# AI-Assisted Nonexistence Proofs for Five Binary Linear Code Parameters

**Anonymous Authors**[1]

## Abstract

We present an AI-assisted mathematical investigation excluding binary linear codes with parameters $[43, 10, \geq 17]$, $[44, 10, \geq 18]$, $[44, 11, \geq 17]$, $[45, 11, \geq 18]$, and $[42, 16, \geq 13]$. The main proof reduces the first target to extending one of 172 classified $[40, 7, 18]$ codes and rules out every extension through complete coset enumeration and pairwise incompatibility certificates. Two independently implemented scans examine $2^{32}$ cosets per mother code and agree on all 429,024 accepted cosets; a separate checker replays 619,053,789 pair rejections. Three targets follow by puncturing and shortening, while the fifth follows from a published $[41, 14, 14]$ nonexistence theorem. Explicit constructions yield four exact optimal distances and the interval $16 \leq d_2(45, 11) \leq 17$. We describe the recorded contributions of AI to exploration and verification design, and formalize the mathematical reductions in Lean with explicit interfaces for published and computational inputs.

## 1. Introduction

A binary linear code is a subspace of $\mathbb{F}_2^n$. Determining the largest possible minimum distance at fixed length and dimension is a finite problem, but a negative answer must cover every subspace, including those far from familiar constructions. A failed search for a generator matrix supplies no such coverage. This makes code nonexistence a useful setting for studying how AI-assisted mathematical work can produce independently checkable results.

We study five parameter targets through two proof routes. The main route starts with a hypothetical $[43, 10, \geq 17]$ code. Parity extension, a low-weight dual-word argument, and shortening force a full-support $[40, 7, 18]$ subcode. A published classification then reduces the unrestricted existence question to 172 concrete mother codes. Each mother has $2^{32}$ even cosets to examine. The successful reduction is stronger than an unsuccessful extension search: every pair of distinct admissible cosets is incompatible, so the three cosets required for an extension cannot exist.

*Table 1.* Five excluded targets and the resulting optimum information. Lower bounds use explicit matrices. The first three exact values and the fourth upper bound share one main proof; the last row is a consequence of published Proposition 2.

| Excluded target | Proof route | $d_2(n, k)$ |
|---|---|---|
| $[43, 10, \geq 17]$ | Main exclusion | 16 |
| $[44, 10, \geq 18]$ | Puncturing | 17 |
| $[44, 11, \geq 17]$ | Shortening | 16 |
| $[45, 11, \geq 18]$ | Puncturing | $[16, 17]$ |
| $[42, 16, \geq 13]$ | E3 reduction | 12 |

The second route illustrates a different useful outcome of AI-assisted research. An apparent target, $[42, 16, \geq 13]$, is already excluded by a short consequence of a published theorem. Parity extension and two shortenings produce a $[41, 14, \geq 14]$ code; an exact-distance normalization connects it to the published exclusion of $[41, 14, 14]$. The contribution here is the explicit, checked connection to the requested target.

Table 1 states the mathematical outcomes. The evidence accompanying them has three components: a structural proof covering arbitrary binary linear codes; concrete matrices, complete enumeration records, and rejection witnesses; and Lean proofs of the reductions with named external inputs. AI contributes to literature discovery, proof development, implementation, and review. Acceptance depends on these evidence components rather than on the model's confidence or the number of favorable reviews.

For AI-assisted mathematics, the case study highlights a specific verification issue: checking that every saved candidate is valid does not show that a search saved every valid candidate. Here that distinction led to a second complete enumeration with different coordinates and traversal. The mathematical argument, computation, and recorded AI interventions are presented together so that each claimed contribution can be assessed at its actual scope.

[1]Anonymous Institution, Anonymous City, Anonymous Region, Anonymous Country. Correspondence to: Anonymous Author <anon.email@domain.com>.

Preliminary work. Under review by the International Conference on Machine Learning (ICML). Do not distribute.

## 2. Background and Proof Obligations

### 2.1. Notation and elementary operations

Write $[n, k, d]$ for a $k$-dimensional binary linear code of length $n$ with minimum nonzero Hamming weight exactly $d$, and $[n, k, \geq d]$ when only a lower bound is imposed. Let $d_2(n, k)$ be the maximum achievable distance. Zero and repeated columns are allowed throughout. A code has *full support* if no coordinate is identically zero. It is *even* if all its words have even weight.

Puncturing deletes coordinates. Deleting $t < d(C)$ coordinates is injective on $C$ and reduces distance by at most $t$. Shortening on a coordinate set $S$ first restricts to words zero on $S$ and then deletes $S$. If the projection onto $S$ has rank $r$, shortening reduces dimension by exactly $r$ and does not reduce minimum distance. Parity extension sends $x$ to $(x, \sum_i x_i)$ and preserves dimension. These operations apply to all codes under consideration, without a symmetry or projectivity assumption.

### 2.2. Classification and computational bounds

Classical coding theory combines general inequalities with classification near extremal parameters. The Griesmer bound gives

$$n \geq g_2(k, d) := \sum_{j=0}^{k-1} \lceil d/2^j \rceil \tag{1}$$

for a binary linear $[n, k, \geq d]$ code (Griesmer, 1960). For the targets considered here, the decisive information is more specific than this bound. The eight-dimensional classification of Bouyukliev et al. (2000) excludes exact $[41, 8, 18]$. We call this input **E1**. Together with $g_2(8, 19) = 42$, E1 also excludes $[41, 8, \geq 18]$.

Bouyukliev & Jaffe (2001) classify optimal binary linear codes of dimension at most seven. The input used here, **E2**, is an upper bound of 172 coordinate-equivalence classes of full-support $[40, 7, 18]$ codes. Our concrete catalogue contains 172 pairwise inequivalent representatives, so E2 establishes its completeness. The distribution by hull dimension is corroborated by Bouyuklieva & Dzhumalieva-Stoeva (2025): dimensions $1, 3, 5$ occur $33, 62, 77$ times. Hull counts are a consistency check; completeness follows from the class bound and actual inequivalence, not from matching these three numbers.

A separate classification technique extends residual codes. Bouyuklieva & Bouyukliev (2020), Proposition 2, prove that a binary linear $[41, 14, 14]$ code does not exist. We call this input **E3**. Our fifth result imports the proposition as a whole and supplies the reduction from $[42, 16, \geq 13]$. The historical classification computations underlying E1–E3 remain published inputs; our computations concern the new extension obstruction and the explicit lower-bound matrices.

### 2.3. Constructions, certification, and formal proof

Code tables organize lower constructions and upper bounds at fixed parameters (Grassl, 2007). They are useful starting points for identifying targets and recovering witnesses. A table entry, however, plays a different role from an explicit construction: the latter can be checked by row reduction and enumeration of all nonzero messages. We include the actual lower-bound generators in the appendix, including matrices reconstructed from the quasicyclic constructions recorded by CodeTables.

Computational nonexistence requires a finite domain with a justified connection to every hypothetical object. In the main proof, the classification fixes the mothers and a linear quotient fixes the coset domain. Two complete enumerators address coverage; a separate witness checker addresses rejection validity. These tasks are logically different. The rejected pairs have small witnesses, but the completeness of the accepted-coset lists still depends on exhaustive enumeration.

Lean 4 provides a further level of verification for definitions and deductions (de Moura & Ullrich, 2021); the formal developments use mathlib (The mathlib Community, 2020). The formal statements refer to actual finite-dimensional subspaces, weights, and generator matrices. Their external hypotheses identify the precise facts supplied by published classification and computational evidence. This arrangement exposes where formal proof ends and ordinary computational trust begins, while checking the entire intervening mathematical argument.

## 3. From an Arbitrary Code to 172 Mothers

**Theorem 3.1.** *There is no binary linear* $[43, 10, \geq 17]$ *code.*

The proof uses E1 and E2 together with the finite computation specified in Section 4. We give the full structural argument here; Appendix A supplies the auxiliary identities and coordinate details.

### 3.1. A forced dual word of weight four

Suppose that $C_0$ is a $[43, 10, \geq 17]$ code. Its parity extension $C$ is an even $[44, 10, \geq 18]$ code: an odd weight at least 17 increases by one, and an even weight at least 17 is already at least 18. Conversely, puncturing any coordinate of an even $[44, 10, \geq 18]$ code gives a $[43, 10, \geq 17]$ code. Thus it suffices to exclude $C$.

