# On the Exact Analysis of an Idealized Quantum Switch

Gayane Vardoyan, Saikat Guha, Philippe Nain, Don Towsley

# On the Exact Analysis of an Idealized Quantum Switch

November 17, 2020

Gayane Vardoyan,[1] Saikat Guha,[2] Philippe Nain,[3] Don Towsley[1]

[1] University of Massachusetts, {gvardoyan, towsley}@cs.umass.edu
[2] Inria, philippe.nain@inria.fr
[3] University of Arizona, saikat@optics.arizona.edu

**Abstract**

We study an entanglement distribution switch that serves $k$ users in a star topology. The function of the switch is to facilitate end-to-end bipartite entangled state generation for pairs of users. We study a simple variant of this problem, wherein all links connecting the users to the switch are identical, the effects of state decoherence are negligible, and the switch can store an arbitrary number of qubits. We model the system using a discrete-time Markov chain and obtain the capacity of the switch. When the switch operates at capacity, we also present a numerical method for computing the expected number of qubits stored at the switch, which depends on the number of users $k$ and the probability of successful entanglement generation at the link level $p$. We then compare the results of our exact analysis to that of a continuous-time Markov chain model of a quantum switch and argue that the latter is a reasonable approximation to the more realistic model presented in this work.

**Keyword:** Quantum switch; Entanglement distribution; Markov chain

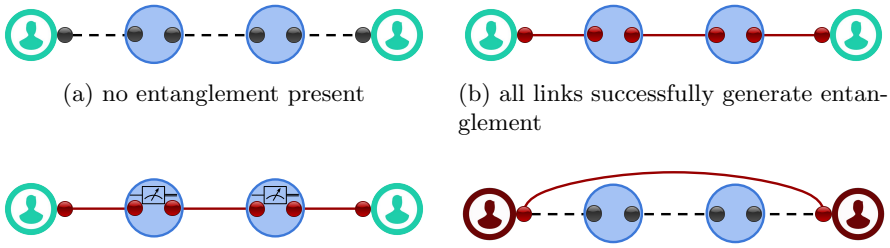
## 1 Introduction

Protocols that exploit quantum communication technology offer two advantages: they can either extend or render feasible the capabilities of their

classical counterparts, or they exhibit functionality entirely unachievable through classical means alone. For an example of the former, quantum key distribution (QKD) protocols such as E91 [6] and BBM92 [3] can in principle yield information-theoretic security by using entanglement to generate secure key bits. These raw secret key bits can then be distilled into a one-time pad to encode messages sent between two parties. For an example of the latter, distributed quantum sensing frameworks such as [7] and [27] employ entanglement to overcome the standard quantum limit [9].

While these applications hold a tremendous amount of potential for distributed quantum communication (and even computation, see, *e.g.*, [14]), a substantial challenge is reliable generation of entanglement – an essential component for many of these tasks – especially over a large distance. This is due to the fact that there is an exponential rate-versus-distance decay for quantum state propagation both through terrestrial free-space and optical fiber channels [18, 23]. Quantum repeaters positioned between communicating nodes can overcome this fundamental rate-versus-distance tradeoff [11, 15]. The process of quantum repeater-assisted entanglement generation is illustrated at a high level in Figure 1 and can be divided into two main steps. In step one, each segment connecting two adjacent nodes attempts to generate an entangled link. Qubits from a successfully-generated entanglement are stored in quantum memories, one in each node (Figure 1b). Once entangled links are present on all segments, the quantum repeaters perform entanglement swapping [28] on their two locally-held qubits (Figure 1c). If all swapping operations succeed, this results in an end-to-end entangled link between the communicating parties (Figure 1d).

In this work, we use the term "quantum switch" instead of "repeater" because in a more complex network than that of Figure 1, the device will likely be connected to several nodes or users; hence it is reasonable to assume that it will be equipped with entanglement switching logic. Quantum repeaters, switches, and similar devices (*e.g.*, trusted nodes) will serve as building blocks for large-scale quantum networks. It is natural, therefore, to ask questions about their fundamental limits from a mathematical perspective, in order to gain insight into what constitutes efficient operation for such a device, as well as to create a performance comparison basis for future protocols and algorithms that rely on these devices. To this end, we study a quantum switch that serves entangled states to pairs of users in a star topology, with the objective of determining the capacity of the switch, as well as the expected number of stored qubits in memory at the switch when it operates at capacity. We use a discrete-time Markov chain (DTMC) to construct a model that abstracts away various architecture and



(a) no entanglement present

(b) all links successfully generate entanglement

(c) repeater nodes perform entangling measurements

(d) end nodes share an entangled state

Figure 1: Long-distance entanglement generation using quantum repeaters. The two nodes at the edges are communicating parties, and the nodes between them are quantum repeaters. Dashed lines represent lack of entangled links, while solid lines represent presence of entanglement. The gray and red circles are unoccupied and occupied quantum memories, respectively.

physical implementation details about the system, *e.g.*, the method used for entanglement generation or how quantum memories are realized.

We focus on the simplest variant of this problem, wherein links connecting users to the switch are identical, there is no quantum state decoherence, and the switch can store arbitrary numbers of qubits. Throughout this paper, we often refer to the number of quantum memories at the switch as its *buffer size*. An unfortunate property of our DTMC model is that it is difficult to extend to include the aforementioned system characteristics. Prior literature on quantum switch modeling utilizes continuous-time Markov chains (CTMCs) to account for these phenomena. Nevertheless, there is value in studying a quantum switch using a DTMC, as the system is inherently a discrete-time system. Hence, while CTMCs have been shown to be more expressive as a modeling technique, there will undoubtedly be some differences in the resulting performance metrics. To quantify these differences, and determine whether a CTMC model provides a reasonable approximation to the original system, we compare the performance metrics obtained from both models.

Following is a summary of our results:

– the DTMC is stable if and only if the number of users $k \geq 3$;

– the capacity of the switch is given by

$$C = \frac{qkp}{2},$$

where $k$ is the number of users or links, $p$ is the probability of successfully generating entanglement at the link level, and $q$ is the probability of a successful swapping operation;

– when the switch operates at capacity (a detailed description of a switching policy that achieves the maximum entanglement switching rate is described in Section 4), the expected number of stored qubits is given by

$$E[Q] = \frac{1+\beta}{2(1-\beta)},$$

where $Q$ is the number of qubits stored at the switch in steady state, across all links, and $\beta$ is in the interval $(0, 1)$ and is the unique solution to the following equation[1] when $k \geq 3$:

$$(\beta p + \overline{p})^{k-1}(p + \beta\overline{p}) - \beta = 0;$$

– the expression for the capacity of the switch obtained using the DTMC matches exactly that of the CTMC model found in literature. On the other hand, the CTMC model overestimates the expected number of qubits in memory in steady state, but since the discrepancy is not significant, we conclude that the CTMC model is a reasonable approximation to the behavior of the system considered in this work.

The rest of this paper is organized as follows: in Section 2, we introduce the relevant background for quantum computation and communication. In Section 3 we discuss related work on quantum switch modeling. In Section 4, we formally introduce the DTMC model and state the objectives. The analysis is performed in Section 5. In Section 6, we compare the DTMC model introduced in this work with an existing CTMC model. We conclude in Section 7.

## 2 Background

A qubit is the quantum analogue of a bit and can be described by a two-level quantum-mechanical system, *e.g.*, the up or down spin of an electron, or the horizontal and vertical polarization of a photon. An important distinction

[1] Throughout this paper, $\overline{p} \equiv 1 - p$.

between bits and qubits is that the latter can be in a superposition of two possibilities. In Dirac notation, this is represented as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \equiv \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix},$$

where $\alpha$ and $\beta$ are complex and $|\alpha|^2 + |\beta|^2 = 1$. The probabilistic interpretation is that if we prepare many states $|\psi\rangle$ and measure them (in the computational basis $\{|0\rangle, |1\rangle\}$), then over time, $P(0) = |\alpha|^2$ and $P(1) = |\beta|^2$, where $P(0)$ and $P(1)$ denote the probability of the qubit's superposition collapsing into state $|0\rangle$ or $|1\rangle$, respectively.

Multi-qubit quantum states can be represented mathematically using tensor products. For an example, if Alice has a qubit $A$ in state $|0\rangle$ and Bob has a qubit $B$ in state $|1\rangle$, we can represent the overall state as $|0\rangle_A \otimes |1\rangle_B \equiv |01\rangle$. Two qubits are said to be entangled if their state cannot be expressed as a tensor product of their individual states (intuitively, this means that the state of one qubit cannot be described independently from the state of the other). One of the most essential resources for quantum communication is a maximally entangled two-qubit state known as a Bell state or Bell pair. An example of such a state is

$$|\Phi^+\rangle = \frac{|0\rangle_A\,|0\rangle_B + |1\rangle_A\,|1\rangle_B}{\sqrt{2}},$$

where the subscripts $A$ and $B$ signify the two qubits, possibly separated by an arbitrary distance. For Bell pairs, the probability of an outcome is always $1/2$. Since the qubits $A$ and $B$ are entangled, measuring one of them, say $A$, and reading out the result tells us with certainty the state of the other qubit, $B$. Note that the outcome of the first measurement is completely random: the state of qubit $A$ may collapse to $|0\rangle$ or $|1\rangle$, each with probability $1/2$, but if $B$ is then measured (in the same basis as $A$), even if it is a large distance away from $A$ and even if the second measurement is performed immediately after the first, the outcome will be the same as that of the first measurement. Thus, $A$ and $B$ are perfectly correlated, but in a much stronger way than is possible classically.

The four Bell pairs are given by

$$|\Phi^\pm\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}} \quad \text{and} \quad |\Psi^\pm\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

and can be used as expendable resources in a number of distributed quantum tasks, such as teleportation [2], superdense coding [4], or to generate a raw secret key bit in entanglement-based QKD protocols.

One of the major challenges of implementation of distributed tasks in quantum networks is the difficulty of safely transmitting a quantum state across a large distance. For optical fiber, channel transmissivity is $\eta = e^{-\alpha L}$, where $L$ is the length of the link and $\alpha$ the fiber attenuation coefficient. The probability of successful entanglement generation $p$ on a link is proportional to its transmissivity $\eta$. Transmission through free space poses its own challenges, such as photon loss and phase changes due to scattering [24]. Non-entanglement-based protocols, such as BB84 [1], also suffer from limited distance for the same reason: the likelihood of losing a quantum state in transit grows exponentially with the distance, while the no-cloning theorem [26] prevents one from making an independent copy of an unknown quantum state, thereby rendering losses irrecoverable. A remedy for the issue of limited distance is the use of quantum repeaters [5] coupled with the process of teleportation. Teleportation works by allowing one user to transport a (possibly unknown) qubit to another user using a shared Bell pair, local operations, and classical communication.

