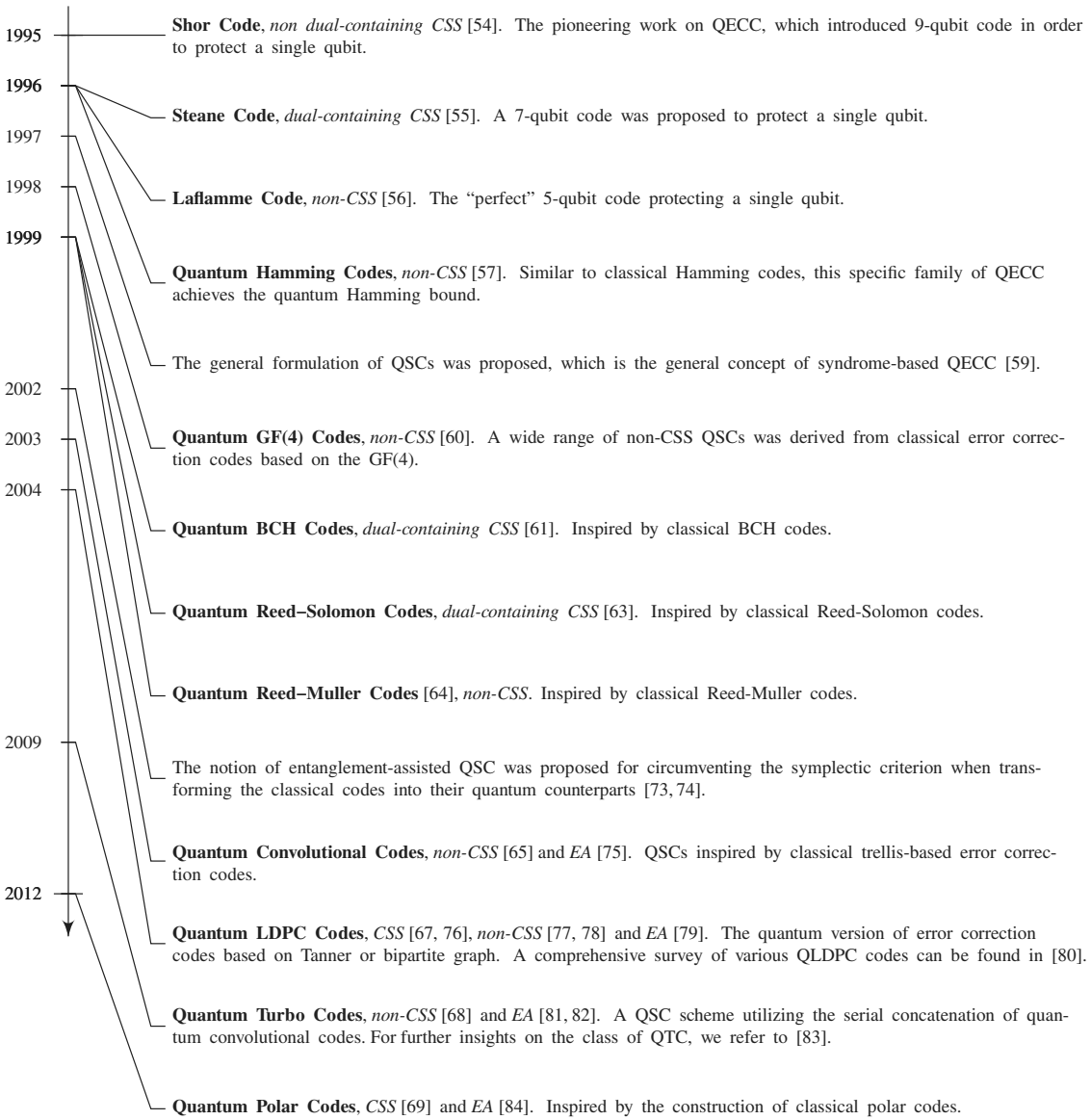


Figure 1.4 Timeline of important milestones in the QECC field, specifically in the development of QSCs. The code construction is highlighted in **bold** font, while the associated code type is printed in *italics*.

the error patterns may preserve the state of physical qubits and therefore they do not necessarily require a recovery procedure. Due to their strong reliance on the degeneracy property exhibited by the set of QECCs that do not have a classical counterpart, the class of DFS codes bears no resemblance to any classical error correction codes. Therefore, in this treatise, we focus our discussion purely on QSCs, which exhibit strong analogies with classical error correction codes.

Even though intensive research efforts have been invested in exploring the field of QSCs, one of its mysteries remains unresolved. Since the development of the first QSC, one of the open problems has been how to determine the realistically achievable size of the codebook $|\mathcal{C}| = 2^k$, given the number of physical qubits n, the minimum distance d, and the quantum coding rate of $r_Q = k/n$, where k denotes the number of logical qubits. The minimum distance d of the legitimate codewords is the parameter that defines the error correction capability of the corresponding code. The complete formulation of the realistically achievable minimum distance d, given the number of physical qubits n and the quantum coding rate r_Q is unknown at the time of writing, but several theoretical lower and upper bounds can be found in the literature [58, 85, 86]. Naturally, finding code constructions associated with growing minimum distances upon reducing the coding rate is desirable, since an increased minimum distance improves the reliability of quantum computation [52, 87–90]. The trade-off between the quantum coding rate and the minimum distance as well as the codeword length is widely recognized, but the achievable minimum distance d of a quantum code given the quantum coding rate r_Q and codeword length n remains unresolved.

For example, for a given codeword length of $n = 128$ and quantum coding rate of $r_Q = 1/2$, the achievable minimum distance is loosely bounded by $11 < d < 22$, while for $n = 1024$ and $r_Q = 1/2$, the achievable minimum distance is bounded by $78 < d < 157$. Naturally, having such a wide range of minimum distances is undesirable. For binary classical codes, this problem has been circumvented by the closed-form approximation proposed by Akhtman *et al.* [91].

The challenge of creating the quantum counterpart of error correction codes lies in the fact that the QSC constructions have to mitigate not only bit-flip errors but also phase-flip errors or both bit-flip and phase-flip errors. Based on how we mitigate those different types of errors, we can simply categorize QSCs as belonging to the class of Calderbank–Shor–Steane (CSS) codes [55, 86, 92] or to the complementary class of non-CSS codes [60]. The CSS codes handle qubit errors by treating bit-flip errors and phase-flip errors as separate entities. By contrast, the class of non-CSS codes treats both bit-flip errors and phase-flip errors simultaneously. Since the CSS codes treat the bit-flip and phase-flip error correction procedures separately, in general, they exhibit a lower coding rate than their non-CSS counterparts having the same code rate. Furthermore, if we also consider the presence of quantum entanglement, we may conceive more powerful quantum code constructions as discussed in [73, 74]. To elaborate, the family of entanglement-assisted quantum stabilizer codes (EA-QSCs) is capable of operating at a higher quantum coding rate than the unassisted QSC constructions at the same error correction capability, provided that error-free maximally entangled qubits have already been preshared [73, 74]. This presharing operation may be carried out when the circuits are not actively harnessed for carrying out urgent impending operations.

