

A Qubit about Quantum Computing

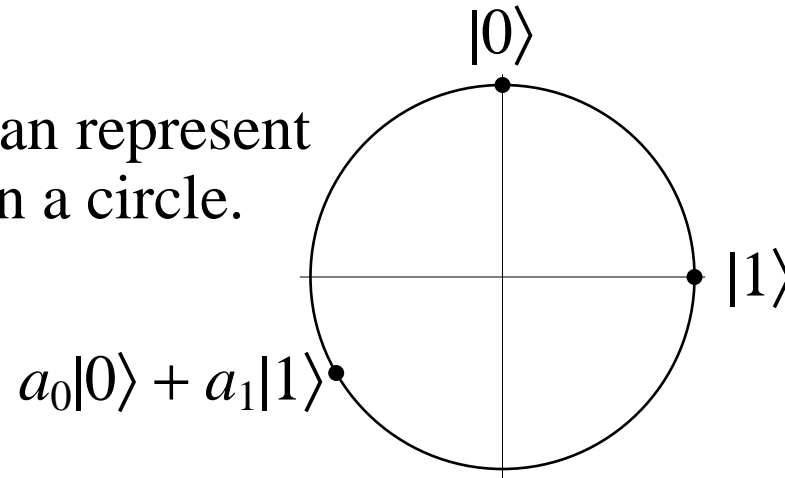
Mike Speciner

What is a qubit?

A linear combination of $|0\rangle$ and $|1\rangle$, specified by two complex amplitudes, the sum of whose squared absolute values is 1.

When we measure a qubit whose state is $a_0|0\rangle + a_1|1\rangle$, we read 0 with probability $|a_0|^2$ and we read 1 with probability $|a_1|^2$.

If the amplitudes are real, we can represent the state of a qubit by a point on a circle.

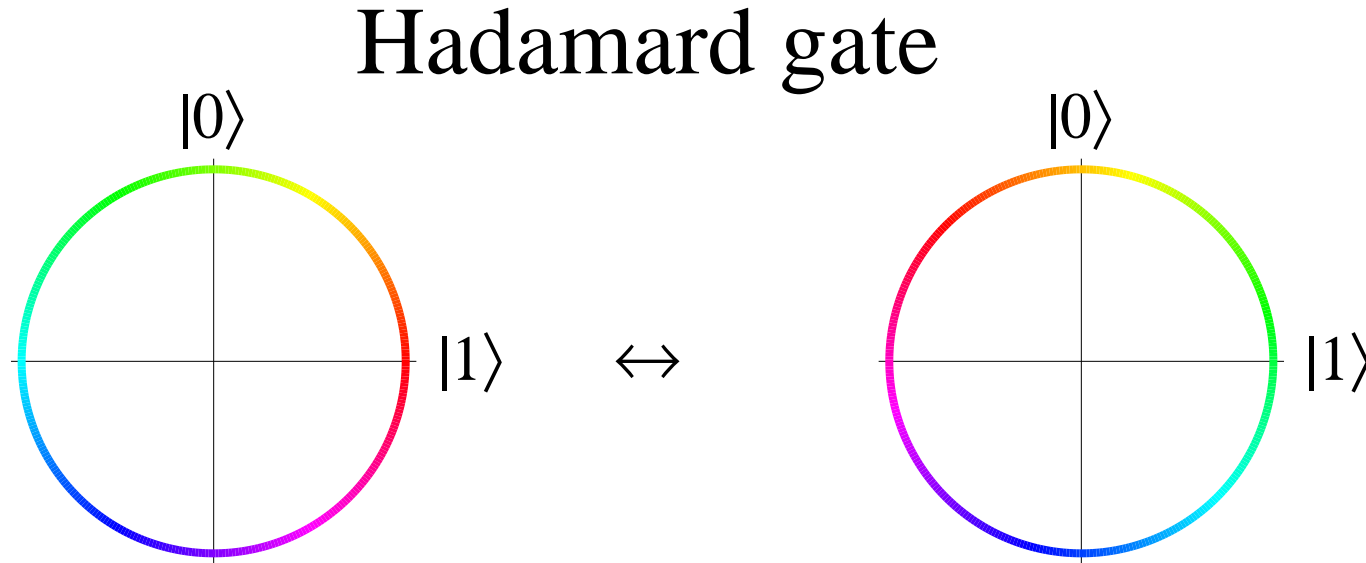


What about a collection of n qubits?

A linear combination of the $N = 2^n$ classical possibilities ($|0\cdots 0\rangle$ through $|1\cdots 1\rangle$), specified by N complex amplitudes, the sum of whose squared absolute values is 1.

So, the state of a collection of n qubits can be represented as a point on a $2N$ -dimensional sphere. The real and imaginary parts of the amplitude of each classical bit configuration comprise two of the $2N$ coordinates.

Quantum operations (known as quantum gates) map one state to another. They must be linear, which means that a quantum gate is completely specified by what it does to each classical bit configuration. These two criteria mean that a quantum gate performs a rigid motion of the sphere of possible states—a rotation and/or a reflection.



The Hadamard gate negates the amplitude of $|1\rangle$, reflecting across the $|0\rangle$ -axis, then rotates 45° from $|0\rangle$ toward $|1\rangle$. In general, applying a Hadamard gate to each of n qubits, results in the old amplitude of $|x\rangle$ contributing to the new amplitude of $|y\rangle$ with a factor of $(-1)^{\text{bitcount}(x\&y)}/\sqrt{N}$, where x and y are bit configurations, and $N = 2^n$.

Grover's algorithm

Purpose: to find an n -bit value (the *target*) satisfying some criterion.

Idea: initialize n qubits so that each of the N classical bit configurations has the same amplitude. Iteratively perform a sequence of operations which raises the probability of the target state until that probability is near 1. Then read the n qubits.

Grover's alternates between two planes (T for target and M for mean) of the $2N$ -dimensional sphere. Switching between planes is accomplished by applying a Hadamard gate to each of the n qubits. In both planes, the amplitudes of the classical bit configurations are all real. In Plane T, the square of the amplitude of each classical state is the probability of reading the corresponding bit configuration. In Plane M, the amplitude of state $|0\cdots 0\rangle$ is proportional to the mean amplitude of all the classical states when in Plane T.

The following pages graphically show the steps of Grover's algorithm, first when there's a single target, and then when there are three. The top of each page graphs the amplitude of each classical bit configuration, the bottom shows the state in each plane.

Grover's Algorithm, Single Target

We start (in Plane M) in state $|0\cdots 0\rangle$ with every qubit initialized to 0, so with probability 1 of reading 0.

(next page) We apply a Hadamard gate to every qubit, moving the state to Plane T and resulting in the amplitude of every bit configuration being $1/\sqrt{N}$.

We repeat the following sequence of four steps until the probability of reading the target value is maximized.

(next page) Using an additional qubit and a sequence of quantum operations, we evaluate the target criterion and negate the amplitude of the passing bit configuration(s).

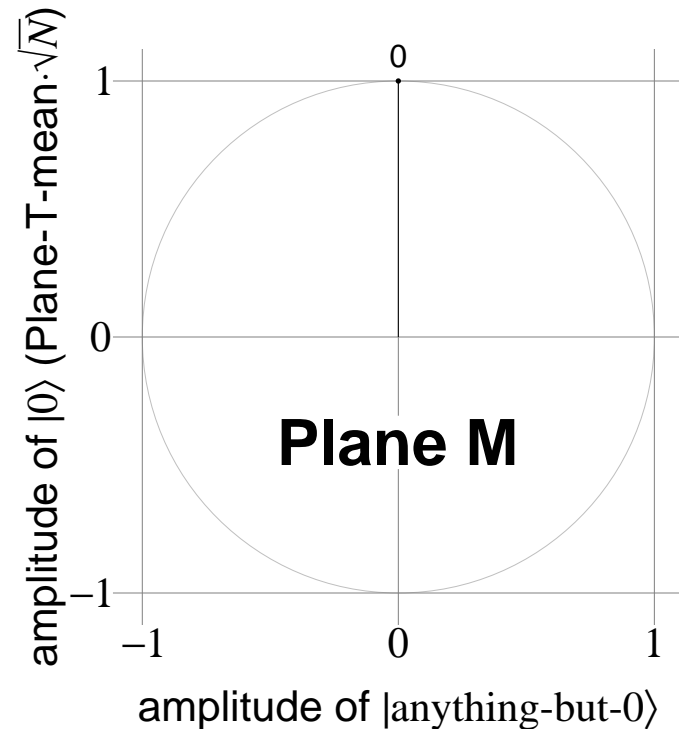
We then reflect across the mean amplitude with a sequence of operations:

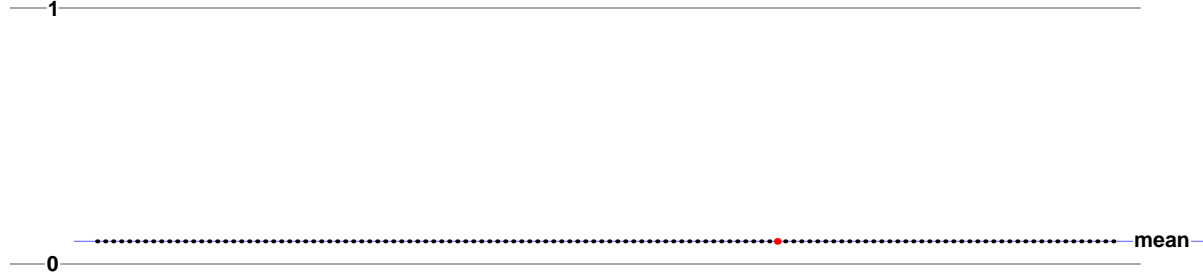
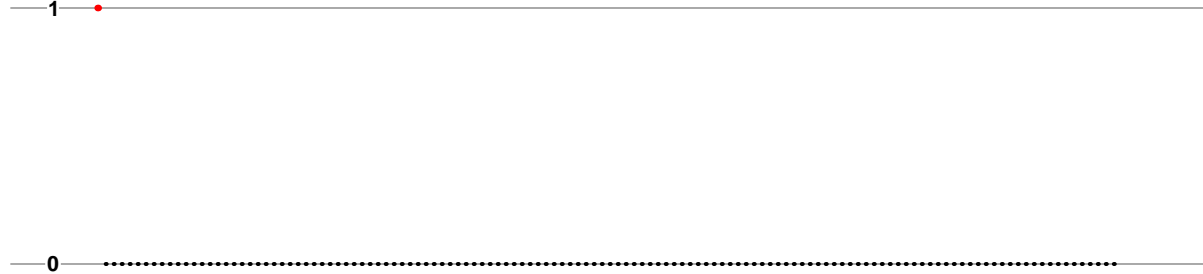
(next page) We apply a Hadamard gate to every qubit, moving back to Plane M. The amplitude of $|0\cdots 0\rangle$ will be \sqrt{N} times the mean amplitude in Plane T.

(next page) We negate the amplitude of every bit configuration other than $|0\cdots 0\rangle$.

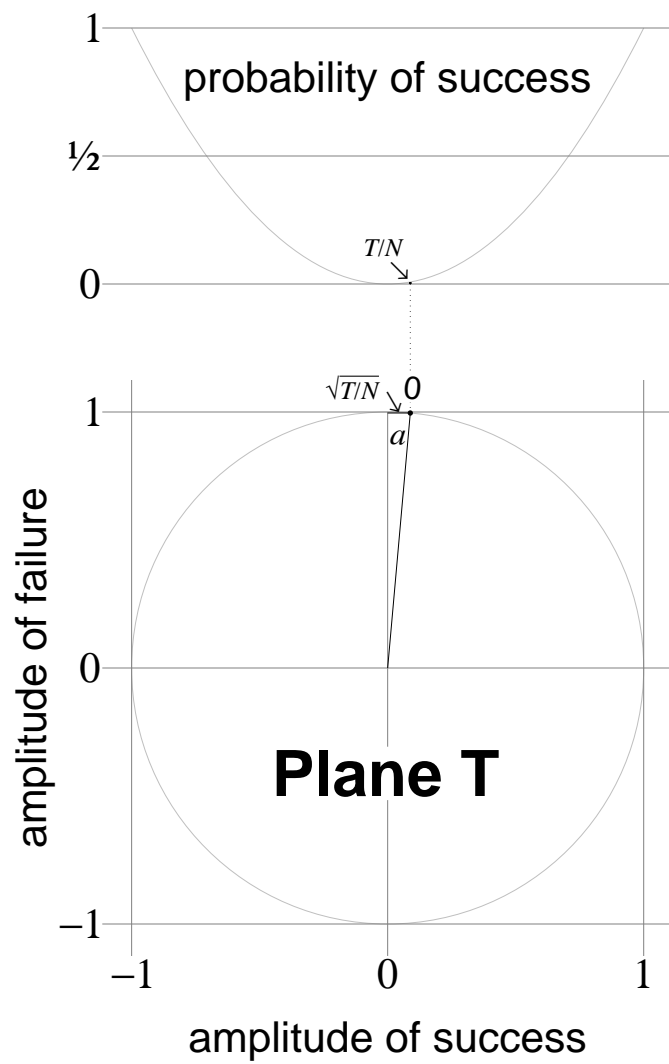
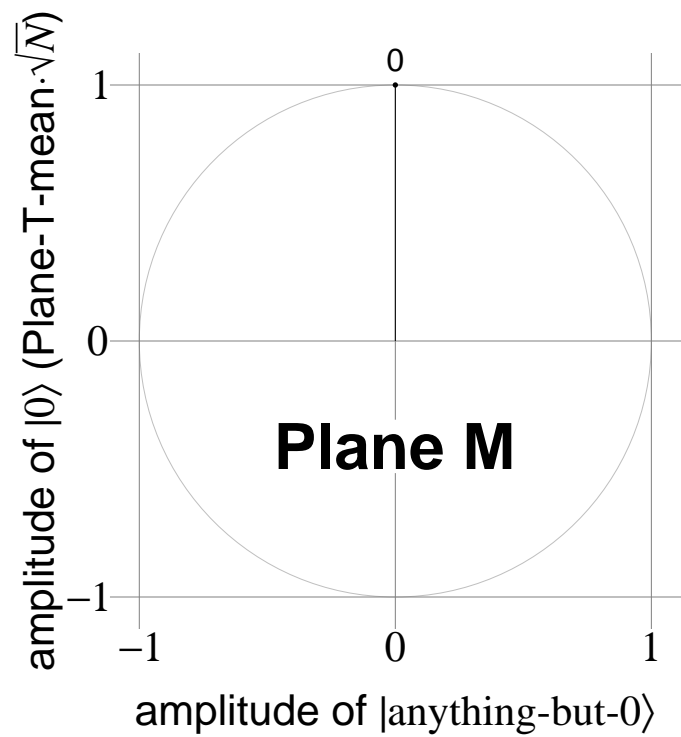
(next page) We apply a Hadamard gate to every qubit, moving back to Plane T.

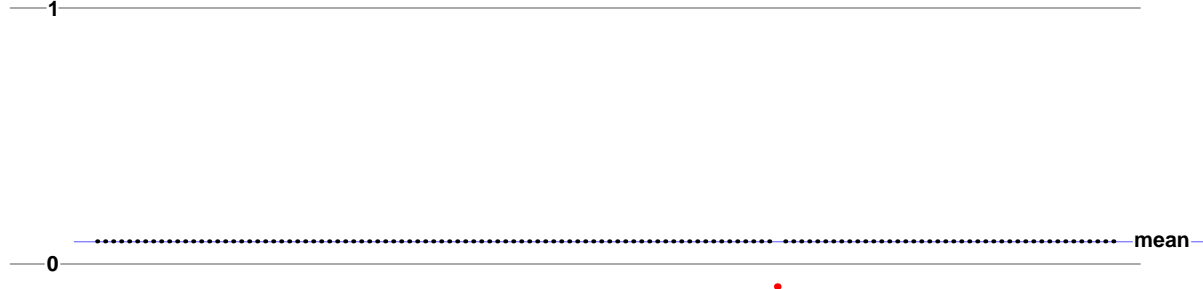
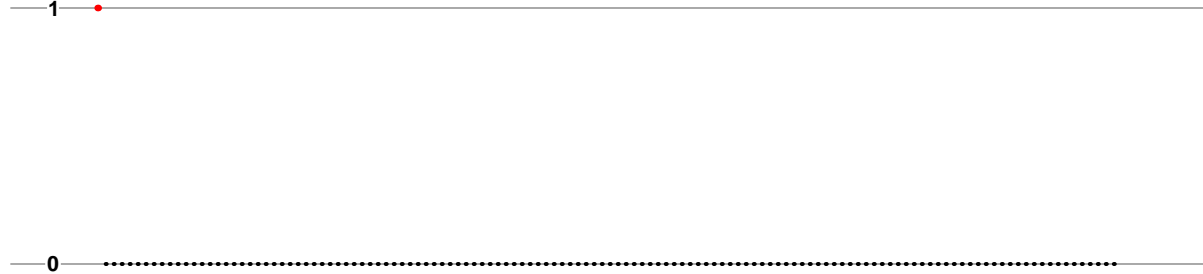
$$N = 128, \quad T = 1$$



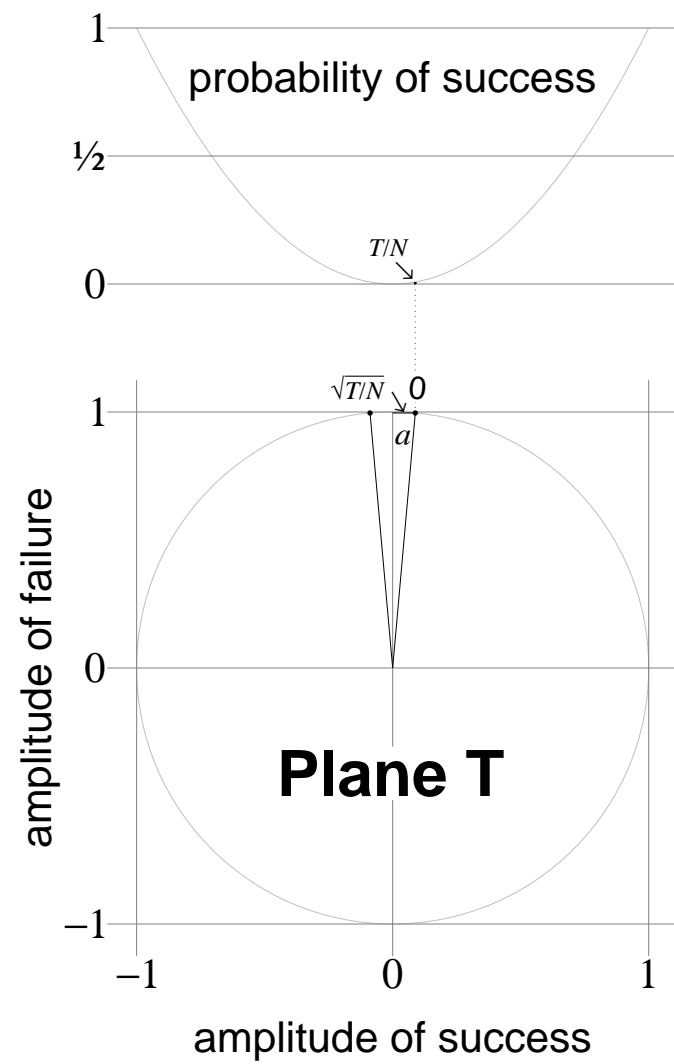
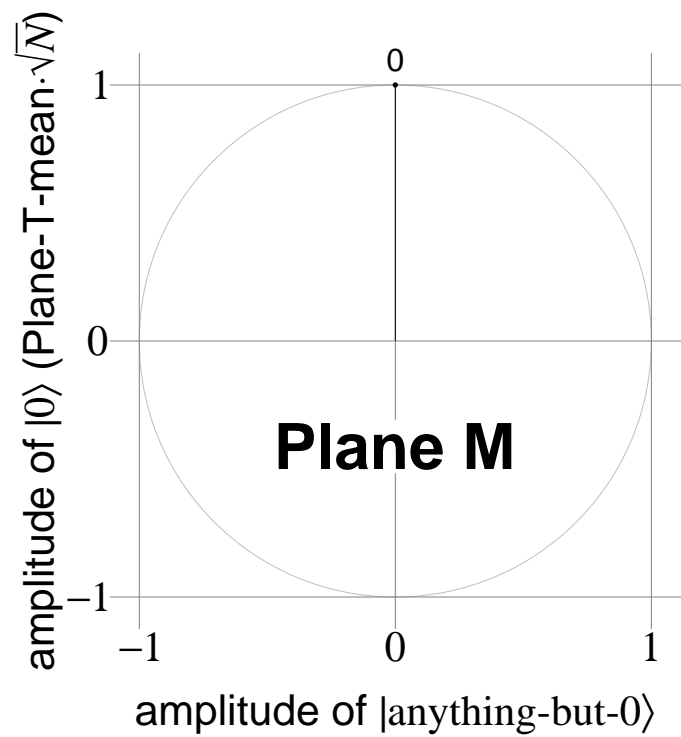


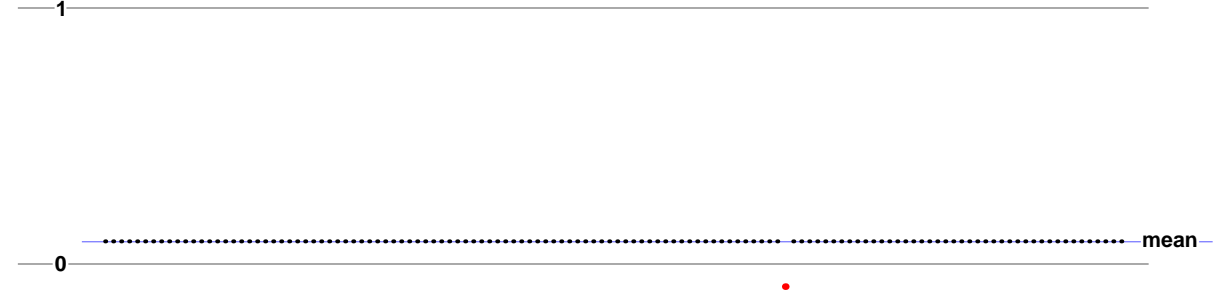
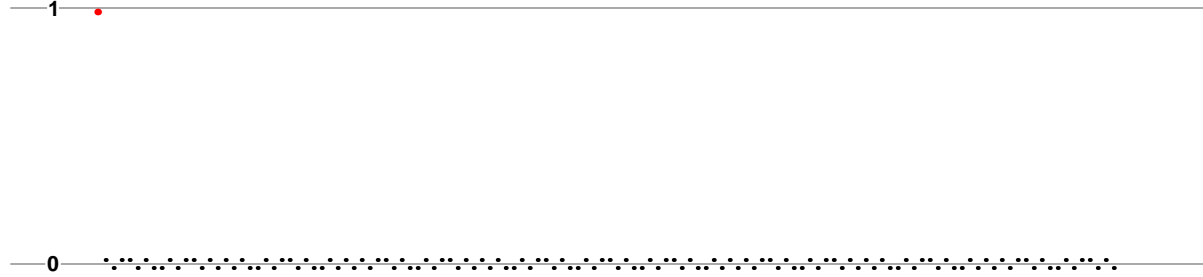
$$N = 128, \quad T = 1$$



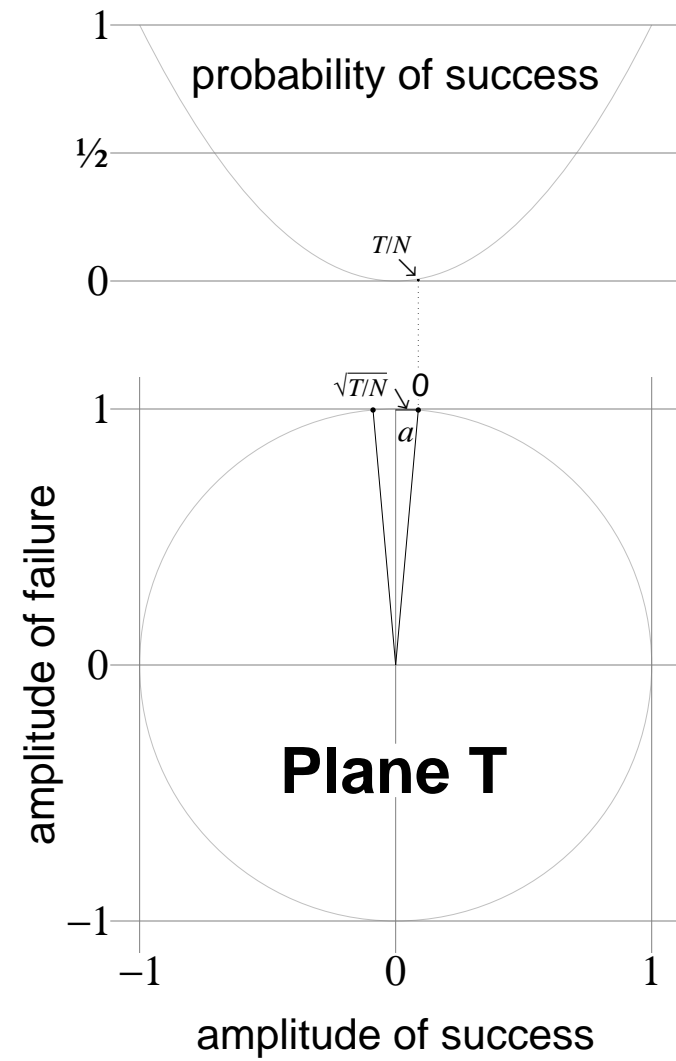
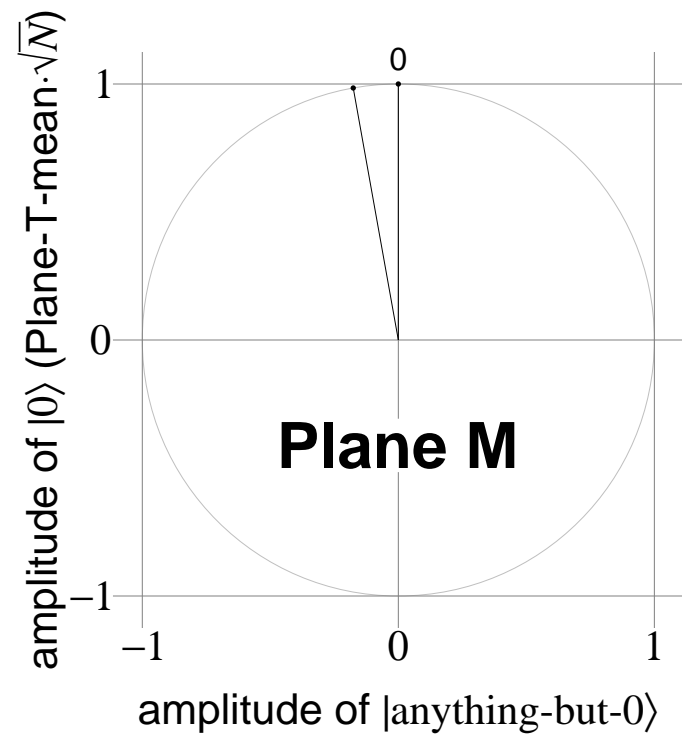


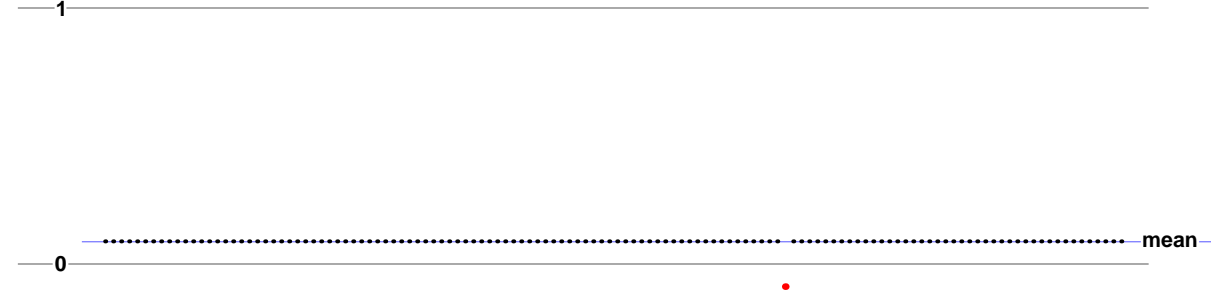
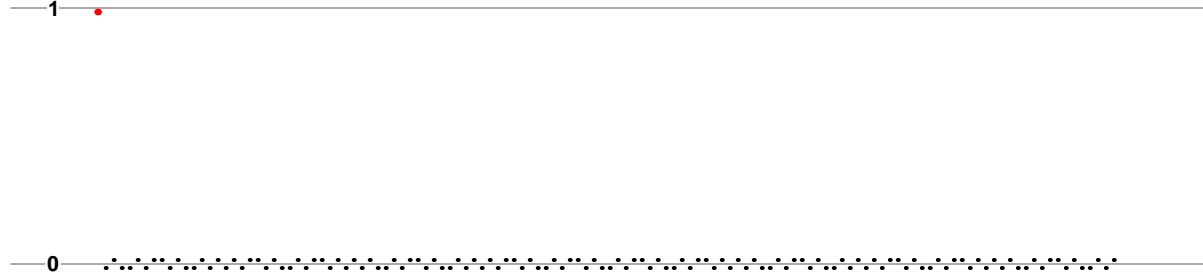
$$N = 128, T = 1$$



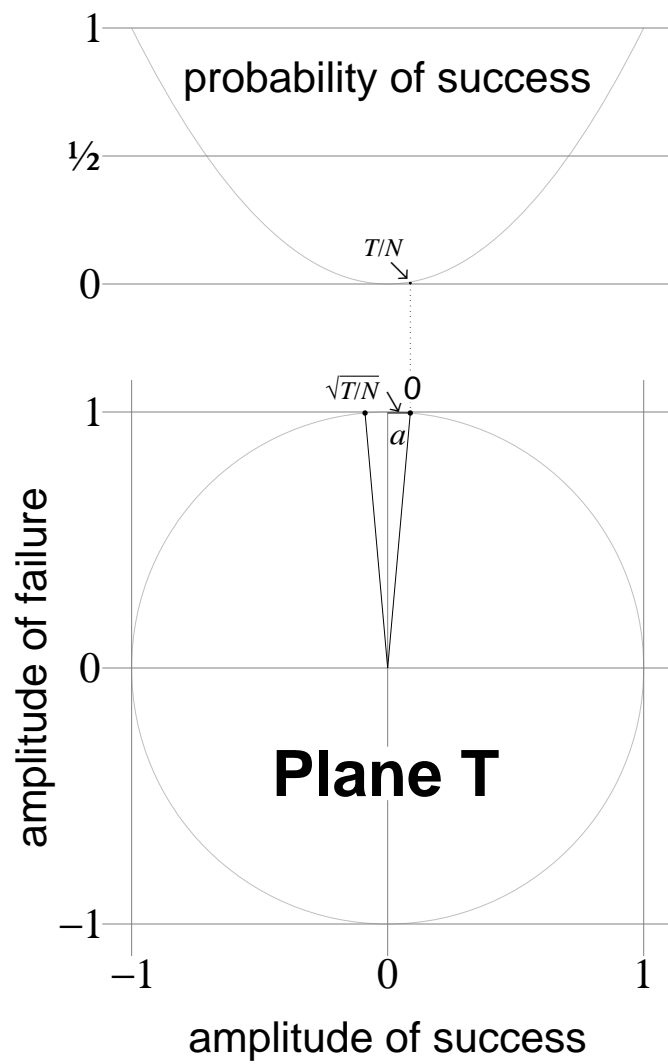
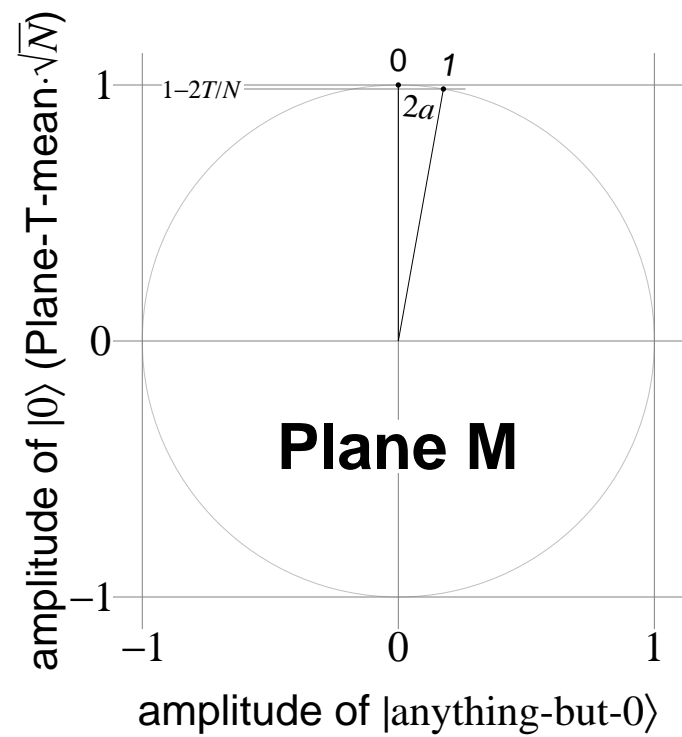


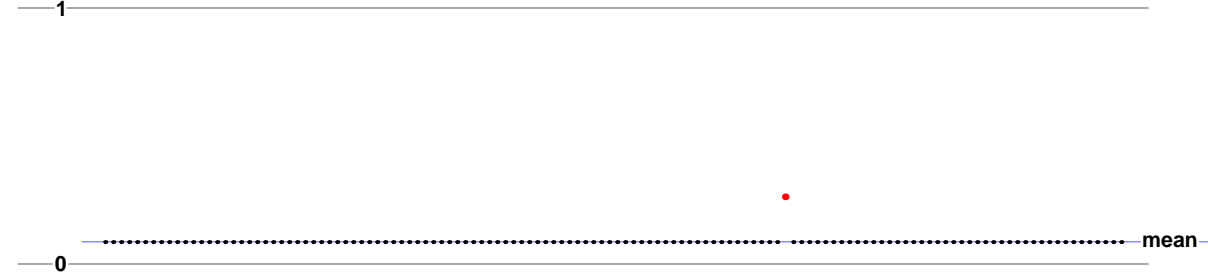
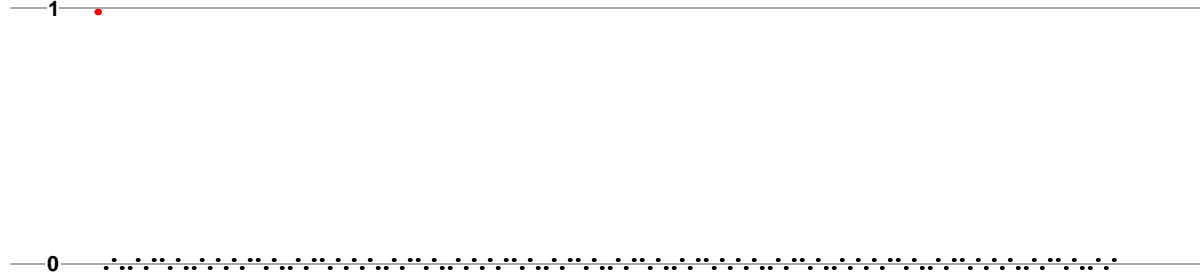
$$N = 128, T = 1$$