**Lemma 3.2.** *Every three columns of a generator matrix for* $C$ *are linearly independent.*

*Proof.* If three columns had rank at most two, shortening on them would give a length-41 code of dimension at least eight and distance at least 18. Taking an eight-dimensional subcode contradicts E1, since the Griesmer bound excludes distance at least 19. □

Let $A_w$ and $B_j$ count weight-$w$ words of $C$ and weight-$j$ words of $C^\perp$, respectively. Lemma 3.2 implies $B_1 = B_2 = B_3 = 0$. Define the length-44 binary Krawtchouk polynomials by

$$K_j(w) = \sum_{t=0}^{j} (-1)^t \binom{w}{t} \binom{44-w}{j-t}.$$

The MacWilliams identities give $\sum_w A_w K_j(w) = 2^{10} B_j$. Consider

$$\begin{aligned} P(w) &= (w-18)(w-20)(w-24)(w-26) \\ &= \tfrac{3}{2} K_4(w) + 22 K_2(w) + \tfrac{403}{2} K_0(w). \end{aligned} \tag{2}$$

Every allowed nonzero weight is even and at least 18, so $P(w) \geq 0$ on these weights. Since $P(0) = 224640$ and $B_0 = 1$,

$$224640 \leq \sum_w A_w P(w) = 1536 B_4 + 206336.$$

Therefore $B_4 \geq 143/12$, hence $B_4 \geq 12$. In particular, $C^\perp$ contains a weight-four word.

### 3.2. Shortening gives a full-support mother

**Lemma 3.3.** *Shortening $C$ on the support of a weight-four dual word produces an even full-support $[40, 7, 18]$ code $K$.*

*Proof.* Permute the four support coordinates to the end. Their generator columns $v_1, v_2, v_3, v_4 \in \mathbb{F}_2^{10}$ satisfy $v_1 + v_2 + v_3 + v_4 = 0$. Any three are independent, so the projection rank is three. Shortening therefore has dimension $10 - 3 = 7$, length 40, and distance at least 18. All its words remain even. If its distance exceeded 18, it would be at least 20, contradicting $g_2(7, 20) = 42 > 40$.

Let $U = \langle v_1, v_2, v_3 \rangle$. A remaining coordinate would vanish on every shortened word precisely if its generator column belonged to $U$. The seven nonzero vectors of $U$ are the four support columns and their three distinct pair sums. An outside column equal to a support column would give a dependent pair; an outside column equal to a pair sum would give a dependent triple. The zero vector is also excluded by Lemma 3.2. Thus no outside coordinate vanishes, and $K$ has full support. □

By E2 and the verified inequivalence of the 172 actual representatives, $K$ is coordinate-equivalent to one catalogue member. A permutation of its 40 coordinates preserves every distance condition below.

### 3.3. Every extension requires compatible cosets

Choose a basis for the shortened subcode and extend it to a basis of $C$. The image on the final four coordinates is the even-weight subspace of $\mathbb{F}_2^4$: it has dimension three and is orthogonal to $(1, 1, 1, 1)$. A change of row basis gives

$$G_C = \begin{pmatrix} G_K & 0000 \\ a_1 & 1001 \\ a_2 & 0101 \\ a_3 & 0011 \end{pmatrix}. \tag{3}$$

The $a_i \in \mathbb{F}_2^{40}$ have even weight because $C$ is even. For a vector $a$, set $\delta_K(a) = \min_{c \in K} \mathrm{wt}(a + c)$. Each nonzero combination of one or two of the final three rows has tail weight two; the combination of all three has tail weight four. Consequently the distance condition for (3) is exactly

$$\begin{aligned} \delta_K(a_i) &\geq 16 \qquad (1 \leq i \leq 3), \\ \delta_K(a_i + a_j) &\geq 16 \qquad (i < j), \\ \delta_K(a_1 + a_2 + a_3) &\geq 14. \end{aligned} \tag{4}$$

Let $E_{40}$ be the even-weight subspace of $\mathbb{F}_2^{40}$. Since $K \subset E_{40}$, the quotient $E_{40}/K$ has dimension $39 - 7 = 32$. Let $F_K$ consist of the cosets satisfying $\delta_K(a) \geq 16$. Join distinct cosets $a+K, b+K \in F_K$ when $\delta_K(a+b) \geq 16$. Conditions (4) require a triangle in this graph; the three cosets must be distinct because equal cosets have sum-distance zero. The computation finds that all 172 graphs have no edges. This stronger obstruction rules out (3) before the triple-sum condition is needed, proving Theorem 3.1.

## 4. Complete Enumeration and Rejection Certificates

The computational statement used in Theorem 3.1 is finite and explicit:

**Proposition 4.1** (Computed incompatibility)**.** *For each of the 172 catalogue codes $K$, and all distinct cosets $a+K, b+K$ with $\delta_K(a), \delta_K(b) \geq 16$, one has $\delta_K(a+b) < 16$.*

Its verification has three parts: validating the catalogue, enumerating the complete $F_K$, and rejecting every unordered pair from that set.

### 4.1. Concrete objects and canonical representatives

For each mother, seven 40-bit integers specify the generator rows. Enumerating all 128 messages checks the rank, evenness, minimum distance 18, and full support. The 172 matrices have 21,844 nonzero messages in total. Coordinate equivalence is tested using a colored incidence graph with

*Table 2.* Recorded complete computation. A coset visit is one element of the explicitly defined even quotient. Pair replay checks saved witnesses and does not repeat the coset scans.

| Quantity | Count |
|---|---|
| Full-support mother codes | 172 |
| Cosets per mother, per scanner | $2^{32}$ |
| Cosets across mothers, per scanner | 738,734,374,912 |
| Accepted cosets, $\sum_K \lvert F_K \rvert$ | 429,024 |
| Unordered pairs, $\sum_K \binom{\lvert F_K \rvert}{2}$ | 619,053,789 |
| Compatible pairs | 0 |
| Replayed pair witnesses | 619,053,789 |
| Invalid or nonrejecting witnesses | 0 |

40 coordinate vertices and 128 codeword vertices. Edges record the 1 entries of codewords and the two vertex types have distinct colors. Isomorphisms of these graphs correspond exactly to coordinate equivalences of the codes. The stored canonicalization results distinguish all 172 graphs.

To enumerate cosets, put a generator of $K$ into systematic form with pivot positions $p_1, \ldots, p_7$ and rows $r_1, \ldots, r_7$. The linear map

$$N_K(x) = x + \sum_{i=1}^{7} x_{p_i} r_i \tag{5}$$

zeros all pivots, has kernel $K$, and preserves parity. It gives a unique zero-pivot representative of each coset. Among the 33 free coordinates, the evenness equation removes one degree of freedom. Thus the scan domain has exactly $2^{32}$ elements, rather than a sampled or symmetry-restricted subset.

### 4.2. Two implementations cover the entire domain

The first scanner splits the 33 free bits into 27 high bits and six low bits. For each high assignment, it intersects 64-bit masks expressing the 128 distance constraints. Parity leaves 32 low assignments, so $2^{27} \cdot 32 = 2^{32}$ even representatives are considered. An affine permutation with odd multiplier reorders the high assignments bijectively. Mask rejection is exact: a bit survives precisely when the corresponding representative has distance at least 16 from every codeword.

The second scanner constructs systematic pivots in the opposite order, builds a different basis for the 32-dimensional even quotient, and enumerates it in Gray-code order. It computes weights on actual 40-bit words against all 128 actual codewords. Early termination rejects a candidate only after a recomputed distance below 16. Its output is converted to the first normalization and compared as a complete set, not only by cardinality. All 172 sets agree.

### 4.3. Independent replay of every rejected pair

Order each complete list $F_K$. For every $i < j$, the certificate stores a message $u \in \{0, \ldots, 127\}$ such that

$$\mathrm{wt}(a_i + a_j + uG_K) < 16. \tag{6}$$

An independent checker reconstructs $uG_K$ from the literal generator rows, verifies the inequality, checks that the number and order of pairs are correct, and requires exact end-of-file. It also checks every saved member of $F_K$ against all 128 codewords, totaling 54,915,072 distance evaluations. The unified replay processes 149 binary streams and 23 text streams and validates all 619,053,789 witnesses.

This replay would detect a false rejection or malformed stream, but it cannot detect an admissible coset omitted from both its input list and the pair stream. Completeness is supplied separately by the two full scans. Together these checks establish Proposition 4.1, with the compiler, runtime, enumeration implementations, and graph canonicalizer remaining part of the computational trust boundary.

## 5. Consequences and the Fifth Target

**Corollary 5.1.** *Binary linear* $[44, 10, \geq 18]$, $[44, 11, \geq 17]$, *and* $[45, 11, \geq 18]$ *codes do not exist.*

*Proof.* Puncturing a $[44, 10, \geq 18]$ code gives a $[43, 10, \geq 17]$ code, contradicting Theorem 3.1. Shortening a $[44, 11, \geq 17]$ code on any coordinate gives a length-43 code of dimension at least ten and distance at least 17; a ten-dimensional subcode gives the same contradiction. Finally, puncturing a $[45, 11, \geq 18]$ code gives the excluded $[44, 11, \geq 17]$ parameters. □

For the fifth target, the exact-distance convention in E3 must be respected. The following elementary lemma supplies the connection.

