The Shared Randomness Cost of Optimal One Use Loop Communication

Daniel A. Pyle
Independent Researcher
ORCID 0009-0005-6456-1370

Preprint
31 October 2026

hexagon:2610.00701v1

Abstract

We determine the minimum support and Shannon entropy of a shared classical seed needed to attain optimal worst-message success in a specified one-use normalized-loop model. The loop contains a backward binary symmetric channel with crossover $0 < p < 1/2$ and a fixed finite-dimensional forward quantum channel. Seed branches are mixed as unnormalized weights before one normalization for each message. For qubit output and interior forward trace-distance diameter, equality at the known unrestricted optimum forces every supported seed to activate exactly two message labels. The seed-cost problem becomes a fractional perfect matching problem: even message counts are optimally covered by disjoint pairs, while odd counts require a triangle and disjoint pairs. We give separate exact formulas at zero and unit diameter, prove a sufficient higher-dimensional extension of the interior result, and exhibit an erasure-channel counterexample to diameter-only seed costs in general dimension. Explicit near-optimal constructions show how the exact-attainment cost discontinuities can be avoided at finite tolerance. Compactness also gives a strict performance gap below the minimum seed support. A complete exact-certificate calculation determines the two-seed classical optimum for three messages at backward and forward crossover 1/10. These are resource-specific mathematical results, not a physical backward-communication protocol or an asymptotic capacity theorem.

1 Introduction

A communication protocol that normalizes its outcome weights can use common randomness differently from an ordinary stochastic protocol. When seed branches are combined before normalization, their posterior weights can depend on the transmitted message. It is therefore important to specify both the stage at which a seed is independent and the resource charged for that seed.

The backward channel is assumed throughout; no mechanism for producing one is proposed. An earlier draft derives an exact worst-message success formula for a single backward binary symmetric channel, a fixed noisy forward carrier, and an unrestricted finite shared seed [1]. Its cyclic attaining construction uses as many seed values as messages, but does not establish that this many are necessary. This paper answers the exact-attainment resource question for qubit-output forward channels. The minimum seed support and entropy depend on the parity of the message count and change at zero and unit forward diameter. The principal step is an equality analysis that applies to arbitrary mixed decoder instruments; an extreme-decoder upper bound alone would not justify a seed-cost lower bound.

For an interior diameter, each seed must select one ordered pair of active labels. Balancing worst-message success then imposes equal weighted graph degrees. This reduces the resource

optimization to a standard fractional perfect matching polytope. Its odd-cycle structure gives the parity effect. At unit diameter a seed may instead select a singleton, and at zero diameter each decoder row may distribute its output among several labels. We analyze both degeneracies directly. We also show why the qubit hypothesis matters: a larger forward carrier can transmit a decoder-generated flag, reducing the common seed cost while keeping the same channel diameter and unrestricted success.

The normalized decoder–memory–encoder architecture and conditional error criteria belong to an established literature [3, 4]. Trace-distance contraction coefficients and the graph-polytope facts used here are also established [5, 6, 7]. The contribution proposed here is their connection through equality in this particular resource-restricted optimization, together with exact endpoint and dimension analyses. A bounded literature screen is not an originality guarantee. The earlier raw-seed and seedless manuscripts are unpublished research manuscripts [1, 2]; their submission to Hexagon is author-reported.

2 Model and the unrestricted optimum

Let $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a completely positive trace-preserving map between finite-dimensional operator spaces. There are $M \geq 2$ classical messages, labeled by $\mathbb{Z}_M$. The backward binary channel is stipulated to be

$$N_p(b \mid a) = \begin{cases} 1-p, & b = a, \\ p, & b \neq a, \end{cases} \qquad 0 < p < \tfrac{1}{2}, \qquad A = 1-p, \quad k = 1-2p. \tag{1}$$

This assumption does not establish the physical availability of a backward channel.

A finite seed has raw probabilities $\pi_s \geq 0$, $\sum_s \pi_s = 1$, independent of the selected message and of b. Both devices know its value. For each s, b, the decoder outputs y and prepares a subnormalized forward state

$$\tau^s_{yb} \succeq 0, \qquad \sum_y \operatorname{Tr} \tau^s_{yb} = 1. \tag{2}$$

The forward carrier undergoes Φ. Knowing m, s, the encoder uses $0 \preceq E^s_m \preceq I$, with $E^s_{0|m} = E^s_m$ and $E^s_{1|m} = I - E^s_m$. The weights and normalizers are

$$w^s_m(y) = \sum_{a,b=0}^{1} N_p(b \mid a) \operatorname{Tr}\left[E^s_{a|m} \Phi(\tau^s_{yb})\right], \tag{3}$$

$$Z^s_m = \sum_y w^s_m(y). \tag{4}$$

No output label or retained side register is forwarded to the encoder. There is no shared entanglement or additional channel use. Local private randomness and a fixed public codebook are allowed. The seed is an additional resource, not part of the forward carrier dimension.