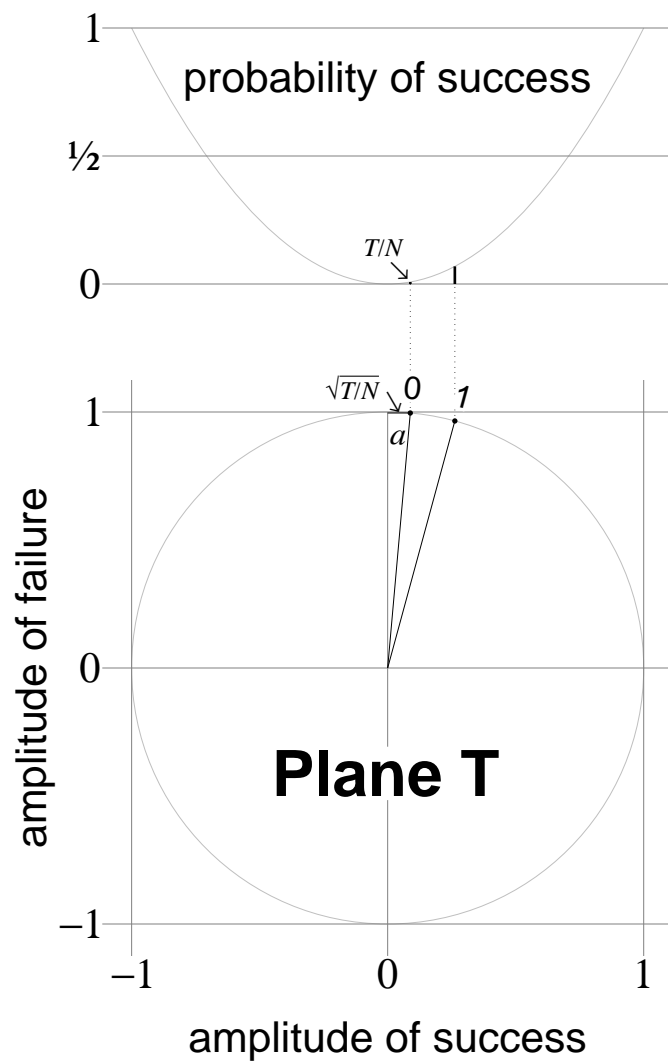
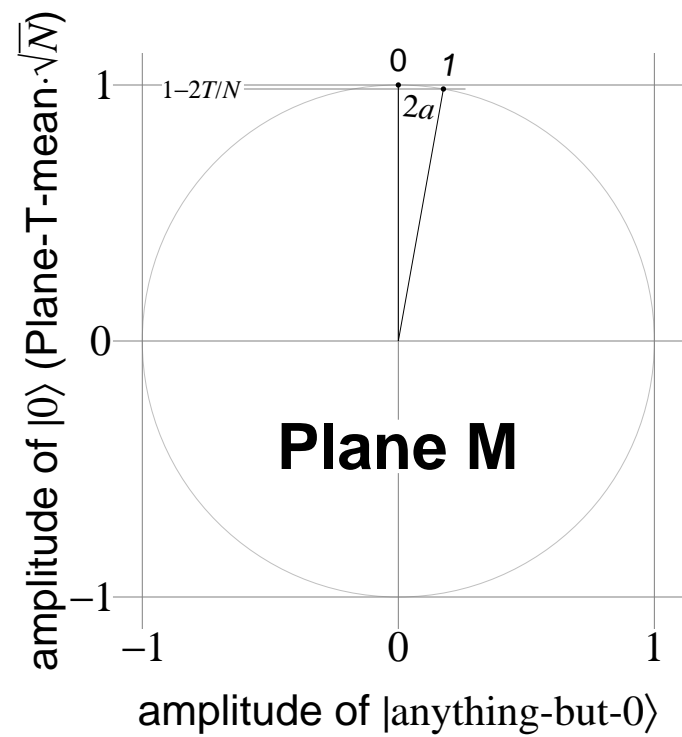


$$N = 128, T = 1$$

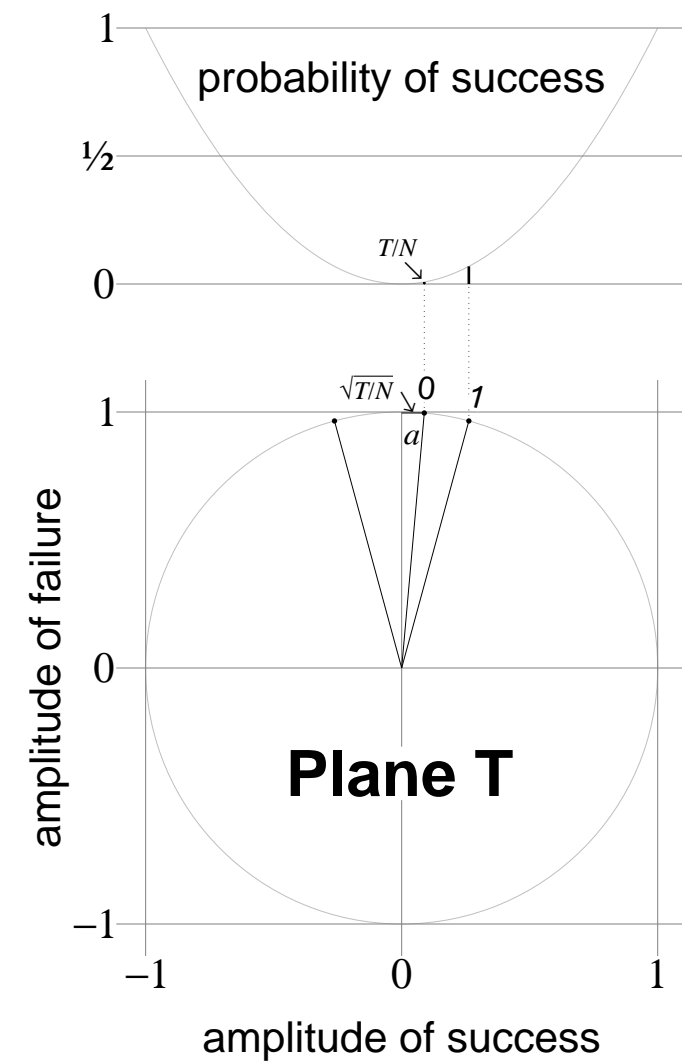
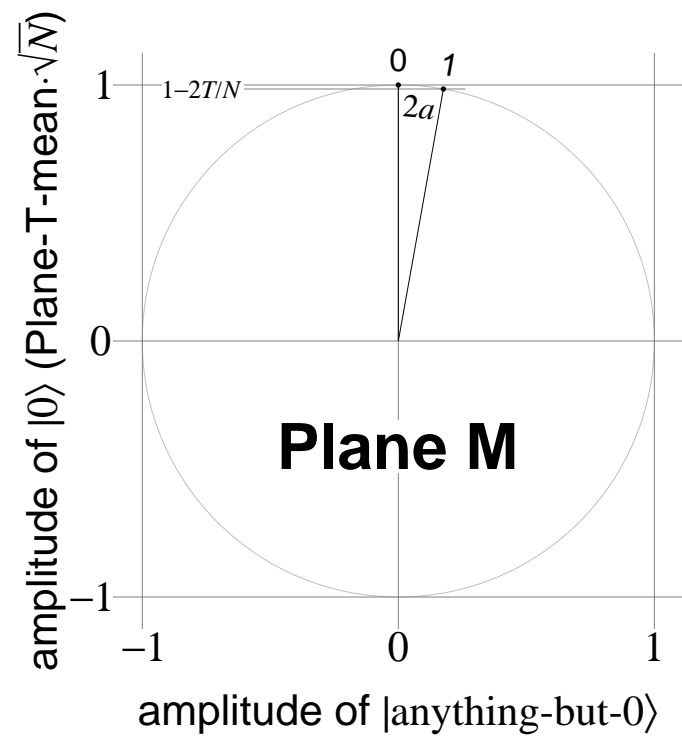


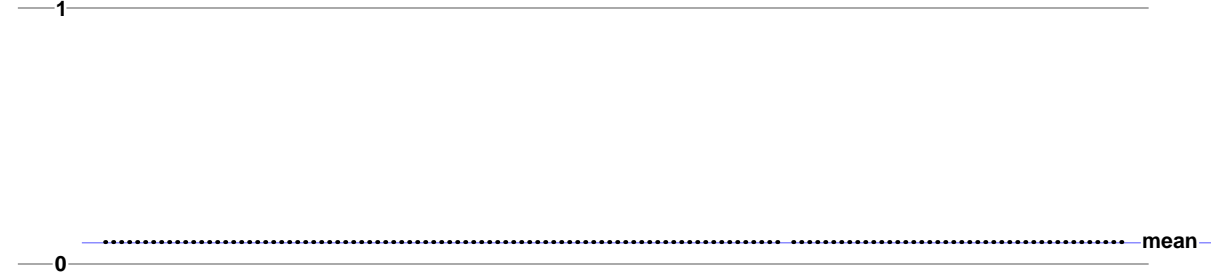


$$N = 128, T = 1$$

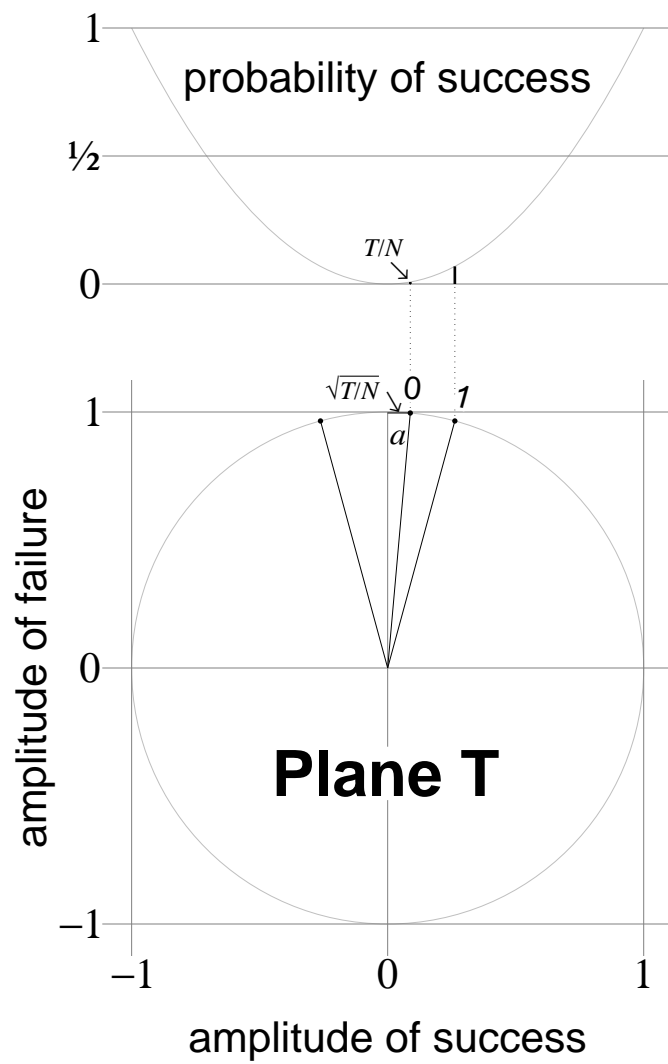
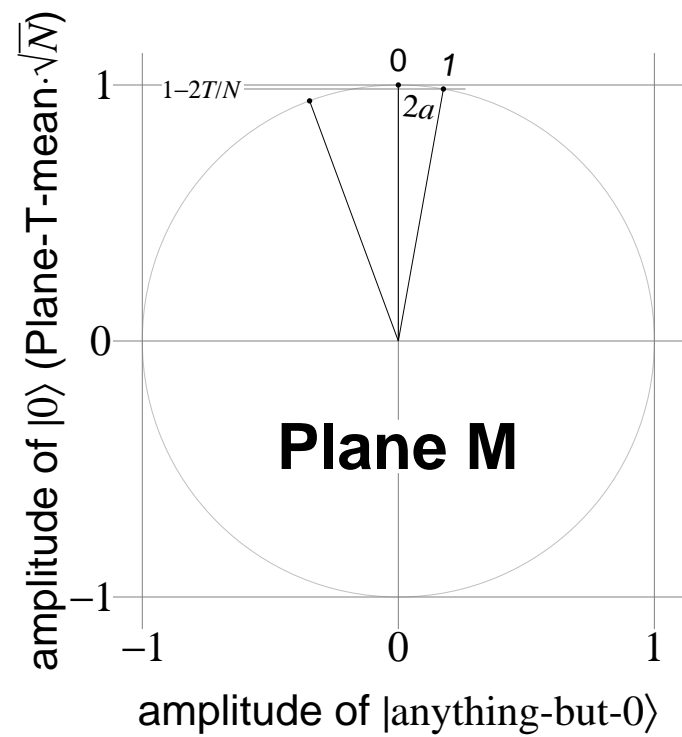


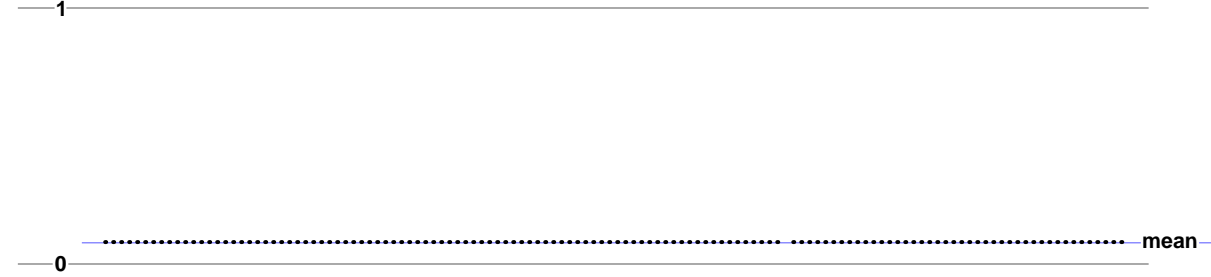
$$N = 128, \quad T = 1$$



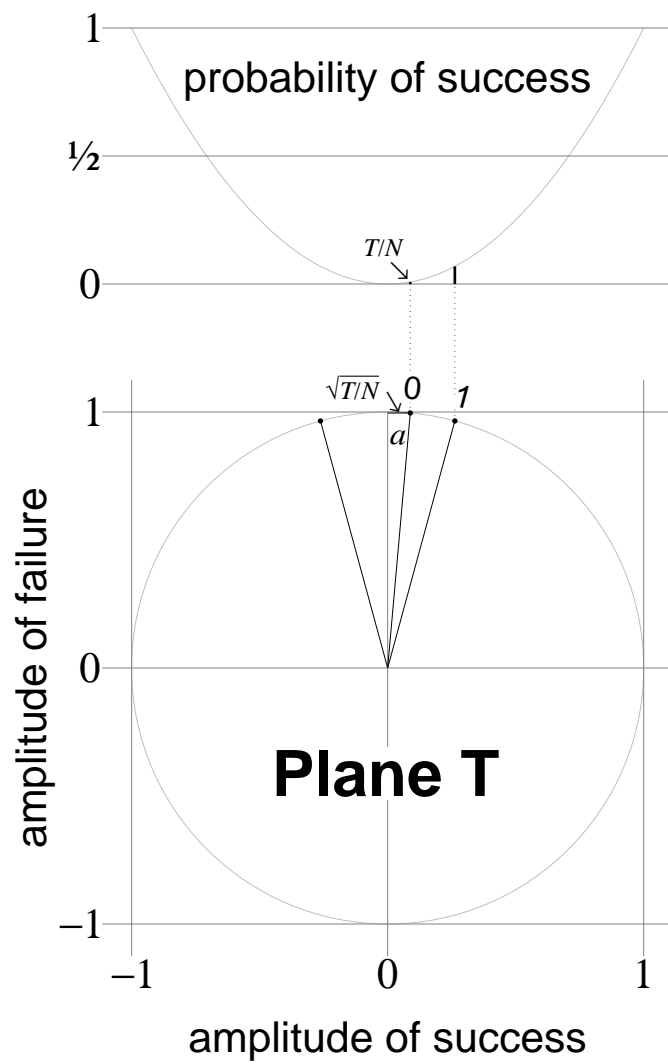
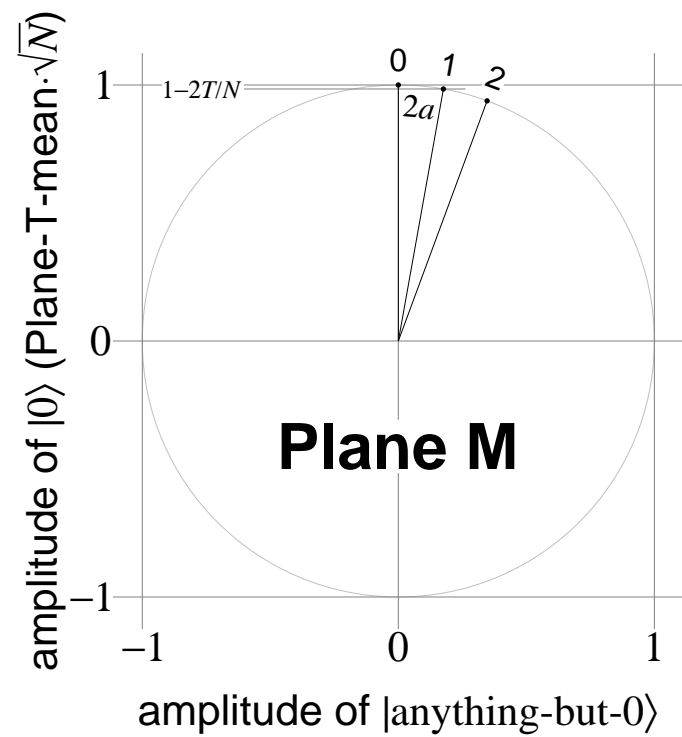


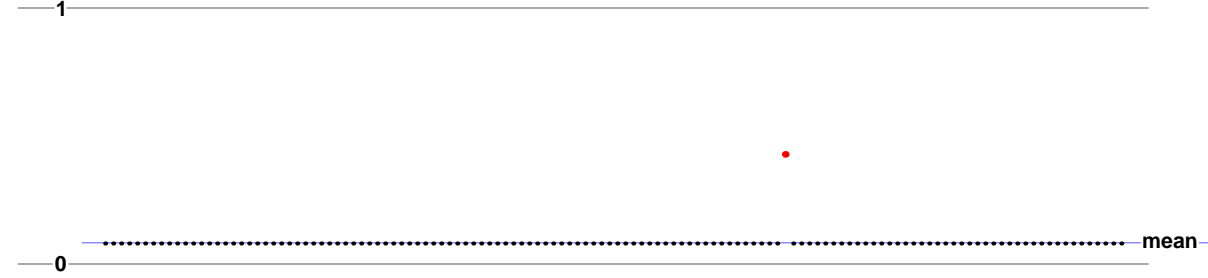
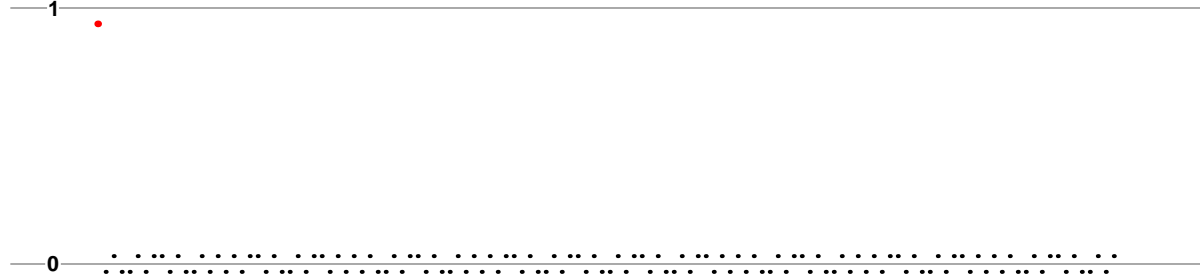
$$N = 128, T = 1$$



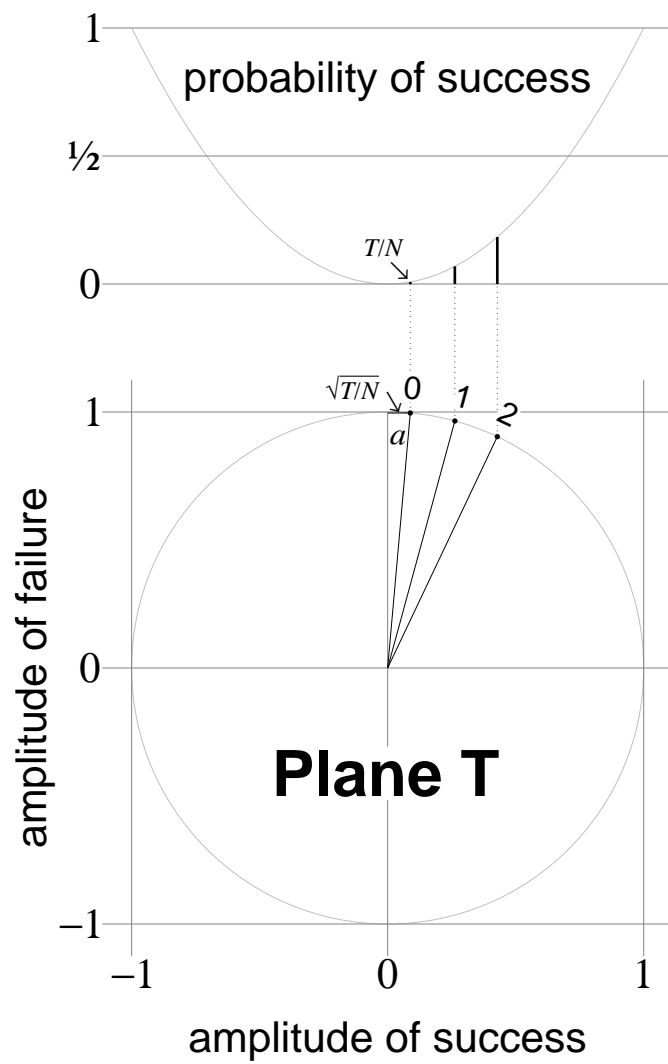
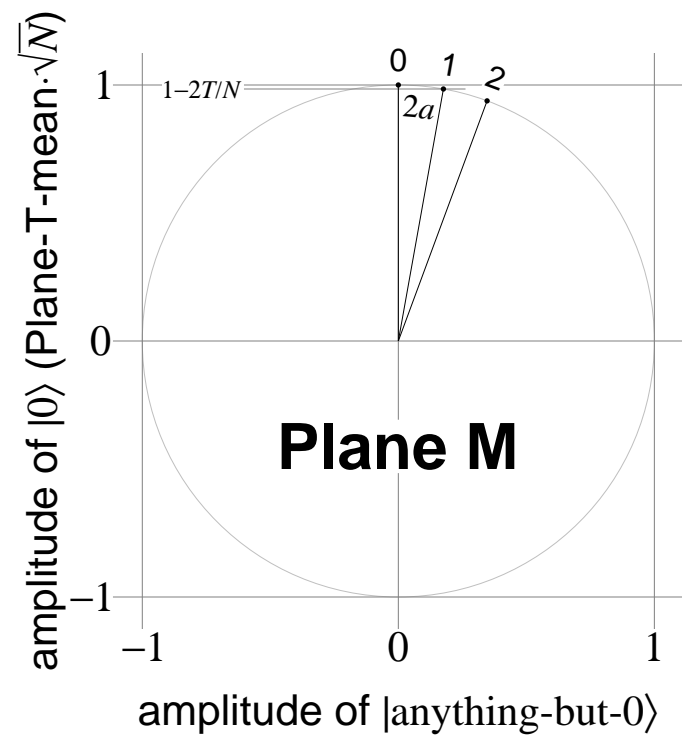


$$N = 128, T = 1$$

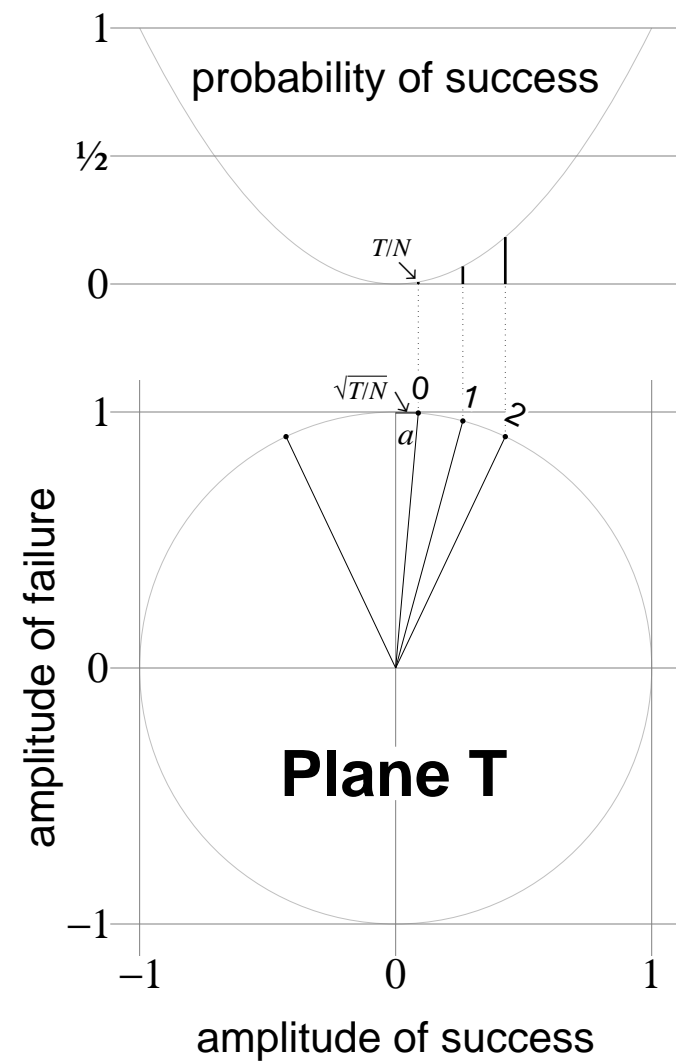
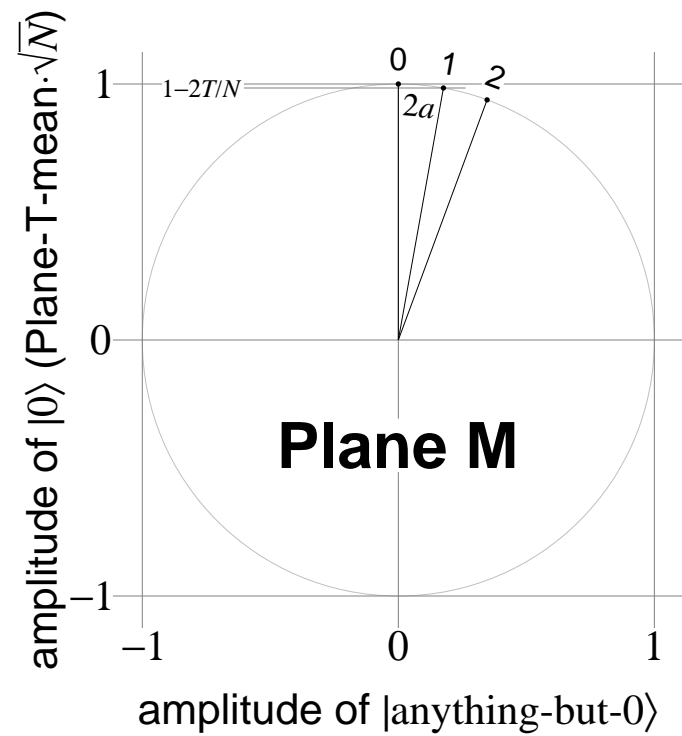




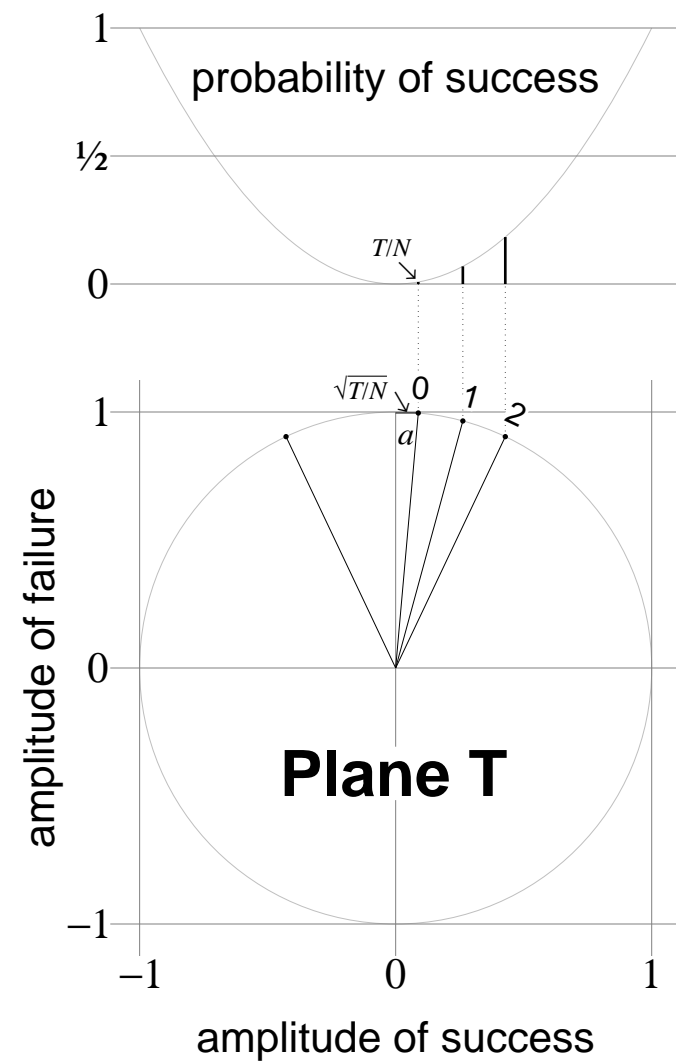
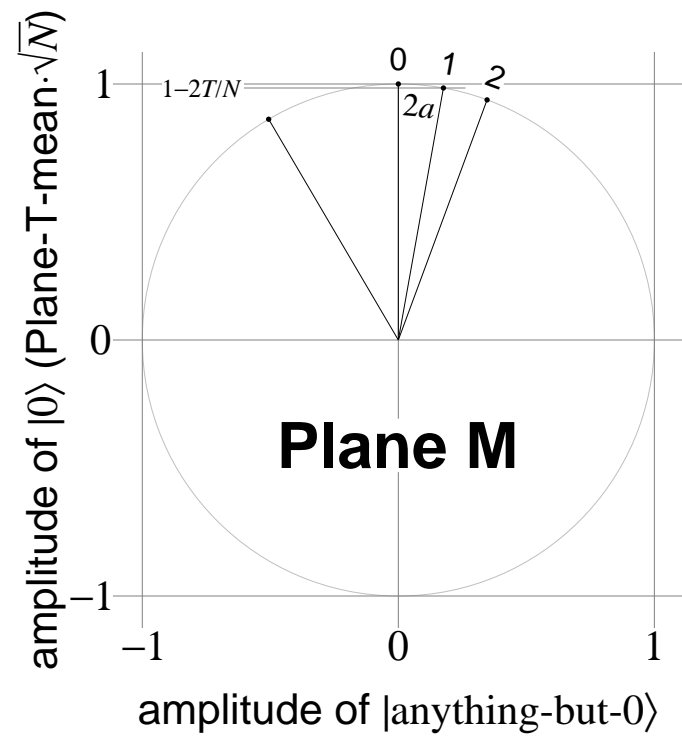
$$N = 128, T = 1$$

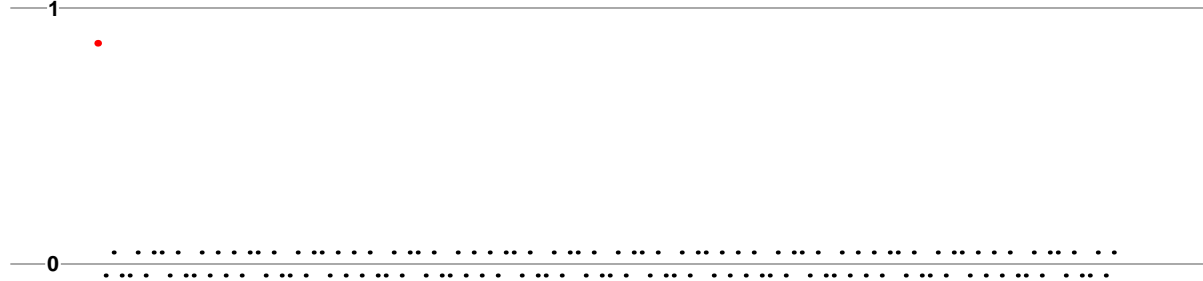


$$N = 128, T = 1$$

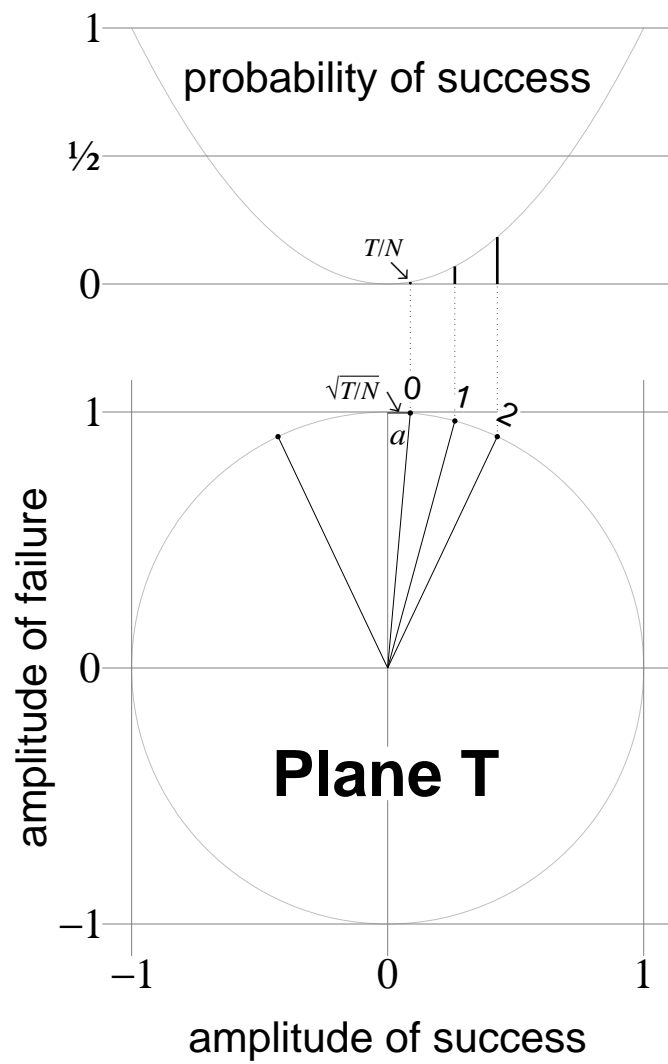
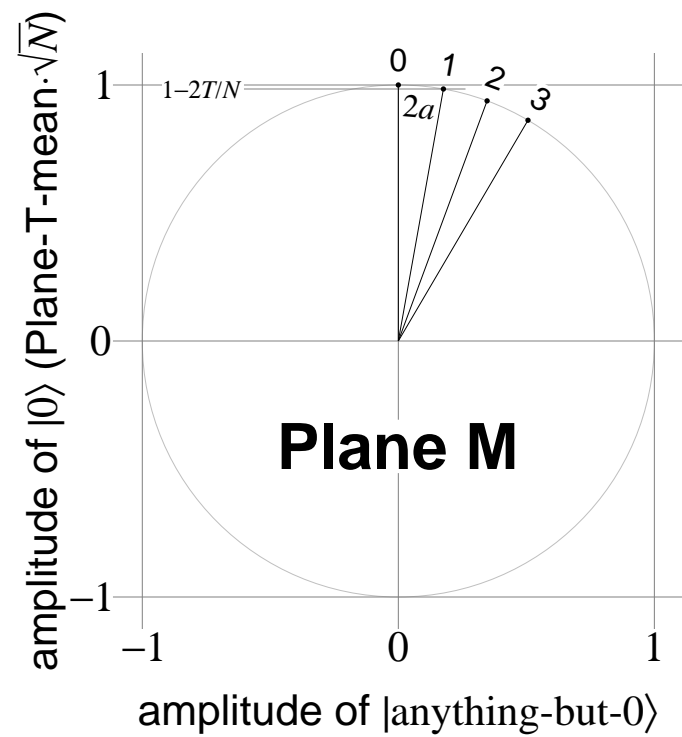