Quantum repeaters extend the distance between two or more communicating parties via entanglement swapping operations. An example of these operations and their effects is illustrated in Figure 1, where each solid line is a Bell state. It is worth noting that Figure 1 depicts one of the most valuable uses of Bell states in a quantum network. In the special case of long-distance Bell pair generation via connection of two shorter-distance Bell pairs, the switch performs the swapping operation via a Bell state measurement (BSM). In linear optics, this is a probabilistic but heralded operation, with the success probability dependent on the exact implementation of the BSM as well as gate operation efficiencies [20, 8, 10]. We address this phenomenon in our model by introducing a parameter that represents the BSM success probability.

In general, all quantum states are subject to decoherence, which can be thought of as leakage of information from the quantum system into the environment. Fidelity, a number in $[0, 1]$, is a measure of closeness of a possibly mixed state to the desired pure state, with unit fidelity implying that the two states have equivalent representations. Intuitively, fidelity can be thought of as the quality of the entanglement. Fidelity may degrade when a qubit is in storage as well as after a swapping operation (*i.e.*, the fidelity of the resulting state will be lower than that of the original states used in the swap). In this work, we assume that each successfully-generated quantum state (whether it is an elementary link-level Bell pair or a longer-distance entanglement resulting from an entanglement swap) has unit fidelity and that the quantum memories used for storing qubits are capable of noiseless

storage and have infinite coherence times. While these assumptions create a highly idealized scenario, it is nevertheless valuable to study as the analysis will yield an upper bound on the entanglement switching rate of a quantum switch operating under more realistic conditions.

## 3 Related Work

In [25], the authors introduce a CTMC-based model to analyze a quantum switch that serves only bipartite end-to-end entangled states to pairs of users. While it is easier to extend this model to represent systems that are more complex than that of this work, an important question that arises is whether the CTMC model is a fair approximation to a more realistic DTMC model. We answer this question in Section 6, from the perspective of the chain's stability condition and expressions for switch capacity and expected number of qubits in memory at the switch in steady state. In [16], the authors use a CTMC to analyze a multipartite entanglement distribution switch for a similarly idealized scenario as studied in our work: identical links, no quantum state decoherence, unit fidelities, and infinite quantum storage. While this switch serves $n$-partite Greenberger-Horne-Zeilinger (GHZ) states [17], note that setting $n = 2$ yields precisely the model presented in [25] (and thus, the analytical results are equivalent for the two CTMCs).

Some analyses focus on specific quantum repeater architectures or protocols; *e.g.*, in [11] the authors perform a rigorous and detailed analysis of the repeater architecture proposed in [21], accounting for various non-idealities at the channel, detectors, and quantum memories. In contrast, our take on analysis is from a rather opposite perspective in that we use mathematical tools to abstract away as many details of the physical platform as possible, while keeping only a few relevant and important parameters in order to complete a high-level analysis and gain a clear understanding of how they relate to the performance metrics of interest.

Note that applications of the problem we have formulated in this work extend far beyond entanglement switching. In general, one may view the system as a stochastic assembly-like queue, or a "kitting" process, *e.g.*, as in [22, 19, 13], since in a sense, the switch "assembles" longer-distance entangled states using shorter-distance ones, whose "arrival" into the system is driven by a stochastic process. Interestingly, none of these similar problem formulations found in literature have a direct correspondence to our problem, as in our case, the number of users being serviced by the central node

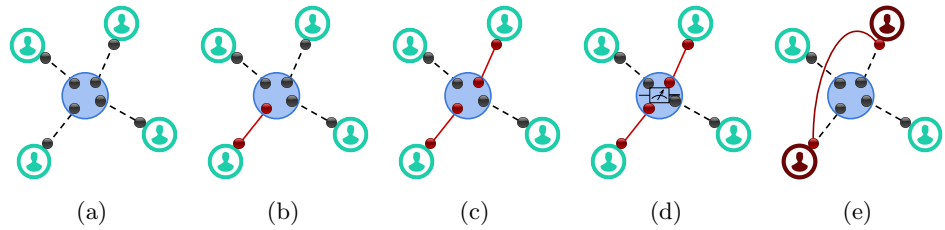



Figure 2: Example of quantum switch operation. No Bell pairs are present in **(a)**. When enough Bell pairs are successfully generated (solid lines in **(b)** and **(c)**), the switch performs a BSM **(d)**, entangling the two users' qubits **(e)**.

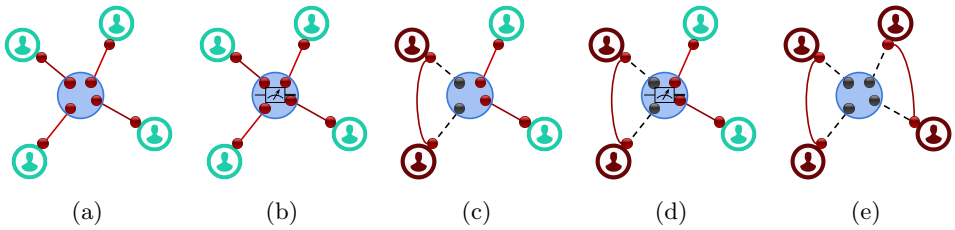



Figure 3: Example switch operation for a single time slot. At the beginning of the slot, **(a)**, all links have successfully generated Bell pairs. In **(b)**, the switch performs a BSM to entangle the two users on the left, see **(c)**. Next, still within the same time slot, the switch performs another BSM to entangle the two users on the right, shown in **(d)**, **(e)**.

is allowed to be, in theory, infinite, and our goal is to derive exact results, as opposed to approximate ones, or bounds. Hence, the problem studied here is a novel one, and the results derived in this work are of independent interest to queueing theory.

## 4 Switch Description and Objectives

Figure 2a illustrates the initial problem setup: $k \geq 2$ users are connected to the quantum switch via dedicated, identical links. Time is slotted; the rest of Figure 2 presents an example of a sequence of events that may take place in subsequent time slots. The purpose of the switch is to facilitate end-to-end entanglement generation for pairs of users that request it. The creation

of an end-to-end entanglement involves two steps. First, in each time slot users attempt to generate pairwise entanglements with the switch, which we call link-level entanglements. A successful link-level entanglement results in a two-qubit Bell state, with one qubit stored at the switch and the other stored at a user. In step two, the switch chooses two locally-held qubits, each entangled with a qubit held in a user's quantum memory, and such that the two users wish to share an entangled state, and performs a BSM. If the measurement is successful, the result is a two-qubit maximally-entangled state between the corresponding pair of users. The switch continues to fulfill entanglement requests as long as there are available link-level entanglements for users who wish to communicate. If, at the end of the time slot, there are available link-level Bell pairs, but the switch cannot use them to fulfill requests based on current user demands, then the switch may choose to store the available entangled qubits in local quantum memories until these qubits can be used in entangling measurements. This two-step process is then repeated in the next time slot. Figure 3 illustrates a sequence of events within a single time slot.

One of our objectives is to derive the capacity of a quantum switch that operates as described above. This quantity serves as a useful benchmark against which to compare the performance of future entanglement switching protocols. In this work, we also compute the expected number of qubits stored in memory at the switch, while the device operates at or near capacity. With this expression, we can obtain insight on the practical memory requirements of a switch. The capacity of the switch is defined as the maximum achievable entanglement switching rate of the device. This rate cannot be achieved with an arbitrary switching policy, or for an arbitrary set of user demands – if the switch is constrained to fulfill specific user requests, then the resulting rate would likely fall below the capacity. One way to ensure that the switch operates at capacity is to allow it to perform a BSM as soon as there are at least two Bell pairs available on two distinct links, during a given time slot. This amounts to the assumption that any pair of users wish to communicate within each time slot. BSMs are assumed to take up a negligible amount of time, and the switch may perform as many of them as necessary in a single time slot, until there are no longer two distinct links with available Bell pairs.

Further, in this work we assume that the switch uses the *Oldest Link Entanglement First (OLEF)*[2] rule when deciding which two users to pair

[2]The OLEF rule can be thought of as a First In, First Out (FIFO) policy for entanglement switching.

up for an entangling measurement. As the name suggests, when using this rule the switch prioritizes the oldest link-level Bell pairs for a BSM, as long as they belong to two different links. When there is more than one possible choice for such a pairing (*e.g.*, if there are three link-level Bell pairs of identical age and they are the oldest in the system), then the switch may choose any two at random. Note that the OLEF rule does not affect the switch capacity, but it does happen to minimize the number of stored Bell pairs at the end of each time slot and thus this rule affects the qubit occupancy distribution. Finally, to ensure that the end users being serviced by the switch do not limit switch performance, we allow end nodes to have infinite and noiseless quantum storage.

Recall from Section 2 that we study a somewhat idealized version of a quantum switch in this work in that the device has an infinite number of noiseless quantum memories, and quantum states that are successfully generated (either at the link or end-to-end level) have unit fidelities and are not subject to decoherence. Studying this simplified scenario is both valuable and prudent: the analysis performed here helps to lay out the foundation for – and possibly inspire – future work in modeling quantum switches, and our model serves as an easily-applicable comparison basis for alternate quantum switch models, such as that of [25]. Finally, note that the capacity of this "idealized" quantum switch can also serve as an upper bound on the capacity of more "limited" systems, such as those with finite quantum memories, non-unit quantum state fidelities, and explicit user requests. Note also that one may obtain an upper bound on the capacity of a system with non-identical links, simply by converting that system into one with identical links, where each link behaves as the most efficient link – in terms of successful entanglement generation – of the original system.

# 5 Analysis

In this section, we describe the DTMC model and present its analysis. Our goal is to derive the switch capacity $C$ (*i.e.*, the number of end-to-end entanglements produced per time unit), the expected number of stored qubits $E[Q]$ in steady state, and system stability conditions. A note on mathematical notation: in this paper, we will use the convention that for any $y > x$, the term $\binom{x}{y} = 0$.

### 5.1 Model Description

We model a switch serving $k$ users, each of whom has a separate, dedicated link to the switch, as a slotted system where each slot is of length $\tau$ seconds. Both link-level entanglement generation and entangling measurements can be modeled as probabilistic phenomena [12]. In this work, we model the former as follows: at each time step of length $\tau$ seconds, all $k$ users attempt to generate link-level entanglements. In general, link $l$ successfully generates an entanglement with probability $p_l \approx e^{-\alpha L}$, where $L$ is the length of the link (*e.g.*, optical fiber) and $\alpha$ its attenuation coefficient. Since in this work, we assume all links are identical, *i.e.*, they have equal length and have the same attenuation coefficient, the entanglement success probabilities on all links are equal. Hence, let $p$ denote the probability that an entangled pair is successfully established on any link, and define $\overline{p} \equiv 1 - p$. Then the expected time to successfully create a link entanglement is given by $\tau/p$ (this will be useful in Section 6, when we make comparisons to a CTMC model). We assume that whenever a link-level entanglement or an end-to-end entanglement is successfully generated, it always has fidelity one to the corresponding ideal Bell state. We also assume that measurements performed by the switch succeed with probability $q$[3]. As discussed in the previous section, we assume that any pair of users wishes to "communicate" (*i.e.*, share an entangled state) as long as link-level entanglements are available, and that the switch serves BSMs based on the OLEF policy described in Section 4.

