Kissing Number of Codes: A Survey

Yi Liu, Wei Cheng, Olivier Rioul, Sylvain Guilley, and Patrick Solé

Abstract
The kissing number of a code is the average number of pairs of codewords at minimum distance from each other. It has fundamental applications in determining codes performances. Besides, a recent interest has arisen from the field of side-channel analysis of algorithms handling sensitive information (e.g., cryptographic keys). Namely, when code-base masking protections are applied, their performance in terms of attacker's signal-to-noise ratio or mutual information is proportional to the kissing number of the masking code. Therefore the kissing number is also a security metric for a given minimum distance in side-channel protected implementation, as it is in codes performance evaluation. It is known exactly for some classical families of codes. To estimate it in general, two types of bounds are given. Linear programming, either numerically or by the polynomial method is the most versatile and the more precise. Spectral graph theory provides bounds on the multiplicity of the subdominant eigenvalue that are easier to state.

Key words: Codes, kissing number, weight distribution, code performance, code-based masking, side-channel analysis, linear programming, spectral graph theory.

Yi Liu, Wei Cheng and Olivier Rioul
LTCI, Télécom Paris, Institut Polytechnique de Paris, 91120, Palaiseau, France. e-mail: yi.liu@telecom-paris.fr, wei.cheng@telecom-paris.fr, olivier.rioul@telecom-paris.fr

Sylvain Guilley
Secure-IC S.A.S., 104 boulevard du Montparnasse (7th floor), 75014, Paris, France. e-mail: sylvain.guilley@secure-ic.com

Patrick Solé
I2M (Aix-Marseille Univ., CNRS), 13009, Marseille, France. e-mail: patrick.sole@telecom-paris.fr

Contents

1 Introduction

The kissing number of a code is the average number of pairs of codewords at minimum distance from each other. Thus for a linear code it equals the number of codewords of minimum nonzero weight. The terminology is adapted from lattices and sphere packings [11] where it is inspired by the snooker game. It occurs naturally in a number of estimates of probability of error events in error detection and correction. More recently it appeared in assessing the security of so-called code-based masking as a measure of resilience to side-channel attacks [6, 8].

In general, estimating the kissing number is a difficult problem. It is known exactly but for a handful of cases: low order BCH (Bose-Chaudhuri-Hocquenghem) codes, RM (Reed-Muller) codes, MDS (Maximum Distance Separable) codes and some low genera geometric codes. To derive upper and lower bounds as functions of the length, minimum distance and dimension, linear programming techniques [25] can be used, where the variables are the weight frequencies, and constraints are based on the Delsarte-MacWilliams inequalities [12]. This kind of technique has been used in the past to derive bounds on frequencies for the whole weight spectrum [1]. It can be used numerically or through the polynomial method which is less precise, but gives simple formulas. Another approach that gives closed form bounds is the connection with spectral graph theory via the coset graph of the dual code [9].

This survey is organized as follows. Section 2 contains the motivation from coding theory and side-channel security. Section 3 is a census of exact results for classical families of codes. Section 4 is an exposition of the Linear Programming (LP) bounds. Section 5 gives some bounds from spectral graph theory. Conclusions and perspectives are in Section 6.

2 Motivations

The kissing number is fundamental in approximating the performance of coded systems for large signal-to-noise ratios. For the sake of the presentation we make the following definitions.

2.1 Definitions

Definition 1 **((n, M) Code)** A (n, M) *code* is any finite set of M equiprobable distinct points $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_M$ in an n-dimensional metric space equipped with a distance denoted by $d(\cdot, \cdot)$.

Codewords are assumed of equal probability $p(\mathbf{x}_i) = \frac{1}{M}$. The minimum distance of a code is

$$d_{\min} = \min_{i \neq j} d(\mathbf{x}_i, \mathbf{x}_j). \tag{1}$$

Definition 2 (Kissing Number) Let $A_d(\mathbf{x})$ be the number of codewords located at distance d from a given codeword $\mathbf{x}$, and

$$A_d = \frac{1}{M} \sum_{i=1}^{M} A_d(\mathbf{x}_i) \tag{2}$$

be the average number of codewords located at distance d from one another. The *kissing number* of a code is $A_{d_{\min}}$, the average number of codewords located at minimum distance from one another.

When the code is distance-invariant (e.g., linear) then $A_d = A_d(\mathbf{x}_i)$ for every i and $A_{d_{\min}}$ is a whole integer.

For simplicity we restrict ourselves in the sequel of this section to *binary codes*: A *binary code* is such that every component $x_{i,j}$ in $\mathbf{x}_i = (x_{i1}, \ldots, x_{in})$ can only take two values. There are two cases that are most often considered for coded systems:

1. the Euclidean space $\mathbb{R}^n$ with Euclidean distance $d_E(\mathbf{x}, \mathbf{y}) = \sqrt{\sum_{j=1}^n (x_j - y_j)^2}$, where each codeword component $x_{i,j}$ take values in $\{\pm\sqrt{E}\}$ where E is the *energy per bit*.
2. the Hamming space with Hamming distance $d_H(\mathbf{x}, \mathbf{y}) = \big|\{j \mid x_j \neq y_j\}\big|$ where $x_{i,j} \in \{0, 1\} = \mathbb{F}_2$.

With the identification $0 \leftrightarrow -\sqrt{E}$ and $1 \leftrightarrow +\sqrt{E}$, the two distances are linked by the relation

$$d_E^2(\mathbf{x}, \mathbf{x}') = 4E\, d_H(\mathbf{x}, \mathbf{x}') \tag{3}$$

for any two codewords $\mathbf{x}$, $\mathbf{x}'$. The Euclidean and Hamming kissing numbers $A_{d_{\min}}$ coincide in this case. Thus in the rest of the paper, we omit to specify the particular distance used.

The binary code is used over a noisy memoryless symmetric channel (input $\mathbf{x}$, output $\mathbf{y}$) defined by its transition probabilities $p(\mathbf{y}|\mathbf{x})$. Decoding is performed on the received noisy codeword $\mathbf{y}$ in order to recover the correct emitted codeword $\mathbf{x}$.

1. The Additive White Gaussian Noise (AWGN) channel has input and output in the Euclidean space $\mathbb{R}^n$ with

$$p(\mathbf{y}|\mathbf{x}) = \frac{1}{\sqrt{\pi N_0}^n} \exp\bigl(-\frac{d_E^2(\mathbf{x}, \mathbf{y})}{N_0}\bigr), \tag{4}$$

   where N_0 denotes the noise power per unit frequency and E/N_0 is the Signal-to-Noise Ratio (SNR). This channel is symmetric because $p(-\mathbf{y}| - \mathbf{x}) = p(\mathbf{y}|\mathbf{x})$.
   Soft decoding occurs on the AWGN channel when decoding is done directly on the noisy codeword $\mathbf{y}$.
2. The Binary Symmetric Channel (BSC) has input and output in the Hamming space with

$$p(\mathbf{y}|\mathbf{x}) = p^{d_H(\mathbf{x}, \mathbf{y})}(1 - p)^{n - d_H(\mathbf{x}, \mathbf{y})}, \tag{5}$$

   where $p < 1/2$ is the channel's bit error probability. The channel is symmetric because for each transmitted bit, $p(0|0) = p(1|1)$ and $p(0|1) = p(1|0)$.
   Hard decoding occurs on the AWGN channel when bitwise detection is performed prior to decoding. In this case the resulting $\mathbf{y}$ is the output of a BSC with parameter

$$p = Q(\sqrt{2E/N_0}), \tag{6}$$

where the Q-function

$$Q(x) = \frac{1}{2}\mathrm{erfc}(x/\sqrt{2}) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} \exp(-\frac{t^2}{2})\,\mathrm{d}t \tag{7}$$

is the tail distribution function of the standard normal distribution. In this case, the *large* SNR hypothesis amounts to considering *small* values of p.