1.2.2 Quantum Topological Error Correction Codes

We have established that one of the essential prerequisites of constructing quantum computers is the employment of QECCs for ensuring that the computers operate reliably by mitigating the deleterious effects of quantum decoherence [49, 52, 93]. However, the laws of quantum mechanics prevent us from transplanting classical error correction codes directly into the quantum domain. To circumvent the constraints imposed by the nature of quantum physics, the notion of quantum stabilizer codes (QSCs) emerged [59, 60, 94]. The invention of QECCs and specifically QSC formalism did not immediately eradicate all of the obstacles of developing reliable quantum computers. Employing the QSCs requires redundancy in the form of *auxiliary* quantum bits (qubits) to encode the logical qubits into physical qubits. The redundant qubits are then exploited during the error correction. These operations rely on the quantum encoder and decoder circuits constructed from quantum gates. Therefore, the circuit-based implementation of a QSC itself has to be fault-tolerant to guarantee that the QSC circuit does not proliferate the existing errors.

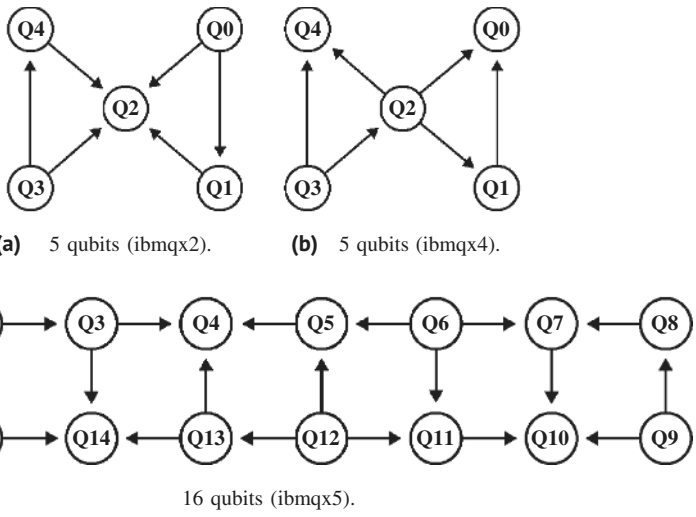
The notion of the QSC triggered numerous discoveries in the domain of QECCs, which are inspired by classical error correction codes. Essentially, QSCs represent the quantum-domain version of the classical syndrome-decoding-based error correction codes. Since the concept of utilizing the syndrome values for error correction is widely exploited in the classical domain, diverse classical error correction codes can be conveniently

"quantumized." Consequently, we can find in the literature the quantum version of error correction codes based on algebraic formalisms such as those of the Bose–Chaudhuri–Hocquenghem (BCH) codes [61] and of Reed–Solomon (RS) codes [63], quantum codes based on a conventional trellis structure such as convolutional codes [65] and turbo codes [68, 83], quantum codes based on bipartite graphs, such as low-density parity-check (LDPC) codes [67, 76–78, 80], as well as quantum codes based on channel polarization, such as polar codes [69, 84].

Apart from exploiting the above isomorphism, there are also significant contributions on directly developing code constructions solely based on the pure quantum topology and homology, as exemplified by the family of so-called toric codes [95–97], surface codes [98, 99], color codes [100], cubic codes [101], hyperbolic surface codes [102, 103], hyperbolic color codes [104], hypergraph product codes [105–107] and homological product codes [108]. Unfortunately, this concept has not been widely explored in the classical domain. By contrast, in the quantum domain, having a code construction relying on the physical configuration of qubits is highly desirable for the conception of low-complexity, high-reliability quantum computers.

For instance, this strategy has been deployed for developing IBM's superconducting quantum computers, as shown in Figure 1.5. From this figure, we can see the qubit arrangement of the three prototypes of IBM's quantum computer—which can be viewed online—namely the ibmqx2, ibmqx4, and ibmqx5 configurations [109]. The first two quantum computers are the 5-qubit quantum computers, while the third one is a 16-qubit quantum computer. The circles in Figure 1.5 represent the qubits, while the arrows represent all their two-qubit interactions. It can be seen that the existing architectures impose a limitation, namely the two-qubit interactions can only be performed between the neighboring qubits. Even though this particular limitation potentially imposes additional challenges, when it comes to QSCs deployment, the stabilizer effect can still be achieved by the corresponding qubit arrangement by invoking the family of QTECCs. A timeline that portrays the milestones in the evolution of QTECCs is portrayed at a glance in Figure 1.6.

Again, Shor's 9-qubit code protects 9 physical qubits from any type of single-qubit error, namely bit-flip (**X**), phase-flip (**Z**), as well as from simultaneous bit and phase-flip (**Y**). Furthermore, as alluded to above, not long after the discovery of the first QECCs, Steane invented the 7-qubit code, which was followed by Laflamme's perfect 5-qubit code [55, 56]. However, the construction of these codes does not naturally exhibit inherent fault-tolerance. Briefly, a QSC is said to be fault-tolerant if the circuit-based implementation of the QSC does not introduce more errors than the error correction capability of the QSC, when the quantum gates required for implementing the QSC are imperfect. The quantum circuit-based implementation of these pioneering QSCs always involves a high number of qubit interactions within the codeword of physical qubits. As a consequence, an error caused by an imperfect gate potentially propagates to other qubits, and instead of being eliminated, the deleterious effects of quantum decoherence are further aggravated.



(a) 5 qubits (ibmqx2). **(b)** 5 qubits (ibmqx4).

(c) 16 qubits (ibmqx5).

Figure 1.5 The qubit arrangement of IBM's superconducting quantum computers. The circles represent the qubits, while the arrows represent the possible qubit interactions within the computers. *Source*: Adapted from [109].