**Lemma 5.2** (Distance normalization)**.** *For* $k \geq 1$ *and* $d \geq 1$*, existence of a binary linear* $[n, k, \geq d]$ *code implies existence of a binary linear* $[n, k, d]$ *code.*

*Proof.* Let the original minimum distance be $D \geq d$, and choose a word of weight $D$. Puncture $D - d$ positions in its support. Since $D - d < D$, puncturing is injective. Every nonzero word retains weight at least $D - (D - d) = d$, and the chosen word attains $d$. Append $D - d$ zero coordinates to restore length $n$ without changing dimension or distance. □

**Theorem 5.3.** *There is no binary linear* $[42, 16, \geq 13]$ *code.*

*Proof.* Parity extension of a hypothetical code gives $[43, 16, \geq 14]$. Shortening one coordinate loses at most

one dimension. Choose a 15-dimensional subcode, shorten another coordinate, and choose a 14-dimensional subcode. The result has parameters $[41, 14, \geq 14]$. Lemma 5.2 gives exact $[41, 14, 14]$, contradicting E3, namely Proposition 2 of Bouyuklieva & Bouyukliev (2020). □

The construction in this proof permits zero columns. This is consistent with both our original domain and the binary linear code domain of E3. In particular, the proof does not assume that a minimum-weight witness survives arbitrary shortening; normalization is performed after the shortening steps.

**Corollary 5.4.** *The optimal distances satisfy*

$$d_2(43, 10) = 16, \qquad d_2(44, 10) = 17,$$
$$d_2(44, 11) = 16, \qquad d_2(42, 16) = 12,$$

*and* $16 \leq d_2(45, 11) \leq 17$.

*Proof.* Theorems 3.1 and 5.3 and Corollary 5.1 give the upper bounds. Appendix E specifies full-rank generators of $[43, 10, 16]$, $[44, 10, 17]$, $[44, 11, 16]$, and $[42, 16, 12]$, together with their fully enumerated weight spectra. Appending a zero coordinate to the $[44, 11, 16]$ code gives $[45, 11, 16]$. □

## 6. AI Assistance and Formal Verification

### 6.1. A workflow with explicit acceptance conditions

The research used an ARIS-style workflow: a persistent formal specification, linked literature and experiment records, parallel exploration, and separate review of proposed arguments. The specification fixed the unrestricted matrix quantifiers before search. A positive candidate required full rank and a complete nonzero-message distance check; a negative conclusion required a reduction covering the entire target class. The research memory retained unsuccessful routes with their actual scope, preventing a fixed-seed exclusion from becoming a global nonexistence claim in a later session.

The final proof does not require replaying the discovery trajectory. Candidate generation, constraint-programming models, prompts, and search order guided exploration. The accepted argument uses the reductions of Section 3, the published class bound, and the finite evidence of Section 4. Figure 1 shows this dependency structure.

### 6.2. Recorded interventions and their scope

The project records support two concrete examples of model contribution. A Gemini consultation suggested testing native early-rejection filters. The subsequent profile found that candidates in the tested instance needed about 3.38 distance checks on average before rejection, motivating further local implementation of bit-parallel low-bit masks. The implemented mask algorithm and its full-domain justification were developed in the local research process; the model's performance prediction was revised by measurement. The profile concerns an early fixed subcode, rather than the final 172-case workload.

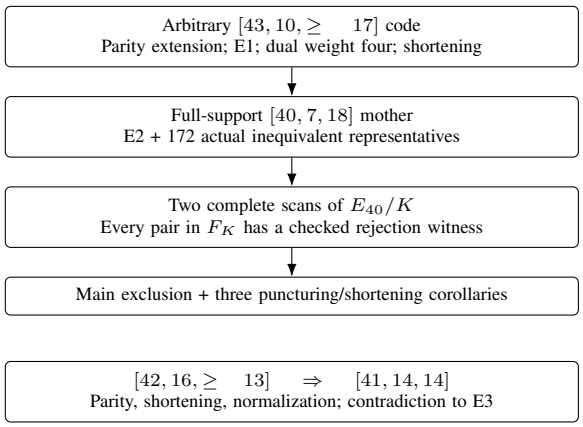



*Figure 1.* Two routes to five exclusions. AI assists in finding and checking the routes. Published theorems, mathematical deductions, and explicit computations supply the proof dependencies. The fifth target uses E3 rather than the 172-mother computation.

A Grok review sharpened the missing completeness check. At that stage, independent validation established that saved cosets satisfied the constraints, while the review packet already noted that an independent full scan was missing. The review explicitly required a second implementation to decide acceptance or rejection over the entire quotient and compare complete output sets. The project then implemented the opposite-pivot, Gray-order scan described above. This intervention has a concrete consequence: it tests omitted admissible cosets, which member validation alone cannot test.

Local agents also worked on source retrieval, structural deductions, mother reconstruction, code, and proof exposition. Later consultations checked equations, quantifiers, classification scope, and evidence connections. These are documented research and review contributions. The final verification procedures operate on ordinary mathematical and computational objects and require no model API.

### 6.3. What the Lean developments establish

Both formal projects use Lean 4.34.1 and pinned mathlib. The first formalizes parity extension, puncturing, shortening, the Griesmer argument, the MacWilliams calculation, the full-support mother reduction, quotient normalization, classification coverage, and the corollaries. Actual mother matrices and lower-bound generators are connected to the abstract code definitions and checked by kernel evaluation.

The final main theorem takes four explicit parameters: E1; E2; pairwise coordinate inequivalence of the catalogue; and pair incompatibility for each catalogue member. Its type therefore records the boundary between kernel-checked deduction and the published or external computational facts. A finer interface expands the scan and certificate assumptions. The second project proves the entire reduction to exact $[41, 14, 14]$ and takes E3 as an explicit parameter.

The audited theorem dependencies contain the usual Lean axioms `propext`, `Classical.choice`, and `Quot.sound`, with no `sorryAx`. Explicit parameters do not appear in this axiom list. Consequently, a clean axiom audit verifies the deductions but does not discharge E1–E3, catalogue inequivalence, or the exhaustive computations. Appendix C gives the exact interfaces.

## 7. Discussion and Conclusion

The central mechanism is a change in proof scale. An unrestricted length-43 existence question reduces to a published finite classification, then to even cosets with a precisely counted domain, and finally to low-weight witnesses for pair incompatibility. The pair obstruction is stronger than the triangle obstruction required by the extension. It makes the final rejection stage simple to replay while leaving enumeration completeness as a separate, explicit obligation.

The five targets illustrate both discovery and reuse. One main computation supplies four exclusions. A distinct literature theorem supplies the fifth through a short formalized reduction. Explicit lower constructions turn four of these upper bounds into exact values; the $[45, 11]$ distance-17 question remains open in the evidence presented here.

**Limitations.** This is a mathematical case study, not a controlled evaluation of AI agents. The records establish specific interventions but do not isolate model effectiveness, compute savings, or an autonomous-discovery rate. Historical classification and external graph canonicalization remain trusted inputs, and the two exhaustive scanners have not been verified inside Lean. The saved pair witnesses alone cannot certify that $F_K$ is complete. Novelty or priority beyond the demonstrated statements also requires a broader literature assessment; the $[42, 16]$ exclusion is presented explicitly as a consequence of the 2020 theorem.

The resulting proof package offers concrete targets for further work: replace the coset enumeration assumptions with a formally checked coverage certificate, or extend the structural method to other parameter sets. For the five targets here, the mathematical conclusions and the respective roles of AI, computation, literature, and formal deduction are fully separated and inspectable.

## Impact Statement

This work studies mathematical proof and error-correcting codes. Its methodological contribution is an auditable separation of AI-generated suggestions from the evidence used to accept a mathematical claim. The results concern finite binary linear codes; the paper does not evaluate deployment decisions or human subjects. Explicit attribution and reproducible verification reduce the risk of presenting model agreement or incomplete search as proof.

## References

Bouyukliev, I. and Jaffe, D. B. Optimal binary linear codes of dimension at most seven. *Discrete Mathematics*, 226(1-3):51–70, 2001. doi: 10.1016/s0012-365x(00)00125-4.

Bouyukliev, I., Jaffe, D. B., and Vavrek, V. The smallest length of eight-dimensional binary linear codes with prescribed minimum distance. *IEEE Transactions on Information Theory*, 46(4):1539–1544, 2000. doi: 10.1109/18.850690.

Bouyuklieva, S. and Bouyukliev, I. Classification of linear codes by extending their residuals. In *Mathematical Software – ICMS 2020*, pp. 173–180. Springer, 2020. doi: 10.1007/978-3-030-52200-1_17.

Bouyuklieva, S. and Dzhumalieva-Stoeva, M. Optimal Linear Codes and Their Hulls. *Mathematics*, 13(15):2491, 2025. doi: 10.3390/math13152491.

de Moura, L. and Ullrich, S. The Lean 4 Theorem Prover and Programming Language. In *Automated Deduction CADE 28*, pp. 625–635, 2021. doi: 10.1007/978-3-030-79876-5_37.

Grassl, M. Bounds on the minimum distance of linear codes and quantum codes. Online code tables, 2007. URL `https://www.codetables.de/`. Construction records for binary parameters (44,10) and (44,11); archived in the accompanying evidence.

Griesmer, J. H. A Bound for Error-Correcting Codes. *IBM Journal of Research and Development*, 4(5):532–542, 1960. doi: 10.1147/rd.45.0532.

The mathlib Community. The Lean mathematical library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*, pp. 367–381, 2020. doi: 10.1145/3372885.3373824.