The defining convention is raw mixing followed by a single per-message normalization:

$$P(m \mid m) = \frac{\overline{w}_m(m)}{\overline{Z}_m}, \qquad \overline{w}_m(y) = \sum_s \pi_s w^s_m(y), \quad \overline{Z}_m = \sum_s \pi_s Z^s_m. \tag{5}$$

We maximize $\min_m P(m \mid m)$ after marginalizing the seed. This differs from externally mixing individually normalized branches, $\sum_s \pi_s w^s_m(y)/Z^s_m$, and from demanding a success guarantee for every seed. In (5), the posterior seed probabilities are

$$\Pr_{\text{norm}}(s \mid m) = \frac{\pi_s Z^s_m}{\overline{Z}_m}, \tag{6}$$

which may depend on m. Entropy in this paper always concerns the raw law π, not (6).

Define the forward output trace-distance diameter

$$\delta = \max_{\rho_0,\rho_1\in\mathcal{D}(\mathcal{H}_A)} \tfrac{1}{2}\|\Phi(\rho_0) - \Phi(\rho_1)\|_1 \in [0,1]. \tag{7}$$

Here $\mathcal{D}(\mathcal{H})$ denotes the density operators and $\mathrm{TD}(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_1$. The quantity δ is the established trace-distance contraction coefficient [5, 6]. Indeed, the Jordan decomposition of $\rho-\sigma$ writes it as $r(\omega_+ - \omega_-)$ with orthogonal-support states and $r = \mathrm{TD}(\rho,\sigma)$. The contraction ratio is at most (7); conversely $r \le 1$ bounds every unscaled output distance by its ratio. Compactness gives a diameter-attaining pair. Convexity of trace norm permits pure inputs, orthogonal when the input dimension is at least two. In dimension one, the unique state may be used twice. For a qubit affine Bloch map $\boldsymbol{x} \mapsto T\boldsymbol{x} + \boldsymbol{t}$, δ is the largest singular value of T; the translation cancels.

Set $\rho_b^s = \sum_y \tau_{yb}^s$ and $\Delta^s = \Phi(\rho_0^s) - \Phi(\rho_1^s)$. Direct expansion gives

$$Z_m^s = 1 + k\,\mathrm{Tr}(E_m^s \Delta^s), \qquad 1 - k\delta \le Z_m^s \le 1 + k\delta. \tag{8}$$

In particular $2p \le Z_m^s \le 2A$, so all denominators are positive. The noiseless backward endpoint $p = 0$, which needs additional admissibility rules, is not covered by this paper.

2.1 A self contained proof of the success bound

We restate and prove the needed result from [1]; its equality conditions will be essential.

Theorem 2.1 (Unrestricted raw-seed success)**.** *For every finite-dimensional Φ, $M \ge 2$, and $0 < p < 1/2$,*

$$S_{\mathrm{raw}}(\Phi, p, M) = t_* := \frac{2A}{M - (M-2)k\delta}. \tag{9}$$

The maximum is attained with a uniform M-valued seed. For $M = 2$, no seed is needed.

Proof. Put $D_s = \sum_m w_m^s(m)$, $Q_s = \sum_m Z_m^s$, $D = \sum_s \pi_s D_s$, and $Q = \sum_s \pi_s Q_s$. Two positive weighted-average identities give

$$\min_m P(m \mid m) \le \frac{D}{Q} = \sum_s \frac{\pi_s Q_s}{Q}\frac{D_s}{Q_s} \le \sup_{\tau,E} \frac{\sum_m w_m(m)}{\sum_m Z_m}. \tag{10}$$

For fixed encoder effects, each decoder factor in (2) is a compact convex set of block-positive unit-trace operators. Its extreme points have one nonzero label block, equal to a pure state. A product extreme decoder therefore chooses a deterministic label y_b and pure preparation ρ_b for each b. Decomposing a decoder into such product extremes makes its aggregate ratio a positive-denominator weighted average. It is enough to bound the extreme ratios.

Write $\sigma_b = \Phi(\rho_b)$, $\Delta = \sigma_0 - \sigma_1$, and $d = \frac{1}{2}\|\Delta\|_1 \le \delta$. Then $1 - kd \le Z_m \le 1 + kd$. If the two labels are distinct, relabel them u, v. For $t \in [0,1]$,

$$w_u(u) - tZ_u = p - t + k\,\mathrm{Tr}\,E_u[(1-t)\sigma_0 + t\sigma_1] \le A - t, \tag{11}$$

$$w_v(v) - tZ_v = A - t - k\,\mathrm{Tr}\,E_v[t\sigma_0 + (1-t)\sigma_1] \le A - t. \tag{12}$$

The bracketed matrices are positive and have trace one. Every inactive message contributes at most $-t(1-kd)$. Substituting

$$R_2(d) = \frac{2A}{2 + (M-2)(1-kd)} \tag{13}$$

for t makes the sum of these upper bounds zero, proving that the aggregate ratio is at most $R_2(d) \le R_2(\delta)$. Equality is attained by $E_u = I$, $E_v = 0$, and a negative spectral projector of Δ at every inactive message.

If the decoder labels coincide at u, only that message can succeed and its correct weight is its whole normalizer. The ratio is at most

$$R_1(d) = \frac{1+kd}{(1+kd)+(M-1)(1-kd)} = \frac{1+kd}{M-(M-2)kd} \le R_2(d). \tag{14}$$

This proves the upper bound.