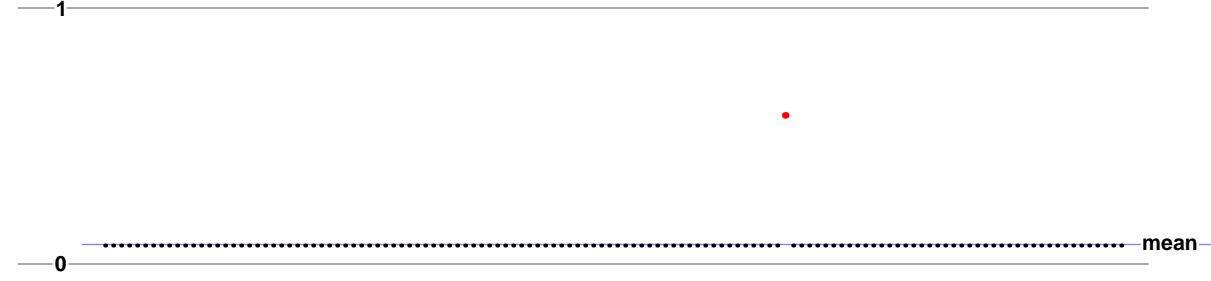
$$N = 128, T = 1$$



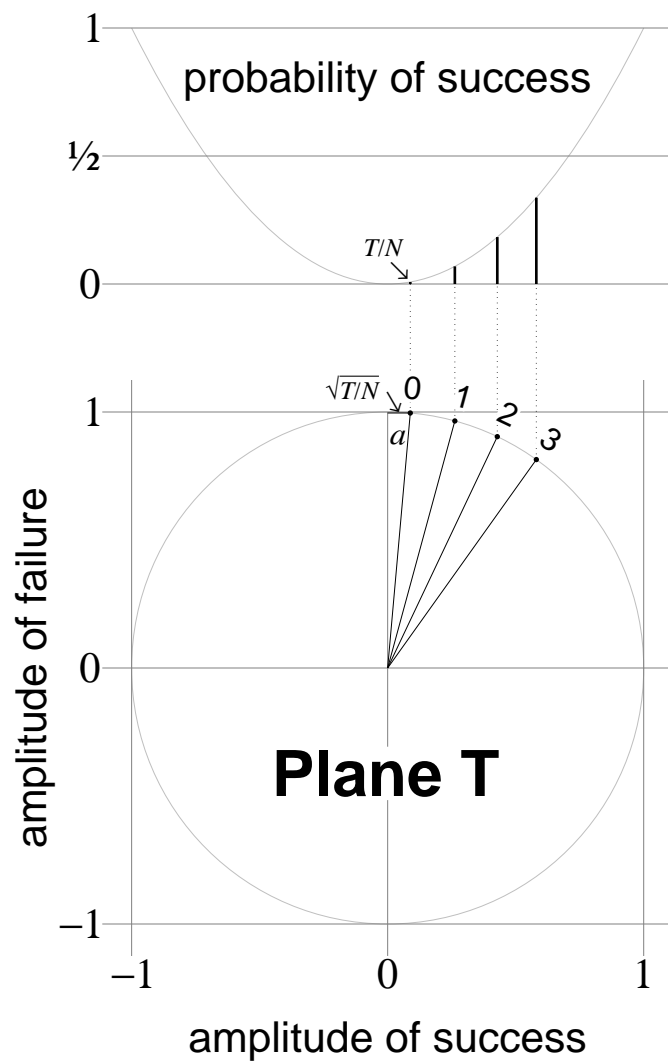
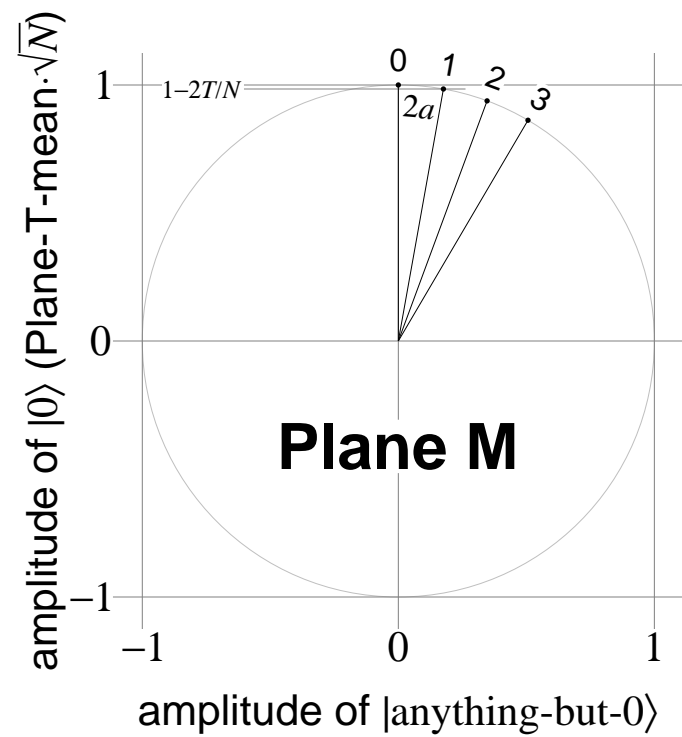


$$N = 128, T = 1$$

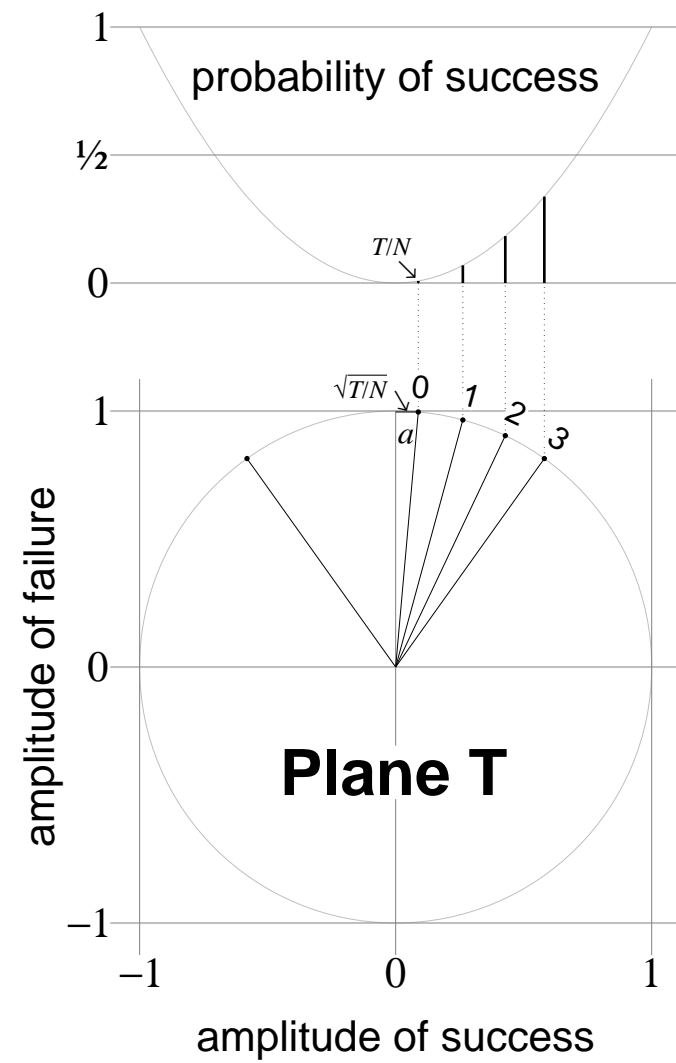
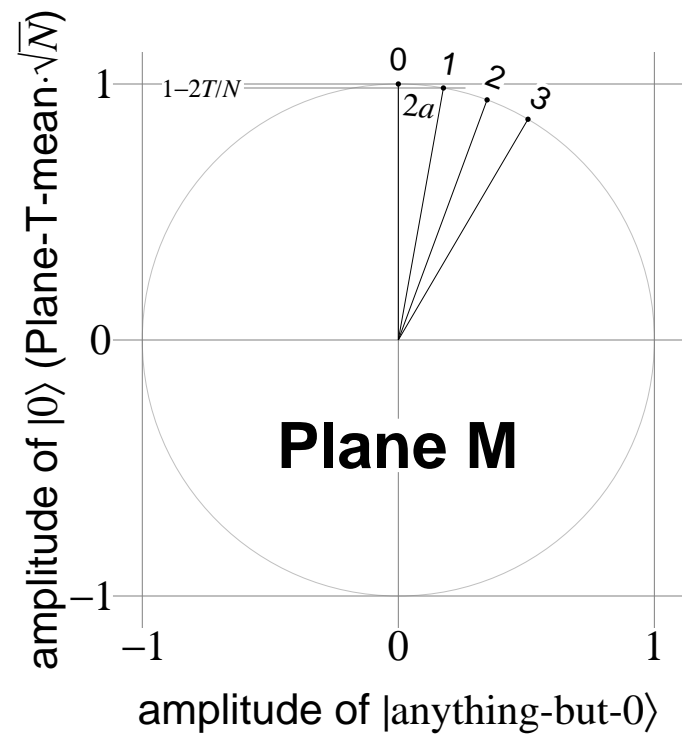


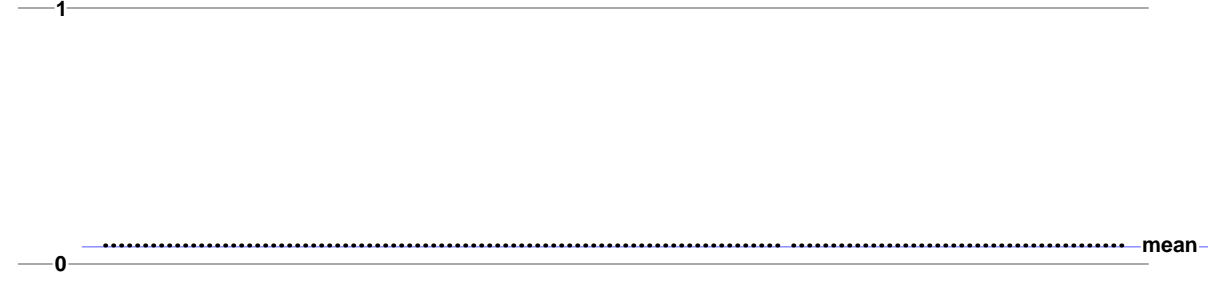
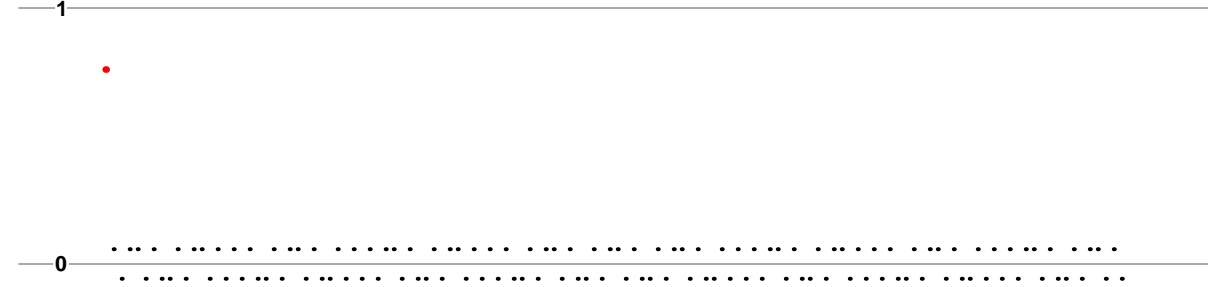


$$N = 128, T = 1$$

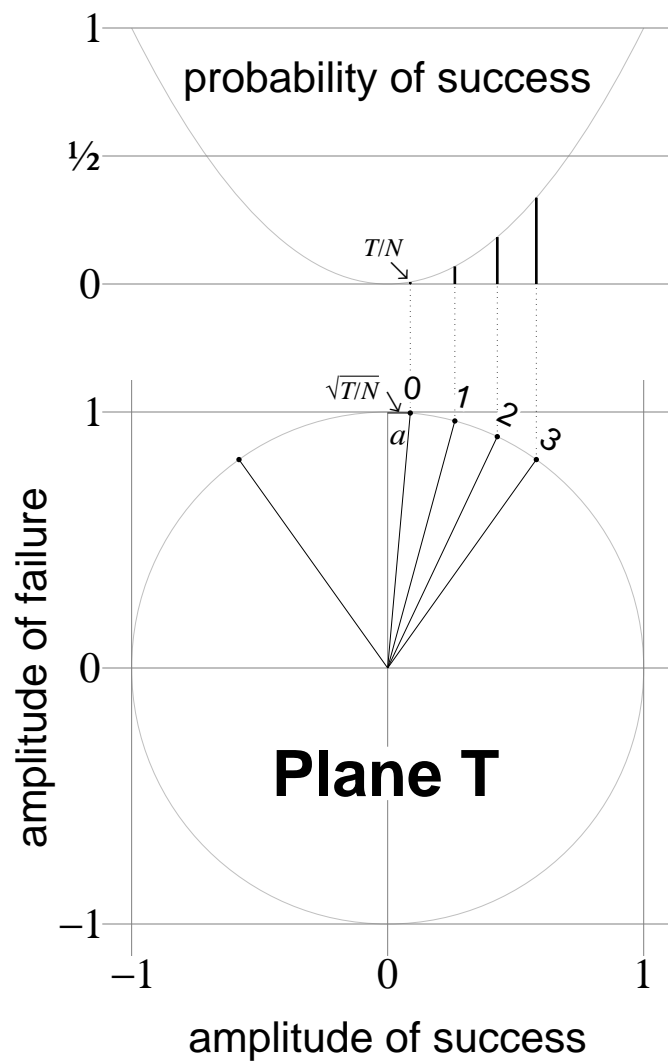
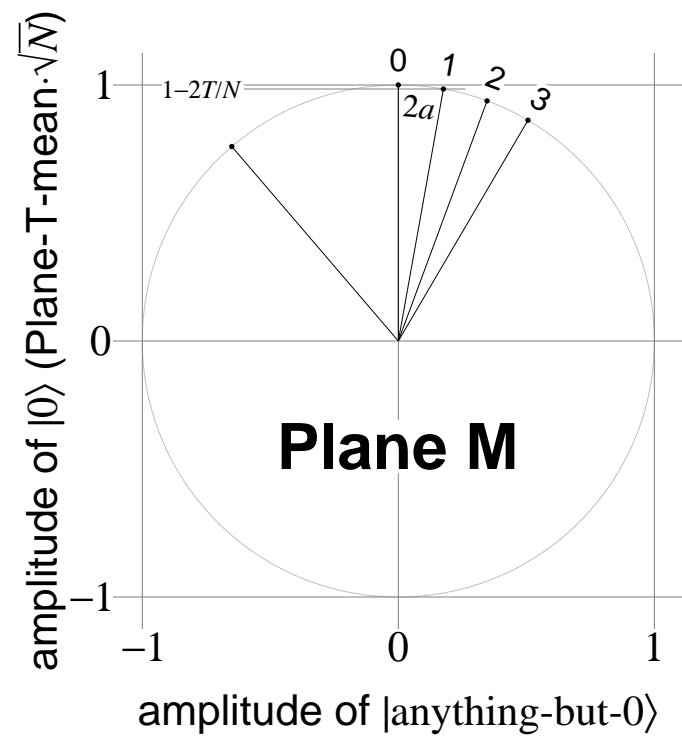


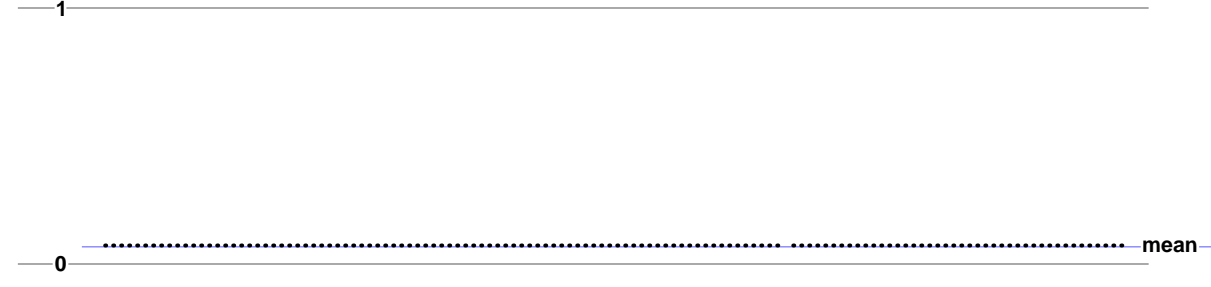
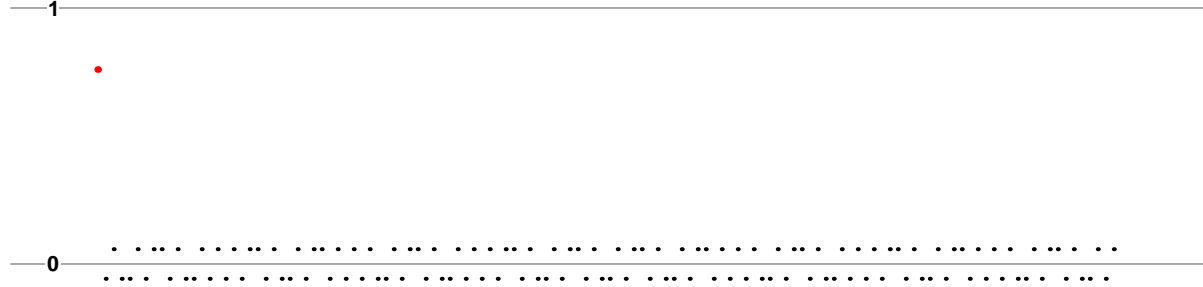
$$N = 128, T = 1$$



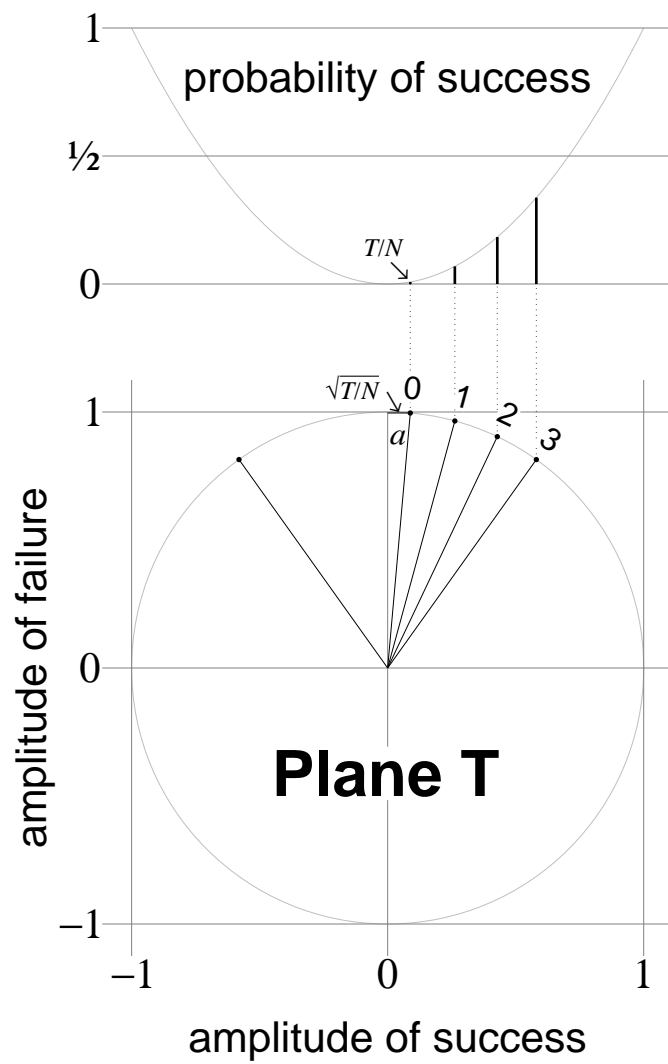
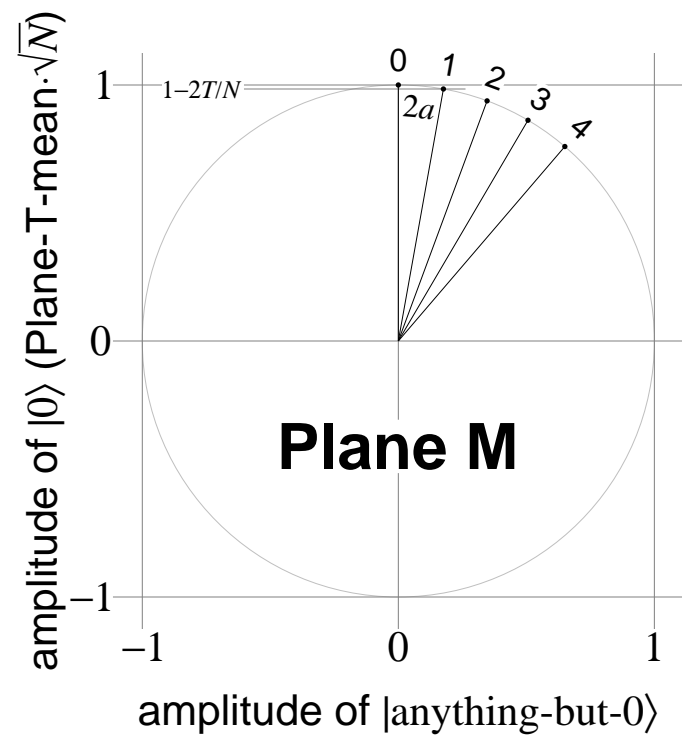


$$N = 128, T = 1$$

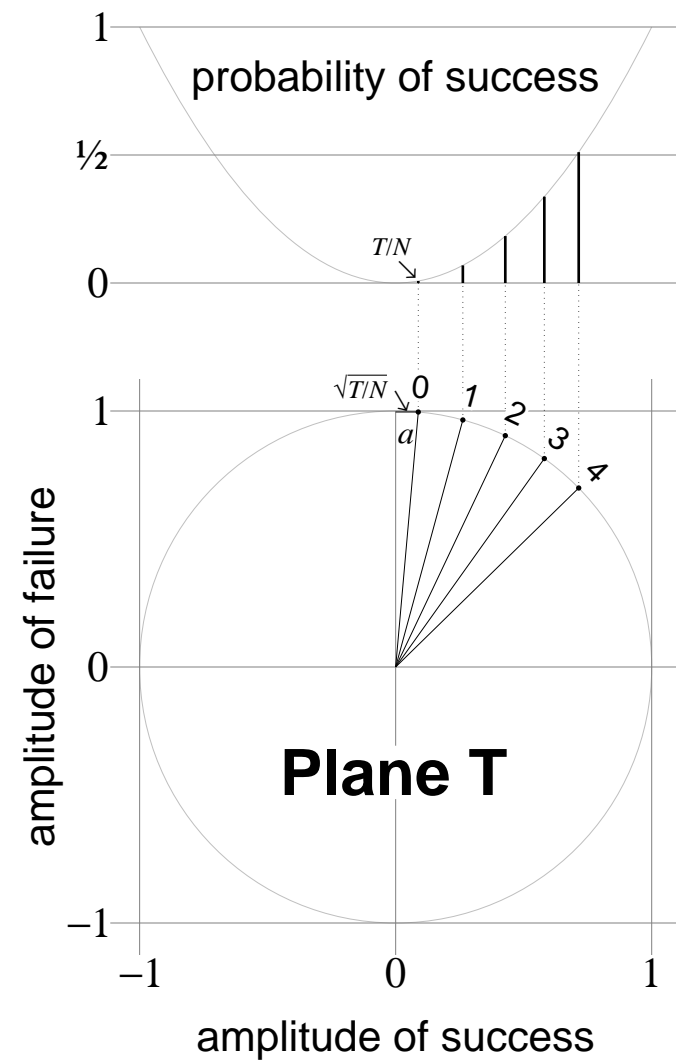
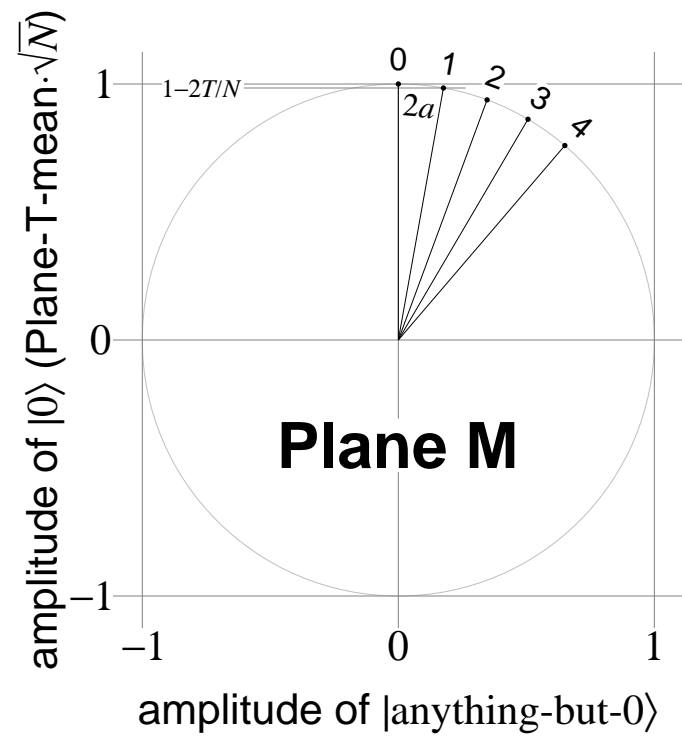




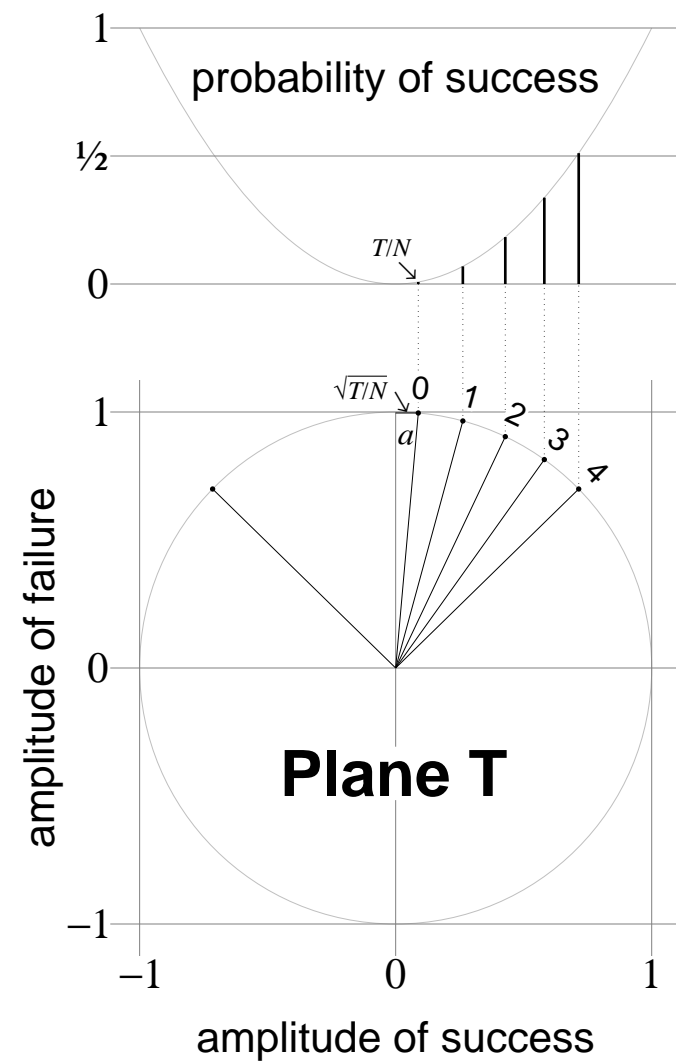
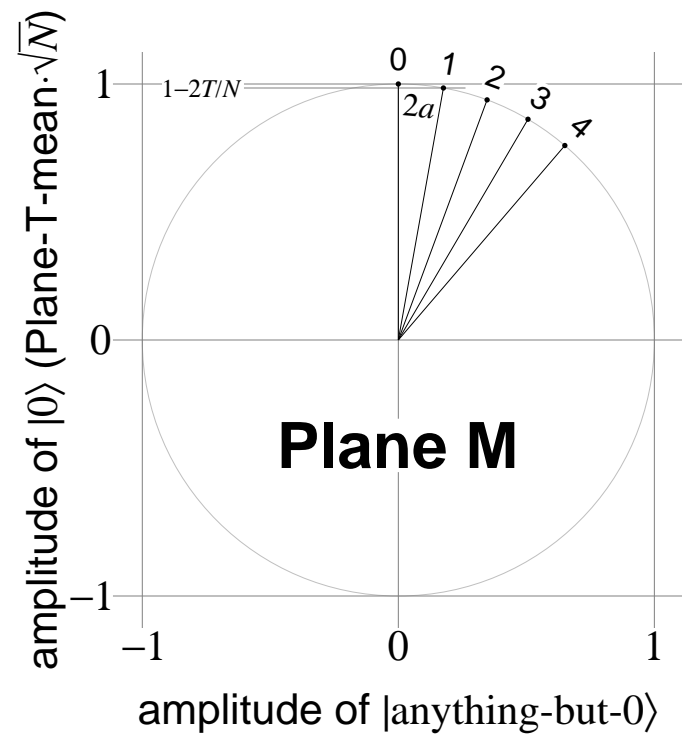
$$N = 128, T = 1$$



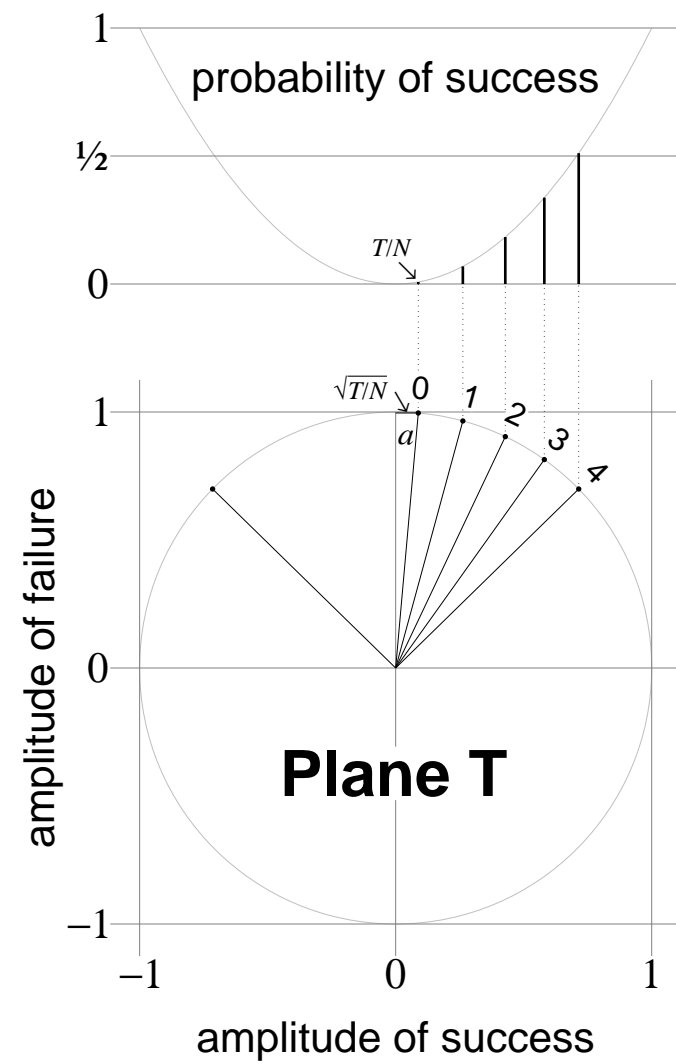
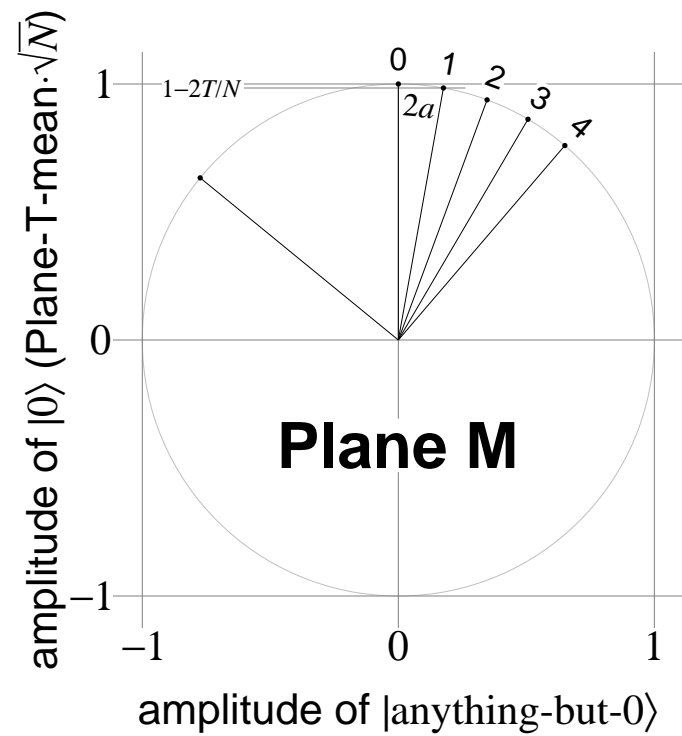
$$N = 128, T = 1$$



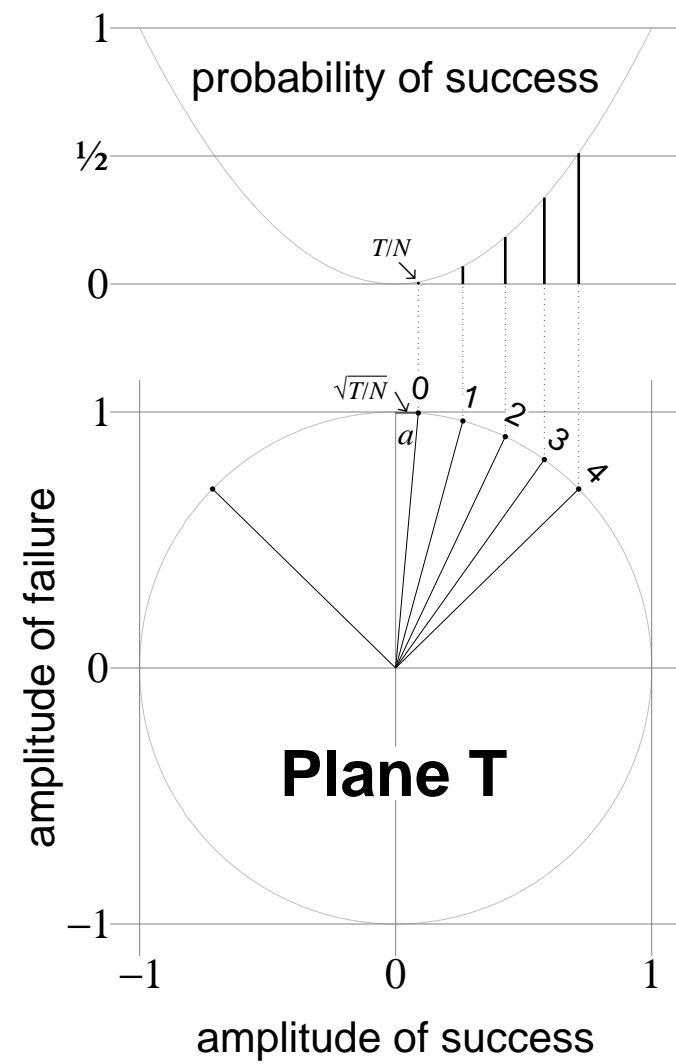
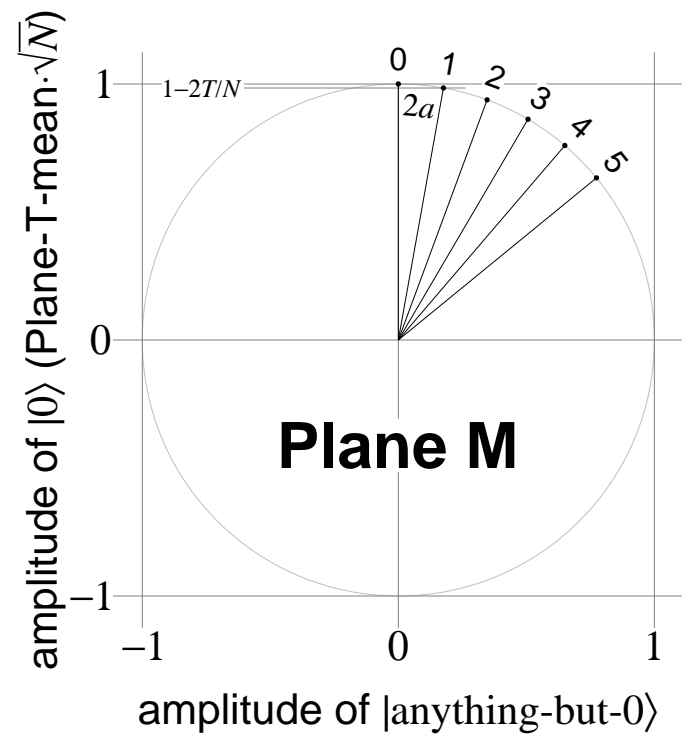
$$N = 128, T = 1$$

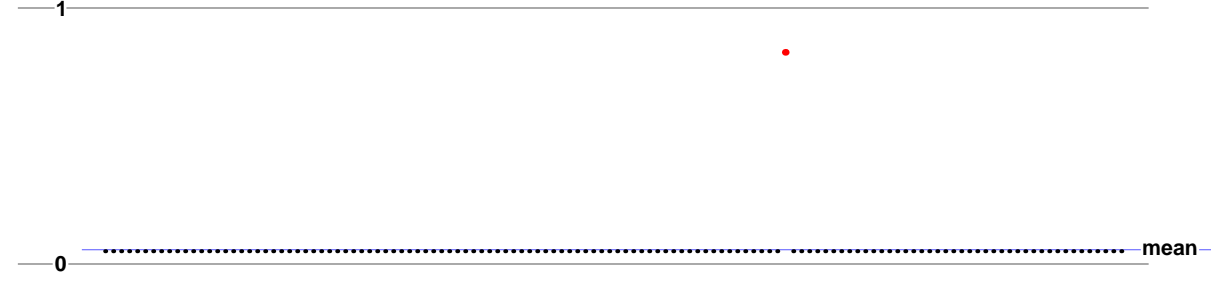
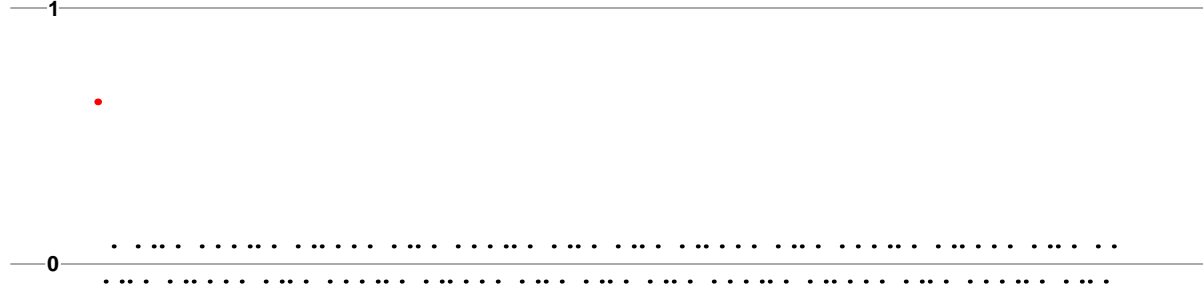


$$N = 128, T = 1$$

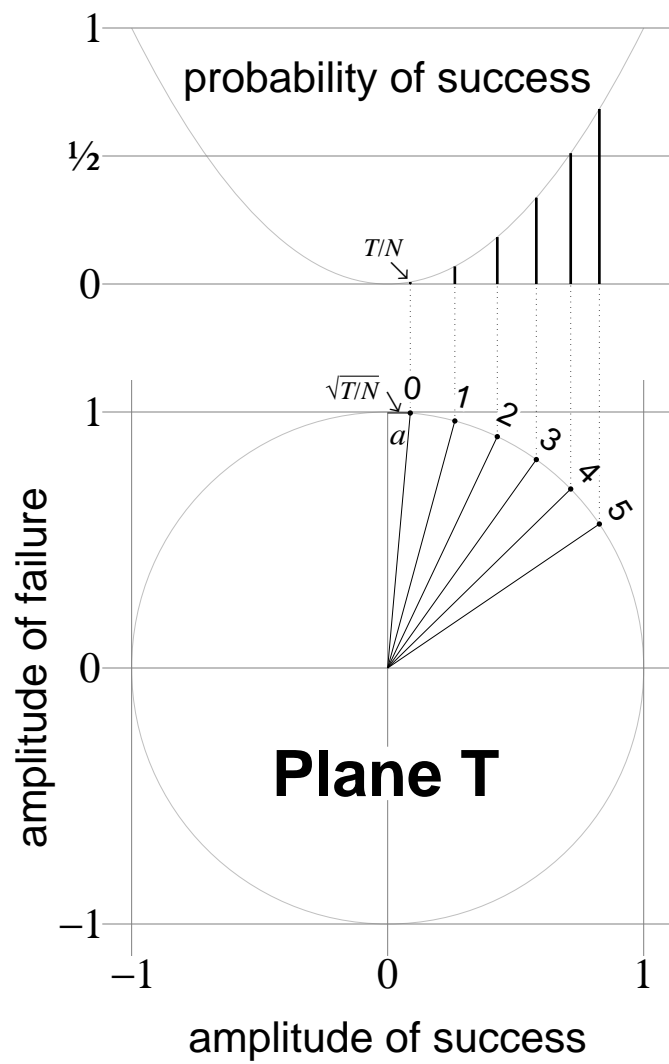
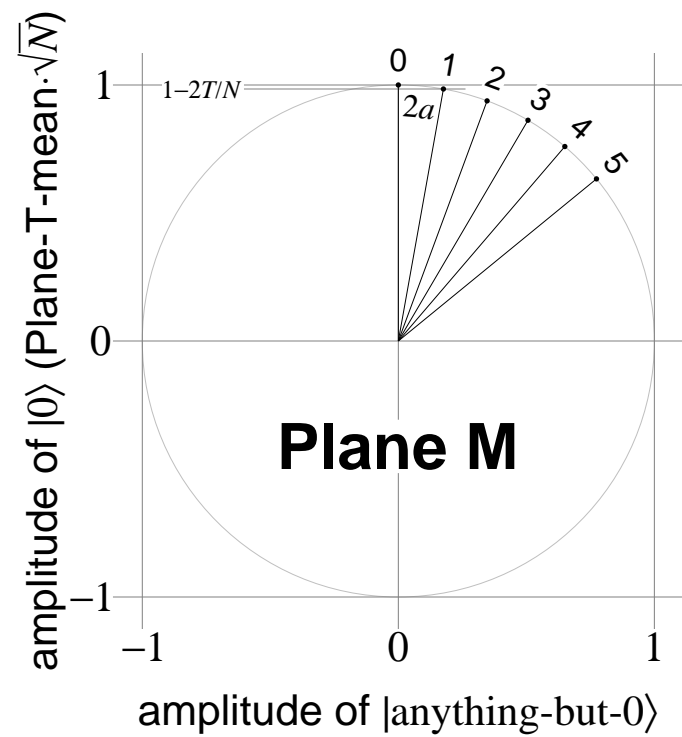