2.2 Probability of Decoding Error

Having received the noisy $\mathbf{y}$, the decoder aims at finding the codeword $\hat{\mathbf{x}}$ that minimizes the word error probability $\mathbb{P}_e = \mathbb{P}(\hat{\mathbf{x}} \neq \mathbf{x})$. This yields the Maximum A Posteriori (MAP) rule

$$\hat{\mathbf{x}} = \arg\max_{\mathbf{x}} p(\mathbf{x}|\mathbf{y}) \tag{8}$$

which, since we assumed equiprobable codewords, is equivalent to maximizing the likelihood:

$$\hat{\mathbf{x}} = \arg\max_{\mathbf{x}} p(\mathbf{y}|\mathbf{x}). \tag{9}$$

From (4) and (5) this gives

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} d(\mathbf{x},\mathbf{y}), \tag{10}$$

where d denotes Euclidean distance for soft decoding and Hamming distance for hard decoding. The performance of a coded system can then be measured by the resulting minimum probability of error:

$$\mathbb{P}_e = \frac{1}{M}\sum_i \mathbb{P}_{e|\mathbf{x}_i} \tag{11}$$

where $\mathbb{P}_{e|\mathbf{x}}$ denotes the probability of decoding error when codeword $\mathbf{x}$ has been transmitted. For linear codes we simply have $\mathbb{P}_e = \mathbb{P}_{e|\mathbf{x}} = \mathbb{P}_{e|\mathbf{0}}$ where $\mathbf{0}$ denotes the zero codeword.

In order to obtain a tight closed form expression (upper bound) for the probability of error for large SNR, one usually applies the *union bound* [28, (2.3.4)][3, (4.50) and (10.71)]:

$$\mathbb{P}_{e|\mathbf{x}_i} \leq \sum_{j\neq i} \mathbb{P}_{\mathbf{x}_i\to\mathbf{x}_j} \tag{12}$$

where $\mathbb{P}_{\mathbf{x}_i\to\mathbf{x}_j}$ denotes the *pairwise error probability* of decoding $\mathbf{x}_j$ rather than $\mathbf{x}_i$ as if they were the only two codewords, that is, the probability that $d(\mathbf{x}_j,\mathbf{y}) \leq d(\mathbf{x}_i,\mathbf{y})$ given that $\mathbf{x}_i$ was transmitted.

The pairwise error probability is computed as

$$\mathbb{P}_{\mathbf{x}_i\to\mathbf{x}_j} = Q\left(\frac{d_E(\mathbf{x}_i,\mathbf{x}_j)}{\sqrt{2N_0}}\right) \tag{13}$$

for soft decoding (AWGN) and

$$\mathbb{P}_{\mathbf{x}_i \to \mathbf{x}_j} = \sum_{k \geq d_H(\mathbf{x}_i,\mathbf{x}_j)/2} \binom{d_H(\mathbf{x}_i,\mathbf{x}_j)}{k} p^k (1-p)^{d_H(\mathbf{x}_i,\mathbf{x}_j)-k} \tag{14}$$

for hard decoding (BSC). Note that the Q-function in (13) is the tail of a Gaussian distribution, whereas (14) is the tail of a binomial distribution.

Yet other simpler upper bounds are obtained using the *Bhattacharyya bound* [28, (2.3.15)] and [3, (10.75)]:

$$\mathbb{P}_{\mathbf{x}_i \to \mathbf{x}_j} \leq \sum\!\!\!\!\!\!\int_{\mathbf{y}} \sqrt{p(\mathbf{y}|\mathbf{x}_i)p(\mathbf{y}|\mathbf{x}_i')}, \tag{15}$$

where the summation is over the entire space (continuous summation in the Euclidean case, discrete summation in the Hamming case). There exists a generalization known as the *Chernov bound* which cannot improve the Bhattacharyya bound for symmetric channels.

This bound writes

$$\mathbb{P}_{\mathbf{x}_i \to \mathbf{x}_j} \leq \exp\Big(-\frac{d_E^2(\mathbf{x}_i,\mathbf{x}_j)}{4N_0}\Big) \tag{16}$$

for soft decoding (AWGN) [28, (2.3.17)], [3, (4.53)] and

$$\mathbb{P}_{\mathbf{x}_i \to \mathbf{x}_j} = \sqrt{4p(1-p)}^{\,d_H(\mathbf{x}_i,\mathbf{x}_j)} \tag{17}$$

for hard decoding (BSC) [28, (3.10.8)], [3, (10.76)]. From (3) it follows that both expressions simply reduce to

$$\mathbb{P}_{\mathbf{x}_i \to \mathbf{x}_j} \leq \zeta^{d_H(\mathbf{x}_i,\mathbf{x}_j)}, \tag{18}$$

where $0 < \zeta < 1$ is defined by

$$\zeta = \begin{cases} e^{-E/N_0} & \text{(soft decoding)} \\ \sqrt{4p(1-p)}. & \text{(hard decoding)} \end{cases} \tag{19}$$

The high SNR hypothesis reduces to the assumption that ζ is small. Putting this together with (12) and (2) gives [28, (3.10.15)], [3, (10.78), (10.88)]

$$\mathbb{P}_e \leq \sum_{d=d_{\min}}^{n} A_d \zeta^d, \tag{20}$$

where the right-hand side is dominated by the first term for high SNR:

$$\boxed{\mathbb{P}_e \lesssim A_{d_{\min}} \zeta^{d_{\min}}.} \tag{21}$$

This shows that maximizing the coding performance amounts to (i) maximizing minimum distance and then (ii) minimizing the kissing number. For a given minimum distance, it is the kissing number that matters the most.