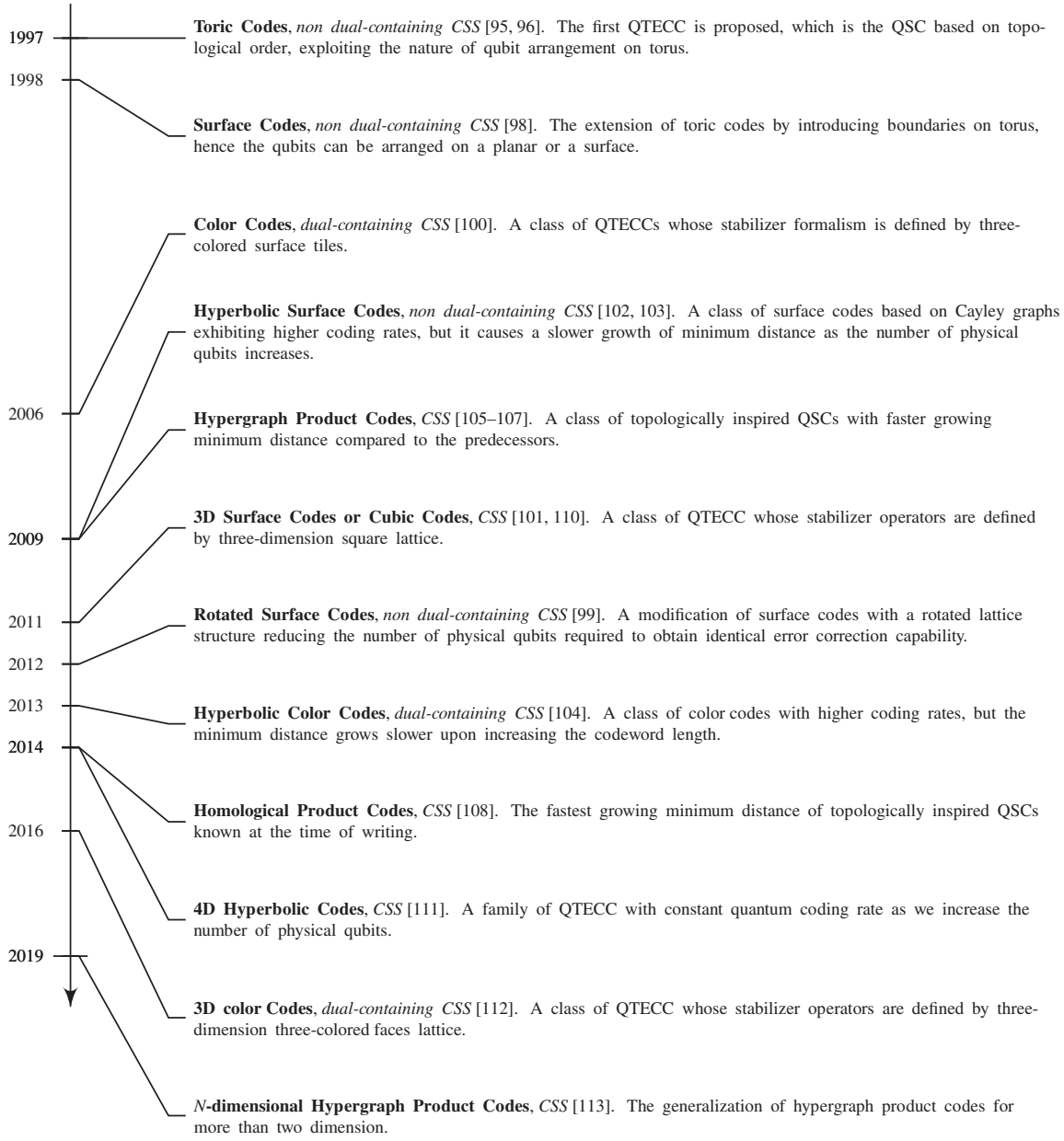


Figure 1.6 Timeline of important milestones in the area of QTECCs. The code construction is highlighted in **bold** while the associated code type is marked in *italics*.

At the current development stage of quantum computers, a QSC exhibiting fault-tolerance is more favorable, since the reliability of quantum gates is substantially lower than that of classical logic gates. The employment of QSCs is expected to mitigate the deleterious effects of the imperfect quantum gates. However, the QSC circuit itself is prone to decoherence. For the sake of constructing a fault-tolerant QSC scheme, the notion of quantum topological error correction codes (QTECCs) was proposed [95, 96]. The formulation of QTECCs offers substantial fault-tolerance improvements because they exhibit an increased minimum distance upon increasing the codeword length. Furthermore, they rely on localized stabilizer measurements. Nonetheless, one of the substantial drawbacks of QTECCs is their low quantum coding rate. More specifically, the quantum coding rate of QTECCs tends to zero for an asymptotically long codeword.

Another class of codes that are considered to be fault-tolerant QSCs is constituted by the family of QLDPC codes. The QLDPC codes inherit the property of fault-tolerance due to having a sparse parity-check matrix, which

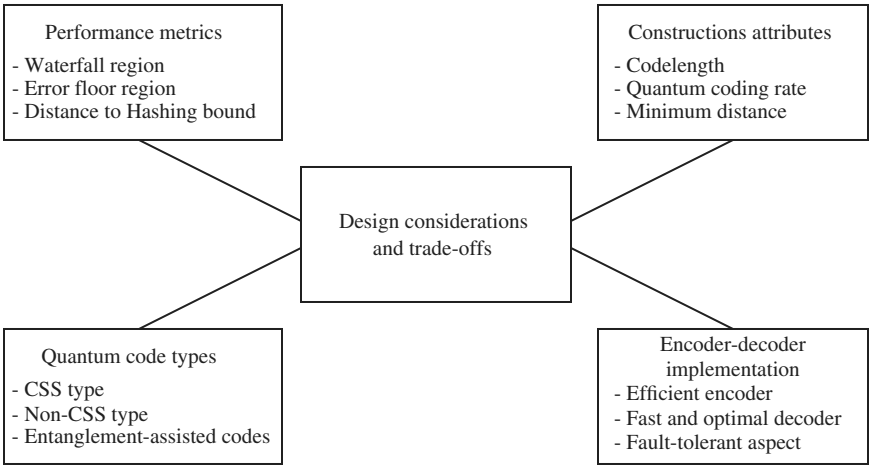


Figure 1.7 The conflicting design factors related to QECC code design.

guarantees the limited interaction of the qubits within the same block of codewords. Even though QLDPC codes can achieve good performance at a relatively high quantum coding rate, the construction of QLDPC has a bounded minimum distance [67, 107] and they tend to perform best for long codeword. Even though intensive research efforts have been invested in exploring the QECC field, the fundamental trade-off between the quantum coding rate and the minimum distance remains unresolved. Having a high minimum distance is important for guaranteeing a low error floor and robust fault-tolerance. However, it is infeasible to construct a QSC exhibiting high minimum distance without unduly reducing the quantum coding rate or increasing the number of physical qubits. Indeed, this is only a specific example of the quantum coding rate versus minimum distance trade-off. Furthermore, the quantum coding rate versus minimum distance trade-off is not the only one involved in designing QSCs, as seen in Figure 1.7. The discussion of these intricately interlinked aspects will pervade the rest of the book.

