

A Good Code Exists and Here Is a Good Code Are Different Sentences

— Shannon's Existence Theorem and Galois's Construction — [Paper 163]

Yuuki YAMAGISHI (山岸 勇輝)

Yamagishi Complexity Torus Lab, Japan

August 2026

— *From thinking to syncing.* —

ABSTRACT

The corpus has carried the discipline of writing down which root an equals sign has. This paper applies that discipline to the form of a theorem itself — a theorem that asserts existence and a theorem that hands over an object have different roots. **NO NEW MATHEMATICAL THEOREM IS CLAIMED.** First, Shannon says a code exists. The capacity of a binary symmetric channel is $C = 1 - H(p)$, giving **0.919207, 0.713603, 0.500084** and **0.188722** at $p = 0.01, 0.05, 0.11, 0.25$ (computed here). But the proof only averages over randomly drawn codes and names none of them (Section 2). Second, Galois hands over one. A Reed–Solomon code over a finite field was built here from scratch, together with a Berlekamp–Welch decoder (Section 3). Third, and this is the core. The boundary is sharp. Over the field of **11** elements with $n = 8$ and $k = 3$, the code recovers the message with **0, 1 and 2** errors and admits no decoding at **3** — the line falls exactly at $t = 2$ (computed here). And the decoder is an algorithm, not an assertion (Section 4). Fourth, the construction is optimal as well. Against the Singleton bound $d \leq n - k + 1 = 6$, the Reed–Solomon minimum distance is **6** (all **1331** codewords enumerated), while **40** random linear codes gave **4** or **5**, with **0** of them reaching the bound (Section 5). Fifth, the brake. The construction carries a constraint the existence theorem never had. A field of order q exists only when q is a prime power, so there is none for $q = 6, 10, 12, 14, \dots$. There is no Reed–Solomon code over a six-letter alphabet — while Shannon's capacity is defined for any alphabet size at all (Section 6).

Scope of this paper: **NO NEW MATHEMATICAL THEOREM IS CLAIMED.** Shannon's channel coding theorem, Reed–Solomon codes, Berlekamp–Welch decoding, the Singleton bound and the existence condition for finite fields are **all** standard. What is added is **building an encoder and a decoder here and showing the boundary falls exactly at t , comparing random linear codes against the bound numerically, giving the existence condition for finite fields its address as a constraint borne only by the construction, and setting existence and construction side by side in the corpus's language of distinct roots.**

1. Notation and position

Write $[n, k, d]$ for a code of length n , dimension k and minimum distance d . The number of correctable errors is $t = \lfloor (n - k)/2 \rfloor$.

Position: Paper 16 wrote that **the equals sign too has distinct roots**, six of them to be told apart. Paper 161 showed that **among five fixed-point theorems, not even the kind of thing promised is the same**. This paper extends that line: **some theorems say a thing is there and others hand it over, and the two cannot be exchanged**.

2. Shannon says a code exists

Verification 2.1: The capacity of a binary symmetric channel is $C = 1 - H(p)$.

p	C (bits per use)	code named by the proof
0.01	0.919207	none
0.05	0.713603	none
0.11	0.500084	none
0.25	0.188722	none
0.5	0.000000	—

(QED)

Observation 2.2

The spine of the proof is a bound on the error probability averaged over randomly drawn codes. Existence follows from one line: at least one must be as good as the average. No particular code appears anywhere in it.

Observation 2.3

This does not mean the proof is incomplete. As an existence theorem it is complete. What differs is what one is handed.

3. Galois hands over one

Construction 3.1: Take $P = 11$, a prime, so that $0, \dots, 10$ form a field modulo 11 . Treat a message of length $k = 3$ as the coefficients of a polynomial and evaluate it at $n = 8$ distinct points (a Reed–Solomon code).

Construction 3.2: Decoding is by Berlekamp–Welch: set up a **linear** system in the unknowns E (the error locator, degree $\leq t$, monic) and $Q = E \cdot P$ (degree $\leq t + k - 1$), then divide Q by E to recover the message.

Observation 3.3

What is handed over is not only a code. A procedure for decoding comes with it. The existence theorem has none.

4. The core: the boundary is sharp

Verification 4.1: The message $[3, 7, 2]$ encodes to $[1, 3, 9, 8, 0, 7, 7, 0]$. Introduce errors one at a time and decode.

errors	received	decoded	recovered
0	$[1, 3, 9, 8, 0, 7, 7, 0]$	$[3, 7, 2]$	yes
1	$[2, 3, 9, 8, 0, 7, 7, 0]$	$[3, 7, 2]$	yes
2	$[2, 5, 9, 8, 0, 7, 7, 0]$	$[3, 7, 2]$	yes
3	$[2, 5, 1, 8, 0, 7, 7, 0]$	no solution	no
4	$[2, 5, 1, 9, 0, 7, 7, 0]$	no solution	no

(QED)

Observation 4.2

The line falls exactly at $t = \lfloor (8 - 3)/2 \rfloor = 2$. Up to two errors are always repaired; from three the system has no solution. A construction theorem shows in numbers where the possible ends.