Note that only one link stores entanglements at any one time, since whenever a distinct pair of users has link-level entanglements, they are immediately paired up for a BSM. As a consequence of this and the identical-link assumption, it is not necessary to keep track of which link has stored entanglements: one need only keep track of *how many* are stored. Hence, the state space is given by $\Omega = \{0, 1, 2, \dots\}$. Let $S$ denote the link that has at least one stored entanglement. Figure 4 illustrates the possible transitions from a state $i \geq k + 1$ (as we will see later, transitions for states $i \in \{0, 1, \dots, k\}$ require special consideration). Table 1 provides a notation reference that is used in the analysis.

[3]With a linear optical circuit, four unentangled ancilla single photons and photon number resolving detectors, with all the devices being lossless, $q = 25/32 = 0.78$ can be achieved for BSMs [8]. With other technologies $q$ close to 1 can be achieved [10].

Table 1: Notation for the DTMC model.

| Notation | Description |
|---|---|
| $p$ | probability of a successful link entanglement |
| $S$ | link with stored entanglements |
| $P_f$ | probability of gaining an entanglement in memory |
| $P_s$ | probability of remaining in current state |
| $P_{(j)}$ | probability of using $j$ of the stored entanglements |
| $P_{j,0}$ | probability of going from state $j \in \{0, \ldots, k-1\}$ to 0 |
| $P_{j,1}$ | probability of going from state $j \in \{0, \ldots, k\}$ to 1 |

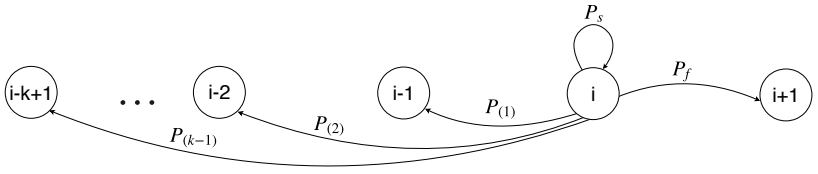



Figure 4: A DTMC model with $k$ users, infinite buffer, and identical links. Here, $i \geq k+1$, $P_f$ is the probability of advancing forward in the Markov chain, $P_s$ is the probability of remaining in the current state, and $P_{(j)}$ is the probability of going back $j$ states.

## 5.2 Analysis

First, we fully define the transition probabilities for this chain. We expect the stationary distribution to have a geometric form and show this to be true. However, a closed-form solution is not obtainable for large $k$, as it requires solving a polynomial of degree $k-1$ for an unknown factor, $\beta$. On the other hand, not having a closed-form solution for the stationary probability vector does not preclude us from deriving a simple expression for the capacity of the switch – it is $qkp/2$. We will also show that this system is stable if and only if $k \geq 3$. Finally, we also obtain a simple expression for the expected number of qubits in memory at the switch, but are constrained to compute it numerically due to its dependence on $\beta$.

### 5.2.1 Transition Probabilities

Figure 5 presents the transition probability matrix $P$ for this DTMC. Note that repetition begins after the $k$th row of the matrix. We derive expressions for all non-zero transition probabilities. In the discussion that follows, we

$$
P = \begin{bmatrix}
P_{0,0} & P_{0,1} & 0 & \cdots & & & & & & & & & & & & & \\
P_{1,0} & P_{1,1} & P_f & 0 & \cdots & & & & & & & & & & & & \\
P_{2,0} & P_{2,1} & P_s & P_f & 0 & \cdots & & & & & & & & & & & \\
\vdots & \vdots & & & & & & & & & & & & & & & \\
P_{i-1,0} & P_{i-1,1} & P_{(i-3)} & \cdots & P_{(3)} & P_{(2)} & P_{(1)} & P_s & P_f & 0 & \cdots & & & & & & \\
P_{i,0} & P_{i,1} & P_{(i-2)} & P_{(i-3)} & \cdots & P_{(3)} & P_{(2)} & P_{(1)} & P_s & P_f & 0 & \cdots & & & & & \\
P_{i+1,0} & P_{i+1,1} & P_{(i-1)} & P_{(i-2)} & P_{(i-3)} & \cdots & P_{(3)} & P_{(2)} & P_{(1)} & P_s & P_f & 0 & \cdots & & & & \\
\vdots & \vdots & & \ddots & & \ddots & \ddots & \ddots & \ddots & \ddots & & & & & & & \\
P_{k-1,0} & P_{k-1,1} & P_{(k-3)} & \cdots & & & & & \cdots & P_{(1)} & P_s & P_f & 0 & \cdots & & & \\
0 & P_{k,1} & P_{(k-2)} & P_{(k-3)} & \cdots & & & & \cdots & P_{(2)} & P_{(1)} & P_s & P_f & 0 & \cdots & & \\
0 & 0 & P_{(k-1)} & P_{(k-2)} & P_{(k-3)} & \cdots & & & \cdots & P_{(3)} & P_{(2)} & P_{(1)} & P_s & P_f & 0 & \cdots & \\
0 & 0 & 0 & P_{(k-1)} & P_{(k-2)} & P_{(k-3)} & \cdots & & \cdots & P_{(4)} & P_{(3)} & P_{(2)} & P_{(1)} & P_s & P_f & 0 & \cdots \\
\vdots & \vdots & \vdots & \ddots & \ddots & & & & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & & \\
\end{bmatrix} \tag{13}
$$

Figure 5: Transition probability matrix $P$ for the DTMC model.

say that a link "succeeds" or "fails" for brevity, when referring to a link that successfully generates an entanglement or fails to do so, respectively. Throughout the following, we will often refer to link $S$, which has at least one stored entanglement. First, consider any state $i > 1$. The transitions for this state are described as follows:

$i \to i+1$**:** the only way to advance forward in the chain is if $S$ successfully generates a new entanglement, but all other links fail to do so. This probability is given by

$$P_f = p\overline{p}^{k-1}.$$

$i \to i$**:** there are two ways to remain in the current state: (a) all links fail or (b) $S$ succeeds and only one of the $k-1$ other links succeeds. This occurs with probability

$$P_s = \overline{p}^k + (k-1)p^2\overline{p}^{k-2}.$$

$i \to i-j$ , for $j \in \{1, \ldots, M\}$, where $M = k-1$ if $i \geq k+1$ and $M = i-2$ otherwise. Here, $M$ signifies the maximum number of stored entanglements that can be used when starting from state $i$. Note that even in the case where all $k$ links succeed and $i \geq k$, only $k-1$ of the stored entanglements are used: the entanglement that was generated by $S$ cannot be paired with another entanglement from $S$. As stated above, we compute transition probabilities to states 0 or 1 separately, since they require special consideration. This is why $M = i-2$ for states $i < k+1$. Keeping these constraints in mind, the transition from $i$ to $i-j$ occurs in two types of events:

(a) $S$ fails and exactly $j$ of the $k-1$ other links succeed,

(b) $S$ succeeds and exactly $j+1$ of the $k-1$ other links succeed.

These events occur with probability

$$\begin{aligned} P_{(j)} &= \overline{p}\binom{k-1}{j}p^j\overline{p}^{k-1-j} + p\binom{k-1}{j+1}p^{j+1}\overline{p}^{k-1-(j+1)} \\ &= \binom{k-1}{j}p^j\overline{p}^{k-j} + \binom{k-1}{j+1}p^{j+2}\overline{p}^{k-j-2}. \end{aligned}$$

Next, we discuss transitions to states 0 and 1, which, unlike the probabilities above, depend on the value $i$ of the state from which the transitions occur. To help with this task, we first need to compute two types of probabilities:

the first is the probability that out of $k$ link-level entanglement events, $j \geq i$ succeed, where $j$ is either zero or an even number, and we call this probability $P_e(i,k)$; and the second is the probability that out of $k$ events, $j \geq i$ succeed, where $j$ is an odd number, and we call this $P_o(i,k)$. To compute these, we use the following two indicator functions:

$$\mathbb{1}\{j \text{ is 0 or even}\} \coloneqq \frac{1+(-1)^j}{2},\ \mathbb{1}\{j \text{ is odd}\} \coloneqq \frac{1-(-1)^j}{2}.$$

$$\text{Then,}\quad P_e(i,k) = \sum_{j=i}^{k} \left(\frac{1+(-1)^j}{2}\right) \binom{k}{j} p^j \overline{p}^{k-j},$$
$$P_o(i,k) = \sum_{j=i}^{k} \left(\frac{1-(-1)^j}{2}\right) \binom{k}{j} p^j \overline{p}^{k-j}.$$

Now, for any state $i$, $1 \leq i \leq k$, the transition to state 1 occurs under the following conditions:

If $i$ is even:

1. $S$ fails and $j \geq i-1$ others succeed, $j$ odd.
2. $S$ succeeds and $j \geq i$ others succeed, $j$ even.

$$P_{i,1} = \overline{p} P_o(i-1, k-1) + p P_e(i, k-1).$$

If $i$ is odd:

1. $S$ fails and $j \geq i-1$ others succeed, $j$ even.
2. $S$ succeeds and $j \geq i$ others succeed, $j$ odd.

$$P_{i,1} = \overline{p} P_e(i-1, k-1) + p P_o(i, k-1).$$

Similarly, for any state $i \in \{1, \ldots, k-1\}$, transitioning to state 0 occurs under the following conditions:

If $i$ is even:

1. $S$ fails and $j \geq i$ others succeed, $j$ even.
2. $S$ succeeds and $j \geq i+1$ others succeed, $j$ odd.

$$P_{i,0} = \overline{p}P_e(i, k-1) + pP_o(i+1, k-1).$$

If $i$ is odd:

1. $S$ fails and $j \geq i$ others succeed, $j$ odd.
2. $S$ succeeds and $j \geq i+1$ others succeed, $j$ even.

$$P_{i,0} = \overline{p}P_o(i, k-1) + pP_e(i+1, k-1).$$

In the special case $0 \to 0$, either all fail or an even number of entanglements are created. Hence, $P_{0,0} = P_e(0, k)$. Finally, in the special case of $0 \to 1$, an odd number of entanglements are created, given by $P_{0,1} = P_o(1, k)$.