2.3 Probability of Undetected Error

The kissing number matters not only for error correction, but also for error detection: When using a code on a q-ary symmetric channel with probability of transition p in a Automatic Repeat reQuest (ARQ) scheme, one easily obtains [3, (10.62)]

$$\mathbb{P}_e = \sum_{d=d_{\min}}^{n} A_d p^d (1-(q-1)p)^{n-d}, \tag{22}$$

where again the right-hand side is dominated by the first term for high SNR:

$$\mathbb{P}_e \simeq A_{d_{\min}} p^{d_{\min}}. \tag{23}$$

2.4 Information Leakage in Code-Based Masking

Randomly masking the implementation of cryptographic algorithms is a method to provably reduce their side-channel leakage. Initially applied at bit-level [18], random masking schemes extended their scope to word-level description of algorithms [23]. A general class of random masking techniques is the so-called *code-based masking schemes* [29]. A recent application of the kissing number lies in quantifying side-channel leakage of cryptographic implementations protected by these code-based masking schemes. Assume that in code-based masking, the information X and the random masks Y are encoded into: $Z = X\mathbf{G} + Y\mathbf{H}$, where $\mathbf{G}$ and $\mathbf{H}$ are generator matrices of two linear codes C and D, respectively. In order to allow for unmasking, codes C and D must not overlap, i.e., $C \cap D = \{0\}$. In [6], it is shown that the Signal-to-Noise Ratio (SNR) of a side-channel attack against a code-based masking scheme under Hamming weight leakage with AWGN is equal to:

$$SNR = \frac{A_{d_D^\perp}}{\sigma^2} \left(\frac{d_D^\perp !}{2^{d_D^\perp}} \right)^2, \tag{24}$$

where σ^2 is the noise variance and $d_D^\perp$ is the dual distance of D. Essentially, (24) is applicable for the code-based masking where the two codes C and D are complementary, e.g., in Inner Product Masking (IPM). Thus the kissing number of $D^\perp$ plays a critical role as a metric of code-based masking efficient.

More generally, in [8], the above result on SNR is further extended for the code-based masking where C and D are not complementary anymore (but still, condition

$C \cap D = \{0\}$ must hold), e.g., in Shamir's Secret Sharing (SSS) based masking scheme. Accordingly, (24) is generalized as:

$$SNR = \frac{A'_{d_D^\perp}}{\sigma^2}\left(\frac{d_D^\perp!}{2^{d_D^\perp}}\right)^2. \tag{25}$$

where $A'_{d_D^\perp}$ is called the adjusted kissing number [8] which is calculated as:

$$A'_{d_D^\perp} = \left|\{(x,y) \in (D^\perp \backslash C^\perp)^2 \mid x+y \in C^\perp,\ w_H(x) = w_H(y) = d_D^\perp\}\right|, \tag{26}$$

and where w_H denotes the Hamming weight function. Particularly, $A'_{d_D^\perp}$ depends on both linear codes $C^\perp$ and $D^\perp$, indicating that the side-channel resistance of the code-based masking relies on both codes.

Furthermore, similar with SNR in (24), the mutual information between side-channel leakage under the Hamming weight model and the sensitive variable is approximated involving both $d_D^\perp$ and $A_{d_D^\perp}$. That is, the information leakage in code-based masking can be quantified accordingly from an information-theoretic perspective [6, 8].

In summary, from a coding-theoretic perspective, (24) and (25) allow us to evaluate the residual leakage, i.e., the side-channel resistance of any code-based masking scheme by investigating the dual distance of D and the (adjusted) kissing number of D (and C). It is also worth mentioning that other terms (e.g., A_{d+1}) in weight distribution affects the residual leakage [7], especially when there is a tie on the kissing number.

3 Classical Values of the Kissing Number

From now on, we use d to denote $d_{\min}$ when there is no ambiguity.

The following observation will be used in the next three subsections. When the codewords of weight d of a q-ary code form a $2-(n,d,\lambda)$ design [13] then we have

$$A_d = \frac{n(n-1)}{d(d-1)}\lambda(q-1). \tag{27}$$

Note that all the nonzero multiples of a given codeword share the same support.

3.1 Hamming and Simplex Codes

Recall that the perfect Hamming code $C(m,q)$ over $\mathbb{F}_q$ has parameters $[\frac{q^m-1)}{(q-1)}, \frac{q^m-1)}{(q-1)} - m, 3]$. Its dual is the $[\frac{q^m-1)}{(q-1)}, m, q^{m-1}]$ simplex code. Theorem 10.15 in [13] gives the kissing number of $C(m,q)$ and its dual to be

$$A_3 = \tfrac{(q^m-1)(q^m-q)}{6}, \tag{28}$$

$$A^{\perp}_{q^{m-1}} = q^m - 1. \tag{29}$$

respectively. The second equality is immediate by observing that $C(m,q)^{\perp}$ is a one-weight code.

3.2 BCH Codes

Let $C(q,n,\delta,b)$ denote the BCH code over $\mathbb{F}_q$ of length n and designed distance δ having zeros at $\alpha^b,\ldots,\alpha^{b+\delta-2}$, with α a primitive element of order n over the algebraic closure of $\mathbb{F}_q$.

- The dual of the binary double error correcting BCH code of length 2^m-1 (primitive length) has $d = 2^{m-1} - 2^{(m-1)/2}$ (resp. $d = 2^{m-1} - 2^{m/2}$) for m odd (resp. m even) and kissing number $A_d = (2^m-1)(2^{m-2} + 2^{(m-3)/2})$ (resp $A_d = \frac{2^{(m-4)/2}}{3}(2^m-1)(2^{(m-2)/2}+1)$). See [20, pp. 451–452].
- The dual of the triple error-correcting BCH code $C(2,2^m-1,7,1)$ has minimum distance $d = \delta = 2^{m-1} - 1 - 2^{(m+1)/2}$ for m odd and kissing number given in [13, Table 7.9].
- The extended BCH code of length 2^m and designed distance $\delta = 2^{m-1} - 1 - 2^{[(m-1)/2]}$ has minimum distance $d = \delta+1$, and kissing number $A_d = (2^m-1)2^{m-1}$ for odd m. For even m its kissing number becomes $A_d = (2^{m/2}-1)2^m$.
- Let $\delta_2 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m-1}{2} \rfloor}$. Then the minimum distance of $C(q,n,\delta_2,0)$ is $\delta_2 + 1$. The kissing number is given by [13, Tables 7.3 & 7.4]

$$A_{\delta_2+1} = \begin{cases} (q-1)(q^m-1)(q^{m-1}+q^{(m-1)/2})/2 & \text{when } m \text{ is odd,} \\ (q-1)(q^{(3m-2)/2} - q^{(m-2)/2}) & \text{when } m \text{ is even.} \end{cases}$$

- Assume q is odd. Let $\delta_3 = (q-1)q^{m-1} - 1 - q^{\lfloor \frac{m+1}{2} \rfloor}$. Then the minimum distance of $C(q,n,\delta_3,0)$ is $\delta_3 + 1$. The kissing number is given in [13, Tables 7.11 & 7.12].

3.3 Reed-Muller Codes

Let q be a prime power, l and m be positive integers such that $0 \le l < (q-1)m$. The generalized Reed-Muller code over $\mathbb{F}_q$ is denoted as $\mathcal{R}_q(l,m)$.

Write l as $l = l_1(q-1) + l_0$, where l_0 and l_1 are non-negative integers, and $0 \le l_0 < q-1$. Then $\mathcal{R}_q(l,m)$ has parameters $[q^m, k, (q-l_0)q^{m-l_1-1}]$, where

$$k = \sum_{i=0}^{l} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{i - jq + m - 1}{i - jq}. \tag{30}$$

The kissing number is given by

$$A_{(q-l_0)q^{m-l_1-1}} = (q-1)\frac{q^{l_1}(q^m-1)(q^{m-1}-1)\cdots(q^{l_1+1}-1)}{(q^{m-l_1}-1)(q^{m-l_1-1}-1)\cdots(q-1)}N_{l_0} \tag{31}$$

where

$$N_{l_0} = \begin{cases} 1, & \text{if } l_0 = 0, \\ \binom{q}{l_0}\frac{q^{m-l_1}-1}{q-1}, & \text{if } 0 < l_0 < q-1. \end{cases} \tag{32}$$

See [13, p.166] for more details.

