壊れた場所が分かれば、符号は二倍直せる

— 長さ 7 のハミング符号は、場所の分からない誤りなら 1 個しか直せないが、場所の分かる消失なら 2 個まで必ず直せる — 誤り一つは消失二つぶんの手間を食う — [論文619]

山岸 勇輝 (Yuuki YAMAGISHI)
Yamagishi Complexity Torus Lab, Japan｜山岸勇輝ラボ
2026年9月

— From thinking to syncing. —

要旨

データに冗長な部分を足しておくと、途中で一部が壊れても元に戻せる（誤り訂正符号）。壊れた場所が分かっている場合（消失）と、分からない場合（誤り）で、何個まで直せるかを総当たりで数える。新しい定理も法則も主張しない。 第一に、ハミング符号は、誤りなら 1 個、消失なら 2 個まで直せる——長さ 7・符号語 16 個・最小距離 3 の符号で、全部の符号語と全部の壊れ方を試すと、誤り 1 個は 112 通りすべて直り、誤り 2 個は 336 通りのうち一つも正しく直らなかった。消失なら 2 個でも 336 通りすべて一つに決まった（第2節）。 第二に、消失 3 個でも、五つに四つは決まる——消失 3 個では 560 通りのうち 448 通り（0.800000）が一つに決まり、決まらないのは、壊れた三つの場所が重さ 3 の符号語の 1 の場所とちょうど重なる 7 通りだけだった（第2節）。 第三に、これが本稿の芯である。誤り一つは、消失二つぶんの手間を食う——13 を法とする数で作った長さ 12・情報 6 個・最小距離 7 のリード・ソロモン符号で、誤りと消失を混ぜて乱数で 30 回ずつ試すと、誤りの数の 2 倍と消失の数の和が 6 以下の組（誤り 3／誤り 2・消失 2／誤り 1・消失 4／消失 6）はすべて直った（第3節）。 第四に、その和が 6 を超えると直らなくなる——誤り 4 個（和 8）では 30 回中 2 回、誤り 3 個・消失 2 個（和 8）では 0 回しか直らなかった。消失 7 個では残る 5 個から情報 6 個は決めようがない（第3節）。 第五に、分離子は、壊れた場所が分かっているかどうかである——場所が分かれば、残りの部分から元を決めるだけでよい。場所が分からなければ、どこが壊れたかを見つける分の冗長さも要り、直せる数が半分になる（第4節）。 キーワード：誤り訂正符号、消失訂正、ハミング符号、リード・ソロモン符号、最小距離。

本稿の射程（射程注記）：新しい定理も法則も主張しない——ハミング符号（ハミング、1950）、リード・ソロモン符号（リードとソロモン、1960）、誤りと消失を合わせて直せる条件（フォーニー、1965 ほか。マクウィリアムズとスローンの教科書にある）は、いずれも既知である。速い復号法を扱わない——ハミング符号は全符号語と全部の壊れ方の総当たり、リード・ソロモン符号は情報の数だけの点を選んで補間する総当たりで確かめる。実装を論じない——QR コードや光ディスクで実際にどう使われているかには立ち入らない。既刊との関係：論文597 は、長さ 7 のハミング符号が半径 1 の球で 128 語をちょうど埋めることと、数の条件だけでは符号の在る無しが決まらないことを示した——本稿は同じハミング符号で、壊れた場所が分かると直せる数が倍になる側を見る。加えたのは、ハミング符号で誤りと消失を全部の壊れ方で数えたこと、消失 3 個で決まらない組が重さ 3 の符号語と一致することを確かめたこと、リード・ソロモン符号で誤りと消失を混ぜ、直せる境目を数で示したこと、分離子を「場所が分かるか」に置いたことである。

1. 記法と問い

設定：長さ n の符号語の集まりを符号といい、二つの符号語の違う位置の数の最小を最小距離 d という。受け取った語の一部が壊れたとき、壊れた位置が分かっているものを消失、分からないものを誤りと呼ぶ。誤りが e 個、消失が f 個のとき、

$$2e + f \le d - 1$$

なら、元の符号語はいつも一つに決まる。

問い：この境目は、実際に試すとどう現れるか。誤りと消失で、なぜ手間が倍違うのか。

2. ハミング符号

計算 2.1：長さ 7 のハミング符号（符号語 16 個、最小距離 3）で、すべての符号語とすべての壊れ方を試した。誤りは最も近い符号語に直し、それが一つに決まって元と同じなら「直った」とした。消失は、壊れていない位置が一致する符号語が一つだけなら「決まった」とした。

壊れ方	数	直った・決まった
誤り 1 個	112	112
誤り 2 個	336	0
消失 1 個	112	112
消失 2 個	336	336
消失 3 個	560	448（0.800000）
消失 4 個	560	0

> **観察 2.2**
>
> 同じ符号で、誤りなら 1 個、消失なら 2 個まで必ず直る。最小距離 3 なら $2e + f \le 2$ で、誤り 1 個か消失 2 個が境目になる——誤り 2 個では、最も近い符号語が別のものになり、一つも正しく直らなかった。直すつもりで、別の符号語に書き換えてしまう。