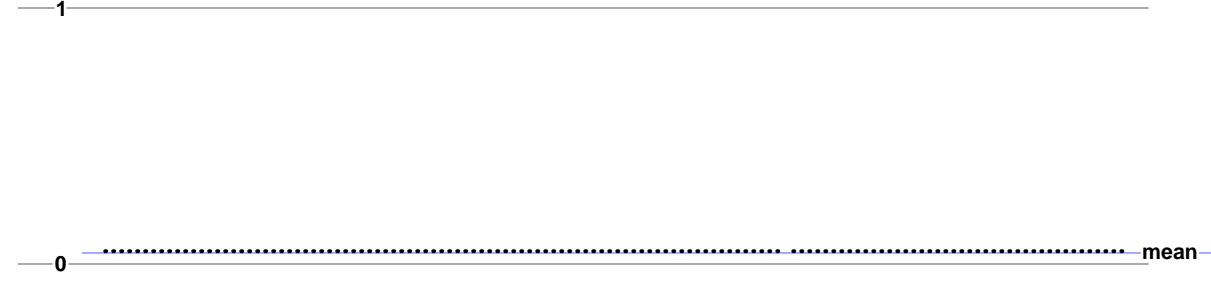
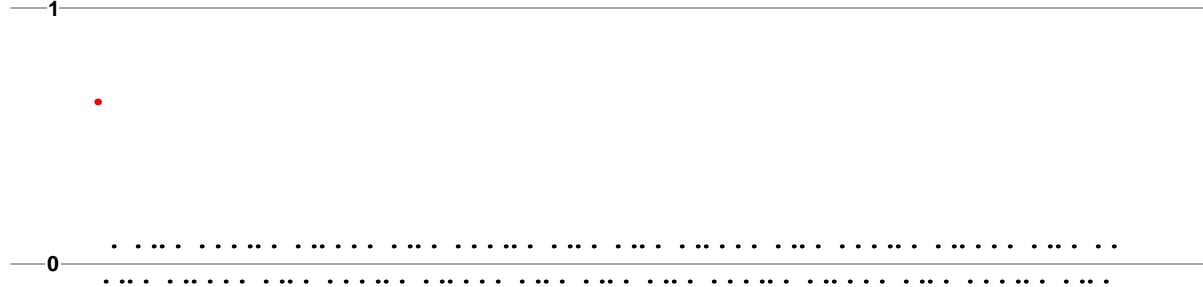
$$N = 128, \quad T = 1$$



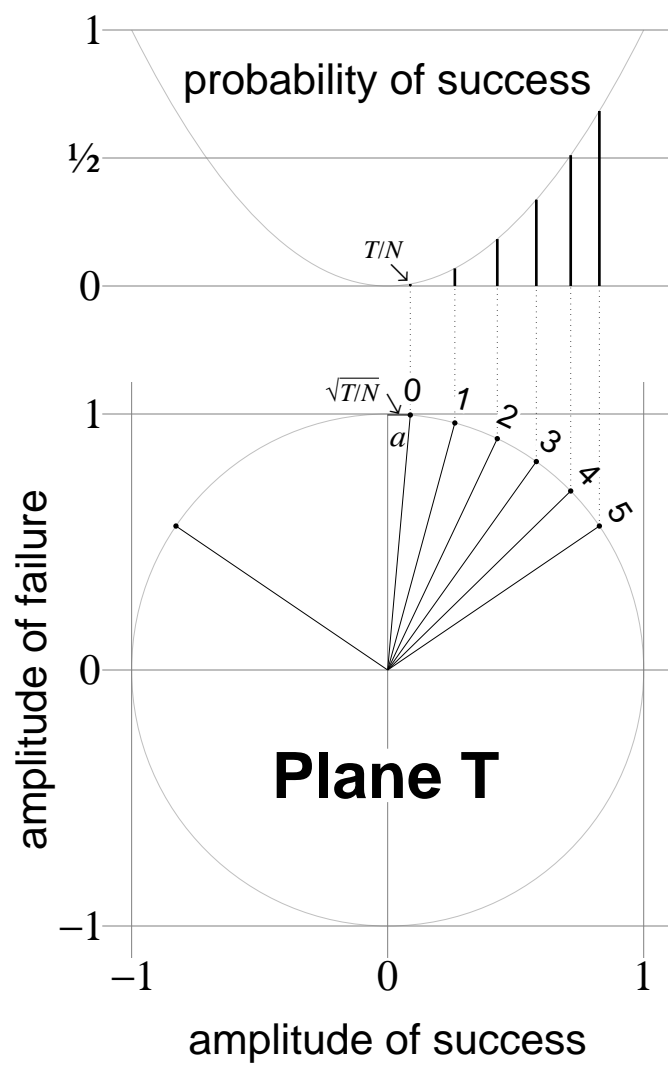
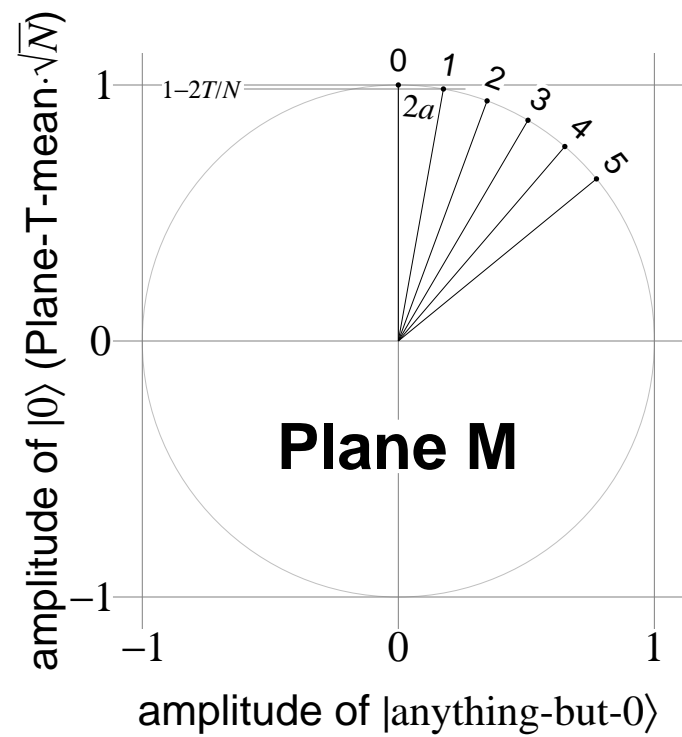


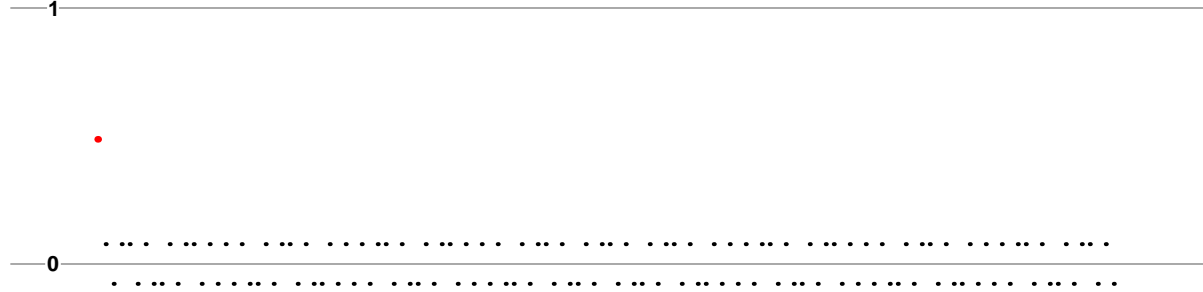
$$N = 128, T = 1$$



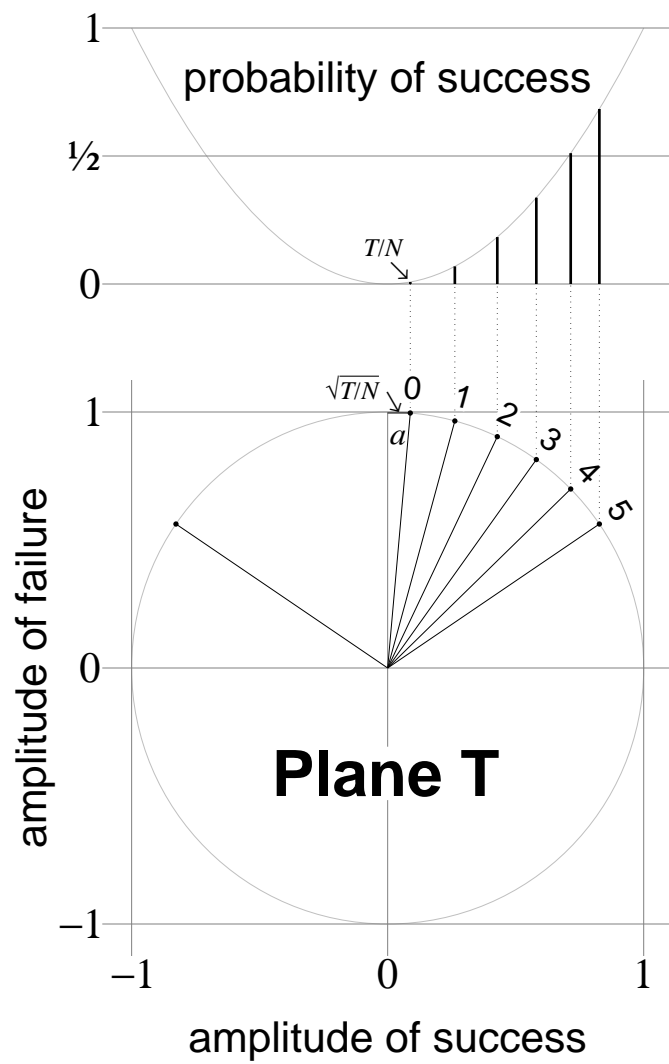
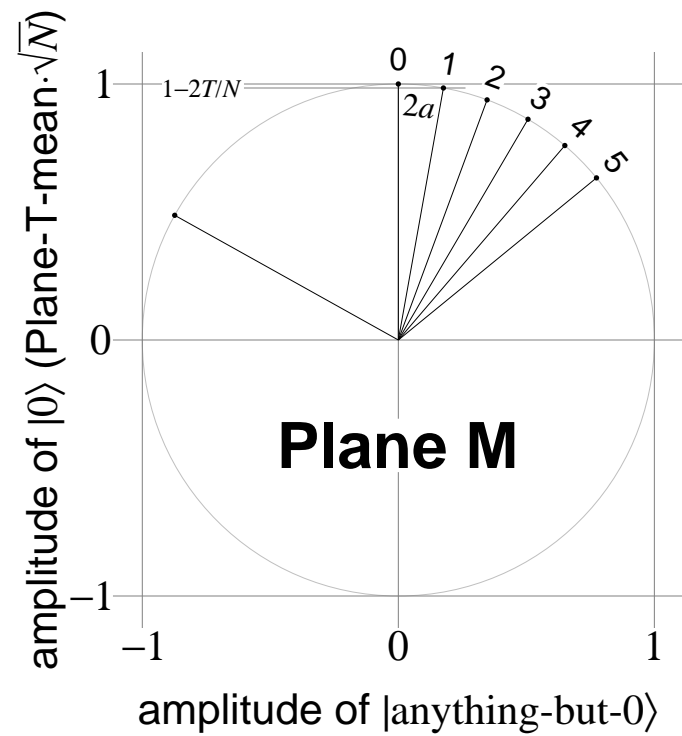


$$N = 128, T = 1$$



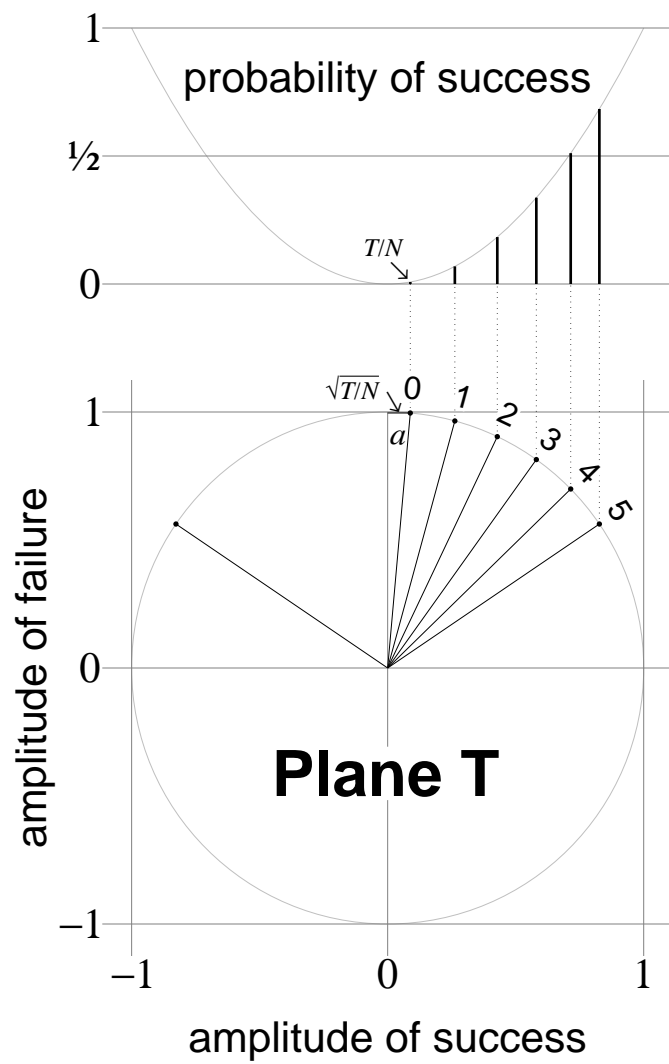
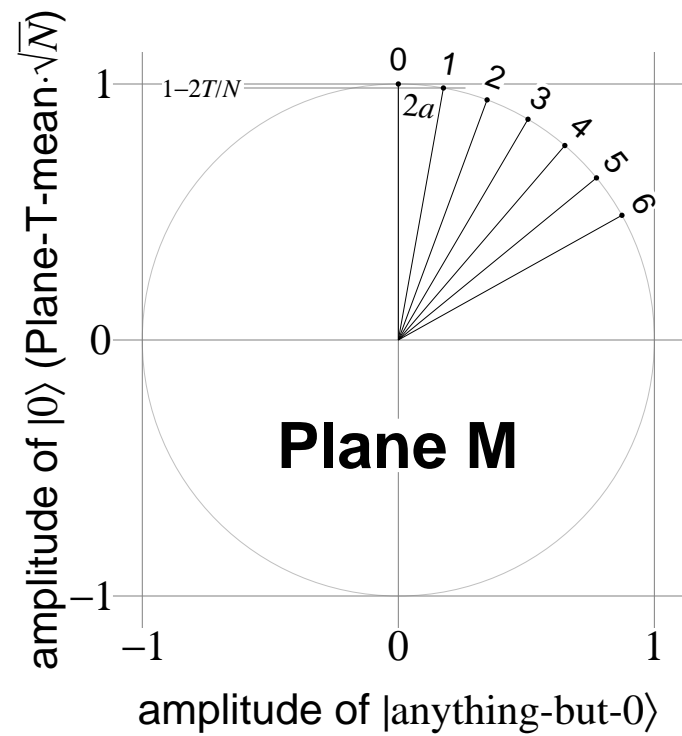


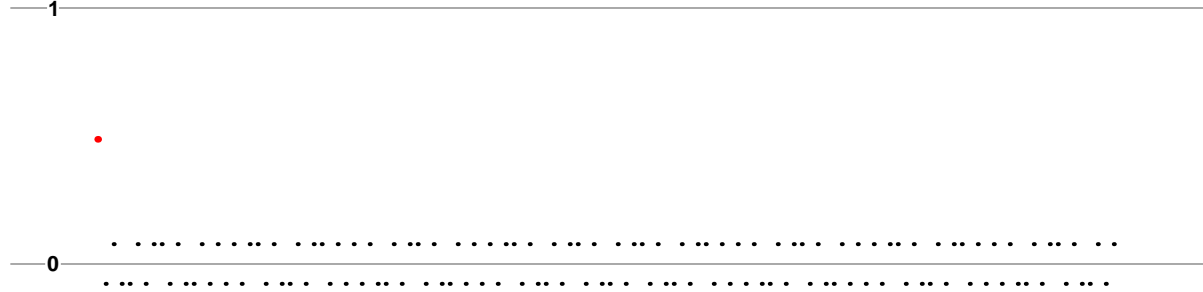
$$N = 128, T = 1$$



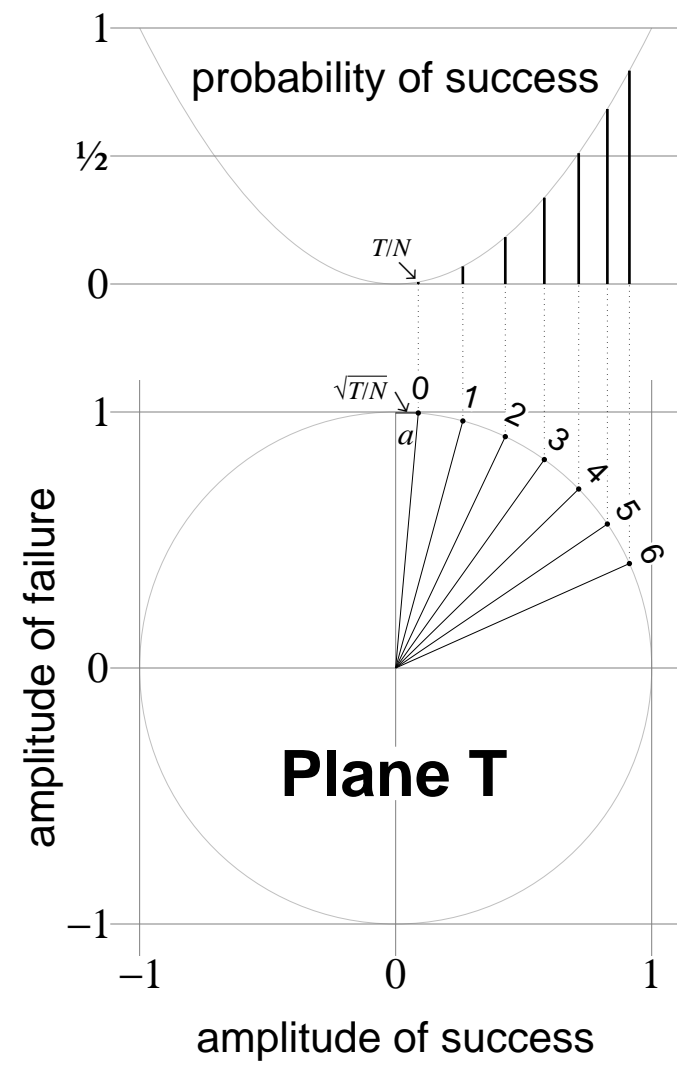
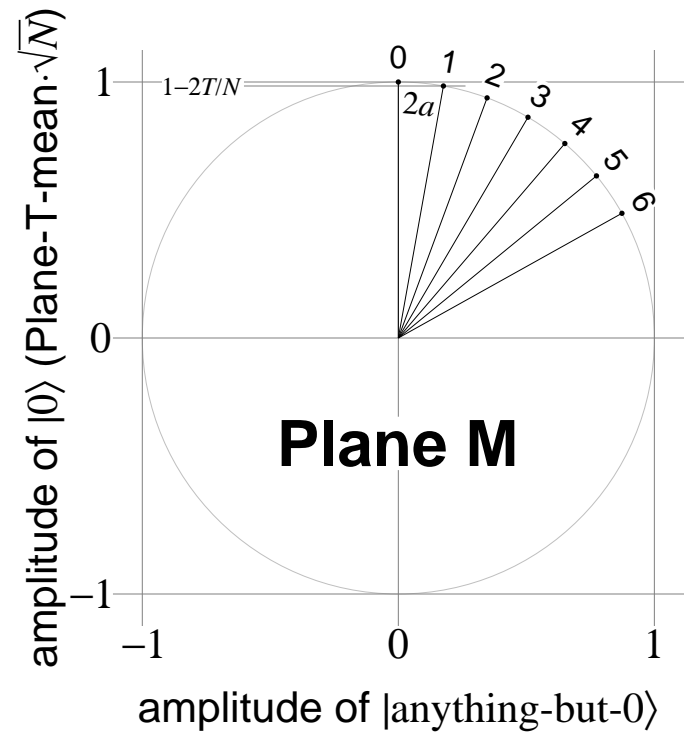


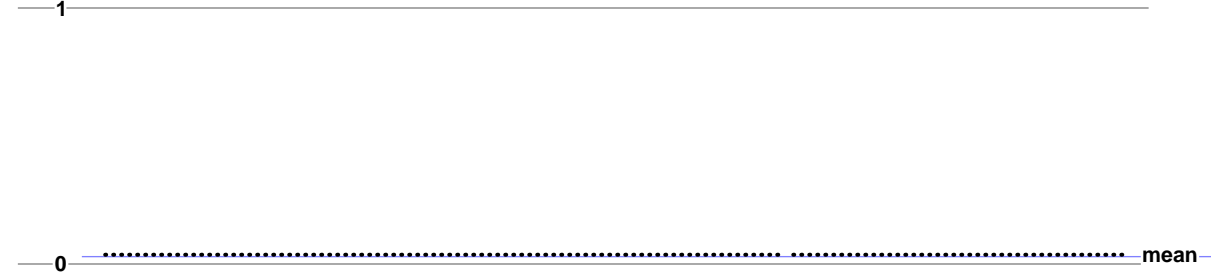
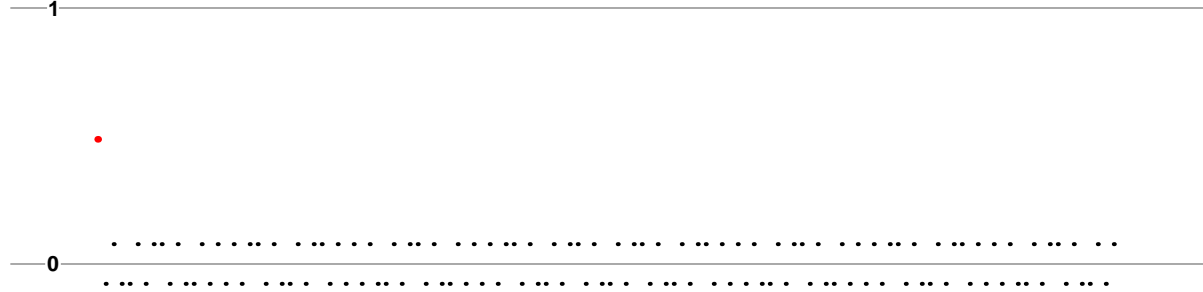
$$N = 128, T = 1$$



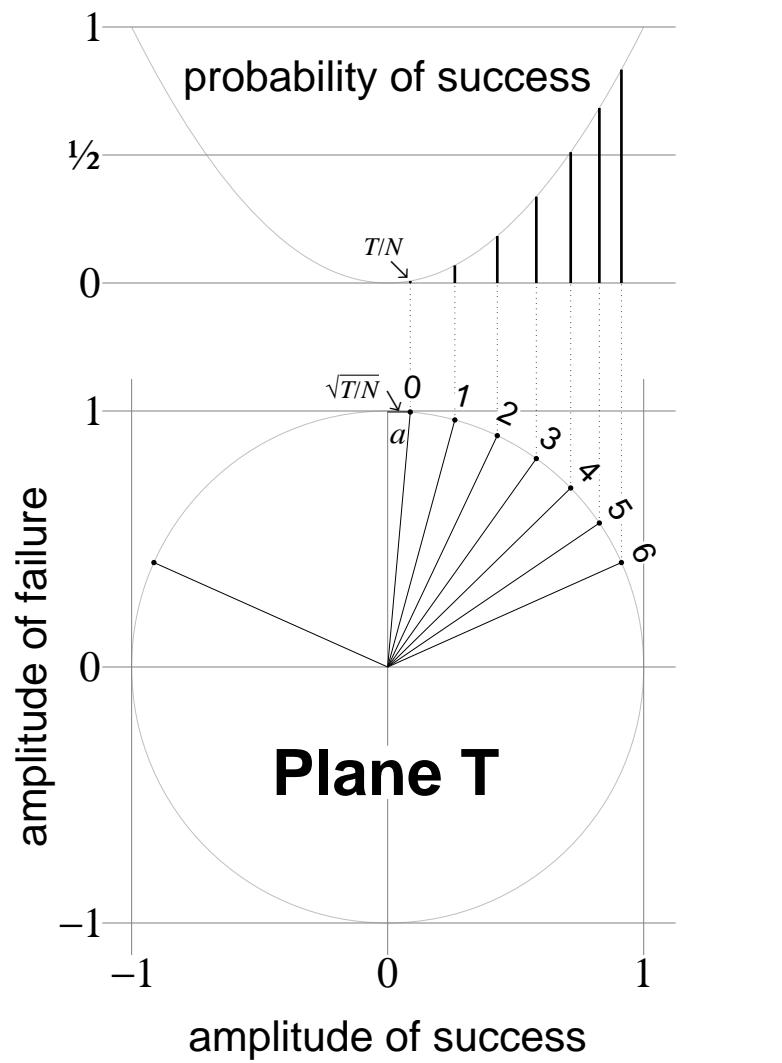
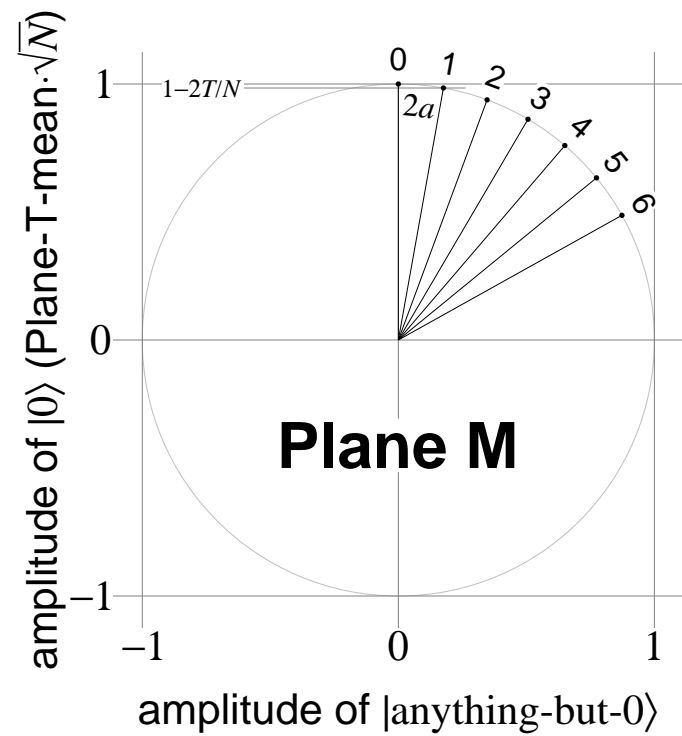


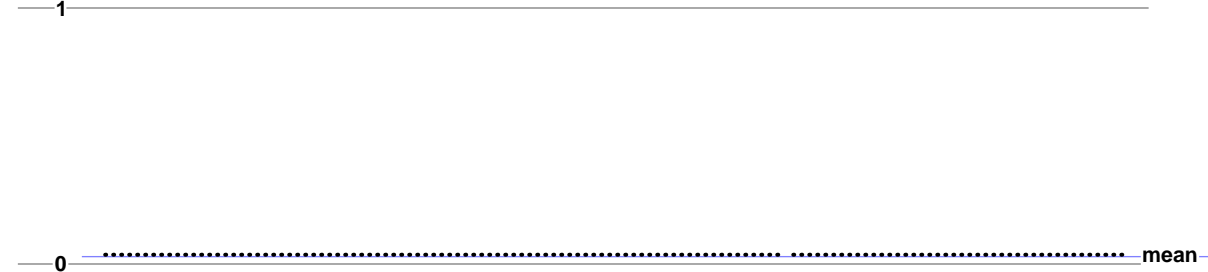
$$N = 128, \quad T = 1$$



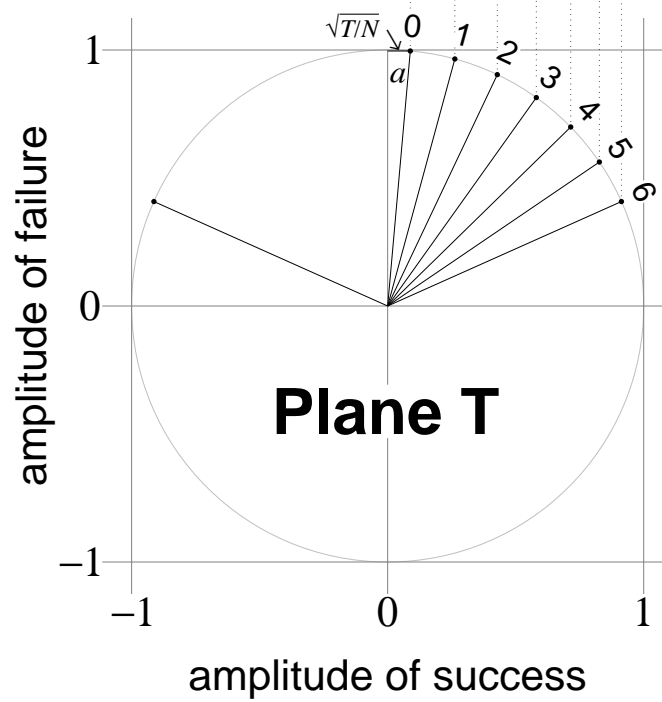


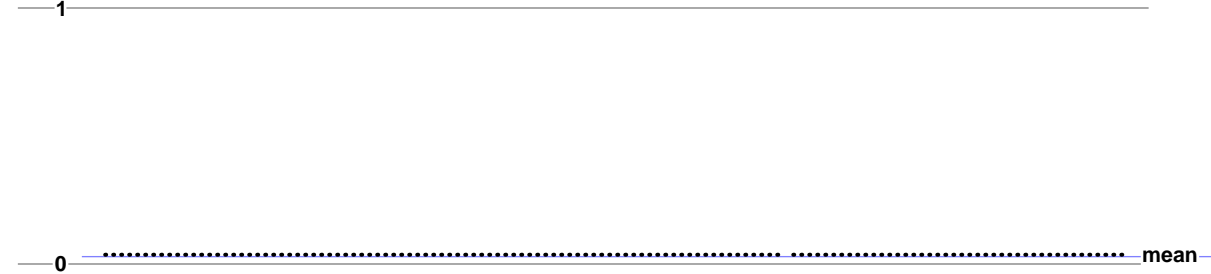
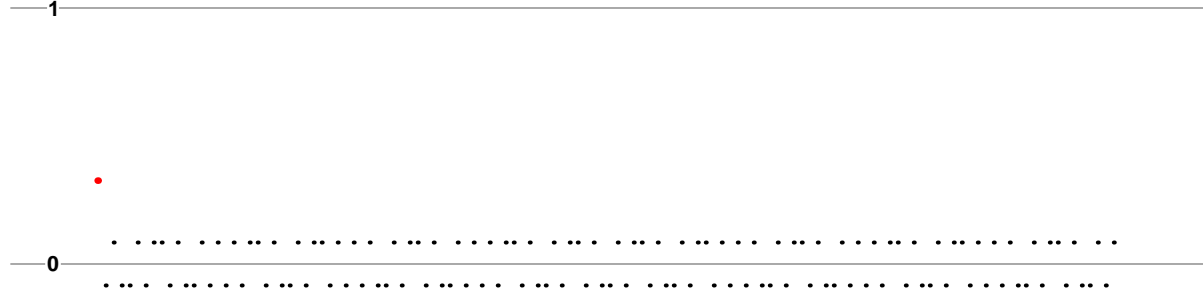
$$N = 128, T = 1$$



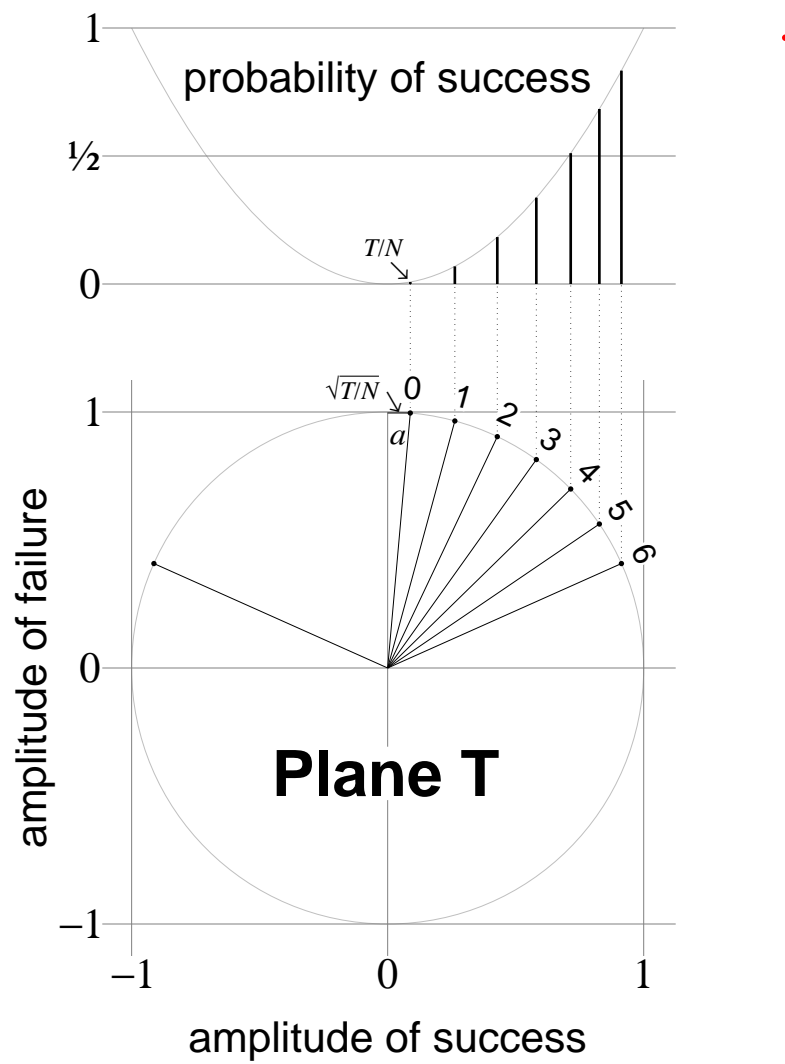
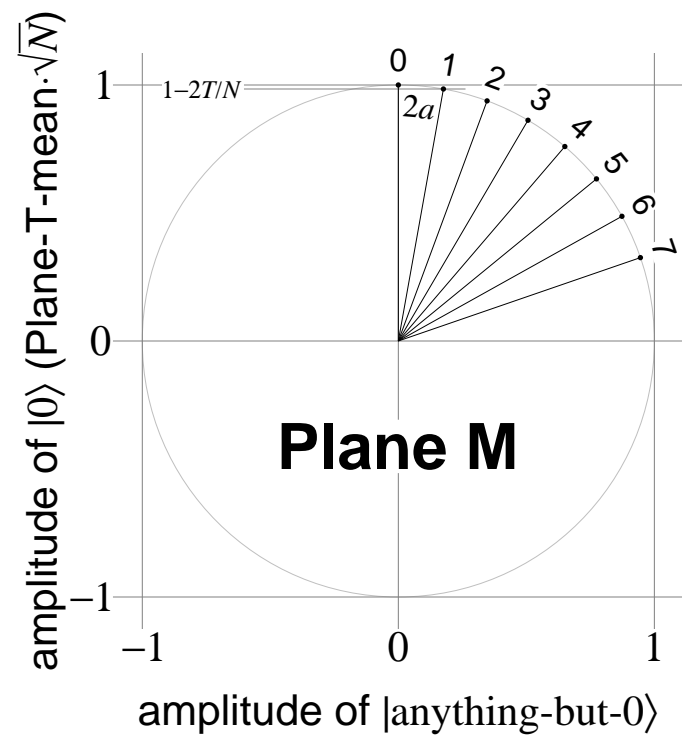


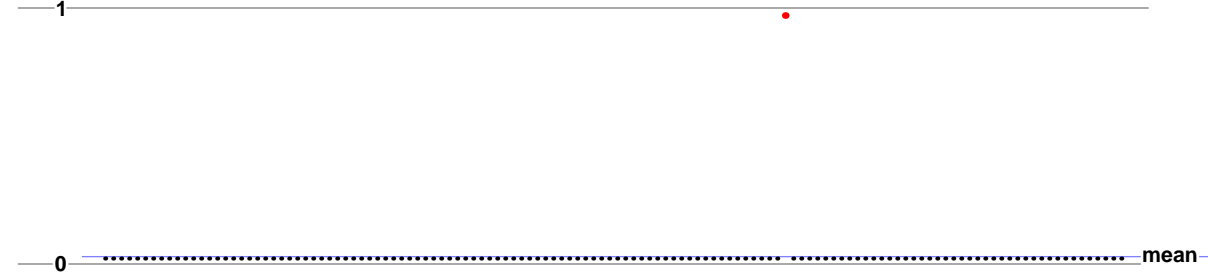
A graph showing the probability of success as a function of T/N . The y-axis is labeled "probability of success" and ranges from 0 to 1. The x-axis is labeled T/N . A curve starts at (0,0) and increases, passing through (1/2, 1/2). Vertical bars of increasing height are shown at regular intervals of T/N , starting from 0.