For instance, if $q = 2$, $l = 1$, we get $A_{2^{m-1}} = 2(2^m-1) = 2^{m+1}-2$, as could have been expected from the fact that binary Reed-Muller code $RM(1,m)$ is a self-complementary two-weight code. In general if $r > 2$, the full weight distribution is not known.

Besides this, if $q > 2$, the code $\mathcal{R}_q((q-1)m-2, m)$ has parameters $[q^m, q^m-m-1, 3]$ with kissing number

$$A_3 = \frac{(q-1)(q-2)(q^m-1)q^m}{6}. \tag{33}$$

See [13, p.169].

3.4 MDS Codes

By definition, an MDS code over $\mathbb{F}_q$ has parameters $[n, k, n-k+1]$. By [20], we know that

$$A_{n-k+1} = (q-1)\binom{n}{n-k+1}. \tag{34}$$

3.5 Elliptic Codes

If C is an Algebraic Geometry (AG) code constructed from an elliptic curve over $\mathbb{F}_q$, of parameters $[n, k, n-k]$ with $(k, n) = 1$, then we have

$$A_{n-k} = \frac{\binom{n}{k}(q-1)}{n}. \tag{35}$$

The full weight distribution is computed in [26, Cor. 3.2.9].

3.6 Extremal Self-Dual Codes

Let C be a binary $[n, \frac{n}{2}, d]$ even self-dual code. If C has the greatest minimum weight we could hope to attain, i.e., it achieves the bound in [13, Thm. 11.4], then C is said to be extremal. If C is an extremal self-dual code of *Type II* or *Type I* with $n \not\equiv 22 \pmod{24}$, let $\mu = [n/24]$, then C has minimum distance $d = 4\mu + 4$, and the kissing number is given by [20, Thm. 19.13]:

$$A_{4\mu+4} = \begin{cases} \binom{n}{5}\binom{5\mu-2}{\mu-1}\Big/\binom{4\mu+4}{5}, & \text{if } n = 24\mu, \\ \frac{1}{4}n(n-2)(n-4)\frac{(5\mu)!}{\mu!(4\mu+4)!}, & \text{if } n = 24\mu+8, \\ \frac{3}{2}n(n-2)\frac{(5\mu+2)!}{\mu!(4\mu+4)!}, & \text{if } n = 24\mu+16. \end{cases} \tag{36}$$

Recall that the Quadratic-Residue (QR) codes are cyclic codes of prime block length n over a field $\mathbb{F}_p$, where n is an odd prime, p is a different prime and a quadratic residue modulo n. Let $QRC_0{}^{(n,p)}$ denote the cyclic code over $\mathbb{F}_p$ of length n with generator polynomial

$$g_0(x) = \prod_{r \in Q}(x - \alpha^r), \tag{37}$$

where Q denote the set of quadratic residues modulo n, and α is a primitive pth root of unity in some field containing $\mathbb{F}_p$. The generator matrix of $QRC_0{}^{(n,p)}$ is denoted as G_i. Let $\overline{QRC_0}^{(n,p)}$ denote the extended code of $QRC_0{}^{(n,p)}$. It has the generator matrix as follows

$$\begin{bmatrix} & & & & 0 \\ & & G_i & & \vdots \\ & & & & 0 \\ 1 & 1 & \cdots & 1 & -\zeta n \end{bmatrix}$$

where $n \equiv -1 \pmod 4$ or $n \equiv 1 \pmod 4$ and $q \equiv -1 \pmod 4$, and ζ is a solution of $1 + \zeta n^2 = 0$. See more details in [13, Section 3.7].

Consider the binary code $\overline{QRC_0}^{(47,2)}$ with parameters $[48, 24, 12]$. It is an extremal self-dual code of *Type II*, see [13, Ex. 11.4]. By (36), the kissing number of C is $A_d = \binom{48}{5}\binom{8}{1}/\binom{12}{5} = 17296$.

3.7 Various Cyclic Codes

If C is an q-ary cyclic code, let α be a generator of $\mathbb{F}_{q^m}^*$ and $\mathbb{M}_{\alpha^i}(x)$ denotes the minimal polynomial of α^i over $\mathbb{F}_q$.

For $q = 2$, let C_e denote the binary cyclic code of length $n = 2^m - 1$ with generator polynomial $g_e(x) = \mathbb{M}_{\alpha}(x)\mathbb{M}_{\alpha^{1+2^e}}(x)$. Let $m \geq 4$ and $1 \leq e \leq m/2$, we have the following results:

- When $m/\gcd(m,e)$ is odd, define $h = (m - \gcd(m,e))/2$. Then the dual code $C_e^{\perp}$ has parameters $[n, 2m, 2^{m-1} - 2^{(m-1-h)/2}]$ and kissing number $A_d = 2^{h-1}(2^m - 1)(2^h + 1)$. See [13, Table 6.2].
- When m is even and $e = m/2$, then $C_e^{\perp}$ has parameters $[n, 3m/2, 2^{m-1} - 2^{(m-2)/2}]$ and kissing number $A_d = (2^{m/2} - 1)(2^{m-1} + 2^{(m-2)/2})$. See [13, Table 6.3].
- When $m/\gcd(m,e)$ is even and $1 \leq e < m/2$, then $C_e^{\perp}$ has parameters $[n, 2m, 2^{m-1} - 2^{(m+l-2)/2}]$ and kissing number is given in [13, Table 6.4].
- When $1 + 2^e$ equals to several special values which are listed in [13, p.219], then the minimum distance of $C_e^{\perp}$ is $2^{m-1} - 2^{\frac{m-1}{2}}$ and kissing number $A_d = 2^{\frac{m-3}{2}}(2^m - 1)(2^{\frac{m-1}{2}} + 1)$. See [13, Table 8.1].

For $q = 3$, let C_m denote the ternary cyclic code of length $v = (3^m - 1)/2$ with generator polynomial

$$g(x) = (x^v - 1)/((x-1)\mathrm{LCM}(\mathbb{M}_{\alpha^1}(x), \mathbb{M}_{\alpha^2}(x), \cdots, \mathbb{M}_{\alpha^{\delta-1}}(x))) \tag{38}$$

where $\delta = 3^{m-1} - 1 - \frac{3^{(m+1)/2} - 1}{2}$. Let $m \geq 3$ be odd. Then $C_m^{\perp}$ has $d = 3^{m-1} - 3^{(m-1)/2}$, and kissing number $A_d = \frac{(3^{m-1} - 3^{(m-1)/2})(3^m - 1)}{2}$, see [13, Table 8.5].

4 Linear Programming Bounds

Let C be a linear code over finite field $\mathbb{F}_q$, with length n, size $M = q^k$ for some integer k, and minimal distance d. The field size q can be any prime power. By definition, $A_0 = 1$, and

$$q^k = 1 + A_d + \sum_{j=d+1}^{n} A_j. \tag{39}$$

4.1 Numerical Method

Definition 3 (Krawtchouk Polynomial [20, Chap 5, §7]) For any prime power q and positive integer n, define the Krawtchouk polynomial

$$P_k(x;n) = P_k(x) = \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{x}{j} \binom{n-x}{k-j} \tag{40}$$

where $k = 0, 1, \ldots, n$.