For attainment choose a diameter-attaining pair and an effect H_- with $\mathrm{Tr}[H_-(\sigma_0-\sigma_1)] = -\delta$. Let s be uniform modulo M. At $b=0$ output s and prepare ρ_0; at $b=1$ output $s+1$ and prepare ρ_1. Set $E^s_m = I$ for $m=s$, $E^s_m = 0$ for $m=s+1$, and $E^s_m = H_-$ otherwise. Each message has two active branches, each with correct weight A and normalizer one; its $M-2$ other branches have correct weight zero and normalizer $1-k\delta$. Their averaged ratio is (9). For $M=2$ the same two active labels and constant encoders work in a single seed. □

3 Exact seed resources

Definition 3.1. The support of the raw seed is $K(\pi) = |\{s : \pi_s > 0\}|$, and its Shannon entropy in bits is $H(\pi) = -\sum_{s:\pi_s>0} \pi_s \log_2 \pi_s$. Let K_* and H_* be their respective minima among protocols attaining t_* in (9).

Seed support counts positive seed probabilities, not decoder outcomes or local random choices. A seed with support K can be stored using $\lceil \log_2 K \rceil$ binary memory cells. Its entropy is not an exact single-trial fair-bit sampling cost; exact sampling may require a variable number of fair bits. No claim equating these different resources is made.

Theorem 3.2 (Minimum support and entropy)**.** *Let $M \ge 3$, $0 < p < 1/2$, and $\dim \mathcal{H}_B = 2$. The exact minimum raw seed support and entropy at the unrestricted optimum are*

Forward diameter	*Message count*	K_*	H_* *in bits*
$0 < \delta < 1$	*even*	$M/2$	$\log_2 M - 1$
$0 < \delta < 1$	*odd*	$(M+3)/2$	$\log_2 M - 1 + 3/M$
$\delta = 1$	*even*	$M/2$	$\log_2 M - 1$
$\delta = 1$	*odd*	$(M+1)/2$	$\log_2 M - 1 + 1/M$
$\delta = 0$	*even*	1	0
$\delta = 0$	*odd*	2	$h_2(1/M)$

Here $h_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$. The support and entropy minima can be attained simultaneously. For $M=2$, $K_*=1$ and $H_*=0$ for every δ.

The $\delta = 0$ statement holds in every finite dimension. For $0 < \delta < 1$, the same formulas hold in arbitrary finite output dimension under the sufficient condition that every diameter-attaining output pair has joint support equal to $\mathcal{H}_B$. In particular, it is sufficient that every channel output is positive definite. No general higher-dimensional lower bound is asserted at $\delta = 1$.

3.1 Why arbitrary decoder mixing cannot hide the seed cost

The next lemma closes the gap between an extreme-point bound on aggregate performance and a resource bound on an arbitrary optimal minimax strategy.

Lemma 3.3 (Equality forces one label pair per seed)**.** *Under the interior hypotheses of Theorem 3.2, every supported seed of an optimal strategy has one deterministic ordered output-label pair (u, v), with $u \neq v$. Its correct weights and normalizers necessarily have the pattern*

$$(w_m(m), Z_m) = \begin{cases} (A, 1), & m \in \{u, v\}, \\ (0, 1 - k\delta), & m \notin \{u, v\}. \end{cases} \tag{15}$$

The forward preparations themselves need not be pure.

Proof. An optimal strategy makes both inequalities in (10) equalities. Thus every message succeeds with probability t_* and every supported seed satisfies $D_s = t_* Q_s$. Fix one seed and its encoder effects. Decompose its decoder into a finite convex combination of product extreme points, as in Theorem 2.1. All extreme ratios are at most t_*, and all aggregate denominators are positive. Every positive component must therefore attain t_* as well.

When $0 < \delta < 1$, (14) is strictly smaller than t_*, so each component has two distinct labels. Since $M > 2$ and $k > 0$, (13) is strictly increasing in d, forcing $d = \delta$. Also $0 < t_* < 1$. Equality in (11)–(12) requires

$$\mathrm{Tr}[(I - E_u)((1 - t_*)\sigma_0 + t_*\sigma_1)] = 0, \tag{16}$$

$$\mathrm{Tr}[E_v(t_*\sigma_0 + (1 - t_*)\sigma_1)] = 0. \tag{17}$$

Two distinct qubit density operators have full joint support: otherwise both would occupy the same one-dimensional subspace and coincide. Both positive convex combinations in (16)–(17) are therefore positive definite. A positive operator with zero trace against a positive definite operator must be zero. Hence $E_u = I$ and $E_v = 0$. Every inactive effect obeys $\mathrm{Tr}(E_m \Delta) = -\delta < 0$, so is neither 0 nor I.