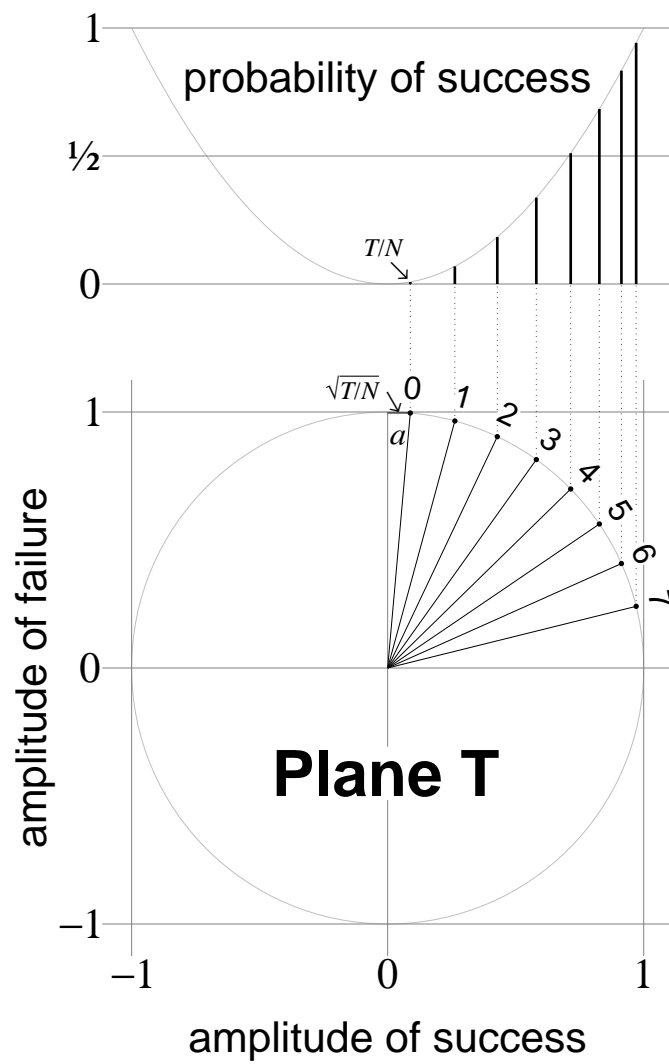
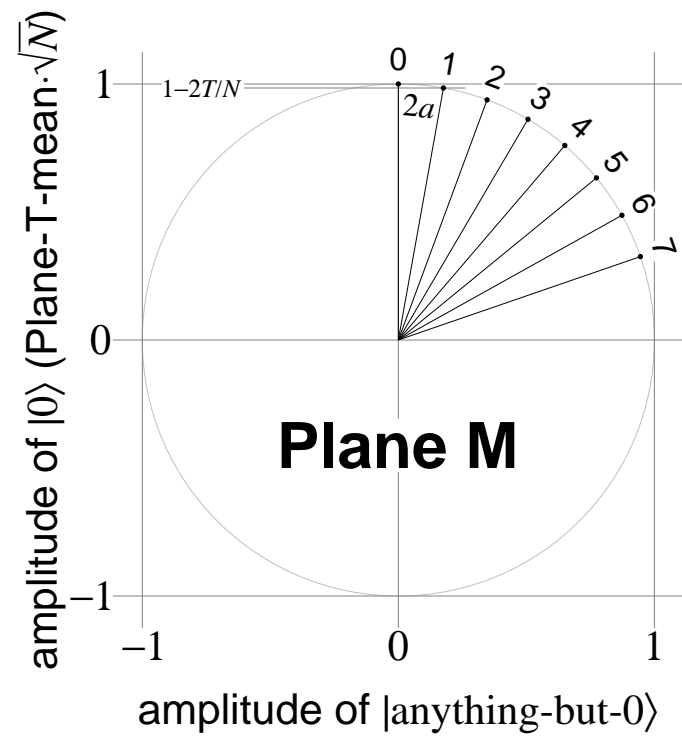


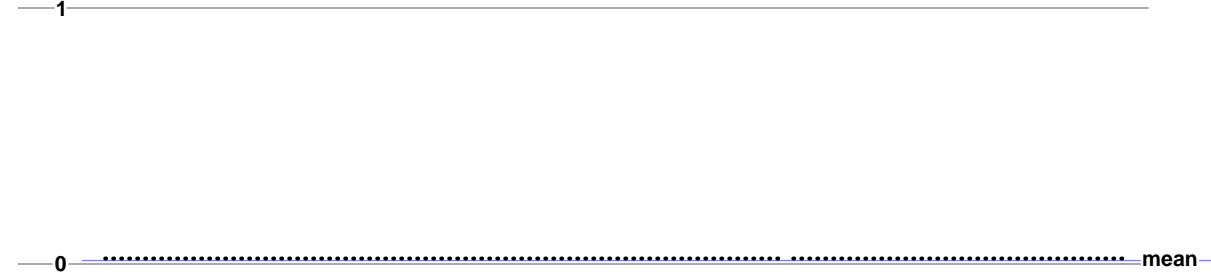
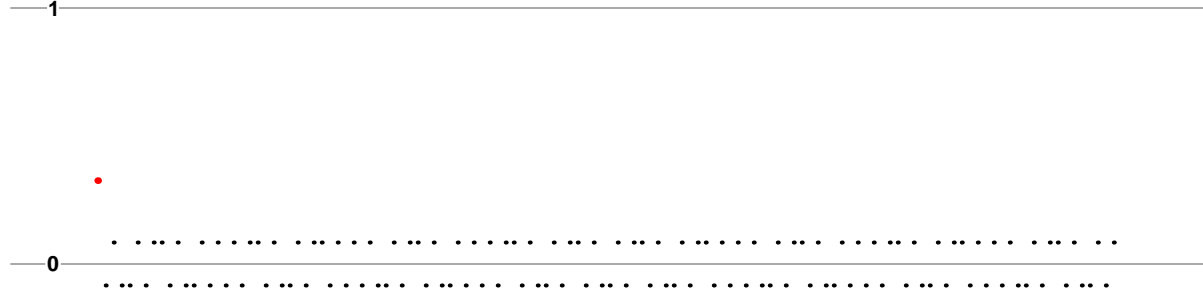
$$N = 128, \quad T = 1$$



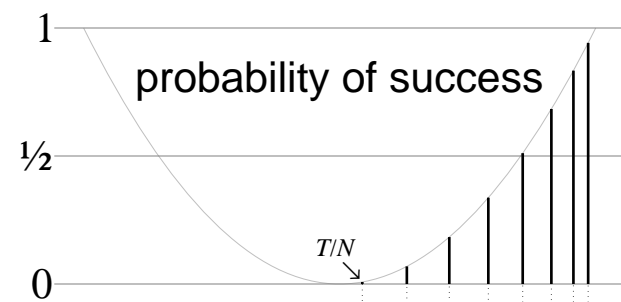
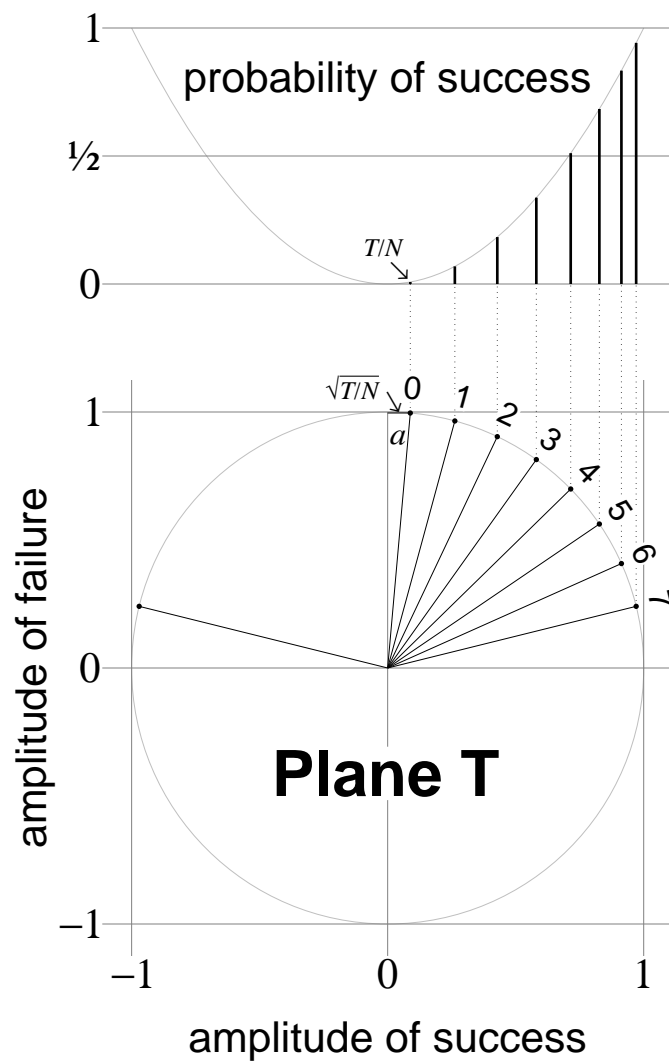
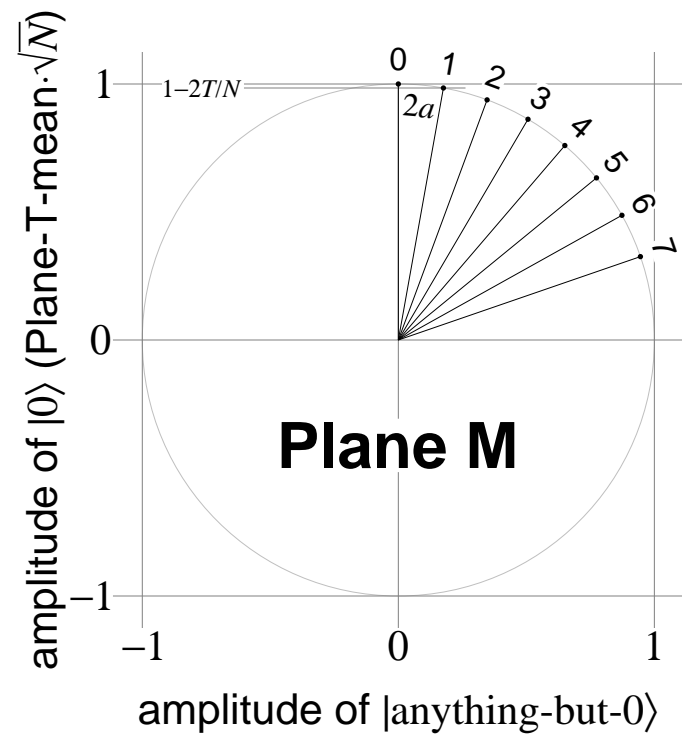


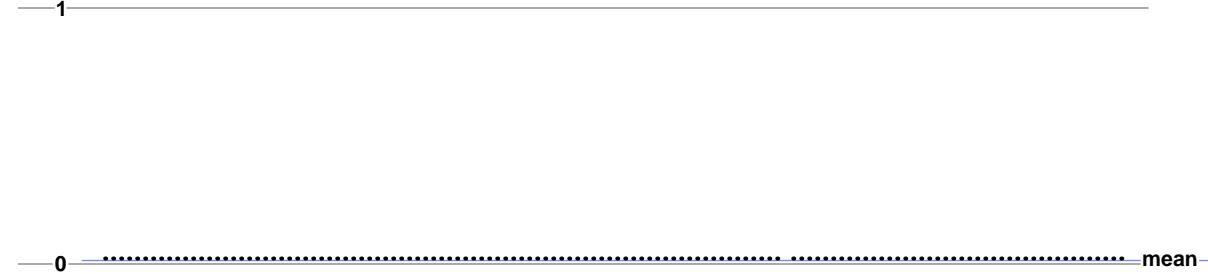
$$N = 128, T = 1$$



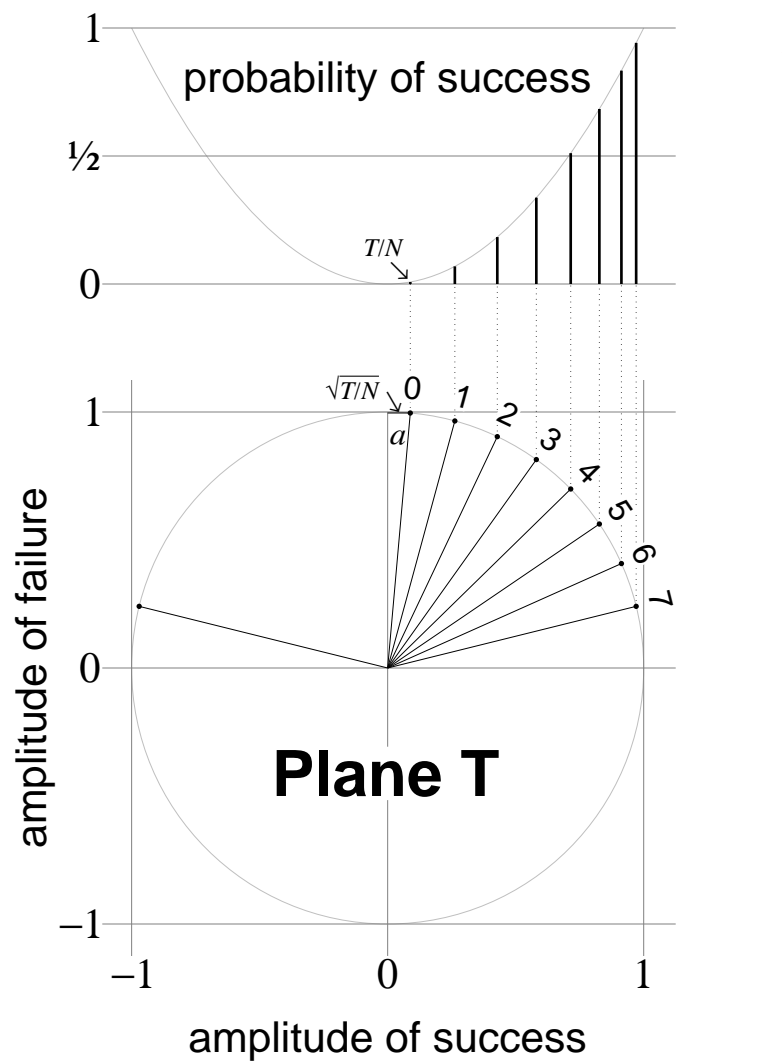
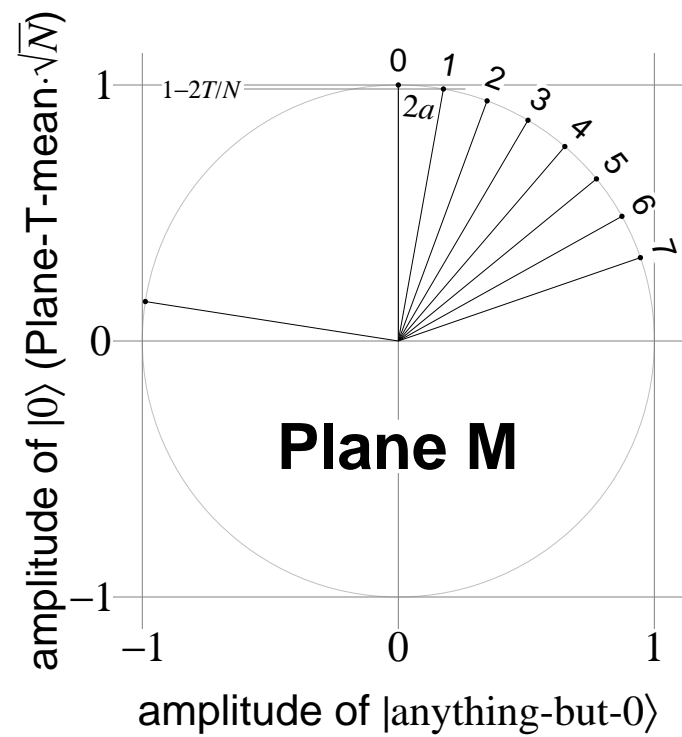


$$N = 128, T = 1$$



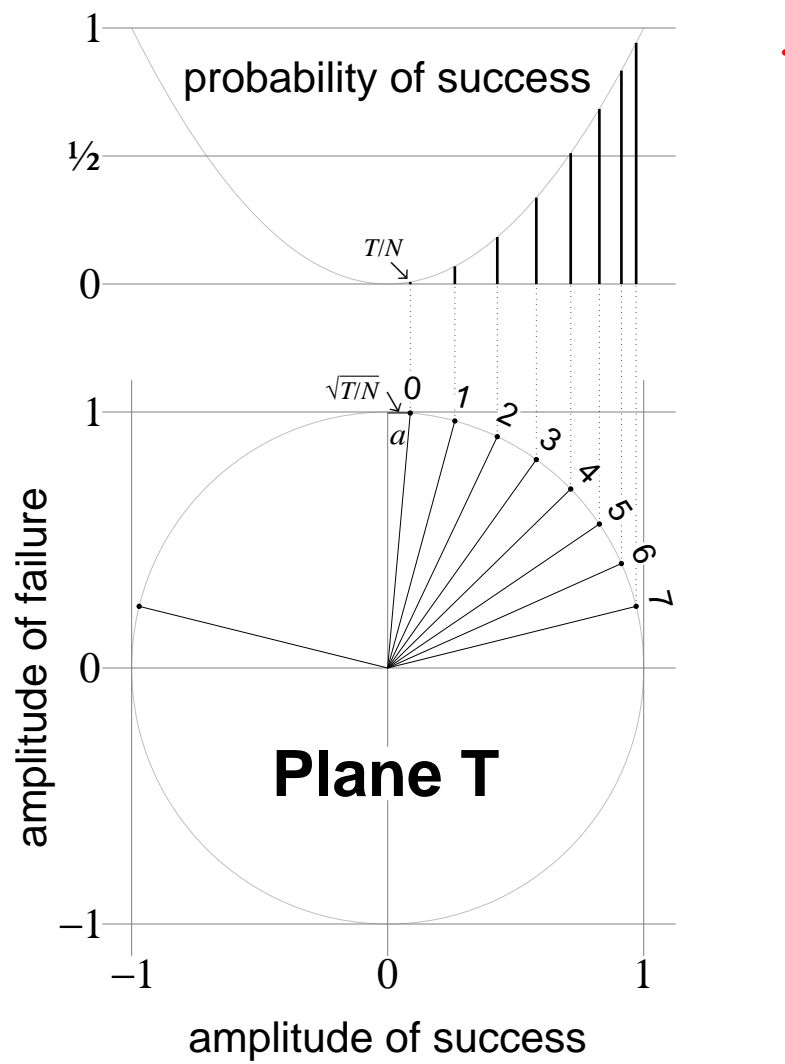
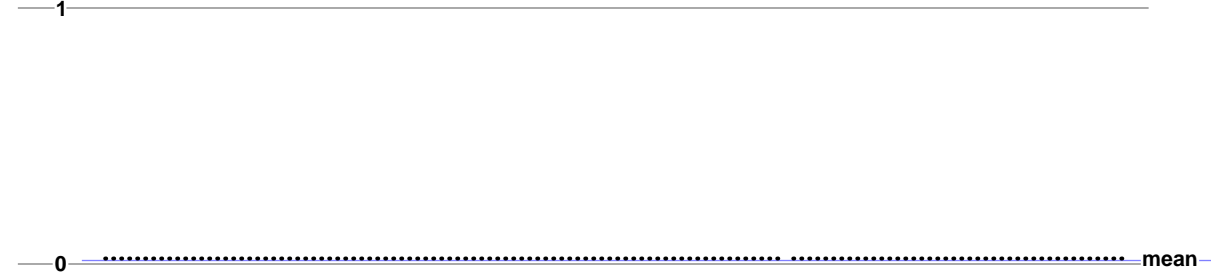
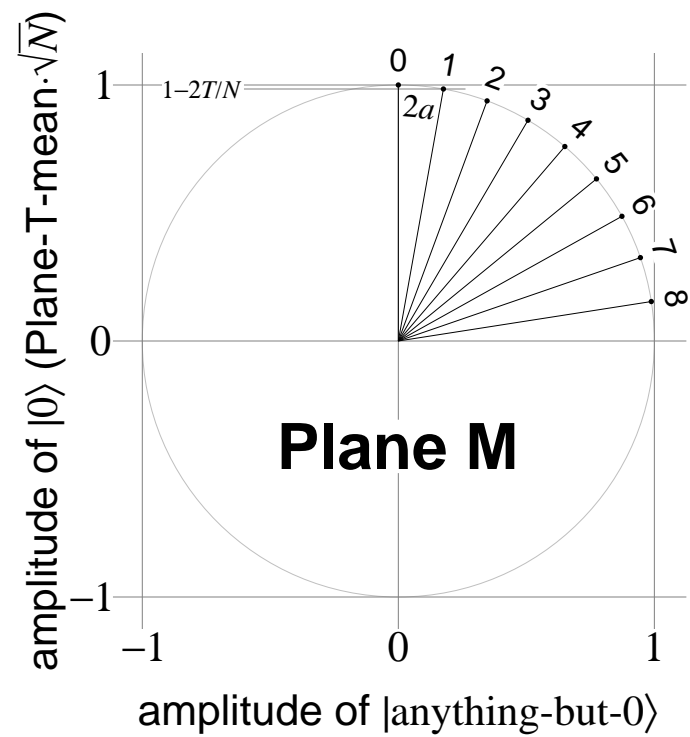


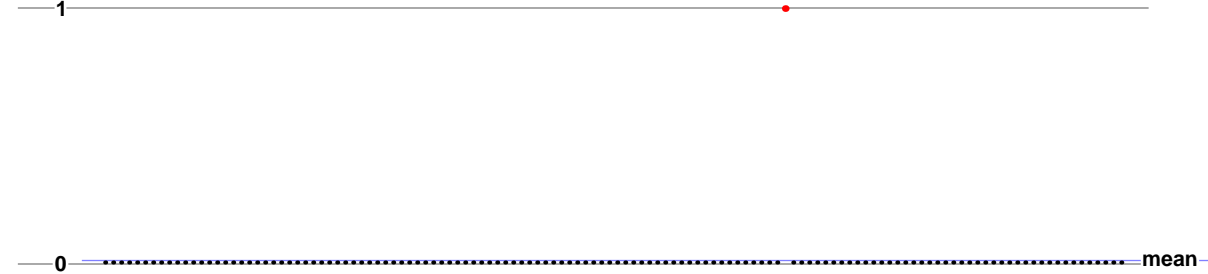
$$N = 128, \quad T = 1$$



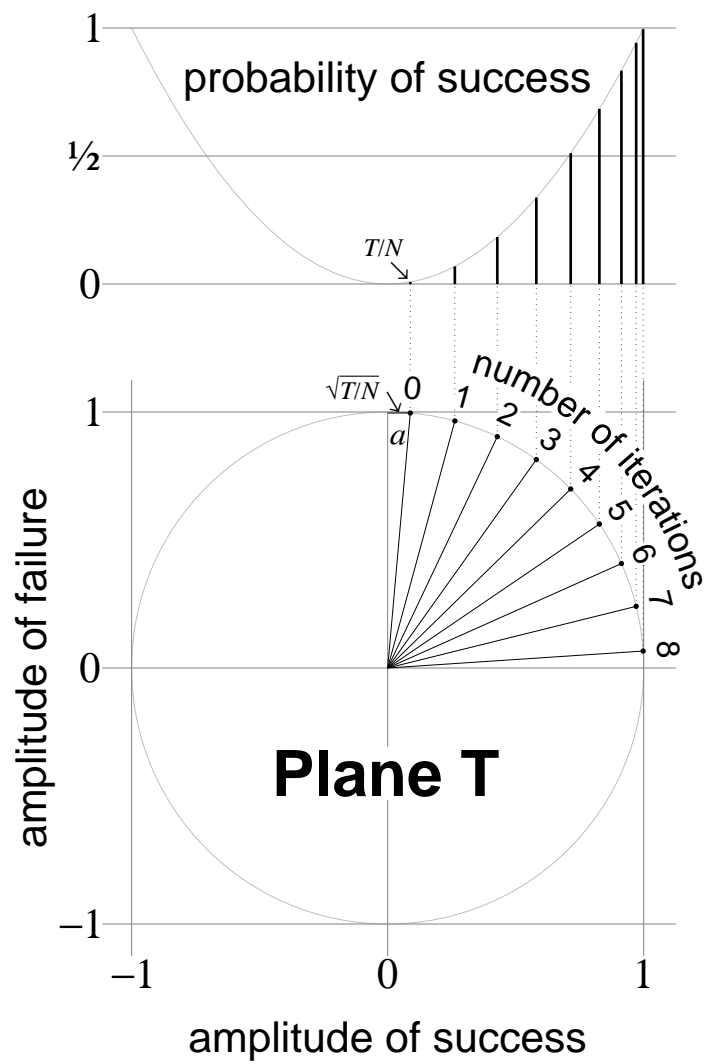
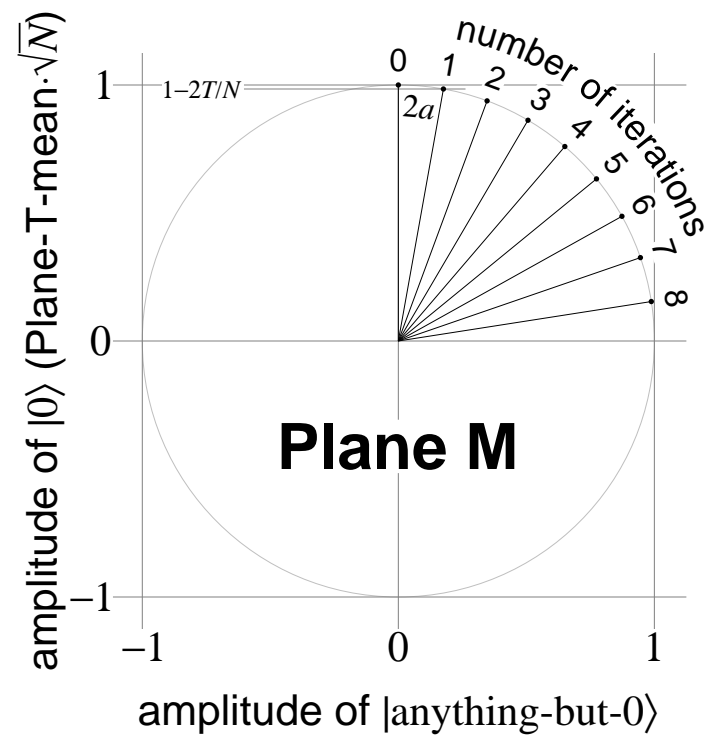


$$N = 128, T = 1$$

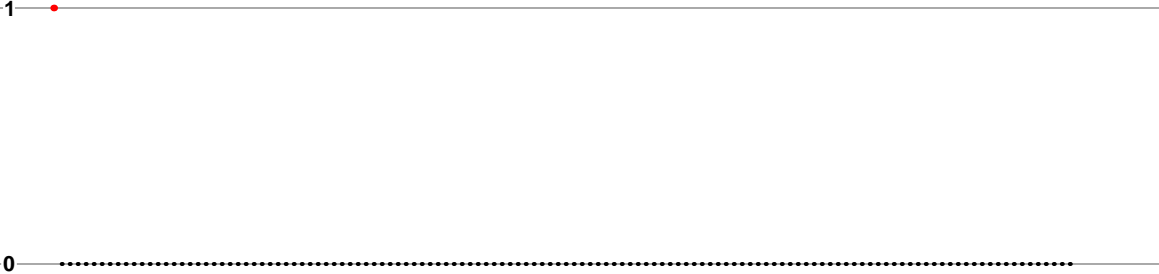




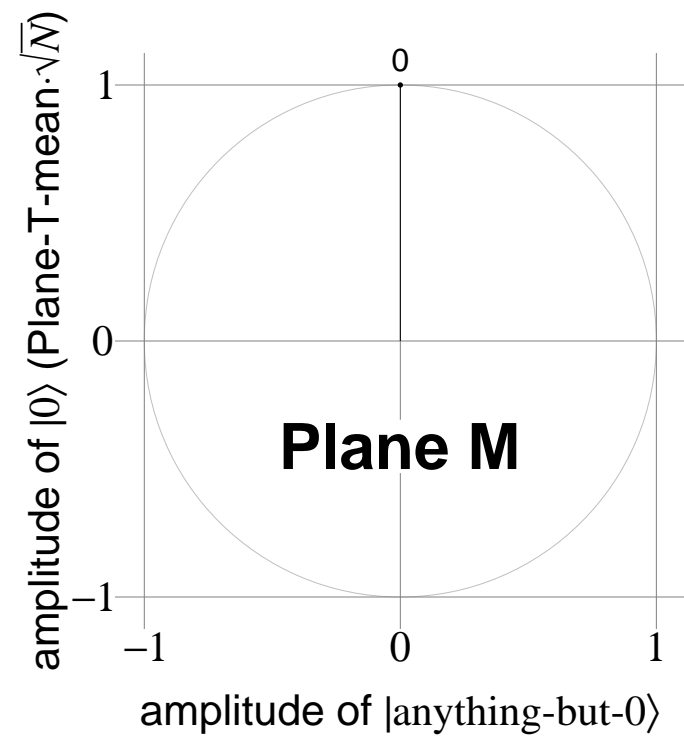
$$N = 128, T = 1$$

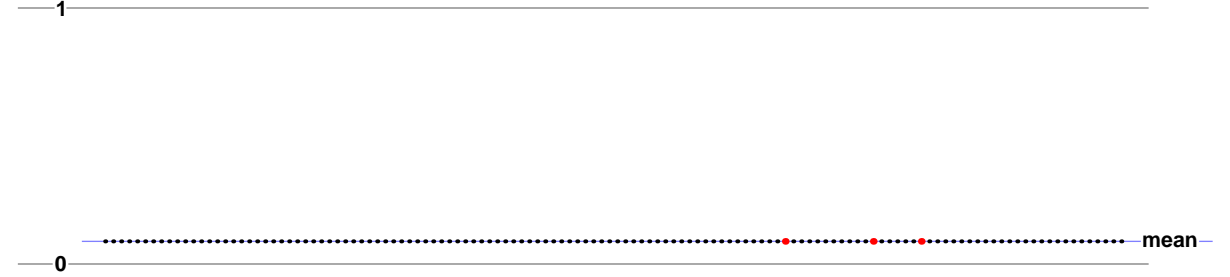
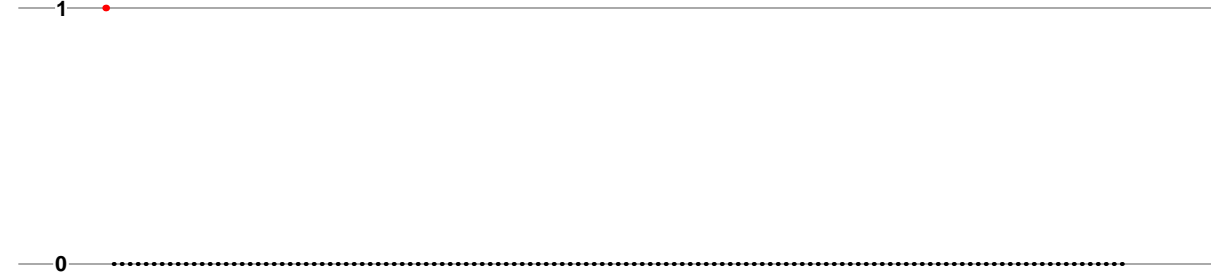


Grover's Algorithm, Triple Target

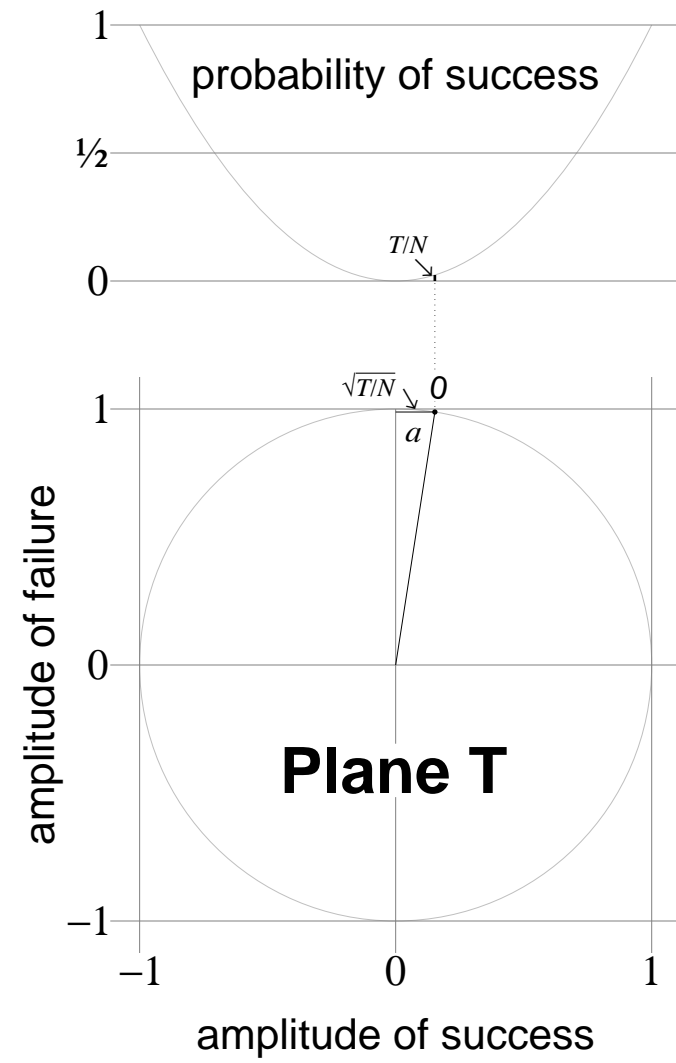
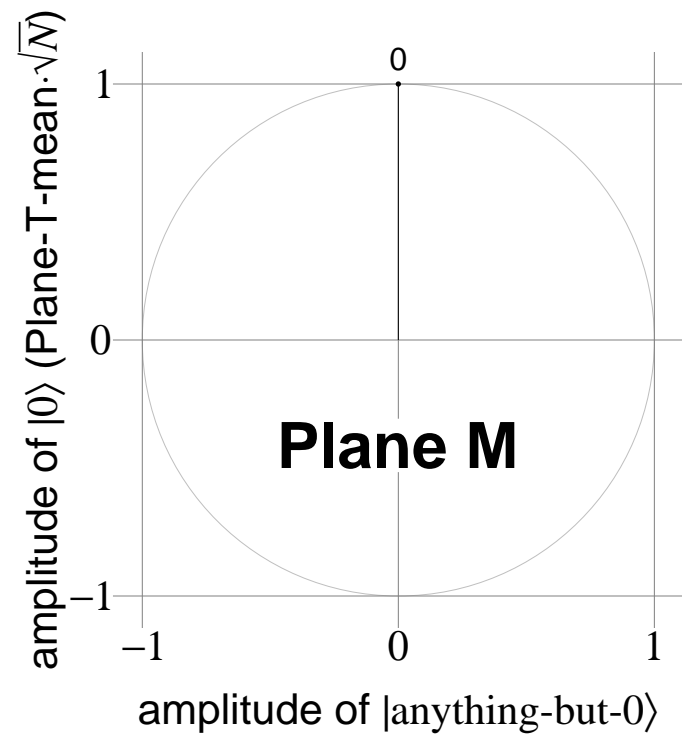