Observation 4.3

The existence theorem draws no such line. It says that making the block long enough drives the error probability as low as one likes, and says nothing about how many errors this length-8 code repairs. An asymptotic statement and a finite one are different sentences.

5. The construction is optimal as well

Verification 5.1: The Singleton bound reads $d \leq n - k + 1 = 6$.

Reed–Solomon minimum distance (all 1331 codewords enumerated)		6
Singleton bound		6

Verification 5.2: Draw 40 random linear codes of the same size and measure their minimum distance.

minimum distance	4	5
count	12	28

0 of the 40 reached the bound of 6. (QED)

Observation 5.3

The explicit construction sits on the bound every time, and a code drawn at random usually does not. Existing and being optimal are, again, two different questions.

Observation 5.4

This paper does not write that random codes are bad. Random codes are known to be good as the length grows, and Shannon's proof rides on exactly that. What is shown here is only that at this small size none of them reached the bound.

6. The brake: a constraint borne only by the construction

Verification 6.1: A field of order q exists if and only if q is a prime power (Galois).

fields exist for q	2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29
no field for q	6, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26, 28, 30

(QED)

Observation 6.2

There is no field of order six. So there is no Reed–Solomon code over a six-letter alphabet either. Yet Shannon's capacity is defined for any alphabet size whatever — only the construction bears the algebraic constraint.

Observation 6.3

This does not make the construction inferior. It says only that the more concrete the thing handed over, the more concrete the constraints that come with it. A theorem that hands over nothing incurs no constraints on what it hands over.

7. The census

Observation 7.1

theorem	what it says	tool	form
Shannon 1948	a code exists	averaging over random codes	existence
Galois / Reed–Solomon	here is a code	polynomials over a finite field	construction (with an algorithm)
Singleton	$d \leq n - k + 1$	counting	an upper bound
existence of finite fields	only prime powers	Galois	a constraint

Observation 7.2

“A good code exists” and “here is a good code” are not two phrasings of one fact. Some sixty years lay between them — explicit constructions approaching capacity appeared more than half a century after Shannon's theorem.

Observation 7.3

The corpus has met this shape repeatedly. In Paper 161, only one of five fixed-point theorems handed over an algorithm. In Paper 159, uniqueness was proved and recovery still was not assured. Writing down the form of a theorem's conclusion is the same discipline as writing down the distinct root of a value.

8. Conclusion

1. Shannon names no code at all (Ver. 2.1, Obs. 2.2).
2. Reed–Solomon comes with its decoder (Constructions 3.1, 3.2).
3. The boundary is exactly $t = 2$ (Ver. 4.1): no solution at three.
4. The construction sits on the bound (Ver. 5.1): 0 of 40 random codes did.
5. There is no field of order six (Ver. 6.1): a constraint only the construction bears.
6. Existence, construction, bound and constraint are four different forms (Obs. 7.1).

Closing: A proof of existence often hands over nothing at all. That is not a shortcoming; it is the kind of theorem it is. So the question to ask on reading one is not whether it was proved but what is left in one's hands.

References

1. Galois, É. (1830). *Sur la théorie des nombres*. Bulletin des Sciences Mathématiques.
2. Shannon, C. E. (1948). *A mathematical theory of communication*. Bell System Technical Journal, 27.
3. Singleton, R. C. (1964). *Maximum distance q -nary codes*. IEEE Transactions on Information Theory, 10(2).
4. Reed, I. S., & Solomon, G. (1960). *Polynomial codes over certain finite fields*. Journal of the Society for Industrial and Applied Mathematics, 8(2).
5. Welch, L. R., & Berlekamp, E. R. (1986). *Error correction for algebraic block codes*. US Patent 4,633,470.
6. Arıkan, E. (2009). *Channel polarization*. IEEE Transactions on Information Theory, 55(7).
7. MacWilliams, F. J., & Sloane, N. J. A. (1977). *The Theory of Error-Correcting Codes*. North-Holland.
8. Yamagishi, Y. (2026). *The Equals Sign Has Distinct Roots Too* [Paper 16], 3rd ed. Zenodo. 10.5281/zenodo.21600471
9. Yamagishi, Y. (2026). *From Galois to Noether* [Paper 85]. Zenodo. 10.5281/zenodo.21741344
10. Yamagishi, Y. (2026). *Two Entropies, Not to Be Conflated* [Paper 88]. Zenodo. 10.5281/zenodo.21747809
11. Yamagishi, Y. (2026). *Ill Posed Is Not One Word* [Paper 159]. Zenodo. 10.5281/zenodo.22092229
12. Yamagishi, Y. (2026). *A Fixed Point Is Not One Theorem* [Paper 161]. Zenodo. 10.5281/zenodo.22092530
13. Yamagishi, Y. (2026). *The Whole Can Be Better Known Than Its Parts* [Paper 162]. Zenodo. 10.5281/zenodo.22092568

— *From thinking to syncing.* —

Yuuki YAMAGISHI (山岸 勇輝)

© 2026 Yamagishi Complexity Torus Lab, Japan · Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0)