### 5.2.2 Stationary Distribution

We will show that a stationary distribution exists for $k \geq 3$. The balance equations for the DTMC are

$$\sum_{i=0}^{k-1} \pi_i P_{i,0} = \pi_0, \tag{1}$$

$$\sum_{i=0}^{k} \pi_i P_{i,1} = \pi_1. \tag{2}$$

For any state $i \geq 2$, the balance equations have the form:

$$\pi_{i-1}P_f + \pi_i P_s + \pi_{i+1}P_{(1)} + \cdots + \pi_{i+k-1}P_{(k-1)} = \pi_i, \tag{3}$$

and finally, the normalizing condition is

$$\sum_{i=0}^{\infty} \pi_i = 1. \tag{4}$$

We postulate that $\pi_i = \beta^{i-1}\pi_1$ for $i \geq 2$, with $\beta \in (0, 1)$. Introducing this value of $\pi_1$ in Eq. (3) yields $f(\beta) = 0$, with

$$f(\beta) \coloneqq (\beta p + \overline{p})^{k-1}(p + \beta\overline{p}) - \beta, \tag{5}$$

see A.1 for a proof. To show that $\pi_i = \beta^{i-1}\pi_1$ for $i \geq 2$ is indeed the solution to this system, we must prove that:

1. There exists $\beta \in (0,1)$ satisfying Eq. (5), and that this $\beta$ is unique.

2. Given the solution above, note that both Eqs (1) and (2) can be written in terms of only $\pi_1$ and $\pi_0$. Hence, for the proposed solution to be valid, one of these equations must be redundant, *i.e.*, we must show that Eq. (1) is equivalent to Eq. (2).

In A.2, we prove that the first statement above holds for $k \geq 3$ and in B we show directly that the DTMC is unstable when $k = 2$; thus, the DTMC is stable if and only if $k \geq 3$. The second statement above is proven in A.3. We conclude that the proposed form for $\pi_i$, $i \geq 2$ is valid. Moreover, we can derive expressions for $\pi_0$ and $\pi_1$ in terms of $\beta$. From the normalizing condition (4), we have

$$\pi_0 = 1 - \frac{\pi_1}{1-\beta}. \tag{6}$$

In A.3, we rearranged (1) to look as follows:

$$\sum_{i=1}^{k-1} \beta^i P_{i,0} = \frac{\beta \pi_0}{\pi_1} P_{0,1} \tag{7}$$

and also showed that the left side of Eq. (7) equals

$$\begin{aligned}
&\frac{1}{2}\left[\frac{\beta}{1-\beta} - \frac{2\beta}{1-\beta^2}(p\beta+\overline{p})^{k-1}(p+\overline{p}\beta) - (\overline{p}-p)^k \frac{\beta}{1+\beta}\right] \\
&= \frac{1}{2}\left[\frac{\beta}{1-\beta} - \frac{2\beta^2}{1-\beta^2} - (\overline{p}-p)^k \frac{\beta}{1+\beta}\right] \text{ by Eq. (5),} \\
&= \frac{1}{2}\left[\frac{\beta}{1+\beta} - (\overline{p}-p)^k \frac{\beta}{1+\beta}\right].
\end{aligned}$$

Therefore, Eq. (7) becomes

$$\begin{aligned}
\frac{\beta\pi_0}{\pi_1} P_{0,1} &= \frac{1}{2}\left[\frac{\beta}{1+\beta} - (\overline{p}-p)^k \frac{\beta}{1+\beta}\right], \text{ or} \\
\frac{\pi_0}{\pi_1} P_{0,1} &= \frac{1-(\overline{p}-p)^k}{2(1+\beta)}.
\end{aligned} \tag{8}$$

Next, we compute

$$P_{0,1} = P_o(1,k) = \sum_{i=1}^{k} \frac{1-(-1)^i}{2} \binom{k}{i} p^i \overline{p}^{k-i}$$

$$= \sum_{i=0}^{k} \frac{1-(-1)^i}{2} \binom{k}{i} p^i \overline{p}^{k-i} = \frac{1}{2} - \frac{1}{2}(\overline{p}-p)^k.$$

Substituting this into Eq. (8),

$$\begin{aligned} \frac{\pi_0}{\pi_1}\left(\frac{1-(\overline{p}-p)^k}{2}\right) &= \frac{1-(\overline{p}-p)^k}{2(1+\beta)}, \\ \frac{\pi_0}{\pi_1} &= \frac{1}{1+\beta}, \\ 1-\frac{\pi_1}{1-\beta} &= \frac{\pi_1}{1+\beta} \text{ by Eq. (6)}, \\ \pi_1 &= \frac{1-\beta^2}{2}. \end{aligned} \tag{9}$$

Now, we can compute $\pi_0$ in terms of only $\beta$:

$$\pi_0 = 1 - \frac{\pi_1}{1-\beta} = 1 - \left(\frac{1}{1-\beta}\right)\frac{1-\beta^2}{2} = \frac{1-\beta}{2}.$$

### 5.2.3 Capacity and Qubits in Memory

Let $Q$ represent the number of stored qubits at the switch in steady state. Let $N$ denote the number of end-to-end entangled pairs generated in one time step of the DTMC at steady state. Then the capacity is defined as follows:

$$C = q \sum_{i=0}^{\infty} \pi_i E[N|Q=i].$$

To compute this expression, we consider two separate cases: case 1 is when $i \geq k-1$ and case 2 is when $i < k-1$. In case 1, there can be at most $k-1$ entanglements; the expected number is given by

$$E[N|Q=i \geq k-1] = \sum_{j=0}^{k-1} j \binom{k-1}{j} p^j \overline{p}^{k-1-j} = (k-1)p.$$

For case 2, we can have up to $i+m$ entanglements, where $m = \lfloor \left(\frac{k-i}{2}\right)^+ \rfloor$. The expected number is then given by

$$E[N|Q=i<k-1] = \sum_{j=0}^{i+m} jP(N=j|Q=i \leq k-2).$$

For the sum above, consider first $j \in \{0, \ldots, i\}$. Here, we are looking for the probability that there are fewer new entanglements than the number stored, so the probability that we generate $j$ pairs is given by

$$P(N = j | Q = i,\ i \leq k-2) = \binom{k-1}{j} p^j \overline{p}^{k-1-j}.$$

However, note that the case $j = i$ is a special one: another way we can generate $i$ entanglements is if there are a total of $i+1$ successes from the $k-1$ links that have nothing stored, while $S$ fails. Then, the extra entanglement has no pair, and the total number of pairs generated is still $i$. This is given by

$$i\binom{k-1}{i+1} p^{i+1} \overline{p}^{k-i-1}.$$

Next, we focus on the case where $j \in \{i+1, \ldots, i+m\}$. After the first $i$ successes, there need to be 2 to at most $k-i$ "extra" successes to generate new pairs. Denote the number of these extra successes by the variable $l \in \{2, \ldots, k-i\}$, and the number of new pairs (or BSMs) generated from them is $\lfloor \frac{l}{2} \rfloor$. We can write the second sum as follows:

$$\sum_{l=2}^{k-i} \left( \left\lfloor \frac{l}{2} \right\rfloor + i \right) \binom{k}{i+l} p^{i+l} \overline{p}^{k-i-l}.$$

Combining everything we have learned, we obtain

$$\begin{aligned} C = q \sum_{i=0}^{k-2} \pi_i \Bigg( & \sum_{j=0}^{i} j \binom{k-1}{j} p^j \overline{p}^{k-1-j} + i \binom{k-1}{i+1} p^{i+1} \overline{p}^{k-i-1} \\ & + \sum_{l=2}^{k-i} \left( \left\lfloor \frac{l}{2} \right\rfloor + i \right) \binom{k}{i+l} p^{i+l} \overline{p}^{k-i-l} \Bigg) + q(k-1)p \sum_{i=k-1}^{\infty} \pi_i. \end{aligned} \tag{10}$$

In C, we show that the above evaluates to

$$C = \frac{qkp}{2}. \tag{11}$$

Next, we derive the expected number of qubits stored at the switch, $E[Q]$. This is given by

$$\begin{aligned} E[Q] &= \sum_{i=1}^{\infty} i\pi_i = \pi_1 \sum_{i=1}^{\infty} i\beta^{i-1} = \frac{\pi_1}{\beta} \sum_{i=1}^{\infty} i\beta^i \\ &= \frac{\pi_1}{\beta} \frac{\beta}{(1-\beta)^2} = \frac{1-\beta^2}{2(1-\beta)^2} = \frac{1+\beta}{2(1-\beta)}. \end{aligned} \tag{12}$$

# 6 Comparison of DTMC Model with a CTMC Model

In this section, we compare the DTMC model from this work to a CTMC model studied in [25] and validate the latter for the case of a system with identical links, no quantum state decoherence, and infinite quantum memories at the switch. We first introduce the CTMC model and the analytical results from [25]. Here, the authors model entanglement generation at the link level as a Poisson process with parameter $\mu$ representing the rate of successful Bell pair creation on any link. For the identical-link, bipartite-only switching case, the CTMC is a simple birth-death process, with each state representing the number of stored qubits corresponding to a single link (note that the assumption that any pair of users wish to communicate is also required for the capacity computation). The resulting capacity of the switch is

$$C_{\text{CTMC}} = \frac{qk\mu}{2}.$$

Recall that in the discrete model, the amount of time it takes to successfully generate a link entanglement is $\tau/p$. In the continuous model, the rate of successful entanglement generation is $\mu$, so the time to generate an entanglement is $1/\mu$. Hence, $\tau/p = 1/\mu$ or equivalently, $\mu = p/\tau$. Then, note that the DTMC capacity that we derived in Section 5.2.3 is the capacity per time slot of length $\tau$ seconds. Therefore, in order to make a comparison against the capacity given by the CTMC model, we must perform a unit conversion: divide the discrete capacity by $\tau$ in order to obtain the number of entanglement pairs per *second*, as opposed to per *time slot*. This yields

$$C_{\text{DTMC}} = \frac{qkp}{2\tau} = \frac{qk\mu}{2} = C_{\text{CTMC}}.$$

We conclude that the capacities produced by the DTMC and CTMC models match exactly.

Next, we compare the expected number of qubits in memory in steady state at the switch, $E[Q]$ as predicted by the DTMC and the CTMC models. The CTMC model yields the following expression:

$$E[Q]_{\text{CTMC}} = \frac{k}{2(k-2)}.$$

Note that this expression has no dependence on $\mu$, the link-level successful entanglement generation rate, implying that according to the CTMC model, the expected number of stored qubits in steady state does not depend on

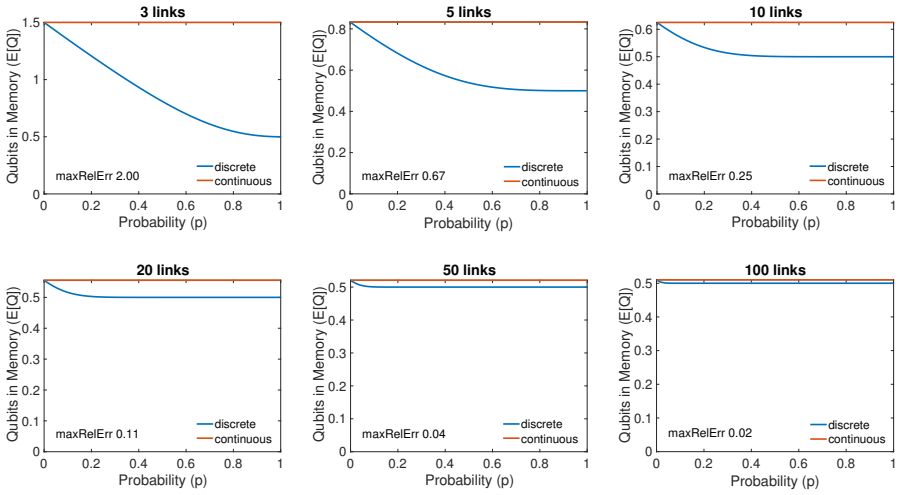



Figure 6: Comparison of the expected number of qubits in memory $E[Q]$ for the DTMC and CTMC models, as the number of links is varied $\in \{3, 5, 10, 20, 50, 100\}$ and for entanglement generation probabilities $p \in (0, 1)$. maxRelErr is the maximum relative error between the discrete and continuous expressions for $E[Q]$.

the probability $p$ of successfully generating a Bell pair on a link. On the other hand, we see from Eq. (12) that $E[Q]$ resulting from the DTMC model *does* depend on $p$, as it is a function of $\beta$. Finally, the DTMC model more accurately describes the buffer occupancy in steady state, at the cost of not being able to produce a closed-form expression for $E[Q]$.