1.2.3 Quantum Convolutional Codes

The inception of QCCs dates back to 1998. Inspired by the higher coding efficiencies of classical convolutional codes (CCCs) as compared to the comparable block codes and the low latency associated with the online encoding and decoding of CCCs [114], Chau conceived the first QCC in [66]. He also generalized the classical Viterbi decoding algorithm for the class of quantum codes in [115], but he overlooked some crucial encoding and decoding aspects. Later, Ollivier *et al.* [65, 116] revisited the class of stabilizer-based convolutional codes. Similar to the classical Viterbi decoding philosophy, they also conceived a look-up table (LUT) based quantum Viterbi algorithm for the maximum likelihood decoding of QCCs, whose complexity increases linearly with the number of encoded qubits. Ollivier *et al.* also derived the corresponding online encoding and decoding circuits having a complexity that increased linearly with the number of encoded qubits. Unfortunately, their proposed rate-1/5 single-error-correcting QCC did not provide any performance or decoding complexity gain over the rate-1/5 single-error correcting block code of [56]. Pursuing this line of research, Almeida *et al.* [117] constructed a rate-1/4 single-error correcting Shor-type concatenated QCC from a CCC$(2, 1, 2)$ and invoked the classical syndrome-based trellis decoding for the quantum domain. Hence, the proposed QCC had a higher coding rate than the QCC of [65, 116]. However, this coding efficiency was achieved at the cost of a relatively high encoding complexity associated with the concatenated trellis structure. It must be pointed out here that the pair of independent trellises used for decoding the bit-flips and phase-flips imposes a lower complexity than a large joint trellis would. Finally, Forney *et al.* [118, 119] designed rate-$(n-2)/n$ QCCs comparable to their classical counterparts, thus providing higher coding efficiencies than the comparable block codes. Forney *et al.* [118, 119] achieved this by invoking arbitrary classical self-orthogonal rate-$1/n$ $\mathbb{F}_4$-linear and $\mathbb{F}_2$-linear convolutional codes for constructing unrestricted and CSS-type QCCs, respectively. Forney *et al.* [118, 119] also conceived a simple decoding algorithm for single-error-correcting codes. Both the coding efficiency and the decoding complexity of the aforementioned QCC structures are compared in Table 1.1.

Table 1.1 Comparison of the quantum convolutional code (QCC) structures.

Author(s)	Coding efficiency	Decoding complexity
Ollivier and Tillich [65, 116]	Low	Moderate
Almeida and Palazzo [117]	Moderate	Moderate
Forney *et al.* [118, 119]	High	Low

Table 1.2 Major contributions to the development of quantum convolutional codes (QCCs).

Year	Author(s)	Contribution
1998	Chau [66]	The first QCCs were developed. Unfortunately, some important encoding/decoding aspects were ignored.
1999	Chau [115]	Classical Viterbi decoding algorithm was generalized to the quantum domain. However, similar to [66], some crucial encoding/decoding aspects were overlooked.
2003	Ollivier and Tillich [65, 116]	Stabilizer-based convolutional codes and their maximum likelihood decoding using the Viterbi algorithm were revisited to overcome the deficiencies of [66, 116]. Failed to provide better performance or decoding complexity than the comparable block codes.
2004	Almeida and Palazzo [117]	Shor-type concatenated QCC was conceived and classical syndrome trellis was invoked for decoding. A high coding efficiency was achieved at the cost of a relatively high encoding complexity.
2005	Forney *et al.* [118, 119]	Unrestricted and CSS-type QCCs were derived from arbitrary classical self-orthogonal $\mathbb{F}_4$ and $\mathbb{F}_2$ CCCs, respectively, yielding a higher coding efficiency as well as a lower decoding complexity than the comparable block codes.
2005	Grassl and Rotteler [120, 121]	Conceived a new construction for QCCs from the classical self-orthogonal product codes.
2007	Aly *et al.* [122]	Algebraic QCCs derived from BCH codes.
2008	Aly *et al.* [123]	Algebraic QCCs constructed from Reed–Solomon and Reed–Muller codes.
2013	Pelchat and Poulin [124]	Degenerate Viterbi decoding was conceived, which runs the MAP algorithm over the equivalent classes of degenerate errors, thereby improving performance.

Furthermore, in the spirit of finding new constructions for QCCs, Grassl *et al.* [120, 121] constructed QCCs using the classical self-orthogonal product codes, while Aly *et al.* explored various algebraic constructions in [122, 123]. Particularly, the QCCs of [122] were derived from classical BCH codes, while the QCCs of [123] were constructed from the classical Reed–Solomon and Reed–Muller codes. Recently, Pelchat and Poulin made a major contribution to the decoding of QCCs by proposing degenerate Viterbi decoding [124], which runs the Maximum *A Posteriori* (MAP) algorithm [125] over the equivalent classes of degenerate errors, thereby improving the attainable performance. The major contributions to the development of QCCs are summarized in Table 1.2.

1.2.4 Quantum Low Density Parity Check Codes

Although convolutional codes provide somewhat better performance than the comparable block codes, yet they are not powerful enough to yield a capacity approaching performance, when used on their own. Consequently, the desire to operate close to the achievable capacity at an affordable decoding complexity further motivated researchers to design beneficial quantum counterparts of the classical LDPC codes [126], which achieve information rates close to the Shannonian capacity limit with the aid of iterative decoding schemes. Furthermore, the sparseness of the LDPC matrix is of particular interest in the quantum domain, because it requires only a small number of interactions per qubit during the error correction procedure, thus facilitating fault-tolerant decoding. Moreover, this sparse nature also makes QLDPC codes highly degenerate.

Postol [76] conceived the first example of a non-dual-containing CSS-based QLDPC code from a finite-geometry-based classical LDPC in 2001. Later, MacKay *et al.* [67] proposed various code structures (e.g. bicycle codes and unicycle codes) for constructing QLDPC codes from the family of classical dual-containing LDPC codes. Additionally, MacKay *et al.* also proposed the class of Cayley graph-based dual-containing codes in [127], which were further investigated by Couvreur *et al.* in [103, 128].

Aly *et al.* contributed to these developments by constructing dual-containing QLDPC codes from finite geometries in [129], while Djordjevic exploited the balanced incomplete block designs (BIBDs) in [130], albeit neither of these provided any gain over MacKay's bicycle codes. Lou *et al.* [131, 132] invoked the non-dual-containing CSS structure by using both the generator and the PCM of classical low-density generator matrix (LDGM)-based codes. Hagiwara *et al.* [133] conceived Quasi-Cyclic (QC) QLDPC codes, whereby the constituent PCMs of non-dual-containing CSS-type QLDPCs were constructed from a pair of QC-LDPC codes found using algebraic combinatorics. Hagiwara's design of [133] was extended to non-binary QLDPC codes in [134, 135], which operate closer to the Hashing limit than MacKay's bicycle codes. The concept of QC-QLDPC codes was further extended to the class of spatially-coupled QC codes in [136]. While all the aforementioned QLDPC constructions were CSS-based, Camara *et al.* [78] were the first authors to conceive non-CSS QLDPC codes. Later, Tan *et al.* [137] proposed several systematic constructions for non-CSS QLDPC codes, four of which were based on classical binary QC-LDPC codes, while one was derived from classical binary LDPC-convolutional codes. Since most of the above-listed QLDPC constructions exhibit an upper-bounded minimum distance, topological QLDPCs[1] were derived from Kitaev's construction in [104, 107, 138]. Amidst these activities, which focused on the construction of QLDPC codes, Poulin *et al.* were the first scientists to address the decoding issues of QLDPC codes [139], which were further improved in [140]. The major contributions made in the context of QLDPC codes are summarized in Table 1.3, while the most promising QLDPC construction methods are compared in Table 1.4[2].

