Optimality of the added-vector code in the 19-dimensional kissing construction

Alexey Mikhailovich Kolosov[1,2]

[1]Department of Mathematical Theory of Intelligent Systems,
Faculty of Mechanics and Mathematics,
Lomonosov Moscow State University, Moscow, Russia

[2]Laboratory of Knowledge Engineering,
Institute for Mathematical Research of Complex Systems,
Lomonosov Moscow State University, Moscow, Russia

6 September 2026

Abstract

Let $D \subseteq \mathbb{F}_2^{19}$ be the five-punctured extended binary Golay code used in Ho's improvement of the Cohn–Li kissing construction. We prove that every subset of D with minimum Hamming distance at least 5 has at most 1280 words. Together with Ho's construction, this determines the exact maximum and proves Conjecture 16 of Gonzalez, version 3. The upper bound has a sixteen-word certificate: five explicitly listed weight-four words span a four-dimensional subspace H whose induced forbidden-distance graph is the Clebsch graph. Each coset of H contains at most five words of an admissible code, so the 256 cosets in D give the bound 1280. The corresponding 1024-vertex component has independence number 320. The certificate was identified through a linear programming relaxation, but the proof is elementary and does not rely on numerical optimization. The result concerns the fixed added-vector scheme, not the unrestricted kissing number in dimension 19.

1 Introduction and main result

In dimension 19, the construction of Cohn and Li [1, Section 2] starts with 10668 fixed vectors and adds vectors indexed by a binary code in an ambient linear code D. The required minimum Hamming distance is 5. Ho [2, Proposition 9] constructed an admissible subset of D of size 1280, giving a kissing configuration of size 11948. Gonzalez [3, Theorem 15 and Conjecture 16] obtained the bounds $1280 \leq \max |A| \leq 1536$ for this added-vector problem and conjectured that the lower bound is sharp. We prove that conjecture.

Write $d_H(x, y) = \mathrm{wt}(x + y)$ for binary Hamming distance. For a finite binary linear code L, let

$$\alpha_5(L) = \max\{|A| : A \subseteq L, \quad d_H(x, y) \geq 5 \text{ for all distinct } x, y \in A\}.$$

Such subsets will be called admissible; they need not be linear. Define

$$S = \{s \in D : 0 < \mathrm{wt}(s) < 5\}, \qquad K = \mathrm{span}(S).$$

We use the explicit coordinate model of D in Appendix A. It has $\dim D = 12$ and $\dim K = 10$; its forbidden set S consists of one word of weight 3 and twenty words of weight 4 [2, Propositions 2 and 5].

Theorem 1. *For these codes,*

$$\alpha_5(D) = 1280, \qquad \alpha_5(K) = 320.$$

Equivalently, $\alpha(\mathrm{Cay}(D, S)) = 1280$ *and* $\alpha(\mathrm{Cay}(K, S)) = 320$.

Here $\mathrm{Cay}(L, S)$ has vertex set L and an edge between distinct x, y when $x + y \in S$. Thus its independent sets are exactly the admissible subsets of L. Our K is the code denoted H_{19} by Gonzalez; our certificate subspace H below is a different, smaller space. The coordinate identification is harmless: any two five-punctured extended binary Golay codes are equivalent under a coordinate permutation [2, Remark 4].

2 A sixteen-word certificate

We identify each binary vector with its support, so addition means symmetric difference. Consider the following five words:

$$\begin{aligned} &h_1 = \{1, 4, 7, 9\}, && h_2 = \{4, 8, 10, 12\}, \\ &h_3 = \{7, 8, 13, 18\}, && h_4 = \{1, 10, 13, 19\}, \\ &h_5 = \{9, 12, 18, 19\}. \end{aligned} \tag{1}$$

Each lies in D and has weight 4. Explicit expressions in the chosen generators are given in (5), so their membership can be checked without enumerating D. Put

$$T = \{h_1, h_2, h_3, h_4, h_5\}, \qquad H = \mathrm{span}\{h_1, h_2, h_3, h_4\}.$$

Since $T \subseteq S$, we have $H \le K \le D$.

Lemma 2. *The space H has 16 elements, and*

$$H = \{0\} \,\dot\cup\, T \,\dot\cup\, \{h_i + h_j : 1 \le i < j \le 5\}.$$

The three parts have weights 0, 4, and 6, respectively. In particular, $S \cap H = T$.

Proof. In (1), every coordinate occurs an even number of times, so $h_1 + h_2 + h_3 + h_4 + h_5 = 0$. Restricting the first four words to coordinates $9, 12, 18, 19$ gives the four standard basis vectors. Therefore $\dim H = 4$ and $|H| = 16$.