Figure 6 compares numerically the predictions made for $E[Q]$ by the discrete and continuous models, as the number of users $k$ and probability $p$ vary. For each value of $p$ and $k$, we use Eq. (5) to numerically solve for $\beta$. For each value of $k$, we report the maximum relative error, defined as

$$maxRelErr(k) = \max_{p \in (0,1)} \frac{|E[Q]_{\text{DTMC}}(k,p) - E[Q]_{\text{CTMC}}(k,p)|}{E[Q]_{\text{DTMC}}(k,p)},$$

where $E[Q]_{\text{DTMC}}$ and $E[Q]_{\text{CTMC}}$ are the discrete and continuous functions for $E[Q]$, respectively. We observe that the error is largest when $p$ is close to 1. Note that

$$\lim_{p \to 1} f(\beta) = \lim_{p \to 1} (\beta p + \overline{p})^{k-1}(p + \beta\overline{p}) - \beta = \beta^{k-1} - \beta.$$

Since $f(\beta) = 0$, we conclude that as $p \to 1$ and $k \to \infty$, $\beta \to 0$ (note: $\beta = 1$ is always a root of $f(\beta)$, but we always discard this root because it is not in $(0, 1)$). As $\beta \to 0$, $E[Q] \to 1/2$ according to Eq. (12), which is consistent with the numerical observations. Meanwhile, as $k \to \infty$, the continuous $E[Q]$ also approaches $1/2$. We conclude that as $k \to \infty$, $maxRelErr \to 0$, as observed in Figure 6. Also, the largest value of $maxRelErr$ occurs for the lowest value of $k = 3$, when $p \to 1$. But even in this (worst case), although the error is $maxRelErr(3) = 2$, it corresponds to discrete and continuous versions of $E[Q]$ differing by a prediction of only a single qubit.

Finally, both the continuous- and discrete-time Markov chains have stationary distributions if and only if $k \geq 3$. From these analytic and numerical observations, we conclude that the CTMC model is sufficiently accurate so as to be useful for exploring issues such as decoherence, link heterogeneity, and switch buffer constraints.

In [25], the authors introduced CTMCs for systems where the switch has finite-size buffers, links are not necessarily identical, and quantum memory coherence time is finite. Construction and analyses of these models is relatively simple compared to the DTMC model in this paper. Even if one were to introduce a finite buffer into this model, several changes would be required to state transitions and balance equations, resulting in even more complex expressions for the stationary distribution (recall that even in the infinite-buffer case, we must solve the model numerically). Attempting to model decoherence in discrete time would require one to consider all possible combinatorial settings of stored qubit decoherence, further complicating the transition probabilities, but also increasing the *number* of possible transitions from each state. Consider, for instance, state $i$ in Figure 4: each of the existing "backward" transitions $P_{(j)}$, $j \in \{1, \ldots, k-1\}$ would have to be modified based on the number of ways that $l$ qubits can decohere and $m$ new entanglements can be generated such that $l + m = j$, and in addition, extra transitions must be added from state $i$ to states $\{0, 1, \ldots, i - k + 2\}$ because any number of the stored qubits can decohere. This process can become highly cumbersome and prone to mistakes, while CTMCs seem to offer much more in modeling power, albeit incurring an accuracy cost that so far has only been quantified for the simplest variant of the entanglement switching problem.

# 7 Conclusion

We studied an entanglement distribution switch that serves bipartite entangled states to pairs of users connected to the device via dedicated links. Using a DTMC, we studied a simple variant of the problem, wherein the links are identical, the switch has an infinite number of quantum memories, and quantum states do not decohere, although entanglement generation may fail both at the link level and at the end-to-end level. By studying this basic system, we learned that the DTMC model exhibits limitations such that introducing additional complexity to this model, such as finite buffers or quantum state decoherence, makes the resulting model exceedingly difficult to analyze, and therefore may not be the most attractive option for modeling more complex entanglement switching mechanisms.

We derived the capacity of the switch, the expected number of stored qubits at the switch in steady state, and the stability conditions for the system. We also derived the stationary distribution of the DTMC, albeit not in closed form. We compared the results of our analysis to those of an existing CTMC model. We conclude that while the CTMC model is easier to analyze, it is less accurate than the DTMC model. We quantified the discrepancy between the two models for the expected number of stored qubits, and found that in the worst case, the predictions differ by less than one qubit. Hence, we conclude that the CTMC is a suitable model for this particular variant of the problem, but more work is required in order to completely assess the accuracy of CTMC models for more complex switching scenarios. Our work is the first attempt at analyzing a quantum switch using a DTMC, and while the problem formulation is relatively simple, the analysis is non-trivial. Moreover, the expression for switch capacity derived in this paper can be used as an upper bound on the capacity of more complex systems, such as those with non-identical links and where quantum states may decohere. Finally, while our work was initially inspired by entanglement switching, the problem is of independent interest from a queueing-theoretic perspective, and the results can be applied to any stochastic assembly-like queueing system that services two customers/jobs at a time.

# References

[1] C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Theor. Comput. Sci.*, 560(P1):7–11, 2014.

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895, 1993.

[3] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68(5):557, 1992.

[4] C. H. Bennett and S. J. Wiesner. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69(20):2881, 1992.

[5] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81(26):5932, 1998.

[6] A. K. Ekert. Quantum Cryptography Based on Bell's Theorem. *Physical review letters*, 67(6):661, 1991.

[7] Z. Eldredge, M. Foss-Feig, J. A. Gross, S. L. Rolston, and A. V. Gorshkov. Optimal and Secure Measurement Protocols for Quantum Sensor Networks. *Physical Review A*, 97(4):042337, 2018.

[8] F. Ewert and P. van Loock. 3/4-Efficient Bell Measurement with Passive Linear Optics and Unentangled Ancillae. *Physical Review Letters*, 113(14):140403, 2014.

[9] V. Giovannetti, S. Lloyd, and L. Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 306(5700):1330–1336, 2004.

[10] W. P. Grice. Arbitrarily Complete Bell-State Measurement Using Only Linear Optical Elements. *Physical Review A*, 84(4):042331, 2011.

[11] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel. Rate-loss analysis of an efficient quantum repeater architecture. *Physical Review A*, 92(2):022357, 2015.

[12] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel. Rate-loss Analysis of an Efficient Quantum Repeater Architecture. *Physical Review A*, 92(2):022357, 2015.

[13] W. J. Hopp and J. T. Simon. Bounds and heuristics for assembly-like queues. *Queueing Systems (QUESTA)*, 4(2):137–155, 1989.

[14] L. Jiang, J. M. Taylor, A. S. Sørensen, and M. D. Lukin. Distributed quantum computation based on small quantum registers. *Physical Review A*, 76(6):062323, 2007.

[15] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang. Optimal architectures for long distance quantum communication. *Scientific reports*, 6:20463, 2016.

[16] P. Nain, G. Vardoyan, S. Guha, and D. Towsley. On the Analysis of a Multipartite Entanglement Distribution Switch. *Proc. ACM Sigmetrics 2020, in Proceedings of the ACM on Measurement and Analysis of Computing Systems (POMACS)*, 4(2, Article 23), June 2020.

[17] M. A. Nielsen and I. Chuang. Quantum Computation and Quantum Information, 2002.

[18] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8(1):1–15, 2017.

[19] S. Ramachandran and D. Delen. Performance analysis of a kitting process in stochastic assembly systems. *Computers & Operations Research*, 32(3):449–463, 2005.

[20] C. Schmid, N. Kiesel, U. K. Weber, R. Ursin, A. Zeilinger, and H. Weinfurter. Quantum teleportation and entanglement swapping with linear optics logic gates. *New Journal of Physics*, 11(3):033008, 2009.

[21] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken, M. P. Hedges, D. Oblak, C. Simon, W. Sohler, et al. Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control. *Physical Review Letters*, 113(5):053603, 2014.

[22] P. Som, W. E. Wilhelm, and R. L. Disney. Kitting process in a stochastic assembly system. *Queueing Systems (QUESTA)*, 17(3-4):471–490, 1994.

[23] M. Takeoka, S. Guha, and M. M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature communications*, 5(1):1–7, 2014.

[24] R. Van Meter. *Quantum Networking*. John Wiley & Sons, 2014.

[25] G. Vardoyan, S. Guha, P. Nain, and D. Towsley. On the stochastic analysis of a quantum entanglement switch. *ACM SIGMETRICS Performance Evaluation Review*, 47(2):27–29, 2019.

[26] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[27] Q. Zhuang, Z. Zhang, and J. H. Shapiro. Distributed quantum sensing using continuous-variable multipartite entanglement. *Physical Review A*, 97(3):032329, 2018.

[28] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "Event-Ready-Detectors" Bell Experiment via Entanglement Swapping. *Physical Review Letters*, 71:4287–4290, 1993.