Table 1.3 Major contributions to the development of iterative quantum codes. The code types "dual-containing CSS" and "non-dual-containing CSS" are abbreviated as "dual" and "non-dual," respectively.

Year	Author(s)	Code Type	Contribution
2001	Postol [76]	Non-dual	The first example of QLDPC code constructed from a finite geometry-based classical code. A generalized formalism for constructing QLDPC codes from the corresponding classical codes was not developed.
2004	MacKay *et al.* [67]	Dual	Various code structures, e.g. bicycle codes and unicycle codes, were conceived for constructing QLDPC codes from classical dual-containing LDPC codes. Performance impairment due to the presence of unavoidable length-4 cycles was first pointed out in this work. Minimum distance of the resulting codes was upper bounded by the row weight.
2005	Lou *et al.* [131, 132]	Non-dual	The generator and PCM of classical LDGM codes were exploited for constructing CSS codes. An increased decoding complexity was imposed and the codes had an upper bounded minimum distance.
2007	MacKay [127]	Dual	Cayley graph-based QLDPC codes were proposed, which had numerous length-4 cycles.
2007	Camara *et al.* [78]	Non-CSS	QLDPC codes derived from classical self-orthogonal quaternary LDPC codes were conceived, which failed to outperform MacKay's bicycle codes.
2007	Hagiwara *et al.* [133]	Non-dual	Quasi-cyclic QLDPC codes were constructed using a pair of quasi-cyclic LDPC codes, which were found using algebraic combinatorics. The resultant codes had at least a girth of 6, but they failed to outperform MacKay's constructions given in [67].
2008	Aly *et al.* [129]	Dual	QLDPC codes were constructed from finite geometries, which failed to outperform MacKay's bicycle codes.

(*Continued*)

1 Topological code structures are beyond the scope of this book.

2 All QLDPC codes must have short cycles in the quaternary formalism, which will be discussed in Chapter 14. The second column only indicates "short cycles" in the binary formalism.

Table 1.3 (Continued)

Year	Author(s)	Code Type	Contribution
2008	Djordjevic [130]	Dual	BIBDs were exploited to design QLDPC codes, which failed to outperform MacKay's bicycle codes.
2010	Tan *et al.* [137]	Non-CSS	Several systematic constructions for non-CSS QLDPC codes were proposed, four of which were based on classical binary quasi-cyclic LDPC codes, while one was derived from classical binary LDPC-convolutional codes. These code designs failed to outperform MacKay's bicycle codes.
2011	Couvreur *et al.* [103, 128]	Dual	Cayley graph-based QLDPC codes of [127] were further investigated. The lower bound on the minimum distance of the resulting QLDPC was logarithmic in the code length, but this was achieved at the cost of an increased decoding complexity.
2011	Kasai [134, 135]	Non-dual	Quasi-cyclic QLDPC codes of [133] were extended to non-binary constructions, which outperformed MacKay's bicycle codes at the cost of an increased decoding complexity. Performance was still not at par with the classical LDPC codes and minimum distance was upper bounded.
2011	Hagiwara *et al.* [136]	Non-dual	Spatially-coupled QC-QLDPC codes were developed, which outperformed the "non-coupled" design of [133] at the cost of a small coding rate loss. Performance was similar to that of [134, 135], but larger block lengths were required.
2008	Poulin *et al.* [139]		Heuristic methods were developed to alleviate the performance degradation caused by unavoidable length-4 cycles and symmetric degeneracy error.
2012	Wang *et al.* [140]		Feedback mechanism was introduced in the context of the heuristic methods of [139] to further improve the performance.
2008	Poulin *et al.* [68, 141]	Non-CSS	QTCs were conceived based on the interleaved serial concatenation of QCCs. QTCs are free from the decoding issue associated with the length-4 cycles and they offer a wider range of code parameters. Degenerate iterative decoding algorithm was also proposed. Unfortunately, QTCs have an upper bounded minimum distance.
2014	Wilde *et al.* [82]		The iterative decoding algorithm of [68, 141] failed to yield performance similar to the classical turbo codes. The decoding algorithm was improved by iteratively exchanging the *extrinsic* rather than the *a posteriori* information.

Table 1.4 Comparison of the quantum low-density parity check (QLDPC) code structures.

Code construction	Short cycles	Minimum distance	Delay	Decoding complexity
Bicycle codes [67]	Yes	Upper-bounded	Standard	Standard
Cayley-graph based codes [103, 127, 128]	Yes	Increases with the code length	Standard	Increases with the code length
LDGM-based codes [131, 132]	Yes	Upper-bounded	Standard	High
Non-binary quasi-cyclic codes [134, 135]	No	Upper-bounded	Standard	High
Spatially-coupled quasi-cyclic codes [136]	No	Upper-bounded	High	High

1.2.5 Quantum Turbo Codes

Pursuing further the direction of iterative code structures, Poulin *et al.* conceived QTCs in [68, 141], based on the interleaved serial concatenation of QCCs. Unlike QLDPC codes, QTCs offer a complete freedom in choosing the code parameters, such as the frame length, coding rate, constraint length and interleaver type. Moreover, their decoding is not impaired by the presence of length-4 cycles associated with the symplectic criterion. Furthermore, in contrast to QLDPC codes, the iterative decoding invoked for QTCs takes into account the inherent degeneracy associated with quantum codes. However, it was found in [68, 141, 142] that the constituent QCCs cannot be simultaneously both recursive and noncatastrophic. Since the recursive nature of the inner code is essential for ensuring an unbounded minimum distance, whereas the noncatastrophic nature is a necessary condition to be satisfied for achieving decoding convergence to a vanishingly low error rate, the QTCs designed in [68, 141] had a bounded minimum distance. The QBER performance curves of the QTCs conceived in [68, 141] also failed to match the classical turbo codes. This issue was dealt with in [82], where the quantum turbo decoding algorithm of [68] was improved by iteratively exchanging the *extrinsic* rather than the *a posteriori* information. The major contributions made in the domain of QTCs are summarized in Table 1.3.