# A. Auxiliary Proofs and Exact Dependencies

This appendix expands the mathematical ingredients used in the main text. Theorems 3.1 and 5.3 retain their original unrestricted code domains. E1, E2, and E3 are published inputs as specified in Section 2; Proposition 4.1 is the external finite computation.

## A.1. Puncturing, shortening, and parity

For a set $S$ of $t$ coordinates, puncturing has kernel consisting of codewords supported in $S$. If $t < d(C)$, the kernel is zero, so dimension is preserved. Every remaining word loses at most $t$ ones, establishing the lower bound $d(C) - t$.

Let $\pi_S : C \to \mathbb{F}_2^S$ be coordinate projection, with rank $r$. The shortened code is the image of $\ker \pi_S$ after deleting $S$. This deletion is injective on the kernel because its members are zero on $S$. Rank-nullity gives dimension $\dim C - r$. No weight changes. For one coordinate, $r \leq 1$; if an exact smaller dimension is needed, choose a subspace of that dimension. This includes a coordinate that was identically zero before shortening.

Parity extension is an injective linear map because its first $n$ coordinates recover its input. Its weight is $\mathrm{wt}(x)$ for even-weight $x$ and $\mathrm{wt}(x) + 1$ for odd-weight $x$. The minimum distance is therefore at least the least even integer greater than or equal to the original lower bound. Puncturing any coordinate of an even $[44, 10, \geq 18]$ code preserves dimension and gives distance at least 17. This proves the equivalence used at the start of Section 3 without assuming that the punctured coordinate was originally a parity coordinate.

## A.2. A proof of the binary Griesmer bound

For completeness, the needed inequality can be obtained by induction on dimension. Let $c \in C$ have minimum weight $D$, and puncture the $D$ positions in its support. The kernel is $\langle c \rangle$: any other nonzero word supported there has weight at least $D$ and thus equals $c$. The residual image has dimension $k - 1$. For a nonzero residual word, take its two preimages $x, x + c$. If the common weight outside the support is $b$ and the weight of $x$ inside is $a$, then

$$a + b \geq D, \qquad D - a + b \geq D.$$

Adding yields $b \geq \lceil D/2 \rceil$. By induction,

$$n - D \geq \sum_{j=0}^{k-2} \left\lceil \frac{\lceil D/2 \rceil}{2^j} \right\rceil = \sum_{j=1}^{k-1} \left\lceil \frac{D}{2^j} \right\rceil.$$

The base $k = 1$ is $n \geq D$. Monotonicity in $D$ gives (1) for a distance lower bound. In particular,

$$g_2(8, 19) = 19 + 10 + 5 + 3 + 2 + 1 + 1 + 1 = 42, \qquad g_2(7, 20) = 20 + 10 + 5 + 3 + 2 + 1 + 1 = 42.$$

Both exceed 41 and 40, respectively. E1 plus the first inequality rules out distance at least 18 at parameters $(41, 8)$.

## A.3. MacWilliams identity and the forcing polynomial

For any $y \in \mathbb{F}_2^{44}$, character orthogonality gives

$$\sum_{x \in C} (-1)^{x \cdot y} = \begin{cases} 2^{10}, & y \in C^\perp, \\ 0, & y \notin C^\perp. \end{cases}$$

In the second case, choose $x_0 \in C$ with $x_0 \cdot y = 1$ and pair each $x$ with $x + x_0$. Summing over all $y$ of weight $j$, then interchanging two finite sums, yields

$$2^{10} B_j = \sum_{x \in C} \sum_{\mathrm{wt}(y) = j} (-1)^{x \cdot y} = \sum_{w=0}^{44} A_w K_j(w).$$

For $z = 44 - 2w$, the needed polynomials are

$$K_0(w) = 1, \quad K_2(w) = \frac{z^2 - 44}{2}, \quad K_4(w) = \frac{z^4 - 256z^2 + 5544}{24}.$$

Substitution or direct expansion proves (2). The potential negative intervals of $P(w)$ are $(18, 20)$ and $(24, 26)$, neither of which contains an even integer. Thus $P(w) \geq 0$ at every allowed nonzero weight. Since $A_0 = B_0 = 1$ and $B_2 = 0$,

$$\tfrac{3}{2}\,2^{10}B_4 + \tfrac{403}{2}\,2^{10} \geq 224640, \qquad B_4 \geq \frac{224640 - 206336}{1536} = \frac{143}{12}.$$

This supplies the weight-four dual word without solving a linear program.

### A.4. Full support and the extension normal form

The full-support claim uses the nondegenerate dot product on the message space $\mathbb{F}_2^{10}$. The shortened messages are $U^\perp$, where $U$ is the span of the four tail columns. A remaining column $v$ vanishes on all shortened messages if and only if $v \in (U^\perp)^\perp = U$. Because $\dim U = 3$ and $v_4 = v_1 + v_2 + v_3$, its nonzero vectors are exactly

$$v_1, v_2, v_3, v_4, \quad v_1 + v_2, v_1 + v_3, v_2 + v_3.$$

Each possibility contradicts independence of every three original columns, as explained in Lemma 3.3. The shortening is therefore genuinely in the full-support class covered by E2.

The tail projection has kernel $K$ and image the dimension-three even subspace of $\mathbb{F}_2^4$. Choose lifts of $1001, 0101, 0011$ and prepend a basis for the kernel. This yields (3) by row operations, without restricting the code. For $s \in \mathbb{F}_2^3$ and $c \in K$, every word has the form

$$(c + s_1a_1 + s_2a_2 + s_3a_3,\ s_1(1001) + s_2(0101) + s_3(0011))\,.$$

For $s = 0$ the weight is at least 18 unless the word is zero. For $\mathrm{wt}(s) = 1$ or 2 the tail weight is 2, and for $s = (1, 1, 1)$ it is 4. This proves necessity and sufficiency of (4). Replacing an $a_i$ by a vector in its coset amounts to adding kernel rows, so all conditions depend only on cosets. A coordinate permutation of $K$ extends by the identity on the tail and preserves every condition.

### A.5. Unique even representatives and pair invariance

In systematic form, $(r_i)_{p_j} = \delta_{ij}$. Hence $N_K(x)$ in (5) is zero at every pivot and $N_K(x + r_i) = N_K(x)$. Conversely, $N_K(x) = 0$ implies $x = \sum_i x_{p_i} r_i \in K$. The map induces a bijection between the quotient and its zero-pivot image. Since the rows of $K$ are even, it preserves parity. On the zero-pivot subspace, evenness is the nonzero equation that the 33 free bits sum to zero; its dimension is 32. All coset and pair distances are unchanged under this normalization because $N_K(x) + x \in K$ and the map is linear.

### A.6. Distance normalization and the fifth target

The condition $d \geq 1$ in Lemma 5.2 is essential to its dimension argument. If one punctured all $D$ positions of a minimum word to obtain target zero, that word would enter the kernel. For positive target $d$, only $D - d < D$ positions are removed, so no nonzero word is lost. Zero padding is permitted because our original domain is the full class of binary linear codes.

After parity extension of a hypothetical $[42, 16, \geq 13]$ code, two one-coordinate shortenings give dimension at least 14 and distance at least 14. Selecting a 14-dimensional subspace preserves that distance lower bound. Normalization then produces exact distance 14 at the same length and dimension. This argument discharges the exact-distance hypothesis of E3; no assertion about preserving a chosen minimum word under shortening is needed.

## B. Certificate Semantics and Reproduction

### B.1. Finite checks and completeness

A complete checker for a mother $K$ must verify three independent properties:

1. The supplied matrix defines an even, full-support $[40, 7, 18]$ code and matches the coordinates used by the scan.
2. The list $F_K$ equals the entire set of even cosets at distance at least 16; membership and completeness are separate obligations.

3. Every unordered pair of distinct entries has a message satisfying (6).

The two scans provide the second property with different systematic bases and enumeration orders. The pair checker reads exactly $\binom{|F_K|}{2}$ witnesses in the declared pair order. Its weight histogram, over all mothers, is

| rejection weight | 2 | 4 | 6 | 8 | 10 | 12 | 14 |
|---|---|---|---|---|---|---|---|
| count | 186172 | 922339 | 4503729 | 16924956 | 61595955 | 171053508 | 363867130. |

These counts sum to 619,053,789. A message value outside $0, \ldots, 127$, a missing or trailing record, a wrong matrix binding, or weight at least 16 is a verification failure.

### B.2. What is supplied with this draft

The accompanying data directory supplies the literal mother matrices, complete per-case coverage metadata, historical pair-replay summary, and lower generators. A dependency-free script recomputes all lower spectra, mother parameters, the forcing-polynomial identity at every integer weight, and coverage counts. A separate catalogue check uses graph canonicalization for pairwise inequivalence. The local evidence map identifies the existing full scan outputs and the approximately 1.68 GB of pair-witness streams; these large streams are not embedded in the compact manuscript-source archive. Historical absolute paths in metadata are resolved against the current project root, with original records preserved.