# A Stationary Distribution

## A.1 Proof of Eq. (5)

Introducing the value of $\pi_i = \beta^{k-1}\pi_1$ into Eq. (3) yields

$$\beta^{i-1}\pi_1 = \beta^{i-2}\pi_1 P_f + \beta^{i-1}\pi_1 P_s + \beta^{i-1}\pi_1 \sum_{j=1}^{k-1} \beta^j P_{(j)}$$

or equivalently

$$\begin{aligned}\beta &= P_f + \beta P_s + \beta \sum_{j=1}^{k-1} \beta^j P_{(j)} \\ &= \beta(\overline{p}^k + (k-1)p^2\overline{p}^{k-2}) + \beta \sum_{j=1}^{k-1} \binom{k-1}{j} (\beta p)^j \overline{p}^{k-j} \\ &\quad + \frac{1}{\beta} \sum_{j=1}^{k-2} \binom{k-1}{j+1} (\beta p)^{j+2} \overline{p}^{k-j-2} + p\overline{p}^{k-1}. \end{aligned} \tag{13}$$

With $\sum_{j=1}^{k-1} \binom{k-1}{j} (\beta p)^j \overline{p}^{k-j} = \overline{p}\left((\beta p + \overline{p})^{k-1} - \overline{p}^{k-1}\right)$ and

$$\sum_{j=1}^{k-2} \binom{k-1}{j+1} (\beta p)^{j+2} \overline{p}^{k-j-2} = \sum_{i=2}^{k-1} \binom{k-1}{i} (\beta p)^{i+1} \overline{p}^{k-1-i}$$

$$= \beta p \left( (\beta p + \overline{p})^{k-1} - (k-1)\beta p \overline{p}^{k-2} - \overline{p}^{k-1} \right),$$

Eq. (13) becomes

$$\begin{aligned}
\beta &= \beta(\overline{p}^k + (k-1)p^2\overline{p}^{k-2}) + \beta\overline{p}\left( (\beta p + \overline{p})^{k-1} - \overline{p}^{k-1} \right) \\
&\quad + p\left( (\beta p + \overline{p})^{k-1} - (k-1)\beta p\overline{p}^{k-2} - \overline{p}^{k-1} \right) + p\overline{p}^{k-1} \\
&= p\overline{p}^{k-1} + \beta\overline{p}^k + \beta(k-1)p^2\overline{p}^{k-2} + \beta\overline{p}(\beta p + \overline{p})^{k-1} \\
&\quad - \beta\overline{p}^k + p(\beta p + \overline{p})^{k-1} - \beta(k-1)p^2\overline{p}^{k-2} - p\overline{p}^{k-1} \\
&= (\beta p + \overline{p})^{k-1}(p + \beta\overline{p}).
\end{aligned}$$

Hence, $\beta$ satisfies the equation $f(\beta) = 0$ with

$$f(\beta) \coloneqq (\beta p + \overline{p})^{k-1}(p + \beta\overline{p}) - \beta. \qquad \square$$

## A.2 Proof that Eq. (5) has a unique solution in $(0,1)$ when $k \geq 3$

We have

$$f'(\beta) = (k-1)p(\beta p + \overline{p})^{k-2}(p + \beta\overline{p}) + \overline{p}(\beta p + \overline{p})^{k-1} - 1$$

and $f''(\beta)$ is given by

$$\begin{aligned}
&(k-1)(k-2)p^2(\beta p + \overline{p})^{k-3}(p + \beta\overline{p}) + 2(k-1)p\overline{p}(\beta p + \overline{p})^{k-2} \\
&= (k-1)p(\beta p + \overline{p})^{k-3}\left[ (k-2)p + 2(k-1)\overline{p}(\beta p + \overline{p}) \right] > 0.
\end{aligned}$$

This shows that the mapping $\beta \to f'(\beta)$ is strictly increasing in $[0,1]$. On the other hand,

$$f'(0) = (k-1)p^2\overline{p}^{k-2} + \overline{p}^k - 1$$

and $f'(1) = (k-1)p + \overline{p} - 1 = (k-2)p > 0$. Let us show that $f'(0) < 0$. Define $g(p) = (k-1)p^2\overline{p}^{k-2} + \overline{p}^k - 1 = f'(0)$. We find

$$g'(p) = -\overline{p}^{k-3}(p^2k^2 + 2p(1-2k) + k).$$

Define $h(p) = p^2k^2 + 2p(1-2k) + k$ so that $g'(p) = -\overline{p}^{k-3}h(p)$. We have $h'(p) = 2(pk^2 + 1 - 2k)$, which vanishes for $p = p_0 \coloneqq (2k-1)/k^2$. Also, $h''(p) = 2k^2 > 0$. We deduce from this that $h(p)$ decreases in $[0, p_0)$ and increases in $(p_0, 1]$. Therefore, $h(p)$ is minimized in $[0,1]$ for $p = p_0$. We have $h(p_0) = (-(2k-1)^2 + k^3)/k^2$ which is easily seen to be strictly positive

for all $k \geq 3$. This shows that $h(p) > 0$ for $p \in [0,1]$, which implies that $g'(p) < 0$ for $p \in [0,1]$, so that $g(p) < g(0) = 0$ for $p \in (0,1]$ and, finally, $f'(0) < 0$.

From $f'(0) < 0$, $f'(1) > 0$ and the fact that the continuous mapping $\beta \to f'(\beta)$ is strictly increasing in $[0,1]$, we deduce that there exists $\beta_0 \in (0,1)$ such that $f'(\beta) < 0$ for $\beta \in [0, \beta_0)$, $f'(\beta_0) = 0$ and $f'(\beta) > 0$ for $\beta \in (\beta_0, 1]$. This in turn shows that $\beta \to f(\beta)$ is strictly decreasing in $[0, \beta_0)$ and strictly increasing in $(\beta_0, 1]$. But since $f(0) > 0$ and $f(1) = 0$, this implies that $f$ has a unique zero in $(0,1)$. This zero is actually located in $(0, \beta_0)$. □

### A.3 Equivalence of Eqs (1) and (2)

We start by rearranging (1):

$$\begin{aligned}
\sum_{i=0}^{k-1} \pi_i P_{i,0} &= \pi_0, \\
\sum_{i=1}^{k-1} \pi_i P_{i,0} &= \pi_0 (1 - P_{0,0}), \\
\pi_1 \sum_{i=1}^{k-1} \beta^{i-1} P_{i,0} &= \pi_0 P_{0,1}, \\
\sum_{i=1}^{k-1} \beta^i P_{i,0} &= \frac{\beta \pi_0}{\pi_1} P_{0,1}.
\end{aligned}$$

Then, we rearrange (2) in a similar fashion:

$$\begin{aligned}
\sum_{i=0}^{k} \pi_i P_{i,1} &= \pi_1, \\
\pi_0 P_{0,1} + \pi_1 \sum_{i=1}^{k} \beta^{i-1} P_{i,1} &= \pi_1, \\
\pi_0 P_{0,1} &= \pi_1 \left( 1 - \frac{1}{\beta} \sum_{i=1}^{k} \beta^i P_{i,1} \right), \\
\frac{\beta \pi_0}{\pi_1} P_{0,1} &= \beta - \sum_{i=1}^{k} \beta^i P_{i,1}.
\end{aligned}$$

Hence, to show that one of (1) and (2) is redundant, it suffices to show that

$$\sum_{i=1}^{k-1} \beta^i P_{i,0} = \beta - \sum_{i=1}^{k} \beta^i P_{i,1}, \tag{14}$$

or equivalently,

$$\sum_{i=1}^{k-1} \beta^i (P_{i,0} + P_{i,1}) + \beta^k P_{k,1} = \beta. \tag{15}$$

Before we continue, we derive a few useful expressions. The first is as follows:

$$P_e(i, k-1) + P_o(i, k-1) = \sum_{j=i}^{k-1} \binom{k-1}{j} p^j \overline{p}^{k-1-j}.$$

Next, we have

$$P_e(i, k-1) - P_o(i, k-1) = \sum_{j=i}^{k-1} \binom{k-1}{j} p^j \overline{p}^{k-1-j} (-1)^j.$$

Finally,

$$P_o(i, k-1) - P_e(i, k-1) = -\sum_{j=i}^{k-1} \binom{k-1}{j} p^j \overline{p}^{k-1-j} (-1)^j.$$

Now, consider the left side of Eq. (14): $\sum_{i=1}^{k-1} \beta^i P_{i,0}$ is equal to

$$\begin{aligned}
&\sum_{i=1}^{k-1} \beta^i \left[ \left( \frac{1 + (-1)^i}{2} \right) (\overline{p} P_e(i, k-1) + p P_o(i+1, k-1)) \right. \\
&\quad \left. + \left( \frac{1 - (-1)^i}{2} \right) (\overline{p} P_o(i, k-1) + p P_e(i+1, k-1)) \right] \\
&= \frac{\overline{p}}{2} \sum_{i=1}^{k-1} \beta^i \left[ \sum_{j=i}^{k-1} \binom{k-1}{j} p^j \overline{p}^{k-1-j} (1 + (-1)^i (-1)^j) \right] \\
&\quad + \frac{p}{2} \sum_{i=1}^{k-2} \beta^i \left[ \sum_{j=i+1}^{k-1} \binom{k-1}{j} p^j \overline{p}^{k-1-j} (1 - (-1)^i (-1)^j) \right]
\end{aligned}$$

$$= \frac{\overline{p}}{2} \sum_{j=1}^{k-1} \binom{k-1}{j} p^j \overline{p}^{k-1-j} \sum_{i=1}^{j} \beta^i (1 + (-1)^i (-1)^j)$$
$$+ \frac{p}{2} \sum_{j=2}^{k-1} \binom{k-1}{j} p^j \overline{p}^{k-1-j} \sum_{i=1}^{j-1} \beta^i (1 - (-1)^i (-1)^j)$$
$$= \frac{1}{2} \left[ \frac{\beta}{1-\beta} - \frac{2\beta}{1-\beta^2} (p\beta + \overline{p})^{k-1} (p + \overline{p}\beta) - (\overline{p} - p)^k \frac{\beta}{1+\beta} \right].$$

Next, we look at $\sum_{i=1}^{k-1} \beta^i P_{i,1}$, which is equal to

$$\sum_{i=1}^{k-1} \beta^i \left[ \left( \frac{1 + (-1)^i}{2} \right) (\overline{p} P_o(i-1, k-1) + p P_e(i, k-1)) \right.$$
$$\left. + \left( \frac{1 - (-1)^i}{2} \right) (\overline{p} P_e(i-1, k-1) + p P_o(i, k-1)) \right]$$
$$= \frac{\overline{p}}{2} \sum_{i=1}^{k-1} \beta^i \left[ \sum_{j=i-1}^{k-1} \binom{k-1}{j} p^j \overline{p}^{k-1-j} \left(1 - (-1)^i (-1)^j\right) \right]$$
$$+ \frac{p}{2} \sum_{i=1}^{k-1} \beta^i \left[ \sum_{j=i}^{k-1} \binom{k-1}{j} p^j \overline{p}^{k-1-j} \left(1 + (-1)^i (-1)^j\right) \right]$$
$$= \beta\overline{p}((\beta p + \overline{p})^{k-1} - (\beta p)^{k-1}) + \frac{1}{2} \left( \frac{\beta}{1-\beta} - \frac{2\beta}{1-\beta^2} (p\beta + \overline{p})^k + \frac{\beta}{1+\beta} (\overline{p} - p)^k \right).$$

Summing these two expressions, we obtain $\sum_{i=1}^{k-1} \beta^i (P_{i,0} + P_{i,1})$,

$$\frac{\beta}{1-\beta} - \frac{\beta}{1-\beta} (p\beta + \overline{p})^{k-1} (p + \overline{p}\beta) - \beta\overline{p}(\beta p)^{k-1}.$$