1.2.6 Entanglement-assisted Quantum Codes

Some of the well-known classical codes cannot be imported into the quantum domain by invoking the aforementioned stabilizer-based code constructions because the stabilizer codes have to satisfy the stringent symplectic product criterion. This limitation was overcome in [73, 74, 143, 144] with the notion of EA quantum codes, which exploit pre-shared entanglement between the transmitter and receiver. Later, this concept was extended to numerous other code structures, e.g. EA-QLDPC codes [79], EA-QCC [75], EA-QTC [81, 82] and EA-polar codes [84]. In [81, 82], it was also found that EA-QCCs may be simultaneously both recursive and non-catastrophic. Therefore, the issue of bounded minimum distance of QTCs was resolved with the notion of entanglement. Furthermore, EA-QLDPC codes are free from length-4 cycles in the binary formalism, which in turn results in an impressive performance similar to that of the corresponding classical LDPC codes. Hence, the concept of the entanglement-assisted regime resulted in a major breakthrough in terms of constructing quantum codes, whose behavior is similar to that of the corresponding classical codes. The major milestones achieved in the history of entanglement-assisted quantum error correction codes are chronologically arranged in Figure 1.8.

1.2.7 Protecting Quantum Gates

Although the field of QECCs benefited from a rapid pace of development, because under certain conditions we can transform various classes of powerful classical error correction codes into their quantum counterparts, several challenges remain, hindering the immediate employment of these powerful QSCs in quantum computers.

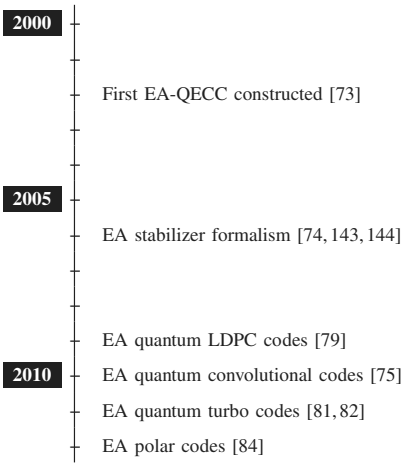


Figure 1.8 Major milestones achieved in the history of entanglement-assisted quantum error correction codes.

First, the reliability of the state-of-the-art quantum gates is still significantly lower compared to classical gates. For example, the reliability of a two-qubit quantum gate is between 90.00% and 99.90% across the various technology platforms, such as spin electronics, photonics, superconducting, trapped-ion, and silicon solutions [37–40, 42, 44–46, 145]. Similar to the classical domain, invoking an error correction code within a quantum computer requires additional components. However, adding components for error correction also implies that we unavoidably introduce an additional source of decoherence into quantum computers, since the encoder and decoder of QSCs are also composed of quantum gates.

Second, the powerful QSCs such as QTCs, QPCs, and QLDPC codes require long codewords in order to operate close to the quantum Hashing bound. In other words, they require a very high number of physical quantum bits (qubits) to correct numerous errors. Additionally, the qubits have a relatively short coherence time [146], and hence, the error correction procedure has to be completed before the ensemble of qubits starts decohering. Consequently, utilizing QSCs having a high number of qubits for correcting many errors has the potential threat of encountering an avalanche of more erroneous qubits before the error correction procedure is even completed. Third, the state-of-the-art architecture of quantum computers imposes an additional challenge, where the interactions among the qubits are ideally limited to the nearest neighbor qubits, which can be arranged by introducing a lattice-based topological architecture. However, the aforementioned challenges impose limitations on creating a fault-tolerant error correction architecture.

The quest for creating fault-tolerant gates was inspired when the notion of transversal configuration was introduced for quantum gates [52, 89]. Briefly, the concept of transversal gates relies on a parallel set of identical quantum gates invoked for carrying out the operation of a single quantum gate, as illustrated in Figure. 1.9. At the right of the figure we can see a controlled NOT (CNOT) gate. This gate does not affect the target qubit if the control bit is 0 otherwise it flips the target qubit. By contrast, the subfigure on the left is a stylized portrayal of this CNOT gate, where the multiple control and target qubits represent protected operands.

The fact that transversal quantum Clifford gates are suitable for combination with the stabilizer formalism creates an opportunity for employing a wide range of QSCs for protecting transversal quantum gates. However, the challenges we have described earlier suggest that the less populous family of QTECCs is the most suitable candidate for protecting the transversal quantum gates. Again, the motivation behind combining the QTECCs with the transversal configuration of quantum gates is that their benefits conveniently complement each other. More explicitly, the QTECCs provide localized stabilizer measurements, which consequently have the benefit of a constant number of qubit interactions, as we increase the number of physical qubits harnessed. Thus, the benefits provided by the topologically inspired stabilizer formalism will not be affected by the transversal implementation

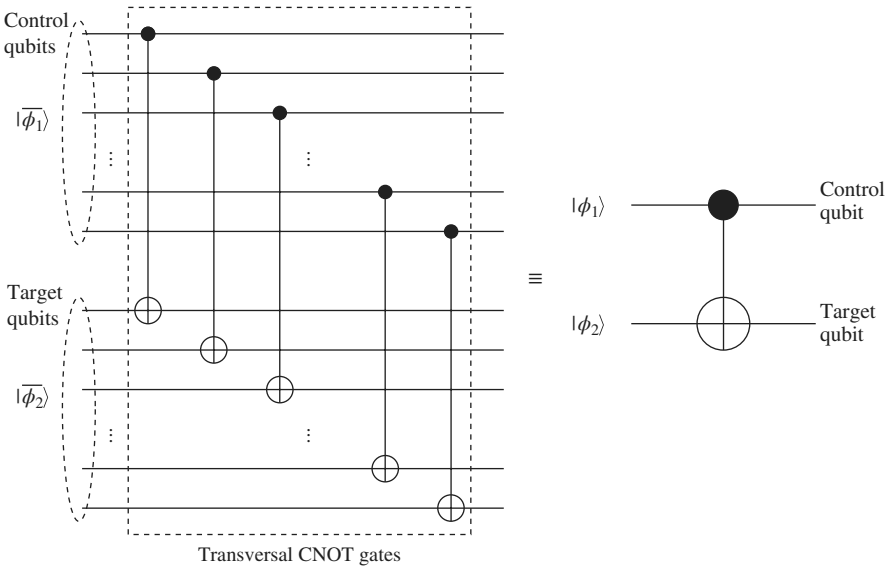


Figure 1.9 Under a certain formulation, a set of less-reliable identical quantum gates in a transversal configuration can be used for conceiving a more reliable quantum gate.

of quantum gates. Hence, the localized action of stabilizer operators among the adjacent qubits—which offers fault-tolerance—is still preserved even after the desired quantum operation has been carried out by the transversal quantum gates.

But again, the amalgamation of the QSCs and the transversal quantum gates can only be implemented for quantum Clifford gates, rather than for the entire wider family of universal quantum gates. To achieve the universality of quantum computation, a set of fault-tolerant non-Clifford quantum gates is also required. Fortunately, this wider set may also be created by using QSCs by harnessing a method referred to as magic state distillation [147], which is however beyond the scope of this work. However, protecting Clifford gates is of significant importance, since the development of large-scale quantum computers relies heavily on improving their fidelity.