During manuscript preparation, we rebuilt both Lean projects and reran their audits, re-enumerated every lower-bound matrix, rechecked all mother parameters and pairwise inequivalence, compared both saved accepted sets with their coordinate bindings, and replayed all 619,053,789 pair witnesses. All these checks passed. The validation log distinguishes these new checks from the original full-domain scans. Rebuilding the Lean projects or rechecking matrix spectra does not re-execute the $172 \cdot 2^{32}$ coset domains. Replaying all saved pair witnesses likewise does not certify that a saved list is exhaustive. Reproduction commands make these scopes explicit.

## C. Formal Interfaces and Imported Facts

The first project exposes the following theorem. Names are reproduced verbatim; line breaks below are typographical.

```
ECC.mainClaim_of_external_results
  (hE1 : PublishedNonexistence41)
  (hE2 : PublishedClassBound)
  (hDistinct : CatalogueInequivalent)
  (hComputed : forall i : Fin 172, PairIncompatible (catalogueCode i))
  : MainClaim
```

Here `MainClaim` means nonexistence of an actual dimension-ten subspace of $\mathbb{F}_2^{43}$ with every nonzero word of weight at least 17. E1 excludes exact $[41, 8, 18]$; E2 bounds the number of full-support exact $[40, 7, 18]$ classes. The theorem proves the connection from these hypotheses to arbitrary target codes, including the full-support reduction and actual matrix catalogue. No unproved "catalogue reduction" parameter remains in this final interface.

The corollary interface is `ECC.four_table_consequences_of_external_results`. Its conclusion combines the three exact entries for $(43, 10), (44, 10), (44, 11)$ with existence of $[45, 11, \geq 16]$ and nonexistence of $[45, 11, \geq 18]$. Kernel checks of packed matrices use `decide +kernel`. The exhaustive coset scans and graph canonicalization are external to these kernel computations.

The second project exposes

```
ECC42.reduction_42_16_to_41_14
  : CodeExists 42 16 13 -> ExactCodeExists 41 14 14
ECC42.nonexistence_of_proposition2
  : Proposition2 -> not (CodeExists 42 16 13)
```

where `Proposition2` is the published exclusion of exact $[41, 14, 14]$. The imported proposition is an explicit argument, not an axiom declaration. Both developments use Lean 4.34.1; their pinned manifests are included with the corresponding local projects. Audit commands inspect both final theorem types and transitive axioms, since an axiom list alone cannot reveal outstanding theorem parameters.

## D. Source Provenance and AI Attribution

The published inputs are Bouyukliev et al. (2000), Bouyukliev & Jaffe (2001), and Proposition 2 (printed page 179) of Bouyuklieva & Bouyukliev (2020). The archived source assessment for E1 additionally locates Theorem 6.3 in Bouyukliev's doctoral thesis, and for E2 locates Table 6.2. These thesis numbering references are not journal theorem numbers. The 2025 hull paper provides a separate count cross-check. Historical classification internals are not presented as rerun computations.

The provenance records for the AI interventions retain original responses, subsequent actions, and reconciliation notes. The early Gemini profiling suggestion is connected to the native-filter experiment; the Grok completeness request is connected to the second full scan and set comparison. Later reviews are recorded as reviews of already assembled evidence. Model agreement is not included among the hypotheses of either mathematical theorem. The local record permits these specific attributions, but does not support a percentage allocation of the proof to humans or models, or a controlled comparison among systems.

## E. Explicit Lower-Bound Generators

In every list below, integer bit $j$ is coordinate $j$, starting from zero; message bit $i$ selects generator row $i$, and addition is XOR. The row order is the displayed order. Leading zero coordinates are retained up to the declared length. Enumeration of all $2^k - 1$ nonzero messages establishes the listed exact distance; distinct message images establish rank $k$.

### E.1. The $[43, 10, 16]$ witness

```
137539745726, 5740911900901, 3801465813127, 7302904556701,
3853442440940, 2103915382859, 5144838248083, 7496890689917,
7842576845701, 8787570300677
```

The nonzero spectrum $(w : A_w)$ is $16 : 12$, $17 : 101$, $18 : 144$, $19 : 70$, $20 : 61$, $21 : 147$, $22 : 146$, $23 : 36$, $24 : 43$, $25 : 123$, $26 : 92$, $27 : 22$, $28 : 11$, $29 : 13$, $30 : 2$.

### E.2. The $[44, 10, 17]$ witness

```
2860005872641, 5720011745283, 11440023490566, 3732392958991,
673493634067, 1809555608628, 204550108262, 408026474701,
57712634350, 114351526877
```

The nonzero spectrum $(w : A_w)$ is $17 : 72$, $18 : 113$, $19 : 82$, $20 : 101$, $21 : 114$, $22 : 111$, $23 : 84$, $24 : 71$, $25 : 108$, $26 : 87$, $27 : 26$, $28 : 19$, $29 : 26$, $30 : 9$.

### E.3. The $[44, 11, 16]$ witness

```
5178737328131, 10357474656262, 1218204696603, 2435335684150,
944061251695, 515129213098, 225190019387, 134966837980,
47094858883, 898731865, 514986475
```

The nonzero spectrum $(w : A_w)$ is $16 : 371$, $20 : 880$, $24 : 706$, $28 : 88$, $32 : 2$.

The $[45, 11, 16]$ generator uses exactly the $[44, 11, 16]$ integers above, interpreted as 45-bit rows. Coordinate 44 is zero. Its nonzero weight spectrum is unchanged.

### E.4. The $[42, 16, 12]$ witness

```
106065092, 139139103, 285387535, 556556412,
1113112824, 2195975476, 4307321038, 8653155535,
17229284152, 34395582853, 68730626717, 137504614505,
274932175173, 549758586446, 1099560464847, 2199058158699
```

The nonzero spectrum $(w : A_w)$ is $12 : 675$, $16 : 9898$, $20 : 30659$, $24 : 21056$, $28 : 3161$, $32 : 85$, $36 : 1$.

## F. The 172 Actual Mothers and Their Complete Coset Counts

Each row gives the frozen zero-based catalogue index, the seven 40-bit generator rows in hexadecimal (leading zeros omitted), the hull dimension $h$, and $|F_K|$. Each pair graph has zero edges; its checked pair count is $\binom{|F_K|}{2}$. Integer bit conventions are as above. The two scans each cover $2^{32}$ cosets for every row. Hexadecimal notation specifies the full matrices rather than just invariants or equivalence-class names.

*Table 3.* Literal mother generators and computed admissible-coset counts.

| Index | Seven generator rows (hexadecimal) | $h$ | $\lvert F_K\rvert$ |
|---|---|---|---|
| 0 | b73e546820 ee7ca8d040 ddf951a0c1 bbf2a74182 f6e74a8b04 edce951e08 db9f2a3430 | 5 | 668 |
| 1 | 373e54d060 ee7ca9a0c1 5df9514182 bbf2a68300 f6e74b1604 6dce943c08 db9f2a6830 | 3 | 833 |
| 2 | b67ca8d060 6cf951a0c1 dff2a34182 bbe54e8300 75ce951604 ef9d2a3c08 5b3e546830 | 3 | 795 |
| 3 | b77ca8d040 6e7951a0c1 5df2a34182 3be54e8304 76ce951608 6d9d2a3c10 5bbe546820 | 5 | 844 |
| 4 | d3e58d3840 afcf1270c1 d59e2c41c2 ab3c58a384 dc7cb1c708 b2f9630e10 edf2c69c20 | 5 | 819 |
| 5 | 55f2c6b081 abe7892182 d6cf160384 ad9e2c4708 5a3e58ce10 357cb19c20 eaf9637840 | 3 | 1334 |
| 6 | 55f2c6b081 abe7892182 56cf164384 ad9e2c4708 da3e588e10 b57cb1dc20 6af9633840 | 3 | 1355 |
| 7 | dbe51a3081 a7cf246182 dd9e58c384 ab3cb18708 d47c634e10 baf9c69c20 e5f28d3840 | 5 | 867 |
| 8 | 000003ffff 0007fe99aa 0f85382aec 107d92e316 26669b33d8 455723c3e0 84cfc3fc00 | 1 | 2578 |
| 9 | 000003ffff 0007fc7b32 0f853a9a54 107d92b346 26669b2398 455723c3e0 84cfc3fc00 | 5 | 3930 |
| 10 | 000003ffff 0007fe95d2 0f853ba94e 107d930ee8 26669bd08c 455723e0f0 84cfc3ff00 | 5 | 2537 |
| 11 | 000003ffff 0007fd35e8 0f853ab942 107d930eac 26669bd0ce 455723e0f0 84cfc3ff00 | 5 | 2489 |
| 12 | 000003ffff 0007fceb52 0f853ab186 107d921ed8 26669b231c 455723c3e0 84cfc3fc00 | 3 | 1950 |
| 13 | 000003ffff 0007fc7752 0f853b7986 107d922ed8 26669bb31c 455723c3e0 84cfc3fc00 | 3 | 1897 |
| 14 | 000003ffff 0007fec59a 0f853997e2 107d9319b4 26669a1ec8 455723e0f0 84cfc3ff00 | 5 | 4037 |
| 15 | 000003ffff 0007ff256c 0f85395dd8 107d9296e8 26669b188e 455723e0f0 84cfc3ff00 | 1 | 3813 |
| 16 | 000003ffff 0007ff0d36 0f853a7f84 107d9329d8 26669bb21e 455723c3e0 84cfc3fc00 | 5 | 4015 |
| 17 | 000003ffff 0007fd1d72 0f8538ada8 107d932a3c 26669a33d0 455723c3e0 84cfc3fc00 | 5 | 4093 |
| 18 | 000003ffff 0007fea6b2 0f853a6b0a 107d90b78c 26669b3bd0 455723c3e0 84cfc3fc00 | 5 | 2575 |
| 19 | 000003ffff 0007fe6734 0f853b4a1a 107d90b78c 26669b3bd0 455723c3e0 84cfc3fc00 | 5 | 4022 |
| 20 | 000003ffff 0007ff0d3c 0f85399632 107d926b54 26669bb398 455723c3e0 84cfc3fc00 | 5 | 4223 |
| 21 | 000003ffff 0007fd8d96 0f853a8acc 107d931ce8 26669bd00e 455723e0f0 84cfc3ff00 | 3 | 998 |
| 22 | 000003ffff 0007ff852e 0f85399992 107d922dd8 26669b321c 455723c3e0 84cfc3fc00 | 1 | 2036 |
| 23 | 000003ffff 0007ff8956 0f8539ceca 107d9293e8 26669b1c8c 455723e0f0 84cfc3ff00 | 5 | 3943 |
| 24 | 000003ffff 0007fdc696 0f853acdcc 107d9316e8 26669b980e 455723e0f0 84cfc3ff00 | 5 | 2455 |
| 25 | 000003ffff 0007fea52e 0f8538ccca 107d93169a 26669b98ec 455723e0f0 84cfc3ff00 | 5 | 4084 |
| 26 | 000003ffff 0007fea34e 0f853acd88 107d93169a 26669b98ec 455723e0f0 84cfc3ff00 | 5 | 4031 |