These effects are fixed throughout the decoder decomposition for this seed. Another optimal component cannot change the first active label, the second active label, or their order: doing so would require one fixed effect to be both constant and nonconstant, or both 0 and I. Thus every component has the same ordered label pair. Each has exactly the pattern (15), which is preserved by averaging. The same proof applies in higher dimension under the stated full-joint-support hypothesis. □

3.2 The fractional matching reduction

Let $\ell = 1 - k\delta > 0$. Associate each seed with an edge between its two active labels and give it weight π_s. Parallel edges can be merged: a standard diameter-pair construction with their summed probability has the same pattern (15). Merging cannot increase support or entropy. If a_m is the total probability of edges incident with message m, then

$$P(m \mid m) = \frac{A a_m}{\ell + (1 - \ell) a_m}. \tag{18}$$

This is strictly increasing in a_m, and $\sum_m a_m = 2$. Equality with t_* for every message is equivalent to

$$a_m = \frac{2}{M} \quad \text{for every } m. \tag{19}$$

Conversely, any weighted graph obeying (19) gives an optimum by using the same diameter-attaining pair on each edge. Rescale $x_e = M\pi_e/2$. The entire seed-resource problem is now

$$x_e \geq 0, \qquad \sum_{e \ni m} x_e = 1 \quad (m \in \mathbb{Z}_M), \tag{20}$$

the loopless fractional perfect matching polytope. Its graph-theoretic structure is standard [7]; we include the needed special-case proof.

3.3 Minimum support in the interior

Every message must lie on an edge, so at least $M/2$ edges are required. For even M, disjoint pairs of weight $2/M$ attain that bound. For odd M, a degree-one vertex forces its unique edge to have probability $2/M$, which saturates its neighbor's degree too. Such vertices therefore form isolated pairs. Remove all such pairs. The remaining graph has minimum degree at least two and, because the original number of vertices was odd, contains at least three vertices. If it has L vertices, it has at least L edges, while the removed pairs contribute $(M - L)/2$. Thus

$$K \geq \frac{M + L}{2} \geq \frac{M + 3}{2}. \tag{21}$$

A triangle whose three edges each have probability $1/M$, together with $(M - 3)/2$ disjoint edges of probability $2/M$, attains this lower bound.

3.4 Minimum entropy in the interior

Entropy is continuous and concave on the compact polytope (20), so a minimum is attained at an extreme point. Its support components are isolated edges with $x_e = 1$ and odd cycles with $x_e = 1/2$. To verify this structure, first remove leaf components, which as above are isolated pairs. Any remaining connected component has minimum degree two. If it had more edges than vertices, its unsigned incidence columns would be linearly dependent, giving a nonzero signed perturbation that preserves the constraints and, for sufficiently small magnitude, nonnegativity. It would not be extreme. Hence it is a cycle. An even cycle admits an alternating perturbation; an odd cycle has the unique solution $x_e = 1/2$. Conversely, these isolated-edge and odd-cycle components each have a unique supported solution.

If L vertices lie on odd cycles, the seed probabilities are $(M - L)/2$ entries of $2/M$ and L entries of $1/M$. Their entropy is

$$H = \log_2 M - 1 + \frac{L}{M}. \tag{22}$$

For even M, $L = 0$ is possible and optimal. For odd M, the minimum is $L = 3$. The constructions minimizing support thus minimize entropy too. This proves the interior rows of Theorem 3.2.

4 The two diameter endpoints

The interior equality argument uses both $\delta > 0$ and $\delta < 1$. Their failures correspond to different feasible decoder structures, not failures of the success formula.

4.1 Perfect distinguishability

Suppose $\delta = 1$ and the output is a qubit. The common-label bound (14) may now attain t_*. Any attaining extreme component uses outputs at distance one, which are orthogonal pure qubit states. Let H_+, H_- be their complementary rank-one projectors, with $\mathrm{Tr}(H_\pm \Delta) = \pm 1$.

A distinct-label component still uses $I, 0$ at its two active labels and H_- elsewhere. A common-label component at u uses H_+ at u and H_- at every other message. No two different optimal label patterns can coexist in one seed's extreme decomposition. Two distinct pair patterns conflict as in Lemma 3.3. A pair and a singleton conflict because the pair has constant active effects but the singleton has only rank-one effects. Two singleton patterns at different labels also conflict: because $M \geq 3$, a third label is inactive in both and fixes their H_- to be the same; the first active label would then need to have both complementary projectors. Thus each supported seed is a single pair or a single singleton.

Represent a singleton at m by a loop and count that loop twice in its weighted degree. This loop convention is stated explicitly; it differs from the once-counted convention used in [7]. If a_m is the weighted degree, the averaged correct weight and normalizer are

$$\overline{w}_m(m) = Aa_m, \qquad \overline{Z}_m = (1-k) + ka_m. \tag{23}$$

A singleton of weight π contributes correct weight $\pi(1+k) = 2A\pi$ and increases the normalizer above its inactive value by $2k\pi$, which explains the double counting. Optimality again requires $a_m = 2/M$.

At least $\lceil M/2 \rceil$ seeds are needed to cover all messages. Disjoint pairs, with one singleton when M is odd, attain this count. Every pair probability is at most $2/M$ and every singleton probability at most $1/M$. Among all probability vectors with atom cap $2/M$, entropy is minimized by filling as many atoms to that cap as possible and placing any residual in one atom. This follows, for example, by transferring mass from a smaller nonzero atom to a larger unsaturated atom: concavity of $-x \log_2 x$ makes entropy nonincreasing. The resulting vector is $M/2$ entries of $2/M$ for even M, or $(M-1)/2$ entries of $2/M$ and one of $1/M$ for odd M. The matching-plus-singleton construction realizes it, proving the unit-diameter rows of Theorem 3.2.