The threshold theorem defined in [148] was introduced for demonstrating that a quantum computation task subject to a vanishingly low qubit error ratio (QBER) can be carried out with the aid of QECCs even when relying on realistic error-prone quantum gates, provided that the error rate imposed by the quantum gates is below a certain threshold. Since the error-prone quantum gates may also provide error-prone stabilizer measurements, typically repeated stabilizer measurements are required for reliably concluding the error correction procedure. The number of stabilizer measurements required for making a high-fidelity observation tends to grow as we increase the number of physical qubits utilized for QECCs. This specific problem has led to the emergence of the so-called "single-shot" QSCs [149–152]. Assuming that the syndrome values acquired from the syndrome measurements are not reliable, we can still achieve a vanishingly low QBER for a specific quantum computation task, given that we only perform a single stabilizer measurement for each stabilizer operator. However, beneficial QSC constructions have to exhibit a commensurately increased minimum distance as a function of the number of physical qubits. Unfortunately, the quantum coding rate of the two-dimensional QTECCs tends to zero as the codeword length increases [153–155]. We have to mention that reliably observing the values from the stabilizer measurements is also of current research interest, which is highly relevant for the study of single-shot QSCs [156–159]. Therefore, we can ask a judicious question: "Can we still utilize the two-dimensional QTECCs for fault-tolerant quantum computation, when relying only on a single stabilizer measurement for each of the stabilizer operators?" Arguably, the answer is yes, although certain conditions should be fulfilled before we can guarantee that the QSCs can offer substantial reliability improvements.

1.3 Outline of the Book

Part I of the book is constituted by Chapters 1–5 and it is dedicated to paving the way **from classical to quantum coding**. This part is organized as follows.

a. **Chapter 2: Preliminaries on Quantum Information**
   In **Chapter 2**, we will provide a rudimentary introduction to quantum information processing. We commence with the definition of the fundamental unit of quantum information constituted by the quantum bit (qubit) in Section 2.2. This is followed by a brief introduction to quantum information processing, including the reversible unitary transformations and the irreversible quantum measurement operation in Section 2.3. The various quantum decoherence models used are elaborated on in Section 2.4. In Section 2.5, we present the *no-cloning theorem*, while in Section 2.6, we highlight the concept of *quantum entanglement*.
b. **Chapter 3: From Classical to Quantum Coding**
   We continue in this chapter by presenting the duality of classical and quantum error correction codes with the aid of QSC constructions. Our objective is to highlight the similarities between the classical and quantum domains as well as to demonstrate how to transplant the well-known syndrome-based classical decoding concept into quantum error correction codes. We commence with a brief review of classical syndrome-based decoding in Section 3.2. In Section 3.3, we present the similarities between the classical syndrome-based decoding and the quantum stabilizer codes (QSCs). Finally, in Section 3.4, we provide detailed examples of the QSC constructions protecting a single qubit, namely a 1/3-rate quantum repetition code, Shor's 9-qubit code, Steane's 7-qubit code, and the Laflamme's perfect 5-qubit code.
c. **Chapter 4: Revisiting Classical Syndrome Decoding**
   In this chapter, we discuss the popular classical syndrome decoding techniques designed for classical channels. We commence our discussion with the conceptually simplest LUT-based syndrome decoding in

Section 4.2, while Section 4.3 details the construction of the syndrome-based error trellis constructed for linear block codes and convolutional codes. Finally, in Section 4.4, we detail a block syndrome decoding (BSD) technique designed for reducing the decoding complexity. In particular, we conceive a syndrome-based block decoder for classical turbo trellis-coded modulation (TTCM) schemes.

d. **Chapter 5: Near-capacity Code Designs for Entanglement-assisted Classical Communication**
In this chapter, we invoke EXtrinsic Information Transfer (EXIT) chart-aided near-capacity classical code designs conceived for reliable transmission of classical bits over quantum communication channels. More specifically, we focus our attention on the entanglement-assisted transmission of classical information over quantum channels[3], which is achieved with the aid of the SuperDense (SD) coding protocol. We commence by reviewing the SD protocol in Section 5.2, which is in essence the "Bit → Qubit Mapper." We next characterize the associated capacity in Section 5.3. In Section 5.4, we conceive a bit-based scheme, which exploits classical channel coding by serially concatenating a classical Irregular Convolutional Code (IRCC) and a classical Unity Rate Code (URC) with a quantum-based SD encoder, hence refer to it as an IRCC-URC-SD system. We present our EXIT-chart aided near-capacity design criterion in Section 5.5, where the IRCC is optimized for achieving a near-capacity performance. Our bit-based code structure of Section 5.4 incurs a capacity loss due to the symbol-to-bit conversion. To overcome this capacity loss, we propose a symbol-based code design in Section 5.7, which employs a single-component Convolutional Code (CC) and a symbol interleaver in contrast to the IRCC and bit interleaver of Section 5.7.

Part II of the book is represented by Chapters 6–9, and it is focused on relatively low-complexity quantum codes requiring a limited number of qubits. Hence, these codes may be viewed as **near-term coding** solutions. This part of the book is organized as follows.

a. **Chapter 6: Quantum Coding Bounds**
In this chapter, we investigate the trade-off between the quantum coding rate and the minimum distance of QSCs. We commence with a survey of the existing quantum coding bounds in the literature. This is followed by our proposal of a simple and invertible closed-form approximation for determining the realistically achievable minimum distance, given the quantum coding rate of both idealized infinite-length and practical finite-length codewords. Specifically, in Section 6.2, we survey the existing quantum coding bounds and derive some bounds by exploiting the classical-to-quantum isomorphism. These discussions are followed by our proposed closed-form approximation for the idealized asymptotic limit of having an infinite-length codeword in Section 6.3. Since the asymptotic limit has little relevance for practical implementations, we also proposed an approximate formula for finite-length codewords. In order to unify our quantum coding bound formulation for both the entanglement-assisted QSCs and the unassisted QSCs dispensing with entanglement, we derive a closed-form approximation for arbitrarily entangled QSCs in Section 6.5.

b. **Chapter 7: Quantum Topological Error Correction Codes**
In this chapter, we continue our discussions by the detailed construction of classical topological error correction codes (TECCs) and their quantum-domain dual pairs, namely of the family of quantum topological error correction codes (QTECCs). We carry out a detailed parametric study and derive the QBER upper bound expression. Explicitly, in Section 7.2, we commence with design examples of classical TECCs to pave the way for delving into the quantum domain, while in Section 7.3 we detail the corresponding QSC design examples of QTECCs. We continue by characterizing the performance of QTECCs in the context of the popular quantum depolarizing channel in terms of their QBER, their distance from Hashing bound, and their fidelity in Section 7.4.

c. **Chapter 8: Protecting Quantum Gates Using Quantum Topological Error Correction Codes**
We then concentrate our attention on the general framework of protecting quantum gates using QSCs. Here, we consider the amalgamation of the transversal configuration of quantum Clifford gates and the QTECCs. This combination has been opted for because it retains the desirable properties of resulting in fault-tolerant QECCs, as a joint benefit of stabilizer preservation and localized stabilizer measurements. First, we proceed