| Index | Seven generator rows (hexadecimal), continued | $h$ | $\lvert F_K \rvert$ |
|---|---|---|---|
| 27 | 000003ffff 0007fdc9a6 0f853aea0a 107d9313b8 26669b9ccc 455723e0f0 84cfc3ff00 | 1 | 2505 |
| 28 | 000003ffff 0007fd55e2 0f853b212e 107d9256ac 26669b98c8 455723e0f0 84cfc3ff00 | 5 | 3944 |
| 29 | 000003ffff 0007fe8b74 0f853a31be 107d90daca 26669b1cec 455723e0f0 84cfc3ff00 | 3 | 1371 |
| 30 | 000003ffff 0007ff0dcc 0f853a66da 107d91ab92 26669a331c 455723c3e0 84cfc3fc00 | 5 | 4032 |
| 31 | 000003ffff 0007fdb0ae 0f853ae116 107d93265c 2666983b98 455723c3e0 84cfc3fc00 | 5 | 2554 |
| 32 | 000003ffff 0007ff9136 0f8539455a 107d929a9c 26669b1ce0 455723e0f0 84cfc3ff00 | 5 | 2505 |
| 33 | 000003ffff 0007fe953a 0f853a3bb4 107d90dcc6 26669b1ee8 455723e0f0 84cfc3ff00 | 1 | 2264 |
| 34 | 000003ffff 0007fd53d4 0f853a7542 107d93869c 26669b18e8 455723e0f0 84cfc3ff00 | 1 | 1908 |
| 35 | 000003ffff 0007fcaeb4 0f853ac49a 107d932b2c 26669a33d0 455723c3e0 84cfc3fc00 | 5 | 2519 |
| 36 | 000003ffff 0007fd8f4a 0f85395532 107d929a5c 26669b2398 455723c3e0 84cfc3fc00 | 5 | 3888 |
| 37 | 000003ffff 0007fe8f32 0f8538e58a 107d932a3c 26669a33d0 455723c3e0 84cfc3fc00 | 5 | 2551 |
| 38 | 000003ffff 0007fe8b6a 0f853839b2 107d92d2cc 26669b1cf8 455723e0f0 84cfc3ff00 | 5 | 2502 |
| 39 | 000003ffff 0007fd2dca 0f85385578 107d93989c 26669a1ee0 455723e0f0 84cfc3ff00 | 3 | 971 |
| 40 | 000003ffff 0007fe8b66 0f853a31ac 107d90dae8 26669b1cce 455723e0f0 84cfc3ff00 | 5 | 4062 |
| 41 | 000003ffff 0007fda556 0f853ab18a 107d93a23c 26669b3bd0 455723c3e0 84cfc3fc00 | 5 | 2497 |
| 42 | 000003ffff 0007fcb972 0f853adaa6 107d9293cc 26669b1cf8 455723e0f0 84cfc3ff00 | 3 | 1658 |
| 43 | 000003ffff 0007fd6b86 0f827065ba 107ad1b1d2 2664da391c 455763c1e0 84cf83fe00 | 3 | 1747 |
| 44 | 000003ffff 0007ff846e 0f827313c6 107ad23d4a 2664dbd98c 455763e1f0 84cf83fe00 | 5 | 2537 |
| 45 | 000003ffff 0007ff8a6c 0f827315c6 107ad2394e 2664dbd188 455763e1f0 84cf83fe00 | 5 | 2592 |
| 46 | 000003ffff 0007fdb946 0f8270e2b6 107ad12d3c 2664da31d8 455763c1e0 84cf83fe00 | 5 | 2652 |
| 47 | 000003ffff 0007fd7986 0f827252bc 107ad3132e 2664db9dc8 455763e1f0 84cf83fe00 | 5 | 2498 |
| 48 | 000003ffff 0007fd718e 0f8272f498 107ad3271c 2664dbb9d0 455763c1e0 84cf83fe00 | 5 | 2507 |
| 49 | 000003ffff 0007ffa45a 0f8272f894 107ad33338 2664da3dc0 455763c1e0 84cf83fe00 | 3 | 1353 |
| 50 | 000003ffff 0007fe9a74 0f8272d4ac 107ad3592a 2664db81cc 455763e1f0 84cf83fe00 | 3 | 1741 |
| 51 | 000003ffff 0007fd5d32 0f8273ac54 107ad2e986 2664db3198 455763c1e0 84cf83fe00 | 3 | 1816 |
| 52 | 000003ffff 0007fc9db2 0f82732d54 107ad3a986 2664da31d8 455763c1e0 84cf83fe00 | 5 | 2584 |
| 53 | 000003ffff 0007fd1db2 0f82736d14 107ad27986 2664dbb1d8 455763c1e0 84cf83fe00 | 1 | 1396 |
| 54 | 000003ffff 0007ffa23c 0f8272b954 107ad2f186 2664db3d98 455763c1e0 84cf83fe00 | 5 | 2552 |
| 55 | 000003ffff 0007fe26f4 0f82708d7a 107ad2b54c 2664db3990 455763c1e0 84cf83fe00 | 3 | 1327 |
| 56 | 000003ffff 0007fcb3ca 0f8273b492 107ad324f8 2664da391c 455763c1e0 84cf83fe00 | 3 | 1695 |
| 57 | 000003ffff 0007fd9734 0f827299aa 107ad30dcc 2664dbd00e 455763e1f0 84cf83fe00 | 3 | 1633 |