Next, we compute

$$P_{k,1} = \left( \frac{1 + (-1)^k}{2} \right) \overline{p} P_o(k-1, k-1) + \left( \frac{1 - (-1)^k}{2} \right) \overline{p} P_e(k-1, k-1)$$
$$= \overline{p} \left( \left( \frac{1 + (-1)^k}{2} \right) \left( \frac{1 - (-1)^{k-1}}{2} \right) p^{k-1} + \left( \frac{1 - (-1)^k}{2} \right) \left( \frac{1 + (-1)^{k-1}}{2} \right) p^{k-1} \right)$$
$$= \overline{p} p^{k-1}.$$

Finally, the left side of Eq. (15) becomes

$$\sum_{i=1}^{k-1} \beta^i (P_{i,0} + P_{i,1}) + \beta^k P_{k,1} =$$
$$\frac{\beta}{1-\beta} - \frac{\beta}{1-\beta}(p\beta + \overline{p})^{k-1}(p + \overline{p}\beta) - \overline{p}\beta^k p^{k-1} + \beta^k \overline{p} p^{k-1}$$
$$= \frac{\beta}{1-\beta} - \frac{\beta}{1-\beta}(p\beta + \overline{p})^{k-1}(p + \overline{p}\beta).$$

Recall from (15) that the expression above must equal to $\beta$. Using Eq. (5), we know that

$$(p\beta + \overline{p})^{k-1}(p + \overline{p}\beta) = \beta,$$

and therefore,

$$\sum_{i=1}^{k-1} \beta^i (P_{i,0} + P_{i,1}) + \beta^k P_{k,1} = \frac{\beta}{1-\beta} - \frac{\beta^2}{1-\beta} = \beta.$$

□

# B Instability When $k = 2$

When $k = 2$, Eq. (3) becomes

$$\pi_{i-1} P_f + \pi_i P_s + \pi_{i+1} P_{(1)} = \pi_i, \tag{16}$$

for $i \geq 2$, and where $P_f = p\overline{p}$, $P_s = \overline{p}^2 + p^2$, and $P_{(1)} = p\overline{p}$. Summing these equations yields

$$p\overline{p} \sum_{i=1}^{\infty} \pi_i + (\overline{p}^2 + p^2) \sum_{i=2}^{\infty} \pi_i + p\overline{p} \sum_{i=3}^{\infty} \pi_i = \sum_{i=2}^{\infty} \pi_i,$$

or equivalently,

$$p\overline{p}(\pi_1 + \pi_2) + (\overline{p}^2 + p^2)\pi_2 + (2p\overline{p} + \overline{p}^2 + p^2) \sum_{i=3}^{\infty} \pi_i = \pi_2 + \sum_{i=3}^{\infty} \pi_i,$$

and since $1 - 2p\overline{p} - \overline{p}^2 - p^2 = 0$, the above equation becomes

$$p\overline{p}(\pi_1 + \pi_2) + (\overline{p}^2 + p^2)\pi_2 = \pi_2,$$

which simplifies to $\pi_1 = \pi_2$. Substituting this relation into (16) when $i = 2$ yields $\pi_3 = \pi_2 = \pi_1$, and iterating this procedure over the remaining $i$'s yields $\pi_1 = \pi_i$, $\forall\ i \geq 2$.

From Eq. (1), we have

$$\pi_0 = \pi_0 P_{0,0} + \pi_1 P_{1,0}, \tag{17}$$

where $P_{0,0} = \overline{p}^2 + p^2$ and $P_{1,0} = p\overline{p}$, so that Eq. (17) is actually

$$\pi_0 = \pi_0(\overline{p}^2 + p^2) + \pi_1 p\overline{p}$$

and

$$\pi_0 = \pi_1 \frac{p\overline{p}}{1 - \overline{p}^2 - p^2}. \tag{18}$$

Using the normalizing condition, along with (18) yields

$$\pi_1 \frac{p\overline{p}}{1 - \overline{p}^2 - p^2} + \sum_{i \geq 1} \pi_i = 1. \tag{19}$$

Since $\pi_1 = \pi_i$, $\forall i \geq 2$, the only solution of (19) is $\pi_i = 0$, for all $i \geq 1$ (and $\pi_\infty = 1$), which proves instability for $k = 2$. □

# C Proof of Capacity

For simplicity, let us first derive $C$ with the assumption that $q = 1$. Since $q$ simply scales the capacity, we will multiply the resulting expression by $q$ at the end. Consider the first term of Eq. (10):

$$\begin{aligned}
\sum_{i=0}^{k-2} \pi_i \sum_{j=0}^{i} j \binom{k-1}{j} p^j \overline{p}^{k-1-j} &= \sum_{j=1}^{k-2} j \binom{k-1}{j} p^j \overline{p}^{k-1-j} \sum_{i=j}^{k-2} \pi_i \\
&= \sum_{j=1}^{k-2} j \binom{k-1}{j} p^j \overline{p}^{k-1-j} \pi_1 \sum_{i=j}^{k-2} \beta^{i-1} \\
&= \frac{\pi_1}{\beta} \sum_{j=1}^{k-2} j \binom{k-1}{j} p^j \overline{p}^{k-1-j} \left( \sum_{i=0}^{k-2} \beta^i - \sum_{i=0}^{j-1} \beta^i \right) \\
&= \frac{\pi_1}{\beta} \sum_{j=1}^{k-2} j \binom{k-1}{j} p^j \overline{p}^{k-1-j} \left( \frac{1 - \beta^{k-1}}{1 - \beta} - \frac{1 - \beta^j}{1 - \beta} \right)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{\pi_1}{\beta}\sum_{j=1}^{k-2} j\binom{k-1}{j}p^j\overline{p}^{k-1-j}\left(\frac{\beta^j-\beta^{k-1}}{1-\beta}\right)\\
&= \frac{\pi_1}{\beta}\sum_{j=1}^{k-1} j\binom{k-1}{j}p^j\overline{p}^{k-1-j}\left(\frac{\beta^j-\beta^{k-1}}{1-\beta}\right)\\
&= \frac{\pi_1}{\beta(1-\beta)}\Big((k-1)(\beta p+\overline{p})^{k-2}\beta p-\beta^{k-1}(k-1)p\Big)\\
&= \frac{\pi_1(k-1)p}{\beta(1-\beta)}\left((\beta p+\overline{p})^{k-2}\beta-\beta^{k-1}\right).
\end{aligned}
$$

Next, keeping in mind that $k-1\geq 2$, the last term of Eq. (10) is

$$
\begin{aligned}
(k-1)p\sum_{i=k-1}^{\infty}\pi_i &= \frac{(k-1)p\pi_1}{\beta}\sum_{i=k-1}^{\infty}\beta^i\\
&= \frac{(k-1)p\pi_1}{\beta}\left(\sum_{i=0}^{\infty}\beta^i-\sum_{i=0}^{k-2}\beta^i\right)\\
&= \frac{(k-1)p\pi_1}{\beta}\left(\frac{1}{1-\beta}-\frac{1-\beta^{k-1}}{1-\beta}\right)=\frac{(k-1)p\pi_1}{\beta}\frac{\beta^{k-1}}{1-\beta}.
\end{aligned}
$$

Hence, so far,

$$
\begin{aligned}
C &= \sum_{i=0}^{k-2}\pi_i\left(i\binom{k-1}{i+1}p^{i+1}\overline{p}^{k-i-1}+\sum_{l=2}^{k-i}\left(\left\lfloor\frac{l}{2}\right\rfloor+i\right)\binom{k}{i+l}p^{i+l}\overline{p}^{k-i-l}\right)\\
&\quad+\frac{\pi_1(k-1)p}{\beta(1-\beta)}\left((\beta p+\overline{p})^{k-2}\beta-\beta^{k-1}\right)+\frac{(k-1)p\pi_1}{\beta}\frac{\beta^{k-1}}{1-\beta}\\
&= \frac{\pi_1(k-1)p}{(1-\beta)}(\beta p+\overline{p})^{k-2}+\sum_{i=0}^{k-2}\pi_i\Bigg(i\binom{k-1}{i+1}p^{i+1}\overline{p}^{k-i-1}\\
&\quad+\sum_{l=2}^{k-i}\left(\left\lfloor\frac{l}{2}\right\rfloor+i\right)\binom{k}{i+l}p^{i+l}\overline{p}^{k-i-l}\Bigg).
\end{aligned}
\tag{20}
$$

Next in Eq. (20) we have the term

$$
\begin{aligned}
\sum_{i=0}^{k-2}\pi_i i\binom{k-1}{i+1}p^{i+1}\overline{p}^{k-i-1} &= \pi_1\sum_{i=1}^{k-2}\beta^{i-1}i\binom{k-1}{i+1}p^{i+1}\overline{p}^{k-i-1}\\
&= \pi_1\sum_{j=2}^{k-1}\beta^{j-2}(j-1)\binom{k-1}{j}p^j\overline{p}^{k-j}
\end{aligned}
$$

$$= \frac{\overline{p}\pi_1}{\beta^2}\left((k-1)(\beta p+\overline{p})^{k-2}\beta p - (\beta p+\overline{p})^{k-1} + \overline{p}^{k-1}\right).$$

Substituting this into Eq. (20), we have

$$\begin{aligned}
C &= \sum_{i=0}^{k-2}\pi_i \sum_{l=2}^{k-i}\left(\left\lfloor\frac{l}{2}\right\rfloor + i\right)\binom{k}{i+l}p^{i+l}\overline{p}^{k-i-l} + \frac{\pi_1(k-1)p}{(1-\beta)}(\beta p+\overline{p})^{k-2} \\
&\quad + \frac{\overline{p}\pi_1}{\beta^2}\left((k-1)(\beta p+\overline{p})^{k-2}\beta p - (\beta p+\overline{p})^{k-1} + \overline{p}^{k-1}\right) \\
&= \sum_{i=0}^{k-2}\pi_i \sum_{l=2}^{k-i}\left(\left\lfloor\frac{l}{2}\right\rfloor + i\right)\binom{k}{i+l}p^{i+l}\overline{p}^{k-i-l} \\
&\quad + \frac{\overline{p}\pi_1}{\beta^2}\left(\overline{p}^{k-1} - (\beta p+\overline{p})^{k-1}\right) + \pi_1(k-1)p(\beta p+\overline{p})^{k-2}\frac{(\beta p+\overline{p})}{\beta(1-\beta)} \\
&= \sum_{i=0}^{k-2}\pi_i \sum_{l=2}^{k-i}\left(\left\lfloor\frac{l}{2}\right\rfloor + i\right)\binom{k}{i+l}p^{i+l}\overline{p}^{k-i-l} \\
&\quad + \frac{\overline{p}\pi_1}{\beta^2}\left(\overline{p}^{k-1} - (\beta p+\overline{p})^{k-1}\right) + \pi_1(k-1)p\frac{(\beta p+\overline{p})^{k-1}}{\beta(1-\beta)}. \qquad (21)
\end{aligned}$$