3 A quantum channel can be used for modeling imperfections in quantum hardware, namely, faults resulting from quantum decoherence and quantum gates. Furthermore, a quantum channel can also model quantum-state flips imposed by the transmission medium, including free-space wireless channels and optical fiber links, when qubits are transmitted across these media.

with the formulation of our framework in Section 8.2. This is followed by the design examples of QSC-protected Hadamard and CNOT gates in Section 8.3, where we invoke a simple quantum repetition code. In order to evaluate the performance of our proposed framework, in Section 8.4, we present the decoherence model utilized in our simulations. Then, in Section 8.5, we quantify the performance of QTECC-protected transversal Hadamard gates and CNOT gates both in terms of their QBER and fidelity along with the derivation of the upper and lower bound of the attainable analytical QBER performance in the face of quantum depolarizing channel.

d. **Chapter 9: Universal Decoding of Quantum BCH and Polar Codes via Classical Guesswork**
In this chapter, a universal decoding scheme is conceived for quantum stabilizer codes (QSCs) by appropriately adapting the "guessing random additive noise decoding" (GRAND) philosophy of classical domain codes. In the spirit of universality, we demonstrate that the generalized quantum decoder conceived is eminently suitable for different QSC decoding paradigms, namely for both stabilizer-measurement-based as well as the inverse-encoder-based decoding of diverse codes. We then harness the resultant decoder for both quantum Bose–Chaudhuri–Hocquenghem (BCH) codes and quantum polar codes and quantify both their quantum block error rate (QBLER) and QBLER per logical qubit as well as their decoding complexity. Furthermore, we provide a parametric study of the associated design trade-offs and offer design guidelines for the implementation of GRAND-based QSC decoders.

Finally, **Part III of the book – namely Chapters 10–14** – delves into the design of more **advanced quantum coding** solutions of the future, when a high number of qubits becomes available. This part is outlined as follows.

a. **Chapter 10: Revisiting the Classical to Quantum Coding Evolution**
As our discussions deepen, in this chapter, we revisit the classical to quantum isomorphism in more detail. In Section 10.2, we review the family of classical linear block codes. We next discuss the class of QSCs in Section 10.3, which are derived from the classical linear block codes of Section 10.2. In particular, we highlight the underlying quantum to classical isomorphism, which forms the basis for morphing arbitrary classical codes into the quantum domain. We then extend our discussions to the construction of QCCs from the CCCs in Section 10.4, while Section 10.5 presents EA-QSCs, which facilitate the design of quantum codes from arbitrary classical codes without imposing any stringent requirements.

b. **Chapter 11: Near-hashing-bound Concatenated Quantum Codes**
Pursuing further the design of QECCs, in this chapter we will construct near-Hashing-bound QECCs. We will commence our discourse by laying out the design objectives in Section 11.2. Section 11.3 then details the circuit-based representation of QCCs, which facilitates the degenerate iterative decoding of concatenated quantum codes. We next present our system model and the associated degenerate iterative decoding in Section 11.4. Finally, in Section 11.5, we extend the application of classical nonbinary EXIT charts to the circuit-based syndrome decoder of QTCs for approaching the Hashing bound[4]. For the sake of further facilitating the Hashing bound approaching code design, we propose the general structure of Quantum Irregular convolutional code (QIRCC) in Section 11.7, which constitutes the outer component of a concatenated quantum code.

c. **Chapter 12: Near-hashing-bound Quantum Turbo Short-block Codes**
In this chapter, we set out to conceive the concept of near-hashing bound quantum turbo short-block codes relying on different-rate quantum encoders for combatting diverse quantum depolarizing probabilities. More explicitly, this multiple-rate scheme was conceived by concatenating quantum short-block codes (QSBCs) as the outer codes with a quantum unity-rate code (QURC) as the inner code, which we refer to as the QSBC-QURC construction. In contrast to two-dimensional QTECCs, whose quantum coding rate tends to zero for long codewords, the resultant QSBC-QURC scheme exhibits a relatively high quantum coding rate. Explicitly, in Section 12.2, we present the general formulation of QSBCs in terms of their code construction, quantum encoder, and stabilizer measurement. This is followed by Section 12.3, where we propose a novel family of serially-concatenated QTCs by utilizing QSBCs as the outer codes and a QURC as the inner code, which we refer to as the QSBC-QURC scheme. We analyze the convergence behavior of our iterative-decoding-aided QSBC-QURC scheme using extrinsic information transfer (EXIT) charts and evaluate its QBER and goodput in Section 12.4.

4 The Hashing bound sets the lower limit on the achievable capacity.

d. Chapter 13: EXIT-chart Aided Design of Irregular Multiple-rate Quantum Turbo Block Codes
This chapter is dedicated to the EXIT-chart aided design of so-called irregular quantum turbo short-block codes, which rely on multiple-rate quantum short-block codes (MR-QSBCs) as the outer codes and a quantum unity-rate code (QURC) as the inner code. The proposed design is denoted as MR-QSBC-QURC. More specifically, the proposed design exhibits multiple quantum coding rates despite relying only on a single quantum encoder. The benefit of having multiple rates is that this scheme is capable of activating that specific code-rate/throughput combination, which meets the specific fidelity requirement. Moreover, the flexibility offered by the single-encoder MR-QSBCs enables us to leverage extrinsic information transfer (EXIT)-chart based heuristic optimization for determining the optimal weighting of each specific code-rate to be used in the MR-QSBCs scheme. Our simulation results show that the MR-QSBC-QURC scheme conceived performs relatively close to the ultimate limit of the quantum hashing bound. Specifically, when considering the target quantum coding rates of $r_Q = \{0.3, 0.4, 0.5, 0.6, 0.7\}$, the MR-QSBC-QURC operates at a distance of $D = \{0.042, 0.029, 0.030, 0.024, 0.017\}$ from the quantum hashing bound, respectively, at a quantum bit error ratio (QBER) of 10^{-3}.

e. Chapter 14: Quantum Low-density Parity Check Codes
Pursuing further the design of iterative code structures, we focus our efforts on QLDPC codes, which may be constructed from the classical binary as well as quaternary codes. In this context, Section 14.2 reviews the various QLDPC construction methods, while the QLDPC decoding methods and the associated challenges are discussed in Section 14.3. In Section 14.4, we propose a formalism for constructing high-rate row-circulant QC-QLDPC codes from arbitrary row-circulant classical LDPC matrices. In Section 14.6, we conceive a modified non-binary decoding algorithm for homogeneous CSS-type QLDPC codes, for the sake of alleviating the problems imposed by unavoidable length-4 cycles. Finally, Section 14.7 details the reweighted BP algorithm, which is known to alleviate the structural flaw of short cycles in classical LDPC codes.

f. Finally, in **Chapter 15** we summarize our findings along with a range of promising future research directions.