| Index | Seven generator rows (hexadecimal), continued | $h$ | $\lvert F_K \rvert$ |
|---|---|---|---|
| 58 | 000003ffff 0007ff839c 0f85aad5a6 107c9ad9c4 2666b31ee8 455723e0f0 84cfc3ff00 | 3 | 1686 |
| 59 | 000003ffff 0007fcda36 0f85a9aada 107c99336c 2666b23b90 455723c3e0 84cfc3fc00 | 3 | 1542 |
| 60 | 000003ffff 0007fed236 0f85a9b2da 107c9b236c 2666b23b90 455723c3e0 84cfc3fc00 | 3 | 1706 |
| 61 | 000003ffff 0007fd5a96 0f85aa2aac 107c9bd03a 2666b39ccc 455723e0f0 84cfc3ff00 | 1 | 2280 |
| 62 | 000003ffff 0007fcf326 0f85aaa954 107c9a8a9e 2666b33318 455723c3e0 84cfc3fc00 | 1 | 1082 |
| 63 | 000003ffff 0007fd5b8a 0f85abab1c 107c9b321e 2666b23fd0 455723c3e0 84cfc3fc00 | 1 | 1794 |
| 64 | 000003ffff 0007fd5a96 0f81ab8b2c 107c9ad0da 2666b31cec 455723e0f0 84cfc3ff00 | 5 | 2471 |
| 65 | 000003ffff 0007ff2c5a 0f81ab55a2 107c9998dc 2666b21ee0 455723e0f0 84cfc3ff00 | 5 | 2462 |
| 66 | 000003ffff 0007fe2db2 0f81aa55ca 107c9b9994 2666b31ee8 455723e0f0 84cfc3ff00 | 3 | 2337 |
| 67 | 000003ffff 0007ff852e 0f81a9b4ca 107c9ad98c 2666b31ee8 455723e0f0 84cfc3ff00 | 3 | 2481 |
| 68 | 000003ffff 0007ff1556 0f81a97392 107c9ba61c 2666b23bd8 455723c3e0 84cfc3fc00 | 3 | 2444 |
| 69 | 000003ffff 0007ff256c 0f81a954ba 107c9b99c4 2666b21ef8 455723e0f0 84cfc3ff00 | 5 | 4022 |
| 70 | 000003ffff 0007ff1678 0f81aa639a 107c9bb30c 2666b03bd0 455723c3e0 84cfc3fc00 | 5 | 4054 |
| 71 | 000003ffff 0007ff153c 0f81a97296 107c9ba748 2666b23b90 455723c3e0 84cfc3fc00 | 3 | 2765 |
| 72 | 000003ffff 0007ff499c 0f81a92ad6 107c9bb328 2666b23fd0 455723c3e0 84cfc3fc00 | 5 | 4036 |
| 73 | 000003ffff 0007fd8db4 0f81aab9c2 107c9bd18c 2666b31ee8 455723e0f0 84cfc3ff00 | 3 | 3022 |
| 74 | 000003ffff 0007ff0bb4 0f81a9bac2 107c9bd28c 2666b21ce8 455723e0f0 84cfc3ff00 | 3 | 1957 |
| 75 | 000003ffff 0007ff1674 0f863a67b2 107e38b558 2666d3399c 455763c1e0 84cf83fe00 | 1 | 3260 |
| 76 | 000003ffff 0007fdacc6 0f86283eb4 107e92c9cc 2664e30ee8 455733f0f0 84cfc3ff00 | 1 | 2510 |
| 77 | 000003ffff 0007feaa4e 0f862926ba 107e92d31c 2664e31bd0 455733e3e0 84cfc3fc00 | 5 | 2458 |
| 78 | 000003ffff 0007fd966c 0f86293b46 107e925ab4 2664e3a338 455733c3c0 84cfc3fc00 | 1 | 2211 |
| 79 | 000003ffff 0007ff84ae 0f862aca9a 107e931ad2 2664e3931c 455733e3e0 84cfc3fc00 | 1 | 1674 |
| 80 | 000003ffff 0007fdc58e 0f862b4ec2 107e9256d2 2664e398e4 455733e0f8 84cfc3ff00 | 5 | 2538 |
| 81 | 000003ffff 0007ff8a4e 0f8628b8d6 107e92d296 2664e31ce4 455733e0f8 84cfc3ff00 | 3 | 2061 |
| 82 | 000003ffff 0007fe9a3a 0f8629b686 107e925b54 2664e36398 45573383e0 84cfc3fc00 | 5 | 2498 |
| 83 | 000003ffff 0007fd36ac 0f862b2a9a 107e9272d2 2664e3c31c 45573383e0 84cfc3fc00 | 3 | 2170 |
| 84 | 000003ffff 0007fe5aaa 0f862874f4 107e92ab4a 2664e3338c 455733c3f0 84cfc3fc00 | 1 | 2573 |
| 85 | 000003ffff 0007fe466e 0f874ab53a 107ecb258a 26655239cc 455663c1f0 84cf83fe00 | 5 | 2444 |
| 86 | 000003ffff 0007feb156 0f8748d478 107ecb198c 2665521fd0 455663e1e0 84cf83fe00 | 5 | 3929 |
| 87 | 000003ffff 0007feb586 0f8748d8b2 107ecb1354 2665531d98 455663e1e0 84cf83fe00 | 3 | 2167 |
| 88 | 000003ffff 0007fe665a 0f874b289c 107ecbb11e 2665503de8 455663c1f0 84cf83fe00 | 3 | 1271 |

| Index | Seven generator rows (hexadecimal), continued | $h$ | $\lvert F_K \rvert$ |
|---|---|---|---|
| 89 | 000003ffff 0007feb236 0f874b14aa 107ec9d93c 2665521fd0 455663e1e0 84cf83fe00 | 5 | 2454 |
| 90 | 000003ffff 0007ff645a 0f87492b92 107ec9b11c 2665523de0 455663c1f0 84cf83fe00 | 5 | 2564 |
| 91 | 000003ffff 0007fc567c 0f874aa75a 107ec935a8 26655239cc 455663c1f0 84cf83fe00 | 5 | 2484 |
| 92 | 000003ffff 0007ff146e 0f87492d38 107eca79ca 266553b18c 455663c1f0 84cf83fe00 | 5 | 3958 |
| 93 | 000003ffff 0007ff1674 0f87498cb2 107eca5958 266553919c 455663e1e0 84cf83fe00 | 5 | 3987 |
| 94 | 000003ffff 0007fe167a 0f87492cd8 107ecab96c 266553318e 455663c1f0 84cf83fe00 | 5 | 4047 |
| 95 | 000003ffff 0007fe5666 0f8748d94a 107eca938c 2665531dd0 455663e1e0 84cf83fe00 | 3 | 1380 |
| 96 | 000003ffff 0007fe0eea 0f874aad5c 107ec8e86c 266553318e 455663c1f0 84cf83fe00 | 5 | 4002 |
| 97 | 000003ffff 0007fe36e4 0f86716a6e 107d925cb8 26661b90ce 455723e0f0 84cfc3ff00 | 3 | 3090 |
| 98 | 000003ffff 0007fe87d4 0f8671ca4c 107d93139a 26661a1cec 455723e0f0 84cfc3ff00 | 5 | 4053 |
| 99 | 000003ffff 0007fcbca6 0f8672c98a 107d9391ac 26661b1ec8 455723e0f0 84cfc3ff00 | 5 | 4070 |
| 100 | 000003ffff 0007ff6136 0f8671ab5a 107d912e78 26661a339c 455723c3e0 84cfc3fc00 | 1 | 2586 |
| 101 | 000003ffff 0007fd7272 0f8672e69a 107d93a0dc 26661b3b18 455723c3e0 84cfc3fc00 | 5 | 3978 |
| 102 | 000003ffff 0007fd8bb2 0f86728dc8 107d930e6c 26661bd08e 455723e0f0 84cfc3ff00 | 1 | 1327 |
| 103 | 000003ffff 0007fcaeb4 0f867156d6 107d919a9a 26661a1cec 455723e0f0 84cfc3ff00 | 5 | 2535 |
| 104 | 000003ffff 0007ff4596 0f8671ceaa 107d92963c 26661b18ce 455723e0f0 84cfc3ff00 | 1 | 2614 |
| 105 | 000003ffff 0007ff32a6 0f867159ba 107d919ad8 26661a1cec 455723e0f0 84cfc3ff00 | 5 | 2493 |
| 106 | 000003ffff 0007fda5b2 0f8672a9ce 107d930ed4 26661bb318 455723c3e0 84cfc3fc00 | 1 | 2434 |
| 107 | 000003ffff 0007fe3374 0f85b3546e 107e5398a6 26669a1ec8 455723e0f0 84cfc3ff00 | 5 | 3959 |
| 108 | 000003ffff 0007fe66a6 0f85b0ab2a 107e512f8c 26669a33d0 455723c3e0 84cfc3fc00 | 5 | 4021 |
| 109 | 000003ffff 0007ff4556 0f85b1598a 107e53a23c 26669a33d0 455723c3e0 84cfc3fc00 | 3 | 1673 |
| 110 | 000003ffff 0007fd8db4 0f85b216b8 107e53a30e 26669b3bd0 455723c3e0 84cfc3fc00 | 5 | 4207 |
| 111 | 000003ffff 0007fd3a56 0f85b14d64 107e53918e 26669a1ec8 455723e0f0 84cfc3ff00 | 5 | 3927 |
| 112 | 000003ffff 0007ff312e 0f85b159c8 107e519c9a 26669a1eec 455723e0f0 84cfc3ff00 | 5 | 3957 |
| 113 | 000003ffff 0007fd66d2 0f81aaa35c 107c5af21c 2666b33b98 455723c3e0 84cfc3fc00 | 5 | 4078 |
| 114 | 000003ffff 0007fdb2c6 0f81aaa758 107c5b361c 2666b23b90 455723c3e0 84cfc3fc00 | 3 | 2023 |
| 115 | 000003ffff 0007fea746 0f81ab0ed8 107c5baa94 2666b33318 455723c3e0 84cfc3fc00 | 3 | 913 |
| 116 | 000003ffff 0007fd9a56 0f81abaa98 107c5b331c 2666b23fd0 455723c3e0 84cfc3fc00 | 3 | 1617 |
| 117 | 000003ffff 0007ff9256 0f81aaa2ba 107c593b2c 2666b23fd0 455723c3e0 84cfc3fc00 | 1 | 1999 |
| 118 | 000003ffff 0007ff924e 0f81aaa2ba 107c593734 2666b23bd8 455723c3e0 84cfc3fc00 | 1 | 3010 |
| 119 | 000003ffff 0007fdd156 0f81aaa56c 107c5b568a 2666b3988c 455723e0f0 84cfc3ff00 | 3 | 1684 |