The first three values for $q = 2$ are:

$$\begin{aligned} P_0(x) &= 1, \\ P_1(x) &= n - 2x, \\ P_2(x) &= n(n-1)/2 - 2nx + 2x^2. \end{aligned}$$

See [20, Chap 5, §7] for background on these polynomials, and [20, Chap 17, §4] for their use in the context of LP bounds.

For linear codes over $\mathbb{F}_q$, by MacWilliams formula for q-ary codes [20, Chap. 5, Eq. (47)] we have

$$q^k \sum_{i=0}^{n} A_i' x^{n-i} y^i = \sum_{i=0}^{n} A_i (x + (q-1)y)^{n-i} (x-y)^i \tag{41}$$

which means

$$q^k A_i' = \sum_{j=0}^{n} A_j P_i(j), \tag{42}$$

for all $i = 0, 1, \ldots, n$.

Linear programming [10] is a method to solve an optimization problem consisting of various inequalities. It is fruitful to derive bounds on the kissing number, as shown in [25]. The rest of this section is based on this reference paper.

Linear programming leads to the following theorem concerning a lower bound on the kissing number.

Theorem 1 (Lower Bound on the Kissing Number)

If C is an $[n,k,d]$ q-ary code then $A_d \geq q^k - 1 - \lfloor L \rfloor$, where L denotes the maximum of $\sum_{j=d+1}^{n} A_j$ subject to the $2n - d$ constraints

$$-P_i(0) - (q^k - 1)P_i(d) \leq \sum_{j=d+1}^{n} A_j (P_i(j) - P_i(d)) \tag{43}$$

for $i = 1, 2, \ldots, n$, and $A_j \geq 0$ for $j = d+1, d+2, \ldots, n$.

Proof By definition of A_i', we have $A_i' \geq 0$ for $i = 1, 2, \ldots, n$ which, from (42), reads $P_i(0) + A_d P_i(d) + \sum_{j=d+1}^{n} A_j P_i(j) \geq 0$. Substituting $A_d = q^k - 1 - \sum_{j=d+1}^{n} A_j$ gives (43). The Theorem is proved by using (39) again. □

We have a similar result for upper bounds.

Theorem 2 (Upper Bound on the Kissing Number)

If C is an $[n,k,d]$ q-ary code then $A_d \leq q^k - 1 - \lceil S \rceil$ where S denotes the minimum of $\sum_{j=d+1}^{n} A_j$ under the same constraints as above.

Proof The proof is similar as Theorem 1, so it is omitted. □

Consider the n inequality constraints (43)

$$-P_i(0) - (q^k - 1)P_i(d) \le \sum_{j=d+1}^{n} A_j(P_i(j) - P_i(d)). \tag{44}$$

for $i = 1, 2, \ldots, n$, along with the $n - d$ constraints $A_j \geq 0$ for $j = d+1, d+2, \cdots, n$. In this mathematical program, the A_j's are considered as rational variables if linear programming is used, or integral variables if integer programming is intended. Both approaches can be implemented in `Magma` [27].

The calculation result of the linear programming method is presented in Fig. 1 and 2 (on the next page). Here we focus on binary codes, and take different rates $R = \frac{k}{n}$ as different examples ($R \approx \frac{1}{2}$ and $R \approx \frac{1}{3}$), with d being the best known for given parameters $[n, k]$. The LP bounds are represented for n ranging from 3 to 16. We omit the cases when $k = 1$ because they are trivial situations with only two codewords. For some choices $[3, 2, 2]$, $[6, 3, 3]$, $[7, 4, 3]$, $[8, 4, 4]$, $[5, 2, 3]$, $[6, 2, 4]$, $[15, 5, 7]$ and $[16, 5, 8]$, the lower and upper bounds agree and the kissing number is necessarily unique.

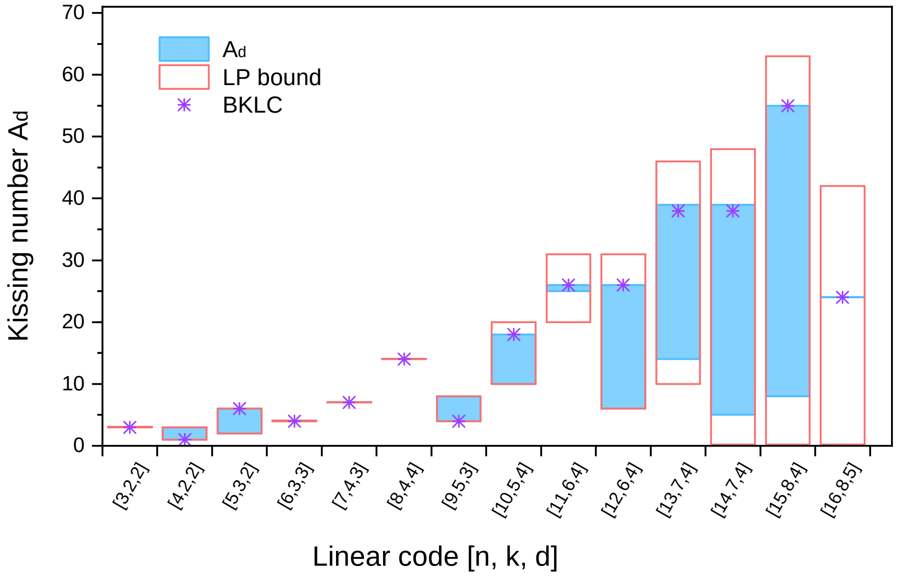

Fig. 1 The rate $R \approx \frac{1}{2}$, with d being the best known for given parameters $[n, k]$. The LP bounds are represented for n ranging from 3 to 16.

However, in general, the lower and upper bounds do not agree, and it is possible to find actual codes with different kissing numbers between those bounds, as rep-

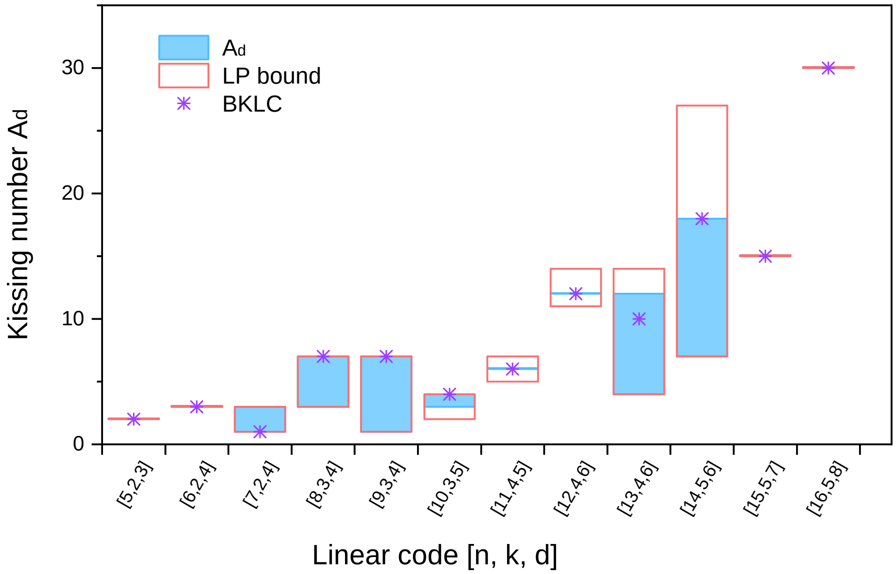

Fig. 2 Take $R \approx \frac{1}{3}$, with d being the best known for given parameters $[n, k]$. The LP bounds are represented for n ranging from 5 to 16.