4.2 Complete erasure of distinguishability

If $\delta = 0$, the channel is a replacer: for a fixed state σ, $\Phi(\tau) = \mathrm{Tr}(\tau)\sigma$. Put $q_{yb} = \mathrm{Tr}\,\tau_{yb}$ and $e_m = \mathrm{Tr}(E_m\sigma)$. Every normalizer is one, and

$$w_m(m) = (p + ke_m)q_{m0} + (A - ke_m)q_{m1}. \tag{24}$$

The sum of correct weights is at most $2A$. Equality forces $e_m = 1$ whenever $q_{m0} > 0$ and $e_m = 0$ whenever $q_{m1} > 0$. Thus the two row label distributions have nonempty disjoint supports. Conversely, any two such distributions with these constant effects attain aggregate correct weight $2A$.

At the unrestricted optimum $2A/M$, every supported seed must attain that aggregate bound. Consider a seed of probability π. Its row supports have sizes r_0, r_1 with $r_0 + r_1 \le M$. One support has at most $\lfloor M/2 \rfloor$ labels and receives total correct weight πA from this seed. Its total correct weight from all seeds is $2A$ times its size divided by M. Hence

$$\pi \le \frac{2\lfloor M/2 \rfloor}{M}. \tag{25}$$

For even M, one seed suffices: split the messages into equal groups and make each row uniform on its group. For odd M, (25) gives the cap $(M-1)/M < 1$, so at least two seeds are required and entropy is at least $h_2(1/M)$ by the same mass-transfer argument.

For an explicit attaining odd construction, write $M = 2r + 1$. Partition the labels into U of size r and V of size $r+1$, and choose distinct $v_1, v_2 \in V$. In a dominant seed of probability $2r/M$, let $q_{\cdot 0}$ be uniform on U. Let $q_{\cdot 1}$ assign probability $1/(2r)$ to each of v_1, v_2 and $1/r$ to each other member of V. In a second seed of probability $1/M$, concentrate row zero at v_1 and row one at v_2. Each seed has disjoint row supports. Each message's averaged $q_{m0} + q_{m1}$ equals $2/M$, and its success is $2A/M$. This attains both lower bounds. No dimensional assumption was used, completing Theorem 3.2.

5 Why output dimension matters

The full-joint-support extension in Theorem 3.2 is sufficient, not asserted necessary. Without an appropriate support condition, the forward output can retain information about the decoder's

private random choice. Then several extreme label patterns may coexist within one seed without forcing contradictory encoder effects.

Proposition 5.1 (Same diameter and different seed cost)**.** *For every $0 < d < 1$, there is a finite-dimensional forward channel of diameter d for which four messages attain the unrestricted raw optimum without a seed. A qubit-output channel of the same diameter requires two seed values and one bit of raw seed entropy.*

Proof. Use four orthogonal inputs $|x_1\rangle, \dots, |x_4\rangle$ and an erasure channel

$$\Phi_d(\rho) = d\rho \oplus (1-d)\,\mathrm{Tr}(\rho)|e\rangle\langle e|, \tag{26}$$

with a fifth orthogonal erasure flag. Its output trace distance is d times the input trace distance, so its diameter is d.

Use one seed. At $b = 0$, output and prepare labels $1, 2$ with probability $1/2$ each; at $b = 1$, use labels $3, 4$ similarly. In coordinates (e, x_1, x_2, x_3, x_4) choose the diagonal effects

$$\begin{aligned} E_1 &= \mathrm{diag}(1,1,0,1,1), \quad E_2 = \mathrm{diag}(1,0,1,1,1), \\ E_3 &= \mathrm{diag}(0,0,0,0,1), \quad E_4 = \mathrm{diag}(0,0,0,1,0). \end{aligned} \tag{27}$$

Direct contraction in (3) gives every message correct weight $A/2$ and normalizer $1 - kd/2$. Its success is

$$\frac{A}{2-kd} = \frac{2A}{4-2kd}, \tag{28}$$

the unrestricted four-message optimum. The qubit comparison follows from the interior even row of Theorem 3.2. □

Thus the diameter determines unrestricted success but not common seed cost in general dimension. The extra carrier dimension in this counterexample is not free shared randomness. It is a distinct communication resource excluded from the qubit comparison.

6 Approximate optimality and restricted seeds

Assume $M \geq 3$ throughout this section; the $M = 2$ optimum already needs no seed. The exact-attainment costs have discontinuities at the diameter endpoints, while the success value (9) is continuous. The following constructions quantify how small performance losses can avoid those cost jumps. Write

$$D = M - (M-2)k\delta, \qquad t_* = 2A/D. \tag{29}$$

A protocol is ε-relative-optimal when its worst-message success is at least $(1-\varepsilon)t_*$.