| Index | Seven generator rows (hexadecimal), continued | $h$ | $\lvert F_K \rvert$ |
|---|---|---|---|
| 120 | `000003ffff 0007fda63c 0f81a97386 107c5bab50 2666b23398 455723c3e0 84cfc3fc00` | 3 | 973 |
| 121 | `000003ffff 0007fde30e 0f81ab946a 107c5ae654 2666b33b98 455723c3e0 84cfc3fc00` | 5 | 2531 |
| 122 | `000003ffff 0007fdd896 0f81ab895c 107c5af28a 2666b31cec 455723e0f0 84cfc3ff00` | 3 | 1325 |
| 123 | `000003ffff 0007fe4d78 0f81ab869c 107c5af42a 2666b318cc 455723e0f0 84cfc3ff00` | 3 | 2371 |
| 124 | `000003ffff 0007fe4d5c 0f81aa86ae 107c5b7438 2666b398ce 455723e0f0 84cfc3ff00` | 5 | 3968 |
| 125 | `000003ffff 0007fd94f8 0f8548e762 107ea2b2ac 2665333b30 45563bc3c0 84cfc3fc00` | 5 | 2654 |
| 126 | `000003ffff 0007ff859c 0f854ad8cc 107ea2e88e 2665330ee8 45563bf0f0 84cfc3ff00` | 3 | 1605 |
| 127 | `000003ffff 0007fdc66c 0f854ae4b2 107ea3643a 26653388bc 45563bf0c0 84cfc3ff00` | 3 | 1590 |
| 128 | `000003ffff 0007ff15a6 0f8549555a 107ea2a6ac 2665333b30 45563bc3c0 84cfc3fc00` | 3 | 1990 |
| 129 | `000003ffff 0007fda696 0f854b4cb8 107ea26cac 26653388ce 45563bf0f0 84cfc3ff00` | 5 | 4033 |
| 130 | `000003ffff 0007fcd9d2 0f866a7164 107ba39296 2664f31ce6 455733e0f8 84cfc3ff00` | 5 | 2517 |
| 131 | `000003ffff 0007fe3b52 0f866b4196 107ba3499a 2664f3921c 455733e3e0 84cfc3fc00` | 3 | 1666 |
| 132 | `000003ffff 0007fceb2c 0f866ac156 107ba2ca56 2664f37398 45573383e0 84cfc3fc00` | 3 | 1216 |
| 133 | `000003ffff 0007fd6a36 0f866a469a 107ba256d2 2664f39b1c 455733e3e0 84cfc3fc00` | 3 | 1524 |
| 134 | `000003ffff 0007fe4ec6 0f8668c87a 107ba17392 2664f2631c 45573383e0 84cfc3fc00` | 5 | 3990 |
| 135 | `000003ffff 0007fe26da 0f82f2cb48 107b4a956c 2664d3198e 455763e1f0 84cf83fe00` | 5 | 2557 |
| 136 | `000003ffff 0007feaa6a 0f81f2d2a4 107e8a9cb4 2664b31ec8 455723e0f0 84cfc3ff00` | 5 | 3937 |
| 137 | `000003ffff 0007fdb2a6 0f84d2a794 107e9b3754 26652a3b98 455633c3e0 84cfc3fc00` | 1 | 2003 |
| 138 | `000003ffff 0007fdc65a 0f84d2d2ac 107e9b40ae 26652b9b30 455633e3c0 84cfc3fc00` | 5 | 2546 |
| 139 | `000003ffff 0007fcd6aa 0f868966cc 107eab9886 2664b21cf8 455723e0f0 84cfc3ff00` | 5 | 4089 |
| 140 | `000003ffff 0007fe6aac 0f8688f354 107ea89b98 2664b3231e 455723c3e0 84cfc3fc00` | 5 | 4361 |
| 141 | `000003ffff 0007ff893a 0f8688eb4c 107ea93278 2664b23f90 455723c3e0 84cfc3fc00` | 1 | 2522 |
| 142 | `000003ffff 0007fe6b46 0f868ab29a 107ce8a71c 2660f33b90 455723c3e0 84cfc3fc00` | 3 | 1956 |
| 143 | `000003ffff 0007fe98f4 0f838aa93a 107abb324c 2664b23f90 455723c3e0 84cfc3fc00` | 3 | 1708 |
| 144 | `000003ffff 0007fd6ca6 0f858955d8 107d9999f4 2666921ee8 455723e0f0 84cfc3ff00` | 3 | 1330 |
| 145 | `000003ffff 0007fdc33c 0f858a96b8 107d9b64ae 26669398cc 455723e0f0 84cfc3ff00` | 3 | 1640 |
| 146 | `000003ffff 0007fdb15a 0f858a8bd8 107d9bd29c 2666931ce8 455723e0f0 84cfc3ff00` | 1 | 2931 |
| 147 | `000003ffff 0007ff315a 0f85894bd8 107d9a929c 2666931ce8 455723e0f0 84cfc3ff00` | 1 | 3008 |
| 148 | `000003ffff 0007fd595c 0f8652748e 107cb298d6 26663b1ee8 455723e0f0 84cfc3ff00` | 5 | 2525 |
| 149 | `000003ffff 0007fd366a 0f86523ab4 107cb272d8 26663ba31e 455723c3e0 84cfc3fc00` | 3 | 1762 |
| 150 | `000003ffff 0007fd8ed4 0f83d2a964 10795b2c66 266563b186 455673c1f8 84cf83fe00` | 5 | 3768 |

| Index | Seven generator rows (hexadecimal), continued | $h$ | $\lvert F_K \rvert$ |
|---|---|---|---|
| 151 | 000003ffff 0007fe5d52 0f83e252a6 107d32a55c 26664b3998 455673c1e0 84cf83fe00 | 1 | 2676 |
| 152 | 000003ffff 0007fd9c72 0f83e238b4 107d332cd8 26664bc11e 455673f1e0 84cf83fe00 | 3 | 1281 |
| 153 | 000003ffff 0007ff0736 0f834b4a78 107d325d58 26645b919c 455663e1e0 84cf83fe00 | 3 | 2756 |
| 154 | 000003ffff 0007fe8cbc 0f834a5578 107d33984e 26645b1f90 455663e1e0 84cf83fe00 | 3 | 1702 |
| 155 | 000003ffff 0007fd956c 0f864966e2 107c729b34 2664ab23b8 455733c3c0 84cfc3fc00 | 1 | 1718 |
| 156 | 000003ffff 0007ff263c 0f86496ae8 107c714b56 2664aa7398 45573383e0 84cfc3fc00 | 3 | 2332 |
| 157 | 000003ffff 0007ff898e 0f8648dab8 107c7292d6 2664ab1ce4 455733e0f8 84cfc3ff00 | 3 | 2189 |
| 158 | 000003ffff 0007ff2672 0f864aab58 107c72b25c 2664ab3ba0 455733c3c0 84cfc3fc00 | 1 | 1943 |
| 159 | 000003ffff 0007fe3a3a 0f8708f362 107db0d34a 2661e3638c 45563383f0 84cfc3fc00 | 5 | 2566 |
| 160 | 000003ffff 0007ff8a56 0f851929ba 107c72d2cc 26669b1ce0 455723e0f0 84cfc3ff00 | 3 | 1673 |
| 161 | 000003ffff 0007ff2a56 0f869956da 107ce2996c 26654b1db0 455673e1c0 84cf83fe00 | 1 | 2936 |
| 162 | 000003ffff 0007ff8656 0f8699379a 107ce2d91c 26654b1de0 455673e1f0 84cf83fe00 | 1 | 2399 |
| 163 | 000003ffff 0007fe387c 0fe388ce96 1719c2d32a 2692f363cc 446ce383f0 85df03fc00 | 3 | 979 |
| 164 | 000003ffff 0007fec74a 0fe30aace6 171ba32554 2691d3c998 446de3f1e0 85de03fe00 | 3 | 983 |
| 165 | 03e47b9cd1 306f897d92 567864bf14 1b53bf2a18 ecc2fcb860 0d9a86f990 ead5d68f90 | 5 | 2570 |
| 166 | 000003ffff 0007fd529e 0ff329a73a 178d33322c 266d5a3bd0 474663c3e0 84df83fc00 | 1 | 2700 |
| 167 | 000003ffff 0007fe4e5a 0ff32aa866 178d33328c 266d5a3cf0 474663c0f8 84df83ff00 | 1 | 1981 |
| 168 | 000003ffff 0007fc5ea6 0ff32b2b5a 178d31b30c 266d5a3f90 474663c3e0 84df83fc00 | 1 | 3588 |
| 169 | 000003ffff 0007fcd752 0ff211c26a 178c62974c 266ea31bf0 455f3be380 84b7c3fc00 | 3 | 546 |
| 170 | 00003fffff 07ff866914 0bf04bae5a 138e730c6c 226d63cfb0 415b7c0fc0 80dcfff000 | 3 | 2514 |
| 171 | ff00ff0f0f ffff000ff0 fffffff000 c5653ac566 69c9acc6aa 8e8eccaaa3 f0f0f0cccc | 3 | 3785 |