resented in light blue color in Fig. 1 and 2. Our experiments have been carried out by randomly selecting linear codes of parameters $[n, k, d]$ and the range displayed in blue correspond to actually discovered codes amongst the ones we explored. Our search could not be exhaustive so that there might exist codes with lower or higher kissing numbers. Some exceptions are when:

- $[n, k, d] = [8, 4, 4]$ and $[16, 8, 5]$, as those are unique codes (extended Hamming code [20] and shortened QR code [20]). The uniqueness of the latter is proven in [4].
- $[n, k, d] \in \{[3, 2, 2], [6, 3, 3], [7, 4, 3], [5, 2, 3], [6, 2, 4], [11, 4, 5], [12, 4, 6], [15, 5, 7], [16, 5, 8]\}$, as the room between lower and upper bounds is limited.

We also superimposed in Fig. 1 and 2 the special case of `Magma` Best Known Linear Code (BKLC). The function BKLC(n,d) returns a code with the largest known dimension, for a given length and minimum distance, consistently with Grassl database [15], which favors codes obtained by some algebraic construction. On several occasions, especially for rate 1/2 codes, the kissing number of BKLC is relatively high, hence `Magma` is not adapted to applications requiring a small kissing number.

4.2 Polynomial Method

The following identity is a polynomial way of expressing the duality of LP.

Lemma 1 (Polynomial Method [12, Eq. (18)])
Let $\beta(x) \in \mathbb{Q}[x]$ denote a polynomial with Krawtchouk expansion

$$\beta(x) = \sum_{j=0}^{n} \beta_j P_j(x). \tag{45}$$

The following identity holds

$$\sum_{i=0}^{n} \beta(i) A_i = q^k \sum_{j=0}^{n} \beta_j A'_j. \tag{46}$$

Proof Immediate by (42), upon swapping the order of summation. □

4.2.1 Lower Bounds

Using Lemma 1 we have the following theorem. This theorem can also be obtained by setting appropriate parameters in [1, Thm 1].

Theorem 3 (Lower Bound [1])
Let $\beta(x) \in \mathbb{Q}[x]$ satisfying

$$\beta_j \geq 0, \forall j = 0, 1, \ldots, n, \tag{47}$$
$$\beta(x) \leq 0, \forall x \in (d, n], \tag{48}$$
$$\beta(d) > 0, \tag{49}$$
$$q^k \beta_0 > \beta(0). \tag{50}$$

Then we have the lower bound

$$A_d \geq \frac{q^k \beta_0 - \beta(0)}{\beta(d)}. \tag{51}$$

Proof By Lemma 1 we have

$$\beta(0) + A_d \beta(d) + \sum_{i=d+1}^{n} \beta(i) A_i = q^k (\beta_0 + \sum_{j=1}^{n} \beta_j A'_j).$$

Combined with (47) and (48), it implies the following inequality:

$$\beta(0) + A_d \beta(d) \geq q^k \beta_0.$$

It gives a non-trivial lower bound on kissing number as long as (49) and (50) hold.□

The main result of this paragraph are the following corollaries. First, we consider the case of β being linear.

Corollary 1 *If* $d = [(n-1)(q-1)/q]$, *then*

$$A_d \geq \frac{q^k - nq + n - 1}{(n-d)q - n + 1}. \tag{52}$$

Proof Take $\beta(x) = nq - n + 1 - qx$, where $P_1(x) = (q-1)n - qx$. By construction $\beta_0 = \beta_1 = 1$. Note that $\beta(0) = nq - n + 1$, and $\beta(d) = nq - n + 1 - qd$. We see that $\beta(x) \leq 0$, for x an integer $\geq \frac{nq-n+1}{q}$. So in order to satisfy $\beta(x) \leq 0$, $\forall x \in (d, n]$, we must have $d + 1 \geq \frac{nq-n+1}{q}$. Combined with $\beta(d) > 0$ we have $(q-1)(n-1) \leq qd < (q-1)(n-1) + q$. Plugging this data into Theorem 3, the result follows. □

Next, we consider the case of β being a quadratic polynomial.

Corollary 2 *If* $qd > nq - n - 2q + 1$ *then*

$$A_d \geq \frac{q^{k-2}n(n - qn + qd + 2q - 1) - nd - n}{n - d}. \tag{53}$$

Proof Assume $\beta = 1 + \beta_1 P_1(x) + \beta_2 P_2(x)$. Here $P_2(x) = \frac{q^2}{2}x^2 + \frac{q(q-2nq+2n-2)}{2}x + (q-1)^2\binom{n}{2}$. To ensure the negativity of β for $x \in (d, n]$ the simplest is to assume $\beta(d+1) = \beta(n) = 0$. This gives a system of two equations in β_1, β_2. The solution according to `Magma` [27] is

$$\beta_1 = \frac{nq - 2n - dq - 2q + 2}{n(n - qn + qd + 2q - 1)}, \beta_2 = \frac{-2}{n(n - qn + qd + 2q - 1)}.$$

This yields $\beta(d) = \frac{q^2(n-d)}{n(n-qn+qd+2q-1)}$, and $\beta(0) = \frac{q^2(d+1)}{(n-nq+qd+2q-1)}$. The result follows by Theorem 3. □

Example Consider the binary code $C = RM(1, m)$, when $k = m+1$, and $d = 2^{m-1}$. It is well-known that C is a two-weight code with $A_0 = A_{2^m} = 1$, and $A_{2^{m-1}} = 2^{m+1} - 2$. Since $2d - n + 3 > 0$, using Corollary 2 we have $A_d \geq 2^{m+1} - 2$. So $RM(1, m)$ meets the lower bound.

This result can be improved in some cases.

Corollary 3 *If C is a binary code and all weights of C lie in the range [d, n-d], with distance* $d < \frac{n}{2}$ *and* $(n - 2d - 1)^2 < n + 1$, *then*

$$A_d \geq \frac{2^{k-2}(n^2 - 4nd - 3n) + (2^k + 1)d(d+1)}{(2d - n)} - d - 1. \tag{54}$$

Proof Because all weights of C lie in the range [d, n-d], for a quadratic β, to ensure its negativity on the weights it is enough to assume $\beta(d+1) = \beta(n-d) = 0$. This gives a system of two equations in β_1, β_2, if we write $\beta = 1 + \beta_1 P_1(x) + \beta_2 P_2(x)$. The solution according to `Magma` [27] is

$$\beta_1 = \beta_2 = \frac{2}{n+1-(n-2d-1)^2}$$

This yields $\beta(d) = \frac{-4n+8d}{n^2-4nd-3n+4d^2+4d}$, and $\beta(0) = \frac{4(d^2+d-nd-n)}{n^2-4nd-3n+4d^2+4d}$. The result follows by Theorem 3. □

4.2.2 Upper Bounds

Like Theorem 3, the following theorem can also be obtained by setting appropriate parameters in [1, Thm 1].