6.1 Ignoring weak forward distinguishability

Choose the same forward input for every decoder branch and implement the zero-diameter construction from Section 4.2. This works for every actual forward channel and achieves

$$S_{\text{ignore}} = \frac{2A}{M} \tag{30}$$

with support one for even M, and support two and entropy $h_2(1/M)$ for odd M. Its absolute and relative losses are exactly

$$t_* - S_{\text{ignore}} = \frac{2A(M-2)k\delta}{MD}, \qquad 1 - \frac{S_{\text{ignore}}}{t_*} = \frac{(M-2)k\delta}{M}. \tag{31}$$

Hence it is ε-relative-optimal whenever $\delta \leq \varepsilon M/[(M-2)k]$. If the right side is at least one, the condition holds for every diameter. This is an achievable resource saving, not an optimal approximate-entropy formula.

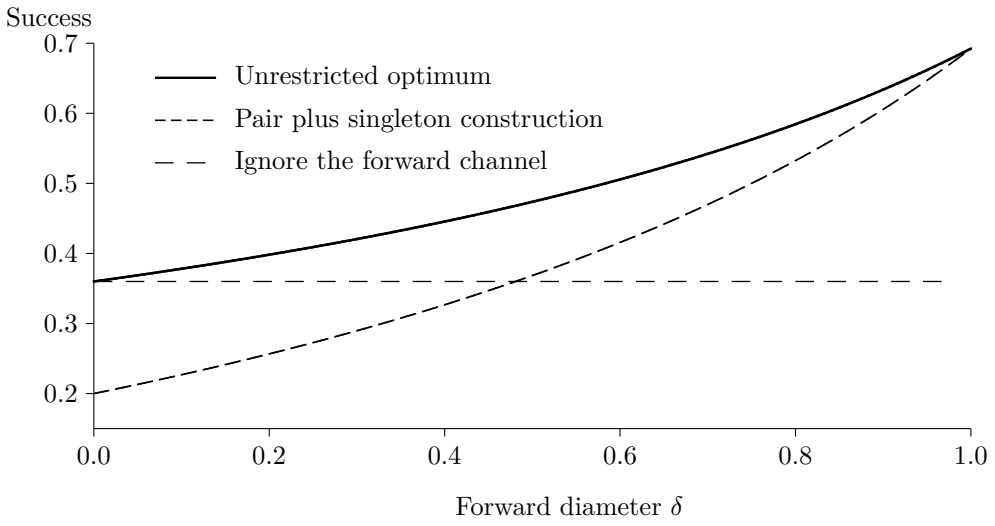


Figure 1: Analytically evaluated success for $M = 5$ and $p = 1/10$. The unrestricted optimum needs four seed values at every interior diameter for qubit output. Ignoring the forward channel uses two seed values; the fixed-weight pair-plus-singleton construction uses three. They approach the optimum at opposite endpoints. The curves are attaining constructions, not upper bounds for the full two- or three-seed optimization.

6.2 Replacing a triangle by a singleton near unit diameter

Let $M = 2r + 1$ be odd. Use r disjoint pair seeds, each of probability $2/M$, and one singleton seed of probability $1/M$. All preparations use a diameter-attaining pair. Pair seeds use the constant active effects and H_- elsewhere. In the singleton seed use an effect H_+ attaining $\mathrm{Tr}(H_+\Delta) = \delta$ at its one active label and H_- at all others.

Every message has averaged normalizer D/M. Pair-covered messages have correct weight $2A/M$, while the singleton message has $(1 + k\delta)/M$. The worst-message success is therefore

$$S_{\mathrm{single}} = \frac{1 + k\delta}{D}, \qquad t_* - S_{\mathrm{single}} = \frac{k(1-\delta)}{D}, \qquad 1 - \frac{S_{\mathrm{single}}}{t_*} = \frac{k(1-\delta)}{1+k}. \tag{32}$$

This code has support $(M + 1)/2$ and entropy $\log_2 M - 1 + 1/M$, saving one seed value and $2/M$ entropy bits relative to exact interior attainment. It is ε-relative-optimal whenever $k(1 - \delta)/(1 + k) \le \varepsilon$. Reweighting its seeds can improve performance; (32) is the value of the stated construction, not the general fixed-support optimum.

6.3 A strict gap below the exact support threshold

Proposition 6.1. *Fix finite input and output dimensions, $0 < p < 1/2$, a forward channel, and an integer K. The maximum raw success over protocols with at most K seed values is attained. Consequently, whenever Theorem 3.2 gives $K < K_*$, that maximum is strictly below t_*.*

Proof. Allow exactly K indexed seed slots, including zero-probability slots. The seed simplex, decoder block sets, and effect intervals are compact in finite-dimensional spaces. Their product is compact. Equation (8) bounds every averaged denominator below by $2p$, so the worst-message success is continuous. Its maximum is attained. If that maximum equaled t_* with $K < K_*$, it would contradict the definition and value of K_*. □

This argument gives a strictly positive gap for each fixed channel and insufficient K, but

neither its magnitude nor a uniform lower bound as the channel approaches an endpoint. Figure 1 explains why such endpoint limits need care.