計算 2.3：消失 3 個で一つに決まらなかった位置の組を調べると、35 通りのうち 7 通りで、重さ 3 の符号語 7 個の 1 の位置の組とちょうど一致した。

> **観察 2.4**
>
> 消失が境目を越えても、すぐには全部だめにならない。壊れた三つの位置が、ある符号語の 1 の位置と重なるときだけ、その符号語を足したものと区別がつかなくなる——それ以外の 28 通りでは、境目を越えても一つに決まった。境目は「必ず直る」の境目で、「直らない」の始まりではない。

3. リード・ソロモン符号

計算 3.1：13 を法とする数で、次数 5 以下の多項式の $x = 1, \dots, 12$ での値を並べた符号（長さ 12・情報 6 個・最小距離 7）を作った。誤りと消失を混ぜて乱数で 30 回ずつ壊し、壊れていない位置から 6 点を選んで補間する総当たりで、最も多くの位置と合う多項式を探した。それが一つに決まって元と同じなら「直った」とした。

誤り	消失	$2e + f$	直った（30 回中）
3	0	6	30
2	2	6	30
1	4	6	30
0	6	6	30
4	0	8	2
3	2	8	0
0	7	7	0

> **観察 3.2**
>
> これが本稿の芯である。誤り一つは、消失二つぶんの手間を食う。$2e + f \le 6$ の四つの組は、誤り 3 個でも消失 6 個でも、どれも 30 回すべて直った。誤り 1 個を消失 2 個に置き換えても、直せることは変わらない——境目を越えた誤り 4 個では 2 回、誤り 3・消失 2 では 0 回しか直らなかった。

4. 分離子

> **観察 4.1**
>
> 分離子は、壊れた場所が分かっているかどうかである。場所の分かる消失なら、残った位置から元を決めればよい。リード・ソロモン符号では、残った 6 点を通る多項式がちょうど一つ決まる——場所の分からない誤りでは、まずどこが壊れたかを見つけなければならない。その見つける分にも冗長さを使うので、直せる数が半分になる。

> **観察 4.2**
>
> 論文597 と並べる。597 は、長さ 7 のハミング符号が符号語のまわりの半径 1 の球で 128 語をちょうど埋めることを示した——その半径 1 は、場所の分からない誤りを直せる範囲である。場所が分かれば、同じ符号で倍の 2 個まで届く。

> **観察 4.3**
>
> 言わないこと。速い復号法は扱わず、総当たりで確かめた。QR コードや光ディスクでの使われ方には立ち入らない——示したのは、誤りと消失の境目が総当たりの結果として現れること、そして誤り一つが消失二つぶんに当たることである。

5. 点呼と結び

1. ハミング符号の誤り 1 個は 112/112（計算 2.1）：必ず直る。
2. 誤り 2 個は 0/336（計算 2.1）：別の符号語に書き換える。
3. 消失 2 個は 336/336（計算 2.1）：倍まで直る。
4. 消失 3 個でも 0.800000 が決まる（計算 2.1）：境目は必ず直るの境目。
5. 決まらない 7 通りは重さ 3 の符号語の位置（計算 2.3）：ちょうど一致。
6. リード・ソロモン符号で $2e + f \le 6$ はすべて直る（計算 3.1）：四つの組で 30/30。
7. 誤り 4 個は 2/30（計算 3.1）：境目を越える。
8. 誤り一つは消失二つぶん（観察 3.2）：本稿の芯。
9. 分離子は場所が分かるか（観察 4.1）：見つける分の冗長さ。
10. 半径 1 の球は誤りの範囲（観察 4.2）：論文597。

結び：誤り訂正符号は、冗長な部分を使って壊れた部分を直す。壊れた場所が分かっていれば、分からないときの二倍直せる——長さ 7 のハミング符号は、場所の分からない誤りなら 1 個しか直せず 2 個では一つも正しく直らないが、場所の分かる消失なら 2 個まで必ず直り、3 個でも 0.800000 が決まった。誤り一つは、消失二つぶんの手間を食う——長さ 12 のリード・ソロモン符号で、誤りの数の 2 倍と消失の数の和が 6 以下ならいつも直り、それを超えると直らなくなった。分離子は、壊れた場所が分かっているかどうかである——分からなければ、見つける分にも冗長さを使う。既刊との位置——論文597 の半径 1 の球は誤りを直す範囲で、場所が分かれば同じ符号が倍まで届く。正直に言えば——速い復号法も実装も扱わず、総当たりで数えただけである。

参考文献

1. Forney, G. D. (1965). On decoding BCH codes. *IEEE Transactions on Information Theory*.
2. Hamming, R. W. (1950). Error detecting and error correcting codes. *The Bell System Technical Journal*.
3. MacWilliams, F. J., & Sloane, N. J. A. (1977). *The Theory of Error-Correcting Codes*. North-Holland.

4. Reed, I. S., & Solomon, G. (1960). Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*.

5. 山岸勇輝 (2026). 『球がぴったり詰まる数の条件を満たしても、その符号は在るとは限らない』[論文597]. Zenodo. 10.5281/zenodo.23014414

— From thinking to syncing. —

山岸 勇輝 (Yuuki YAMAGISHI)

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