Theorem 4 (Upper Bound [1])
Let $\beta(x) \in \mathbb{Q}[x]$ satisfying

$$\beta_j \leq 0, \forall j = 1, \ldots, n, \tag{55}$$

$$\beta(x) \geq 0, \forall x \in (d, n], \tag{56}$$

$$\beta(d) > 0, \tag{57}$$

$$q^k \beta_0 > \beta(0). \tag{58}$$

Then we have the upper bound

$$A_d \leq \frac{q^k \beta_0 - \beta(0)}{\beta(d)}. \tag{59}$$

The proof is analogous to that of Theorem 3 and is omitted.

The main result of this paragraph are the following corollaries. First, we consider the case of β linear.

Corollary 4 *If $n - nq + 1 + qd > 0$, then*

$$A_d \leq \frac{q^k + nq - n - 1}{n - nq + 1 + qd}. \tag{60}$$

Proof Take $\beta(x) = n - nq + 1 + qx$, where $P_1(x) = (q-1)n - qx$. By construction $\beta_0 = 1$, and $\beta_1 = -1$. Note that $\beta(0) = n - nq + 1$, and $\beta(d) = n - nq + 1 + qd$. We see that $\beta(x) > 0$, for x an integer $> \frac{n-nq+1}{q}$. Plugging this data into Theorem 4, the result follows. □

Next, we consider the case of β being a quadratic polynomial.

Corollary 5 *If $d < \frac{(q-1)n+1}{q}$, then*

$$A_d \leq \frac{q^{k-2} n(qn - n - qd + 1) + n(d-1)}{n-d}. \tag{61}$$

Proof Assume $\beta = 1 - \beta_1 P_1(x) - \beta_2 P_2(x)$, with β_1, $\beta_2 > 0$. To ensure the positivity of β for $x \in (d, n]$ the simplest is to assume $\beta(d-1) = \beta(n) = 0$. This gives a system of two equations in β_1, β_2. The solution according to `Magma` [27] is

$$\beta_1 = \frac{2n + dq - 2 - nq}{qn^2 - n^2 - qdn + n}, \beta_2 = \frac{2}{qn^2 - n^2 - qdn + n}.$$

This yields $\beta(d) = \frac{q^2(n-d)}{qn^2-n^2-qdn+n}$, and $\beta(0) = \frac{q^2(1-d)}{qn-n-qd+1}$. The result follows by Theorem 4. □

Example Still consider the binary code $C = RM(1, m)$, where $n = 2^m$, $k = m + 1$, and $d = 2^{m-1}$. Using Corollary 5, we have $A_d \leq 2^{m+1} - 2$. From Corollary 2 we know $A_d \geq 2^{m+1} - 2$. So $A_d = 2^{m+1} - 2$. Because $A_0 = 1$, it proved that $RM(1, m)$ is a two-weight code. $RM(1, m)$ is the only code we know that satisfies the upper bound and the lower bound at the same time.

This result can be improved in some cases.

Corollary 6 *If C is a binary code and all weights of C lie in the range [d, n-d], with* $n - 2d > 0$ *and* $(n - 2d + 2)^2 > n$, *then*

$$A_d \leq \frac{2^{k-2}\big((n - 2d + 2)^2 - n\big) + (d - 1)(n + 1 - d)}{n + 1 - 2d}. \tag{62}$$

Proof For a quadratic β, of concavity $\cap$, to ensure its positivity on the weights it is enough to assume $\beta(d-1) = \beta(n-d+1) = 0$.

This gives a system of two equations in β_1, β_2, if we write $\beta = 1 - \beta_1 P_1(x) - \beta_2 P_2(x)$. The solution according to `Magma` [27] is

$$\beta_1 = 0, \beta_2 = \frac{2}{(n - 2d + 2)^2 - n}$$

This yields $\beta(0) = \frac{4(d-1)(d-n-1)}{(n-2d+2)^2-n}$ and $\beta(d) = \frac{4(1-2d+n)}{(n-2d+2)^2-n}$. The result follows then by Theorem 4. □

5 Eigenvalue Bounds

Let C be a q-ary code with parameters $[n, k, d]$. The *coset graph* $\Gamma(C)$ of a code C is then the graph defined on the q^{n-k} cosets, two of them being connected if they differ by a coset of weight one. We give without proof the following theorem of [5, 11.1.11].

Lemma 2 *If C is a q-ary code of minimum distance at least three, with dual weight distribution* $[\langle i, A_i \rangle]$, *then the spectrum of the adjacency matrix of* $\Gamma(C)$ *is* $\{(n(q-1) - qi)^{A_i}\}$. *Thus* A_i *is the frequency of weight i in* $C^\perp$ *and the multiplicity of the eigenvalue* $(q-1)n - qi$.

Theorem 5 *If C is a q-ary code with parameters $[n, k, d]$ with $\frac{n(q-1)}{q} > d$ and dual distance ≥ 3, then $A_d \leq q^k - 2 - 2n(q-1) + 2qd$.*

Proof Apply [22, thm 4] to the graph $\Gamma(C^{\perp})$ along with Lemma 2. □

Denote by $V(C, r)$ the volume of the ball of radius r in $\Gamma(C^{\perp})$. It is immediate that $V(C, r) \leq B(n, q, r)$ where $B(n, q, r)$ denotes the volume of the Hamming ball of radius r in length n over an alphabet of size q. As is well-known

$$B(n, q, r) = \sum_{j=0}^{r} \binom{n}{j} (q-1)^j. \tag{63}$$

Theorem 6 *If C is a q-ary code with parameters $[n, k, d]$ with dual distance ≥ 3, then $A_d + 1 \geq q^k / B(n, q, \lceil \frac{\cosh^{-1}(q^k)}{\cosh^{-1}(\frac{2+\lambda_1}{2-\lambda_1})} \rceil)$ with $\lambda_1 = \frac{qd}{n(q-1)}$.*

Proof The expression for the first nontrivial element of the Laplacian spectrum λ_1 follows by combining Lemma 1 with the expression at the end of [9, §2]. Apply Corollary 3 of [9] with $k = 1$ in the graph $\Gamma(C^{\perp})$, which is regular of degree $n(q-1)$ on q^k vertices. The proof follows then by the same argument as that of Theorem 5 of [9]. □

Table 1 Upper/Lower Bounds for some Linear Codes

Binary code	Eigenvalue bound of A_d		LP bound of A_d	
$[n, k, d]$	Lower bound	Upper bound	Lower bound	Upper bound
$[5, 3, 2]$	−0.5000	4	2	6
$[7, 4, 3]$	−0.7500	12	7	7
$[9, 5, 3]$	−0.8750	24	4	8
$[10, 5, 4]$	−0.8182	26	10	20
$[11, 6, 4]$	−0.8861	56	20	31
$[12, 6, 4]$	−0.9194	54	6	31
$[13, 7, 4]$	−0.9462	116	10	46
$[14, 7, 4]$	−0.9631	114	0	48
$[15, 8, 4]$	−0.9743	240	0	63
$[16, 8, 5]$	−0.9628	242	0	42
$[9, 3, 4]$	−0.8261	4	1	7
$[11, 4, 5]$	−0.9310	12	5	7
$[13, 4, 6]$	−0.9577	12	4	14
$[14, 5, 6]$	−0.9319	26	7	27
$[15, 5, 7]$	−0.9444	28	15	15

Tab. 1 contains the results of binary codes. It shows the eigenvalue bounds and the LP bounds for the same binary codes as those used in Fig. 1 and 2. Because Thm. 5 and 6 hold only when $n > 2d$, some codes in Fig. 1 and 2 that do not satisfy this condition are not presented in this table.