Consider the remaining sum above. Let $m = i + l$. Then

$$\begin{aligned}
&\sum_{i=0}^{k-2}\pi_i \sum_{l=2}^{k-i}\left(\left\lfloor\frac{l}{2}\right\rfloor + i\right)\binom{k}{i+l}p^{i+l}\overline{p}^{k-i-l} = \sum_{m=2}^{k}\binom{k}{m}p^m\overline{p}^{k-m}\left(\sum_{i=0}^{m-2}\pi_i\left(\left\lfloor\frac{m-i}{2}\right\rfloor + i\right)\right) \\
&= \sum_{m=2}^{k}\binom{k}{m}p^m\overline{p}^{k-m}\left(\sum_{i=0}^{m}\pi_i\left(\left\lfloor\frac{m-i}{2}\right\rfloor + i\right) - (m-1)\pi_{m-1} - m\pi_m\right) := S. \qquad (22)
\end{aligned}$$

The inner sum above can be rewritten as follows:

$$\begin{aligned}
\sum_{i=0}^{m}\pi_i\left(\left\lfloor\frac{m-i}{2}\right\rfloor + i\right) &= \sum_{i=0}^{m}\pi_i\left(i + \left(\frac{m-i}{2}\right)\frac{1+(-1)^{m-i}}{2} + \left(\frac{m-i-1}{2}\right)\frac{1-(-1)^{m-i}}{2}\right) \\
&= \sum_{i=0}^{m}\pi_i\left(i + \frac{m-i}{2} - \frac{1}{2}\frac{(1-(-1)^{m-i})}{2}\right) \\
&= \sum_{i=0}^{m}\pi_i\left(\frac{2m-1}{4} + \frac{i}{2} + \frac{(-1)^{m-i}}{4}\right) \\
&= \frac{\pi_1}{\beta}\sum_{i=1}^{m}\beta^i\left(\frac{2m-1}{4} + \frac{i}{2} + \frac{(-1)^{m-i}}{4}\right) + \pi_0\left(\frac{2m-1+(-1)^m}{4}\right)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{\pi_1}{\beta}\left(\frac{2m-1}{4}\left(\frac{1-\beta^{m+1}}{1-\beta}-1\right)+\frac{1}{2}\sum_{i=1}^{m} i\beta^i+\frac{(-1)^m}{4}\left(\frac{1-(-\beta)^{m+1}}{1+\beta}-1\right)\right)\\
&\quad+\pi_0\left(\frac{2m-1+(-1)^m}{4}\right)\\
&= \pi_1\left(\frac{2m-1}{4}\left(\frac{1-\beta^m}{1-\beta}\right)+\frac{1}{2}\frac{(m\beta^{m+1}-(m+1)\beta^m+1)}{(1-\beta)^2}+\frac{\beta^m-(-1)^m}{4(1+\beta)}\right)\\
&\quad+\pi_0\left(\frac{2m-1+(-1)^m}{4}\right).
\end{aligned}
$$

Now, we can use the fact that $\pi_0+\pi_1/(1-\beta)=1$ to obtain

$$
\pi_1\frac{2m-1}{4}\frac{1}{1-\beta}+\frac{2m-1}{4}\pi_0=\frac{2m-1}{4}.
$$

Using the same relation, we have

$$
\frac{(-1)^m}{4}\left(\pi_0-\frac{\pi_1}{1+\beta}\right)=\frac{(-1)^m}{4}\left(1-\frac{2\pi_1}{1-\beta^2}\right).
$$

Therefore,

$$
\begin{aligned}
\sum_{i=0}^{m}\pi_i\left(\left\lfloor\frac{m-i}{2}\right\rfloor+i\right) &= \pi_1\left(\frac{2m-1}{4}\left(\frac{-\beta^m}{1-\beta}\right)+\frac{m\beta^{m+1}-(m+1)\beta^m+1}{2(1-\beta)^2}+\frac{\beta^m}{4(1+\beta)}\right)\\
&\quad+\frac{2m-1}{4}+\frac{(-1)^m}{4}\left(1-\frac{2\pi_1}{1-\beta^2}\right)\\
&= -\pi_1\beta^m\frac{\beta}{(1-\beta)^2(1+\beta)}-\pi_1\frac{m\beta^m}{1-\beta}+\frac{m}{2}+\frac{(-1)^m}{4}\left(1-\frac{2\pi_1}{1-\beta^2}\right)+\frac{\pi_1}{2(1-\beta)^2}-\frac{1}{4}.
\end{aligned}
$$

From Eq. (9), we know that $\pi_1=(1-\beta^2)/2$. Using this,

$$
\sum_{i=0}^{m}\pi_i\left(\left\lfloor\frac{m-i}{2}\right\rfloor+i\right)=-\pi_1\beta^m\frac{\beta}{(1-\beta)^2(1+\beta)}-\pi_1\frac{m\beta^m}{1-\beta}+\frac{m}{2}+\frac{\pi_1}{2(1-\beta)^2}-\frac{1}{4}.
$$

Next, we can write

$$
\begin{aligned}
&\sum_{i=0}^{m}\pi_i\left(\left\lfloor\frac{m-i}{2}\right\rfloor+i\right)-(m-1)\pi_{m-1}-m\pi_m\\
&\quad=\frac{-\pi_1\beta^m\beta}{(1-\beta)^2(1+\beta)}-\pi_1\frac{m\beta^m}{1-\beta}+\frac{m}{2}+\frac{\pi_1}{2(1-\beta)^2}-\frac{1}{4}-\frac{\pi_1}{\beta}m\beta^m\left(\frac{1}{\beta}+1\right)+\frac{\pi_1}{\beta^2}\beta^m\\
&\quad=\frac{m}{2}+\frac{\pi_1}{2(1-\beta)^2}-\frac{1}{4}+\pi_1\beta^m\left(\frac{1}{\beta^2}-\frac{\beta}{(1-\beta)^2(1+\beta)}\right)-\frac{\pi_1 m\beta^m}{\beta^2(1-\beta)}.
\end{aligned}
$$

Hence, Eq. (22) becomes

$$
\begin{aligned}
S &= \sum_{m=2}^{k} \binom{k}{m} p^m \overline{p}^{k-m} \left( \pi_1 \beta^m \left( \frac{1}{\beta^2} - \frac{\beta}{(1-\beta)^2(1+\beta)} \right) - \frac{\pi_1 m \beta^m}{\beta^2(1-\beta)} + \frac{m}{2} + \frac{\pi_1}{2(1-\beta)^2} - \frac{1}{4} \right) \\
&= \pi_1 \left( \frac{1}{\beta^2} - \frac{\beta}{(1-\beta)^2(1+\beta)} \right) (p\beta + \overline{p})^k - \frac{\pi_1 kp\beta (p\beta + \overline{p})^{k-1}}{\beta^2(1-\beta)} \\
&\quad - \overline{p}^k \left( \pi_1 \left( \frac{1}{\beta^2} - \frac{\beta}{(1-\beta)^2(1+\beta)} \right) + \frac{\pi_1}{2(1-\beta)^2} - \frac{1}{4} \right) \\
&\quad - kp\overline{p}^{k-1} \left( \pi_1 \beta \left( \frac{1}{\beta^2} - \frac{\beta}{(1-\beta)^2(1+\beta)} \right) - \frac{\pi_1 \beta}{\beta^2(1-\beta)} + \frac{1}{2} + \frac{\pi_1}{2(1-\beta)^2} - \frac{1}{4} \right) \\
&\quad + \frac{kp}{2} + \frac{\pi_1}{2(1-\beta)^2} - \frac{1}{4} \\
&= \pi_1 \left( \frac{1}{\beta^2} - \frac{\beta}{(1-\beta)^2(1+\beta)} \right) (p\beta + \overline{p})^k - \frac{\pi_1 kp (p\beta + \overline{p})^{k-1}}{\beta(1-\beta)} - \overline{p}^k \left( \frac{\pi_1}{\beta^2} + \frac{\pi_1}{2(1-\beta^2)} - \frac{1}{4} \right) \\
&\quad - kp\overline{p}^{k-1} \left( \frac{-\pi_1}{2(1-\beta^2)} + \frac{1}{4} \right) + \frac{kp}{2} + \frac{\pi_1}{2(1-\beta)^2} - \frac{1}{4}.
\end{aligned}
$$

Substituting $\pi_1 = (1-\beta^2)/2$ above and simplifying yields

$$
S = \pi_1 \left( \frac{1}{\beta^2} - \frac{\beta}{(1-\beta)^2(1+\beta)} \right) (p\beta + \overline{p})^k - \frac{\pi_1 kp}{\beta(1-\beta)} (p\beta + \overline{p})^{k-1} + \frac{kp}{2} + \frac{\pi_1}{2(1-\beta)^2} - \frac{1}{4} - \overline{p}^k \frac{\pi_1}{\beta^2}.
$$

Finally, substituting this result into Eq. (21), $C$ becomes

$$
\begin{aligned}
C &= \frac{\overline{p}\pi_1}{\beta^2} \left( \overline{p}^{k-1} - (\beta p + \overline{p})^{k-1} \right) + \pi_1 (k-1) p \frac{(\beta p + \overline{p})^{k-1}}{\beta(1-\beta)} \\
&\quad + \pi_1 \left( \frac{1}{\beta^2} - \frac{\beta}{(1-\beta)^2(1+\beta)} \right) (p\beta + \overline{p})^k \\
&\quad - \frac{\pi_1 kp}{\beta(1-\beta)} (p\beta + \overline{p})^{k-1} + \frac{kp}{2} + \frac{\pi_1}{2(1-\beta)^2} - \frac{1}{4} - \overline{p}^k \frac{\pi_1}{\beta^2} \\
&= \frac{-\pi_1 (\beta p + \overline{p})^{k-1} (\overline{p}\beta + p)}{(1-\beta)^2(1+\beta)} + \frac{kp}{2} + \frac{\pi_1}{2(1-\beta)^2} - \frac{1}{4}.
\end{aligned}
$$

We know from Eq. (5) that

$$
(\beta p + \overline{p})^{k-1} (p + \beta \overline{p}) - \beta = 0.
$$

Using this above, we obtain

$$\begin{aligned} C &= -\frac{\pi_1 \beta}{(1-\beta)^2(1+\beta)} + \frac{kp}{2} + \frac{\pi_1}{2(1-\beta)^2} - \frac{1}{4} \\ &= \frac{\pi_1}{2(1-\beta^2)} - \frac{1}{4} + \frac{kp}{2}. \end{aligned}$$

Recall that $\pi_1 = (1-\beta^2)/2$. Hence,

$$\begin{aligned} C &= \frac{1-\beta^2}{2}\frac{1}{2(1-\beta^2)} - \frac{1}{4} + \frac{kp}{2}, \\ C &= \frac{kp}{2}. \end{aligned}$$

Finally, recall that we earlier assumed $q = 1$. Removing this assumption, we obtain

$$C = \frac{qkp}{2}. \qquad \square$$