7 An exact two seed classical benchmark

The complete fixed-seed performance frontier is not determined by Theorem 3.2. A finite certificate calculation gives one nontrivial subthreshold value. This section concerns a *classical* forward binary symmetric channel only; it does not assert equality with a two-seed qubit protocol.

Theorem 7.1 (Computer-assisted classical benchmark)**.** *For three messages, backward and forward crossover probabilities $p = q = 1/10$, and at most two raw seed values, the exact classical optimum is*

$$T_2 = \frac{3895 - \sqrt{1237585}}{3776} = 0.7368993704800834\ldots. \tag{33}$$

Here $\delta = 1 - 2q = 4/5$. The unrestricted value is $45/59$, approximately 0.7627118644, and requires three seed values. The absolute loss is approximately 0.02581249393.

Proof and exact certificate specification. For a fixed decoder, raw seed law, and target t, each inequality $\overline{w}_m(m) - t\overline{Z}_m \geq 0$ is linear in each encoder response coordinate. A response for one message appears in no other message's inequality. Maximizing each coordinate's contribution independently therefore yields deterministic encoders without increasing the seed support. There are four deterministic functions $a(c)$ of the received forward bit c. Encode a function by $2a(0) + a(1)$, so the four types are constant zero, identity, bit flip, and constant one. A seed has $4^3 = 64$ profiles, and seed exchange leaves $64 \cdot 65/2 = 2080$ unordered profile pairs to consider, including identical profiles and zero-probability seeds.

For a profile pair P_s, set

$$x_{sbyd} = \pi_s D_s(y, d \mid b) \geq 0, \qquad W_{smbd} = \sum_c N_q(c \mid d) N_p(b \mid a_{sm}(c)).$$

The decoder constraints are $\sum_{y,d} x_{s0yd} = \sum_{y,d} x_{s1yd} = \pi_s$ and $\sum_s \pi_s = 1$. Correct weights and normalizers are

$$C_m = \sum_{s,b,d} x_{sbmd} W_{smbd}, \qquad Z_m = \sum_{s,b,y,d} x_{sbyd} W_{smbd}.$$

For nonnegative multipliers μ_m summing to one, define

$$g_{sbyd} = \sum_m \mu_m (t - \mathbf{1}_{y=m}) W_{smbd}. \tag{34}$$

Every allowed decoder obeys

$$\sum_m \mu_m (t Z_m - C_m) \geq \min_s \left[\min_{y,d} g_{s0yd} + \min_{y,d} g_{s1yd} \right]. \tag{35}$$

A strictly positive right side rules out target t for those profiles. A nonnegative bound with strictly positive μ_m rules out success strictly greater than t for every message.

For achievability take

$$x = \frac{1271 - \sqrt{1237585}}{256}, \qquad y = 1 - x. \tag{36}$$

Both probabilities are positive. Seed one is a pair on messages $0, 2$, with profile $(0, 1, 3)$: it outputs message zero and forward bit one at $b = 0$, and message two and forward bit zero at $b = 1$. Seed two is a singleton on message one with profile $(1, 2, 1)$, preparing forward bit one at

$b = 0$ and bit zero at $b = 1$. Put $b_* = k\delta = 16/25$ and $\ell_* = 1 - b_* = 9/25$. The pair-message and singleton-message successes are respectively

$$\frac{Ax}{\ell_* + b_* x}, \qquad \frac{(1 + b_*)y}{\ell_* + 2b_* y}, \tag{37}$$

both equal to (33). Equivalently, T_2 is the smaller root of $1888T_2^2 - 3895T_2 + 1845 = 0$.

For the winning profile pair, choose $t = T_2$ and $\mu = (x/2, y, x/2)$. Exact arithmetic in $\mathbb{Q}(\sqrt{1237585})$ verifies $g_{sbyd} \geq 0$ for every index, giving the matching upper bound. Simultaneous forward-bit relabeling, simultaneous backward-bit relabeling, global message permutation, and seed exchange preserve the problem. Forward and backward relabelings can be chosen independently in each seed. Explicitly enumerating the winning orbit yields 24 profile pairs. For each of the other 2056 pairs, the companion certificate file gives rational μ for which (35) is strictly positive at $t_0 = 7368993/10000000 < T_2$.

The standalone verifier reconstructs all 2080 pairs, the 24-element orbit, and every coefficient in (34). It checks the exact winning construction and upper bound, positivity of the probabilities, and all 2056 rational exclusions, with no floating-point operations or optimization solver. Complete coverage therefore proves the global classical bound; numerical optimization was used only to discover certificates. □

8 Relation to previous work and remaining questions

Theorem 3.2 addresses the raw common seed required to attain a performance optimum, not exact synthesis of a prescribed joint distribution. Minimum entropy of a shared variable is already a standard resource in exact common information: Kumar, Li, and El Gamal minimize $H(W)$ subject to a fixed law and conditional independence [8]. Their setting also distinguishes entropy from expected description length. Applying such a theorem here would require a fixed-target-law and cost-preserving reduction, including the message-dependent normalization. None is assumed.