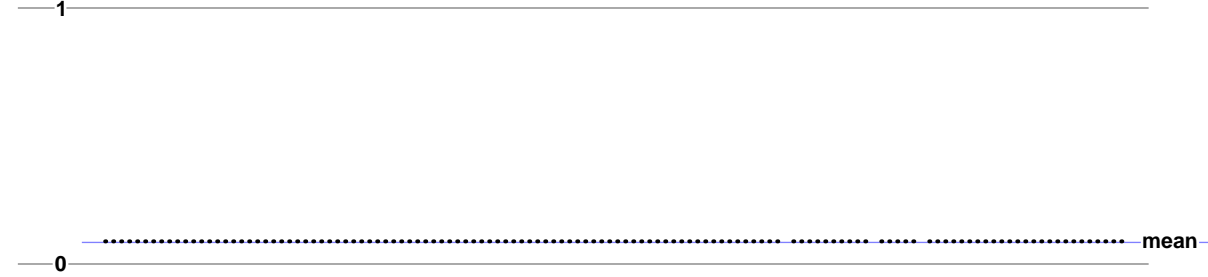
$$N = 128, \quad T = 3$$



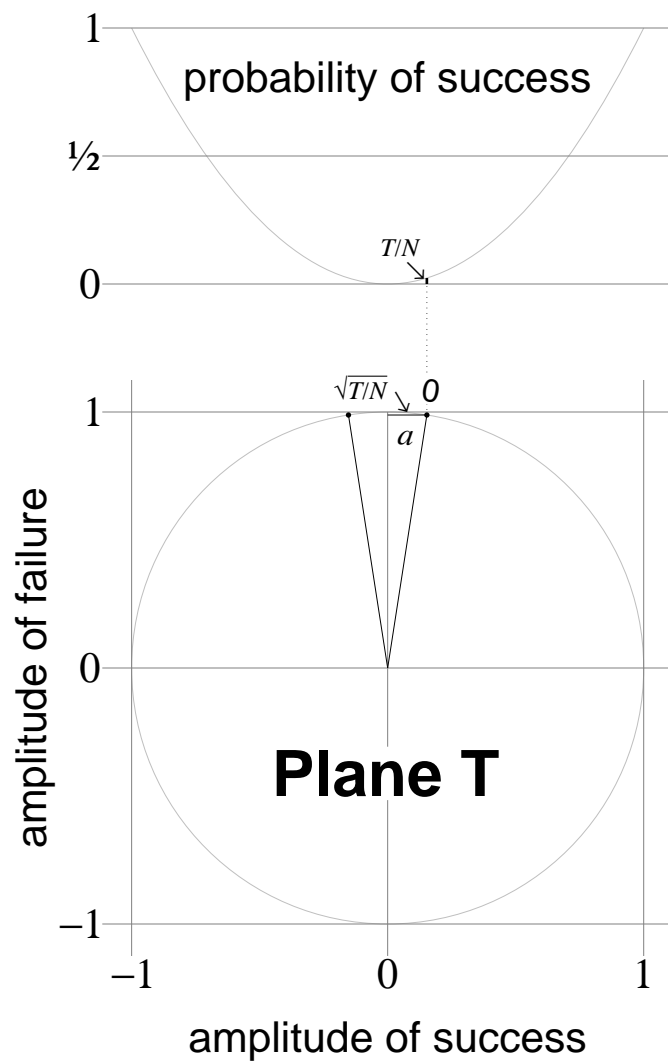
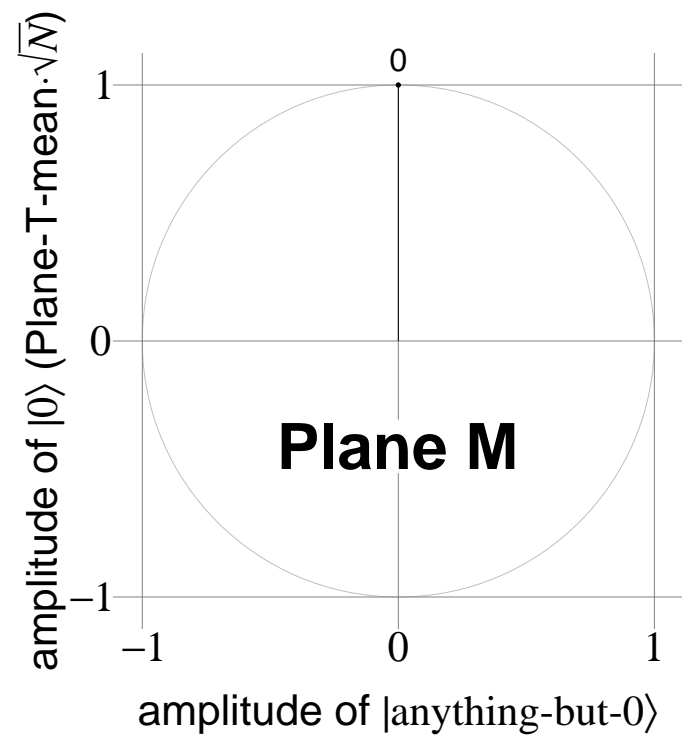


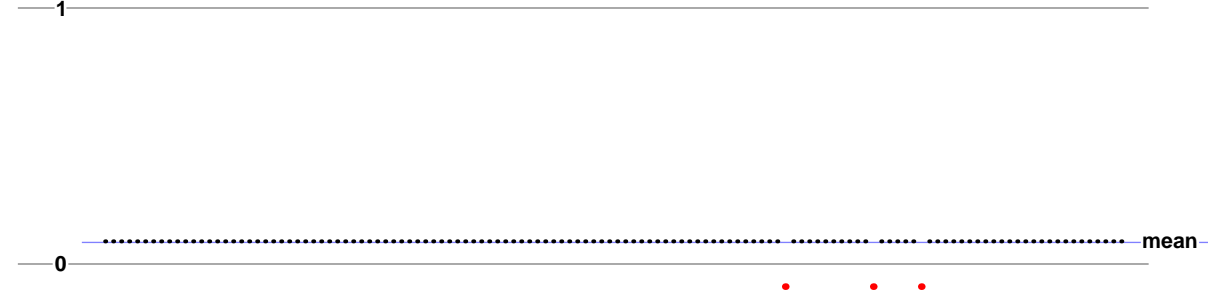
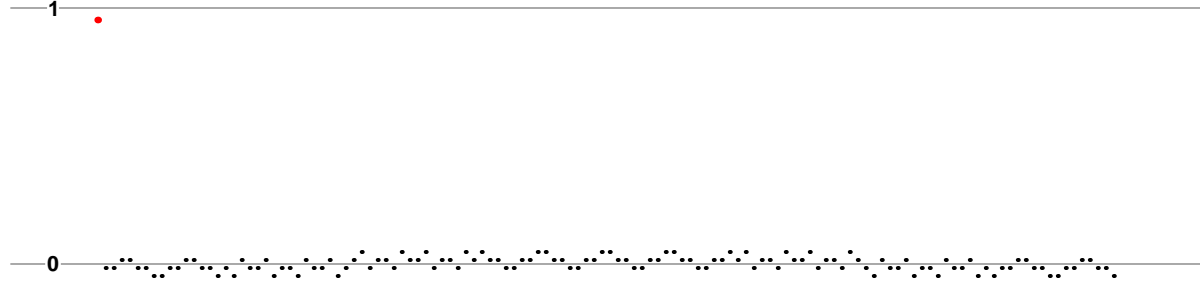
$$N = 128, T = 3$$



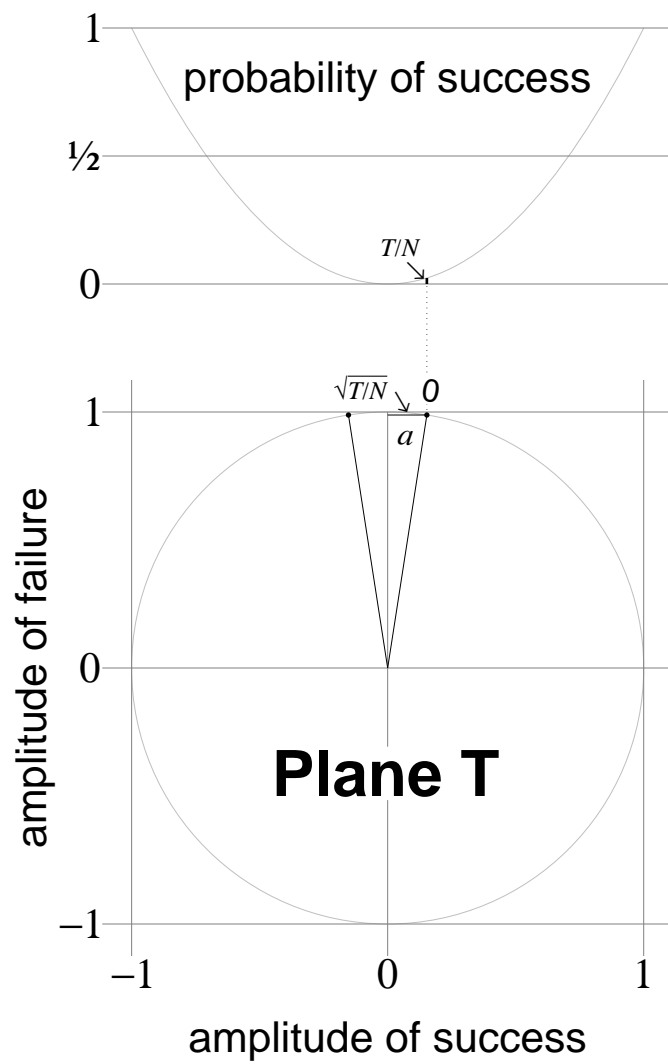
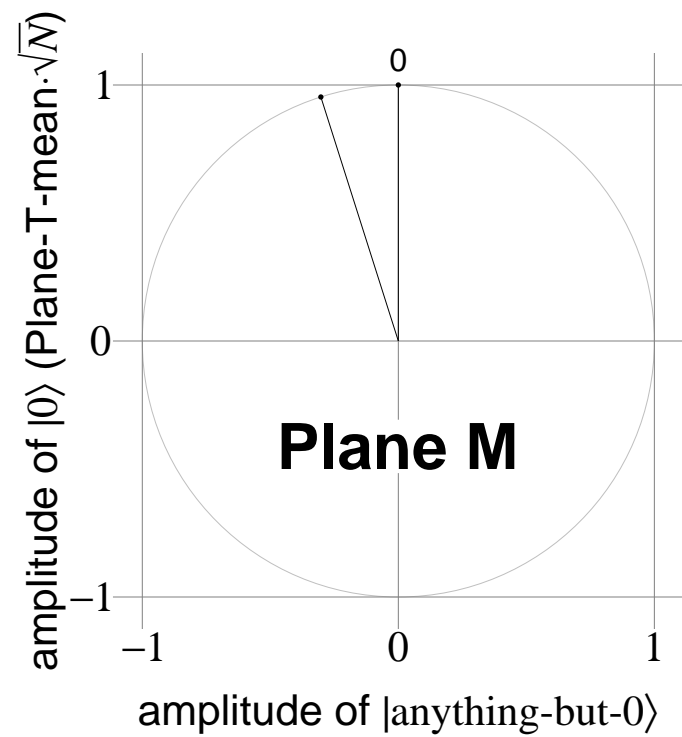


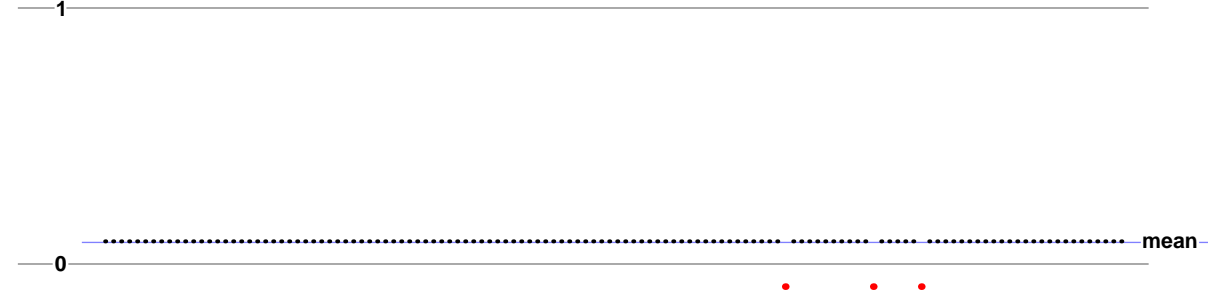
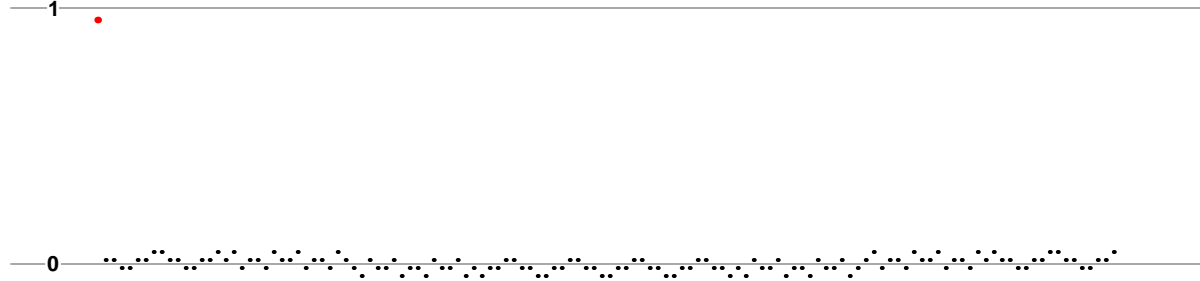
$$N = 128, \quad T = 3$$



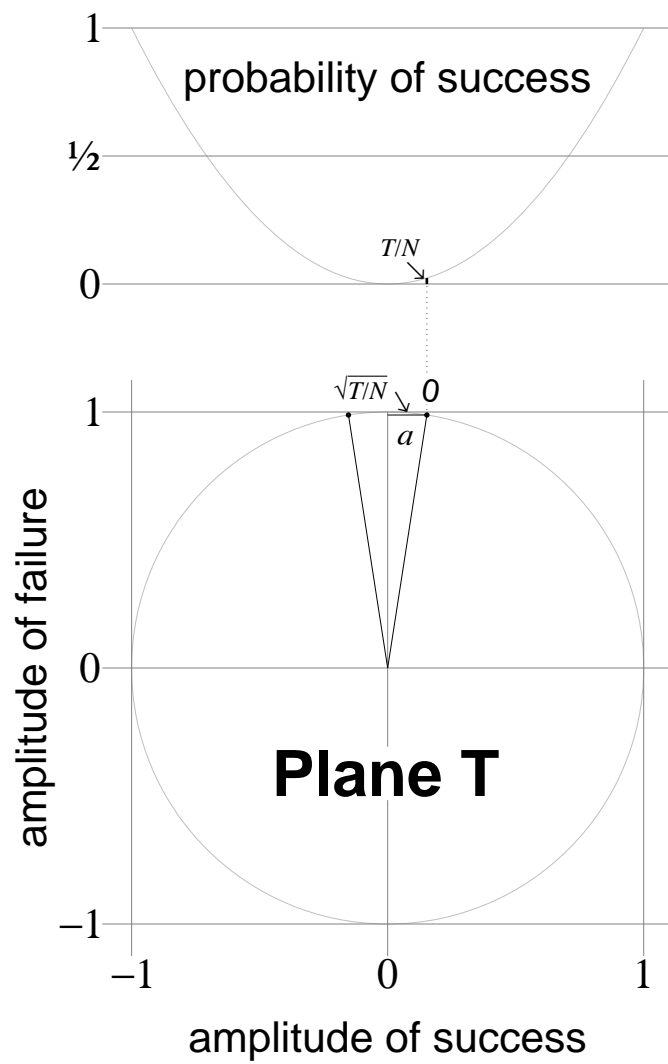
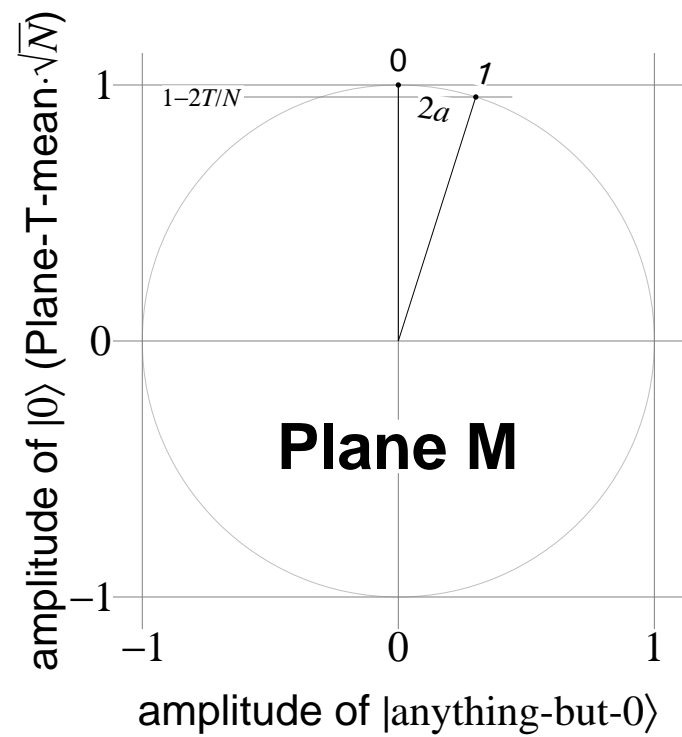


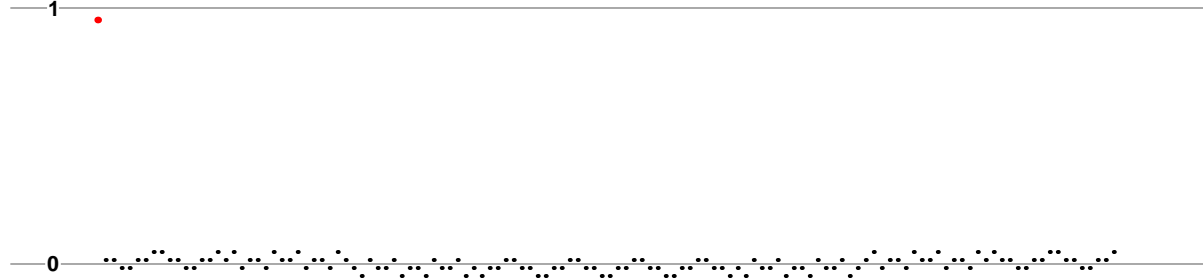
$$N = 128, T = 3$$



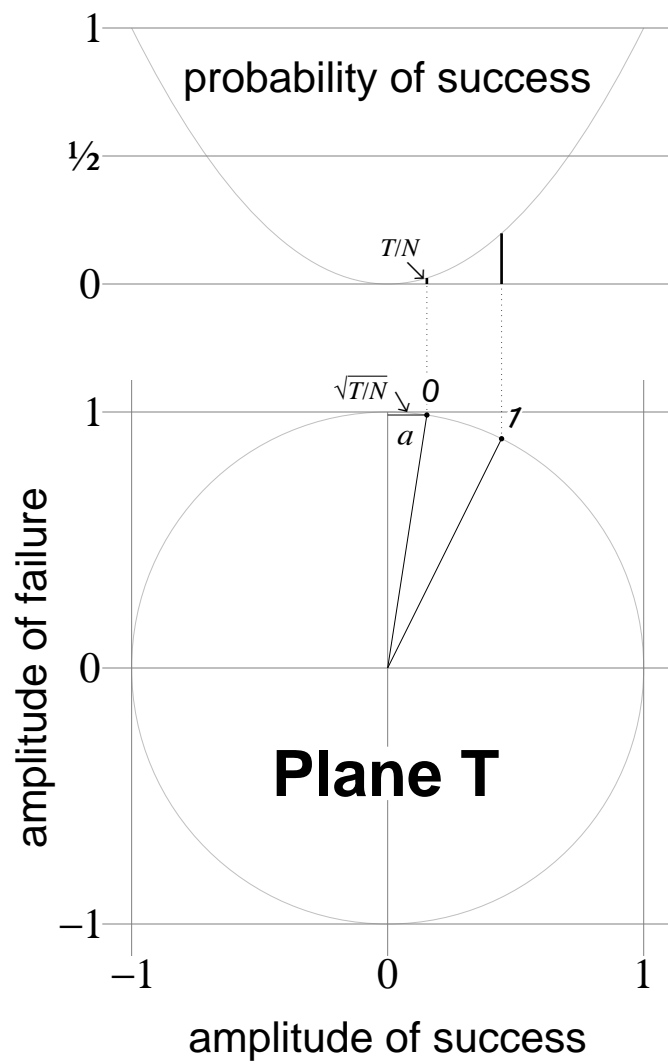
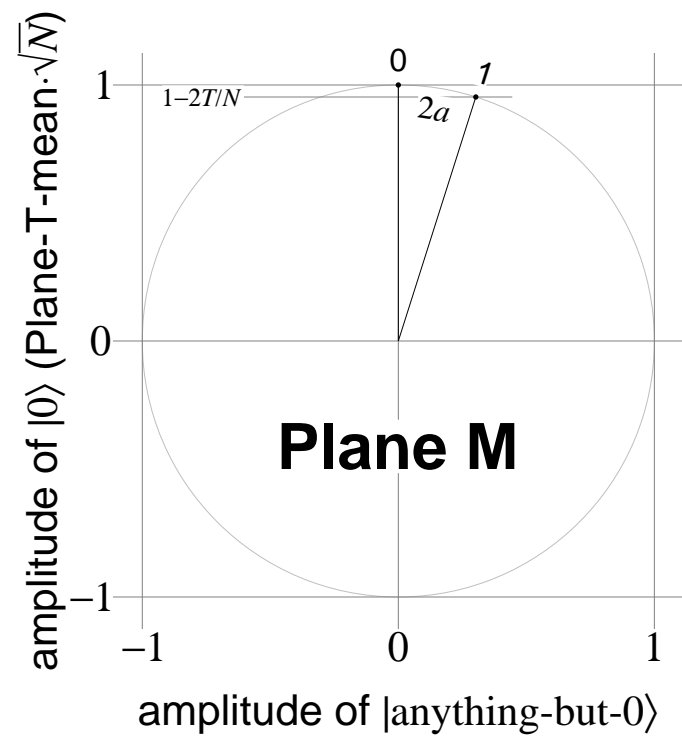


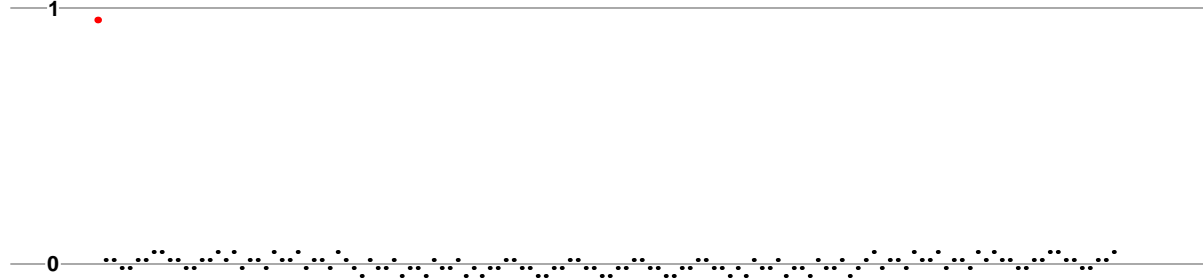
$$N = 128, T = 3$$



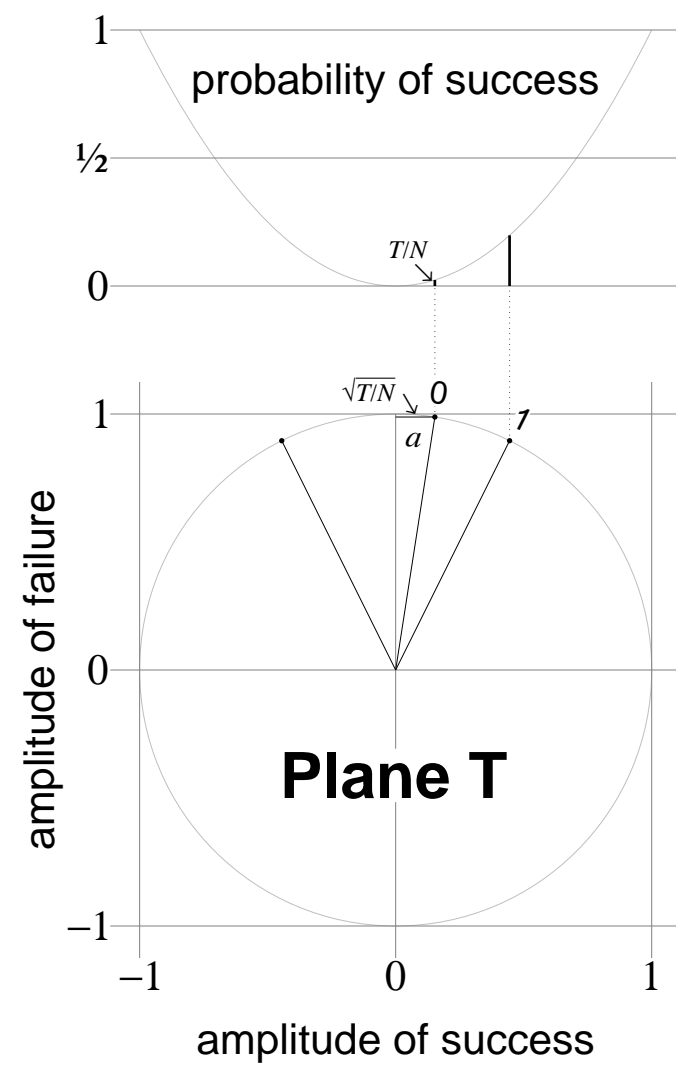
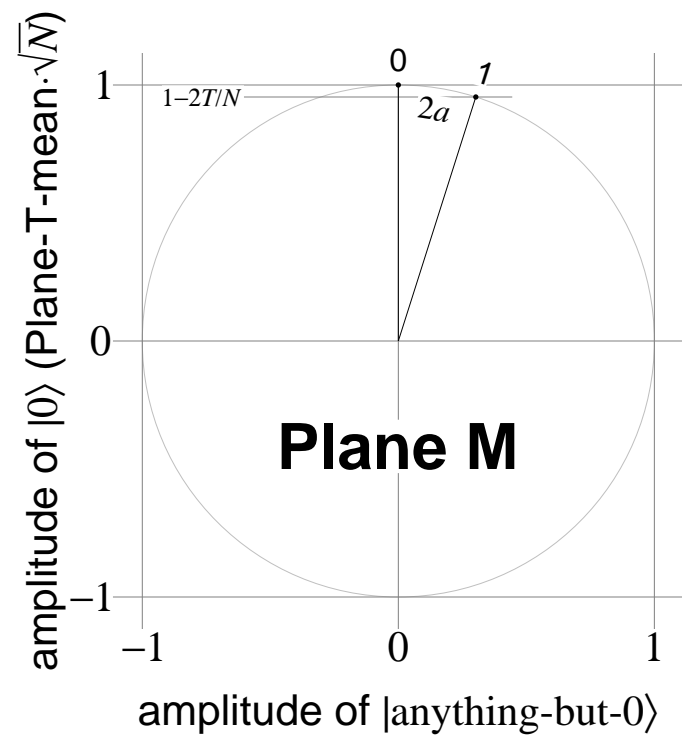


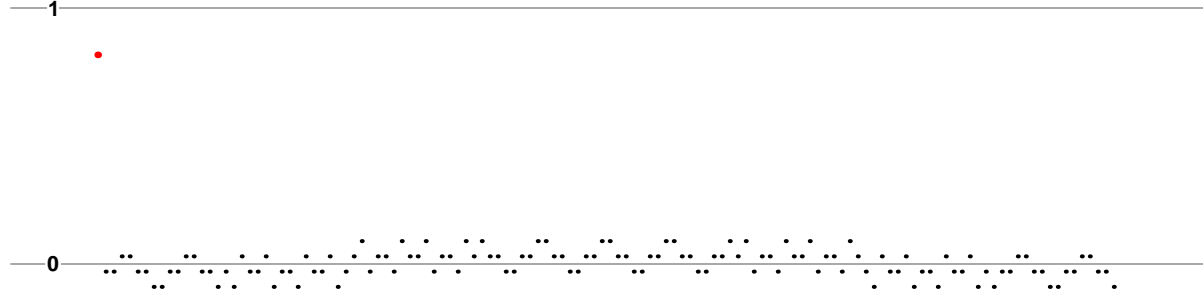
$$N = 128, T = 3$$



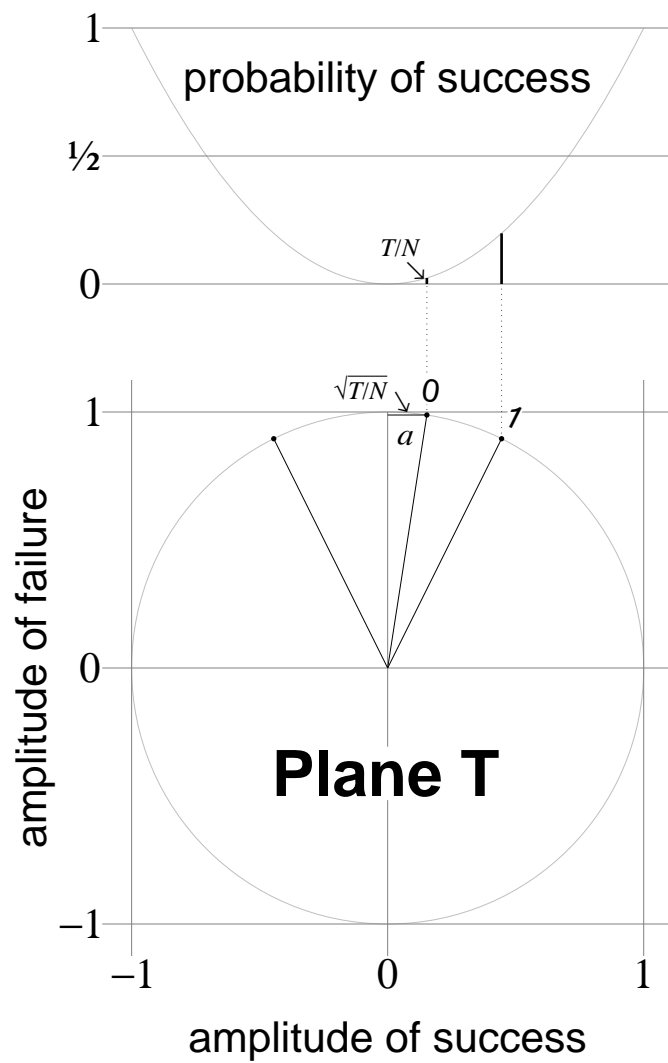
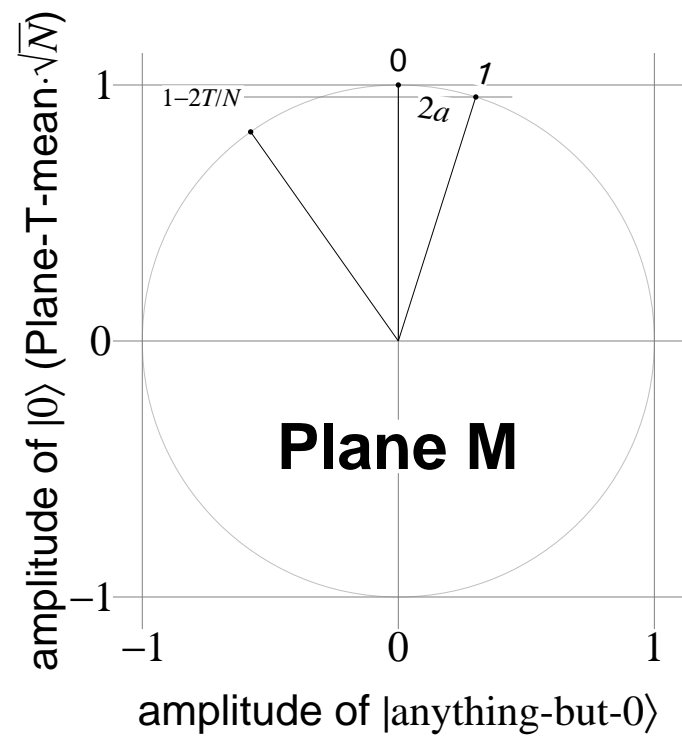


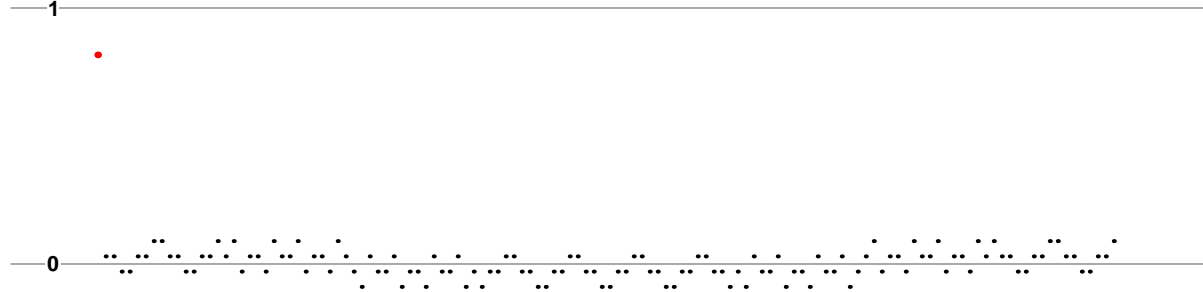
$$N = 128, T = 3$$



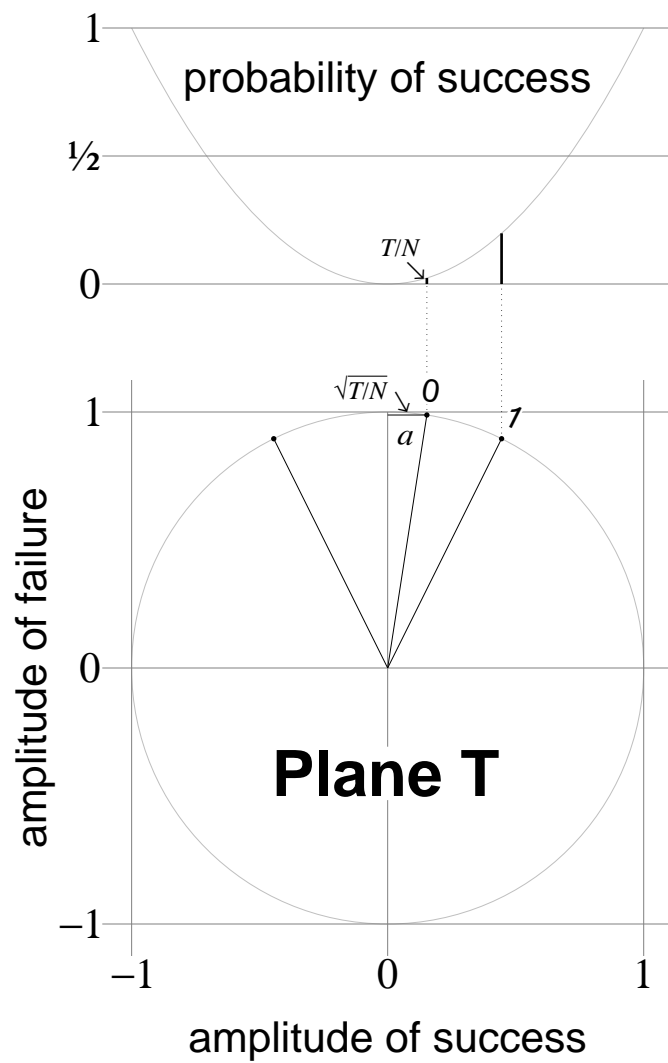
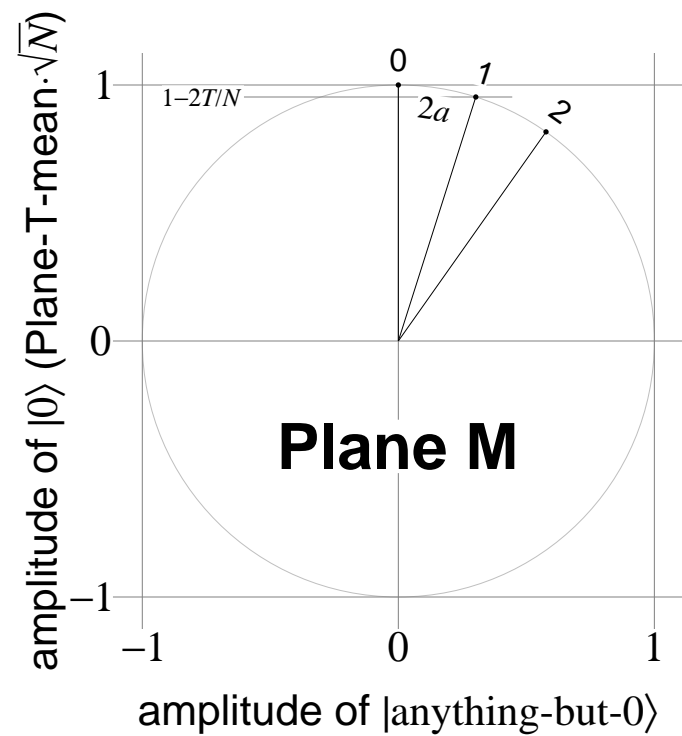


