Mathematical Modeling of Quantum Repeaters Chains

Lorenzo La Corte

June 13, 2024

Mathematical Background

Convolution

Convolution is a fundamental mathematical operation used to combine two functions to produce a third function, which represents how the shape of one function is modified by the other.

For two discrete functions a and b, the convolution $a * b$ is defined as:

$$(a * b)(z) = \sum_{x=0}^{z} a(x) \cdot b(z - x) \tag{1}$$

Convolution of two Probability Distributions In the context of probability distributions, if X and Y are independent random variables with probability distribution functions p_X and p_Y, their sum $Z = X + Y$ has a probability distribution function p_Z given by the convolution of p_X and p_Y:

$$p_Z(z) = \sum_{x=0}^{z} p_X(x) \cdot p_Y(z - x) \tag{2}$$

Thus, convolution is used to determine the probability distribution of the sum of independent random variables by combining their individual probability distributions.

Example Consider this simple example. Let X and Y discrete independent random variables.

The probability distribution $\Pr(Z = z)$ of the random variable $Z = X + Y$ is computed as follows:

x	$\Pr(X=x)$	y	$\Pr(Y=y)$	z	$\Pr(Z=z)$	Derivation of $\Pr(Z=z)$
0	0.2	0	0.3	0	0.06	$0.2 \cdot 0.3$
1	0.5	1	0.4	1	0.23	$0.2 \cdot 0.4 + 0.5 \cdot 0.3$
2	0.3	2	0.3	2	0.35	$0.2 \cdot 0.3 + 0.5 \cdot 0.4 + 0.3 \cdot 0.3$
				3	0.27	$0.5 \cdot 0.3 + 0.3 \cdot 0.4$
				4	0.09	$0.3 \cdot 0.3$

(3)

Note that $\Pr(Z = z)$ has five elements (all the possible sums), and it is valid as its probabilities sum to 1.

The convolution operator $*$ is associative, meaning that for any three functions a, b, and c:

$$(a * b) * c = a * (b * c) \tag{4}$$

Random Variables

In this section, we fix notation on random variables and operations on them.

Most random variables in the context of quantum repeaters

- are discrete,
- have as domain a subset of nonnegative integers.

PDF Let X be such a random variable, then its probability distribution function is a map

$$p_X : x \mapsto \Pr(X = x) \tag{5}$$

which describes the probability that its outcome will be $x \in \{0, 1, 2, \ldots\}$.

CDF Equivalently, X is described by its cumulative distribution function

$$\Pr(X \leq x) = \sum_{y=0}^{x} \Pr(X = y), \tag{6}$$

which is transformed to the probability distribution function as

$$\Pr(X = x) = \Pr(X \leq x) - \Pr(X \leq x - 1). \tag{7}$$

Independent Random Variables Two random variables X and Y are independent if

$$\Pr(X = x \text{ and } Y = y) = \Pr(X = x) \cdot \Pr(Y = y) \tag{8}$$

for all x and y in the domain.

Copies of a Random Variable By a *copy* of X, we mean a fresh random variable which is independent from X and identically distributed (i.i.d.). We will denote a copy by a superscript in parentheses. For example, $X^{(1)}$, $X^{(142)}$ and $X^{(A)}$ are all copies of X.

The mean of X is denoted by

$$E[X] = \sum_{x=0}^{\infty} \Pr(X = x) \cdot x \tag{9}$$

and can equivalently be computed as

$$E[X] = \sum_{x=1}^{\infty} \Pr(X \geq x). \tag{10}$$

Function of Random Variables If f is a function which takes two nonnegative integers as input, then the random variable $f(X, Y)$ has probability distribution function defined as

$$\Pr(f(X, Y) = z) := \sum_{\substack{x=0,y=0 \\ f(x,y)=z}}^{\infty} \Pr(X = x \text{ and } Y = y). \tag{11}$$

Sum of Random Variables An example of such a function is addition.

Define $Z := X + Y$ where X and Y are independent, then the probability distribution p_Z of Z is given by

$$p_Z(z) = \Pr(Z = z) = \sum_{\substack{x=0,y=0 \\ x+y=z}}^{\infty} \Pr(X = x \text{ and } Y = y). \tag{12}$$

But since $y = z - x$ this is equivalent to

$$p_Z(z) = \Pr(Z = z) = \sum_{x=0}^{z} \Pr(X = x \text{ and } Y = z - x) \tag{13}$$

$$= \sum_{x=0}^{z} \Pr(X = x) \cdot Pr(Y = z - x) \tag{14}$$

$$= \sum_{x=0}^{z} p_X(x) \cdot p_Y(z - x) \tag{15}$$

which is the convolution of the distributions p_X and p_Y, denoted as $p_Z = p_X * p_Y$ (see convolution).