As we can see from the table, the LP bound is more precise in general than the eigenvalue bound. However, for some values (namely $[5, 3, 2]$ and $[9, 3, 4]$), the eigenvalue method leads to a tighter upper bound. We should notice that compared to the LP bound, the eigenvalue bound has one more constraint: the dual distance of the code should be no less than 3.

6 Conclusions and perspectives

The kissing number is an important invariant of codes. We illustrate several situations where it is the dominating factor influencing system's properties. Namely, it is instrumental in determining codes performances, with applications in implementation-level security leveraging code-based masking to thwart side-channel attacks. We compute its values for some important codes, and derive upper and lower bounds in general, using linear programming techniques. We provide both analytical and numerical bounds. To the best of our knowledge, such compilation has never been carried out previously.

As a perspective, we note it would be beneficial to relate the code design to its kissing number (especially since codes with structures are, in general, not those with small kissing number). Besides, there is a need to build codes of optimal minimum distance while at the same time featuring a small kissing number.

There are two main open problems.

Firstly, the definition of the kissing number should be extended to other metrics that have been used in Coding Theory, like the Lee metric, or, more recently, the poset metrics [17, Ch. 22]. One technical difficulty is that the Lee association scheme, unlike the Hamming association scheme is not P-polynomial [24]. This makes the LP bounds less easy to establish.

Secondly, the results described so far have been about exact values of the kissing number. It would be insightful to give asymptotic lower and upper bounds of A_d when the code considered ranges over a family of codes of relative distance $\delta \in (0, 1)$, with $d \sim \delta n$ for $n \to \infty$. The existence result of [2] maximizes the kissing number, when our security application demands to minimize it.

Recent results on graph eigenvalues [19] might turn out to be relevant. The asymptotic properties of zeros of Krawtchouk polynomials may play a role in the LP bound similar to their use in the bound of McEliece, Rodemich, Rumsey, and Welch [21].

References

1. A. Ashikmin, A. Barg, and S. Litsyn, “Estimates on the distance distribution of Codes and Designs,” *IEEE Trans. on Information Theory*, Vol. IT-47, 2001. 1056–1061.
2. A. Ashikmin, A. Barg, and S. G. Vladut, “Linear Codes with Exponentially Many Light Vectors,” *J. Comb. Theory, Ser. A*, vol. 96, pp. 396-399, 2001.
3. S. Benedetto and E. Biglieri, *Principles of Digital Transmission: With Wireless Applications*, Kluwer Academic Publishers, 2002.
4. K. Betsumiya and M. Harada, “Binary optimal odd formally self-dual codes,” *Des. Codes Cryptography*, Vol. 23, No. 1, pp. 11–22, 2001. http://www.math.nagoya-u.ac.jp/ koichi/paper/fsd-odd.pdf.
5. A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs*. Berlin: Springer-Verlag, 1989,
6. W. Cheng, S. Guilley, C. Carlet, S. Mesnager, and J.-L. Danger. Optimizing Inner Product Masking Scheme by a Coding Theory Approach. *IEEE Trans. Inf. Forensics Secur.*, 16:220–235, 2021.
7. W. Cheng, Y. Liu, S. Guilley and O. Rioul, Towards finding best linear codes for side-channel protections, in Proc. 10th International Workshop on Security Proofs for Embedded Systems (PROOFS’2021), Beijing, China, Sept. 17, 2021.
8. W. Cheng, S. Guilley, C. Carlet, J.-L. Danger, and S. Mesnager. Information leakages in code-based masking: A unified quantification approach. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(3):465–495, 2021.
9. F. Chung, C. Delorme, P. Solé, Multidiameters and Multiplicities, Europ. J. Combinatorics **20**, (1999), 629–640.
10. Vašek Chvátal, *Linear Programming*, W. H. Freeman, New York, 1983; 478 pages.
11. J. Conway and N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer, G.T.M. 290 (second edition), 1993.
12. P. Delsarte, “Bounds on unrestricted codes, by linear programming,” *Philips Res. Repts*, vol. 27, 1972
13. C. Ding, *Designs from Linear Codes*, Singapore: World Scientific, 2018.
14. G.D Forney, G. Ungerboeck, Modulation and Coding for Linear Gaussian Channels, IEEE Trans. on Information Theory, Vol. 44, No. 6, Oct. 1998, 2384–2415.
15. M. Grassl, “Bounds on the minimum distance of linear codes and quantum codes,” Online available at http://www.codetables.de/, 2007, accessed on 2012-07-23.
16. W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge Univ. Press, 2003.
17. W. C. Huffman, J.-L. Kim, P. Solé, *Concise Encyclopedia of Coding Theory*, (1st ed.), Chapman and Hall/CRC, 2021
18. Y. Ishai, A. Sahai and D. Wagner, *Private Circuits: Securing Hardware against Probing Attacks*, CRYPTO 2003, pp. 463-481, Springer LNCS 2729.

19. Z. Jiang, J. Tidor, Y. Yao, S. Zhang, Y. Zhao, “Equiangular lines with a fixed angle”, 2019, arXiv preprint, arXiv:1907.12466.
20. F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland (1977).
21. R. J. McEliece, E. R. Rodemich, H. Rumsey, and L. R. Welch, “New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities”, *IEEE Trans. on Information Theory*, vol. 23, pp. 157-166, 1977
22. D.L. Powers, Graph partitioning by eigenvectors, Linear Algebra and its Appl. **101**, (1988), 121–133.
23. M. Rivain and E. Prouff, *Provably Secure Higher-Order Masking of AES*, CHES 2010, pp. 413-427, Springer LNCS 6225.
24. P. Solé, The Lee Association Scheme, in Proc. Coding Theory and Applications, 2nd International Colloquium, Cachan-Paris, France, Nov. 24-26, 1986.
25. P. Solé, Y. Liu, W. Cheng, S. Guilley, and O. Rioul, "Linear programming bounds on the kissing number of q-ary codes," in Proc. 2021 IEEE Information Theory Workshop (ITW2021), Kanazawa, Japan, Oct. 17-21, 2021.
26. M. Tsfasman, S. Vladut, *Algebraic Geometric codes*, Kluwer (1991).
27. University of Sydney (Australia). Magma Computational Algebra System. http://magma.maths.usyd.edu.au/magma/, Accessed on 2021-01-08.
28. A. J. Viterbi and J. K. Omura, *Principles of Digital Communication and Coding*, McGraw Hill, 1979.
29. W. Wang, P. Méaux, G. Cassiers and F.-X. Standaert, *Efficient and Private Computations with Code-Based Masking*, IACR Trans. Cryptogr. Hardw. Embed. Syst., 2020, number 2, pp. 128-171, Springer.