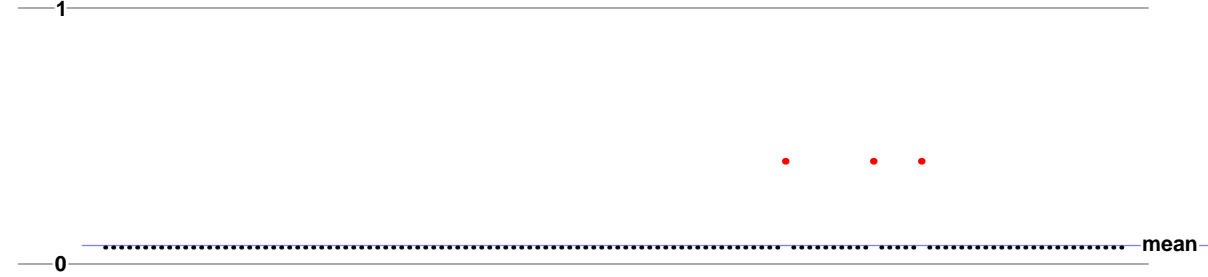
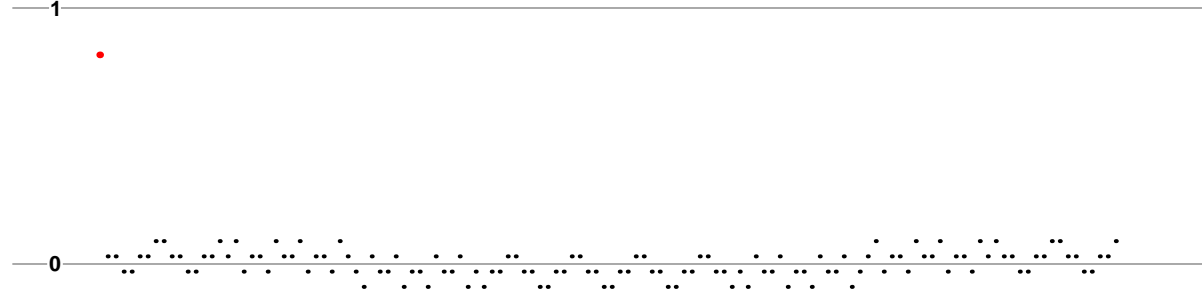
$$N = 128, T = 3$$



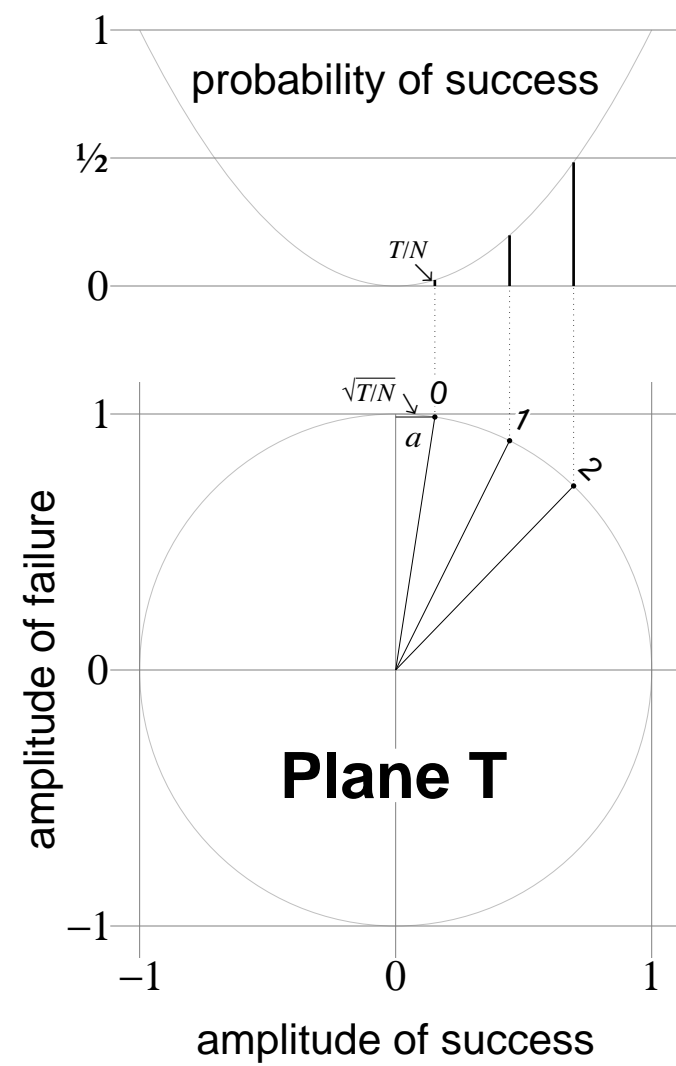
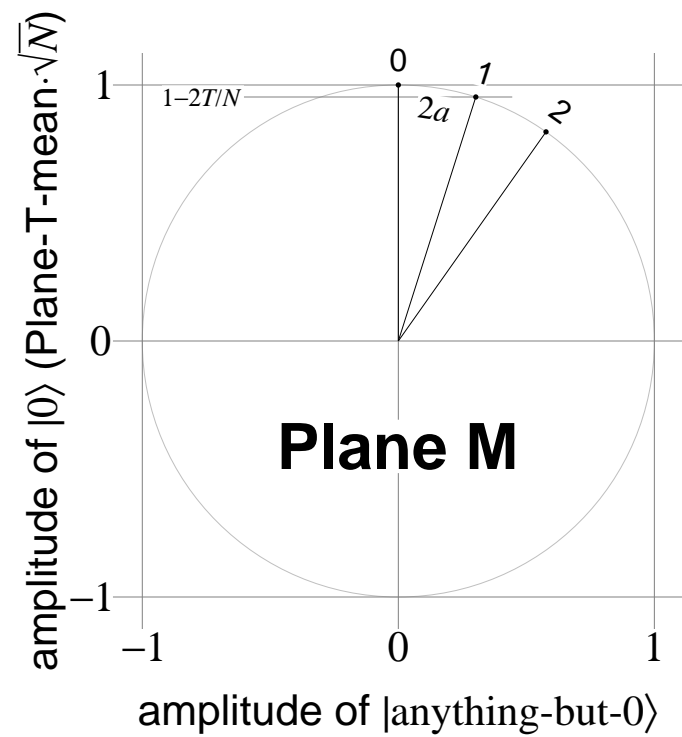


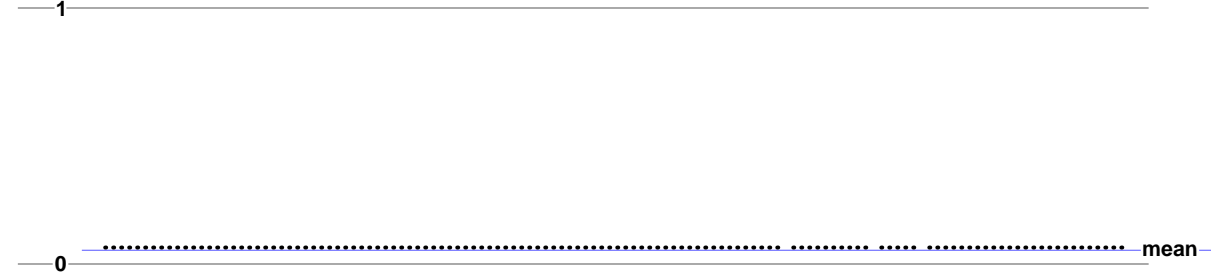
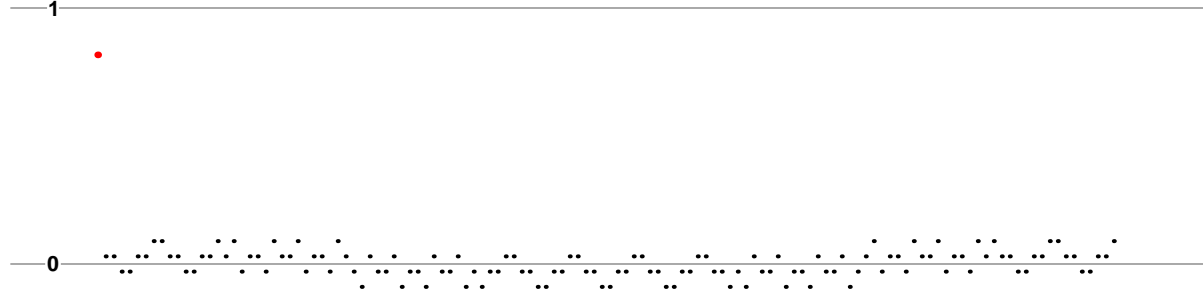
$$N = 128, T = 3$$



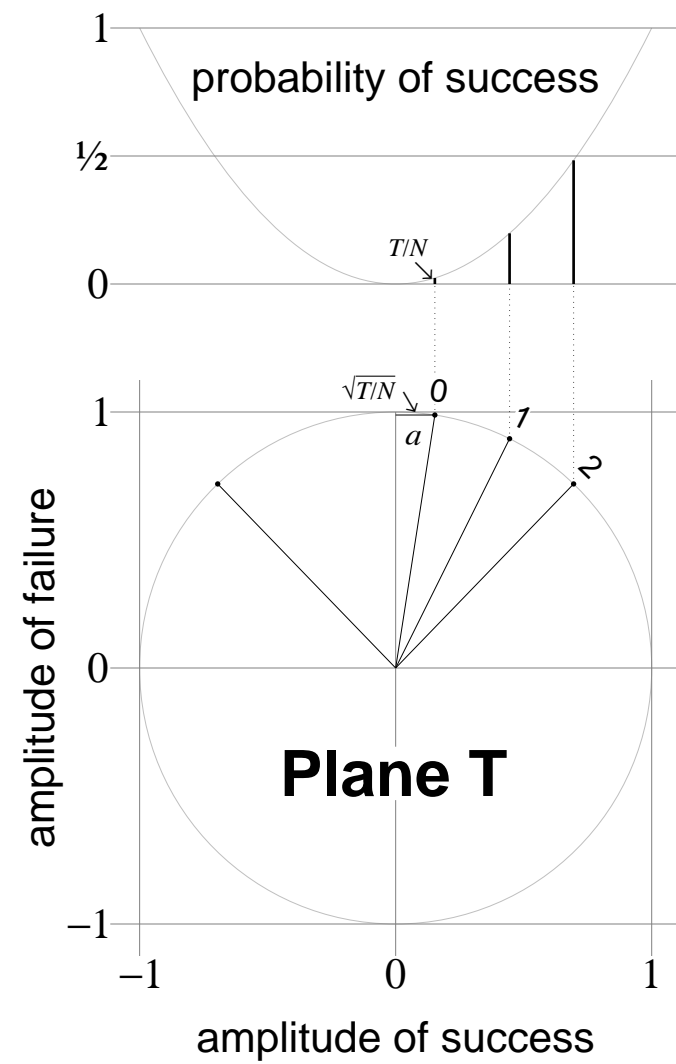
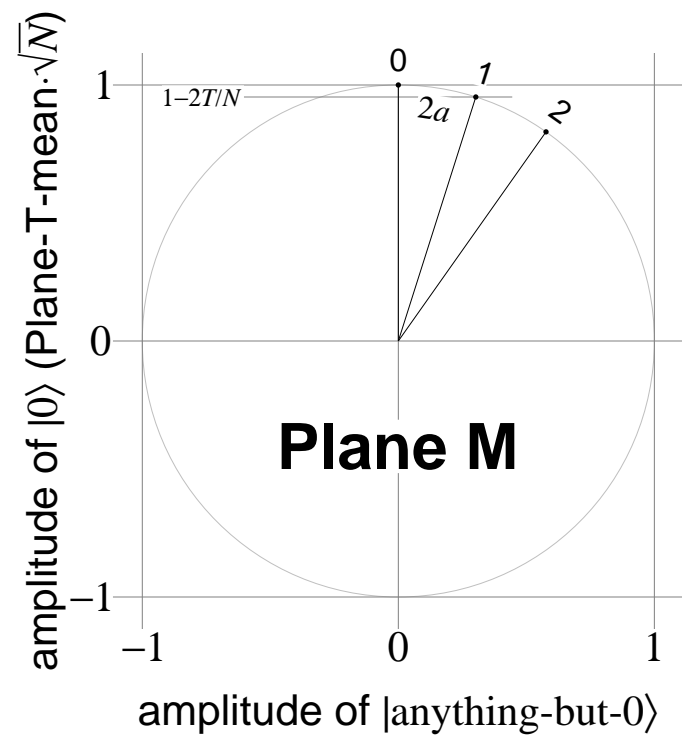


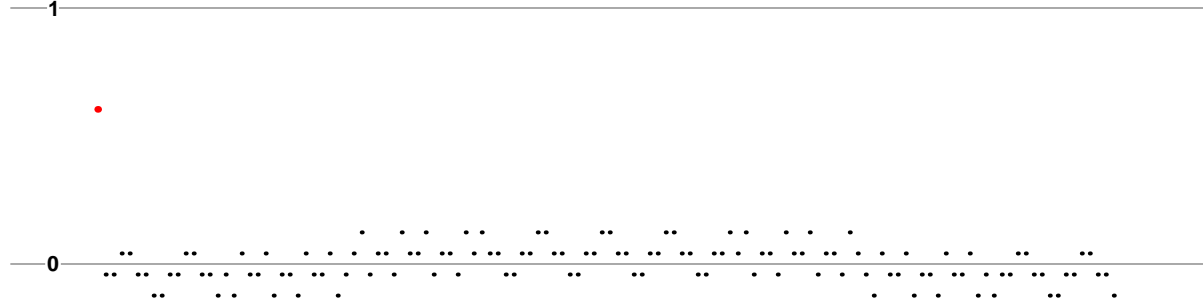
$$N = 128, T = 3$$



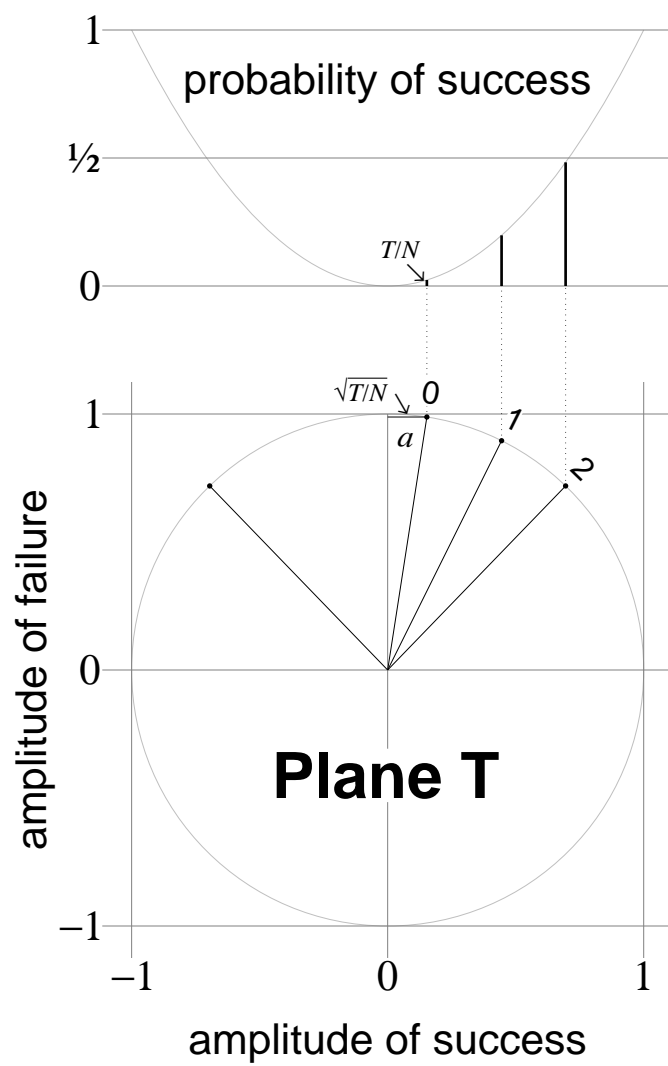
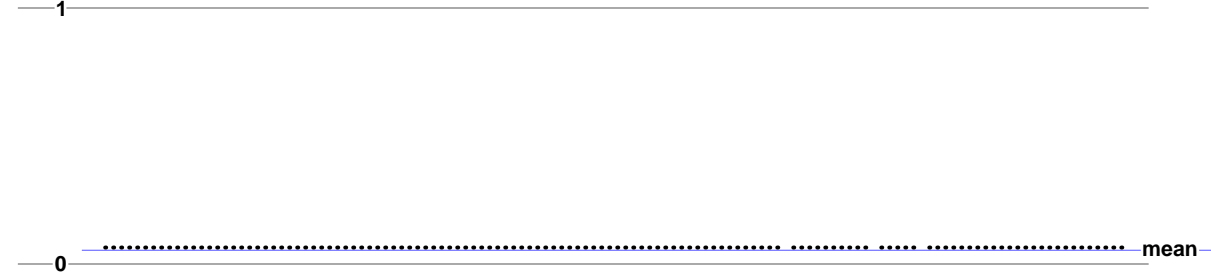
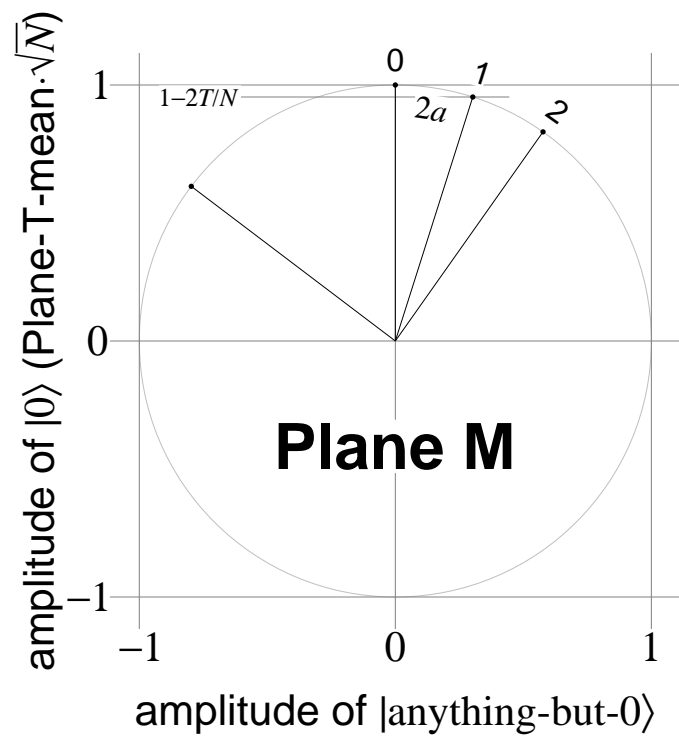


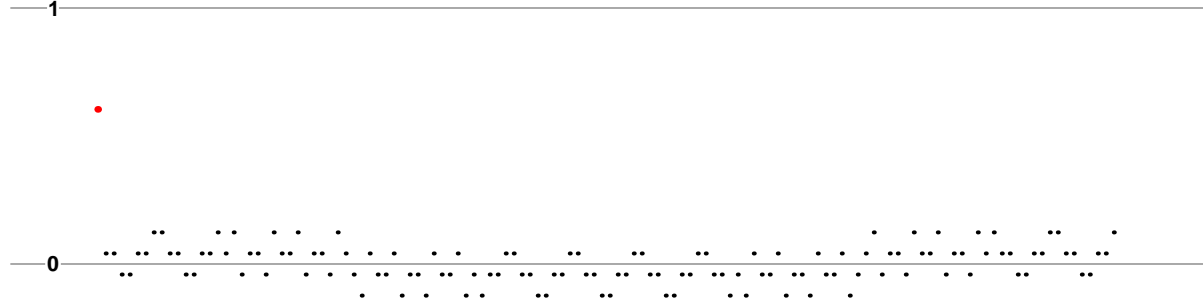
$$N = 128, T = 3$$



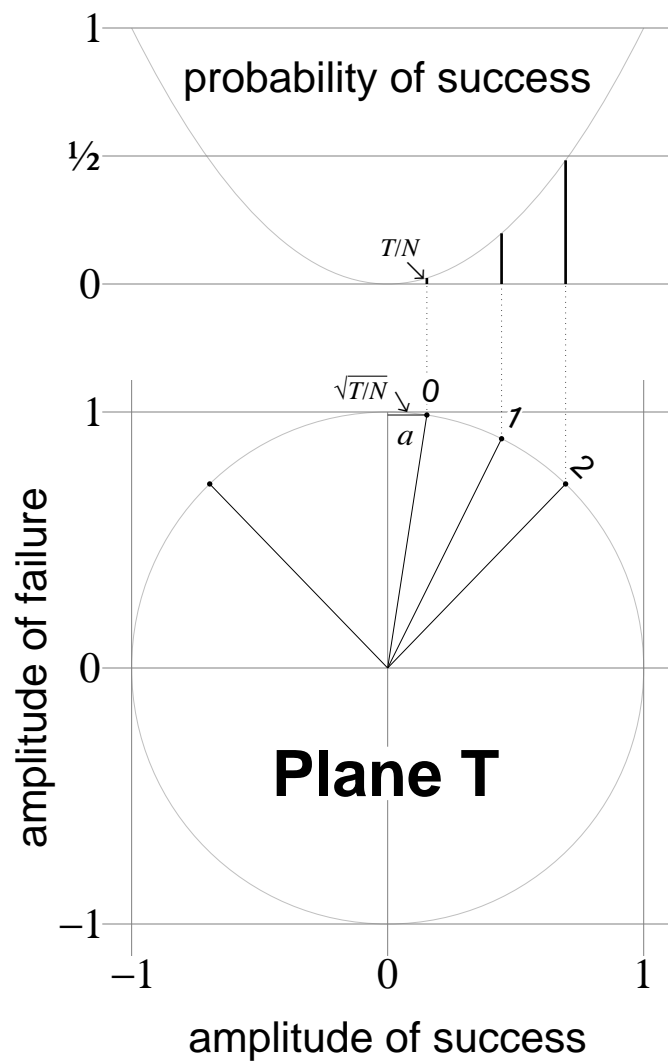
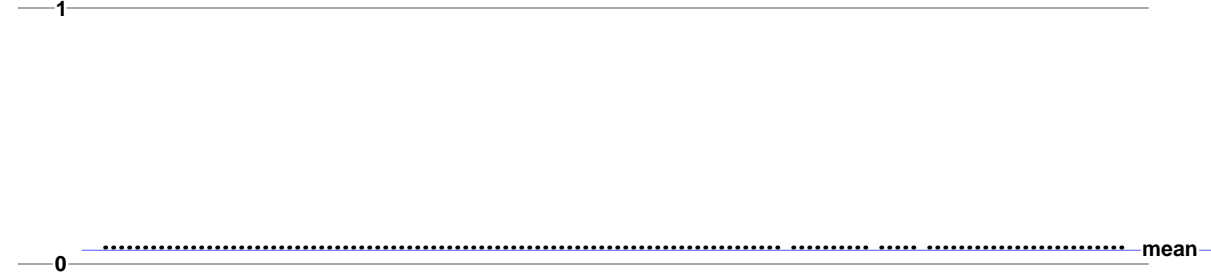
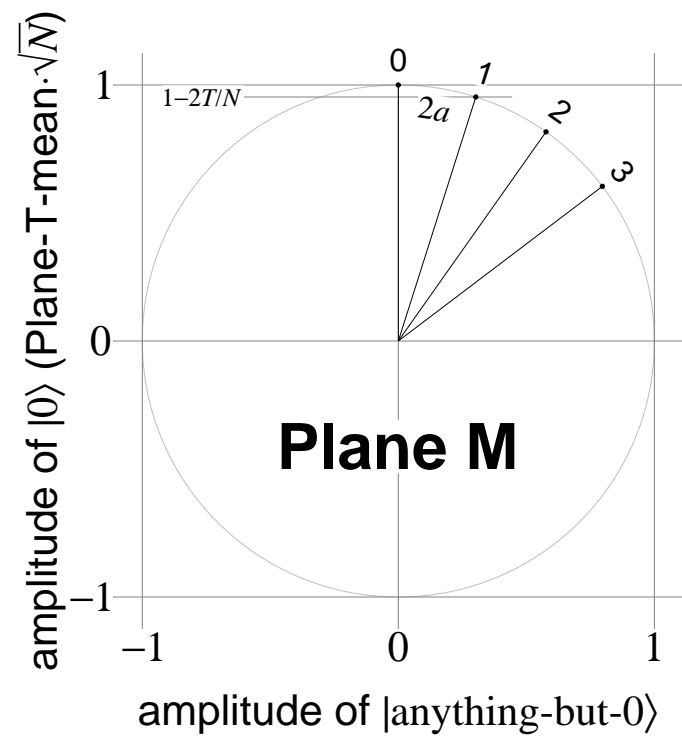


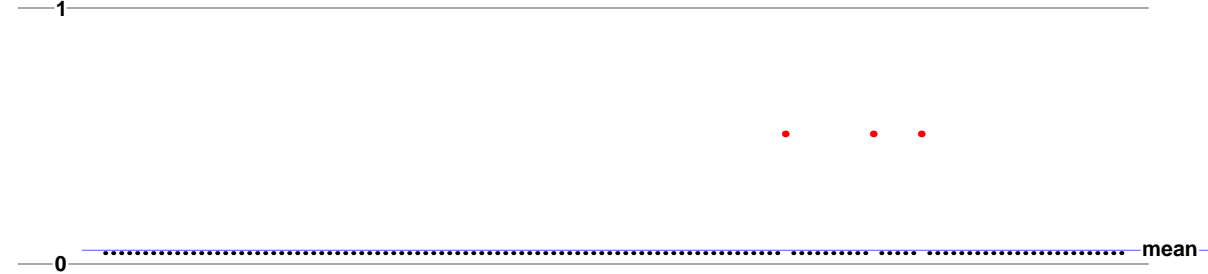
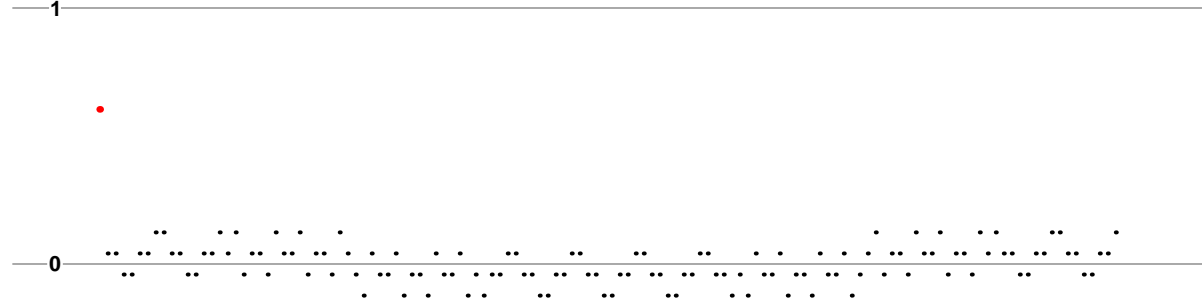
$$N = 128, T = 3$$



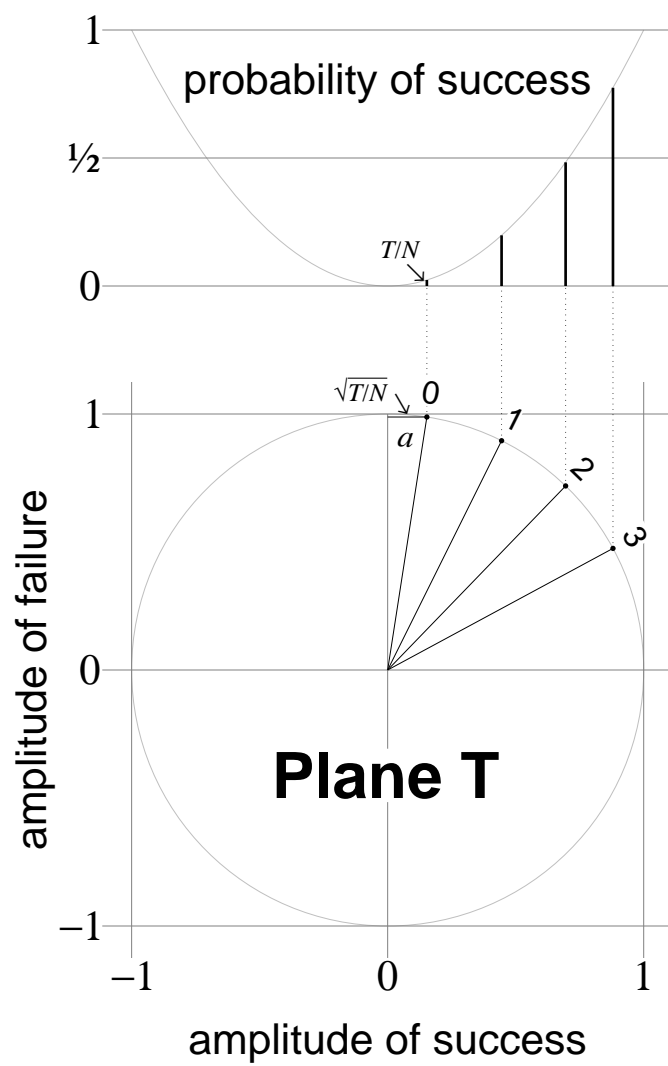
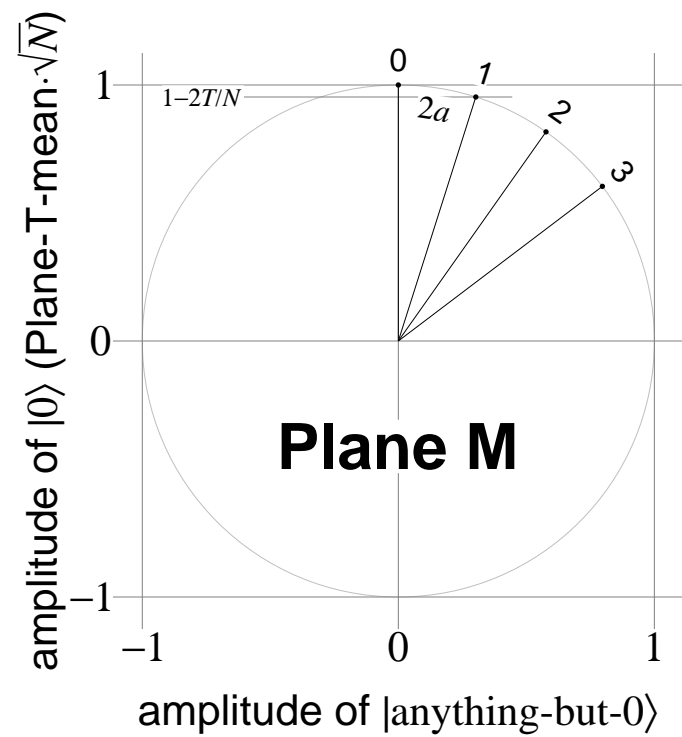


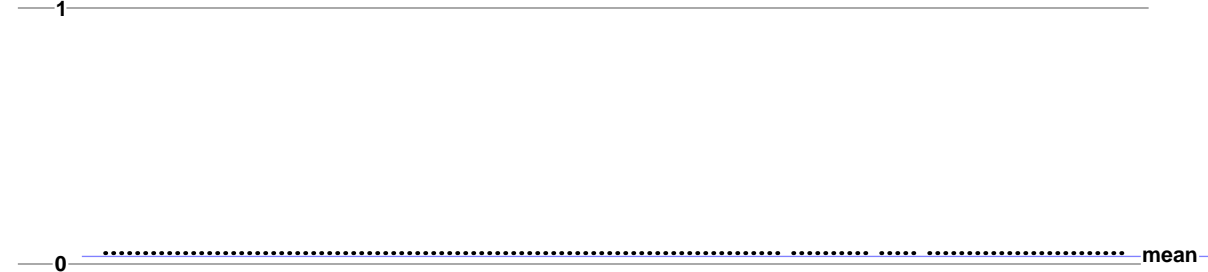
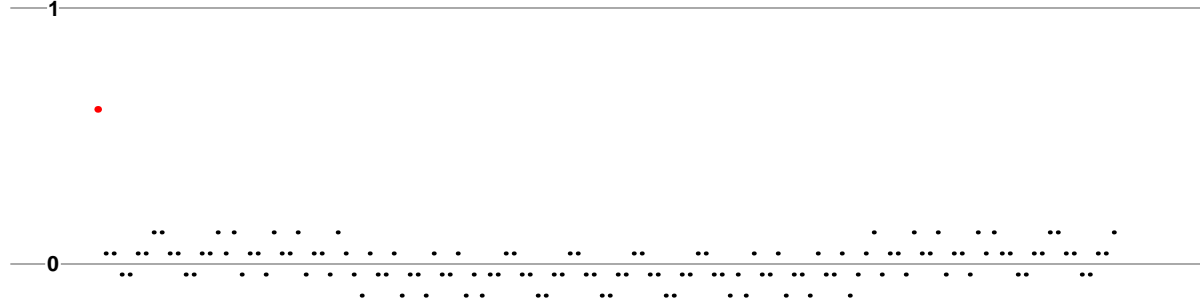
$$N = 128, T = 3$$



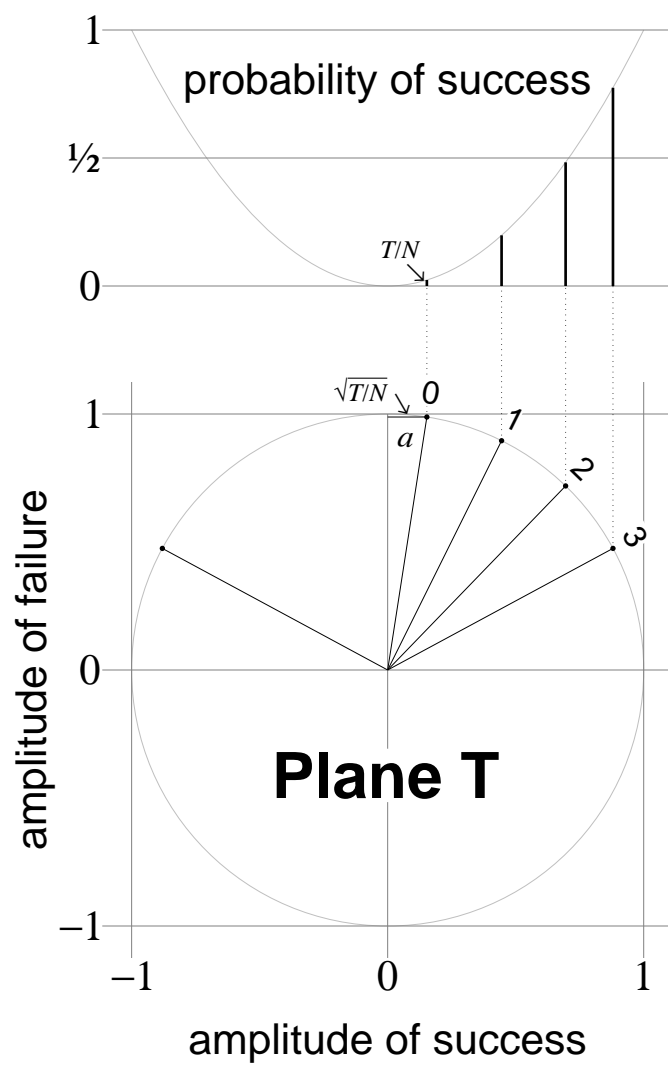
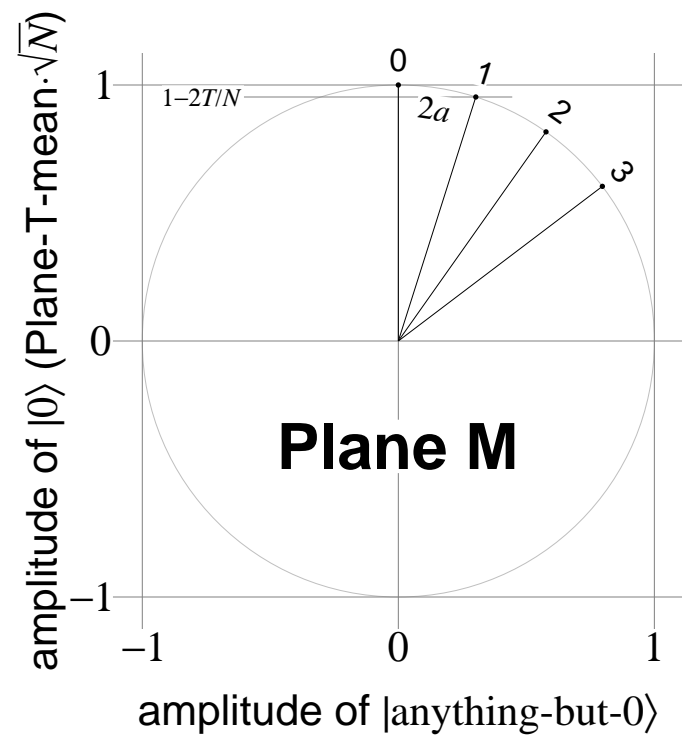