Since convolution operator $*$ is associative, writing $a * b * c$ is well-defined, for functions a, b, c from the nonnegative integers to the real numbers (see associativity of convolution). In general, **the probability distribution of sums of independent random variables equals the convolutions of their individual probability distribution functions**.

Geometric Distribution

The Geometric Distribution is a discrete probability distribution that models the number of trials needed to achieve the first success in a sequence of independent Bernoulli trials, each with the same success probability p.

Probability Distribution Function (PDF)

The Probability Distribution Function (PDF) of a Geometric Distribution gives the probability that the first success occurs on the t-th trial. It is defined as:

$$\Pr(T = t) = p(1 - p)^{t-1} \quad \text{for} \quad t \in \{1, 2, 3, \ldots\}, \tag{16}$$

where: - T is the random variable representing the trial number of the first success, - p is the probability of success on each trial, - $(1 - p)$ is the probability of failure on each trial.

This formula expresses that the first $t - 1$ trials must be failures (each occurring with probability $1 - p$), and the t-th trial must be a success (with probability p).

Cumulative Distribution Function (CDF)

The Cumulative Distribution Function (CDF) of a Geometric Distribution gives the probability that the first success occurs on or before the t-th trial. It is defined as:

$$\Pr(T \leq t) = 1 - (1-p)^t. \tag{17}$$

Derivation of the CDF This is the derivation of the CDF of a Geometric Distribution, from its PDF

$$\begin{aligned}
\Pr(T \leq t) &= 1 - \Pr(T > t) && (18)\\
&= 1 - \sum_{k=t+1} \Pr(T = k) && (19)\\
&= 1 - \left\{ p(1-p)^t + p(1-p)^{t+1} + p(1-p)^{t+2} + \dots \right\} && (20)\\
&= 1 - p(1-p)^t \sum_{k=0} (1-p)^k && (21)\\
&= 1 - (1-p)^t \sum_{k=0} p(1-p)^k && (22)\\
&= 1 - (1-p)^t. && (23)
\end{aligned}$$

This CDF formula indicates the probability that the first success occurs within the first t trials.

Mathematical Model for Waiting Time and Fidelity

We derive expressions for the waiting time and fidelity of the first generated end-to-end link in the repeater chain protocol.

We derive a recursive definition for the random variable T_n, which **represents the waiting time in a $2n$-segment repeater chain**.

Extending this definition to the Werner parameter W_n of the pair, which stands in one-to-one correspondence to its fidelity F_n using the equation:

$$F_n = \frac{1 + 3W_n}{4}. \tag{24}$$

Note that all operations in the repeater chain protocols we study

- Entanglement generation over a single hop
- Distillation
- Swapping

take a duration that is a multiple of L_0/c, the time to send information over a single segment.

For this reason, it is common to denote the waiting time in **discrete units** of L_0/c, which is a convention we comply with for T_n.

Regarding cutoffs, ...

Heraldeld Entanglement Generation

Waiting Time for Elementary Entanglement

In modeling the random variable T_n, which represents the waiting time in a 2^n segment repeater chain, we can reason by induction.

The base case T_0 **is the waiting time for the generation of elementary entanglement**.

Since we model the generation of single-hop entanglement by attempts which succeed with a fixed probability p_{gen}, the waiting time T_0 is a discrete random variable (in units of L_0/c) which follows a geometric distribution with probability distribution given by

$$\Pr(T_0 = t) = p_{\text{gen}}(1 - p_{\text{gen}})^{t-1} \quad \text{for} \quad t \in \{1, 2, 3, \ldots\}. \tag{25}$$

For what follows, it will be more convenient to specify T_0 by its cumulative distribution function (CDF), which is given by

$$\Pr(T_0 \leq t) = 1 - (1 - p_{\text{gen}})^t. \tag{26}$$

Werner Parameter for Elementary Entanglement

...

Entanglement Swapping

Once we have generated elementary entanglement, we can use it to create entanglement over longer distances by entanglement swapping.

We defined T_0 as the waiting time for the generation of elementary entanglement, and our base for the induction.

We now define our inductive step assuming that we have found an expression for T_n and we want to construct T_{n+1}.

In order to perform the entanglement swap to produce a single $(2^n + 1)$-hop link, a node needs to wait for the production of two (2^n)-hop links, one on each side.

Denote the waiting time for the pairs by $T_n^{(A)}$ and $T_n^{(B)}$, both of which are i.i.d. with T_n, as they are copies of it.

The time until both pairs are available is now given by

$$M_n := \max(T_n^{(A)}, T_n^{(B)}) \tag{27}$$

which is distributed according to

$$\Pr(M_n \leq t) = \Pr(T_n^{(A)} \leq t \text{ and } T_n^{(B)} \leq t) = \Pr(T_n \leq t)^2. \tag{28}$$