Similarly, Ji, Lloyd, and Wilde's normalized retrocausal framework includes shared randomness and forward registers beyond the fixed carrier allowed here [3]. Their general noisy-memory rate tradeoff is not solved by a one-use seed-cost theorem. Ji, Regula, and Wilde already use a worst-message ratio of correct conclusive weight to total conclusive weight in postselected communication [4]; the present contribution is not the conditional error criterion. A postselected simulation alone does not establish a resource-preserving equivalence to their entanglement- or nonsignalling-assisted optimizations.

The earlier seedless result [2] is also a different resource problem. Under matched binary symmetric and depolarizing memories, three messages have equal classical and quantum seedless optima, while a rational four-message qubit protocol can exceed a universal classical ceiling of $1/2$. Adding raw seed assistance equalizes their unrestricted optima through their matched diameter, but Theorem 7.1 does not equalize their subthreshold finite-seed curves. If success is required for every supported seed, the optimum equals the seedless minimax exactly: each branch is an admissible seedless protocol, and a one-valued seed attains that optimum. Thus no advantage follows from common randomness under a worst-seed requirement.

Several questions remain open in this work. The full function of allowed support K is unknown even for matched bit and qubit memories; the exact benchmark in Section 7 is one classical instance. The minimum entropy at a prescribed suboptimal success is also unknown. In higher dimension, a channel invariant richer than diameter may be needed to characterize exact seed resources. Asymmetric backward channels, larger backward alphabets, and multiple uses require separate equality analyses. Finally, changing the order of mixing and normalization changes the optimization and cannot be handled by silently reusing these seed-cost formulas.

The model assumes a backward channel and studies coding and resources conditional on that assumption. It supplies no mechanism for creating such a channel. In particular, correlations obtained by postselection do not, by themselves, provide an earlier readable record of a freely chosen later message. Physical implementation would require a separate model and evidence absent from this paper.

9 Computational verification and provenance

The analytic statements in Sections 2–6 are proved above. Computations supplement their proofs: the main suite checks 1434 exact-rational construction identities and 114 floating-point entropy values, and samples 1000 fractional-matching vertices using linear objectives; a separately implemented suite checks 672 rational construction cases and 16 direct erasure-channel contractions. These counts describe distinct cases within the named suites, not independent discoveries or accumulated rerun counts. The vertex sampling is a numerical consistency test, not a proof of the graph theorem.

Section 7 is explicitly computer-assisted. Its upper bound uses a complete finite set of exact certificates, not sampled protocols or an optimizer's convergence claim. The reader-facing archive includes the certificate specification, complete machine-readable certificate data, a solver-free verifier using integer and rational quadratic-field arithmetic, and optional numerical discovery scripts. A fresh verification run and its environment record accompany the archive.

Availability and version history Verification code and complete certificates are supplied in the companion archive `seed_cost_reproducibility.zip`; editable manuscript source is supplied separately. The project repository, https://github.com/dapyle11/normalized-loop-memory, hosts related earlier material, including the raw-seed reproducibility archive identified in [1]. The earlier submitted files are preserved unchanged.

AI assistance and review status Lyra, an OpenAI AI assistant, performed technical derivation, proof checking, code development and verification, bounded literature screening, and manuscript drafting in an AI-assisted workflow directed by Daniel A. Pyle. Separate AI checking passes were used; they are not independent human peer review. The assistant is disclosed as a tool, not a coauthor. Independent human review of the model, proofs, computer-assisted certificates, bibliography, and originality remains pending.

References

[1] D. A. Pyle, "Shared randomness and normalization in one-use loop communication," unpublished research manuscript, 30 October 2026. Earlier computational material: https://github.com/dapyle11/normalized-loop-memory, archive `shared_seed_loop_reproducibility (1).zip`.

[2] D. A. Pyle, "Finite alphabet communication with noisy forward memory in a normalized loop," unpublished research manuscript, 30 October 2026. Related materials: https://github.com/dapyle11/normalized-loop-memory.

[3] K. Ji, S. Lloyd, and M. M. Wilde, "Retrocausal capacity of a quantum channel: Communicating through noisy closed timelike curves," *Physical Review Letters* **136**, 230801 (2026). doi:10.1103/znyd-npk5. arXiv:2509.08965v3.

[4] K. Ji, B. Regula, and M. M. Wilde, "Postselected communication over quantum channels," *International Journal of Quantum Information* **22**(5), 2440012 (2024). doi:10.1142/S0219749924400124. arXiv:2308.02583v3.

[5] O. Fawzi, A. Müller-Hermes, and A. Shayeghi, "A lower bound on the space overhead of fault-tolerant quantum computation," in *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, LIPIcs **215**, 68:1–68:20 (2022). doi:10.4230/LIPIcs.ITCS.2022.68.

[6] F. Hiai and M. B. Ruskai, "Contraction coefficients for noisy quantum channels," *Journal of Mathematical Physics* **57**(1), 015211 (2016). doi:10.1063/1.4936215.

[7] R. E. Behrend, "Fractional perfect b-matching polytopes. I: General theory," arXiv:1301.7356 (2013), especially Section 7, Theorem 22. https://arxiv.org/abs/1301.7356.

[8] G. R. Kumar, C. T. Li, and A. El Gamal, "Exact common information," arXiv:1402.0062 (2014), especially Sections II and V. https://arxiv.org/abs/1402.0062.