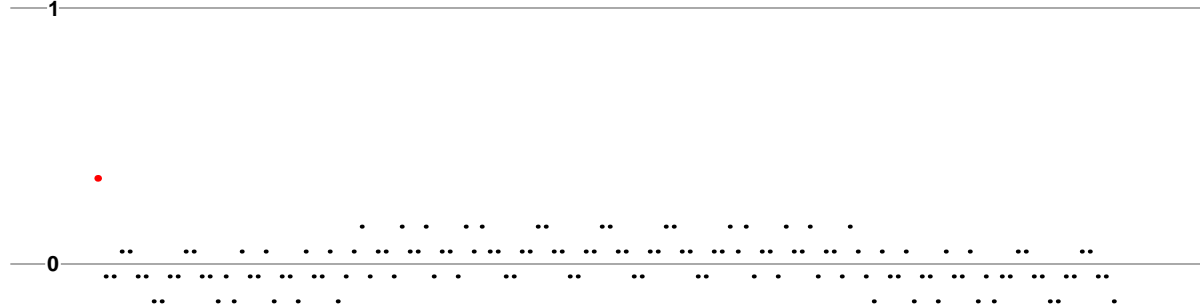
$$N = 128, T = 3$$



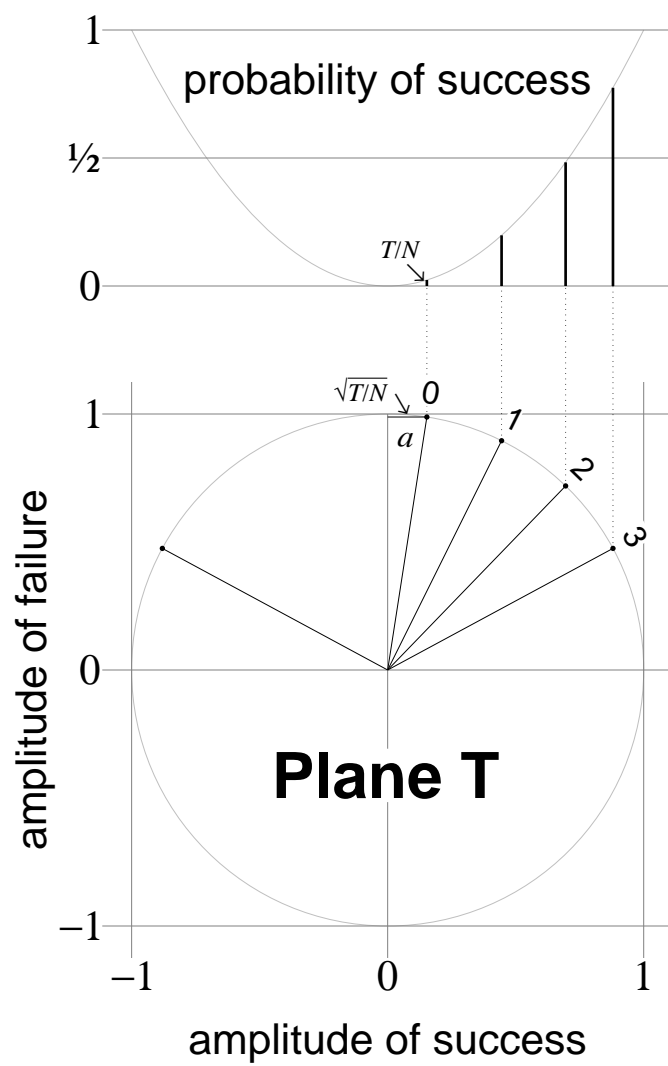
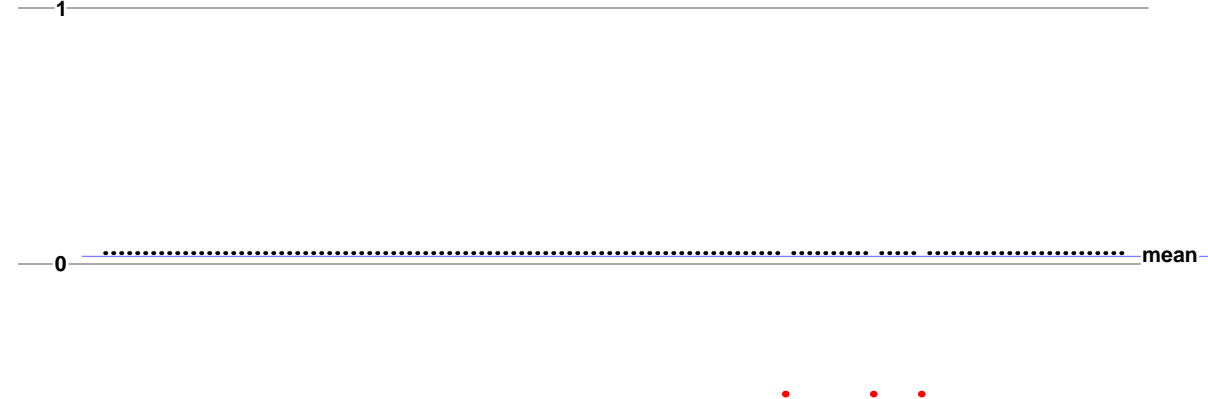
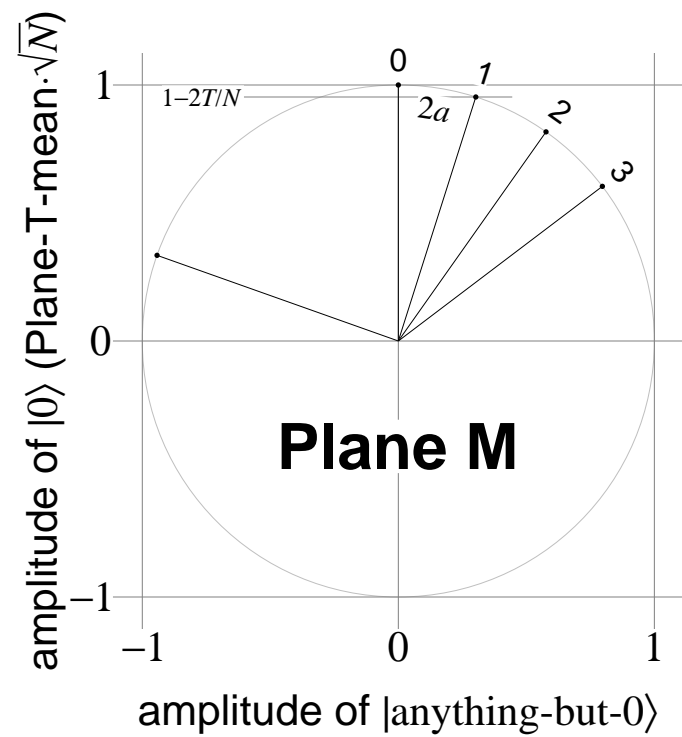


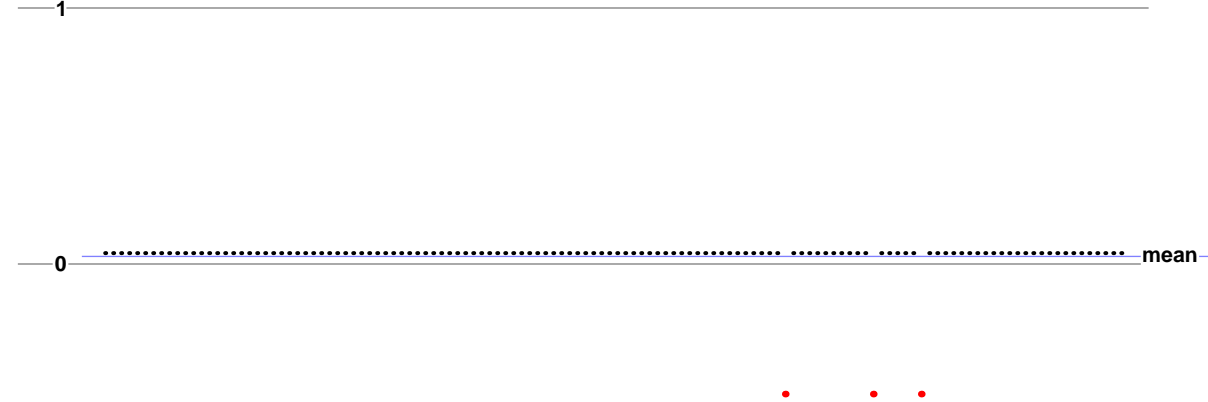
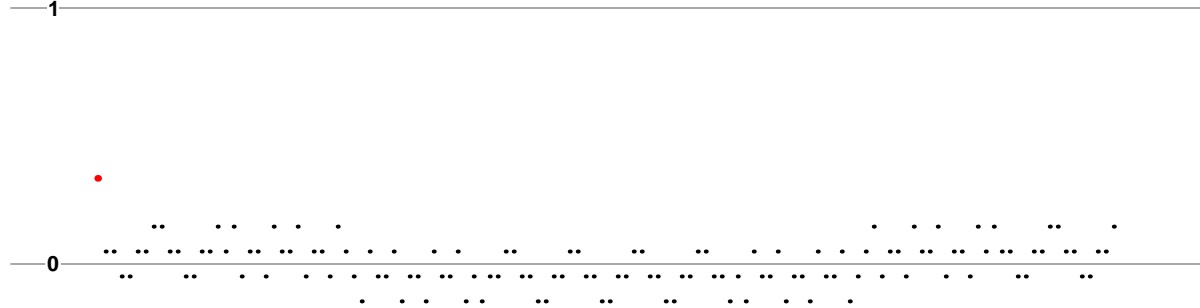
$$N = 128, T = 3$$



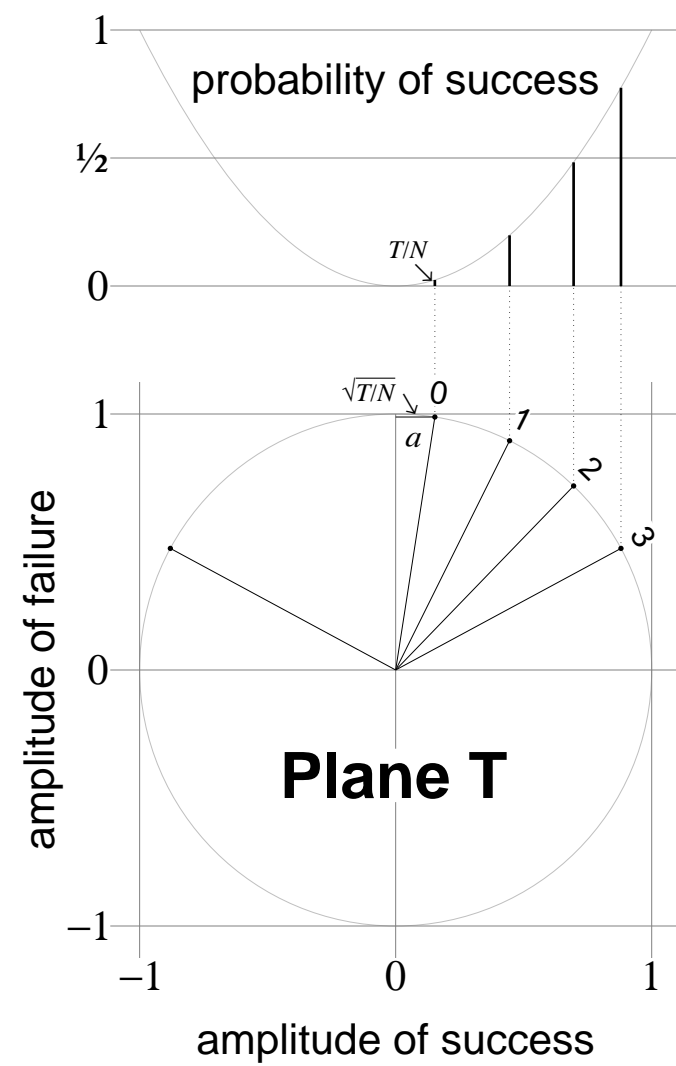
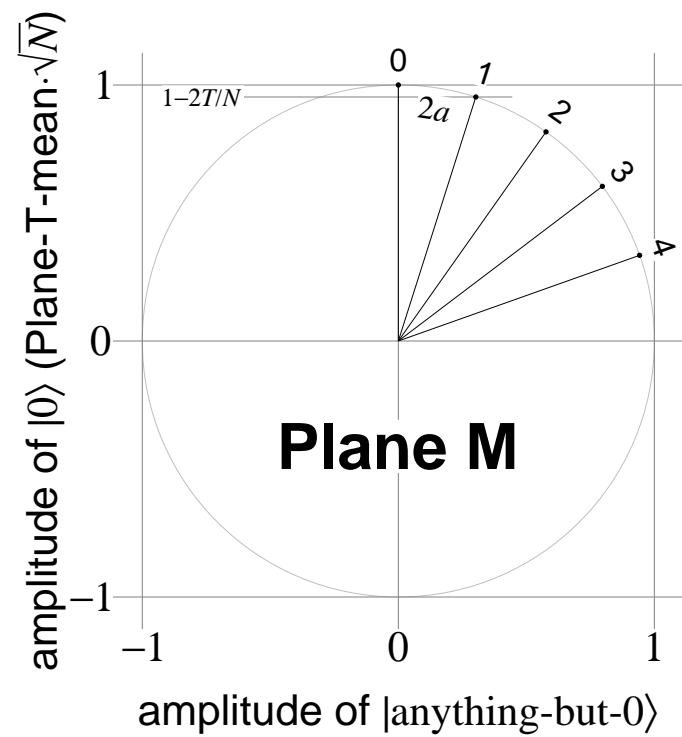


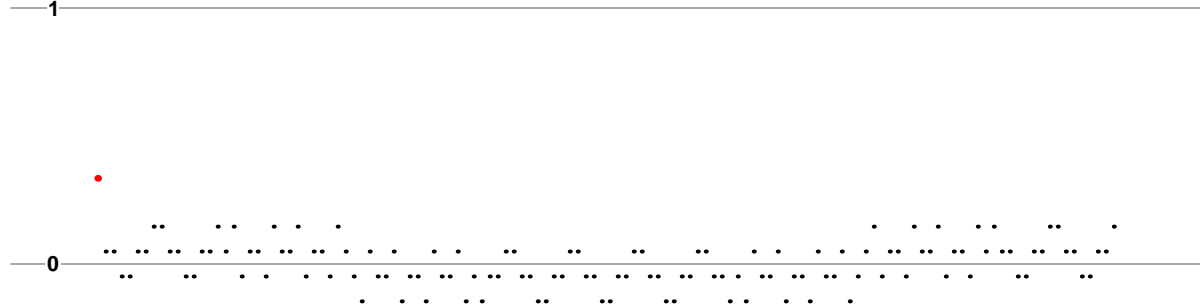
$$N = 128, T = 3$$



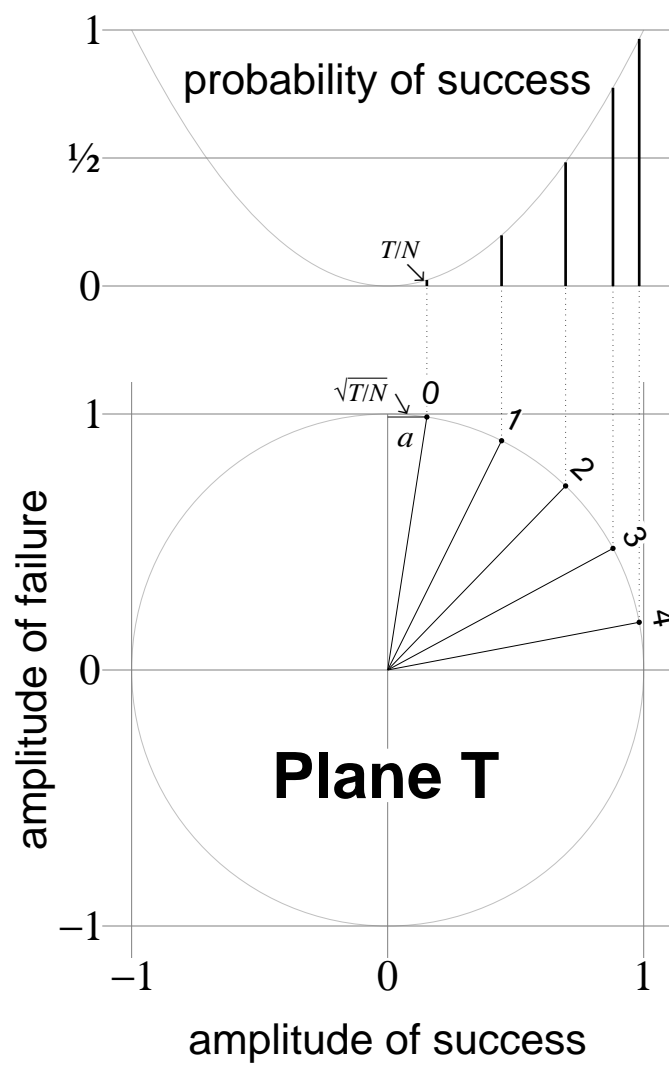
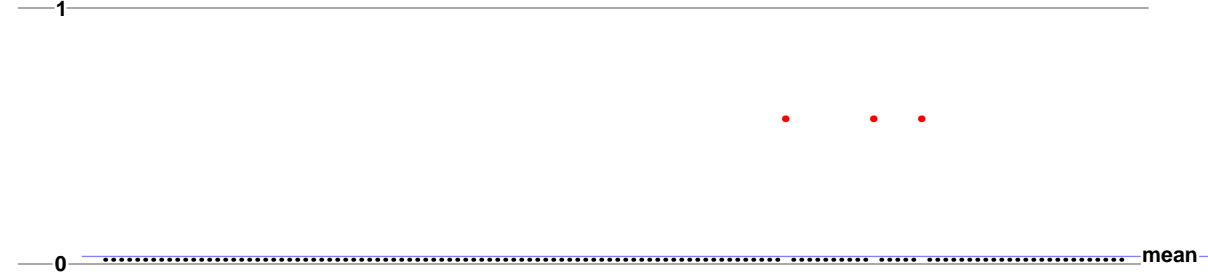
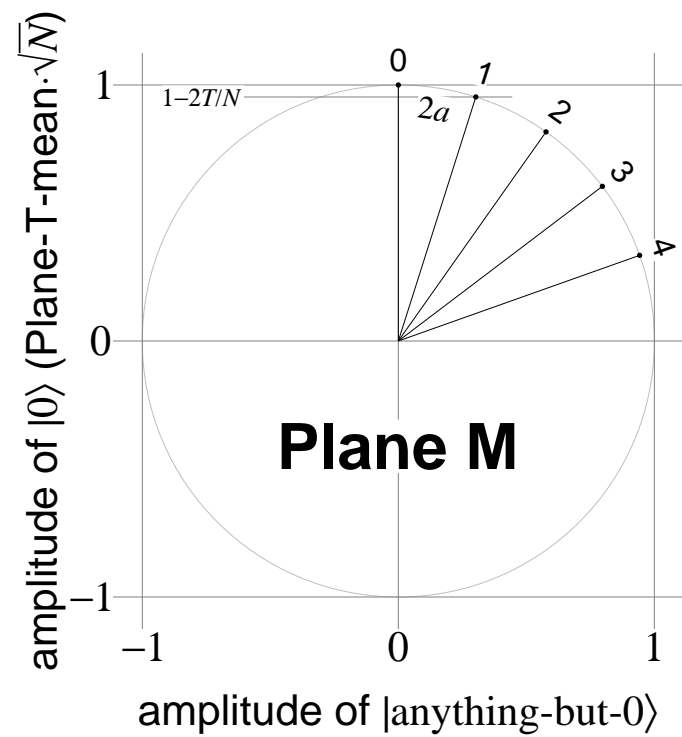


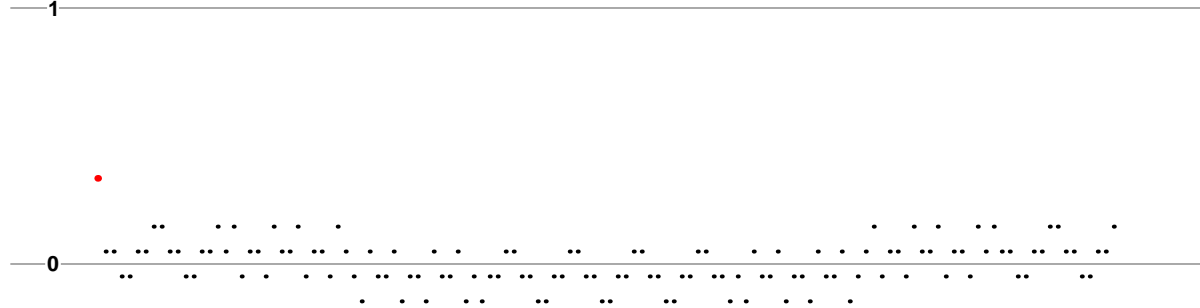
$$N = 128, T = 3$$



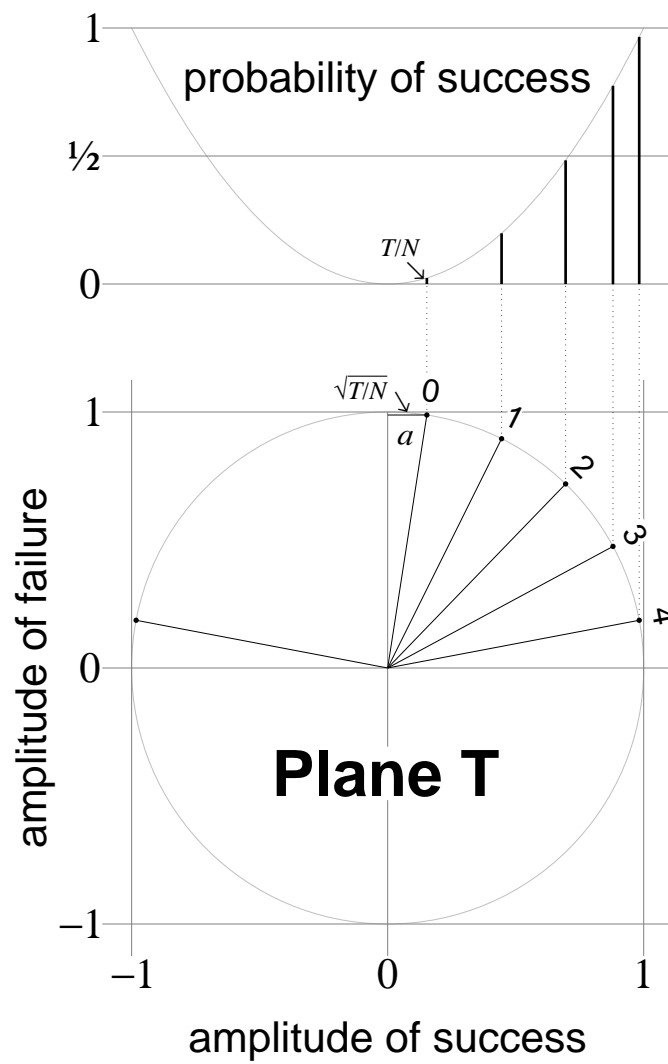
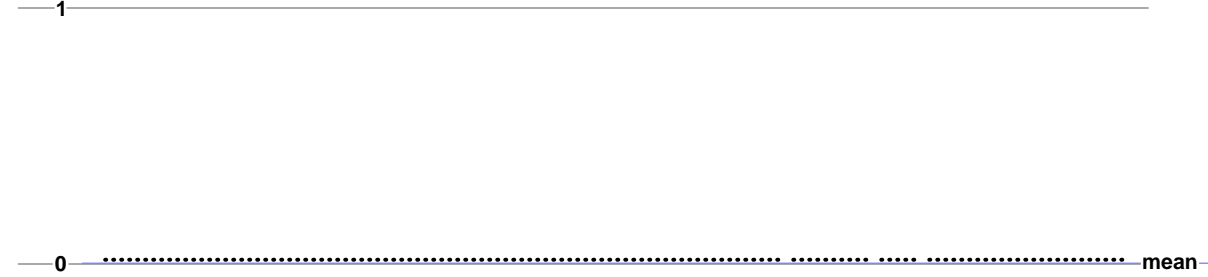
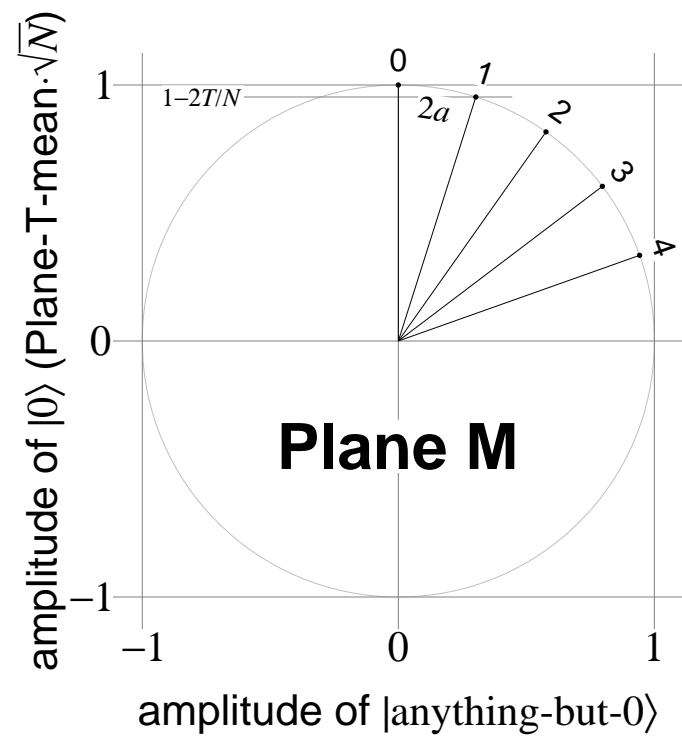


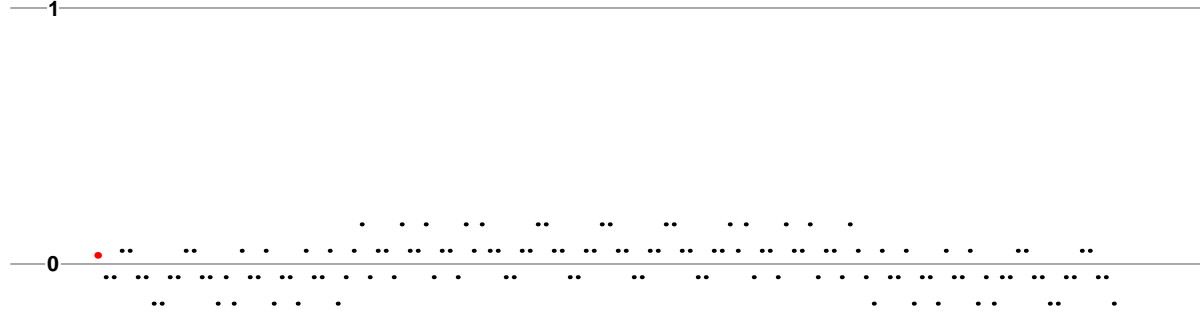
$$N = 128, T = 3$$



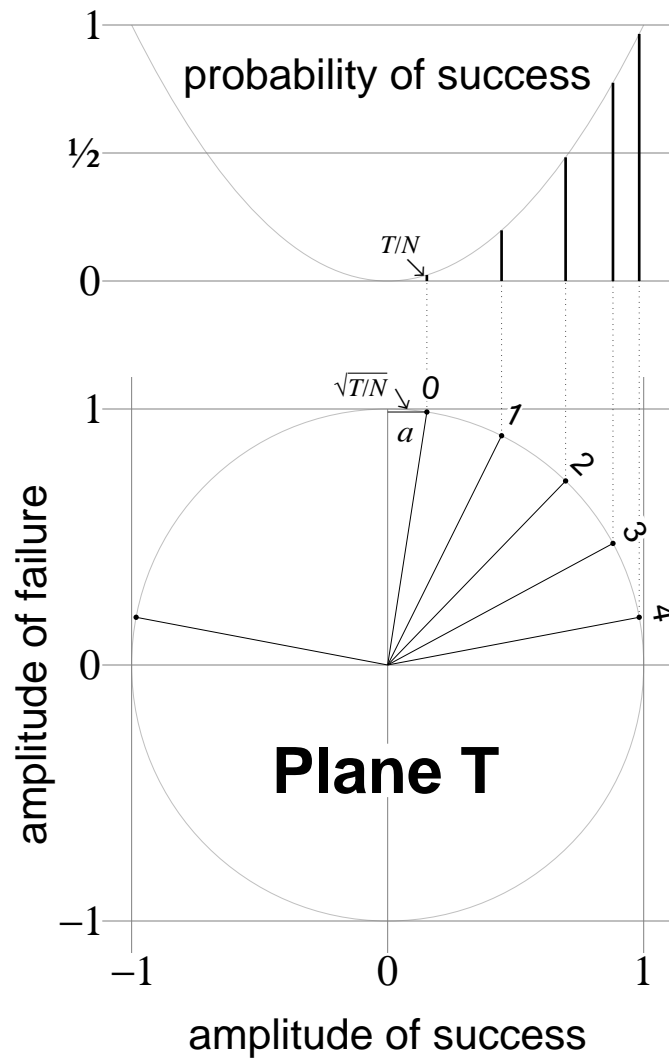
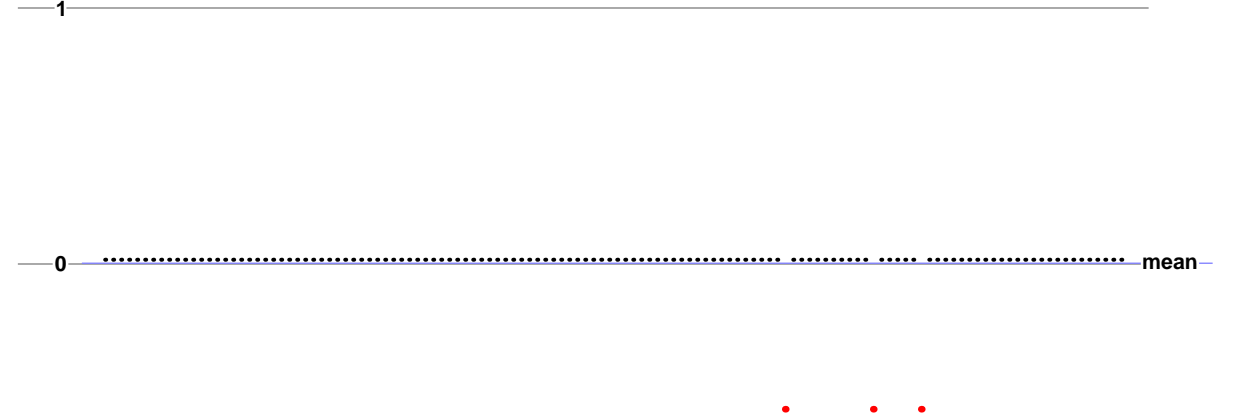
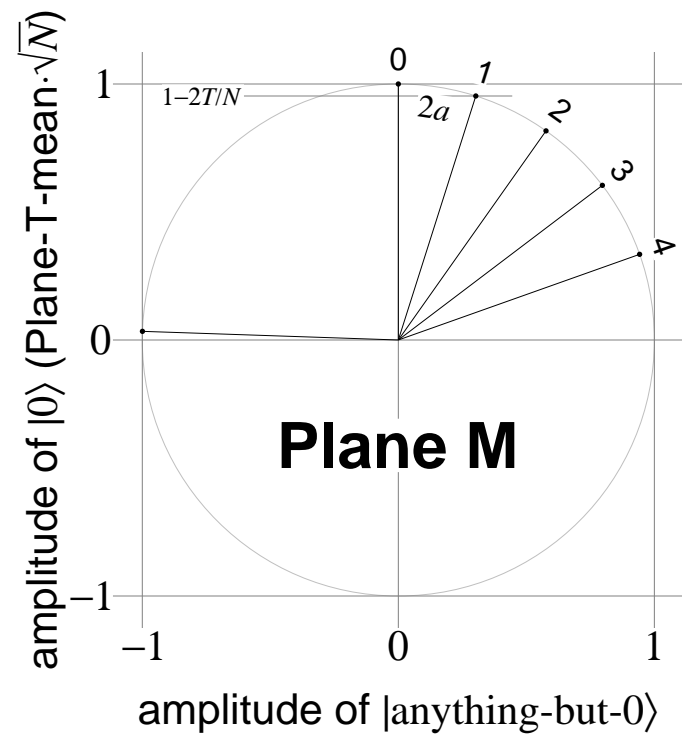


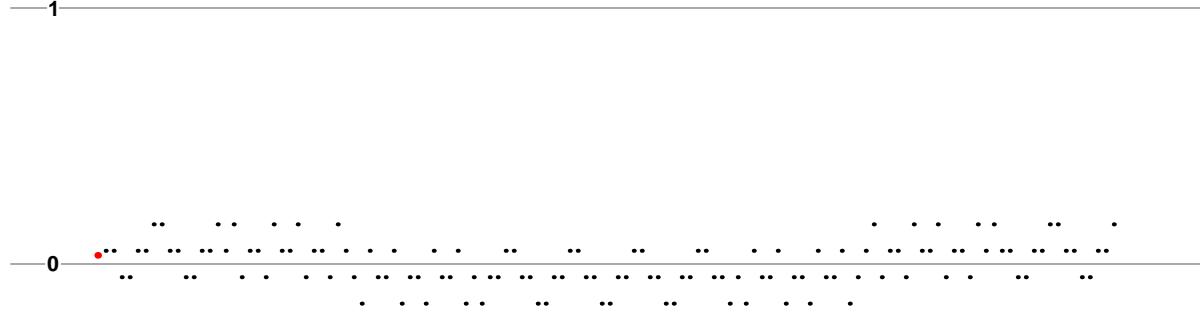
$$N = 128, T = 3$$



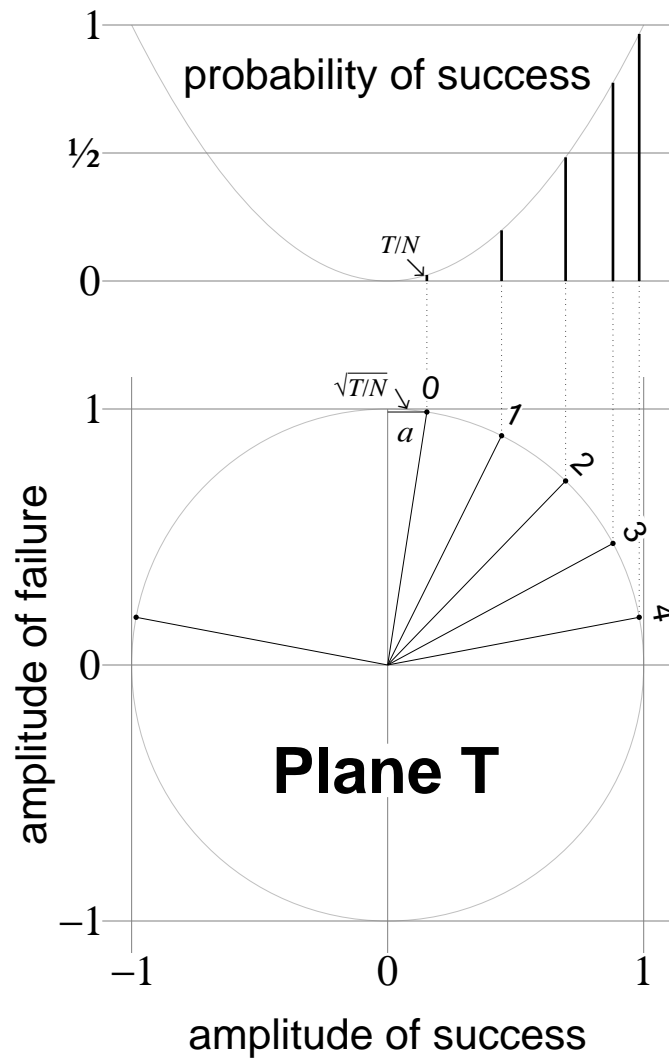
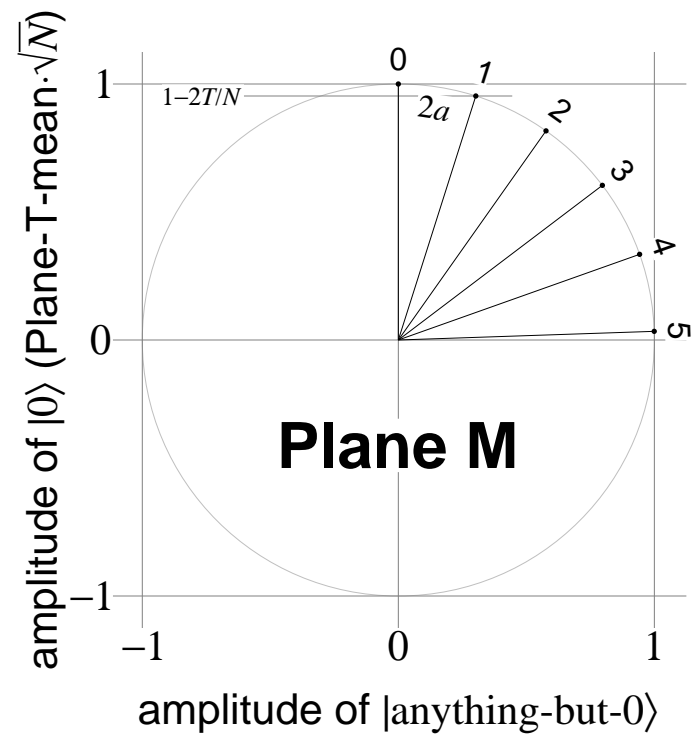


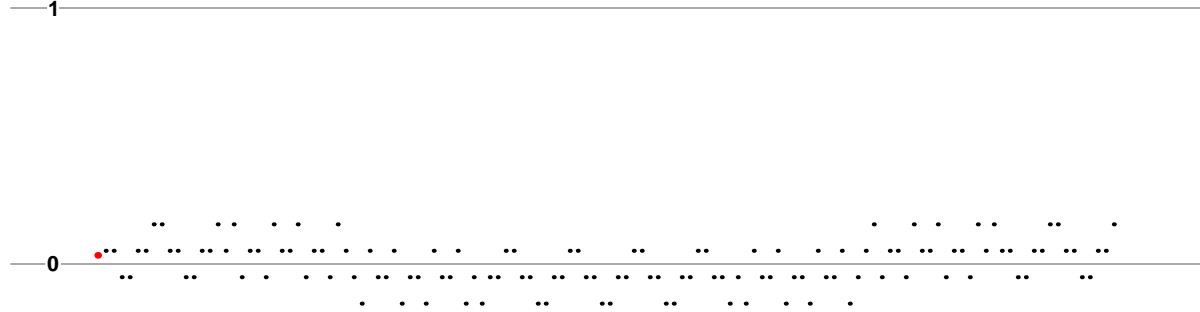
$$N = 128, T = 3$$





$$N = 128, T = 3$$





$$N = 128, T = 3$$