The relation among the five words allows any sum of them to be replaced by a sum of at most two: replace a set of at least three summands by its complementary set. This gives at most $1+5+10 = 16$ representations. Since $|H| = 16$, all these representations are distinct and exhaust H. Any two distinct supports in (1) meet in exactly one coordinate. Consequently

$$\mathrm{wt}(h_i + h_j) = 4 + 4 - 2 = 6 \qquad (i \neq j).$$

This proves the assertions about weights and forbidden differences. $\square$

Let e_1, e_2, e_3, e_4 be the standard basis of $\mathbb{F}_2^4$, and write

$$\Sigma = \{e_1, e_2, e_3, e_4, e_1 + e_2 + e_3 + e_4\}.$$

The isomorphism $e_i \mapsto h_i$ identifies the induced graph on H with $\mathcal{C} = \mathrm{Cay}(\mathbb{F}_2^4, \Sigma)$, the Clebsch graph. We give a direct proof of the only property of this graph that is needed.

Lemma 3. *The graph $\mathcal{C}$ has independence number* 5.

Proof. The set Σ is independent, since the sum of two distinct elements has weight 2 or 3. Thus $\alpha(\mathcal{C}) \geq 5$.

Translate a nonempty independent set to contain 0. Its other words have weights 2 or 3. Let r count its two-element supports. These supports intersect pairwise, since disjoint pairs sum to $(1,1,1,1)$. Hence $r \leq 3$: after choosing $\{1,2\}$ and $\{1,3\}$, the only possible further pairs are $\{1,4\}$ and $\{2,3\}$, which are disjoint.

A selected triple cannot contain a selected pair, since their sum would be a standard basis vector. If $r = 0$, at most four triples remain. If $r = 1$, the selected pair forbids two of the four triples. If $r \geq 2$, two intersecting pairs together forbid three triples. Including 0, the respective bounds are $1 + 4$, $1 + 1 + 2$, and $1 + 3 + 1$, all at most 5. $\square$

3 The coset bound and optimality

Lemma 4. *Let L be a finite binary linear code and let $H \leq L$. If every admissible subset of H has at most a elements, then*

$$\alpha_5(L) \leq \frac{|L|}{|H|}\, a.$$

Proof. The cosets of H partition L. Translation by a representative of any coset preserves Hamming distance and maps that coset to H. Thus an admissible subset contains at most a words in each coset. Summing over the $|L|/|H|$ cosets proves the inequality. $\square$

Proof of Theorem 1. Lemmas 2 and 3 give $\alpha_5(H) = 5$. Lemma 4, first with $L = D$ and then with $L = K$, yields

$$\alpha_5(D) \leq \frac{4096}{16} \cdot 5 = 1280, \qquad \alpha_5(K) \leq \frac{1024}{16} \cdot 5 = 320.$$

The matching subsets of sizes 1280 and 320 are the sets A_0 and B_0 in Ho's construction [2, Proposition 9]; their formulas are recalled in Appendix A. This proves both equalities. $\square$

Corollary 5. *Every admissible subset of D of size* 1280 *meets every coset of H in exactly five words. The analogous assertion holds for a* 320*-word subset of K.*

Proof. Each coset contributes at most five words, and equality holds in the sum of these bounds. $\square$

Remark 6. The small induced graph used here should not be confused with a quotient graph. In the notation of Appendix A, (5) shows that $h_i + M = s_i + M$ for $1 \leq i \leq 4$. Thus $K = M \oplus H$. Ho's lower bound lifts an independent set from the quotient K/M [2, Sections 3–4]. A quotient construction alone does not upper-bound arbitrary subsets that are not unions of M-cosets. The induced Clebsch graph on H, by contrast, gives a bound on every H-coset and hence on every admissible subset.

The theorem fixes the maximum number of added words in this scheme. It does not provide an upper bound on the unrestricted kissing number $k(19)$, nor does it rule out larger configurations obtained by changing the fixed vectors or using other types of additional vectors.

4 Optimization-guided discovery and verification

We briefly record how the certificate can be found. Let $n = |K| = 1024$ and let $\widehat{K}$ be the set of characters $\chi : K \to \{\pm 1\}$. Denote the trivial character by $\mathbf{1}$. Consider the linear program

$$\begin{aligned} \text{maximize} \quad & np_{\mathbf{1}} \\ \text{subject to} \quad & p_\chi \geq 0 \quad (\chi \in \widehat{K}), \\ & \sum_{\chi \in \widehat{K}} p_\chi = 1, \\ & \sum_{\chi \in \widehat{K}} p_\chi \chi(s) = 0 \quad (s \in S). \end{aligned} \tag{2}$$

This is the translation-invariant Fourier form of the Lovász theta relaxation [4]. Its upper-bound property can also be verified directly. For a nonempty independent set $B \subseteq K$, set

$$p_\chi = \frac{1}{n|B|} \left(\sum_{x \in B} \chi(x) \right)^2 .$$

Character orthogonality gives feasibility in (2); more explicitly, its moment at s is $|B|^{-1} \#\{(x, y) \in B^2 : x + y = s\}$. Moreover $np_{\mathbf{1}} = |B|$.

A numerical run returned the value 384 and a dual solution supported on the five differences in (1). Its relevant part has the following exact form:

$$q(\chi) = 384 + 128 \sum_{i=1}^{5} \chi(h_i) \;\; \geq \;\; 1024\, \mathbf{1}_{\{\chi = \mathbf{1}\}} \qquad (\chi \in \widehat{K}). \tag{3}$$

Indeed, $\prod_{i=1}^{5} \chi(h_i) = 1$, so the sum of these five signs is 5, 1, or -3. Thus $q(\chi)$ is 1024, 512, or 0, and $q(\mathbf{1}) = 1024$. Multiplying (3) by p_χ and summing proves the relaxation bound $np_{\mathbf{1}} \leq 384$.

The value 384 is not the desired independence bound 320. The useful output of the optimization is instead the small support T: its span is the space H above. The exact local bound $\alpha_5(H) = 5$ then supplies the stronger coset inequalities. No floating-point output is used as a certificate for Theorem 1.

The ancillary file `verify_golay_1280_optimality.py` checks the code dimensions, the five membership identities, the weights in H, the independence number of its sixteen-vertex graph, and both matching lower-bound constructions. Its default mode uses only the Python standard library and exact integer arithmetic. The optional flag `--discover` repeats the numerical search using NumPy and SciPy. Different optimal dual solutions may be returned by different solvers; the fixed certificate is verified independently of that choice.

A Coordinate data and the matching construction

For reproducibility, we use the generators from Ho's coordinate model [2, Section 2]. Their supports are listed below.

Generator	Support
m_1	$\{1, 8, 9, 12, 16, 17, 18, 19\}$
m_2	$\{2, 10, 11, 14, 15, 17, 18\}$
m_3	$\{3, 7, 9, 13, 15, 16, 17, 19\}$
m_4	$\{4, 7, 8, 10, 12, 15, 16, 19\}$
m_5	$\{5, 10, 12, 13, 15, 16, 17, 18\}$
m_6	$\{6, 7, 8, 9, 10, 13, 16, 18\}$
s_1	$\{1, 4, 7, 9\}$
s_2	$\{1, 5, 6, 18\}$
s_3	$\{1, 3, 12, 15\}$
s_4	$\{1, 10, 13, 19\}$
r_1	$\{1, 3, 5, 6, 7, 13, 14, 15, 18\}$
r_2	$\{2, 4, 6, 7, 8, 13, 14, 16, 17, 18\}$

Define

$$\begin{aligned} M &= \operatorname{span}\{m_1, \ldots, m_6\}, \\ K &= \operatorname{span}\{m_1, \ldots, m_6, s_1, s_2, s_3, s_4\}, \\ D &= \operatorname{span}\{m_1, \ldots, m_6, s_1, s_2, s_3, s_4, r_1, r_2\}. \end{aligned} \tag{4}$$

The twelve rows are linearly independent: their restriction to the first twelve coordinates is nonsingular over $\mathbb{F}_2$. In particular, $|M| = 64$, $|K| = 1024$, and $|D| = 4096$. The identification of K in (4) with $\operatorname{span}(S)$ is Ho's Proposition 5. The upper bound for D requires only the displayed generators and the identities below, not a complete list of S.

Direct addition of supports gives

$$\begin{aligned} h_1 &= s_1, \\ h_2 &= m_1 + m_4 + m_5 + m_6 + s_2, \\ h_3 &= m_1 + m_3 + s_3, \\ h_4 &= s_4, \\ h_5 &= m_3 + m_4 + m_5 + m_6 + s_1 + s_2 + s_3 + s_4. \end{aligned} \tag{5}$$

These identities are an explicit membership certificate for all five words used in the upper bound.

For completeness, the matching construction of Ho is

$$\begin{aligned} s_5 &= \{3, 5, 7, 10\}, \\ B_0 &= \bigcup_{i=1}^{5} (s_i + M), \\ A_0 &= B_0 \cup (B_0 + r_1) \cup (B_0 + r_2) \cup (B_0 + r_1 + r_2). \end{aligned} \tag{6}$$

Ho's Proposition 9 establishes $B_0 \subseteq K$, $A_0 \subseteq D$, $|B_0| = 320$, $|A_0| = 1280$, and minimum distance at least 5 for both sets. The ancillary program also checks these statements directly. These lower-bound constructions are prior work; the contribution of this note is the matching upper bound.

Use of artificial intelligence

ChatGPT (OpenAI) was used for literature search, the optimization-based search for the five-word certificate, development and checking of the proof, preparation of the verification program, and drafting and translation of the manuscript. The mathematical argument and the exact verification data are given explicitly; a language-model output or a numerical solver status is not used as a substitute for proof.

References

[1] H. Cohn and A. Li, *Improved kissing numbers in seventeen through twenty-one dimensions*, arXiv:2411.04916, version 3, 1 September 2026. `https://arxiv.org/abs/2411.04916v3`.

[2] B. S. Ho, *A new lower bound for the kissing number in 19 dimensions*, arXiv:2603.10425, version 2, 20 March 2026. `https://arxiv.org/abs/2603.10425v2`.

[3] V. Gonzalez, *Maximality of the added-vector codes in the Cohn–Li kissing constructions*, preprint, version 3, 2026, Section 7, Conjecture 16. `https://f-keys.com/papers/maximality-added-vector-codes-cohn-li/`. Version consulted on 6 September 2026.

[4] L. Lovász, *On the Shannon capacity of a graph*, IEEE Transactions on Information Theory **25** (1979), no. 1, 1–7. doi:10.1109/TIT.1979.1055985.